Visualizar processo

1101330 - Disputa Encerrada

Instrumento Convocatório
044/2026

Número do Processo
528/2026

Modalidade
Pregão

Critério de disputa
Menor preço

Pregoeiro
DIANE SANTOS PINHEIRO

Prazo para impugnação
5 dias

Participação do fornecedor
Ampla

Equalização ICMS
SEM ICMS

Data de publicação
24/09/2026

Início do acolhimento de propostas
24/09/2026
08:00

Limite do acolhimento de propostas
20/10/2026
08:30

Data e hora da disputa
20/10/2026
08:30

Lotes

LOTE	VALOR ESTIMADO	VALOR ARREMATADO
Lote 1	R$ 3.540.730,00	R$ 3.297.050,00

Mostrar tudo

Mostrando 1-1 de 1 item 1

• Dados PNCP

Link PNCP
Visualizar Publicação PNCP

Id PNCP
13018171000190-1-000011/2026

Documentos anexos

PROCESSO | FORNECEDORES

- EDITAL44.2026.pdf
  23/09/2026 07:16:20
  Baixar
- TERMO_REFERENCIA.pdf
  23/09/2026 07:16:34
  Baixar

VOLTAR

Uma solução

Os números do suporte técnico são:
• 4004 0001 - Capitais e Regiões Metropolitanas
• 0800 729 0001 - Demais localidades
Escolhendo pela ordem a

Contato SAC BB | 0800 729 0722
Ouvidoria | 0800 729 5678

Banco do Brasil

seguinte sequência de opções numéricas:
• 5 – Múltiplos atendimentos > 5 – Suporte Técnico > 6 – Licitações

Deficientes auditivos/fala | 0800 729 0088

Dúvidas Frequentes

Política de privacidade

Licitações-e © Banco do Brasil - v1.73.1

TRIBUNAL DE CONTAS DA UNIÃO

Consulta Consolidada de Pessoa Jurídica

Este relatório tem por objetivo apresentar os resultados consolidados de consultas eletrônicas realizadas diretamente nos bancos de dados dos respectivos cadastros. A responsabilidade pela veracidade do resultado da consulta é do Órgão gestor de cada cadastro consultado. A informação relativa à razão social da Pessoa Jurídica é extraída do Cadastro Nacional da Pessoa Jurídica, mantido pela Receita Federal do Brasil.

Consulta realizada em: 21/10/2026 11:35:54

Informações da Pessoa Jurídica:

Razão Social: **JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA**
CNPJ: **24.425.034/0001-96**

Resultados da Consulta Eletrônica:

Órgão Gestor: **TCU**
Cadastro: **Licitantes Inidôneos**
Resultado da consulta: **Nada Consta**

Para acessar a certidão original no portal do órgão gestor, clique AQUI.

Órgão Gestor: **CNJ**
Cadastro: **CNIA - Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade**
Resultado da consulta: **Sistema do CNJ está indisponível**

Para acessar a certidão original no portal do órgão gestor, clique AQUI.

Órgão Gestor: **Portal da Transparência**
Cadastro: **Cadastro Nacional de Empresas Inidôneas e Suspensas**
Resultado da consulta: **Nada Consta**

Para acessar a certidão original no portal do órgão gestor, clique AQUI.

Órgão Gestor: **Portal da Transparência**
Cadastro: **CNEP - Cadastro Nacional de Empresas Punidas**
Resultado da consulta: **Nada Consta**

Para acessar a certidão original no portal do órgão gestor, clique AQUI.

Obs: A consulta consolidada de pessoa jurídica visa atender aos princípios de simplificação e racionalização de serviços públicos digitais. Fundamento legal: Lei nº 12.965, de 23 de abril de 2014, Lei nº 13.460, de 26 de junho de 2017, Lei nº 13.726, de 8 de outubro de 2018, Decreto nº 8.638 de 15, de janeiro de 2016.

GOVERNO DE SERGIPE

SECRETARIA ESPECIAL DE GESTÃO DAS CONTRATAÇÕES, LICITAÇÕES E LOGÍSTICA.

CADFIMP - Cadastro de Fornecedores Impedidos de Licitar e Contratar com a Administração Pública Estadual (Instituído pelo Decreto nº 24.912 de 20 de dezembro de 2007)

** NADA CONSTA **

Data da consulta: 21/10/2026 11:37:12

EMPRESA OU PESSOA SANCIONADA

CNPJ: 24.***.***/0001-96
Nome fantasia: JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA
Razão Social: JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA

NÃO CONSTA, EM NOSSO CADASTRO, COM NENHUMA RESTRIÇÃO DE CONTRATAR COM A ADMINISTRAÇÃO PÚBLICA

Link do sistema: https://sistema.comprasnet.se.gov.br/v2/cadfim.aspx

Fornecedores Penalizados

24.425.034/0001-96

01/01/2010 - 21/10/2026

Pesquisar

Listado registro 0 até 0 de 0

Empresa	Penalidade	Base Legal	Prazo de Impedimento

Certidão Negativa

Certifico que nesta data (23/10/2026 às 08:44) NÃO CONSTA no Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade registros de condenação com trânsito em julgado ou sanção ativa quanto ao CNPJ nº 24.425.034/0001-96.

A condenação por atos de improbidade administrativa não implica automático e necessário reconhecimento da inelegibilidade do condenado.
Para consultas sobre inelegibilidade acesse portal do TSE em http://divulgacandcontas.tse.jus.br/

Esta certidão é expedida gratuitamente. Sua autenticidade pode ser por meio do número de controle 6GTA.695I.9LFN.E17V no seguinte endereço: https://www.cnj.jus.br/improbidade_adm/autenticar_certidao.php

PROPOSTA COMERCIAL

À COMPANHIA DE SANEAMENTO DE SERGIPE – DESO

Referência: PREGÃO ELETRÔNICO Nº 44/2026 – DESO

JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, pessoa jurídica de direito privado, inscrita no CNPJ/MF sob o nº 24.425.034/0001-96, portadora da inscrição estadual nº 0776048100140, sediada no SCES Trecho 2, Centro de Lazer Beira Lago, Conj 08, Loja 03, Asa Sul, Brasília/DF, CEP: 70.200-002, por meio de seu representante legal José André Mendes Coimbra, brasileiro, solteiro, sócio-diretor, inscrito no CPF/MF sob o nº 471.539.891-53, vem, apresentar, proposta para contratação de solução de detecção e resposta a incidentes, auditoria e proteção de dados, detecção e resposta a ame aças baseadas em dados, coleta de fluxos de meta dados, e analise constante de dados e de seus repositórios de dados corporativos, plataforma de compartilhamento colaborativo, incluindo prestação de serviço de instalação e configuração, com garantia técnica de 12 (doze meses) meses, com treinamento para capacitação de técnicos da companhia de saneamento de Sergipe e serviço de operação assistida e apoio operacional, conforme condições, quantidades e exigências estabelecidas no edital referente ao PE nº 044/2026 (Processo Administrativo e-Doc nº 528/2026)

ITEM	DESCRIÇÃO	UND	QTDE	VALOR UNITÁRIO	VALOR TOTAL
1	Licença de uso de software de auditoria e controle de ameaças sobre dados não estruturados on premise, com treinamento, instalação e suporte por 12 meses.	Usuários	1000	R$ 1.691,56	R$ 1.691.560,00
2	Licença de uso de software de auditoria e controle de ameaças sobre dados não estruturados armazenados em serviço de nuvem, com treinamento, instalação e suporte por 12 meses.	Usuários	1000	R$ 1.377,26	R$ 1.377.260,00
VALOR TOTAL DO LOTE					**R$ 3.068.820,00**

Valor total: R$ 3.068.820,00 (Três milhões, sessenta e oito mil, oitocentos e vinte reais).

Prazo de Validade da Proposta será de: **90 (noventa) dias.**

Prazo de entrega dos produtos será de: **até 30 (trinta) dias**.

Prazo de Garantia dos equipamentos de no mínimo **12 (doze) meses**, contra qualquer defeito de fabricação, instalação e desempenho, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

Modalidade de garantia contratual: **Seguro-garantia.**

Nos preços propostos estão inclusos todos os custos necessários para o atendimento do objeto da licitação, bem como todos os impostos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, deslocamentos de pessoal, treinamento, garantia, montagem, instalação, eventuais materiais e equipamentos, e quaisquer outros que incidam ou venham a incidir sobre o objeto licitado constante da proposta;

Dados Bancários:

Banco: SICOOB (756)
Agência: 5004
Conta corrente: 1.021.449-6

DESCRIÇÃO DO OBJETO

O **Varonis DataAdvantage** é uma solução de segurança e governança de dados projetada para ambientes de dados não estruturados. Ele permite que as organizações protejam, monitorem e gerenciem seus dados armazenados em plataformas SaaS e on-premise, garantindo conformidade, segurança e eficiência operacional.

Principais Funcionalidades

1. Visibilidade e Controle de Dados:

o Mapeamento de Dados: Identifica e mapeia dados sensíveis armazenados em repositórios não estruturados.

o Análise de Permissões: Avalia e gerencia permissões de acesso para garantir que apenas usuários autorizados tenham acesso a informações críticas.

o Auditoria: Coleta de telemetria e acesso de contas aos dados monitorados para investigação de eventos ocorridos no ambiente.

2. Segurança e Conformidade:

o Detecção de Ameaças Internas: Monitora atividades suspeitas e potenciais ameaças internas, como acesso não autorizado ou transferência de dados sensíveis.

o **Conformidade Regulatória:** Facilita a conformidade com regulamentações como LGPD, PII, SOX, entre outras, através de relatórios e auditorias detalhadas.

3. Gestão de Acessos e Direitos:
o **Automação de Políticas de Acesso:** Implementa políticas de acesso baseadas em funções e necessidades de negócio, reduzindo riscos de acessos excessivos.
o **Revisões de Acesso:** Simplifica o processo de revisão e certificação de acessos, garantindo que as permissões estejam sempre atualizadas e adequadas.

4. Análise e Relatórios Avançados:
o **Dashboards Personalizáveis:** Fornece visualizações intuitivas e personalizáveis sobre o estado da segurança e conformidade dos dados.
o **Relatórios Detalhados:** Gera relatórios abrangentes para auditorias internas e externas, facilitando a demonstração de conformidade e práticas de segurança.

A solução proposta já contempla serviço de investigação e resposta a incidentes ofertado pelo fabricante assim como o serviço de apoio operacional pela Contratada de forma a garantir melhor uso da solução, conforme descrito no Termo de Referência e suas especificações técnicas.

Esta proposta contempla todo o treinamento conforme exigido no Edital e seus anexos.

O treinamento oficial do fabricante da solução será ofertado de acordo com a ementa e todo o material disponibilizado e aprovados pelo fabricante, garantindo, assim, a conformidade e a adequação às normas e padrões estabelecidos pela VARONIS.

Anexamos a esta proposta a grade de treinamentos oficial do fabricante, incluindo a ementa detalhada do curso, como forma de comprovação de que o treinamento ofertado atende integralmente aos requisitos indicados no item 6.4.2.12 do TR e que as datas de realização do Treinamento serão cumpridas conforme as condições a serem acordadas.

DECLARAÇÃO DE CONFORMIDADE COM NORMAS DE SEGURANÇA DA INFORMAÇÃO E CERTIFICAÇÕES

Em conformidade com os requisitos estabelecidos no item 5.1 do documento contratual, declaramos que a solução proposta para proteção de dados sensíveis e análise comportamental de usuários em ambiente de nuvem está devidamente certificada de acordo com as normas e padrões internacionais relevantes para garantir a segurança, privacidade e integridade das informações. As certificações que comprovam essa conformidade são as seguintes:

1. **ISO/IEC 27017** – Certificação em **Segurança de Serviços em Nuvem**, que estabelece diretrizes específicas para controles de segurança em serviços de computação em nuvem, assegurando a proteção dos dados processados nesse ambiente.
2. **ISO/IEC 27018** – Certificação em **Proteção de Dados Pessoais em Nuvem**, que define diretrizes para a proteção de dados pessoais armazenados e processados em ambientes de nuvem, atendendo aos requisitos legais de privacidade e segurança.
3. **ISO/IEC 27701** – Certificação em **Gestão da Privacidade da Informação**, que complementa a ISO/IEC 27001 e orienta sobre a implementação e manutenção de controles de privacidade dentro da organização, com foco na proteção de dados pessoais e conformidade com legislações de privacidade, como o GDPR.
4. **SOC 2 e SOC 3** – Certificações que validam a conformidade com os princípios de **segurança, confidencialidade, disponibilidade, privacidade e integridade das informações**, por meio de auditorias independentes. A certificação SOC 2 inclui relatórios detalhados e internos, enquanto a SOC 3 disponibiliza um relatório resumido, acessível publicamente, para comprovar o cumprimento dos controles de segurança e privacidade.

Confirmamos que todas as certificações mencionadas estão em vigor e que a solução proposta adota as melhores práticas de segurança da informação e proteção de dados sensíveis, garantindo a conformidade com as normas internacionais de segurança e privacidade, tais declarações podem ser consultadas através do seguinte link: https://www.varonis.com/trust

Brasília, 22 de outubro de 2026

JOSE ANDRE MENDES COIMBRA:47153989153

Assinado de forma digital por JOSE ANDRE MENDES COIMBRA:47153989153
Dados: 2026.10.22 11:21:12 -03'00'

JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA
Sócio-diretor: José André Mendes Coimbra
CPF: 471.539.891-53 / RG: 1179715 - SSP/DF

REPÚBLICA FEDERATIVA DO BRASIL
CADASTRO NACIONAL DA PESSOA JURÍDICA

COMPROVANTE DE INSCRIÇÃO E DE SITUAÇÃO CADASTRAL

NÚMERO DE INSCRIÇÃO	DATA DE ABERTURA
24.425.034/0001-96 MATRIZ	21/03/2016

NOME EMPRESARIAL
JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA

TÍTULO DO ESTABELECIMENTO (NOME DE FANTASIA)	PORTE
PETA	DEMAIS

CÓDIGO E DESCRIÇÃO DA ATIVIDADE ECONÔMICA PRINCIPAL
62.03-1-00 - Desenvolvimento e licenciamento de programas de computador não-customizáveis

CÓDIGO E DESCRIÇÃO DAS ATIVIDADES ECONÔMICAS SECUNDÁRIAS
47.51-2-01 - Comércio varejista especializado de equipamentos e suprimentos de informática
62.01-5-01 - Desenvolvimento de programas de computador sob encomenda
62.02-3-00 - Desenvolvimento e licenciamento de programas de computador customizáveis
62.04-0-00 - Consultoria em tecnologia da informação
62.09-1-00 - Suporte técnico, manutenção e outros serviços em tecnologia da informação
63.99-2-00 - Outras atividades de prestação de serviços de informação não especificadas anteriormente
74.90-1-04 - Atividades de intermediação e agenciamento de serviços e negócios em geral, exceto imobiliários
77.33-1-00 - Aluguel de máquinas e equipamentos para escritórios

CÓDIGO E DESCRIÇÃO DA NATUREZA JURÍDICA
206-2 - Sociedade Empresária Limitada

LOGRADOURO	NÚMERO	COMPLEMENTO
TR SCES TRECHO 2, CENTRO DE LAZER BEIRA LAGO	03	CONJ 08 LOJA 03

CEP	BAIRRO/DISTRITO	MUNICÍPIO	UF
70.200-002	ASA SUL	BRASILIA	DF

ENDEREÇO ELETRÔNICO	TELEFONE
JURIDICO@PETACORP.COM.BR	(61) 2017-0771

ENTE FEDERATIVO RESPONSÁVEL (EFR)
*****

SITUAÇÃO CADASTRAL	DATA DA SITUAÇÃO CADASTRAL
ATIVA	21/03/2016

MOTIVO DE SITUAÇÃO CADASTRAL

SITUAÇÃO ESPECIAL	DATA DA SITUAÇÃO ESPECIAL
********	********

Aprovado pela Instrução Normativa RFB nº 2.119, de 06 de dezembro de 2022.
Emitido no dia 15/10/2026 às 15:02:57 (data e hora de Brasília).

CADASTRO FISCAL DO DISTRITO FEDERAL

COMPROVANTE DE INSCRIÇÃO E DE SITUAÇÃO NO CADASTRO FISCAL DO DISTRITO FEDERAL - DIF

Imprimir

CF/DF	CPF/CNPJ	DataConcessão	FAC - Número do Protocolo	Natureza Jurídica/Tipo de Contribuinte
07.760.481/001-40	24.425.034/0001-96	21/03/2016	789747/40	SOCIEDADE EMPRESÁRIA LIMITADA

Denominação social	Título do Estabelecimento - Nome Fantasia	Situação Cadastral	Data Situação
JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA	PETA	ATIVO	21/03/2016

Endereço	Bairro	Cidade	UF	CEP
SCES TRECHO 2, CENTRO DE LAZER BEIRA LAGO 03 CONJ 08 LOJA 03	ASA SUL	BRASILIA	DF	70200002

Qualificação do Contribuinte ICMS

Regime de Tributação	Data de enquadramento
NORMAL	01/01/2018

Descrição Atividade Econômica Principal	Código da Atividade	Data de Início de Atividade
COMÉRCIO VAREJISTA ESPECIALIZADO DE EQUIPAMENTOS E SUPRIMENTOS DE INFORMÁTICA	G475120100	21/03/2016

Atividades secundárias

Descrição Atividade Econômica	Código da Atividade	Data de Início de Atividade

Qualificação do Contribuinte ISS

Regime de Tributação	Data de enquadramento
NORMAL	01/01/2018

Descrição Atividade Econômica Principal	Código da Atividade	Data de Início de Atividade
DESENVOLVIMENTO E LICENCIAMENTO DE PROGRAMAS DE COMPUTADOR NÃO-CUSTOMIZÁVEIS	J620310000	28/01/2026

Atividades secundárias

Descrição Atividade Econômica	Código da Atividade	Data de Início de Atividade
DESENVOLVIMENTO DE PROGRAMAS DE COMPUTADOR SOB ENCOMENDA	J620150100	21/03/2016
DESENVOLVIMENTO E LICENCIAMENTO DE PROGRAMAS DE COMPUTADOR CUSTOMIZÁVEIS	J620230000	21/03/2016
CONSULTORIA EM TECNOLOGIA DA INFORMAÇÃO	J620400000	21/03/2016
SUPORTE TÉCNICO, MANUTENÇÃO E OUTROS SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO	J620910000	21/03/2016
OUTRAS ATIVIDADES DE PRESTAÇÃO DE SERVIÇOS DE INFORMAÇÃO NÃO ESPECIFICADAS ANTERIORMENTE	J639920000	21/03/2016
ATIVIDADES DE INTERMEDIAÇÃO E AGENCIAMENTO DE SERVIÇOS E NEGÓCIOS EM GERAL, EXCETO IMOBILIÁRIOS	M749010400	21/03/2016
ALUGUEL DE MÁQUINAS E EQUIPAMENTOS PARA ESCRITÓRIO	N773310000	21/03/2016

Este documento foi emitido no dia 19/10/2026 na Internet pelo portal Agênci@Net
.

CONTRATO DE CONSTITUIÇÃO DE JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA

1. JOSE ANDRE MENDES COIMBRA, brasileiro(a), RG 1179715, profissão EMPRESÁRIO, natural de MONTES CLAROS, MINAS GERAIS, nascido(a) em 26 de Janeiro de 1970, casado(a) sob o regime de comunhão parcial de bens, CPF 471.539.891-53, residente na(o) Quadra SMPW Quadra 17 Conjunto 7, S/N, LOTE 03, Setor de Mansões Park Way, BRASILIA, DISTRITO FEDERAL, CEP 71741707;

2. PAMELLA RODRIGUES ANDRE, brasileiro(a), RG 06432830350, profissão EMPRESÁRIA, natural de BRASILIA, DISTRITO FEDERAL, nascido(a) em 22 de Junho de 1997, solteiro(a), CPF 058.022.651-40, residente na(o) Quadra SMPW Quadra 17 Conjunto 7, S/N, LOTE 03, Setor de Mansões Park Way, BRASILIA, DISTRITO FEDERAL, CEP 71741707;

Constituem uma Sociedade Empresária Limitada que reger-se-á pelas seguintes cláusulas:

Cláusula Primeira – Do nome
A sociedade adotará o nome empresarial JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA.

Cláusula Segunda – Do objeto social
A sociedade terá por objeto o exercício das seguintes atividades econômicas: Comercialização, consultoria e representação de software, comércio de equipamentos e suprimentos de informática. (4751-2/01, 6202-3/00, 6201-5/01).

Cláusula Terceira – Do domicílio ou sede
A sociedade terá domicílio ou sede na(o) Setor SCN QUADRA 02 BL A , 190, SALA 504 PARTE O-1, ASA SUL, BRASILIA, DISTRITO FEDERAL, CEP 70712900.

Cláusula Quarta – Do(s) local(is) de exercício e respectivas atividades
Sem prejuízo da possibilidade de abrir ou fechar filial, ou qualquer estabelecimento, mediante alteração deste instrumento de contrato, deliberada na forma da lei, a Sociedade atuará:

4.1 Em estabelecimento eleito como Sede (Matriz) situado na(o) Setor SCN QUADRA 02 BL A , 190, SALA 504 PARTE O-1, ASA SUL, BRASILIA, DISTRITO FEDERAL, CEP 70712900, no qual será(ão) exercida(s) a(s) atividade(s): Comércio varejista especializado de equipamentos e suprimentos de informática (4751-2/01), Desenvolvimento e licenciamento de programas de computador customizáveis (6202-3/00),

Desenvolvimento de programas de computador sob encomenda (6201-5/01).

Cláusula Quinta – Do capital social
O capital social será R$ 10.000,00 (dez mil reais) dividido em 10.000 quotas sociais no valor de R$ 1,00 (UM REAL) cada uma, cuja integralização pelos sócios se dará em moeda corrente do País e da seguinte forma:

NOME	Nº QUOTAS	VALOR TOTAL (R$)	VALOR INTEGRALIZADO NESTE ATO (R$)
JOSE ANDRE MENDES COIMBRA	9.900	9.900,00	9.900,00
PAMELLA RODRIGUES ANDRE	100	100,00	100,00
TOTAL	10.000	10.000,00	10.000,00

Cláusula Sexta – Da cessão das quotas
As quotas são indivisíveis e não poderão ser cedidas ou transferidas a terceiros sem o consentimento do(s) outro(s) sócio(s), a quem fica assegurado, em igualdade de condições e preço direito de preferência para a sua aquisição se postas a venda, formalizando, se realizada a cessão, a alteração contratual pertinente.

Cláusula Sétima – Das responsabilidades dos sócios
A responsabilidade de cada sócio é restrita ao valor de suas quotas, mas todos respondem solidariamente pela integralização do capital social.

Cláusula Oitava – Da administração
A administração da Sociedade caberá ao(s) sócio(s) administrador(es) JOSE ANDRE MENDES COIMBRA, PAMELLA RODRIGUES ANDRE, cujos respectivos atos poderão ser executados de forma conjunta ou de forma isolada, com os poderes e atribuições de representação ativa e passiva na sociedade, judicial e extrajudicial, sempre podendo praticar todos os atos decorrentes do objeto social no interesse da sociedade, autorizado o uso do nome empresarial, vedado, no entanto, fazê-lo em atividades estranhas ao interesse da sociedade ou assumir obrigações seja em favor de qualquer dos quotistas ou de terceiros, bem como onerar ou alienar bens imóveis da sociedade, sem autorização do(s) outro(s) sócio(s).

Cláusula Nona – Do início das atividades e da duração
A sociedade iniciará suas atividades em 11 de Março de 2016 e seu prazo de duração é indeterminado.

Cláusula Décima – da prestação e deliberação das contas
Ao término de cada exercício social, em 31 de Dezembro, o(s) administrador(es), sócio(s) ou não, prestará(ão) contas justificadas de sua gestão, procedendo à elaboração do inventário, do balanço patrimonial e do balanço de resultado econômico, cabendo aos sócios,

na proporção de suas quotas, os lucros ou perdas apurados.
Parágrafo Único – Nos quatro meses seguintes ao término do exercício social, os sócios deliberarão sobre as contas e designarão administrador(es) quando for o caso.

Cláusula Décima Primeira – Do "pro labore"
Os sócios poderão, de comum acordo, fixar uma retirada mensal, a título de "pro labore", observadas as disposições regulamentares pertinentes.

Cláusula Décima Segunda – Da morte ou interdição de sócio
Falecendo ou sendo interditado um sócio, a sociedade continuará suas atividades com os herdeiros, sucessores e o incapaz. Não sendo possível ou inexistindo interesse destes ou do(s) sócio(s) remanescente(s), o valor de seus haveres será apurado e liquidado com base na situaçãopatrimonial da sociedade, à data da resolução, verificada em balanço especialmente levantado.
Parágrafo Único – O mesmo procedimento será adotado em outros casos em que a sociedade se resolva em relação a seu sócio.

Cláusula Décima Terceira – Das declarações de desimpedimento
O(s) Administrador(es), sócio(s) ou não, declara(m), sob as penas da lei, de que não está(ão) impedidos de exercer a administração da sociedade, por lei especial, ou em virtude de condenação criminal, ou por se encontrar(em) sob os efeitos dela, a pena que vede, ainda que temporariamente, o acesso a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato, ou contra a economia popular, contra o sistema financeiro nacional, contra normas de defesa da concorrência, contra as relações de consumo, fé pública, ou a propriedade.

Cláusula Décima Quarta – Do foro ou circunscrição judiciária
Fica eleito o foro ou circunscrição judiciária de BRASILIA para o exercício e o cumprimento dos direitos e obrigações resultantes deste contrato.

E por estarem assim justos e contratados assinam o presente instrumento.

BRASILIA, 11 de Março de 2016

Assinaturas

JOSE ANDRE MENDES COIMBRA

OFÍCIO DE NOTAS DO DF

PAMELLA RODRIGUES ANDRE

Wallison
4º OFÍCIO DE NOTAS DO DF

Advogado
OAB Nº - DF30801

Karina A. D. Costacurta Nazareth
OAB/DF 30.801

4o. OFICIO DE NOTAS DE BRASILIA
M/3 NORTE QD. 504 - ED.MARIANA-TERREO
BRASILIA-DF - FONE:(0XX61)3326-5234

RECONHECO e dou fe por AUTENTICIDADE
a(s)firma(s) de:
[0655174]-PAMELLA RODRIGUES ANDRE.....
DOCUMENTO CONTENDO 04 PAGS. REFERENTE
AO CONTRATO DE CONSTITUICAO DE JAMC
CONSULTORIA E REPRESENTACAO LTDA.

Em testemunho [illegible] da verdade.
BRASILIA, 15 de Marco de 2016
Selo: TJDFT20160090290619WLUB
Disponivel no site www.tjdft.jus.br

010-LEONIDAS FABIANO RODRIGUES CRUZ
ESCREVENTE AUTORIZADO
WPDS hora da impressao: 13:31:34

Leônidas Fabiano R. Cruz
4º Ofício de Notas de Brasília DF
Escrevente Autorizado

JUNTA COMERCIAL DO DISTRITO FEDERAL
CERTIFICO O REGISTRO EM: 21/03/2016 SOB N.: 53203049806
Protocolo: 16/014122-2, DE 24/02/2016
Empresa: 53 2 0204989-6
JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE

GIRELA SIMIONA CESCHIN
PRESIDENTE

Ofício de Notas
DOCUMENTO AUTENTICADO



JUNTA COMERCIAL DO DISTRITO FEDERAL
CERTIFICO O REGISTRO EM 24/06/2017 SOB N. 20170696723
Protocolo: 17/696672-3, DE 23/06/2017
Empresa: 53 2 0204080-6
JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA EPP

JAMC Consultoria e Representação de Software Ltda
CNPJ/MF nº 24.425.034/0001-96
1ª Alteração Contratual

José André Mendes Coimbra, brasileiro, solteiro, estatistico, residente e domiciliado na SMPW QD 17 Conjunto 07 Lote 03, Nucleo Bandeirante, Brasilia/DF CEP: 71.741-707, nascido em 26.01.1970, natural de Montes Claros/MG, filho de José André Coimbra e Terezinha Angelica Mendes Coimbra, portador da carteira de Identidade Identidade n°. 1.179.715 expedida pelo SSP/DF em 24.06.1987, e inscrito no CPF/MF sob o n°. 471.539.891-53 e;

Pamella Rodrigues Andre, brasileira, solteira, estudante, residente e domiciliada na, SMPW QD 17 Conjunto 07 Lote 03, Nucleo Bandeirante, Brasilia/DF CEP: 71.741-707, nascida em 22.06.1997, natural de Brasília/DF, filha de Wallyson da Silva Andre i e Renata Sá Rodrigues de Souza, portadora da carteira nacional de habilitação n°. 06432830350, expedida pelo DETRAN/DF em 10.11.2015, e inscrita no CPF/MF sob o n°. 058.022.651-40.

Únicas sócias componentes da sociedade limitada, **JAMC Consultoria e Representação de Software Ltda,** estabelecida no **SCN Quadra 02 Bloco A nº 190 Sala 504 Parte O-1, Asa Sul, Brasília/DF, CEP: 70.710-500.**, inscrita no **CNPJ sob o nº. 24.425.034/0001-96**, com seu contrato social arquivado na JCDF sob o nº. 53202049896, por despacho em 21/03/2016. **RESOLVEM** alterar e consolidar de pleno a comum acordo as disposições contratuais vigentes, conforme a cláusulas e condições seguintes:

Cláusula 1ª A sociedade resolve altera endereço para: **SCN Quadra 02 Bloco A nº 190 Sala 504 Parte O-1, Asa Norte, Brasília/DF, CEP: 70.710-500.**

Cláusula 2ª - A sociedade passará a ter como objetivo social: **Comercialização, consultoria e representação de software, comércio de equipamentos e suprimentos de informática, agenciamento, corretagem ou intermediação de títulos em geral, valores mobiliários e contratos quaisquer ou agenciamento, corretagem ou intermediação de bens móveis ou imóveis, não abrangidos em outros itens ou subitens, inclusive aqueles realizados no âmbito de bolsas de mercadoria.**

Cláusula 3ª - Em face da alteração acordada, os sócios resolvem efetuar a Consolidação do Contrato Social, que passa a vigorar com a redação dada a seguir:

JAMC Consultoria e Representação de Software Ltda
Consolidação do Contrato Social

Cláusula 1º:
A sociedade gira sob a denominação social de **"JAMC CONSULTORIA E RREPRESENTAÇÃO DE SOFTWARE LTDA".**

Parágrafo 1º. A sociedade tem como nome de fantasia **"PETACORP".**

Parágrafo 2º: A Sociedade é constituída sob a forma do tipo jurídico das Sociedades Limitadas.

Cláusula 2ª: A sociedade tem sua sede no **SCN Quadra 02 Bloco A nº 190 Sala 504 Parte O-1, Asa Norte, Brasília/DF, CEP: 70.710-500,** e pode constituir filiais, sucursais, escritórios e franquias em qualquer parte do território nacional ou no exterior, por deliberação dos sócios e, mediante alteração contratual para o devido fim.

Cláusula 3ª: A sociedade tem como objetivo social:- **Comercialização, consultoria e representação de software, comércio de equipamentos e suprimentos de informática, agenciamento, corretagem ou intermediação de títulos em geral, valores mobiliários e contratos quaisquer ou agenciamento, corretagem ou intermediação de bens móveis ou imóveis, não abrangidos em outros itens ou subitens, inclusive aqueles realizados no âmbito de bolsas de mercadoria.**

Cláusula 4ª: O capital social é de R$ 10.000,00 (dez mil reais), dividido em 10.000 quotas sociais no valor de R$ 1,00 (UM REAL) cada uma, cuja integralização pelos sócios se dará em moeda corrente do País e da seguinte forma:

NOME	Nº QUOTAS	VALOR TOTAL (R$)	VALOR INTEGRALIZADO NESTE ATO (R$)
José André Mendes Coimbra	9.900 quotas	9.900,00	R$ 9.900,00
Pamella Rodrigues Andre	100 quotas	100	R$ 100,00
TOTAL	10.000 quotas	10.000,000	R$ 10.000,00

Cláusula 5ª: As quotas da sociedade são indivisíveis e não poderão ser cedidas ou transferidas sem o expresso consentimento dos demais sócios, cabendo em igualdade de condições e preço, o direito de preferência ao sócio que queira adquiri-las. O sócio que pretenda ceder ou transferir todas ou parte de suas quotas deverá manifestar sua intenção por escrito aos outros sócios, assistindo a estes o prazo de 30 (trinta) dias para que possam exercer o direito de preferência, ou ainda, optar pela dissolução da sociedade antes mesmo da cessão ou transferência das cotas.

Cláusula 4ª: Das responsabilidades de cada sócio é restrita ao valor de suas quotas, mas todas respondem solidariamente pela integralização do capital social.

Cláusula 5ª: A administração da sociedade caberá aos sócios, **Pamella Rodrigues André** e **José André Mendes Coimbra**, cujos nos respectivos atos poderão ser executados de forma conjunta ou de forma isolada, com os poderes e atribuições de representação ativa e passiva na sociedade, judicial e extrajudicial, sempre podendo praticar todos os atos decorrentes do objeto social no interesse da sociedade, autorizado o uso do nome empresarial, vedado, no entanto, em atividades estranhas ao interesse da sociedade, ou assumir obrigações seja em favor de qualquer dos quotistas ou de terceiro, bem como onerar ou alienar bens imóveis da sociedade, sem autorização do outro sócio.

Cláusula 6ª: A sociedade iniciou suas atividades em **14 de maio de 2007** e seu prazo de duração é por tempo indeterminado.

Cláusula 7ª: Ao termino de cada exercício social, em 31 dezembro os, administradores, sócios ou não, prestarão contas justificadas de sua gestão, procedendo à elaboração do inventário, do balanço patrimonial e do balanço de resultado econômico, cabendo aos sócios, na proporção de suas cotas, os lucros ou perdas apurados.

Parágrafo Único: Nos quatro meses seguintes ao término do exercício social, os sócios deliberarão sobre as contas e designarão administrador, quando for o caso.

Cláusula 8º: Os sócios poderão de comum acordo, fixar uma retirada mensal, a título de "pró-labore", observadas as disposições regulamentares pertinentes.

Cláusula 9º: Falecendo ou sendo interditado qualquer sócio (a), a sociedade continuará suas atividades com os herdeiros, sucessores e o incapaz. Não sendo possível ou inexistindo interesse destes ou do sócio remanescente, o valor de seus haveres será apurado e liquidado com base na situação patrimonial da sociedade, à data da resolução, verificada em balanço especialmente levantado.

Parágrafo Único: O mesmo procedimento será adotado em outros casos em que a sociedade se resolva em relação a seu sócio.

Cláusula 10º: Os administradores declaram, sob pena da lei, de que não está impedidos de exercer a administração da sociedade, por lei especial, ou em virtude de condenação criminal, ou por se encontrar sob os efeitos dela, a pena que vede, ainda que temporariamente, o acesso a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato, ou contra a economia popular, contra o sistema financeiro nacional, contra normas de defesa da concorrência, contra as relações de consumo, fé pública, ou à propriedade.

Cláusula 11º: Fica eleito o foro de Brasília (DF) para a solução de quaisquer dúvidas ou questões oriundas deste contrato, com desistência de qualquer outro, por parte dos sócios, por mais privilegiado que venha a ser.

E por estarem assim justos e contratados, assinam o presente instrumento em 04 (quatro) vias, de igual teor e forma, para um só efeito, mandando arquivar a original na Junta Comercial do Distrito Federal, para devido registro.

Brasília – DF, 13 de Junho de 2017.

Wallison 4º OFÍCIO DE NOTAS DO DF

JOSÉ ANDRÉ MENDES COIMBRA

Wallison 4º OFÍCIO DE NOTAS DO DF

PAMELLA RODRIGUES ANDRE

JUNTA COMERCIAL DO DISTRITO FEDERAL
CERTIFICO O REGISTRO EM: 28/06/2017 SOB N.: 20170499136
Protocolo: 17/049913-8, DE 21/06/2017
Empresa: 53 2 0204989-6
JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA EPP
SAULO IZIDORIO VIEIRA
SECRETÁRIO-GERAL

4º Ofício de Notas

JAMC Consultoria e Representação de Software Ltda
CNPJ/MF nº 24.425.034/0001-96
2ª Alteração Contratual

José André Mendes Coimbra, brasileiro, solteiro, estatistico, residente e domiciliado na SMPW QD 17 Conjunto 07 Lote 03, Nucleo Bandeirante, Brasilia/DF CEP: 71.741-707, nascido em 26.01.1970, natural de Montes Claros/MG, filho de José André Coimbra e Terezinha Angelica Mendes Coimbra, portador da carteira de Identidade Identidade n°. 1.179.715 expedida pelo SSP/DF em 24.06.1987, e inscrito no CPF/MF sob o n°. 471.539.891-53 e;

Pamella Rodrigues Andre, brasileira, solteira, estudante, residente e domiciliada na, SMPW QD 17 Conjunto 07 Lote 03, Nucleo Bandeirante, Brasilia/DF CEP: 71.741-707, nascida em 22.06.1997, natural de Brasília/DF, filha de Wallyson da Silva Andre i e Renata Sá Rodrigues de Souza, portadora da carteira nacional de habilitação n°. 06432830350, expedida pelo DETRAN/DF em 10.11.2015, e inscrita no CPF/MF sob o n°. 058.022.651-40.

Únicas sócias componentes da sociedade limitada, **JAMC Consultoria e Representação de Software Ltda,** estabelecida no **SCN Quadra 02 Bloco A nº 190 Sala 504 Parte O-1, Asa Sul, Brasília/DF, CEP: 70.710-500.**, inscrita no **CNPJ sob o nº. 24.425.034/0001-96**, com seu contrato social arquivado na JCDF sob o nº. 53202049896, por despacho em 21/03/2016. **RESOLVEM** alterar e consolidar de pleno e comum acordo as disposições contratuais vigentes, conforme a cláusulas e condições seguintes:

Cláusula Primeira – Aumento Capital

O Capital da sociedade que era de **R$ 10.000,00** (dez mil reais) representados por 10.000 (dez mil) cotas no valor nominal de **R$ 1,00** (um real) cada, neste ato, totalmente integralizada em moeda corrente nacional, doravante fica elevado para **R$ 2000.000,00** (duzentos mil reais), da seguinte forma, o sócio **José André Mendes Coimbra,** já qualificado no preambolo integraliza nete ato **R$ 90.000,00** (noventa mil reais) divididos em 90.000 (noventa mil), quotas no valor nominal de 1,00 (um real) cada uma totalmente integralizado em moeda corrente nacional, e **R$ 100.000,00** (cem mil reais) divididos em 100.000 (cem mil) quotas, no valor nominal de 1,00 (um real) cada uma totalmente integralizado em moeda corrente nacional, através de lucros acumulados levantado em 31/07/2017.

Cláusula Segunda - Distribuição

Com a presente alteração, o capital social passa a ser de **R$ 200.000,00** (duzentos mil reais) representada por 200.000 (duzentas mil), quotas no valor nominal de **R$ 1,00** (um real) cada, neste ato, totalmente integralizada em moeda corrente nacional, assim distribuída entre os sócios:

SOCIO	%	*Nº Cotas*	Valor R$
José André Mendes Coimbra	90 %	180.000	R$ 180.000,00
Pamella Rodrigues Andre	10 %	20.000	R$ 20.000,00
TOTAL	**100 %**	**200.000**	**R$ 200.000,00**

Cláusula Terceira - Em face da alteração acordada, os sócios resolvem efetuar a Consolidação do Contrato Social, que passa a vigorar com a redação dada a seguir:

JAMC Consultoria e Representação de Software Ltda

Consolidação do Contrato Social

Cláusula 1º:
A sociedade gira sob a denominação social de **"JAMC CONSULTORIA E RREPRESENTAÇÃO DE SOFTWARE LTDA".**

Parágrafo 1º. A sociedade tem como nome de fantasia **"PETACORP".**

Parágrafo 2º: A Sociedade é constituída sob a forma do tipo jurídico das Sociedades Limitadas.

Cláusula 2º: A sociedade tem sua sede no **SCN Quadra 02 Bloco A nº 190 Sala 504 Parte O-1, Asa Norte, Brasília/DF, CEP: 70.710-500,** e pode constituir filiais, sucursais, escritórios e franquias em qualquer parte do território nacional ou no exterior, por deliberação dos sócios e, mediante alteração contratual para o devido fim.

Cláusula 3º: A sociedade tem como objetivo social:- **Comercialização, consultoria e representação de software, comércio de equipamentos e suprimentos de informática, agenciamento, corretagem ou intermediação de títulos em geral, valores mobiliários e contratos quaisquer ou agenciamento, corretagem ou intermediação de bens móveis ou imóveis, não abrangidos em outros itens ou subitens, inclusive aqueles realizados no âmbito de bolsas de mercadoria.**

Cláusula 4º: O capital social é de R$ 200.000,00 (duzentos mil reais), dividido em 200.000 quotas sociais no valor de R$ 1,00 (UM REAL) cada uma, cuja integralização pelos sócios se dará em moeda corrente do País e da seguinte forma:

SOCIO	%	*Nº Cotas*	Valor R$
José André Mendes Coimbra	90 %	180.000	R$ 180.000,00
Pamella Rodrigues Andre	10 %	20.000	R$ 20.000,00
TOTAL	**100 %**	**200.000**	**R$ 200.000,00**

Cláusula 5º: As quotas da sociedade são indivisíveis e não poderão ser cedidas ou transferidas sem o expresso consentimento dos demais sócios, cabendo em igualdade de condições e preço, o direito de preferência ao sócio que queira adquiri-las. O sócio que pretenda ceder ou transferir todas ou parte de suas quotas deverá manifestar sua intenção por escrito aos outros sócios, assistindo a estes o prazo de 30 (trinta) dias para que possam exercer o direito de preferência, ou ainda, optar pela dissolução da sociedade antes mesmo da cessão ou transferência das cotas.

Cláusula 4º: Das responsabilidades de cada sócio é restrita ao valor de suas quotas, mas todas respondem solidariamente pela integralização do capital social.

Cláusula 5º: A administração da sociedade caberá aos sócios, **Pamella Rodrigues André** e **José André Mendes Coimbra,** cujos nos respectivos atos poderão ser executados de forma conjunta ou de forma isolada, com os poderes e atribuições de representação ativa e passiva na sociedade, judicial e extrajudicial, sempre podendo praticar todos os atos decorrentes do objeto social no interesse da sociedade, autorizado o uso do nome empresarial, vedado, no entanto, em atividades estranhas ao interesse da sociedade, ou assumir obrigações seja em favor de qualquer dos quotistas ou de terceiro, bem como onerar ou alienar bens imóveis da sociedade, sem autorização do outro sócio.



Cláusula 6º: A sociedade iniciou suas atividades em **14 de maio de 2007** e seu prazo de duração é por tempo indeterminado.

Cláusula 7º: Ao termino de cada exercício social, em 31 dezembro os, administradores, sócios ou não, prestarão contas justificadas de sua gestão, procedendo à elaboração do inventário, do balanço patrimonial e do balanço de resultado econômico, cabendo aos sócios, na proporção de suas cotas, os lucros ou perdas apurados.

Parágrafo Único: Nos quatro meses seguintes ao término do exercício social, os sócios deliberarão sobre as contas e designarão administrador, quando for o caso.

Cláusula 8º: Os sócios poderão de comum acordo, fixar uma retirada mensal, a título de "pró-labore", observadas as disposições regulamentares pertinentes.

Cláusula 9º: Falecendo ou sendo interditado qualquer sócio (a), a sociedade continuará suas atividades com os herdeiros, sucessores e o incapaz. Não sendo possível ou inexistindo interesse destes ou do sócio remanescente, o valor de seus haveres será apurado e liquidado com base na situação patrimonial da sociedade, à data da resolução, verificada em balanço especialmente levantado.

Parágrafo Único: O mesmo procedimento será adotado em outros casos em que a sociedade se resolva em relação a seu sócio.

Cláusula 10º: Os administradores declaram, sob pena da lei, de que não está impedidos de exercer a administração da sociedade, por lei especial, ou em virtude de condenação criminal, ou por se encontrar sob os efeitos dela, a pena que vede, ainda que temporariamente, o acesso a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato, ou contra a economia popular, contra o sistema financeiro nacional, contra normas de defesa da concorrência, contra as relações de consumo, fé pública, ou à propriedade.

Cláusula 11º: Fica eleito o foro de Brasília (DF) para a solução de quaisquer dúvidas ou questões oriundas deste contrato, com desistência de qualquer outro, por parte dos sócios, por mais privilegiado que venha a ser.

E por estarem assim justos e contratados, assinam o presente instrumento em 04 (quatro) vias, de igual teor e forma, para um só efeito, mandando arquivar a original na Junta Comercial do Distrito Federal, para devido registro.

Brasília – DF, 21 de Agosto de 2017.

JOSÉ ANDRÉ MENDES COIMBRA

PAMELLA RODRIGUES ANDRÉ

JAMC Consultoria e Representação de Software Ltda.

CNPJ/MF nº 24.425.034/0001-96

3ª Alteração Contratual

José André Mendes Coimbra, brasileiro, solteiro, estatistico, residente e domiciliado na SMPW QD 17 Conjunto 07 Lote 03, Nucleo Bandeirante, Brasilia/DF CEP: 71.741-707, nascido em 26.01.1970, natural de Montes Claros/MG, filho de José André Coimbra e Terezinha Angelica Mendes Coimbra, portador da carteira de Identidade identidade n°. 1.179.715 expedida pelo SSP/DF em 24.06.1987, e inscrito no CPF/MF sob o n°. 471.539.891-53 e;

Pamella Rodrigues Andre, brasileira, solteira, estudante, residente e domiciliada na, SMPW QD 17 Conjunto 07 Lote 03, Nucleo Bandeirante, Brasilia/DF CEP: 71.741-707, nascida em 22.06.1997, natural de Brasília/DF, filha de Wallyson da Silva Andre i e Renata Sá Rodrigues de Souza, portadora da carteira nacional de habilitação n°. 06432830350, expedida pelo DETRAN/DF em 10.11.2015, e inscrita no CPF/MF sob o n°. 058.022.651-40.

Únicos sócios componentes da sociedade limitada, **JAMC Consultoria e Representação de Software Ltda,** estabelecida no **SCN Quadra 02 Bloco A nº 190 Sala 504 Parte O-1, Asa Norte, Brasília/DF, CEP: 70.710-500**, inscrita no **CNPJ sob o nº. 24.425.034/0001-96**, com seu contrato social arquivado na JCDF sob o nº. 53202049896, por despacho em 21/03/2016. **RESOLVEM** alterar e consolidar de pleno e comum acordo as disposições contratuais vigentes, conforme a cláusulas e condições seguintes:

Cláusula Primeira – A sociedade tem como objetivo social:

- Comercialização, consultoria, representação *importação e exportação* de software;
- Comércio de equipamentos e suprimentos de informática;
- Agenciamento, corretagem ou intermediação de títulos em geral, valores mobiliários e contratos quaisquer ou agenciamento, corretagem ou intermediação de bens móveis ou imóveis, não abrangidos em outros itens ou subitens, inclusive aqueles realizados no âmbito de bolsas de mercadoria.

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1334394 em 13/11/2019 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA EPP, Nire 53202049896 e protocolo DFP1900162746 - 25/10/2019. Autenticação: 185DE51860E1C03331DEA7EA3F57EDE258029D7B. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 19/175.498-4 e o código de segurança wV9O Esta cópia foi autenticada digitalmente e assinada em 13/11/2019 por Maxmiliam Patriota Carneiro – Secretário-Geral.

Cláusula Segunda – Da alteração de Capital Social e distribuição:

O capital social que é de R$ 200.000,00 (duzentos mil reais) representados 200.000 (duzentas mil) quotas sociais no valor de R$ 1,00 (um real) cada, neste ato, totalmente integralizadas em moeda corrente nacional, doravante fica elevado para R$ 600.000,00 (seiscentos mil reais), da seguinte forma, o sócios já qualificados no preambulo integralizam neste ato R$ 400.000,00 (quatrocentos mil reais), divididos em 400.000 (quatrocentas mil) quotas, no valor de R$ 1,00 (um real) cada uma totalmente integralizadas em moeda corrente nacional, através de lucros acumulados levantados em 31.12.2018.

Com a presente alteração, o capital social passa a ser de R$ 600.000,00 (seiscentos mil reais), representado por 600.000 (seiscentas mil) quotas no valor nominal de R$ 1,00 (um real) cada, neste ato totalmente integralizado em moeda corrente nacional, assim distribuída entre os sócios:

Sócios	%	Quotas	Valor R$
José André Mendes Coimbra	90 %	540.000	R$ 540.000,00
Pamella Rodrigues Andre	10 %	60.000	R$ 60.000,00
TOTAL	**100 %**	**600.000**	**R$ 600.000,00**

Cláusula Terceira - Em face da alteração acordada, os sócios resolvem efetuar a Consolidação do Contrato Social, que passa a vigorar com a redação dada a seguir:

JAMC Consultoria e Representação de Software Ltda

Consolidação do Contrato Social

Cláusula 1º: A sociedade gira sob a denominação social de **"JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA".**

Parágrafo 1º. A sociedade tem como nome de fantasia **"PETACORP".**

Parágrafo 2º: A Sociedade é constituída sob a forma do tipo jurídico das Sociedades Limitadas.

Cláusula 2º: A sociedade tem sua sede no **SCN Quadra 02 Bloco A nº 190 Sala 504 Parte O-1, Asa Norte, Brasília/DF, CEP: 70.710-500,** e pode constituir filiais, sucursais, escritórios e franquias em qualquer

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1334394 em 13/11/2019 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA EPP, Nire 53202049896 e protocolo DFP1900162746 - 25/10/2019. Autenticação: 185DE51868E1C03331DEA7EA3F57EDE258829D7B. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 19/175.499-4 e o código de segurança wV9O Esta cópia foi autenticada digitalmente e assinada em 13/11/2019 por Maxmiliam Patriota Carneiro – Secretário-Geral.

parte do território nacional ou no exterior, por deliberação dos sócios e, mediante alteração contratual para o devido fim.

Cláusula 3ª: A sociedade tem como objetivo social:

- Comercialização, consultoria, representação *importação e exportação* de software;
- Comércio de equipamentos e suprimentos de informática;
- Agenciamento, corretagem ou intermediação de títulos em geral, valores mobiliários e contratos quaisquer ou agenciamento, corretagem ou intermediação de bens móveis ou imóveis, não abrangidos em outros itens ou subitens, inclusive aqueles realizados no âmbito de bolsas de mercadoria.

Cláusula 4º: O capital social é de R$ 600.000,00 (seiscentos mil reais), dividido em 600.000 (seiscentas mil) quotas sociais no valor de R$ 1,00 (um real) cada uma, cuja integralização pelos sócios se dará em moeda corrente do País e da seguinte forma:

Sócios	%	Quotas	Valor R$
José André Mendes Coimbra	90 %	540.000	R$ 540.000,00
Pamella Rodrigues Andre	10 %	60.000	R$ 60.000,00
TOTAL	**100 %**	**600.000**	**R$ 600.000,00**

Cláusula 5º: As quotas da sociedade são indivisíveis e não poderão ser cedidas ou transferidas sem o expresso consentimento dos demais sócios, cabendo em igualdade de condições e preço, o direito de preferência ao sócio que queira adquiri-las. O sócio que pretenda ceder ou transferir toda ou parte de suas quotas deverá manifestar sua intenção por escrito aos outros sócios, assistindo a estes o prazo de 30 (trinta) dias para que possam exercer o direito de preferência, ou ainda, optar pela dissolução da sociedade antes mesmo da cessão ou transferência das cotas.

Parágrafo Único: Das responsabilidades de cada sócio é restrita ao valor de suas quotas, mas todas respondem solidariamente pela integralização do capital social.

Cláusula 6º: A administração da sociedade caberá aos sócios, **Pamella Rodrigues André** e **José André Mendes Coimbra**, cujos nos respectivos atos poderão ser executados de forma conjunta ou de forma isolada, com os poderes e atribuições de representação ativa e passiva na sociedade, judicial e extrajudicial, sempre podendo praticar todos os atos decorrentes do objeto social no interesse da

Pâmela

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1334394 em 13/11/2019 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA EPP, Nire 53202049696 e protocolo DFP1900152746 - 25/10/2019. Autenticação: 1B5DE51860E1C03331DEA7EA3F57EDE258829D78. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 19/175.499-4 e o código de segurança wV9O Esta cópia foi autenticada digitalmente e assinada em 13/11/2019 por Maxmiliam Patriota Carneiro – Secretário-Geral.

sociedade, autorizado o uso do nome empresarial, vedado, no entanto, em atividades estranhas ao interesse da sociedade, ou assumir obrigações seja em favor de qualquer dos quotistas ou de terceiros, bem como onerar ou alienar bens imóveis da sociedade, sem autorização do outro sócio.

Cláusula 7º: A sociedade iniciou suas atividades em **11/03/2016** e seu prazo de duração é por tempo indeterminado.

Cláusula 8º: Ao termino de cada exercício social, em 31 dezembro os, administradores, sócios ou não, prestarão contas justificadas de sua gestão, procedendo à elaboração do inventário, do balanço patrimonial e do balanço de resultado econômico, cabendo aos sócios, na proporção de suas cotas, os lucros ou perdas apuradas.

Parágrafo Primeiro: Nos quatro meses seguintes ao término do exercício social, os sócios deliberarão sobre as contas e designarão administrador, quando for o caso.

Parágrafo Segundo: Os sócios poderão de comum acordo, fixar uma retirada mensal, a título de "pró-labore", observadas as disposições regulamentares pertinentes.

Cláusula 9º: Falecendo ou sendo interditado qualquer sócio (a), a sociedade continuará suas atividades com os herdeiros, sucessores e o incapaz. Não sendo possível ou inexistindo interesse destes ou do sócio remanescente, o valor de seus haveres será apurado e liquidado com base na situação patrimonial da sociedade, à data da resolução, verificada em balanço especialmente levantado.

Parágrafo Único: O mesmo procedimento será adotado em outros casos em que a sociedade se resolva em relação a seu sócio.

Cláusula 10º: Os administradores declaram, sob pena da lei, de que não estão impedidos de exercer a administração da sociedade, por lei especial, ou em virtude de condenação criminal, ou por se encontrar sob os efeitos dela, a pena que vede, ainda que temporariamente, o acesso a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato, ou contra a economia popular, contra o sistema financeiro nacional, contra normas de defesa da concorrência, contra as relações de consumo, fé pública, ou à propriedade.

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1334394 em 13/11/2019 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA EPP, Nire 53202049896 e protocolo DFP1900182746 - 25/10/2019. Autenticação: 1B5DE51886E1C03331DEA7EA3F57EDE259829D7B. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 19/175.496-4 e o código de segurança wW9O Esta cópia foi autenticada digitalmente e assinada em 13/11/2019 por Maxmiliam Patriota Carneiro – Secretário-Geral.

Cláusula 11º: Fica eleito o foro de Brasília (DF) para a solução de quaisquer dúvidas ou questões oriundas deste contrato, com desistência de qualquer outro, por parte dos sócios, por mais privilegiado que venha a ser.

E por estarem assim justos e contratados, assinam o presente instrumento em via única, para um só efeito, mandando arquivar a original na Junta Comercial do Distrito Federal, para devido registro.

Brasília – DF, 09 de outubro de 2019.

Lucas
4º OFÍCIO DE NOTAS DO DF

JOSÉ ANDRÉ MENDES COIMBRA

Lucas
4º OFÍCIO DE NOTAS DO DF

PAMELLA RODRIGUES ANDRÉ

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1334394 em 13/11/2019 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA EPP, Nire 53202049696 e protocolo DFP1900162746 - 25/10/2019. Autenticação: 1B5DE51660E1C03331DEA7EA3F57EDE258829D7B. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 19/175.499-4 e o código de segurança wV9O Este cópia foi autenticada digitalmente e assinada em 13/11/2019 por Maxmiliam Patriota Carneiro – Secretário-Geral.

4º OFÍCIO DE NOTAS - DF
LEONIDAS FABIANO RODRIGUES CRUZ - TABELIÃO TITULAR

CARTÓRIO ASA NORTE
SEPN CD 504, ED. MARIANNA, LOJA 136/114 - BRASÍLIA / DF
FONE: (61) 3038-2515, 3038-2334, 3038-2500 - (Cel61) 99123.1003
cartorio@4oficiodenotas.com.br

RECONHECO e dou fé por SEMELHANÇA a(s) firma(s) de:
[0133911]-JOSÉ ANDRE XXXXXX CUNHA
[0e55174]-CAMELLA RODRIGUES ANDRE
TJDFT20190090631615GQCR1 e TJDFT20190090631615TLTP
Selo tjdft.jus.br - SSB, 16/10/2019 - 09:18:06
LMA-Tabeliã Estela Fetosa dos Santos

LEONIDAS FABIANO RODRIGUES CRUZ

Leônidas Fabiano Rodrigues Cruz
4º Ofício de Notas de Brasília/DF
Escrevente Autorizado

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1334394 em 13/11/2019 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA EPP, Nire 53202049886 e protocolo DFP1900162746 - 25/10/2019. Autenticação: 1B5DE51868E1C03331DEA7EA3F57EDE258829D75. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 19/175.499-4 e o código de segurança wV9O Esta cópia foi autenticada digitalmente e assinada em 13/11/2019 por Maxmiliam Patriota Carneiro – Secretário-Geral.

Ministério da Indústria, Comércio Exterior e Serviços
Secretaria Especial da Micro e Pequena Empresa
Departamento de Registro Empresarial e Integração

Nº DO PROTOCOLO (Uso da Junta Comercial)

NIRE (da sede ou filial, quando a sede for em outra UF)	Código da Natureza Jurídica	Nº de Matrícula do Agente Auxiliar do Comércio
53202049896	2062	

1 - REQUERIMENTO

ILMO(A). SR.(A) PRESIDENTE DA Junta Comercial, Industrial e Serviços do Distrito Federal

Nome: JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA EPP

(da Empresa ou do Agente Auxiliar do Comércio)

Nº FCN/REMP

DFP2100150699

requer a V.Sª o deferimento do seguinte ato:

Nº DE VIAS	CÓDIGO DO ATO	CÓDIGO DO EVENTO	QTDE	DESCRIÇÃO DO ATO / EVENTO
1	002			ALTERACAO
		051	1	CONSOLIDACAO DE CONTRATO/ESTATUTO
		2001	1	ENTRADA DE SOCIO/ADMINISTRADOR
		2211	1	ALTERACAO DE ENDERECO DENTRO DO MESMO MUNICIPIO
		2247	1	ALTERACAO DE CAPITAL SOCIAL

BRASILIA
Local

16 Setembro 2021
Data

Representante Legal da Empresa / Agente Auxiliar do Comércio:
Nome: _____
Assinatura: _____
Telefone de Contato: _____

2 - USO DA JUNTA COMERCIAL

☐ DECISÃO SINGULAR ☐ DECISÃO COLEGIADA

Nome(s) Empresarial(ais) igual(ais) ou semelhante(s):

☐ SIM ☐ SIM

_____ _____
_____ _____
_____ _____
_____ _____
_____ _____

☐ NÃO ___/___/_____ _____ ☐ NÃO ___/___/_____ _____
Data Responsável Data Responsável

Processo em Ordem
À decisão

___/___/_____
Data

_____
Responsável

DECISÃO SINGULAR

	2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência
☐ Processo em exigência. (Vide despacho em folha anexa)	☐	☐	☐	☐
☐ Processo deferido. Publique-se e arquive-se.				
☐ Processo indeferido. Publique-se.				

___/___/_____ _____
Data Responsável

DECISÃO COLEGIADA

	2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência
☐ Processo em exigência. (Vide despacho em folha anexa)	☐	☐	☐	☐
☐ Processo deferido. Publique-se e arquive-se.				
☐ Processo indeferido. Publique-se.				

___/___/_____ _____ _____ _____
Data Vogal Vogal Vogal

Presidente da _____ Turma

OBSERVAÇÕES

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1732609 em 16/09/2021 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA EPP, CNPJ 24425034000196 e protocolo DFP2100150699 - 30/08/2021. Autenticação: E375778F0DB6F2ABE134591EABDD103E3B12DF. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 21/113.421-0 e o código de segurança is7z Esta cópia foi autenticada digitalmente e assinada em 16/09/2021 por Maxmiliam Patriota Carneiro – Secretário-Geral.

JUNTA COMERCIAL, INDUSTRIAL E SERVIÇOS DO DISTRITO FEDERAL

Registro Digital

Capa de Processo

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
21/113.421-0	DFP2100150699	26/08/2021

Identificação do(s) Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	16/09/2021
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital		
029.485.647-19	GUILHERME LOPES MARANHAO	16/09/2021
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital, Selo Prata - Biometria Facial		
471.539.891-53	JOSE ANDRE MENDES COIMBRA	16/09/2021
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital		
058.022.651-40	PAMELLA RODRIGUES ANDRE	16/09/2021
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital		

Junta Comercial, Industrial e Serviços do Distrito Federal

VENTVRIS VENTIS

Junta Comercial, Industrial e Serviços do Distrito Federal

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1732609 em 16/09/2021 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA EPP, CNPJ 24425034000196 e protocolo DFP2100150699 - 30/08/2021. Autenticação: E375778F0DB6F2ABE134591EABDD103E3B12DF. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 21/113.421-0 e o código de segurança is7z Esta cópia foi autenticada digitalmente e assinada em 16/09/2021 por Maxmiliam Patriota Carneiro – Secretário-Geral.

JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA EPP
CNPJ/MF nº 24.425.034/0001-96
4ª Alteração Contratual

José André Mendes Coimbra, brasileiro, solteiro, estatistico, residente e domiciliado na SMPW QD 17 Conjunto 07 Lote 03, Nucleo Bandeirante, Brasilia/DF CEP 71.741-707, nascido em 26.01.1970, natural de Montes Claros/MG, filho de José André Coimbra e Terezinha Angelica Mendes Coimbra, portador da carteira de Identidade n°. 1.179.715 expedida pelo SSP/DF em 24.06.1987, e inscrito no CPF/MF sob o n°. 471.539.891-53 e;

Pamella Rodrigues Andre, brasileira, solteira, estudante, residente e domiciliada na, SMPW QD 17 Conjunto 07 Lote 03, Nucleo Bandeirante, Brasilia/DF CEP 71.741-707, nascida em 22.06.1997, natural de Brasília/DF, filha de Wallyson da Silva Andre i e Renata Sá Rodrigues de Souza, portadora da carteira nacional de habilitação n°. 06432830350, expedida pelo DETRAN/DF em 10.11.2015, e inscrita no CPF/MF sob o n°. 058.022.651-40.

Únicos sócios componentes da sociedade limitada, **JAMC Consultoria e Representação de Software Ltda EPP,** estabelecida no **SCN Quadra 02 Bloco A nº 190 Sala 504 Parte O-1, Asa Norte, Brasília/DF, CEP: 70.712-010.**, inscrita no **CNPJ sob o nº. 24.425.034/0001-96**, com seu contrato social arquivado na JCDF sob o nº. 53202049896, por despacho em 21/03/2016. **RESOLVEM** alterar e consolidar de pleno e comum acordo as disposições contratuais vigentes, conforme a cláusulas e condições seguintes:

I. RETIRADA DE SÓCIO, CESSÃO DE QUOTAS E ALTERAÇÕES DO QUADRO SÓCIETÁRIO

1. A sócia **PAMELLA RODRIGUES ANDRÉ**, acima, qualificada, possuidora de 60.000 (sessenta mil) quotas, no valor nominal unitário de **R$ 1,00** (um real), totalizando **R$ 60.000,00** (sessenta mil reais), totalmente subscritas e integralizadas, neste ato, retira-se da sociedade, cede e transfere de forma onerosa a totalidade de suas quotas que possui no capital social da sociedade para o sócio **JOSÉ ANDRÉ MENDES COIMBRA,** qualificado acima**.**

2. A sócio cedente declara, para todos os fins de direitos, que as quotas objeto da presente sessão, encontram-se livres e desembaraçadas de quaisquer ônus ou gravames, judiciais ou extrajudiciais, e que referida cessão de quotas compreende e inclui a cessão de todos os direitos e obrigações inerentes a titularidade das mesmas.

3. Em virtude da cessão e transferência de quotas ora pactuada, o sócio **JOSÉ ANDRÉ MENDES COIMBA,** detentor de 540.000 (quinhentos e quarenta mil) quotas, adquiri neste ato 60.000 (sessenta mil) quotas da sócia **PAMELLA RODRIGUES ANDRÉ,** ao valor nominal de R$ 1,00 (um real) cada, totalizando o montante de R$ 60.000,00 (sessenta mil reais), e passa a deter um total de 600.000 (seiscentos mil) quotas, totalizando o montante de R$ 600.000,00 (seiscentos mil reais).

II. ADMISSÃO DE SÓCIOS

1. Admite-se na sociedade:

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1732609 em 16/09/2021 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA EPP, CNPJ 24425034000196 e protocolo DFP2100150699 - 30/08/2021. Autenticação: E375778F0DB6F2ABE134591EABDD103E3B12DF. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 21/113.421-0 e o código de segurança is7z Esta cópia foi autenticada digitalmente e assinada em 16/09/2021 por Maxmiliam Patriota Carneiro – Secretário-Geral.

André Casimiro Costa, brasileiro, empresário, casado sob o regime de comunhão parcial de bens, residente e domiciliado no Condomínio Solar de Brasília, 0 Quadra 03, Conjunto 20, Casa 20, Setor Habitacional Jardim Botânico, Brasília/DF CEP 71.680-349, nascido em 03/06/1981, natural de Brasília/DF, filho de Herlandes Antônio da Costa e Maria do Socorro Casimiro Silva Costa, portador da carteira nacional de habilitação n° 007246677714, expedida pelo DETRAN/DF em 30/01/2020, e inscrito no CPF/MF sob o n° 923.876.321-68.

Guilherme Lopes Maranhão, brasileiro, solteiro, empresário, residente e domiciliado no Q SHDB QL 32, Conjunto 20, QL 32, Casa 132, Setor de Habitações Individuais Sul, Brasília/DF CEP 71.676-200, nascido em 18/02/1975, natural do Rio de Janeiro/RJ, filho de Carlos Fernando dos Reis Maranhão e Tereza Cristina Lopes Maranhão, portador da carteira nacional de habilitação n° 05801102104, expedida pelo DETRAN/DF em 13/09/2018, e inscrito no CPF/MF sob o n° 029.485.647-19.

III. CESSÃO DE QUOTAS E ALTERAÇÕES DO QUADRO SOCIETÁRIO

O sócio **JOSÉ ANDRE MENDES COIMBRA**, acima qualificado, possuidor de 600.000 (seiscentos mil) quotas, de valor nominal de R$ 1,00 (um real) cada, totalizando assim, R$ 600.000,00 (seiscentas mil reais), cede e transfere, parte das quotas que possui no capital social, para os sócios:

1. **ANDRÉ CASIMIRO COSTA,** a quantidade de 199.980 (cento e noventa e nove mil e novecentos e oitenta) quotas de valor nominal de R$ 1,00 (um real) cada, totalizando assim, R$ 199.980,00 (cento e noventa e nove mil e novecentos e oitenta reais);
2. **GUILHERME LOPES MARANHÃO,** a quantidade de 199.980 (cento e noventa e nove mil e novecentos e oitenta) quotas de valor nominal de R$ 1,00 (um real) cada, totalizando assim, R$ 199.980,00 (cento e noventa e nove mil e novecentos e oitenta reais);

Em razão da retirada e admissão de sócios, cessão de quotas e alterações do quadro societário, a cláusula Quarta do Contrato Social da Sociedade, passa a vigorar com a seguinte redação:
O capital da sociedade é de R$ 600.00,00 (seiscentos mil reais), dividido em 600.000 (seiscentas mil) quotas sociais no valor de R$ 1,00 (um real) cada uma, cuja integralização pelos sócios se dará em moeda corrente do País e da seguinte forma:

Sócios	%	Quotas	Valor R$
José André Mendes Coimbra	33,34%	200.040	R$ 200.040,00
André Casimiro Costa	33,33%	199.980	R$ 199.980,00
Guilherme Lopes Maranhão	33,33%	199.980	R$ 199.980,00
TOTAL	**100 %**	**600.000**	**R$ 600.000,00**

IV. ALTERAÇÃO DO CAPITAL SOCIAL E DISTRIBUIÇÃO

O capital social que é de R$ 600.000,00 (seiscentos mil reais) representados por 600.000 (seiscentos mil) quotas sociais no valor de R$ 1,00 (um real) cada, neste ato, totalmente integralizadas em moeda corrente nacional, doravante fica elevado para R$ 1.000.000,00 (hum milhão de reais), da seguinte forma, os sócios já qualificados no preambulo integralizam neste ato R$ 400.000,00 (quatrocentos mil reais), divididos em 400.000 (quatrocentas mil) quotas, no valor de R$ 1,00 (um real) cada uma totalmente

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1732609 em 16/09/2021 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA EPP, CNPJ 24425034000196 e protocolo DFP2100150699 - 30/08/2021. Autenticação: E375778F0DB6F2ABE134591EABDD103E3B12DF. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 21/113.421-0 e o código de segurança is7z Esta cópia foi autenticada digitalmente e assinada em 16/09/2021 por Maxmiliam Patriota Carneiro – Secretário-Geral.

integralizadas em moeda corrente nacional, através de lucros acumulados levantados em 31.12.2020.

Com a presente alteração, o capital social passa a ser de R$ 1.000.000,00 (hum milhão de reais), representado por 1.000.000 (hum milhão) quotas no valor nominal de R$ 1,00 (um real) cada, neste ato totalmente integralizado em moeda corrente nacional, assim distribuída entre os sócios:

Sócios	%	Quotas	Valor R$
José André Mendes Coimbra	33,34%	333.400	R$ 333.400,00
André Casimiro Costa	33,33%	333.300	R$ 333.300,00
Guilherme Lopes Maranhão	33,33%	333.300	R$ 333.300,00
TOTAL	**100 %**	**1.000.000**	**R$ 1.000.000,00**

V. ALTERAÇÃO DE ENDEREÇO DA SEDE

Alteração de endereço da sede para: **SRTVN QUADRA 701, CONJUNTO C, N° 124, SALA 421, ALA B, PARTE "V", ASA NORTE, BRASÍLIA/DF, CEP: 70.719-903.**

VI. DA ADMINISTRAÇÃO

A administração da sociedade caberá a todos os sócios, cujos nos respectivos atos poderão ser executados de forma conjunta, com os poderes e atribuições de representação ativa e passiva na sociedade, judicial e extrajudicial, sempre podendo praticar todos os atos decorrentes do objeto social no interesse da sociedade, autorizado o uso do nome empresarial, vedado, no entanto, em atividades estranhas ao interesse da sociedade, ou assumir obrigações seja em favor de qualquer dos quotistas ou de terceiros, bem como onerar ou alienar bens imóveis da sociedade, sem autorização do outro sócio.

VII. DECLARAÇÃO DE DESIMPEDIMENTO

Os administradores declaram, sob pena da lei, de que não estão impedidos de exercer a administração da sociedade, por lei especial, ou em virtude de condenação criminal, ou por se encontrar sob os efeitos dela, a pena que vede, ainda que temporariamente, o acesso a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato, ou contra a economia popular, contra o sistema financeiro nacional, contra normas de defesa da concorrência, contra as relações de consumo, fé pública, ou à propriedade.

Em face da alteração acordada, os sócios resolvem efetuar a Consolidação do Contrato Social, que passa a vigorar com a redação dada a seguir:

JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA EPP
Consolidação do Contrato Social

Cláusula 1º:
A sociedade gira sob a denominação social de **"JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA EPP".**

Parágrafo 1º. A sociedade tem como nome de fantasia **"PETACORP".**

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1732609 em 16/09/2021 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA EPP, CNPJ 24425034000196 e protocolo DFP2100150699 - 30/08/2021. Autenticação: E375778F0DB6F2ABE134591EABDD103E3B12DF. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 21/113.421-0 e o código de segurança is7z Esta cópia foi autenticada digitalmente e assinada em 16/09/2021 por Maxmiliam Patriota Carneiro – Secretário-Geral.

Parágrafo 2º: A Sociedade é constituída sob a forma do tipo jurídico das Sociedades Limitadas.

Cláusula 2º: A sociedade tem sua sede no **SRTVN QUADRA 701, CONJUNTO C, N° 124, SALA 421, ALA B, PARTE "V", ASA NORTE, BRASÍLIA/DF, CEP: 70.719-903,** e pode constituir filiais, sucursais, escritórios e franquias em qualquer parte do território nacional ou no exterior, por deliberação dos sócios e, mediante alteração contratual para o devido fim.

Cláusula 3º: A sociedade tem como objetivo social:

- Comercialização, consultoria, representação *importação e exportação* de software;
- Comércio de equipamentos e suprimentos de informática;
- Agenciamento, corretagem ou intermediação de títulos em geral, valores mobiliários e contratos quaisquer ou agenciamento, corretagem ou intermediação de bens móveis ou imóveis, não abrangidos em outros itens ou subitens, inclusive aqueles realizados no âmbito de bolsas de mercadoria.

Cláusula 4º: O capital social é de R$ 1.000.000,00 (hum milhão de reais), representado por 1.000.000 (hum milhão) quotas no valor nominal de R$ 1,00 (um real) cada, cuja integralização pelos sócios se dará em moeda corrente do país e da seguinte forma:

Sócios	%	Quotas	Valor R$
José André Mendes Coimbra	33,34%	333.400	R$ 333.400,00
André Casimiro Costa	33,33%	333.300	R$ 333.300,00
Guilherme Lopes Maranhão	33,33%	333.300	R$ 333.300,00
TOTAL	**100 %**	**1.000.000**	**R$ 1.000.000,00**

Cláusula 5º: As quotas da sociedade são indivisíveis e não poderão ser cedidas ou transferidas sem o expresso consentimento dos demais sócios, cabendo em igualdade de condições e preço, o direito de preferência ao sócio que queira adquiri-las. O sócio que pretenda ceder ou transferir toda ou parte de suas quotas deverá manifestar sua intenção por escrito aos outros sócios, assistindo a estes o prazo de 30 (trinta) dias para que possam exercer o direito de preferência, ou ainda, optar pela dissolução da sociedade antes mesmo da cessão ou transferência das cotas.

Cláusula 6º: Das responsabilidades de cada sócio é restrita ao valor de suas quotas, mas todas respondem solidariamente pela integralização do capital social.

Cláusula 7º: A administração da sociedade caberá a todos os sócios, cujos nos respectivos atos poderão ser executados de forma conjunta, com os poderes e atribuições de representação ativa e passiva na sociedade, judicial e extrajudicial, sempre podendo praticar todos os atos decorrentes do objeto social no interesse da sociedade, autorizado o uso do nome empresarial, vedado, no entanto, em atividades estranhas ao interesse da sociedade, ou assumir obrigações seja em favor de qualquer dos quotistas ou de terceiros, bem como onerar ou alienar bens imóveis da sociedade, sem autorização do outro sócio.

Cláusula 8º: A sociedade iniciou suas atividades em **11/03/2016** e seu prazo de duração é por tempo indeterminado.

Cláusula 9º: Ao termino de cada exercício social, em 31 dezembro os, administradores, sócios ou não, prestarão contas justificadas de sua gestão, procedendo à elaboração do inventário, do balanço patrimonial e do balanço de resultado econômico, cabendo aos sócios, na proporção de suas cotas, os lucros ou perdas apuradas.

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1732609 em 16/09/2021 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA EPP, CNPJ 24425034000196 e protocolo DFP2100150699 - 30/08/2021. Autenticação: E375778F0DB6F2ABE134591EABDD103E3B12DF. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 21/113.421-0 e o código de segurança is7z Esta cópia foi autenticada digitalmente e assinada em 16/09/2021 por Maxmiliam Patriota Carneiro – Secretário-Geral.

Parágrafo Único: Nos quatro meses seguintes ao término do exercício social, os sócios deliberarão sobre as contas e designarão administrador, quando for o caso.

Cláusula 10º: Os sócios poderão de comum acordo, fixar uma retirada mensal, a título de "pró-labore", observadas as disposições regulamentares pertinentes.

Cláusula 11º: Falecendo ou sendo interditado qualquer sócio (a), a sociedade continuará suas atividades com os herdeiros, sucessores e o incapaz. Não sendo possível ou inexistindo interesse destes ou do sócio remanescente, o valor de seus haveres será apurado e liquidado com base na situação patrimonial da sociedade, à data da resolução, verificada em balanço especialmente levantado.

Parágrafo Único: O mesmo procedimento será adotado em outros casos em que a sociedade se resolva em relação a seu sócio.

Cláusula 12º: Os administradores declaram, sob pena da lei, de que não estão impedidos de exercer a administração da sociedade, por lei especial, ou em virtude de condenação criminal, ou por se encontrar sob os efeitos dela, a pena que vede, ainda que temporariamente, o acesso a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato, ou contra a economia popular, contra o sistema financeiro nacional, contra normas de defesa da concorrência, contra as relações de consumo, fé pública, ou à propriedade.

Cláusula 13º: Fica eleito o foro de Brasília (DF) para a solução de quaisquer dúvidas ou questões oriundas deste contrato, com desistência de qualquer outro, por parte dos sócios, por mais privilegiado que venha a ser.

E por estarem assim justos e contratados, assinam o presente instrumento em 01 (uma) via, de igual teor e forma, para um só efeito, mandando arquivar a original na Junta Comercial do Distrito Federal, para devido registro.

Brasília – DF, 23 de agosto de 2021.

JOSÉ ANDRÉ MENDES COIMBRA

ANDRÉ CASIMIRO COSTA

GUILHERME LOPES MARANHÃO

PAMELLA RODRIGUES ANDRÉ

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1732609 em 16/09/2021 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA EPP, CNPJ 24425034000196 e protocolo DFP2100150699 - 30/08/2021. Autenticação: E375778F0DB6F2ABE134591EABDD103E3B12DF. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 21/113.421-0 e o código de segurança is7z Esta cópia foi autenticada digitalmente e assinada em 16/09/2021 por Maxmiliam Patriota Carneiro – Secretário-Geral.

Documento Principal

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
21/113.421-0	DFP2100150699	26/08/2021

Identificação do(s) Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	16/09/2021
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital		
029.485.647-19	GUILHERME LOPES MARANHAO	16/09/2021
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital, Selo Prata - Biometria Facial		
471.539.891-53	JOSE ANDRE MENDES COIMBRA	16/09/2021
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital		
058.022.651-40	PAMELLA RODRIGUES ANDRE	16/09/2021
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital		

Junta Comercial, Industrial e Serviços do Distrito Federal

TERMO DE AUTENTICAÇÃO - REGISTRO DIGITAL

Certifico que o ato, assinado digitalmente, da empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA EPP, de CNPJ 24.425.034/0001-96 e protocolado sob o número 21/113.421-0 em 30/08/2021, encontra-se registrado na Junta Comercial sob o número 1732609, em 16/09/2021. O ato foi deferido eletronicamente pelo examinador THAIS RODRIGUES CRUZ.

Certifica o registro, o Secretário-Geral, Maxmiliam Patriota Carneiro. Para sua validação, deverá ser acessado o sitio eletrônico do Portal de Serviços / Validar Documentos (https://portalservicos.jucis.df.gov.br/Portal/pages/imagemProcesso/viaUnica.jsf) e informar o número de protocolo e chave de segurança.

Capa de Processo

Assinante(s)		
CPF	Nome	Data Assinatura
471.539.891-53	JOSE ANDRE MENDES COIMBRA	16/09/2021
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital		
029.485.647-19	GUILHERME LOPES MARANHAO	16/09/2021
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital, Selo Prata - Biometria Facial		
923.876.321-68	ANDRE CASIMIRO COSTA	16/09/2021
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital		
058.022.651-40	PAMELLA RODRIGUES ANDRE	16/09/2021
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital		

A autencidade desse documento pode ser conferida no portal de serviços da jucisdf informando o número do protocolo 21/113.421-0.

TERMO DE AUTENTICAÇÃO - REGISTRO DIGITAL

Documento Principal

Assinante(s)		
CPF	Nome	Data Assinatura
471.539.891-53	JOSE ANDRE MENDES COIMBRA	16/09/2021
Assinado utilizando o(s) seguinte(s) selo(s) do Selo Ouro - Certificado Digital		
029.485.647-19	GUILHERME LOPES MARANHAO	16/09/2021
Assinado utilizando o(s) seguinte(s) selo(s) do Selo Ouro - Certificado Digital, Selo Prata - Biometria Facial		
923.876.321-68	ANDRE CASIMIRO COSTA	16/09/2021
Assinado utilizando o(s) seguinte(s) selo(s) do Selo Ouro - Certificado Digital		
058.022.651-40	PAMELLA RODRIGUES ANDRE	16/09/2021
Assinado utilizando o(s) seguinte(s) selo(s) do Selo Ouro - Certificado Digital		

Data de início dos efeitos do registro (art. 36, Lei 8.934/1994): 23/08/2021

Documento assinado eletronicamente por THAIS RODRIGUES CRUZ, Servidor(a) Público(a), em 16/09/2021, às 15:37.

A autencidade desse documento pode ser conferida no portal de serviços da jucisdf informando o número do protocolo 21/113.421-0.

O ato foi deferido e assinado digitalmente por :

Identificação do(s) Assinante(s)	
CPF	Nome
702.261.211-00	MAXMILIAM PATRIOTA CARNEIRO

Brasília. quinta-feira, 16 de setembro de 2021

Ministério da Indústria, Comércio Exterior e Serviços
Secretaria Especial da Micro e Pequena Empresa
Departamento de Registro Empresarial e Integração

Nº DO PROTOCOLO (Uso da Junta Comercial)

NIRE (da sede ou filial, quando a sede for em outra UF)	Código da Natureza Jurídica	Nº de Matrícula do Agente Auxiliar do Comércio
53202049896	2062	

1 - REQUERIMENTO

ILMO(A). SR.(A) PRESIDENTE DA Junta Comercial, Industrial e Serviços do Distrito Federal

Nome: JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA

(da Empresa ou do Agente Auxiliar do Comércio)

Nº FCN/REMP

SPP2230218286

requer a V.Sª o deferimento do seguinte ato:

Nº DE VIAS	CÓDIGO DO ATO	CÓDIGO DO EVENTO	QTDE	DESCRIÇÃO DO ATO / EVENTO
1	002			ALTERACAO
		051	1	CONSOLIDACAO DE CONTRATO/ESTATUTO
		026	1	ABERTURA DE FILIAL EM OUTRA UF

BRASILIA
Local

20 Abril 2022
Data

Representante Legal da Empresa / Agente Auxiliar do Comércio:
Nome: _____
Assinatura: _____
Telefone de Contato: _____

2 - USO DA JUNTA COMERCIAL

☐ DECISÃO SINGULAR ☐ DECISÃO COLEGIADA

Nome(s) Empresarial(ais) igual(ais) ou semelhante(s):

☐ SIM ☐ SIM

_____ _____
_____ _____
_____ _____
_____ _____
_____ _____

☐ NÃO ___/___/_____ _____ ☐ NÃO ___/___/_____ _____
Data Responsável Data Responsável

Processo em Ordem
À decisão

___/___/_____
Data

_____
Responsável

DECISÃO SINGULAR

	2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência
☐ Processo em exigência. (Vide despacho em folha anexa)				
☐ Processo deferido. Publique-se e arquive-se.	☐	☐	☐	☐
☐ Processo indeferido. Publique-se.				

___/___/_____ _____
Data Responsável

DECISÃO COLEGIADA

	2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência
☐ Processo em exigência. (Vide despacho em folha anexa)				
☐ Processo deferido. Publique-se e arquive-se.	☐	☐	☐	☐
☐ Processo indeferido. Publique-se.				

___/___/_____ _____ _____ _____
Data Vogal Vogal Vogal

Presidente da _____ Turma

OBSERVAÇÕES

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1828829 em 25/04/2022 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo SPP2230218286 - 30/03/2022. Autenticação: C9F6CC822DFE3AE878C6630D3167B9CF7858B. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 22/037.424-4 e o código de segurança cStT Esta cópia foi autenticada digitalmente e assinada em 25/04/2022 por Maxmiliam Patriota Carneiro – Secretário-Geral.

Capa de Processo

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
22/037.424-4	SPP2230218286	30/03/2022

Identificação do(s) Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	20/04/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital		

Junta Comercial, Industrial e Serviços do Distrito Federal

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1828829 em 25/04/2022 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo SPP2230218286 - 30/03/2022. Autenticação: C9F6CC822DFE3AE878C6630D3167B9CF7858B. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 22/037.424-4 e o código de segurança cStT Esta cópia foi autenticada digitalmente e assinada em 25/04/2022 por Maxmiliam Patriota Carneiro – Secretário-Geral.

5ª ALTERAÇÃO DO CONTRATO SOCIAL
JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA
NIRE 53202049896
CNPJ 24.425.034/0001-96

JOSÉ ANDRÉ MENDES COIMBRA, brasileiro, solteiro, estatistico, residente e domiciliado na SMPW QD 17 Conjunto 07 Lote 03, Nucleo Bandeirante, Brasilia/DF CEP 71.741-707, nascido em 26.01.1970, natural de Montes Claros/MG, filho de José André Coimbra e Terezinha Angelica Mendes Coimbra, portador da carteira de Identidade n°. 1.179.715 expedida pelo SSP/DF em 24.06.1987, e inscrito no CPF/MF sob o n°. 471.539.891-53;

ANDRÉ CASIMIRO COSTA, brasileiro, empresário, casado sob o regime de comunhão parcial de bens, residente e domiciliado no Condomínio Solar de Brasília, 0 Quadra 03, Conjunto 20, Casa 20, Setor Habitacional Jardim Botânico, Brasília/DF CEP 71.680-349, nascido em 03/06/1981, natural de Brasília/DF, filho de Herlandes Antônio da Costa e Maria do Socorro Casimiro Silva Costa, portador da carteira nacional de habilitação n° 007246677714, expedida pelo DETRAN/DF em 30/01/2020, e inscrito no CPF/MF sob o n° 923.876.321-68.

GUILHERME LOPES MARANHÃO, brasileiro, solteiro, empresário, residente e domiciliado no Q SHDB QL 32, Conjunto 20, QL 32, Casa 132, Setor de Habitações Individuais Sul, Brasília/DF CEP 71.676-200, nascido em 18/02/1975, natural do Rio de Janeiro/RJ, filho de Carlos Fernando dos Reis Maranhão e Tereza Cristina Lopes Maranhão, portador da carteira nacional de habilitação n° 05801102104, expedida pelo DETRAN/DF em 13/09/2018, e inscrito no CPF/MF sob o n° 029.485.647-19.

Únicos sócios componentes da sociedade limitada, **JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA**, estabelecida no SRTVN QUADRA 701, CONJUNTO C, N° 124, SALA 421, ALA B, PARTE "V", ASA NORTE, BRASÍLIA/DF, CEP: 70.719-903, inscrita no CNPJ sob o nº. 24.425.034/0001-96, com seu contrato social arquivado na JCDF sob o nº. 53202049896, por despacho em 21/03/2016. RESOLVEM alterar e consolidar de pleno e comum acordo as disposições contratuais vigentes, conforme a cláusulas e condições seguintes:

1. DA ABERTURA DA FILIAL
Os sócios decidem constituir uma filial situada a Alameda Rio Negro, 1105, Sala 71, Anexo 66, Alphaville Centro Industrial e Empresarial, Barueri/SP, 06454-000 a qual desempenhará as mesmas atividades da matriz.

Parágrafo Primeiro: As atividades empresariais da filial serão executadas, exclusivamente, de forma digital pela internet, salvo quando o contratante indicar local ou estabelecimento para tanto.

Parágrafo Segundo: Surgindo a necessidade de controle e manutenção de estoques, a Sociedade utilizará depósitos e ou armazéns de terceiros.

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1828829 em 25/04/2022 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo SPP2230218286 - 30/03/2022. Autenticação: C9F6CC822DFE3AE878C6630D3167B9CF7858B. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 22/037.424-4 e o código de segurança cStT Esta cópia foi autenticada digitalmente e assinada em 25/04/2022 por Maxmiliam Patriota Carneiro – Secretário-Geral.

2. DA CONSOLIDAÇÃO
Em face da alteração acordada, os sócios resolvem efetuar a Consolidação do Contrato Social, que passa a vigorar com a redação dada a seguir:

CONSOLIDAÇÃO DO CONTRATO SOCIAL
JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA

Cláusula 1º:
A sociedade gira sob a denominação social de **JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA.**

Parágrafo 1º. A sociedade tem como nome de fantasia "**PETACORP**".

Parágrafo 2º: A Sociedade é constituída sob a forma do tipo jurídico das Sociedades Limitadas.

Cláusula 2º: A sociedade tem sua sede no SRTVN QUADRA 701, CONJUNTO C, N° 124, SALA 421, ALA B, PARTE "V", ASA NORTE, BRASÍLIA/DF, CEP: 70.719-903, e pode constituir filiais, sucursais, escritórios e franquias em qualquer parte do território nacional ou no exterior, por deliberação dos sócios e, mediante alteração contratual para o devido fim.

Parágrafo Primeiro: A Sociedade possui uma filial situada a Alameda Rio Negro, 1105, Sala 71, Anexo 66, Alphaville Centro Industrial e Empresarial, Barueri/SP, 06454-000 a qual desempenhará as mesmas atividades da matriz.

Parágrafo Segundo: As atividades empresariais da filial serão executadas, exclusivamente, de forma digital pela internet, salvo quando o contratante indicar local ou estabelecimento para tanto.

Parágrafo Terceiro: Surgindo a necessidade de controle e manutenção de estoques, a Sociedade utilizará depósitos e ou armazéns de terceiros

Cláusula 3º: A sociedade tem como objetivo social:
- Comercialização, consultoria, representação importação e exportação de software;
- Comércio de equipamentos e suprimentos de informática;
- Agenciamento, corretagem ou intermediação de títulos em geral, valores mobiliários e contratos quaisquer ou agenciamento, corretagem ou intermediação de bens móveis ou imóveis, não abrangidos em outros itens ou subitens, inclusive aqueles realizados no âmbito de bolsas de mercadoria.

Cláusula 4º: O capital social é de R$ 1.000.000,00 (hum milhão de reais), representado por 1.000.000 (hum milhão) quotas no valor nominal de R$ 1,00 (um real) cada, cuja integralização pelos sócios se daráem moeda corrente do país e da seguinte forma:

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1828829 em 25/04/2022 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo SPP2230218286 - 30/03/2022. Autenticação: C9F6CC822DFE3AE878C6630D3167B9CF7858B. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 22/037.424-4 e o código de segurança cStT Esta cópia foi autenticada digitalmente e assinada em 25/04/2022 por Maxmiliam Patriota Carneiro – Secretário-Geral.

Sócios	%	Quotas	Valor R$
JOSÉ ANDRÉ MENDES COIMBRA	33,34%	333.400	R$ 333.400,00
ANDRÉ CASIMIRO COSTA	33,33%	333.300	R$ 333.300,00
GUILHERME LOPES MARANHÃO	33,33%	333.300	R$ 333.300,00
TOTAL	**100 %**	**1.000.000**	**R$ 1.000.000,00**

Cláusula 5º: As quotas da sociedade são indivisíveis e não poderão ser cedidas ou transferidas sem o expresso consentimento dos demais sócios, cabendo em igualdade de condições e preço, o direito de preferência ao sócio que queira adquiri-las. O sócio que pretenda ceder ou transferir toda ou parte de suas quotas deverá manifestar sua intenção por escrito aos outros sócios, assistindo a estes o prazo de 30 (trinta) dias para que possam exercer o direito de preferência, ou ainda, optar pela dissolução da sociedade antes mesmo da cessão ou transferência das cotas.

Cláusula 6º: Das responsabilidades de cada sócio é restrita ao valor de suas quotas, mas todas respondem solidariamente pela integralização do capital social.

Cláusula 7º: A administração da sociedade caberá a todos os sócios, cujos nos respectivos atos poderão ser executados de forma conjunta, com os poderes e atribuições de representação ativa e passiva na sociedade, judicial e extrajudicial, sempre podendo praticar todos os atos decorrentes do objeto social no interesse da sociedade, autorizado o uso do nome empresarial, vedado, no entanto, em atividades estranhas ao interesse da sociedade, ou assumir obrigações seja em favor de qualquer dos quotistas ou de terceiros, bem como onerar ou alienar bens imóveis da sociedade, sem autorização do outro sócio.

Cláusula 8º: A sociedade iniciou suas atividades em 11/03/2016 e seu prazo de duração é por tempo indeterminado.

Cláusula 9º: Ao termino de cada exercício social, em 31 dezembro os, administradores, sócios ou não, prestarão contas justificadas de sua gestão, procedendo à elaboração do inventário, do balanço patrimonial e do balanço de resultado econômico, cabendo aos sócios, na proporção de suas cotas, os lucros ou perdas apuradas.

Parágrafo Único: Nos quatro meses seguintes ao término do exercício social, os sócios deliberarão sobre as contas e designarão administrador, quando for o caso.

Cláusula 10º: Os sócios poderão de comum acordo, fixar uma retirada mensal, a título de "pró-labore", observadas as disposições regulamentares pertinentes.

Cláusula 11º: Falecendo ou sendo interditado qualquer sócio (a), a sociedade continuará suas atividades com os herdeiros, sucessores e o incapaz. Não sendo possível ou inexistindo interesse destes ou do sócio remanescente, o valor de seus haveres será apurado e liquidado com base na situação patrimonial da sociedade, à data da resolução, verificada em balanço especialmente levantado.

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1828829 em 25/04/2022 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo SPP2230218286 - 30/03/2022. Autenticação: C9F6CC822DFE3AE878C6630D3167B9CF7858B. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 22/037.424-4 e o código de segurança cStT Esta cópia foi autenticada digitalmente e assinada em 25/04/2022 por Maxmiliam Patriota Carneiro – Secretário-Geral.

Parágrafo Único: O mesmo procedimento será adotado em outros casos em que a sociedade se resolva em relação a seu sócio.

Cláusula 12º: Os administradores declaram, sob pena da lei, de que não estão impedidos de exercer a administração da sociedade, por lei especial, ou em virtude de condenação criminal, ou por se encontrar sob os efeitos dela, a pena que vede, ainda que temporariamente, o acesso a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato, ou contra a economia popular, contra o sistema financeiro nacional, contra normas de defesa da concorrência, contra as relações de consumo, fé pública, ou à propriedade.

Cláusula 13º: Fica eleito o foro de Brasília (DF) para a solução de quaisquer dúvidas ou questões oriundas deste contrato, com desistência de qualquer outro, por parte dos sócios, por mais privilegiado que venha a ser.

E por estarem assim justos e contratados, assinam o presente instrumento em 3 (três) vias, de igual teor e forma para re na JUCESP.

São Paulo/SP, 17 de Março de 2022

JOSE ANDRE MENDES COIMBRA **ANDRE CASIMIRO COSTA**

GUILHERME LOPES MARANHÃO

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1828829 em 25/04/2022 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo SPP2230218286 - 30/03/2022. Autenticação: C9F6CC822DFE3AE878C6630D3167B9CF7858B. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 22/037.424-4 e o código de segurança cStT Esta cópia foi autenticada digitalmente e assinada em 25/04/2022 por Maxmiliam Patriota Carneiro – Secretário-Geral.

Documento Principal

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
22/037.424-4	SPP2230218286	30/03/2022

Identificação do(s) Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	20/04/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital		
029.485.647-19	GUILHERME LOPES MARANHAO	20/04/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital, Selo Prata - Banco do Brasil - Internet Banking, Selo Prata - Biometria Facial, Selo Prata - Cadastro via Internet Banking		
471.539.891-53	JOSE ANDRE MENDES COIMBRA	25/04/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital, Selo Prata - Biometria Facial		

Junta Comercial, Industrial e Serviços do Distrito Federal

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1828829 em 25/04/2022 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo SPP2230218286 - 30/03/2022. Autenticação: C9F6CC822DFE3AE878C6630D3167B9CF7858B. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 22/037.424-4 e o código de segurança cStT Esta cópia foi autenticada digitalmente e assinada em 25/04/2022 por Maxmiliam Patriota Carneiro – Secretário-Geral.

Relatório de Filiais Abertas

Informamos que, do processo 22/037.424-4 arquivado nesta Junta Comercial sob o número 1828829 em 25/04/2022 da empresa 5320204989-6 JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, consta a abertura da(s) seguinte(s) filial(ais):

NIRE	**ENDEREÇO**
xxxxxxx	ALAMEDA RIO NEGRO 1105 SALA 71 ANEXO 66 - BAIRRO ALPHAVILLE CENTRO INDUSTRIAL E EMPRESARIAL/ALPHAV CEP 06454-000 - BARUERI/SP

25/04/2022

TERMO DE AUTENTICAÇÃO - REGISTRO DIGITAL

Certifico que o ato, assinado digitalmente, da empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, de CNPJ 24.425.034/0001-96 e protocolado sob o número 22/037.424-4 em 30/03/2022, encontra-se registrado na Junta Comercial sob o número 1828829, em 25/04/2022. O ato foi deferido eletronicamente pelo examinador FILIPE MOREIRA GANDRA DOS SANTOS.

Certifica o registro, o Secretário-Geral, Maxmiliam Patriota Carneiro. Para sua validação, deverá ser acessado o sitio eletrônico do Portal de Serviços / Validar Documentos (https://portalservicos.jucis.df.gov.br/Portal/pages/imagemProcesso/viaUnica.jsf) e informar o número de protocolo e chave de segurança.

Capa de Processo

Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	20/04/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital		

Documento Principal

Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	20/04/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital		
029.485.647-19	GUILHERME LOPES MARANHAO	20/04/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital, Selo Prata - Banco do Brasil - Internet Banking, Selo Prata - Biometria Facial, Selo Prata - Cadastro via Internet Banking		
471.539.891-53	JOSE ANDRE MENDES COIMBRA	25/04/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital, Selo Prata - Biometria Facial		

Data de início dos efeitos do registro (art. 36, Lei 8.934/1994): 07/03/2022

Documento assinado eletronicamente por FILIPE MOREIRA GANDRA DOS SANTOS, Servidor(a) Público(a), em 25/04/2022, às 16:56.

A autencidade desse documento pode ser conferida no portal de serviços da jucisdf informando o número do protocolo 22/037.424-4.

Junta Comercial, Industrial e Serviços do Distrito Federal

O ato foi assinado digitalmente por :

Identificação do(s) Assinante(s)	
CPF	Nome
702.261.211-00	MAXMILIAM PATRIOTA CARNEIRO

Brasília. segunda-feira, 25 de abril de 2022

Ministério da Indústria, Comércio Exterior e Serviços
Secretaria Especial da Micro e Pequena Empresa
Departamento de Registro Empresarial e Integração

Nº DO PROTOCOLO (Uso da Junta Comercial)

NIRE (da sede ou filial, quando a sede for em outra UF)	Código da Natureza Jurídica	Nº de Matrícula do Agente Auxiliar do Comércio
53202049896	2062	

1 - REQUERIMENTO

ILMO(A). SR.(A) PRESIDENTE DA Junta Comercial, Industrial e Serviços do Distrito Federal

Nome: JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA

(da Empresa ou do Agente Auxiliar do Comércio)

Nº FCN/REMP

DFE2200468941

requer a V.Sª o deferimento do seguinte ato:

Nº DE VIAS	CÓDIGO DO ATO	CÓDIGO DO EVENTO	QTDE	DESCRIÇÃO DO ATO / EVENTO
1	002			ALTERACAO
		051	1	CONSOLIDACAO DE CONTRATO/ESTATUTO
		027	1	ALTERACAO DE FILIAL EM OUTRA UF

BRASILIA
Local

17 Novembro 2022
Data

Representante Legal da Empresa / Agente Auxiliar do Comércio:
Nome: _____
Assinatura: _____
Telefone de Contato: _____

2 - USO DA JUNTA COMERCIAL

☐ DECISÃO SINGULAR ☐ DECISÃO COLEGIADA

Nome(s) Empresarial(ais) igual(ais) ou semelhante(s):

☐ SIM

_____
_____
_____
_____
_____

☐ NÃO ___/___/_____ _____
Data Responsável

☐ SIM

_____
_____
_____
_____
_____

☐ NÃO ___/___/_____ _____
Data Responsável

Processo em Ordem
À decisão

___/___/_____
Data

_____
Responsável

DECISÃO SINGULAR

☐ Processo em exigência. (Vide despacho em folha anexa)
☐ Processo deferido. Publique-se e arquive-se.
☐ Processo indeferido. Publique-se.

2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência
☐	☐	☐	☐

___/___/_____ _____
Data Responsável

DECISÃO COLEGIADA

☐ Processo em exigência. (Vide despacho em folha anexa)
☐ Processo deferido. Publique-se e arquive-se.
☐ Processo indeferido. Publique-se.

2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência
☐	☐	☐	☐

___/___/_____ _____ _____ _____
Data Vogal Vogal Vogal

Presidente da _____ Turma

OBSERVAÇÕES

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1921513 em 21/11/2022 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2200468941 - 16/11/2022. Autenticação: 379B7A7ED6C72B8D3876A4FF34CABC8F9C4198. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 22/131.885-2 e o código de segurança zzag Esta cópia foi autenticada digitalmente e assinada em 21/11/2022 por Maxmiliam Patriota Carneiro Secretário-Geral.

Capa de Processo

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
22/131.885-2	DFE2200468941	04/11/2022

Identificação do(s) Assinante(s)		
CPF	Nome	Data Assinatura
471.539.891-53	JOSE ANDRE MENDES COIMBRA	21/11/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital, Selo Prata - Biometria Facial, Selo Prata - Cadastro via Internet Banking, Selo Prata - Itaú - Internet Banking		

Junta Comercial, Industrial e Serviços do Distrito Federal

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1921513 em 21/11/2022 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2200468941 - 16/11/2022. Autenticação: 379B7A7ED6C72B8D3876A4FF34CABC8F9C4198. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 22/131.885-2 e o código de segurança zzag Esta cópia foi autenticada digitalmente e assinada em 21/11/2022 por Maxmiliam Patriota Carneiro Secretário-Geral.

6ª ALTERAÇÃO DO CONTRATO SOCIAL
JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA
NIRE 53202049896
CNPJ 24.425.034/0001-96

JOSÉ ANDRÉ MENDES COIMBRA, brasileiro, solteiro, estatistico, residente e domiciliado na SMPW QD 17 Conjunto 07 Lote 03, Nucleo Bandeirante, Brasilia/DF CEP 71.741-707, nascido em 26.01.1970, natural de Montes Claros/MG, filho de José André Coimbra e Terezinha Angelica Mendes Coimbra, portador da carteira de Identidade n°. 1.179.715 expedida pelo SSP/DF em 24.06.1987, e inscrito no CPF/MF sob o n°. 471.539.891-53;

ANDRÉ CASIMIRO COSTA, brasileiro, empresário, casado sob o regime de comunhão parcial de bens, residente e domiciliado no Condomínio Solar de Brasília, 0 Quadra 03, Conjunto 20, Casa 20, Setor Habitacional Jardim Botânico, Brasília/DF CEP 71.680-349, nascido em 03/06/1981, natural de Brasília/DF, filho de Herlandes Antônio da Costa e Maria do Socorro Casimiro Silva Costa, portador da carteira nacional de habilitação n° 007246677714, expedida pelo DETRAN/DF em 30/01/2020, e inscrito no CPF/MF sob o n° 923.876.321-68.

GUILHERME LOPES MARANHÃO, brasileiro, solteiro, empresário, residente e domiciliado no Q SHDB QL 32, Conjunto 20, QL 32, Casa 132, Setor de Habitações Individuais Sul, Brasília/DF CEP 71.676-200, nascido em 18/02/1975, natural do Rio de Janeiro/RJ, filho de Carlos Fernando dos Reis Maranhão e Tereza Cristina Lopes Maranhão, portador da carteira nacional de habilitação n° 05801102104, expedida pelo DETRAN/DF em 13/09/2018, e inscrito no CPF/MF sob o n° 029.485.647-19.

Únicos sócios componentes da sociedade limitada, **JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA**, estabelecida no SRTVN QUADRA 701, CONJUNTO C, N° 124, SALA 421, ALA B, PARTE "V", ASA NORTE, BRASÍLIA/DF, CEP: 70.719-903, inscrita no CNPJ sob o nº. 24.425.034/0001-96, com seu contrato social arquivado na JCDF sob o nº. 53202049896, por despacho em 21/03/2016 e filial **JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA** estabelecida na Alameda Rio Negro, 1105, sala 71, anexo 66, Alphaville Centro Industrial e Empresarial/Alphav, Barueri, CEP: 06.454- 000, inscrita no CNPJ sob o n°. 24.425.034/0002-77, resolvem alterar e consolidar de pleno e comum acordo as disposições contratuais vigentes, conforme a cláusulas e condições seguintes:

1. DA ALTERAÇÃO DE ENDEREÇO DA FILIAL
1.1. Altera-se o endereço da filial para Alameda Rio Negro, 500, TORRE B; SALA: 501 A 508; ANDAR: 5Alphaville Centro Industrial e Empresarial/Alphav, Barueri, SP, CEP: 06454000.

2. DA CONSOLIDAÇÃO
2.1 Continuam em pleno vigor todas as demais cláusulas que não foram alvo de nenhuma alteração pelo presente instrumento particular e em razão do acima exposto, o Sócio decide consolidar o Contrato Social da Sociedade que passará a vigorar com a seguinte redação.

CONSOLIDAÇÃO DO CONTRATO SOCIAL
JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA

Cláusula 1º: Os sócios decidem, para incorporar a alteração expressamente mencionada no item, anterior, consolidar o ato de alteração da "**JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA",** passando este a ter a seguinte, nova e integral redação:

Parágrafo Primeiro. A sociedade tem como nome de fantasia "**PETACORP**".

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1921513 em 21/11/2022 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2200468941 - 16/11/2022. Autenticação: 379B7A7ED6C72B8D3876A4FF34CABC8F9C4198. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 22/131.885-2 e o código de segurança zzag Esta cópia foi autenticada digitalmente e assinada em 21/11/2022 por Maxmiliam Patriota Carneiro Secretário-Geral.

Cláusula 2º: A matriz tem sua sede no SRTVN QUADRA 701, CONJUNTO C, N° 124, SALA 421, ALA B, PARTE "V", ASA NORTE, BRASÍLIA/DF, CEP: 70.719-903, e pode constituir filiais, sucursais, escritórios e franquias em qualquer parte do território nacional ou no exterior, por deliberação dos sócios e, mediante alteração contratual para o devido fim.

Parágrafo Primeiro: A Sociedade possui uma filial situada a Rio Negro, 500, TORRE B; SALA: 501 A 508; ANDAR: 5 Alphaville Centro Industrial eEmpresarial/Alphav, Barueri, SP, CEP: 06454000.

Parágrafo Segundo: As atividades empresariais da filial serão executadas, exclusivamente, de formadigital pela internet, salvo quando o contratante indicar local ou estabelecimento para tanto.

Parágrafo Terceiro: Surgindo a necessidade de controle e manutenção de estoques, a Sociedade utilizará depósitos e ou armazéns de terceiros

Cláusula 3º: A sociedade tem como objetivo social:

COMERCIALIZACAO, CONSULTORIA, REPRESENTACAO IMPORTACAO E EXPORTACAO DE SOFTWARE, COMERCIO DE EQUIPAMENTOS E SUPRIMENTOS DE INFORMATICA, AGENCIAMENTO, CORRETAGEM OU INTERMEDIACAO DE TITULOS, VALORES MOBILIARIOS E CONTRATOS QUAISQUER OU AGENCIAMENTO, CORRETAGEM OU INTERMEDIACAO DE BENS MOVEIS OU IMOVEIS, NAO ABRANGIDOS EM OUTROS ITENS OU SUBITENS, INCLUSIVE AQUELES REALIZADOS NO AMBITO DE BOLSAS DE MERCADORIA.

Cláusula 4º: O capital social é de R$ 1.000.000,00 (um milhão de reais), representado por 1.000.000 (hum milhão) quotas no valor nominal de R$ 1,00 (um real) cada, cuja integralizaçãopelos sócios se daráem moeda corrente do país e da seguinte forma

Sócios	%	Quotas	Valor R$
JOSÉ ANDRÉ MENDESCOIMBRA	33,34 %	333.400	R$ 333.400,00
ANDRÉ CASIMIRO COSTA	33,33 %	333.300	R$ 333.300,00
GUILHERME LOPES MARANHÃO	33,33 %	333.300	R$ 333.300,00
TOTAL	**100 %**	**1.000.000**	**R$ 1.000.000,00**

Cláusula 5º: As quotas da sociedade são indivisíveis e não poderão ser cedidas ou transferidas sem o expresso consentimento dos demais sócios, cabendo em igualdade de condições e preço, o direito de preferência ao sócio que queira adquiri-las. O sócio que pretenda ceder ou transferir toda ou parte de suas quotas deverá manifestar sua intenção por escrito aos outros sócios, assistindo a estes o prazo de 30 (trinta) dias para que possam exercer o direito de preferência, ou ainda, optar pela dissolução da sociedade antes mesmo da cessão ou transferência das cotas.

Cláusula 6º: Das responsabilidades de cada sócio é restrita ao valor de suas quotas, mas todas respondem solidariamente pela integralização do capital social.

Cláusula 7º: A administração da sociedade caberá a todos os sócios, cujos nos respectivos atos poderão ser executados de forma conjunta, com os poderes e atribuições de representação ativa e passiva na sociedade, judicial e extrajudicial, sempre podendo praticar todos os atos decorrentes do objeto socialno interesse da sociedade, autorizado o uso do nome empresarial, vedado, no entanto, em atividades estranhas ao interesse da sociedade, ou assumir obrigações seja em favor de qualquer dos quotistas ou de terceiros, bem como onerar ou alienar bens imóveis da sociedade, sem autorização do outro sócio.

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1921513 em 21/11/2022 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2200468941 - 16/11/2022. Autenticação: 379B7A7ED6C72B8D3876A4FF34CABC8F9C4198. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 22/131.885-2 e o código de segurança zzag Esta cópia foi autenticada digitalmente e assinada em 21/11/2022 por Maxmiliam Patriota Carneiro Secretário-Geral.

Cláusula 8º: A sociedade iniciou suas atividades em 11/03/2016 e seu prazo de duração é por tempo indeterminado.

Cláusula 9º: Ao termino de cada exercício social, em 31 dezembro os, administradores, sócios ou não, prestarão contas justificadas de sua gestão, procedendo à elaboração do inventário, do balanço patrimonial e do balanço de resultado econômico, cabendo aos sócios, na proporção de suas cotas, os lucros ou perdas apuradas.

Parágrafo Único: Nos quatro meses seguintes ao término do exercício social, os sócios deliberarão sobre as contas e designarão administrador, quando for o caso.

Cláusula 10º: Os sócios poderão de comum acordo, fixar uma retirada mensal, a título de "pró-labore", observadas as disposições regulamentares pertinentes.

Cláusula 11º: Falecendo ou sendo interditado qualquer sócio(a), a sociedade continuará suas atividades com os herdeiros, sucessores e o incapaz. Não sendo possível ou inexistindo interesse destes ou do sócio remanescente, o valor de seus haveres será apurado e liquidado com base na situação patrimonial da sociedade, à data da resolução, verificada em balanço especialmente levantado.

Parágrafo Único: O mesmo procedimento será adotado em outros casos em que a sociedade se resolvaem relação a seu sócio.

Cláusula 12º: Os administradores declaram, sob pena da lei, de que não estão impedidos de exercer a administração da sociedade, por lei especial, ou em virtude de condenação criminal, ou por se encontrar sob os efeitos dela, a pena que vede, ainda que temporariamente, o acesso a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato, ou contra a economia popular, contra o sistema financeiro nacional, contra normas de defesa da concorrência, contra as relações de consumo, fé pública, ou à propriedade.

Cláusula 13º: Fica eleito o foro de Brasília (DF) para a solução de quaisquer dúvidas ou questões oriundas deste contrato, com desistência de qualquer outro, por parte dos sócios, por mais privilegiadoque venha a ser.

DA PROTEÇÃO DE DADOS (LGPD)

Cláusula 14º – Os sócios se comprometem a proteger todos os dados oriundos da sociedade aqui formada, na forma da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

Parágrafo Primeiro - Se qualquer dos sócios for responsável pelo vazamento de dados, deverá esta arcar com aseventuais consequências previstas na mesma lei citada.

Parágrafo Segundo - O sócio responsável pelos vazamentos de dados deverá indenizar a sócia prejudicada no montante de R$ 100.000,00 (cem mil reais), fora as demais penalidades impostas pela Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) e apuração de perdas e danos.

DA ASSINATURA ELETRÔNICA E/OU DIGITAL

Cláusula 15º – O presente instrumento será firmado através de assinatura eletrônica e/ou digital, certificada pelo Sistema Eletrônico de Informações do Ministério da Cidadania, garantida a eficácia das Cláusulas. As Partes envolvidas neste instrumento afirmam e declaram que esse poderá ser assinado eletronicamente através da plataforma "D4Sign", atualmente no endereço

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1921513 em 21/11/2022 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2200468941 - 16/11/2022. Autenticação: 379B7A7ED6C72B8D3876A4FF34CABC8F9C4198. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 22/131.885-2 e o código de segurança zzag Esta cópia foi autenticada digitalmente e assinada em 21/11/2022 por Maxmiliam Patriota Carneiro Secretário-Geral.

https://secure.d4sign.com.br, conformidade com o disposto § 1º do art. 10 da MPV 2.200-02/01, a assinatura deste termo pelo representante oficial da contratada, pressupõem declarada, de forma inequívoca, a sua a sua concordância, bem como o reconhecimento de validade e aceite do presente documento. Consigna-se no presente instrumento que a assinatura com Certificado Digital/eletrônica tem a mesma validade jurídica de um registro e autenticação feita em cartório, seja mediante utilizaçãode certificados e-CPF, e-CNPJ.

Parágrafo Primeiro: A assinatura deste instrumento pelas partes, pressupõe declarada, de forma inequívoca, a sua concordância, bem como o reconhecimento da validade e do aceite ao presente documento.

Parágrafo Segundo: A sua autenticidade poderá ser atestada a qualquer tempo, seguindo os procedimentos da certificação digital, não podendo, desta forma, as partes se oporem a sua utilização.

Brasília/DF, 31 de Outubro de 2022

JOSE ANDRE MENDES COIMBRA

ANDRE CASIMIRO COSTA

GUILHERME LOPES MARANHÃO

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1921513 em 21/11/2022 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2200468941 - 16/11/2022. Autenticação: 379B7A7ED6C72B8D3876A4FF34CABC8F9C4198. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 22/131.885-2 e o código de segurança zzag Esta cópia foi autenticada digitalmente e assinada em 21/11/2022 por Maxmiliam Patriota Carneiro Secretário-Geral.

Documento Principal

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
22/131.885-2	DFE2200468941	04/11/2022

Identificação do(s) Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	21/11/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital		
029.485.647-19	GUILHERME LOPES MARANHAO	21/11/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Biometria TSE, Selo Ouro - Certificado Digital, Selo Prata - Banco do Brasil - Internet Banking, Selo Prata - Biometria Facial, Selo Prata - Cadastro via Internet Banking		
471.539.891-53	JOSE ANDRE MENDES COIMBRA	21/11/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital, Selo Prata - Biometria Facial, Selo Prata - Cadastro via Internet Banking, Selo Prata - Itaú - Internet Banking		

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1921513 em 21/11/2022 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2200468941 - 16/11/2022. Autenticação: 379B7A7ED6C72B8D3876A4FF34CABC8F9C4198. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 22/131.885-2 e o código de segurança zzag Esta cópia foi autenticada digitalmente e assinada em 21/11/2022 por Maxmiliam Patriota Carneiro Secretário-Geral.

TERMO DE AUTENTICAÇÃO - REGISTRO DIGITAL

Certifico que o ato, assinado digitalmente, da empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, de CNPJ 24.425.034/0001-96 e protocolado sob o número 22/131.885-2 em 16/11/2022, encontra-se registrado na Junta Comercial sob o número 1921513, em 21/11/2022. O ato foi deferido eletronicamente pelo examinador MARIA APARECIDA CYPRIANO BARBOSA.

Certifica o registro, o Secretário-Geral, Maxmiliam Patriota Carneiro. Para sua validação, deverá ser acessado o sitio eletrônico do Portal de Serviços / Validar Documentos (https://portalservicos.jucis.df.gov.br/Portal/pages/imagemProcesso/viaUnica.jsf) e informar o número de protocolo e chave de segurança.

Capa de Processo

Assinante(s)		
CPF	Nome	Data Assinatura
471.539.891-53	JOSE ANDRE MENDES COIMBRA	21/11/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital, Selo Prata - Biometria Facial, Selo Prata - Cadastro via Internet Banking, Selo Prata - Itaú - Internet Banking		

Documento Principal

Assinante(s)		
CPF	Nome	Data Assinatura
029.485.647-19	GUILHERME LOPES MARANHAO	21/11/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Biometria TSE, Selo Ouro - Certificado Digital, Selo Prata - Banco do Brasil - Internet Banking, Selo Prata - Biometria Facial, Selo Prata - Cadastro via Internet Banking		
923.876.321-68	ANDRE CASIMIRO COSTA	21/11/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital		
471.539.891-53	JOSE ANDRE MENDES COIMBRA	21/11/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital, Selo Prata - Biometria Facial, Selo Prata - Cadastro via Internet Banking, Selo Prata - Itaú - Internet Banking		

Data de início dos efeitos do registro (art. 36, Lei 8.934/1994): 31/10/2022

Documento assinado eletronicamente por MARIA APARECIDA CYPRIANO BARBOSA, Servidor(a) Público(a), em 21/11/2022, às 15:20.

A autencidade desse documento pode ser conferida no portal de serviços da jucisdf informando o número do protocolo 22/131.885-2.

O ato foi assinado digitalmente por :

Identificação do(s) Assinante(s)	
CPF	Nome
702.261.211-00	MAXMILIAM PATRIOTA CARNEIRO

Brasília. segunda-feira, 21 de novembro de 2022

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1921513 em 21/11/2022 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2200468941 - 16/11/2022. Autenticação: 379B7A7ED6C72B8D3876A4FF34CABC8F9C4198. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 22/131.885-2 e o código de segurança zzag Esta cópia foi autenticada digitalmente e assinada em 21/11/2022 por Maxmiliam Patriota Carneiro Secretário-Geral.

Ministério da Indústria, Comércio Exterior e Serviços
Secretaria Especial da Micro e Pequena Empresa
Departamento de Registro Empresarial e Integração

Nº DO PROTOCOLO (Uso da Junta Comercial)

NIRE (da sede ou filial, quando a sede for em outra UF)	Código da Natureza Jurídica	Nº de Matrícula do Agente Auxiliar do Comércio
53202049896	2062	

1 - REQUERIMENTO

ILMO(A). SR.(A) PRESIDENTE DA Junta Comercial, Industrial e Serviços do Distrito Federal

Nome: JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA

(da Empresa ou do Agente Auxiliar do Comércio)

Nº FCN/REMP

DFP2200485526

requer a V.Sª o deferimento do seguinte ato:

Nº DE VIAS	CÓDIGO DO ATO	CÓDIGO DO EVENTO	QTDE	DESCRIÇÃO DO ATO / EVENTO
1	002			ALTERACAO
		051	1	CONSOLIDACAO DE CONTRATO/ESTATUTO
		2211	1	ALTERACAO DE ENDERECO DENTRO DO MESMO MUNICIPIO

BRASILIA
Local

22 Dezembro 2022
Data

Representante Legal da Empresa / Agente Auxiliar do Comércio:
Nome: _____
Assinatura: _____
Telefone de Contato: _____

2 - USO DA JUNTA COMERCIAL

☐ DECISÃO SINGULAR ☐ DECISÃO COLEGIADA

Nome(s) Empresarial(ais) igual(ais) ou semelhante(s):

☐ SIM ☐ SIM

_____ _____
_____ _____
_____ _____
_____ _____
_____ _____

☐ NÃO ___/___/_____ _____ ☐ NÃO ___/___/_____ _____
Data Responsável Data Responsável

Processo em Ordem
À decisão

___/___/_____
Data

_____
Responsável

DECISÃO SINGULAR

	2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência
☐ Processo em exigência. (Vide despacho em folha anexa)	☐	☐	☐	☐
☐ Processo deferido. Publique-se e arquive-se.				
☐ Processo indeferido. Publique-se.				

___/___/_____ _____
Data Responsável

DECISÃO COLEGIADA

	2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência
☐ Processo em exigência. (Vide despacho em folha anexa)	☐	☐	☐	☐
☐ Processo deferido. Publique-se e arquive-se.				
☐ Processo indeferido. Publique-se.				

___/___/_____ _____ _____ _____
Data Vogal Vogal Vogal

Presidente da _____ Turma

OBSERVAÇÕES

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1978176 em 26/12/2022 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFP2200485526 - 23/12/2022. Autenticação: ECE94AA12EDA50748864FFB2FF48D9ADC3CAB4. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 22/182.144-9 e o código de segurança yC1W Esta cópia foi autenticada digitalmente e assinada em 27/12/2022 por Maxmiliam Patriota Carneiro Secretário-Geral.

Capa de Processo

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
22/182.144-9	DFP2200485526	22/12/2022

Identificação do(s) Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	23/12/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital		
029.485.647-19	GUILHERME LOPES MARANHAO	22/12/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Biometria TSE, Selo Ouro - Certificado Digital, Selo Prata - Banco do Brasil - Internet Banking, Selo Prata - Biometria Facial, Selo Prata - Cadastro via Internet Banking		
471.539.891-53	JOSE ANDRE MENDES COIMBRA	22/12/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital, Selo Prata - Biometria Facial, Selo Prata - Cadastro via Internet Banking, Selo Prata - Itaú - Internet Banking		

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1978176 em 26/12/2022 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFP2200485526 - 23/12/2022. Autenticação: ECE94AA12EDA50748864FFB2FF48D9ADC3CAB4. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 22/182.144-9 e o código de segurança yC1W Esta cópia foi autenticada digitalmente e assinada em 27/12/2022 por Maxmiliam Patriota Carneiro Secretário-Geral.

EMPRESA BRASÍLIA DE CONTABILIDADE

7ª ALTERAÇÃO DO CONTRATO SOCIAL
JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA
NIRE 53202049896
CNPJ 24.425.034/0001-96

JOSÉ ANDRÉ MENDES COIMBRA, brasileiro, solteiro, estatistico, residente e domiciliado na SMPW QD 17 Conjunto 07 Lote 03, Núcleo Bandeirante, Brasilia/DF CEP 71.741-707, nascido em 26.01.1970, natural de Montes Claros/MG, filho de José André Coimbra e Terezinha Angelica Mendes Coimbra, portador da carteira de Identidade n°: 1.179.715 expedida pelo SSP/DF em 24.06.1987, e inscrito no CPF/MF sob o n°. 471.539.891-53;

ANDRÉ CASIMIRO COSTA, brasileiro, empresário, casado sob o regime de comunhão parcial de bens, residente e domiciliado no Condomínio Solar de Brasília, 0 Quadra 03, Conjunto 20, Casa 20, Setor Habitacional Jardim Botânico, Brasília/DF CEP 71.680-349, nascido em 03/06/1981, natural de Brasília/DF, filho de Herlandes Antônio da Costa e Maria do Socorro Casimiro Silva Costa, portador da carteira nacional de habilitação n° 007246677714, expedida pelo DETRAN/DF em 30/01/2020, e inscrito no CPF/MF sob o n° 923.876.321-68.

GUILHERME LOPES MARANHÃO, brasileiro, solteiro, empresário, residente e domiciliado no Q SHDB QL 32, Conjunto 20, QL 32, Casa 132, Setor de Habitações Individuais Sul, Brasília/DF CEP 71.676-200, nascido em 18/02/1975, natural do Rio de Janeiro/RJ, filho de Carlos Fernando dos Reis Maranhão e Tereza Cristina Lopes Maranhão, portador da carteira nacional de habilitação n° 05801102104, expedida pelo DETRAN/DF em 13/09/2018, e inscrito no CPF/MF sob o n° 029.485.647-19.

Únicos sócios componentes da sociedade limitada, **JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTD**A, estabelecida no SRTVN QUADRA 701, CONJUNTO C, N° 124, SALA 421, ALA B, PARTE "V", ASA NORTE, BRASÍLIA/DF, CEP: 70.719-903, inscrita no CNPJ sob o nº. 24.425.034/0001-96, com seu contrato social arquivado na JCDF sob o nº. 53202049896, por despacho em 21/03/2016 e filial **JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA** estabelecida na Alameda Rio Negro, 500, TORRE B; SALA: 501 A 508; ANDAR: 5Alphaville Centro Industrial e Empresarial/Alphav, Barueri, SP, CEP: 06.454-000, inscrita no CNPJ sob o n°. 24.425.034/0002-77, resolvem alterar e consolidar de pleno e comum acordo as disposições contratuais vigentes, conforme a cláusulas e condições seguintes:

1. DA ALTERAÇÃO DE ENDEREÇO DA MATRIZ
1.1 - Altera-se o endereço da matriz SCES TRECHO 2, CENTRO DE LAZER BEIRA LAGO, CONJ 08; LOJA 03; Asa Sul, Brasília – DF, CEP:70.200-002.

2. DA CONSOLIDAÇÃO
2.1 - Continuam em pleno vigor todas as demais cláusulas que não foram alvo de nenhuma alteração pelo presente instrumento particular e em razão do acima exposto, o Sócio decide consolidar o Contrato Social da Sociedade que passará a vigorar com a seguinte redação.

CONSOLIDAÇÃO DO CONTRATO SOCIAL
JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA

Cláusula 1º: Os sócios decidem, para incorporar a alteração expressamente mencionada no item, anterior, consolidar o ato de alteração da "**JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA**", passando este a ter a seguinte, nova e integral redação:

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1978176 em 26/12/2022 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFP2200485526 - 23/12/2022. Autenticação: ECE94AA12EDA50748864FFB2FF48D9ADC3CAB4. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 22/182.144-9 e o código de segurança yC1W Esta cópia foi autenticada digitalmente e assinada em 27/12/2022 por Maxmiliam Patriota Carneiro Secretário-Geral.

Parágrafo Primeiro. A sociedade tem como nome de fantasia "**PETACORP**".

Cláusula 2º: A matriz tem sua sede no SCES TRECHO 2, CENTRO DE LAZER BEIRA LAGO, CONJ: 08; LOJA: 03; Asa Sul, Brasilia – DF, CEP:70.200-002, e pode constituir filiais, sucursais, escritórios e franquias em qualquer parte do território nacional ou no exterior, por deliberação dos sócios e, mediante alteração contratual para o devido fim.

Parágrafo Primeiro: A Sociedade possui uma filial situada a Rio Negro, 500, TORRE B; SALA: 501 A 508; ANDAR: 5 Alphaville Centro Industrial eEmpresarial/Alphav, Barueri, SP, CEP: 06454-000.

Parágrafo Segundo: As atividades empresariais da filial serão executadas, exclusivamente, de forma digital pela internet, salvo quando o contratante indicar local ou estabelecimento para tanto.

Parágrafo Terceiro: Surgindo a necessidade de controle e manutenção de estoques, a Sociedade utilizará depósitos e ou armazéns de terceiros

Cláusula 3º: A sociedade tem como objetivo social:

COMERCIALIZACAO, CONSULTORIA, REPRESENTACAO IMPORTACAO E EXPORTACAO DE SOFTWARE, COMERCIO DE EQUIPAMENTOS E SUPRIMENTOS DE INFORMATICA, AGENCIAMENTO, CORRETAGEM OU INTERMEDIACAO DE TITULOS, VALORES MOBILIARIOS E CONTRATOS QUAISQUER OU AGENCIAMENTO, CORRETAGEM OU INTERMEDIACAO DE BENS MOVEIS OU IMOVEIS, NAO ABRANGIDOS EM OUTROS ITENS OU SUBITENS, INCLUSIVE AQUELES REALIZADOS NO AMBITO DE BOLSAS DE MERCADORIA.

Cláusula 4º: O capital social é de R$ 1.000.000,00 (um milhão de reais), representado por 1.000.000 (hum milhão) quotas no valor nominal de R$ 1,00 (um real) cada, cuja integralização pelos sócios se dará em moeda corrente do país e da seguinte forma

Sócios	%	Quotas	Valor R$
JOSÉ ANDRÉ MENDES COIMBRA	33,34 %	333.400	R$ 333.400,00
ANDRÉ CASIMIRO COSTA	33,33 %	333.300	R$ 333.300,00
GUILHERME LOPES MARANHÃO	33,33 %	333.300	R$ 333.300,00
TOTAL	**100 %**	**1.000.000**	**R$ 1.000.000,00**

Cláusula 5º: As quotas da sociedade são indivisíveis e não poderão ser cedidas ou transferidas sem o expresso consentimento dos demais sócios, cabendo em igualdade de condições e preço, o direito de preferência ao sócio que queira adquiri-las. O sócio que pretenda ceder ou transferir toda ou parte de suas quotas deverá manifestar sua intenção por escrito aos outros sócios, assistindo a estes o prazo de 30 (trinta) dias para que possam exercer o direito de preferência, ou ainda, optar pela dissolução da sociedade antes mesmo da cessão ou transferência das cotas.

Cláusula 6º: Das responsabilidades de cada sócio é restrita ao valor de suas quotas, mas todas respondem solidariamente pela integralização do capital social.

Cláusula 7º: A administração da sociedade caberá a todos os sócios, cujos nos respectivos atos poderão ser executados de forma conjunta ou isoladamente, com os poderes e atribuições de representação ativa e passiva na sociedade, judicial e extrajudicial, sempre podendo praticar todos os atos decorrentes do objeto social no interesse da sociedade, autorizado o uso do nome empresarial, vedado, no entanto, em atividades estranhas ao interesse da sociedade, ou assumir

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1978176 em 26/12/2022 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFP2200485526 - 23/12/2022. Autenticação: ECE94AA12EDA50748864FFB2FF48D9ADC3CAB4. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 22/182.144-9 e o código de segurança yC1W Esta cópia foi autenticada digitalmente e assinada em 27/12/2022 por Maxmiliam Patriota Carneiro Secretário-Geral.

obrigações seja em favor de qualquer dos quotistas ou de terceiros, bem como onerar ou alienar bens imóveis da sociedade, sem autorização do outro sócio.

Cláusula 8º: A sociedade iniciou suas atividades em 11/03/2016 e seu prazo de duração é por tempo indeterminado.

Cláusula 9º: Ao termino de cada exercício social, em 31 dezembro os, administradores, sócios ou não, prestarão contas justificadas de sua gestão, procedendo à elaboração do inventário, do balanço patrimonial e do balanço de resultado econômico, cabendo aos sócios, na proporção de suas cotas, os lucros ou perdas apuradas.

Parágrafo Único: Nos quatro meses seguintes ao término do exercício social, os sócios deliberarão sobre as contas e designarão administrador, quando for o caso.

Cláusula 10º: Os sócios poderão de comum acordo, fixar uma retirada mensal, a título de "pró-labore", observadas as disposições regulamentares pertinentes.

Cláusula 11º: Falecendo ou sendo interditado qualquer sócio(a), a sociedade continuará suas atividades com os herdeiros, sucessores e o incapaz. Não sendo possível ou inexistindo interesse destes ou do sócio remanescente, o valor de seus haveres será apurado e liquidado com base na situação patrimonial da sociedade, à data da resolução, verificada em balanço especialmente levantado.

Parágrafo Único: O mesmo procedimento será adotado em outros casos em que a sociedade se resolva em relação a seu sócio.

Cláusula 12º: Os administradores declaram, sob pena da lei, de que não estão impedidos de exercer a administração da sociedade, por lei especial, ou em virtude de condenação criminal, ou por se encontrar sob os efeitos dela, a pena que vede, ainda que temporariamente, o acesso a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato, ou contra a economia popular, contra o sistema financeiro nacional, contra normas de defesa da concorrência, contra as relações de consumo, fé pública, ou à propriedade.

Cláusula 13º: Fica eleito o foro de Brasília (DF) para a solução de quaisquer dúvidas ou questões oriundas deste contrato, com desistência de qualquer outro, por parte dos sócios, por mais privilegiado que venha a ser.

DA PROTEÇÃO DE DADOS (LGPD)

Cláusula 14º – Os sócios se comprometem a proteger todos os dados oriundos da sociedade aqui formada, na forma da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

Parágrafo Primeiro - Se qualquer dos sócios for responsável pelo vazamento de dados, deverá esta arcar com as eventuais consequências previstas na mesma lei citada.

Parágrafo Segundo - O sócio responsável pelos vazamentos de dados deverá indenizar a sócia prejudicada no montante de R$ 100.000,00 (cem mil reais), fora as demais penalidades impostas pela Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) e apuração de perdas e danos.

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1978176 em 26/12/2022 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFP2200485526 - 23/12/2022. Autenticação: ECE94AA12EDA50748864FFB2FF48D9ADC3CAB4. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 22/182.144-9 e o código de segurança yC1W Esta cópia foi autenticada digitalmente e assinada em 27/12/2022 por Maxmiliam Patriota Carneiro Secretário-Geral.

EMPRESA BRASÍLIA DE CONTABILIDADE

DA ASSINATURA ELETRÔNICA E/OU DIGITAL

Cláusula 15º – O presente instrumento será firmado através de assinatura eletrônica e/ou digital, certificada pelo Sistema Eletrônico de Informações do Ministério da Cidadania, garantida a eficácia das Cláusulas. As Partes envolvidas neste instrumento afirmam e declaram que esse poderá ser assinado eletronicamente através da plataforma "D4Sign", atualmente no endereço https://secure.d4sign.com.br, conformidade com o disposto § 1º do art. 10 da MPV 2.200-02/01, a assinatura deste termo pelo representante oficial da contratada, pressupõem declarada, de forma inequívoca, a sua a sua concordância, bem como o reconhecimento de validade e aceite do presente documento. Consigna-se no presente instrumento que a assinatura com Certificado Digital/eletrônica tem a mesma validade jurídica de um registro e autenticação feita em cartório, seja mediante utilização de certificados e-CPF, e-CNPJ.

Parágrafo Primeiro: A assinatura deste instrumento pelas partes, pressupõe declarada, de forma inequívoca, a sua concordância, bem como o reconhecimento da validade e do aceite ao presente documento.

Parágrafo Segundo: A sua autenticidade poderá ser atestada a qualquer tempo, seguindo os procedimentos da certificação digital, não podendo, desta forma, as partes se oporem a sua utilização.

Brasília/DF, 19 de dezembro de 2022

JOSE ANDRE MENDES COIMBRA
Sócio Administrador

ANDRE CASIMIRO COSTA
Sócio Administrador

GUILHERME LOPES MARANHÃO
Sócio Administrador

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1978176 em 26/12/2022 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFP2200485526 - 23/12/2022. Autenticação: ECE94AA12EDA50748864FFB2FF48D9ADC3CAB4. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 22/182.144-9 e o código de segurança yC1W Esta cópia foi autenticada digitalmente e assinada em 27/12/2022 por Maxmiliam Patriota Carneiro Secretário-Geral.

Documento Principal

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
22/182.144-9	DFP2200485526	22/12/2022

Identificação do(s) Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	23/12/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital		
029.485.647-19	GUILHERME LOPES MARANHAO	22/12/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Biometria TSE, Selo Ouro - Certificado Digital, Selo Prata - Banco do Brasil - Internet Banking, Selo Prata - Biometria Facial, Selo Prata - Cadastro via Internet Banking		
471.539.891-53	JOSE ANDRE MENDES COIMBRA	22/12/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital, Selo Prata - Biometria Facial, Selo Prata - Cadastro via Internet Banking, Selo Prata - Itaú - Internet Banking		

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1978176 em 26/12/2022 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFP2200485526 - 23/12/2022. Autenticação: ECE94AA12EDA50748864FFB2FF48D9ADC3CAB4. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 22/182.144-9 e o código de segurança yC1W Esta cópia foi autenticada digitalmente e assinada em 27/12/2022 por Maxmiliam Patriota Carneiro Secretário-Geral.

DECLARAÇÃO DE VERACIDADE DO DOCUMENTO PRINCIPAL
REGISTRO DIGITAL

Eu, JOSÉ ANDRÉ MENDES COIMBRA, BRASILEIRA, SOLTEIRO, EMPRESARIO, DATA DE NASCIMENTO 26/01/1970, RG Nº 1.179.715 SSP-DF, CPF 471.539.891-53, QUADRA SMPW QUADRA 17 CONJUNTO 7, Nº 03, BAIRRO PARK WAY, CEP 71741-707, BRASILIA - DF, DECLARO, SOB AS PENAS DA LEI, que os documentos apresentados digitalizados ao presente protocolo de registro digital na Junta Comercial, sem possibilidade de validação digital, SÃO VERDADEIROS E CONFEREM COM OS RESPECTIVOS ORIGINAIS.

Brasilia, 22 de dezembro de 2022.

JOSÉ ANDRÉ MENDES COIMBRA
Assinatura Eletrônica Avançada

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1978176 em 26/12/2022 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFP2200485526 - 23/12/2022. Autenticação: ECE94AA12EDA50748864FFB2FF48D9ADC3CAB4. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 22/182.144-9 e o código de segurança yC1W Esta cópia foi autenticada digitalmente e assinada em 27/12/2022 por Maxmiliam Patriota Carneiro Secretário-Geral.

TERMO DE AUTENTICAÇÃO - REGISTRO DIGITAL

Certifico que o ato, assinado digitalmente, da empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, de CNPJ 24.425.034/0001-96 e protocolado sob o número 22/182.144-9 em 23/12/2022, encontra-se registrado na Junta Comercial sob o número 1978176, em 26/12/2022. O ato foi deferido eletronicamente pelo examinador RAFAELA NASCIMENTO SILVA.

Certifica o registro, o Secretário-Geral, Maxmiliam Patriota Carneiro. Para sua validação, deverá ser acessado o sitio eletrônico do Portal de Serviços / Validar Documentos (https://portalservicos.jucis.df.gov.br/Portal/pages/imagemProcesso/viaUnica.jsf) e informar o número de protocolo e chave de segurança.

Capa de Processo

Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	23/12/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital		
029.485.647-19	GUILHERME LOPES MARANHAO	22/12/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Biometria TSE, Selo Ouro - Certificado Digital, Selo Prata - Banco do Brasil - Internet Banking, Selo Prata - Biometria Facial, Selo Prata - Cadastro via Internet Banking		
471.539.891-53	JOSE ANDRE MENDES COIMBRA	22/12/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital, Selo Prata - Biometria Facial, Selo Prata - Cadastro via Internet Banking, Selo Prata - Itaú - Internet Banking		

Documento Principal

Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	23/12/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital		
029.485.647-19	GUILHERME LOPES MARANHAO	22/12/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Biometria TSE, Selo Ouro - Certificado Digital, Selo Prata - Banco do Brasil - Internet Banking, Selo Prata - Biometria Facial, Selo Prata - Cadastro via Internet Banking		
471.539.891-53	JOSE ANDRE MENDES COIMBRA	22/12/2022
Assinado utilizando o(s) seguinte(s) selo(s) do gov.br Selo Ouro - Certificado Digital, Selo Prata - Biometria Facial, Selo Prata - Cadastro via Internet Banking, Selo Prata - Itaú - Internet Banking		

A autencidade desse documento pode ser conferida no portal de serviços da jucisdf informando o número do protocolo 22/182.144-9.

TERMO DE AUTENTICAÇÃO - REGISTRO DIGITAL

Declaração Documento Principal

Assinante(s)		
CPF	Nome	Data Assinatura
471.539.891-53	JOSÉ ANDRÉ MENDES COIMBRA	22/12/2022

Assinado utilizando o(s) seguinte(s) selo(s) do

Selo Ouro - Certificado Digital, Selo Prata - Biometria Facial, Selo Prata - Cadastro via Internet Banking, Selo Prata - Itaú - Internet Banking

Data de início dos efeitos do registro (art. 36, Lei 8.934/1994): 19/12/2022

Documento assinado eletronicamente por RAFAELA NASCIMENTO SILVA, Servidor(a) Público(a), em 26/12/2022, às 16:41.

A autencidade desse documento pode ser conferida no portal de serviços da jucisdf informando o número do protocolo 22/182.144-9.

Junta Comercial, Industrial e Serviços do Distrito Federal

O ato foi assinado digitalmente por :

Identificação do(s) Assinante(s)	
CPF	Nome
702.261.211-00	MAXMILIAM PATRIOTA CARNEIRO

Brasília. segunda-feira, 26 de dezembro de 2022

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 1978176 em 26/12/2022 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFP2200485526 - 23/12/2022. Autenticação: ECE94AA12EDA50748864FFB2FF48D9ADC3CAB4. Maxmiliam Patriota Carneiro - Secretário-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 22/182.144-9 e o código de segurança yC1W Esta cópia foi autenticada digitalmente e assinada em 27/12/2022 por Maxmiliam Patriota Carneiro Secretário-Geral.

Ministério da Indústria, Comércio Exterior e Serviços
Secretaria Especial da Micro e Pequena Empresa
Departamento de Registro Empresarial e Integração

Nº DO PROTOCOLO (Uso da Junta Comercial)

NIRE (da sede ou filial, quando a sede for em outra UF)	Código da Natureza Jurídica	Nº de Matrícula do Agente Auxiliar do Comércio
53202049896	2062	

1 - REQUERIMENTO

ILMO(A). SR.(A) PRESIDENTE DA Junta Comercial, Industrial e Serviços do Distrito Federal

Nome: JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA

(da Empresa ou do Agente Auxiliar do Comércio)

Nº FCN/REMP

DFE2300192671

requer a V.Sª o deferimento do seguinte ato:

Nº DE VIAS	CÓDIGO DO ATO	CÓDIGO DO EVENTO	QTDE	DESCRIÇÃO DO ATO / EVENTO
1	002			ALTERACAO
		051	1	CONSOLIDACAO DE CONTRATO/ESTATUTO
		026	1	ABERTURA DE FILIAL EM OUTRA UF

BRASILIA
Local

14 Setembro 2023
Data

Representante Legal da Empresa / Agente Auxiliar do Comércio:
Nome: _____
Assinatura: _____
Telefone de Contato: _____

2 - USO DA JUNTA COMERCIAL

☐ DECISÃO SINGULAR ☐ DECISÃO COLEGIADA

Nome(s) Empresarial(ais) igual(ais) ou semelhante(s):

☐ SIM ☐ SIM

_____ _____
_____ _____
_____ _____
_____ _____
_____ _____

☐ NÃO ___/___/_____ _____ ☐ NÃO ___/___/_____ _____
Data Responsável Data Responsável

Processo em Ordem
À decisão

___/___/_____
Data

_____
Responsável

DECISÃO SINGULAR

	2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência
☐ Processo em exigência. (Vide despacho em folha anexa)				
☐ Processo deferido. Publique-se e arquive-se.	☐	☐	☐	☐
☐ Processo indeferido. Publique-se.				

___/___/_____ _____
Data Responsável

DECISÃO COLEGIADA

	2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência
☐ Processo em exigência. (Vide despacho em folha anexa)				
☐ Processo deferido. Publique-se e arquive-se.	☐	☐	☐	☐
☐ Processo indeferido. Publique-se.				

___/___/_____ _____ _____ _____
Data Vogal Vogal Vogal

Presidente da _____ Turma

OBSERVAÇÕES

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2175050 em 15/09/2023 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2300192671 - 13/09/2023. Autenticação: D2F2FA2D45ADBA5974AAF7C7A8BDD4D9ABA414F. Anna Cláudia Leite Mesquita Garcia - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 23/118.730-1 e o código de segurança r4RB Esta cópia foi autenticada digitalmente e assinada em 18/09/2023 por Anna Cláudia Leite Mesquita Garcia Secretária-Geral.

Junta Comercial, Industrial e Serviços do Distrito Federal

JUNTA COMERCIAL, INDUSTRIAL E SERVIÇOS DO DISTRITO FEDERAL

Registro Digital

Capa de Processo

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
23/118.730-1	DFE2300192671	11/09/2023

Identificação do(s) Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	15/09/2023
Assinado utilizando assinaturas avançadas gov.br		

029.485.647-19	GUILHERME LOPES MARANHAO	15/09/2023
Assinado utilizando assinaturas avançadas gov.br		

471.539.891-53	JOSE ANDRE MENDES COIMBRA	15/09/2023
Assinado utilizando assinaturas avançadas gov.br		

VENTVRIS VENTIS

EMPRESA BRASÍLIA DE CONTABILIDADE

8ª ALTERAÇÃO DO CONTRATO SOCIAL
JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA
NIRE 53202049896
CNPJ 24.425.034/0001-96

JOSÉ ANDRÉ MENDES COIMBRA, brasileiro, solteiro, estatistico, residente e domiciliado na SMPW QD 17 Conjunto 07 Lote 03, Núcleo Bandeirante, Brasilia/DF CEP 71.741-707, nascido em 26.01.1970, natural de Montes Claros/MG, filho de José André Coimbra e Terezinha Angelica Mendes Coimbra, portador da carteira de Identidade n°: 1.179.715 expedida pelo SSP/DF em 24.06.1987, e inscrito no CPF/MF sob o n°. 471.539.891-53;

ANDRÉ CASIMIRO COSTA, brasileiro, empresário, casado sob o regime de comunhão parcial de bens, residente e domiciliado no Condomínio Solar de Brasília, 0 Quadra 03, Conjunto 20, Casa 20, Setor Habitacional Jardim Botânico, Brasília/DF CEP 71.680-349, nascido em 03/06/1981, natural de Brasília/DF, filho de Herlandes Antônio da Costa e Maria do Socorro Casimiro Silva Costa, portador da carteira nacional de habilitação n° 007246677714, expedida pelo DETRAN/DF em 30/01/2020, e inscrito no CPF/MF sob o n° 923.876.321-68.

GUILHERME LOPES MARANHÃO, brasileiro, solteiro, empresário, residente e domiciliado no Q SHDB QL 32, Conjunto 20, QL 32, Casa 132, Setor de Habitações Individuais Sul, Brasília/DF CEP 71.676-200, nascido em 18/02/1975, natural do Rio de Janeiro/RJ, filho de Carlos Fernando dos Reis Maranhão e Tereza Cristina Lopes Maranhão, portador da carteira nacional de habilitação n° 05801102104, expedida pelo DETRAN/DF em 13/09/2018, e inscrito no CPF/MF sob o n° 029.485.647-19.

Únicos sócios componentes da sociedade limitada, **JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTD**A, estabelecida no SCES TRECHO 2, CENTRO DE LAZER BEIRA LAGO, CONJ 08; LOJA 03; Asa Sul, Brasília – DF, CEP:70.200-002, inscrita no CNPJ sob o nº. 24.425.034/0001-96, com seu contrato social arquivado na JCDF sob o nº. 53202049896, por despacho em 21/03/2016 e filial **JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA** estabelecida na Alameda Rio Negro, 500, TORRE B; SALA: 501 A 508; ANDAR: 5Alphaville Centro Industrial e Empresarial/Alphav, Barueri, SP, CEP: 06.454-000, inscrita no CNPJ sob o n°. 24.425.034/0002-77, resolvem alterar e consolidar de pleno e comum acordo as disposições contratuais vigentes, conforme a cláusulas e condições seguintes:

1. DA ABERTURA DA FILIAL
Os sócios decidem constituir uma filial situada na RUA FRANCISCO DRUMOND, 41, EDIF MACEDO, ANDAR 1 SALA 103, CENTRO CAMAÇARI, BAHIA, CEP:42.800-063.

Parágrafo Primeiro: As atividades empresariais da filial serão executadas, exclusivamente, de forma digital pela internet, salvo quando o contratante indicar local ou estabelecimento para tanto.

Parágrafo Segundo: Surgindo a necessidade de controle e manutenção de estoques, a Sociedade utilizará depósitos e ou armazéns de terceiros.

2. DA CONSOLIDAÇÃO
Em face da alteração acordada, os sócios resolvem efetuar a Consolidação do Contrato Social, que passa a vigorar com a redação dada a seguir:

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2175050 em 15/09/2023 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2300192671 - 13/09/2023. Autenticação: D2F2FA2D45ADBA5974AAF7C7A8BDD4D9ABA414F. Anna Cláudia Leite Mesquita Garcia - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 23/118.730-1 e o código de segurança r4RB Esta cópia foi autenticada digitalmente e assinada em 18/09/2023 por Anna Cláudia Leite Mesquita Garcia Secretária-Geral.

CONSOLIDAÇÃO DO CONTRATO SOCIAL
JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA

Cláusula 1º: Os sócios decidem, para incorporar a alteração expressamente mencionada no item, anterior, consolidar o ato de alteração da "**JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA**", passando este a ter a seguinte, nova e integral redação:

Parágrafo Primeiro. A sociedade tem como nome de fantasia "**PETACORP**".

Cláusula 2º: A matriz tem sua sede no SCES TRECHO 2, CENTRO DE LAZER BEIRA LAGO, CONJ: 08; LOJA: 03; Asa Sul, Brasilia – DF, CEP:70.200-002, e pode constituir filiais, sucursais, escritórios e franquias em qualquer parte do território nacional ou no exterior, por deliberação dos sócios e, mediante alteração contratual para o devido fim.

Parágrafo Primeiro: A Sociedade possui uma filial situada a Rio Negro, 500, TORRE B; SALA: 501 A 508; ANDAR: 5 Alphaville Centro Industrial eEmpresarial/Alphav, Barueri, SP, CEP: 06454000, inscrita no CNPJ sob o n°. 24.425.034/0002-77.

Parágrafo Segundo: A Sociedade possui uma filial situada na RUA FRANCISCO DRUMOND, 41, EDIF MACEDO, ANDAR 1 SALA 103, CENTRO CAMAÇARI, BAHIA, CEP:42.800-063.

Parágrafo Terceiro: As atividades empresariais da filial serão executadas, exclusivamente, de forma digital pela internet, salvo quando o contratante indicar local ou estabelecimento para tanto.

Parágrafo Quarto: Surgindo a necessidade de controle e manutenção de estoques, a Sociedade utilizará depósitos e ou armazéns de terceiros

Cláusula 3º: A sociedade tem como objetivo social:

COMERCIALIZACAO, CONSULTORIA, REPRESENTACAO IMPORTACAO E EXPORTACAO DE SOFTWARE, COMERCIO DE EQUIPAMENTOS E SUPRIMENTOS DE INFORMATICA, AGENCIAMENTO, CORRETAGEM OU INTERMEDIACAO DE TITULOS, VALORES MOBILIARIOS E CONTRATOS QUAISQUER OU AGENCIAMENTO, CORRETAGEM OU INTERMEDIACAO DE BENS MOVEIS OU IMOVEIS, NAO ABRANGIDOS EM OUTROS ITENS OU SUBITENS, INCLUSIVE AQUELES REALIZADOS NO AMBITO DE BOLSAS DE MERCADORIA.

Cláusula 4º: O capital social é de R$ 1.000.000,00 (um milhão de reais), representado por 1.000.000 (hum milhão) quotas no valor nominal de R$ 1,00 (um real) cada, cuja integralização pelos sócios se dará em moeda corrente do país e da seguinte forma

Sócios	%	Quotas	Valor R$
JOSÉ ANDRÉ MENDES COIMBRA	33,34 %	333.400	R$ 333.400,00
ANDRÉ CASIMIRO COSTA	33,33 %	333.300	R$ 333.300,00
GUILHERME LOPES MARANHÃO	33,33 %	333.300	R$ 333.300,00
TOTAL	**100 %**	**1.000.000**	**R$ 1.000.000,00**

Cláusula 5º: As quotas da sociedade são indivisíveis e não poderão ser cedidas ou transferidas sem o expresso consentimento dos demais sócios, cabendo em igualdade de condições e preço, o direito de preferência ao sócio que queira adquiri-las. O sócio que pretenda ceder ou transferir toda ou parte de suas quotas deverá manifestar sua intenção por escrito aos outros sócios, assistindo a estes

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2175050 em 15/09/2023 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2300192671 - 13/09/2023. Autenticação: D2F2FA2D45ADBA5974AAF7C7A8BDD4D9ABA414F. Anna Cláudia Leite Mesquita Garcia - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 23/118.730-1 e o código de segurança r4RB Esta cópia foi autenticada digitalmente e assinada em 18/09/2023 por Anna Cláudia Leite Mesquita Garcia Secretária-Geral.

o prazo de 30 (trinta) dias para que possam exercer o direito de preferência, ou ainda, optar pela dissolução da sociedade antes mesmo da cessão ou transferência das cotas.

Cláusula 6º: Das responsabilidades de cada sócio é restrita ao valor de suas quotas, mas todas respondem solidariamente pela integralização do capital social.

Cláusula 7º: A administração da sociedade caberá a todos os sócios, cujos nos respectivos atos poderão ser executados de forma conjunta ou isoladamente, com os poderes e atribuições de representação ativa e passiva na sociedade, judicial e extrajudicial, sempre podendo praticar todos os atos decorrentes do objeto social no interesse da sociedade, autorizado o uso do nome empresarial, vedado, no entanto, em atividades estranhas ao interesse da sociedade, ou assumir obrigações seja em favor de qualquer dos quotistas ou de terceiros, bem como onerar ou alienar bens imóveis da sociedade, sem autorização do outro sócio.

Cláusula 8º: A sociedade iniciou suas atividades em 11/03/2016 e seu prazo de duração é por tempo indeterminado.

Cláusula 9º: Ao termino de cada exercício social, em 31 dezembro os, administradores, sócios ou não, prestarão contas justificadas de sua gestão, procedendo à elaboração do inventário, do balanço patrimonial e do balanço de resultado econômico, cabendo aos sócios, na proporção de suas cotas, os lucros ou perdas apuradas.

Parágrafo Único: Nos quatro meses seguintes ao término do exercício social, os sócios deliberarão sobre as contas e designarão administrador, quando for o caso.

Cláusula 10º: Os sócios poderão de comum acordo, fixar uma retirada mensal, a título de "pró-labore", observadas as disposições regulamentares pertinentes.

Cláusula 11º: Falecendo ou sendo interditado qualquer sócio(a), a sociedade continuará suas atividades com os herdeiros, sucessores e o incapaz. Não sendo possível ou inexistindo interesse destes ou do sócio remanescente, o valor de seus haveres será apurado e liquidado com base na situação patrimonial da sociedade, à data da resolução, verificada em balanço especialmente levantado.

Parágrafo Único: O mesmo procedimento será adotado em outros casos em que a sociedade se resolva em relação a seu sócio.

Cláusula 12º: Os administradores declaram, sob pena da lei, de que não estão impedidos de exercer a administração da sociedade, por lei especial, ou em virtude de condenação criminal, ou por se encontrar sob os efeitos dela, a pena que vede, ainda que temporariamente, o acesso a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato, ou contra a economia popular, contra o sistema financeiro nacional, contra normas de defesa da concorrência, contra as relações de consumo, fé pública, ou à propriedade.

Cláusula 13º: Fica eleito o foro de Brasília (DF) para a solução de quaisquer dúvidas ou questões oriundas deste contrato, com desistência de qualquer outro, por parte dos sócios, por mais privilegiado que venha a ser.

DA PROTEÇÃO DE DADOS (LGPD)

Cláusula 14º – Os sócios se comprometem a proteger todos os dados oriundos da sociedade aqui formada, na forma da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2175050 em 15/09/2023 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2300192671 - 13/09/2023. Autenticação: D2F2FA2D45ADBA5974AAF7C7A8BDD4D9ABA414F. Anna Cláudia Leite Mesquita Garcia - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 23/118.730-1 e o código de segurança r4RB Esta cópia foi autenticada digitalmente e assinada em 18/09/2023 por Anna Cláudia Leite Mesquita Garcia Secretária-Geral.

Parágrafo Primeiro - Se qualquer dos sócios for responsável pelo vazamento de dados, deverá esta arcar com as eventuais consequências previstas na mesma lei citada.

Parágrafo Segundo - O sócio responsável pelos vazamentos de dados deverá indenizar a sócia prejudicada no montante de R$ 100.000,00 (cem mil reais), fora as demais penalidades impostas pela Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) e apuração de perdas e danos.

DA ASSINATURA ELETRÔNICA E/OU DIGITAL

Cláusula 15º – O presente instrumento será firmado através de assinatura eletrônica e/ou digital, certificada pelo Sistema Eletrônico de Informações do Ministério da Cidadania, garantida a eficácia das Cláusulas. As Partes envolvidas neste instrumento afirmam e declaram que esse poderá ser assinado eletronicamente através da plataforma "D4Sign", atualmente no endereço https://secure.d4sign.com.br, conformidade com o disposto § 1º do art. 10 da MPV 2.200-02/01, a assinatura deste termo pelo representante oficial da contratada, pressupõem declarada, de forma inequívoca, a sua a sua concordância, bem como o reconhecimento de validade e aceite do presente documento. Consigna-se no presente instrumento que a assinatura com Certificado Digital/eletrônica tem a mesma validade jurídica de um registro e autenticação feita em cartório, seja mediante utilização de certificados e-CPF, e-CNPJ.

Parágrafo Primeiro: A assinatura deste instrumento pelas partes, pressupõe declarada, de forma inequívoca, a sua concordância, bem como o reconhecimento da validade e do aceite ao presente documento.

Parágrafo Segundo: A sua autenticidade poderá ser atestada a qualquer tempo, seguindo os procedimentos da certificação digital, não podendo, desta forma, as partes se oporem a sua utilização.

Brasília/DF, 04 de Setembro de 2023

JOSE ANDRE MENDES COIMBRA
Sócio Administrador

ANDRE CASIMIRO COSTA
Sócio Administrador

GUILHERME LOPES MARANHÃO
Sócio Administrador

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2175050 em 15/09/2023 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2300192671 - 13/09/2023. Autenticação: D2F2FA2D45ADBA5974AAF7C7A8BDD4D9ABA414F. Anna Cláudia Leite Mesquita Garcia - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 23/118.730-1 e o código de segurança r4RB Esta cópia foi autenticada digitalmente e assinada em 18/09/2023 por Anna Cláudia Leite Mesquita Garcia Secretária-Geral.

Documento Principal

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
23/118.730-1	DFE2300192671	11/09/2023

Identificação do(s) Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	15/09/2023
Assinado utilizando assinaturas avançadas		

029.485.647-19	GUILHERME LOPES MARANHAO	15/09/2023
Assinado utilizando assinaturas avançadas		

471.539.891-53	JOSE ANDRE MENDES COIMBRA	15/09/2023
Assinado utilizando assinaturas avançadas		

Junta Comercial, Industrial e Serviços do Distrito Federal

DECLARAÇÃO DE VERACIDADE DO DOCUMENTO PRINCIPAL
REGISTRO DIGITAL

Eu, JOSÉ ANDRÉ MENDES COIMBRA, BRASILEIRA, SOLTEIRO, EMPRESARIO, DATA DE NASCIMENTO 26/01/1970, RG Nº 1.179.715 SSP-DF, CPF 471.539.891-53, QUADRA SMPW QUADRA 17 CONJUNTO 7, Nº 03, BAIRRO PARK WAY, CEP 71741-707, BRASILIA - DF, DECLARO, SOB AS PENAS DA LEI, que os documentos apresentados digitalizados ao presente protocolo de registro digital na Junta Comercial, sem possibilidade de validação digital, SÃO VERDADEIROS E CONFEREM COM OS RESPECTIVOS ORIGINAIS.

Brasilia, 14 de setembro de 2023.

JOSÉ ANDRÉ MENDES COIMBRA
Assinatura Eletrônica Avançada

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2175050 em 15/09/2023 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2300192671 - 13/09/2023. Autenticação: D2F2FA2D45ADBA5974AAF7C7A8BDD4D9ABA414F. Anna Cláudia Leite Mesquita Garcia - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 23/118.730-1 e o código de segurança r4RB Esta cópia foi autenticada digitalmente e assinada em 18/09/2023 por Anna Cláudia Leite Mesquita Garcia Secretária-Geral.

TERMO DE AUTENTICAÇÃO - REGISTRO DIGITAL

Certifico que o ato, assinado digitalmente, da empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, de CNPJ 24.425.034/0001-96 e protocolado sob o número 23/118.730-1 em 13/09/2023, encontra-se registrado na Junta Comercial sob o número 2175050, em 15/09/2023. O ato foi deferido eletronicamente pelo examinador RAFAELA NASCIMENTO SILVA.

Certifica o registro, a Secretária-Geral, Anna Cláudia Leite Mesquita Garcia. Para sua validação, deverá ser acessado o sitio eletrônico do Portal de Serviços / Validar Documentos (https://portalservicos.jucis.df.gov.br/Portal/pages/imagemProcesso/viaUnica.jsf) e informar o número de protocolo e chave de segurança.

Capa de Processo

Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	15/09/2023
Assinado utilizando assinaturas avançadas		
029.485.647-19	GUILHERME LOPES MARANHAO	15/09/2023
Assinado utilizando assinaturas avançadas		
471.539.891-53	JOSE ANDRE MENDES COIMBRA	15/09/2023
Assinado utilizando assinaturas avançadas		

Documento Principal

Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	15/09/2023
Assinado utilizando assinaturas avançadas		
029.485.647-19	GUILHERME LOPES MARANHAO	15/09/2023
Assinado utilizando assinaturas avançadas		
471.539.891-53	JOSE ANDRE MENDES COIMBRA	15/09/2023
Assinado utilizando assinaturas avançadas		

Declaração Documento Principal

Assinante(s)		
CPF	Nome	Data Assinatura
471.539.891-53	JOSÉ ANDRÉ MENDES COIMBRA	15/09/2023
Assinado utilizando assinaturas avançadas		

Data de início dos efeitos do registro (art. 36, Lei 8.934/1994): 04/09/2023

A autencidade desse documento pode ser conferida no portal de serviços da jucisdf informando o número do protocolo 23/118.730-1.

TERMO DE AUTENTICAÇÃO - REGISTRO DIGITAL

Documento assinado eletronicamente por RAFAELA NASCIMENTO SILVA, Servidor(a) Público(a), em 15/09/2023, às 16:58.

A autencidade desse documento pode ser conferida no portal de serviços da jucisdf informando o número do protocolo 23/118.730-1.

Junta Comercial, Industrial e Serviços do Distrito Federal

Junta Comercial, Industrial e Serviços do Distrito Federal

O ato foi assinado digitalmente por :

Identificação do(s) Assinante(s)	
CPF	Nome
816.021.031-00	ANNA CLAUDIA LEITE MESQUITA GARCIA

Brasília. sexta-feira, 15 de setembro de 2023

Relatório de Filiais Abertas

Informamos que, do processo 23/118.730-1 arquivado nesta Junta Comercial sob o número 2175050 em 15/09/2023 da empresa 5320204989-6 JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, consta a abertura da(s) seguinte(s) filial(ais):

NIRE	ENDEREÇO
2990206916-5	RUA FRANCISCO DRUMOND 41 EDIF MACEDO ANDAR 1 SALA 103 - BAIRRO CENTRO CEP 42800-063 - CAMACARI/BA

15 de set de 2023

Ministério da Indústria, Comércio Exterior e Serviços
Secretaria Especial da Micro e Pequena Empresa
Departamento de Registro Empresarial e Integração

Nº DO PROTOCOLO (Uso da Junta Comercial)

NIRE (da sede ou filial, quando a sede for em outra UF)	Código da Natureza Jurídica	Nº de Matrícula do Agente Auxiliar do Comércio
53202049896	2062	

1 - REQUERIMENTO

ILMO(A). SR.(A) PRESIDENTE DA Junta Comercial, Industrial e Serviços do Distrito Federal

Nome: JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA

(da Empresa ou do Agente Auxiliar do Comércio)

Nº FCN/REMP

DFE2300210437

requer a V.Sª o deferimento do seguinte ato:

Nº DE VIAS	CÓDIGO DO ATO	CÓDIGO DO EVENTO	QTDE	DESCRIÇÃO DO ATO / EVENTO
1	002			ALTERACAO
		051	1	CONSOLIDACAO DE CONTRATO/ESTATUTO
		026	1	ABERTURA DE FILIAL EM OUTRA UF

BRASILIA
Local

5 Outubro 2023
Data

Representante Legal da Empresa / Agente Auxiliar do Comércio:
Nome: _____
Assinatura: _____
Telefone de Contato: _____

2 - USO DA JUNTA COMERCIAL

☐ DECISÃO SINGULAR ☐ DECISÃO COLEGIADA

Nome(s) Empresarial(ais) igual(ais) ou semelhante(s):

☐ SIM ☐ SIM

_____ _____
_____ _____
_____ _____
_____ _____
_____ _____

☐ NÃO ___/___/_____ _____ ☐ NÃO ___/___/_____ _____
Data Responsável Data Responsável

Processo em Ordem
À decisão

___/___/_____
Data

_____
Responsável

DECISÃO SINGULAR

	2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência
☐ Processo em exigência. (Vide despacho em folha anexa)	☐	☐	☐	☐
☐ Processo deferido. Publique-se e arquive-se.				
☐ Processo indeferido. Publique-se.				

___/___/_____ _____
Data Responsável

DECISÃO COLEGIADA

	2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência
☐ Processo em exigência. (Vide despacho em folha anexa)	☐	☐	☐	☐
☐ Processo deferido. Publique-se e arquive-se.				
☐ Processo indeferido. Publique-se.				

___/___/_____ _____ _____ _____
Data Vogal Vogal Vogal

Presidente da _____ Turma

OBSERVAÇÕES

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2188896 em 06/10/2023 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2300210437 - 03/10/2023. Autenticação: 8E638E14FB3F2817FE7F61FFB4B0F08D17CEF. Anna Cláudia Leite Mesquita Garcia - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 23/128.648-1 e o código de segurança 6uMe Esta cópia foi autenticada digitalmente e assinada em 06/10/2023 por Anna Cláudia Leite Mesquita Garcia Secretária-Geral.

Capa de Processo

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
23/128.648-1	DFE2300210437	03/10/2023

Identificação do(s) Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	05/10/2023
Assinado utilizando assinaturas avançadas gov.br		
029.485.647-19	GUILHERME LOPES MARANHAO	05/10/2023
Assinado utilizando assinaturas avançadas gov.br		
471.539.891-53	JOSE ANDRE MENDES COIMBRA	05/10/2023
Assinado utilizando assinaturas avançadas gov.br		

Junta Comercial, Industrial e Serviços do Distrito Federal

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2188896 em 06/10/2023 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2300210437 - 03/10/2023. Autenticação: 8E638E14FB3F2817FE7F61FFB4B0F08D17CEF. Anna Cláudia Leite Mesquita Garcia - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 23/128.648-1 e o código de segurança 6uMe Esta cópia foi autenticada digitalmente e assinada em 06/10/2023 por Anna Cláudia Leite Mesquita Garcia Secretária-Geral.

9ª ALTERAÇÃO DO CONTRATO SOCIAL
JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA
NIRE 53202049896
CNPJ 24.425.034/0001-96

JOSÉ ANDRÉ MENDES COIMBRA, brasileiro, solteiro, estatistico, residente e domiciliado na SMPW QD 17 Conjunto 07 Lote 03, Núcleo Bandeirante, Brasilia/DF CEP 71.741-707, nascido em 26.01.1970, natural de Montes Claros/MG, filho de José André Coimbra e Terezinha Angelica Mendes Coimbra, portador da carteira de Identidade n°: 1.179.715 expedida pelo SSP/DF em 24.06.1987, e inscrito no CPF/MF sob o n°. 471.539.891-53;

ANDRÉ CASIMIRO COSTA, brasileiro, empresário, casado sob o regime de comunhão parcial de bens, residente e domiciliado no Condomínio Solar de Brasília, 0 Quadra 03, Conjunto 20, Casa 20, Setor Habitacional Jardim Botânico, Brasília/DF CEP 71.680-349, nascido em 03/06/1981, natural de Brasília/DF, filho de Herlandes Antônio da Costa e Maria do Socorro Casimiro Silva Costa, portador da carteira nacional de habilitação n° 007246677714, expedida pelo DETRAN/DF em 30/01/2020, e inscrito no CPF/MF sob o n° 923.876.321-68.

GUILHERME LOPES MARANHÃO, brasileiro, solteiro, empresário, residente e domiciliado no Q SHDB QL 32, Conjunto 20, QL 32, Casa 132, Setor de Habitações Individuais Sul, Brasília/DF CEP 71.676-200, nascido em 18/02/1975, natural do Rio de Janeiro/RJ, filho de Carlos Fernando dos Reis Maranhão e Tereza Cristina Lopes Maranhão, portador da carteira nacional de habilitação n° 05801102104, expedida pelo DETRAN/DF em 13/09/2018, e inscrito no CPF/MF sob o n° 029.485.647-19.

Únicos sócios componentes da sociedade limitada, **JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTD**A, estabelecida no SCES TRECHO 2, CENTRO DE LAZER BEIRA LAGO, CONJ 08; LOJA 03; Asa Sul, Brasília – DF, CEP:70.200-002, inscrita no CNPJ sob o nº. 24.425.034/0001-96, com seu contrato social arquivado na JCDF sob o nº. 53202049896, por despacho em 21/03/2016, filial **JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA** estabelecida na Alameda Rio Negro, 500, TORRE B; SALA: 501 A 508; ANDAR: 5Alphaville Centro Industrial e Empresarial/Alphav, Barueri, SP, CEP: 06.454-000, inscrita no CNPJ sob o n°. 24.425.034/0002-77, filial **JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA** estabelecida na RUA FRANCISCO DRUMOND, 41, EDIF MACEDO, ANDAR 1 SALA 103, CENTRO CAMAÇARI, BAHIA, CEP:42.800-063, inscrita no CNPJ sob o n°. 24.425.034/0003-58, resolvem alterar e consolidar de pleno e comum acordo as disposições contratuais vigentes, conforme a cláusulas e condições seguintes:

1. DA ABERTURA DA FILIAL
Os sócios decidem constituir uma filial situada na AVENIDA JOSUE DI BERNARDI 185, SALA 31P, CAMPINAS, SÃO JOSE, SANTA CATARINA, CEP:88.101-200.

Parágrafo Primeiro: As atividades empresariais da filial serão executadas, exclusivamente, de forma digital pela internet, salvo quando o contratante indicar local ou estabelecimento para tanto.

Parágrafo Segundo: Surgindo a necessidade de controle e manutenção de estoques, a Sociedade utilizará depósitos e ou armazéns de terceiros.

2. DA CONSOLIDAÇÃO
Em face da alteração acordada, os sócios resolvem efetuar a Consolidação do Contrato Social, que passa a vigorar com a redação dada a seguir:

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2188896 em 06/10/2023 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2300210437 - 03/10/2023. Autenticação: 8E638E14FB3F2817FE7F61FFB4B0F08D17CEF. Anna Cláudia Leite Mesquita Garcia - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 23/128.648-1 e o código de segurança 6uMe Esta cópia foi autenticada digitalmente e assinada em 06/10/2023 por Anna Cláudia Leite Mesquita Garcia Secretária-Geral.

CONSOLIDAÇÃO DO CONTRATO SOCIAL
JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA

Cláusula 1º: Os sócios decidem, para incorporar a alteração expressamente mencionada no item, anterior, consolidar o ato de alteração da "**JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA**", passando este a ter a seguinte, nova e integral redação:

Parágrafo Primeiro. A sociedade tem como nome de fantasia "**PETACORP**".

Cláusula 2º: A matriz tem sua sede no SCES TRECHO 2, CENTRO DE LAZER BEIRA LAGO, CONJ: 08; LOJA: 03; Asa Sul, Brasilia – DF, CEP:70.200-002, e pode constituir filiais, sucursais, escritórios e franquias em qualquer parte do território nacional ou no exterior, por deliberação dos sócios e, mediante alteração contratual para o devido fim.

Parágrafo Primeiro: A Sociedade possui uma filial situada a Rio Negro, 500, TORRE B; SALA: 501 A 508; ANDAR: 5 Alphaville Centro Industrial eEmpresarial/Alphav, Barueri, SP, CEP: 06454000, inscrita no CNPJ sob o n°. 24.425.034/0002-77.

Parágrafo Segundo: A Sociedade possui uma filial situada na RUA FRANCISCO DRUMOND, 41, EDIF MACEDO, ANDAR 1 SALA 103, CENTRO CAMAÇARI, BAHIA, CEP:42.800-063, inscrita no CNPJ sob o n°. 24.425.034/0003-58.

Parágrafo Terceiro: A Sociedade possui uma filial situada na AVENIDA JOSUE DI BERNARDI 185, SALA 31P, CAMPINAS, SÃO JOSE, SANTA CATARINA, CEP:88.101-200.

Parágrafo Quarto: As atividades empresariais da filial serão executadas, exclusivamente, de forma digital pela internet, salvo quando o contratante indicar local ou estabelecimento para tanto.

Parágrafo Quinto: Surgindo a necessidade de controle e manutenção de estoques, a Sociedade utilizará depósitos e ou armazéns de terceiros

Cláusula 3º: A sociedade tem como objetivo social:

COMERCIALIZACAO, CONSULTORIA, REPRESENTACAO IMPORTACAO E EXPORTACAO DE SOFTWARE, COMERCIO DE EQUIPAMENTOS E SUPRIMENTOS DE INFORMATICA, AGENCIAMENTO, CORRETAGEM OU INTERMEDIACAO DE TITULOS, VALORES MOBILIARIOS E CONTRATOS QUAISQUER OU AGENCIAMENTO, CORRETAGEM OU INTERMEDIACAO DE BENS MOVEIS OU IMOVEIS, NAO ABRANGIDOS EM OUTROS ITENS OU SUBITENS, INCLUSIVE AQUELES REALIZADOS NO AMBITO DE BOLSAS DE MERCADORIA.

Cláusula 4º: O capital social é de R$ 1.000.000,00 (um milhão de reais), representado por 1.000.000 (hum milhão) quotas no valor nominal de R$ 1,00 (um real) cada, cuja integralização pelos sócios se dará em moeda corrente do país e da seguinte forma

Sócios	%	Quotas	Valor R$
JOSÉ ANDRÉ MENDES COIMBRA	33,34 %	333.400	R$ 333.400,00
ANDRÉ CASIMIRO COSTA	33,33 %	333.300	R$ 333.300,00
GUILHERME LOPES MARANHÃO	33,33 %	333.300	R$ 333.300,00
TOTAL	**100 %**	**1.000.000**	**R$ 1.000.000,00**

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2188896 em 06/10/2023 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2300210437 - 03/10/2023. Autenticação: 8E638E14FB3F2817FE7F61FFB4B0F08D17CEF. Anna Cláudia Leite Mesquita Garcia - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 23/128.648-1 e o código de segurança 6uMe Esta cópia foi autenticada digitalmente e assinada em 06/10/2023 por Anna Cláudia Leite Mesquita Garcia Secretária-Geral.

Cláusula 5º: As quotas da sociedade são indivisíveis e não poderão ser cedidas ou transferidas sem o expresso consentimento dos demais sócios, cabendo em igualdade de condições e preço, o direito de preferência ao sócio que queira adquiri-las. O sócio que pretenda ceder ou transferir toda ou parte de suas quotas deverá manifestar sua intenção por escrito aos outros sócios, assistindo a estes o prazo de 30 (trinta) dias para que possam exercer o direito de preferência, ou ainda, optar pela dissolução da sociedade antes mesmo da cessão ou transferência das cotas.

Cláusula 6º: Das responsabilidades de cada sócio é restrita ao valor de suas quotas, mas todas respondem solidariamente pela integralização do capital social.

Cláusula 7º: A administração da sociedade caberá a todos os sócios, cujos nos respectivos atos poderão ser executados de forma conjunta ou isoladamente, com os poderes e atribuições de representação ativa e passiva na sociedade, judicial e extrajudicial, sempre podendo praticar todos os atos decorrentes do objeto social no interesse da sociedade, autorizado o uso do nome empresarial, vedado, no entanto, em atividades estranhas ao interesse da sociedade, ou assumir obrigações seja em favor de qualquer dos quotistas ou de terceiros, bem como onerar ou alienar bens imóveis da sociedade, sem autorização do outro sócio.

Cláusula 8º: A sociedade iniciou suas atividades em 11/03/2016 e seu prazo de duração é por tempo indeterminado.

Cláusula 9º: Ao termino de cada exercício social, em 31 dezembro os, administradores, sócios ou não, prestarão contas justificadas de sua gestão, procedendo à elaboração do inventário, do balanço patrimonial e do balanço de resultado econômico, cabendo aos sócios, na proporção de suas cotas, os lucros ou perdas apuradas.

Parágrafo Único: Nos quatro meses seguintes ao término do exercício social, os sócios deliberarão sobre as contas e designarão administrador, quando for o caso.

Cláusula 10º: Os sócios poderão de comum acordo, fixar uma retirada mensal, a título de "pró-labore", observadas as disposições regulamentares pertinentes.

Cláusula 11º: Falecendo ou sendo interditado qualquer sócio(a), a sociedade continuará suas atividades com os herdeiros, sucessores e o incapaz. Não sendo possível ou inexistindo interesse destes ou do sócio remanescente, o valor de seus haveres será apurado e liquidado com base na situação patrimonial da sociedade, à data da resolução, verificada em balanço especialmente levantado.

Parágrafo Único: O mesmo procedimento será adotado em outros casos em que a sociedade se resolva em relação a seu sócio.

Cláusula 12º: Os administradores declaram, sob pena da lei, de que não estão impedidos de exercer a administração da sociedade, por lei especial, ou em virtude de condenação criminal, ou por se encontrar sob os efeitos dela, a pena que vede, ainda que temporariamente, o acesso a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato, ou contra a economia popular, contra o sistema financeiro nacional, contra normas de defesa da concorrência, contra as relações de consumo, fé pública, ou à propriedade.

Cláusula 13º: Fica eleito o foro de Brasília (DF) para a solução de quaisquer dúvidas ou questões oriundas deste contrato, com desistência de qualquer outro, por parte dos sócios, por mais privilegiado que venha a ser.

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2188896 em 06/10/2023 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2300210437 - 03/10/2023. Autenticação: 8E638E14FB3F2817FE7F61FFB4B0F08D17CEF. Anna Cláudia Leite Mesquita Garcia - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 23/128.648-1 e o código de segurança 6uMe Esta cópia foi autenticada digitalmente e assinada em 06/10/2023 por Anna Cláudia Leite Mesquita Garcia Secretária-Geral.

EMPRESA BRASÍLIA DE CONTABILIDADE

DA PROTEÇÃO DE DADOS (LGPD)

Cláusula 14º – Os sócios se comprometem a proteger todos os dados oriundos da sociedade aqui formada, na forma da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

Parágrafo Primeiro - Se qualquer dos sócios for responsável pelo vazamento de dados, deverá esta arcar com as eventuais consequências previstas na mesma lei citada.

Parágrafo Segundo - O sócio responsável pelos vazamentos de dados deverá indenizar a sócia prejudicada no montante de R$ 100.000,00 (cem mil reais), fora as demais penalidades impostas pela Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) e apuração de perdas e danos.

DA ASSINATURA ELETRÔNICA E/OU DIGITAL

Cláusula 15º – O presente instrumento será firmado através de assinatura eletrônica e/ou digital, certificada pelo Sistema Eletrônico de Informações do Ministério da Cidadania, garantida a eficácia das Cláusulas. As Partes envolvidas neste instrumento afirmam e declaram que esse poderá ser assinado eletronicamente através da plataforma "D4Sign", atualmente no endereço https://secure.d4sign.com.br, conformidade com o disposto § 1º do art. 10 da MPV 2.200-02/01, a assinatura deste termo pelo representante oficial da contratada, pressupõem declarada, de forma inequívoca, a sua a sua concordância, bem como o reconhecimento de validade e aceite do presente documento. Consigna-se no presente instrumento que a assinatura com Certificado Digital/eletrônica tem a mesma validade jurídica de um registro e autenticação feita em cartório, seja mediante utilização de certificados e-CPF, e-CNPJ.

Parágrafo Primeiro: A assinatura deste instrumento pelas partes, pressupõe declarada, de forma inequívoca, a sua concordância, bem como o reconhecimento da validade e do aceite ao presente documento.

Parágrafo Segundo: A sua autenticidade poderá ser atestada a qualquer tempo, seguindo os procedimentos da certificação digital, não podendo, desta forma, as partes se oporem a sua utilização.

Brasília/DF, 02 de Outubro de 2023

JOSE ANDRE MENDES COIMBRA
Sócio Administrador

ANDRE CASIMIRO COSTA
Sócio Administrador

GUILHERME LOPES MARANHÃO
Sócio Administrador

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2188896 em 06/10/2023 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2300210437 - 03/10/2023. Autenticação: 8E638E14FB3F2817FE7F61FFB4B0F08D17CEF. Anna Cláudia Leite Mesquita Garcia - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 23/128.648-1 e o código de segurança 6uMe Esta cópia foi autenticada digitalmente e assinada em 06/10/2023 por Anna Cláudia Leite Mesquita Garcia Secretária-Geral.

Documento Principal

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
23/128.648-1	DFE2300210437	03/10/2023

Identificação do(s) Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	05/10/2023
Assinado utilizando assinaturas avançadas gov.br		
029.485.647-19	GUILHERME LOPES MARANHAO	05/10/2023
Assinado utilizando assinaturas avançadas gov.br		
471.539.891-53	JOSE ANDRE MENDES COIMBRA	05/10/2023
Assinado utilizando assinaturas avançadas gov.br		

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2188896 em 06/10/2023 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2300210437 - 03/10/2023. Autenticação: 8E638E14FB3F2817FE7F61FFB4B0F08D17CEF. Anna Cláudia Leite Mesquita Garcia - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 23/128.648-1 e o código de segurança 6uMe Esta cópia foi autenticada digitalmente e assinada em 06/10/2023 por Anna Cláudia Leite Mesquita Garcia Secretária-Geral.

DECLARAÇÃO DE VERACIDADE DO DOCUMENTO PRINCIPAL
REGISTRO DIGITAL

Eu, JOSÉ ANDRÉ MENDES COIMBRA, BRASILEIRA, SOLTEIRO, EMPRESÁRIO, DATA DE NASCIMENTO 26/01/1970, RG Nº 1.179.715 SSP-DF, CPF 471.539.891-53, QUADRA SMPW QUADRA 17 CONJUNTO 7, Nº 03, BAIRRO PARK WAY, CEP 71741-707, BRASILIA - DF, DECLARO, SOB AS PENAS DA LEI, que os documentos apresentados digitalizados ao presente protocolo de registro digital na Junta Comercial, sem possibilidade de validação digital, SÃO VERDADEIROS E CONFEREM COM OS RESPECTIVOS ORIGINAIS.

Brasilia, 05 de outubro de 2023.

JOSÉ ANDRÉ MENDES COIMBRA
Assinatura Eletrônica Avançada

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2188896 em 06/10/2023 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2300210437 - 03/10/2023. Autenticação: 8E638E14FB3F2817FE7F61FFB4B0F08D17CEF. Anna Cláudia Leite Mesquita Garcia - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 23/128.648-1 e o código de segurança 6uMe Esta cópia foi autenticada digitalmente e assinada em 06/10/2023 por Anna Cláudia Leite Mesquita Garcia Secretária-Geral.

TERMO DE AUTENTICAÇÃO - REGISTRO DIGITAL

Certifico que o ato, assinado digitalmente, da empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, de CNPJ 24.425.034/0001-96 e protocolado sob o número 23/128.648-1 em 03/10/2023, encontra-se registrado na Junta Comercial sob o número 2188896, em 06/10/2023. O ato foi deferido eletronicamente pelo examinador CIBELLE NATHALY LUCENA DA SILVA GUEIROS.

Certifica o registro, a Secretária-Geral, Anna Cláudia Leite Mesquita Garcia. Para sua validação, deverá ser acessado o sitio eletrônico do Portal de Serviços / Validar Documentos (https://portalservicos.jucis.df.gov.br/Portal/pages/imagemProcesso/viaUnica.jsf) e informar o número de protocolo e chave de segurança.

Capa de Processo

Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	05/10/2023
Assinado utilizando assinaturas avançadas		
029.485.647-19	GUILHERME LOPES MARANHAO	05/10/2023
Assinado utilizando assinaturas avançadas		
471.539.891-53	JOSE ANDRE MENDES COIMBRA	05/10/2023
Assinado utilizando assinaturas avançadas		

Documento Principal

Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	05/10/2023
Assinado utilizando assinaturas avançadas		
029.485.647-19	GUILHERME LOPES MARANHAO	05/10/2023
Assinado utilizando assinaturas avançadas		
471.539.891-53	JOSE ANDRE MENDES COIMBRA	05/10/2023
Assinado utilizando assinaturas avançadas		

Declaração Documento Principal

Assinante(s)		
CPF	Nome	Data Assinatura
471.539.891-53	JOSÉ ANDRÉ MENDES COIMBRA	05/10/2023
Assinado utilizando assinaturas avançadas		

Data de início dos efeitos do registro (art. 36, Lei 8.934/1994): 02/10/2023

A autencidade desse documento pode ser conferida no portal de serviços da jucisdf informando o número do protocolo 23/128.648-1.

TERMO DE AUTENTICAÇÃO - REGISTRO DIGITAL

Documento assinado eletronicamente por CIBELLE NATHALY LUCENA DA SILVA GUEIROS, Servidor(a) Público(a), em 06/10/2023, às 07:13.

A autencidade desse documento pode ser conferida no portal de serviços da jucisdf informando o número do protocolo 23/128.648-1.

Junta Comercial, Industrial e Serviços do Distrito Federal

O ato foi assinado digitalmente por :

Identificação do(s) Assinante(s)	
CPF	Nome
816.021.031-00	ANNA CLAUDIA LEITE MESQUITA GARCIA

Brasília. sexta-feira, 06 de outubro de 2023

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2188896 em 06/10/2023 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2300210437 - 03/10/2023. Autenticação: 8E638E14FB3F2817FE7F61FFB4B0F08D17CEF. Anna Cláudia Leite Mesquita Garcia - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 23/128.648-1 e o código de segurança 6uMe Esta cópia foi autenticada digitalmente e assinada em 06/10/2023 por Anna Cláudia Leite Mesquita Garcia Secretária-Geral.

Relatório de Filiais Abertas

Informamos que, do processo 23/128.648-1 arquivado nesta Junta Comercial sob o número 2188896 em 06/10/2023 da empresa 5320204989-6 JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, consta a abertura da(s) seguinte(s) filial(ais):

NIRE	**ENDEREÇO**
4290213270-3	AVENIDA JOSUE DI BERNARDI 185 SALA 31P - BAIRRO CAMPINAS CEP 88101-200 - SAO JOSE/SC

6 de out de 2023

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2188896 em 06/10/2023 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2300210437 - 03/10/2023. Autenticação: 8E638E14FB3F2817FE7F61FFB4B0F08D17CEF. Anna Cláudia Leite Mesquita Garcia - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 23/128.648-1 e o código de segurança 6uMe Esta cópia foi autenticada digitalmente e assinada em 06/10/2023 por Anna Cláudia Leite Mesquita Garcia Secretária-Geral.

Ministério do Empreendedorismo, da Microempresa e da Empresa de Pequeno Porte
Secretaria Nacional de Microempresa e Empresa de Pequeno Porte
Diretoria Nacional de Registro Empresarial e Integração
Junta Comercial, Industrial e Serviços do Distrito Federal

Nº DO PROTOCOLO (Uso da Junta Comercial)

NIRE (da sede ou filial, quando a sede for em outra UF)	Código da Natureza Jurídica	Nº de Matrícula do Agente Auxiliar do Comércio
53202049896	2062	

1 - REQUERIMENTO

ILMO(A). SR.(A) PRESIDENTE DA Junta Comercial, Industrial e Serviços do Distrito Federal

Nome: JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA

(da Empresa ou do Agente Auxiliar do Comércio)

Nº FCN/REMP

DFE2400102528

requer a V.Sª o deferimento do seguinte ato:

Nº DE VIAS	CÓDIGO DO ATO	CÓDIGO DO EVENTO	QTDE	DESCRIÇÃO DO ATO / EVENTO
1	002			ALTERACAO
		051	1	CONSOLIDACAO DE CONTRATO/ESTATUTO
		027	1	ALTERACAO DE FILIAL EM OUTRA UF

BRASILIA
Local

21 Maio 2024
Data

Representante Legal da Empresa / Agente Auxiliar do Comércio:
Nome: _____
Assinatura: _____
Telefone de Contato: _____

2 - USO DA JUNTA COMERCIAL

☐ DECISÃO SINGULAR ☐ DECISÃO COLEGIADA

Nome(s) Empresarial(ais) igual(ais) ou semelhante(s):

☐ SIM

_____
_____
_____
_____
_____

☐ NÃO ___/___/_____ _____
Data Responsável

☐ SIM

_____
_____
_____
_____
_____

☐ NÃO ___/___/_____ _____
Data Responsável

Processo em Ordem
À decisão

___/___/_____
Data

_____
Responsável

DECISÃO SINGULAR

☐ Processo em exigência. (Vide despacho em folha anexa)
☐ Processo deferido. Publique-se e arquive-se.
☐ Processo indeferido. Publique-se.

2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência
☐	☐	☐	☐

___/___/_____ _____
Data Responsável

DECISÃO COLEGIADA

☐ Processo em exigência. (Vide despacho em folha anexa)
☐ Processo deferido. Publique-se e arquive-se.
☐ Processo indeferido. Publique-se.

2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência
☐	☐	☐	☐

___/___/_____ _____ _____ _____
Data Vogal Vogal Vogal

Presidente da _____ Turma

OBSERVAÇÕES

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2546341 em 21/05/2024 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2400102528 - 20/05/2024. Autenticação: 54EC3D3D11300AB927F4626AB16A3CBBC1B5FCB. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 24/071.625-6 e o código de segurança 1iOw Esta cópia foi autenticada digitalmente e assinada em 21/05/2024 por Fabianne Raissa da Fonseca Secretária-Geral.

Capa de Processo

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
24/071.625-6	DFE2400102528	20/05/2024

Identificação do(s) Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	21/05/2024
Assinado utilizando assinaturas avançadas		
029.485.647-19	GUILHERME LOPES MARANHAO	21/05/2024
Assinado utilizando assinaturas avançadas		
471.539.891-53	JOSE ANDRE MENDES COIMBRA	21/05/2024
Assinado utilizando assinaturas avançadas		

Junta Comercial, Industrial e Serviços do Distrito Federal

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2546341 em 21/05/2024 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2400102528 - 20/05/2024. Autenticação: 54EC3D3D11300AB927F4626AB16A3CBBC1B5FCB. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 24/071.625-6 e o código de segurança 1iOw Esta cópia foi autenticada digitalmente e assinada em 21/05/2024 por Fabianne Raissa da Fonseca Secretária-Geral.

DÉCIMA ALTERAÇÃO DO CONTRATO SOCIAL
JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA
NIRE 53 2 0204989-6
CNPJ 24.425.034/0001-96

JOSÉ ANDRÉ MENDES COIMBRA, brasileiro, solteiro, estat st co, residente e domiciliado na SMPW QD 17 Conjunto 07 Lote 03, Núcleo Bandeirante, Brasília/DF CEP: 71.741-707, nascido em 26.01.1970, natural de Montes Claros/MG, f lho de José André Coimbra e Terezinha Angelica Mendes Coimbra, portador da carteira de Ident dade n°: 1.179.715 expedida pelo SSP/DF em 24.06.1987, e inscrito no CPF/MF sob o n°. 471.539.891-53;

ANDRÉ CASIMIRO COSTA, brasileiro, empresário, casado sob o regime de comunhão parcial de bens, residente e domiciliado no Condomínio Solar de Brasília, 0 Quadra 03, Conjunto 20, Casa 20, Setor Habitacional Jardim Botânico, Brasília/DF CEP: 71.680-349, nascido em 03/06/1981, natural de Brasília/DF, f lho de Herlandes Antônio da Costa e Maria do Socorro Casimiro Silva Costa, portador da carteira nacional de habilitação n° 007246677714, expedida pelo DETRAN/DF em 30/01/2020, e inscrito no CPF/MF sob o n° 923.876.321-68;

GUILHERME LOPES MARANHÃO, brasileiro, solteiro, empresário, residente e domiciliado no Q SHDB QL 32, Conjunto 20, QL 32, Casa 132, Setor de Habitações Individuais Sul, Brasília/DF CEP 71.676-200, nascido em 18/02/1975, natural do Rio de Janeiro/RJ, f lho de Carlos Fernando dos Reis Maranhão e Tereza Crist na Lopes Maranhão, portador da carteira nacional de habilitação n° 05801102104, expedida pelo DETRAN/DF em 13/09/2018, e inscrito no CPF/MF sob o n° 029.485.647-19; Únicos sócios componentes da sociedade limitada, **JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA**, estabelecida no SCES TRECHO 2, CENTRO DE LAZER BEIRA LAGO, CONJ 08; LOJA 03; Asa Sul, Brasília – DF, CEP:70.200-002, inscrita no CNPJ sob o nº. 24.425.034/0001-96, com seu contrato social arquivado na JCDF sob o nº. 53 2 0204989-6, por despacho em 21/03/2016, **filial 1:** JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA estabelecida na Alameda Rio Negro, 500, TORRE B; SALA: 501 A 508; ANDAR: 5 Alphaville Centro Industrial e Empresarial/Alphav, Barueri, SP, CEP: 06.454-000, inscrita no CNPJ sob o n°. 24.425.034/0002-77, **filial 2:** JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA estabelecida na RUA FRANCISCO DRUMOND, 41, EDIF MACEDO, ANDAR 1 SALA 103, CENTRO CAMAÇARI, BAHIA, CEP:42.800-063, inscrita no CNPJ sob o n°. 24.425.034/0003-58; **filial 3:** JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA estabelecida na AVENIDA JOSUE DI BERNARDI 185, SALA 31P, CAMPINAS, SÃO JOSE, SANTA CATARINA, CEP:88.101-200 inscrita no CNPJ sob o n°. 24.425.034/0004-39, resolvem alterar e consolidar de pleno e comum acordo as disposições contratuais vigentes, conforme a cláusulas e condições seguintes:

1. DA ALTERAÇÃO DE ENDEREÇO DA FILIAL

O endereço da f lial **JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA** inscrita no CNPJ sob o n°. 24.425.034/0002-77, passa a ser: **Alameda Rio Negro n° 503, Conj. 2005, sala 02, Alphaville Centro Industrial e Empresarial/Alphav, Barueri – SP, CEP. 06.454-000.**

2. DA CONSOLIDAÇÃO

Em face da alteração acordada, os sócios resolvem efetuar a Consolidação do Contrato Social, que passa a vigorar com a redação dada a seguir:

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2546341 em 21/05/2024 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2400102528 - 20/05/2024. Autenticação: 54EC3D3D11300AB927F4626AB16A3CBBC1B5FCB. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 24/071.625-6 e o código de segurança 1iOw Esta cópia foi autenticada digitalmente e assinada em 21/05/2024 por Fabianne Raissa da Fonseca Secretária-Geral.

CONSOLIDAÇÃO DO CONTRATO SOCIAL
JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA

CLÁUSULA 1º: Os sócios decidem, para incorporar a alteração expressamente mencionada no item, anterior, consolidar o ato de alteração da **JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA**, passando este a ter a seguinte, nova e integral redação:

Parágrafo Primeiro. A sociedade tem como nome de fantasia **PETACORP**

CLÁUSULA 2º: A matriz tem sua sede no SCES TRECHO 2, CENTRO DE LAZER BEIRA LAGO, CONJ: 08; LOJA:03; Asa Sul, Brasília – DF, CEP:70.200-002, e pode const tuir f liais, sucursais, escritórios e franquias em qualquer parte do território nacional ou no exterior, por deliberação dos sócios e, mediante alteração contratual para o devido f m.

Parágrafo Primeiro: A Sociedade possui uma f lial situada Alameda Rio Negro n° 503, Conj. 2005, sala 02, Alphaville Centro Industrial e Empresarial/Alphav, Barueri – SP, CEP. 06.454-000, inscrita no CNPJ sob o n°. 24.425.034/0002-77.

Parágrafo Segundo: A Sociedade possui uma f lial situada na RUA FRANCISCO DRUMOND, 41, EDIF MACEDO, ANDAR 1 SALA 103, CENTRO CAMAÇARI, BAHIA, CEP:42.800-063, inscrita no CNPJ sob o n°. 24.425.034/0003-58.

Parágrafo Terceiro: A Sociedade possui uma f lial situada na AVENIDA JOSUE DI BERNARDI 185, SALA 31P, CAMPINAS, SÃO JOSE, SANTA CATARINA, CEP:88.101-200, inscrita no CNPJ sob o n°. 24.425.034/0004-39.

Parágrafo Quarto: As at vidades empresariais da f lial serão executadas, exclusivamente, de forma digital pela internet, salvo quando o contratante indicar local ou estabelecimento para tanto.

Parágrafo Quinto: Surgindo a necessidade de controle e manutenção de estoques, a Sociedade ut lizará depósitos e ou armazéns de terceiros

Cláusula 3º: A sociedade tem como objet vo social: COMERCIALIZACAO, CONSULTORIA, REPRESENTACAO IMPORTACAO E EXPORTACAO DE SOFTWARE, COMERCIO DE EQUIPAMENTOS E SUPRIMENTOS DE INFORMATICA, AGENCIAMENTO, CORRETAGEM OU INTERMEDIACAO DE TITULOS, VALORES MOBILIARIOS E CONTRATOS QUAISQUER OU AGENCIAMENTO, CORRETAGEM OU INTERMEDIACAO DE BENS MOVEIS OU IMOVEIS, NÃO ABRANGIDOS EM OUTROS ITENS OU SUBITENS, INCLUSIVE AQUELES REALIZADOS NO AMBITO DE BOLSAS DE MERCADORIA.

Cláusula 4º: O capital social é de R$ 1.000.000,00 (um milhão de reais), representado por 1.000.000 (hum milhão) quotas no valor nominal de R$ 1,00 (um real) cada, cuja integralização pelos sócios se dará em moeda corrente do país e da seguinte forma

SÓCIOS	QUOTAS	R$	%
JOSÉ ANDRÉ MENDES COIMBRA	Com 333.400 quotas totalizando	R$ 333.400,00	33,34%
ANDRÉ CASIMIRO COSTA	Com 333.300 quotas totalizando	R$ 333.300,00	33,33%
GUILHERME LOPES MARANHÃO	Com 333.300 quotas totalizando	R$ 333.300,00	33,33%
Total	**1.000.000 quotas totalizando**	**R$ 1.000.000,00**	**100%**

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2546341 em 21/05/2024 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2400102528 - 20/05/2024. Autenticação: 54EC3D3D11300AB927F4626AB16A3CBBC1B5FCB. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 24/071.625-6 e o código de segurança 1iOw Esta cópia foi autenticada digitalmente e assinada em 21/05/2024 por Fabianne Raissa da Fonseca Secretária-Geral.

Cláusula 5º: As quotas da sociedade são indivisíveis e não poderão ser cedidas ou transferidas sem o expresso consent mento dos demais sócios, cabendo em igualdade de condições e preço, o direito de preferência ao sócio que queira adquiri-las. O sócio que pretenda ceder ou transferir toda ou parte de suas quotas deverá manifestar sua intenção por escrito aos outros sócios, assist ndo a estes o prazo de 30 (trinta) dias para que possam exercer o direito de preferência, ou ainda, optar pela dissolução da sociedade antes mesmo da cessão ou transferência das cotas.

Cláusula 6º: Das responsabilidades de cada sócio é restrita ao valor de suas quotas, mas todas respondem solidariamente pela integralização do capital social.

Cláusula 7º: A administração da sociedade caberá a todos os sócios, cujos nos respect vos atos poderão ser executados de forma conjunta ou isoladamente, com os poderes e atribuições de representação at va e passiva na sociedade, judicial e extrajudicial, sempre podendo prat car todos os atos decorrentes do objeto social no interesse da sociedade, autorizado o uso do nome empresarial, vedado, no entanto, em at vidades estranhas ao interesse da sociedade, ou assumir obrigações seja em favor de qualquer dos quot stas ou de terceiros, bem como onerar ou alienar bens imóveis da sociedade, sem autorização do outro sócio.

Cláusula 8º: A sociedade iniciou suas at vidades em 11/03/2016 e seu prazo de duração é por tempo indeterminado.

Cláusula 9º: Ao termino de cada exercício social, em 31 dezembro os, administradores, sócios ou não, prestarão contas just f cadas de sua gestão, procedendo à elaboração do inventário, do balanço patrimonial e do balanço de resultado econômico, cabendo aos sócios, na proporção de suas cotas, os lucros ou perdas apuradas.

Parágrafo Único: Nos quatro meses seguintes ao término do exercício social, os sócios deliberarão sobre as contas e designarão administrador, quando for o caso.

Cláusula 10º: Os sócios poderão de comum acordo, f xar uma ret rada mensal, a t tulo de "pró-labore", observadas as disposições regulamentares pert nentes.

Cláusula 11º: Falecendo ou sendo interditado qualquer sócio(a), a sociedade cont nuará suas at vidades com os herdeiros, sucessores e o incapaz. Não sendo possível ou inexist ndo interesse destes ou do sócio remanescente, o valor de seus haveres será apurado e liquidado com base na situação patrimonial da sociedade, à data da resolução, verif cada em balanço especialmente levantado.

Parágrafo Único: O mesmo procedimento será adotado em outros casos em que a sociedade se resolva em relação a seu sócio.

Cláusula 12º: Os administradores declaram, sob pena da lei, de que não estão impedidos de exercer a administração da sociedade, por lei especial, ou em virtude de condenação criminal, ou por se encontrar sob os efeitos dela, a pena que vede, ainda que temporariamente, o acesso a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato, ou contra a economia popular, contra o sistema f nanceiro nacional, contra normas de defesa da concorrência, contra as relações de consumo, fé pública, ou à propriedade.

Cláusula 13º: Fica eleito o foro de Brasília (DF) para a solução de quaisquer dúvidas ou questões oriundas deste contrato, com desistência de qualquer outro, por parte dos sócios, por mais privilegiado que venha a ser.

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2546341 em 21/05/2024 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2400102528 - 20/05/2024. Autenticação: 54EC3D3D11300AB927F4626AB16A3CBBC1B5FCB. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 24/071.625-6 e o código de segurança 1iOw Esta cópia foi autenticada digitalmente e assinada em 21/05/2024 por Fabianne Raissa da Fonseca Secretária-Geral.

Cláusula 14º: Os sócios se comprometem a proteger todos os dados oriundos da sociedade aqui formada, na forma da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

Parágrafo Primeiro - Se qualquer dos sócios for responsável pelo vazamento de dados, deverá esta arcar com as eventuais consequências previstas na mesma lei citada.

Parágrafo Segundo - O sócio responsável pelos vazamentos de dados deverá indenizar a sócia prejudicada no montante de R$ 100.000,00 (cem mil reais), fora as demais penalidades impostas pela Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) e apuração de perdas e danos.

Cláusula 15º: O presente instrumento será f rmado através de assinatura eletrônica e/ou digital, cert f cada pelo Sistema Eletrônico de Informações do Ministério da Cidadania, garant da a ef cácia das Cláusulas. As Partes envolvidas neste instrumento af rmam e declaram que esse poderá ser assinado eletronicamente através da plataforma "D4Sign", atualmente no endereço ht ps://secure.d4sign.com.br, conformidade com o disposto § 1º do art. 10 da MPV 2.200-02/01, a assinatura deste termo pelo representante of cial da contratada, pressupõem declarada, de forma inequívoca, a sua a sua concordância, bem como o reconhecimento de validade e aceite do presente documento. Consigna-se no presente instrumento que a assinatura com Cert f cado Digital/eletrônica tem a mesma validade jurídica de um registro e autent cação feita em cartório, seja mediante ut lização de cert f cados e-CPF, e-CNPJ.

Parágrafo Primeiro: A assinatura deste instrumento pelas partes, pressupõe declarada, de forma inequívoca, a sua concordância, bem como o reconhecimento da validade e do aceite ao presente documento.

Parágrafo Segundo: A sua autent cidade poderá ser atestada a qualquer tempo, seguindo os procedimentos da cert f cação digital, não podendo, desta forma, as partes se oporem a sua ut lização.

Brasília/DF, 01 de maio de 2024.

JOSE ANDRE MENDES COIMBRA ANDRE CASIMIRO COSTA
Sócio Administrador

GUILHERME LOPES MARANHÃO
Sócio Administrador

ANDRE CASIMIRO COSTA
Sócio Administrador

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2546341 em 21/05/2024 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2400102528 - 20/05/2024. Autenticação: 54EC3D3D11300AB927F4626AB16A3CBBC1B5FCB. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 24/071.625-6 e o código de segurança 1iOw Esta cópia foi autenticada digitalmente e assinada em 21/05/2024 por Fabianne Raissa da Fonseca Secretária-Geral.

Documento Principal

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
24/071.625-6	DFE2400102528	20/05/2024

Identificação do(s) Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	21/05/2024
Assinado utilizando assinaturas avançadas gov.br		
029.485.647-19	GUILHERME LOPES MARANHAO	21/05/2024
Assinado utilizando assinaturas avançadas gov.br		
471.539.891-53	JOSE ANDRE MENDES COIMBRA	21/05/2024
Assinado utilizando assinaturas avançadas gov.br		

Junta Comercial, Industrial e Serviços do Distrito Federal

TERMO DE AUTENTICAÇÃO - REGISTRO DIGITAL

Certifico que o ato, assinado digitalmente, da empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, de CNPJ 24.425.034/0001-96 e protocolado sob o número 24/071.625-6 em 20/05/2024, encontra-se registrado na Junta Comercial sob o número 2546341, em 21/05/2024. O ato foi deferido eletronicamente pelo examinador MICHELINE OLIVEIRA GENNARI ANDRADE.

Certifica o registro, a Secretária-Geral, Fabianne Raissa da Fonseca. Para sua validação, deverá ser acessado o sitio eletrônico do Portal de Serviços / Validar Documentos (https://portalservicos.jucis.df.gov.br/Portal/pages/imagemProcesso/viaUnica.jsf) e informar o número de protocolo e chave de segurança.

Capa de Processo

Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	21/05/2024
Assinado utilizando assinaturas avançadas		
029.485.647-19	GUILHERME LOPES MARANHAO	21/05/2024
Assinado utilizando assinaturas avançadas		
471.539.891-53	JOSE ANDRE MENDES COIMBRA	21/05/2024
Assinado utilizando assinaturas avançadas		

Documento Principal

Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	21/05/2024
Assinado utilizando assinaturas avançadas		
029.485.647-19	GUILHERME LOPES MARANHAO	21/05/2024
Assinado utilizando assinaturas avançadas		
471.539.891-53	JOSE ANDRE MENDES COIMBRA	21/05/2024
Assinado utilizando assinaturas avançadas		

Data de início dos efeitos do registro (art. 36, Lei 8.934/1994): 01/05/2024

Documento assinado eletronicamente por MICHELINE OLIVEIRA GENNARI ANDRADE, Servidor(a) Público(a), em 21/05/2024, às 11:51.

A autencidade desse documento pode ser conferida no portal de serviços da jucisdf informando o número do protocolo 24/071.625-6.

O ato foi assinado digitalmente por :

Identificação do(s) Assinante(s)	
CPF	Nome
017.057.021-55	FABIANNE RAISSA DA FONSECA

Brasília. terça-feira, 21 de maio de 2024

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2546341 em 21/05/2024 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2400102528 - 20/05/2024. Autenticação: 54EC3D3D11300AB927F4626AB16A3CBBC1B5FCB. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 24/071.625-6 e o código de segurança 1iOw Esta cópia foi autenticada digitalmente e assinada em 21/05/2024 por Fabianne Raissa da Fonseca Secretária-Geral.

Ministério do Empreendedorismo, da Microempresa e da Empresa de Pequeno Porte
Secretaria Nacional de Microempresa e Empresa de Pequeno Porte
Diretoria Nacional de Registro Empresarial e Integração
Junta Comercial, Industrial e Serviços do Distrito Federal

Nº DO PROTOCOLO (Uso da Junta Comercial)

NIRE (da sede ou filial, quando a sede for em outra UF)	Código da Natureza Jurídica	Nº de Matrícula do Agente Auxiliar do Comércio
53202049896	2062	

1 - REQUERIMENTO

ILMO(A). SR.(A) PRESIDENTE DA Junta Comercial, Industrial e Serviços do Distrito Federal

Nome: JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA

(da Empresa ou do Agente Auxiliar do Comércio)

Nº FCN/REMP

DFE2500243803

requer a V.Sª o deferimento do seguinte ato:

Nº DE VIAS	CÓDIGO DO ATO	CÓDIGO DO EVENTO	QTDE	DESCRIÇÃO DO ATO / EVENTO
1	002			ALTERACAO
		051	1	CONSOLIDACAO DE CONTRATO/ESTATUTO
		021	1	ALTERACAO DE DADOS (EXCETO NOME EMPRESARIAL)
		027	1	ALTERACAO DE FILIAL EM OUTRA UF
		2221	1	ALTERACAO DO TITULO DO ESTABELECIMENTO (NOME DE FANTASIA)

BRASILIA
Local

27 Outubro 2025
Data

Representante Legal da Empresa / Agente Auxiliar do Comércio:
Nome: _____
Assinatura: _____
Telefone de Contato: _____

2 - USO DA JUNTA COMERCIAL

☐ DECISÃO SINGULAR ☐ DECISÃO COLEGIADA

Nome(s) Empresarial(ais) igual(ais) ou semelhante(s):

☐ SIM ☐ SIM

_____ _____
_____ _____
_____ _____
_____ _____
_____ _____

☐ NÃO ___/___/_____ _____ ☐ NÃO ___/___/_____ _____
Data Responsável Data Responsável

Processo em Ordem
À decisão

___/___/_____
Data

_____
Responsável

DECISÃO SINGULAR

	2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência
☐ Processo em exigência. (Vide despacho em folha anexa)	☐	☐	☐	☐
☐ Processo deferido. Publique-se e arquive-se.				
☐ Processo indeferido. Publique-se.				

___/___/_____ _____
Data Responsável

DECISÃO COLEGIADA

	2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência
☐ Processo em exigência. (Vide despacho em folha anexa)	☐	☐	☐	☐
☐ Processo deferido. Publique-se e arquive-se.				
☐ Processo indeferido. Publique-se.				

___/___/_____ _____ _____ _____
Data Vogal Vogal Vogal

Presidente da _____ Turma

OBSERVAÇÕES

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2856203 em 05/11/2025 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2500243803 - 03/11/2025. Autenticação: 94F5FA2F364B7BF69143956744111615EE2DC. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 25/161.824-2 e o código de segurança MRvG Esta cópia foi autenticada digitalmente e assinada em 05/11/2025 por Fabianne Raissa da Fonseca Secretária-Geral.

Capa de Processo

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
25/161.824-2	DFE2500243803	27/10/2025

Identificação do(s) Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	03/11/2025 11:56:04
Assinado utilizando assinaturas avançadas gov.br		
029.485.647-19	GUILHERME LOPES MARANHAO	29/10/2025 08:21:14
Assinado utilizando assinatura qualificada		
471.539.891-53	JOSE ANDRE MENDES COIMBRA	29/10/2025 08:25:35
Assinado utilizando assinatura qualificada		

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2856203 em 05/11/2025 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2500243803 - 03/11/2025. Autenticação: 94F5FA2F364B7BF69143956744111615EE2DC. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 25/161.824-2 e o código de segurança MRvG Esta cópia foi autenticada digitalmente e assinada em 05/11/2025 por Fabianne Raissa da Fonseca Secretária-Geral.

DÉCIMA ALTERAÇÃO DO CONTRATO SOCIAL
JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA
NIRE 53 2 0204989-6
CNPJ 24.425.034/0001-96

JOSÉ ANDRÉ MENDES COIMBRA, brasileiro, solteiro, estatístico, residente e domiciliado na SMPW QD 17 Conjunto 07 Lote 03, Núcleo Bandeirante, Brasília/DF CEP: 71.741-707, nascido em 26.01.1970, natural de Montes Claros/MG, filho de José André Coimbra e Terezinha Angelica Mendes Coimbra, portador da carteira de Identidade n°: 1.179.715 expedida pelo SSP/DF em 24.06.1987, e inscrito no CPF/MF sob o n°. 471.539.891-53;

ANDRÉ CASIMIRO COSTA, brasileiro, empresário, casado sob o regime de comunhão parcial de bens, residente e domiciliado no Condomínio Solar de Brasília, 0 Quadra 03, Conjunto 20, Casa 20, Setor Habitacional Jardim Botânico, Brasília/DF CEP: 71.680-349, nascido em 03/06/1981, natural de Brasília/DF, filho de Herlandes Antônio da Costa e Maria do Socorro Casimiro Silva Costa, portador da carteira nacional de habilitação n° 007246677714, expedida pelo DETRAN/DF em 30/01/2020, e inscrito no CPF/MF sob o n° 923.876.321-68;

GUILHERME LOPES MARANHÃO, brasileiro, solteiro, empresário, residente e domiciliado no Q SHDB QL 32, Conjunto 20, QL 32, Casa 132, Setor de Habitações Individuais Sul, Brasília/DF CEP 71.676-200, nascido em 18/02/1975, natural do Rio de Janeiro/RJ, filho de Carlos Fernando dos Reis Maranhão e Tereza Cristina Lopes Maranhão, portador da carteira nacional de habilitação n° 05801102104, expedida pelo DETRAN/DF em 13/09/2018, e inscrito no CPF/MF sob o n° 029.485.647-19; Únicos sócios componentes da sociedade limitada, JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA, estabelecida no SCES TRECHO 2, CENTRO DE LAZER BEIRA LAGO, CONJ 08; LOJA 03; Asa Sul, Brasília – DF, CEP:70.200-002, inscrita no CNPJ sob o nº. 24.425.034/0001-96, com seu contrato social arquivado na JCDF sob o nº. 53 2 0204989-6, por despacho em 21/03/2016, filial 1: JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA estabelecida na Alameda Rio Negro n° 503, Conj. 2005, sala 02, Alphaville Centro Industrial e Empresarial/Alphav, Barueri – SP, CEP. 06.454-000, inscrita no CNPJ sob o n°. 24.425.034/0002-77, filial 2: JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA estabelecida na RUA FRANCISCO DRUMOND, 41, EDIF MACEDO, ANDAR 1 SALA 103, CENTRO CAMAÇARI, BAHIA, CEP:42.800-063, inscrita no CNPJ sob o n°. 24.425.034/0003-58; filial 3: JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA estabelecida na AVENIDA JOSUE DI BERNARDI 185, SALA 31P, CAMPINAS, SÃO JOSE, SANTA CATARINA, CEP:88.101-200 inscrita no CNPJ sob o n°. 24.425.034/0004-39, resolvem alterar e consolidar de pleno e comum acordo as disposições contratuais vigentes, conforme a cláusulas e condições seguintes:

1. DA ALTERAÇÃO DE ENDEREÇO DA FILIAL

O endereço da filial JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA inscrita no CNPJ sob o n°. 24.425.034/0002-77, passa a ser: Alameda Rio Negro n° 503, Sala 2005, Alphaville Centro Industrial e Empresarial/Alphav, Barueri – SP, CEP. 06.454-000.

2. DA ALTERAÇÃO NO NOME FANTASIA

O nome fantasia passa a ser PETA.

3. DA CONSOLIDAÇÃO

Em face da alteração acordada, os sócios resolvem efetuar a Consolidação do Contrato Social, que passa a vigorar com a redação dada a seguir:

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2856203 em 05/11/2025 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2500243803 - 03/11/2025. Autenticação: 94F5FA2F364B7BF69143956744111615EE2DC. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 25/161.824-2 e o código de segurança MRvG Esta cópia foi autenticada digitalmente e assinada em 05/11/2025 por Fabianne Raissa da Fonseca Secretária-Geral.

CONSOLIDAÇÃO DO CONTRATO SOCIAL
JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA

CLÁUSULA 1º: Os sócios decidem, para incorporar a alteração expressamente mencionada no item, anterior, consolidar o ato de alteração da **JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA**, passando este a ter a seguinte, nova e integral redação:

Parágrafo Primeiro. A sociedade tem como nome de fantasia **PETA**

CLÁUSULA 2º: A matriz tem sua sede no SCES TRECHO 2, CENTRO DE LAZER BEIRA LAGO, CONJ: 08; LOJA:03; Asa Sul, Brasília – DF, CEP:70.200-002, e pode constituir filiais, sucursais, escritórios e franquias em qualquer parte do território nacional ou no exterior, por deliberação dos sócios e, mediante alteração contratual para o devido fim.

Parágrafo Primeiro: A Sociedade possui uma filial situada na Alameda Rio Negro n° 503, Sala 2005, Alphaville Centro Industrial e Empresarial/Alphav, Barueri – SP, CEP. 06.454-000, inscrita no CNPJ sob o n°. 24.425.034/0002-77.

Parágrafo Segundo: A Sociedade possui uma filial situada na Rua Francisco Drumond, 41, Edif Macedo, Andar 1 Sala 103, Centro Camaçari, Bahia, CEP: 42.800-063, inscrita no CNPJ sob o n°. 24.425.034/0003-58.

Parágrafo Terceiro: A Sociedade possui uma filial situada na Avenida Josue Di Bernardi 185, Sala 31p, Campinas, São Jose, Santa Catarina, CEP: 88.101-200, inscrita no CNPJ sob o n°. 24.425.034/0004-39.

Parágrafo Quarto: As atividades empresariais da filial serão executadas, exclusivamente, de forma digital pela internet, salvo quando o contratante indicar local ou estabelecimento para tanto.

Parágrafo Quinto: Surgindo a necessidade de controle e manutenção de estoques, a Sociedade utilizará depósitos e ou armazéns de terceiros

Cláusula 3º: A sociedade tem como objetivo social: **COMERCIALIZACAO, CONSULTORIA, REPRESENTACAO IMPORTACAO E EXPORTACAO DE SOFTWARE, COMERCIO DE EQUIPAMENTOS E SUPRIMENTOS DE INFORMATICA, AGENCIAMENTO, CORRETAGEM OU INTERMEDIACAO DE TITULOS, VALORES MOBILIARIOS E CONTRATOS QUAISQUER OU AGENCIAMENTO, CORRETAGEM OU INTERMEDIACAO DE BENS MOVEIS OU IMOVEIS, NÃO ABRANGIDOS EM OUTROS ITENS OU SUBITENS, INCLUSIVE AQUELES REALIZADOS NO AMBITO DE BOLSAS DE MERCADORIA**.

Cláusula 4º: O capital social é de R$ 1.000.000,00 (um milhão de reais), representado por 1.000.000 (um milhão) quotas no valor nominal de R$ 1,00 (um real) cada, cuja integralização pelos sócios se dará em moeda corrente do país e da seguinte forma:

SÓCIOS	QUOTAS	R$	%
JOSÉ ANDRÉ MENDES COIMBRA	333.400 quotas	R$ 333.400,00	33,34%
ANDRÉ CASIMIRO COSTA	333.300 quotas	R$ 333.300,00	33,33%
GUILHERME LOPES MARANHÃO	333.300 quotas	R$ 333.300,00	33,33%
Total	1.000.000 quotas	R$ 1.000.000,00	100%

Cláusula 5º: As quotas da sociedade são indivisíveis e não poderão ser cedidas ou transferidas sem o expresso consentimento dos demais sócios, cabendo em igualdade de condições e preço, o direito de preferência ao sócio que queira adquiri-las. O sócio que pretenda ceder ou transferir toda ou parte de suas quotas deverá manifestar sua intenção por escrito aos outros sócios, assistindo a estes o prazo de 30 (trinta) dias para que possam exercer o direito de preferência, ou ainda, optar pela dissolução da sociedade antes mesmo da cessão ou transferência das cotas.

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2856203 em 05/11/2025 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2500243803 - 03/11/2025. Autenticação: 94F5FA2F364B7BF69143956744111615EE2DC. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 25/161.824-2 e o código de segurança MRvG Esta cópia foi autenticada digitalmente e assinada em 05/11/2025 por Fabianne Raissa da Fonseca Secretária-Geral.

Cláusula 6º: Das responsabilidades de cada sócio é restrita ao valor de suas quotas, mas todas respondem solidariamente pela integralização do capital social.

Cláusula 7º: A administração da sociedade caberá a todos os sócios, cujos nos respectivos atos poderão ser executados de forma conjunta ou isoladamente, com os poderes e atribuições de representação ativa e passiva na sociedade, judicial e extrajudicial, sempre podendo praticar todos os atos decorrentes do objeto social no interesse da sociedade, autorizado o uso do nome empresarial, vedado, no entanto, em atividades estranhas ao interesse da sociedade, ou assumir obrigações seja em favor de qualquer dos quotistas ou de terceiros, bem como onerar ou alienar bens imóveis da sociedade, sem autorização do outro sócio.

Cláusula 8º: A sociedade iniciou suas atividades em 11/03/2016 e seu prazo de duração é por tempo indeterminado.

Cláusula 9º: Ao termino de cada exercício social, em 31 dezembro os, administradores, sócios ou não, prestarão contas justificadas de sua gestão, procedendo à elaboração do inventário, do balanço patrimonial e do balanço de resultado econômico, cabendo aos sócios, na proporção de suas cotas, os lucros ou perdas apuradas.

Parágrafo Único: Nos quatro meses seguintes ao término do exercício social, os sócios deliberarão sobre as contas e designarão administrador, quando for o caso.

Cláusula 10º: Os sócios poderão de comum acordo, fixar uma retirada mensal, a título de "prólabore", observadas as disposições regulamentares pertinentes.

Cláusula 11º: Falecendo ou sendo interditado qualquer sócio(a), a sociedade continuará suas atividades com os herdeiros, sucessores e o incapaz. Não sendo possível ou inexistindo interesse destes ou do sócio remanescente, o valor de seus haveres será apurado e liquidado com base na situação patrimonial da sociedade, à data da resolução, verificada em balanço especialmente levantado.

Parágrafo Único: O mesmo procedimento será adotado em outros casos em que a sociedade se resolva em relação a seu sócio.

Cláusula 12º: Os administradores declaram, sob pena da lei, de que não estão impedidos de exercer a administração da sociedade, por lei especial, ou em virtude de condenação criminal, ou por se encontrar sob os efeitos dela, a pena que vede, ainda que temporariamente, o acesso a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato, ou contra a economia popular, contra o sistema financeiro nacional, contra normas de defesa da concorrência, contra as relações de consumo, fé pública, ou à propriedade.

Cláusula 13º: Fica eleito o foro de Brasília (DF) para a solução de quaisquer dúvidas ou questões oriundas deste contrato, com desistência de qualquer outro, por parte dos sócios, por mais privilegiado que venha a ser.

Cláusula 14º: Os sócios se comprometem a proteger todos os dados oriundos da sociedade aqui formada, na forma da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

Parágrafo Primeiro - Se qualquer dos sócios for responsável pelo vazamento de dados, deverá esta arcar com as eventuais consequências previstas na mesma lei citada.

Parágrafo Segundo - O sócio responsável pelos vazamentos de dados deverá indenizar a sócia prejudicada no montante de R$ 100.000,00 (cem mil reais), fora as demais penalidades impostas pela Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) e apuração de perdas e danos.

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2856203 em 05/11/2025 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2500243803 - 03/11/2025. Autenticação: 94F5FA2F364B7BF69143956744111615EE2DC. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 25/161.824-2 e o código de segurança MRvG Esta cópia foi autenticada digitalmente e assinada em 05/11/2025 por Fabianne Raissa da Fonseca Secretária-Geral.

Cláusula 15º: O presente instrumento será firmado através de assinatura eletrônica e/ou digital, certificada pelo Sistema Eletrônico de Informações do Ministério da Cidadania, garantida a eficácia das Cláusulas. As Partes envolvidas neste instrumento afirmam e declaram que esse poderá ser assinado eletronicamente através da plataforma "D4Sign", atualmente no endereço https://secure.d4sign.com.br, conformidade com o disposto § 1º do art. 10 da MPV 2.200-02/01, a assinatura deste termo pelo representante oficial da contratada, pressupõem declarada, de forma inequívoca, a sua a sua concordância, bem como o reconhecimento de validade e aceite do presente documento. Consigna-se no presente instrumento que a assinatura com Certificado Digital/eletrônica tem a mesma validade jurídica de um registro e autenticação feita em cartório, seja mediante utilização de certificados e-CPF, e-CNPJ.

Parágrafo Primeiro: A assinatura deste instrumento pelas partes, pressupõe declarada, de forma inequívoca, a sua concordância, bem como o reconhecimento da validade e do aceite ao presente documento.

Parágrafo Segundo: A sua autenticidade poderá ser atestada a qualquer tempo, seguindo os procedimentos da certificação digital, não podendo, desta forma, as partes se oporem a sua utilização.

Brasília/DF, 01 de outubro de 2025.

JOSE ANDRE MENDES COIMBRA ANDRE CASIMIRO COSTA
Sócio Administrador

GUILHERME LOPES MARANHÃO
Sócio Administrador

ANDRE CASIMIRO COSTA
Sócio Administrador

LETICIA LEAL OLIVEIRA LAFETÁ
Advogada
65784 OAB – DF

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2856203 em 05/11/2025 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2500243803 - 03/11/2025. Autenticação: 94F5FA2F364B7BF69143956744111615EE2DC. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 25/161.824-2 e o código de segurança MRvG Esta cópia foi autenticada digitalmente e assinada em 05/11/2025 por Fabianne Raissa da Fonseca Secretária-Geral.

Documento Principal

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
25/161.824-2	DFE2500243803	27/10/2025

Identificação do(s) Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	03/11/2025 11:56:04
Assinado utilizando assinaturas avançadas gov.br		
029.485.647-19	GUILHERME LOPES MARANHAO	29/10/2025 08:21:15
Assinado utilizando assinatura qualificada		
471.539.891-53	JOSE ANDRE MENDES COIMBRA	29/10/2025 08:25:36
Assinado utilizando assinatura qualificada		
050.467.451-00	LETICIA LEAL OLIVEIRA LAFETÁ	28/10/2025 08:19:43
Assinado utilizando assinaturas avançadas gov.br		

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2856203 em 05/11/2025 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2500243803 - 03/11/2025. Autenticação: 94F5FA2F364B7BF69143956744111615EE2DC. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 25/161.824-2 e o código de segurança MRvG Esta cópia foi autenticada digitalmente e assinada em 05/11/2025 por Fabianne Raissa da Fonseca Secretária-Geral.

TERMO DE AUTENTICAÇÃO - REGISTRO DIGITAL

Certifico que o ato, assinado digitalmente, da empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, de CNPJ 24.425.034/0001-96 e protocolado sob o número 25/161.824-2 em 03/11/2025, encontra-se registrado na Junta Comercial sob o número 2856203, em 05/11/2025. O ato foi deferido eletronicamente pelo examinador FILIPE ELIEZER JACINTO DA SILVA.

Certifica o registro, a Secretária-Geral, Fabianne Raissa da Fonseca. Para sua validação, deverá ser acessado o sitio eletrônico do Portal de Serviços / Validar Documentos (https://portalservicos.jucis.df.gov.br/Portal/pages/imagemProcesso/viaUnica.jsf) e informar o número de protocolo e chave de segurança.

Capa de Processo

Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	03/11/2025
Assinado utilizando assinaturas avançadas		
029.485.647-19	GUILHERME LOPES MARANHAO	29/10/2025 08:21:14
Assinado utilizando assinatura qualificada	AC SEMPRE RFB v2	
471.539.891-53	JOSE ANDRE MENDES COIMBRA	29/10/2025 08:25:35
Assinado utilizando assinatura qualificada	AC SAFEWEB RFB v5	

Documento Principal

Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	03/11/2025
Assinado utilizando assinaturas avançadas		
029.485.647-19	GUILHERME LOPES MARANHAO	29/10/2025 08:21:15
Assinado utilizando assinatura qualificada	AC SEMPRE RFB v2	
471.539.891-53	JOSE ANDRE MENDES COIMBRA	29/10/2025 08:25:36
Assinado utilizando assinatura qualificada	AC SAFEWEB RFB v5	
050.467.451-00	LETICIA LEAL OLIVEIRA LAFETÁ	28/10/2025
Assinado utilizando assinaturas avançadas		

Data de início dos efeitos do registro (art. 36, Lei 8.934/1994): 05/11/2025

Documento assinado eletronicamente por FILIPE ELIEZER JACINTO DA SILVA, Servidor(a) Público(a), em 05/11/2025, às 15:35.

A autencidade desse documento pode ser conferida no portal de serviços da jucisdf informando o número do protocolo 25/161.824-2.

O ato foi assinado digitalmente por :

Identificação do(s) Assinante(s)	
CPF	Nome
017.057.021-55	FABIANNE RAISSA DA FONSECA

Brasília. quarta-feira, 05 de novembro de 2025

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2856203 em 05/11/2025 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2500243803 - 03/11/2025. Autenticação: 94F5FA2F364B7BF69143956744111615EE2DC. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 25/161.824-2 e o código de segurança MRvG Esta cópia foi autenticada digitalmente e assinada em 05/11/2025 por Fabianne Raissa da Fonseca Secretária-Geral.

Ministério do Empreendedorismo, da Microempresa e da Empresa de Pequeno Porte
Secretaria Nacional de Microempresa e Empresa de Pequeno Porte
Diretoria Nacional de Registro Empresarial e Integração
Junta Comercial, Industrial e Serviços do Distrito Federal

Nº DO PROTOCOLO (Uso da Junta Comercial)

NIRE (da sede ou filial, quando a sede for em outra UF)	Código da Natureza Jurídica	Nº de Matrícula do Agente Auxiliar do Comércio
53202049896	2062	

1 - REQUERIMENTO

ILMO(A). SR.(A) PRESIDENTE DA Junta Comercial, Industrial e Serviços do Distrito Federal

Nome: JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA

(da Empresa ou do Agente Auxiliar do Comércio)

Nº FCN/REMP

DFE2500277665

requer a V.Sª o deferimento do seguinte ato:

Nº DE VIAS	CÓDIGO DO ATO	CÓDIGO DO EVENTO	QTDE	DESCRIÇÃO DO ATO / EVENTO
1	002			ALTERACAO
		051	1	CONSOLIDACAO DE CONTRATO/ESTATUTO
		021	1	ALTERACAO DE DADOS (EXCETO NOME EMPRESARIAL)
		048	1	RE-RATIFICACAO

BRASILIA
Local

18 Dezembro 2025
Data

Representante Legal da Empresa / Agente Auxiliar do Comércio:
Nome: _____
Assinatura: _____
Telefone de Contato: _____

2 - USO DA JUNTA COMERCIAL

☐ DECISÃO SINGULAR ☐ DECISÃO COLEGIADA

Nome(s) Empresarial(ais) igual(ais) ou semelhante(s):

☐ SIM ☐ SIM

_____ _____
_____ _____
_____ _____
_____ _____
_____ _____

☐ NÃO ___/___/_____ _____ ☐ NÃO ___/___/_____ _____
Data Responsável Data Responsável

Processo em Ordem
À decisão

___/___/_____
Data

_____
Responsável

DECISÃO SINGULAR

	2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência
☐ Processo em exigência. (Vide despacho em folha anexa)	☐	☐	☐	☐
☐ Processo deferido. Publique-se e arquive-se.				
☐ Processo indeferido. Publique-se.				

___/___/_____ _____
Data Responsável

DECISÃO COLEGIADA

	2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência
☐ Processo em exigência. (Vide despacho em folha anexa)	☐	☐	☐	☐
☐ Processo deferido. Publique-se e arquive-se.				
☐ Processo indeferido. Publique-se.				

___/___/_____ _____ _____ _____
Data Vogal Vogal Vogal

Presidente da _____ Turma

OBSERVAÇÕES

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2881045 em 18/12/2025 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2500277665 - 04/12/2025. Autenticação: BE96C8D871DBC323F2A7233CDDE089D5268B68. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 25/186.265-8 e o código de segurança vy5S Esta cópia foi autenticada digitalmente e assinada em 19/12/2025 por Fabianne Raissa da Fonseca Secretária-Geral.

Capa de Processo

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
25/186.265-8	DFE2500277665	04/12/2025

Identificação do(s) Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	18/12/2025 12:15:51
Assinado utilizando assinatura qualificada		
029.485.647-19	GUILHERME LOPES MARANHAO	18/12/2025 12:02:05
Assinado utilizando assinatura qualificada		
471.539.891-53	JOSE ANDRE MENDES COIMBRA	18/12/2025 12:14:49
Assinado utilizando assinatura qualificada		

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2881045 em 18/12/2025 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2500277665 - 04/12/2025. Autenticação: BE96C8D871DBC323F2A7233CDDE089D5268B68. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 25/186.265-8 e o código de segurança vy5S Esta cópia foi autenticada digitalmente e assinada em 19/12/2025 por Fabianne Raissa da Fonseca Secretária-Geral.

DÉCIMA SEGUNDA ALTERAÇÃO DO CONTRATO SOCIAL
JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA
NIRE 53 2 0204989-6
CNPJ 24.425.034/0001-96

JOSÉ ANDRÉ MENDES COIMBRA, brasileiro, solteiro, estatístico, residente e domiciliado na SMPW QD 17 Conjunto 07 Lote 03, Núcleo Bandeirante, Brasília/DF CEP: 71.741-707, nascido em 26.01.1970, natural de Montes Claros/MG, filho de José André Coimbra e Terezinha Angelica Mendes Coimbra, portador da carteira de Identidade n°: 1.179.715 expedida pelo SSP/DF em 24.06.1987, e inscrito no CPF/MF sob o n°. 471.539.891-53;

ANDRÉ CASIMIRO COSTA, brasileiro, empresário, casado sob o regime de comunhão parcial de bens, residente e domiciliado no Condomínio Solar de Brasília, 0 Quadra 03, Conjunto 20, Casa 20, Setor Habitacional Jardim Botânico, Brasília/DF CEP: 71.680-349, nascido em 03/06/1981, natural de Brasília/DF, filho de Herlandes Antônio da Costa e Maria do Socorro Casimiro Silva Costa, portador da carteira nacional de habilitação n° 007246677714, expedida pelo DETRAN/DF em 30/01/2020, e inscrito no CPF/MF sob o n° 923.876.321-68;

GUILHERME LOPES MARANHÃO, brasileiro, solteiro, empresário, residente e domiciliado no Q SHDB QL 32, Conjunto 20, QL 32, Casa 132, Setor de Habitações Individuais Sul, Brasília/DF CEP 71.676-200, nascido em 18/02/1975, natural do Rio de Janeiro/RJ, filho de Carlos Fernando dos Reis Maranhão e Tereza Cristina Lopes Maranhão, portador da carteira nacional de habilitação n° 05801102104, expedida pelo DETRAN/DF em 13/09/2018, e inscrito no CPF/MF sob o n° 029.485.647-19; Únicos sócios componentes da sociedade limitada, JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA, estabelecida no SCES TRECHO 2, CENTRO DE LAZER BEIRA LAGO, CONJ 08; LOJA 03; Asa Sul, Brasília – DF, CEP:70.200-002, inscrita no CNPJ sob o nº. 24.425.034/0001-96, com seu contrato social arquivado na JCDF sob o nº. 53 2 0204989-6, por despacho em 21/03/2016, filial 1: JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA estabelecida na Alameda Rio Negro n° 503, Sala 2005, Alphaville Centro Industrial e Empresarial/Alphav, Barueri – SP, CEP. 06.454-000, inscrita no CNPJ sob o n°. 24.425.034/0002-77, filial 2: JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA estabelecida na RUA FRANCISCO DRUMOND, 41, EDIF MACEDO, ANDAR 1 SALA 103, CENTRO CAMAÇARI, BAHIA, CEP:42.800-063, inscrita no CNPJ sob o n°. 24.425.034/0003-58; filial 3: JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA estabelecida na AVENIDA JOSUE DI BERNARDI 185, SALA 31P, CAMPINAS, SÃO JOSE, SANTA CATARINA, CEP:88.101-200 inscrita no CNPJ sob o n°. 24.425.034/0004-39, resolvem alterar e consolidar de pleno e comum acordo as disposições contratuais vigentes, conforme a cláusulas e condições seguintes:

1. DA RERRATIFICAÇÃO DO NÚMERO DA ALTERAÇÃO CONTRATUAL

Neste ato, rerratifica-se o número da alteração contratual anteriormente registrada sob o nº 2856203, em 05/11/2025, a qual foi inadvertidamente identificada como DÉCIMA ALTERAÇÃO, quando o correto seria DÉCIMA PRIMEIRA ALTERAÇÃO, a fim de que a presente passe a ser regularmente registrada como DÉCIMA SEGUNDA ALTERAÇÃO, em estrita observância à ordem cronológica dos atos arquivados na Junta Comercial.

2. DA CESSÃO E TRANSFERÊNCIA DE QUOTAS

Neste ato, os sócios JOSÉ ANDRÉ MENDES COIMBRA, GUILHERME LOPES MARANHÃO e ANDRÉ CASIMIRO COSTA, acima qualificados, decidem usar o total de suas quotas, respectivamente, de 333.400 (trezentas e trinta e três mil e quatrocentas), 333.300 (trezentas e trinta e três mil e trezentas) e 333.300 (trezentas e trinta e três mil e trezentas) quotas, todas no valor nominal de R$ 1,00 (um real) cada, perfazendo o valor total de R$ 1.000.000,00 (um milhão de reais), pertencentes à sociedade JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA, para integralizar o capital da empresa em constituição PETAHOLD PARTICIPAÇÕES LTDA, sociedade empresária limitada, com sede

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2881045 em 18/12/2025 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2500277665 - 04/12/2025. Autenticação: BE96C8D871DBC323F2A7233CDDE089D5268B68. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 25/186.265-8 e o código de segurança vy5S Esta cópia foi autenticada digitalmente e assinada em 19/12/2025 por Fabianne Raissa da Fonseca Secretária-Geral.

no Trecho SCES Trecho 2, Centro De Lazer Beira Lago, Conjunto 08, Loja 03, Asa Sul, Brasília/DF, CEP: 70200-002 cujo protocolo de registro é 25/185.206-7.

Os sócios declaram que, após a constituição e obtenção de CNPJ da sociedade PETAHOLD PARTICIPAÇÕES LTDA cujo protocolo de registro é 25/185.206-7, utilizarão a totalidade de suas quotas da sociedade JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA para fins de integralização de capital na referida sociedade, mediante ato próprio de cessão a ser oportunamente arquivado na Junta Comercial competente.

3. DO VALOR

Os sócios declarantes afirmam, sob as penas da lei, que as quotas utilizadas para fins de integralização do capital social encontram-se livres e desembaraçadas de quaisquer ônus ou gravames, e que a presente operação será formalizada pelo valor histórico de integralização constante do contrato social da sociedade JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA, não havendo, neste ato, apuração de ganho de capital, ficando a efetiva cessão das quotas condicionada ao posterior registro do ato próprio na sociedade cedente, após a obtenção do CNPJ da empresa ora constituída.

4. DA CONSOLIDAÇÃO

Em face da alteração acordada, os sócios resolvem efetuar a Consolidação do Contrato Social, que passa a vigorar com a redação dada a seguir:

CONSOLIDAÇÃO DO CONTRATO SOCIAL
JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA

CLÁUSULA 1º: A sócia decide, para incorporar a alteração expressamente mencionada no item, anterior, consolidar o ato de alteração da JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA, passando este a ter a seguinte, nova e integral redação:

Parágrafo Primeiro. A sociedade tem como nome de fantasia PETA

CLÁUSULA 2º: A matriz tem sua sede no SCES TRECHO 2, CENTRO DE LAZER BEIRA LAGO, CONJ: 08; LOJA:03; Asa Sul, Brasília – DF, CEP:70.200-002, e pode constituir filiais, sucursais, escritórios e franquias em qualquer parte do território nacional ou no exterior, por deliberação dos sócios e, mediante alteração contratual para o devido fim.

Parágrafo Primeiro: A Sociedade possui uma filial situada na Alameda Rio Negro n° 503, Sala 2005, Alphaville Centro Industrial e Empresarial/Alphav, Barueri – SP, CEP. 06.454-000, inscrita no CNPJ sob o n°. 24.425.034/0002-77.

Parágrafo Segundo: A Sociedade possui uma filial situada na Rua Francisco Drumond, 41, Edif Macedo, Andar 1 Sala 103, Centro Camaçari, Bahia, CEP: 42.800-063, inscrita no CNPJ sob o n°. 24.425.034/0003-58.

Parágrafo Terceiro: A Sociedade possui uma filial situada na Avenida Josue Di Bernardi 185, Sala 31p, Campinas, São Jose, Santa Catarina, CEP: 88.101-200, inscrita no CNPJ sob o n°. 24.425.034/0004-39.

Parágrafo Quarto: As atividades empresariais da filial serão executadas, exclusivamente, de forma digital pela internet, salvo quando o contratante indicar local ou estabelecimento para tanto.

Parágrafo Quinto: Surgindo a necessidade de controle e manutenção de estoques, a Sociedade utilizará depósitos e ou armazéns de terceiros

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2881045 em 18/12/2025 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2500277665 - 04/12/2025. Autenticação: BE96C8D871DBC323F2A7233CDDE089D5268B68. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 25/186.265-8 e o código de segurança vy5S Esta cópia foi autenticada digitalmente e assinada em 19/12/2025 por Fabianne Raissa da Fonseca Secretária-Geral.

Cláusula 3º: A sociedade tem como objetivo social: COMERCIALIZACAO, CONSULTORIA, REPRESENTACAO IMPORTACAO E EXPORTACAO DE SOFTWARE, COMERCIO DE EQUIPAMENTOS E SUPRIMENTOS DE INFORMATICA, AGENCIAMENTO, CORRETAGEM OU INTERMEDIACAO DE TITULOS, VALORES MOBILIARIOS E CONTRATOS QUAISQUER OU AGENCIAMENTO, CORRETAGEM OU INTERMEDIACAO DE BENS MOVEIS OU IMOVEIS, NÃO ABRANGIDOS EM OUTROS ITENS OU SUBITENS, INCLUSIVE AQUELES REALIZADOS NO AMBITO DE BOLSAS DE MERCADORIA.

Cláusula 4º: O capital social é de **R$ 1.000.000,00 (um milhão de reais)**, representado por 1.000.000 (um milhão) quotas no valor nominal de R$ 1,00 (um real) cada, cuja integralização pelos sócios se deu em moeda corrente do país e da seguinte forma:

SÓCIOS	QUOTAS	R$	%
JOSÉ ANDRÉ MENDES COIMBRA	333.400 quotas	R$ 333.400,00	33,34%
ANDRÉ CASIMIRO COSTA	333.300 quotas	R$ 333.300,00	33,33%
GUILHERME LOPES MARANHÃO	333.300 quotas	R$ 333.300,00	33,33%
Total	1.000.000 quotas	R$ 1.000.000,00	100%

Parágrafo Primeiro: Os sócios **JOSÉ ANDRÉ MENDES COIMBRA**, **GUILHERME LOPES MARANHÃO** e **ANDRÉ CASIMIRO COSTA**, acima qualificados, decidem usar o total de suas quotas, respectivamente, de 333.400, 333.300 e 333.300 quotas, todas no valor nominal de R$ 1,00 (um real) cada, perfazendo o valor total de R$ 1.000.000,00 (um milhão de reais), pertencentes à sociedade JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA, para integralizar o capital da empresa em constituição PETAHOLD PARTICIPAÇÕES LTDA, sociedade empresária limitada, com sede no Trecho SCES Trecho 2, Centro De Lazer Beira Lago, Conjunto 08, Loja 03, Asa Sul, Brasília/DF, CEP: 70200-002 cujo protocolo de registro é 25/185.206-7.

Parágrafo Segundo: Os sócios declaram, sob as penas da lei, que as quotas utilizadas para fins de integralização do capital social encontram-se livres e desembaraçadas de quaisquer ônus ou gravames, e que a operação será formalizada pelo valor histórico de integralização constante do contrato social da sociedade JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA, sem apuração de ganho de capital, ficando a efetiva cessão das quotas condicionada ao posterior registro do ato próprio na sociedade cedente, após a obtenção do CNPJ da sociedade ora constituída.

Parágrafo Terceiro: Até que seja efetivado o registro da cessão das quotas na sociedade cedente, os sócios permanecem responsáveis pela integralização do capital social nos termos da legislação vigente.

Cláusula 5º: As quotas da sociedade são indivisíveis e não poderão ser cedidas ou transferidas sem o expresso consentimento dos demais sócios, cabendo em igualdade de condições e preço, o direito de preferência ao sócio que queira adquiri-las. O sócio que pretenda ceder ou transferir toda ou parte de suas quotas deverá manifestar sua intenção por escrito aos outros sócios, assistindo a estes o prazo de 30 (trinta) dias para que possam exercer o direito de preferência, ou ainda, optar pela dissolução da sociedade antes mesmo da cessão ou transferência das cotas.

Cláusula 6º: Das responsabilidades de cada sócio é restrita ao valor de suas quotas, mas todas respondem solidariamente pela integralização do capital social.

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2881045 em 18/12/2025 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2500277665 - 04/12/2025. Autenticação: BE96C8D871DBC323F2A7233CDDE089D5268B68. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 25/186.265-8 e o código de segurança vy5S Esta cópia foi autenticada digitalmente e assinada em 19/12/2025 por Fabianne Raissa da Fonseca Secretária-Geral.

Cláusula 7º: A administração da sociedade caberá a todos os sócios, cujos nos respectivos atos poderão ser executados de forma conjunta ou isoladamente, com os poderes e atribuições de representação ativa e passiva na sociedade, judicial e extrajudicial, sempre podendo praticar todos os atos decorrentes do objeto social no interesse da sociedade, autorizado o uso do nome empresarial, vedado, no entanto, em atividades estranhas ao interesse da sociedade, ou assumir obrigações seja em favor de qualquer dos quotistas ou de terceiros, bem como onerar ou alienar bens imóveis da sociedade, sem autorização do outro sócio.

Cláusula 8º: A sociedade iniciou suas atividades em **11/03/2016** e seu prazo de duração é por tempo indeterminado.

Cláusula 9º: Ao termino de cada exercício social, em 31 dezembro os, administradores, sócios ou não, prestarão contas justificadas de sua gestão, procedendo à elaboração do inventário, do balanço patrimonial e do balanço de resultado econômico, cabendo aos sócios, na proporção de suas cotas, os lucros ou perdas apuradas.

Parágrafo único: Nos quatro meses seguintes ao término do exercício social, os sócios deliberarão sobre as contas e designarão administrador, quando for o caso.

Cláusula 10º: Os sócios poderão de comum acordo, fixar uma retirada mensal, a título de "pró-labore", observadas as disposições regulamentares pertinentes.

Cláusula 11º: Falecendo ou sendo interditado qualquer sócio(a), a sociedade continuará suas atividades com os herdeiros, sucessores e o incapaz. Não sendo possível ou inexistindo interesse destes ou do sócio remanescente, o valor de seus haveres será apurado e liquidado com base na situação patrimonial da sociedade, à data da resolução, verificada em balanço especialmente levantado.

Parágrafo único: O mesmo procedimento será adotado em outros casos em que a sociedade se resolva em relação a seu sócio.

Cláusula 12º: Os administradores declaram, sob pena da lei, de que não estão impedidos de exercer a administração da sociedade, por lei especial, ou em virtude de condenação criminal, ou por se encontrar sob os efeitos dela, a pena que vede, ainda que temporariamente, o acesso a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato, ou contra a economia popular, contra o sistema financeiro nacional, contra normas de defesa da concorrência, contra as relações de consumo, fé pública, ou à propriedade.

Cláusula 13º: Fica eleito o foro de Brasília (DF) para a solução de quaisquer dúvidas ou questões oriundas deste contrato, com desistência de qualquer outro, por parte dos sócios, por mais privilegiado que venha a ser.

Cláusula 14º: Os sócios se comprometem a proteger todos os dados oriundos da sociedade aqui formada, na forma da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

Parágrafo Primeiro - Se qualquer dos sócios for responsável pelo vazamento de dados, deverá esta arcar com as eventuais consequências previstas na mesma lei citada.

Parágrafo Segundo - O sócio responsável pelos vazamentos de dados deverá indenizar a sócia prejudicada no montante de R$ 100.000,00 (cem mil reais), fora as demais penalidades impostas pela Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) e apuração de perdas e danos.

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2881045 em 18/12/2025 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2500277665 - 04/12/2025. Autenticação: BE96C8D871DBC323F2A7233CDDE089D5268B68. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 25/186.265-8 e o código de segurança vy5S Esta cópia foi autenticada digitalmente e assinada em 19/12/2025 por Fabianne Raissa da Fonseca Secretária-Geral.

Cláusula 15º: O presente instrumento será firmado através de assinatura eletrônica e/ou digital, certificada pelo Sistema Eletrônico de Informações do Ministério da Cidadania, garantida a eficácia das Cláusulas. As Partes envolvidas neste instrumento afirmam e declaram que esse poderá ser assinado eletronicamente através da plataforma "D4Sign", atualmente no endereço https://secure.d4sign.com.br, conformidade com o disposto § 1º do art. 10 da MPV 2.200-02/01, a assinatura deste termo pelo representante oficial da contratada, pressupõem declarada, de forma inequívoca, a sua a sua concordância, bem como o reconhecimento de validade e aceite do presente documento. Consigna-se no presente instrumento que a assinatura com Certificado Digital/eletrônica tem a mesma validade jurídica de um registro e autenticação feita em cartório, seja mediante utilização de certificados e-CPF, e-CNPJ.

Parágrafo Primeiro: A assinatura deste instrumento pelas partes, pressupõe declarada, de forma inequívoca, a sua concordância, bem como o reconhecimento da validade e do aceite ao presente documento.

Parágrafo Segundo: A sua autenticidade poderá ser atestada a qualquer tempo, seguindo os procedimentos da certificação digital, não podendo, desta forma, as partes se oporem a sua utilização.

Brasília/DF, 01 de dezembro de 2025.

JOSE ANDRE MENDES COIMBRA
Sócio Administrador

GUILHERME LOPES MARANHÃO
Sócio Administrador

ANDRE CASIMIRO COSTA
Sócio Administrador

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2881045 em 18/12/2025 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2500277665 - 04/12/2025. Autenticação: BE96C8D871DBC323F2A7233CDDE089D5268B68. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 25/186.265-8 e o código de segurança vy5S Esta cópia foi autenticada digitalmente e assinada em 19/12/2025 por Fabianne Raissa da Fonseca Secretária-Geral.

Documento Principal

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
25/186.265-8	DFE2500277665	04/12/2025

Identificação do(s) Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	18/12/2025 12:15:51
Assinado utilizando assinatura qualificada		
019.610.441-61	FELIPE ORSETTI PRADO	18/12/2025 12:29:50
Assinado utilizando assinaturas avançadas gov.br		
029.485.647-19	GUILHERME LOPES MARANHAO	18/12/2025 12:02:05
Assinado utilizando assinatura qualificada		
471.539.891-53	JOSE ANDRE MENDES COIMBRA	18/12/2025 12:14:49
Assinado utilizando assinatura qualificada		

Junta Comercial, Industrial e Serviços do Distrito Federal

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2881045 em 18/12/2025 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2500277665 - 04/12/2025. Autenticação: BE96C8D871DBC323F2A7233CDDE089D5268B68. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 25/186.265-8 e o código de segurança vy5S Esta cópia foi autenticada digitalmente e assinada em 19/12/2025 por Fabianne Raissa da Fonseca Secretária-Geral.

TERMO DE AUTENTICAÇÃO - REGISTRO DIGITAL

Certifico que o ato, assinado digitalmente, da empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, de CNPJ 24.425.034/0001-96 e protocolado sob o número 25/186.265-8 em 04/12/2025, encontra-se registrado na Junta Comercial sob o número 2881045, em 18/12/2025. O ato foi analisado pelo examinador MICHELINE OLIVEIRA GENNARI ANDRADE e deferido eletronicamente.

Certifica o registro, a Secretária-Geral, Fabianne Raissa da Fonseca. Para sua validação, deverá ser acessado o sitio eletrônico do Portal de Serviços / Validar Documentos (https://portalservicos.jucis.df.gov.br/Portal/pages/imagemProcesso/viaUnica.jsf) e informar o número de protocolo e chave de segurança.

Capa de Processo

Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	18/12/2025 12:15:51
Assinado utilizando assinatura qualificada	AC REDE IDEIA RFB	
029.485.647-19	GUILHERME LOPES MARANHAO	18/12/2025 12:02:05
Assinado utilizando assinatura qualificada	AC SEMPRE RFB v2	
471.539.891-53	JOSE ANDRE MENDES COIMBRA	18/12/2025 12:14:49
Assinado utilizando assinatura qualificada	AC SAFEWEB RFB v5	

Documento Principal

Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	18/12/2025 12:15:51
Assinado utilizando assinatura qualificada	AC REDE IDEIA RFB	
029.485.647-19	GUILHERME LOPES MARANHAO	18/12/2025 12:02:05
Assinado utilizando assinatura qualificada	AC SEMPRE RFB v2	
471.539.891-53	JOSE ANDRE MENDES COIMBRA	18/12/2025 12:14:49
Assinado utilizando assinatura qualificada	AC SAFEWEB RFB v5	
019.610.441-61	FELIPE ORSETTI PRADO	18/12/2025
Assinado utilizando assinaturas avançadas		

Data de início dos efeitos do registro (art. 36, Lei 8.934/1994): 01/12/2025

Documento assinado eletronicamente por FABIANNE RAISSA DA FONSECA, Servidor(a) Público(a), em 18/12/2025, às 12:29.

A autencidade desse documento pode ser conferida no portal de serviços da jucisdf informando o número do protocolo 25/186.265-8.

O ato foi assinado digitalmente por :

Identificação do(s) Assinante(s)	
CPF	Nome
017.057.021-55	FABIANNE RAISSA DA FONSECA

Brasília. quinta-feira, 18 de dezembro de 2025

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2881045 em 18/12/2025 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2500277665 - 04/12/2025. Autenticação: BE96C8D871DBC323F2A7233CDDE089D5268B68. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 25/186.265-8 e o código de segurança vy5S Esta cópia foi autenticada digitalmente e assinada em 19/12/2025 por Fabianne Raissa da Fonseca Secretária-Geral.

Ministério do Empreendedorismo, da Microempresa e da Empresa de Pequeno Porte
Secretaria Nacional de Microempresa e Empresa de Pequeno Porte
Diretoria Nacional de Registro Empresarial e Integração
Junta Comercial, Industrial e Serviços do Distrito Federal

Nº DO PROTOCOLO (Uso da Junta Comercial)

NIRE (da sede ou filial, quando a sede for em outra UF)	Código da Natureza Jurídica	Nº de Matrícula do Agente Auxiliar do Comércio
53202049896	2062	

1 - REQUERIMENTO

ILMO(A). SR.(A) PRESIDENTE DA Junta Comercial, Industrial e Serviços do Distrito Federal

Nome: JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA

(da Empresa ou do Agente Auxiliar do Comércio)

Nº FCN/REMP

DFN2543420151

requer a V.Sª o deferimento do seguinte ato:

Nº DE VIAS	CÓDIGO DO ATO	CÓDIGO DO EVENTO	QTDE	DESCRIÇÃO DO ATO / EVENTO
1	002			ALTERACAO
		051	1	CONSOLIDACAO DE CONTRATO/ESTATUTO
		2001	1	ENTRADA DE SOCIO/ADMINISTRADOR
		2003	1	ALTERACAO DE SOCIO/TITULAR / ADMINISTRADOR
		2005	1	SAIDA DE SOCIO/ADMINISTRADOR

BRASILIA
Local

27 Janeiro 2026
Data

Representante Legal da Empresa / Agente Auxiliar do Comércio:
Nome: _____
Assinatura: _____
Telefone de Contato: _____

2 - USO DA JUNTA COMERCIAL

☐ DECISÃO SINGULAR ☐ DECISÃO COLEGIADA

Nome(s) Empresarial(ais) igual(ais) ou semelhante(s):

☐ SIM ☐ SIM

_____ _____
_____ _____
_____ _____
_____ _____
_____ _____

☐ NÃO ___/___/_____ _____ ☐ NÃO ___/___/_____ _____
Data Responsável Data Responsável

Processo em Ordem
À decisão

___/___/_____
Data

_____
Responsável

DECISÃO SINGULAR

	2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência
☐ Processo em exigência. (Vide despacho em folha anexa)	☐	☐	☐	☐
☐ Processo deferido. Publique-se e arquive-se.				
☐ Processo indeferido. Publique-se.				

___/___/_____ _____
Data Responsável

DECISÃO COLEGIADA

	2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência
☐ Processo em exigência. (Vide despacho em folha anexa)	☐	☐	☐	☐
☐ Processo deferido. Publique-se e arquive-se.				
☐ Processo indeferido. Publique-se.				

___/___/_____ _____ _____ _____
Data Vogal Vogal Vogal

Presidente da _____ Turma

OBSERVAÇÕES

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2932004 em 28/01/2026 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFN2543420151 - 22/12/2025. Autenticação: 60494231193B4F96449778EE842F87AB68E81C9. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 25/200.731-0 e o código de segurança HNdg Esta cópia foi autenticada digitalmente e assinada em 28/01/2026 por Fabianne Raissa da Fonseca Secretária-Geral.

Capa de Processo

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
25/200.731-0	DFN2543420151	22/12/2025

Identificação do(s) Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	28/01/2026 08:44:50
Assinado utilizando assinatura qualificada		
029.485.647-19	GUILHERME LOPES MARANHAO	28/01/2026 08:43:47
Assinado utilizando assinatura qualificada		
471.539.891-53	JOSE ANDRE MENDES COIMBRA	28/01/2026 08:42:28
Assinado utilizando assinatura qualificada		

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2932004 em 28/01/2026 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFN2543420151 - 22/12/2025. Autenticação: 60494231193B4F96449778EE842F87AB68E81C9. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 25/200.731-0 e o código de segurança HNdg Esta cópia foi autenticada digitalmente e assinada em 28/01/2026 por Fabianne Raissa da Fonseca Secretária-Geral.

DÉCIMA TERCEIRA ALTERAÇÃO DO CONTRATO SOCIAL
JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA
NIRE 53 2 0204989-6
CNPJ 24.425.034/0001-96

JOSÉ ANDRÉ MENDES COIMBRA, brasileiro, solteiro, estatístico, residente e domiciliado na SMPW QD 17 Conjunto 07 Lote 03, Núcleo Bandeirante, Brasília/DF CEP: 71.741-707, nascido em 26.01.1970, natural de Montes Claros/MG, filho de José André Coimbra e Terezinha Angelica Mendes Coimbra, portador da carteira de Identidade n°: 1.179.715 expedida pelo SSP/DF em 24.06.1987, e inscrito no CPF/MF sob o n°. 471.539.891-53;

ANDRÉ CASIMIRO COSTA, brasileiro, empresário, casado sob o regime de comunhão parcial de bens, residente e domiciliado no Condomínio Solar de Brasília, Quadra 03, Conjunto 20, Casa 20, Setor Habitacional Jardim Botânico, Brasília/DF CEP: 71.680-349, nascido em 03/06/1981, natural de Brasília/DF, filho de Herlandes Antônio da Costa e Maria do Socorro Casimiro Silva Costa, portador da carteira nacional de habilitação n° 007246677714, expedida pelo DETRAN/DF em 30/01/2020, e inscrito no CPF/MF sob o n° 923.876.321-68;

GUILHERME LOPES MARANHÃO, brasileiro, solteiro, empresário, residente e domiciliado no Q SHDB QL 32, Conjunto 20, Casa 132, Setor de Habitações Individuais Sul, Brasília/DF CEP 71.676-200, nascido em 18/02/1975, natural do Rio de Janeiro/RJ, filho de Carlos Fernando dos Reis Maranhão e Tereza Cristina Lopes Maranhão, portador da carteira nacional de habilitação n° 05801102104, expedida pelo DETRAN/DF em 13/09/2018, e inscrito no CPF/MF sob o n° 029.485.647-19;

Únicos sócios componentes da sociedade limitada, JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA, estabelecida no SCES TRECHO 2, CENTRO DE LAZER BEIRA LAGO, CONJ 08; LOJA 03; Asa Sul, Brasília/DF, CEP:70.200-002, inscrita no CNPJ sob o nº. 24.425.034/0001-96, com seu contrato social arquivado na JCDF sob o nº. 53 2 0204989-6, por despacho em 21/03/2016, filial 1: JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA estabelecida na Alameda Rio Negro n° 503, Conj. 2005, sala 02, Alphaville Centro Industrial e Empresarial/Alphav, Barueri/SP, CEP: 06.454-000, inscrita no CNPJ sob o n°. 24.425.034/0002-77, filial 2: JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA estabelecida na RUA FRANCISCO DRUMOND, 41, EDIF MACEDO, ANDAR 1 SALA 103, CENTRO CAMAÇARI, BAHIA, CEP:42.800-063, inscrita no CNPJ sob o n°. 24.425.034/0003-58; filial 3: JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA estabelecida na AVENIDA JOSUE DI BERNARDI 185, SALA 31P, CAMPINAS, SÃO JOSE, SANTA CATARINA, CEP:88.101-200 inscrita no CNPJ sob o n°. 24.425.034/0004-39, resolvem alterar e consolidar de pleno e comum acordo as disposições contratuais vigentes, conforme a cláusulas e condições seguintes:

1. DA CESSÃO E TRANSFERÊNCIA DE QUOTAS

Os sócios JOSÉ ANDRÉ MENDES COIMBRA, GUILHERME LOPES MARANHÃO e ANDRÉ CASIMIRO COSTA, titulares, respectivamente, de 333.400 (trezentas e trinta e três mil e quatrocentas), 333.300 (trezentas e trinta e três mil e trezentas) e 333.300 (trezentas e trinta e três mil e trezentas) quotas da sociedade JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA, resolvem transferir, neste ato, a totalidade das quotas de sua titularidade à sociedade PETAHOLD PARTICIPAÇÕES LTDA, pessoa jurídica de direito privado inscrita no CNPJ sob o nº 64.138.953/0001-01 , com seu contrato social arquivado sob o nº de aprovação 53203623855, data da aprovação 18/12/2025 e protocolo DFB2500269287 em 03/12/2025, com sede no SCES Trecho 2, Centro de Lazer Beira Lago, Conjunto 08, Loja 03, Asa Sul, Brasília/DF, CEP: 70.200-002, a título de integralização de capital social da referida sociedade PETAHOLD PARTICIPAÇÕES LTDA, conforme consta de seu contrato de constituição arquivado concomitantemente perante a Junta Comercial competente.

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2932004 em 28/01/2026 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFN2543420151 - 22/12/2025. Autenticação: 60494231193B4F96449778EE842F87AB68E81C9. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 25/200.731-0 e o código de segurança HNdg Esta cópia foi autenticada digitalmente e assinada em 28/01/2026 por Fabianne Raissa da Fonseca Secretária-Geral.

2. DO VALOR

Os sócios cedentes declaram, sob as penas da lei, que as quotas objeto da cessão estão livres e desembaraçadas de quaisquer ônus ou gravames, e que a presente operação se dá pelo valor histórico de integralização constante do contrato social da JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA, sem apuração de ganho de capital.

3. DO NOVO QUADRO SOCIETÁRIO

Em razão da cessão e integralização de quotas acima mencionadas, o quadro societário da JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA passa a ser o seguinte:

SÓCIO	QUOTAS	R$	%
PETAHOLD PARTICIPAÇÕES LTDA	1.000.000 quotas	R$ 1.000.000,00	100%
Total	1.000.000 quotas	R$ 1.000.000,00	100%

4. DA ADMINISTRAÇÃO

Considerando que a PETAHOLD PARTICIPAÇÕES LTDA passa a ser a única titular das quotas representativas do capital social da JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA, procede-se também ao ajuste da cláusula de administração, para refletir a nova estrutura societária, mantendo-se os mesmos administradores, que passam a exercer suas funções na qualidade de administradores não sócios.

A administração da sociedade será exercida por JOSÉ ANDRÉ MENDES COIMBRA, brasileiro, solteiro, estatístico, residente e domiciliado na SMPW QD 17 Conjunto 07 Lote 03, Núcleo Bandeirante, Brasília/DF CEP: 71.741-707, nascido em 26.01.1970, natural de Montes Claros/MG, filho de José André Coimbra e Terezinha Angelica Mendes Coimbra, portador da carteira de Identidade n°: 1.179.715 expedida pelo SSP/DF em 24.06.1987, e inscrito no CPF/MF sob o n°. 471.539.891-53; ANDRÉ CASIMIRO COSTA, brasileiro, empresário, casado sob o regime de comunhão parcial de bens, residente e domiciliado no Condomínio Solar de Brasília, 0 Quadra 03, Conjunto 20, Casa 20, Setor Habitacional Jardim Botânico, Brasília/DF CEP: 71.680-349, nascido em 03/06/1981, natural de Brasília/DF, filho de Herlandes Antônio da Costa e Maria do Socorro Casimiro Silva Costa, portador da carteira nacional de habilitação n° 007246677714, expedida pelo DETRAN/DF em 30/01/2020, e inscrito no CPF/MF sob o n° 923.876.321-68; e GUILHERME LOPES MARANHÃO, brasileiro, solteiro, empresário, residente e domiciliado no Q SHDB QL 32, Conjunto 20, QL 32, Casa 132, Setor de Habitações Individuais Sul, Brasília/DF CEP 71.676-200, nascido em 18/02/1975, natural do Rio de Janeiro/RJ, filho de Carlos Fernando dos Reis Maranhão e Tereza Cristina Lopes Maranhão, portador da carteira nacional de habilitação n° 05801102104, expedida pelo DETRAN/DF em 13/09/2018, e inscrito no CPF/MF sob o n° 029.485.647-19, que atuarão na qualidade de administradores não sócios, com poderes para representar a sociedade ativa e passivamente, em juízo ou fora dele, podendo praticar todos os atos necessários ao cumprimento de seu objeto social, sendo vedado, no entanto, em atividades estranhas ao interesse da sociedade, ou assumir obrigações seja em favor de qualquer dos quotistas ou de terceiros, bem como onerar ou alienar bens imóveis da sociedade, sem autorização do outro sócio.

5. DECLARAÇÃO DE DESIMPEDIMENTO

Os administradores declaram, sob pena da lei, de que não estão impedidos de exercer a administração da sociedade, por lei especial, ou em virtude de condenação criminal, ou por se encontrar sob os efeitos dela, a pena que vede, ainda que temporariamente, o acesso a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato, ou contra a economia popular, contra o sistema financeiro nacional, contra normas de defesa da concorrência, contra as relações de consumo, fé pública, ou à propriedade.

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2932004 em 28/01/2026 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFN2543420151 - 22/12/2025. Autenticação: 60494231193B4F96449778EE842F87AB68E81C9. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 25/200.731-0 e o código de segurança HNdg Esta cópia foi autenticada digitalmente e assinada em 28/01/2026 por Fabianne Raissa da Fonseca Secretária-Geral.

6. DA CONSOLIDAÇÃO

Em face da alteração acordada, os sócios resolvem efetuar a Consolidação do Contrato Social, que passa a vigorar com a redação dada a seguir:

CONSOLIDAÇÃO DO CONTRATO SOCIAL
JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA

Cláusula 1º: A sócia decide, para incorporar a alteração expressamente mencionada no item, anterior, consolidar o ato de alteração da **JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA**, passando este a ter a seguinte, nova e integral redação:

Parágrafo Primeiro. A sociedade tem como nome de fantasia **PETA**

Cláusula 2º: A matriz tem sua sede no SCES TRECHO 2, CENTRO DE LAZER BEIRA LAGO, CONJ: 08; LOJA:03; Asa Sul, Brasília/DF, CEP:70.200-002, e pode constituir filiais, sucursais, escritórios e franquias em qualquer parte do território nacional ou no exterior, por deliberação dos sócios e, mediante alteração contratual para o devido fim.

Parágrafo Primeiro: A Sociedade possui uma filial situada na Alameda Rio Negro n° 503, Sala 2005, Alphaville Centro Industrial e Empresarial/Alphav, Barueri/SP, CEP: 06.454-000, inscrita no CNPJ sob o n°. 24.425.034/0002-77.

Parágrafo Segundo: A Sociedade possui uma filial situada na Rua Francisco Drumond, 41, Edif. Macedo, Andar 1 Sala 103, Centro Camaçari, Bahia, CEP: 42.800-063, inscrita no CNPJ sob o n°. 24.425.034/0003-58.

Parágrafo Terceiro: A Sociedade possui uma filial situada na Avenida Josue Di Bernardi 185, Sala 31p, Campinas, São Jose, Santa Catarina, CEP: 88.101-200, inscrita no CNPJ sob o n°. 24.425.034/0004-39.

Parágrafo Quarto: As atividades empresariais da filial serão executadas, exclusivamente, de forma digital pela internet, salvo quando o contratante indicar local ou estabelecimento para tanto.

Parágrafo Quinto: Surgindo a necessidade de controle e manutenção de estoques, a Sociedade utilizará depósitos e ou armazéns de terceiros

Cláusula 3º: A sociedade tem como objetivo social: **COMERCIALIZACAO, CONSULTORIA, REPRESENTACAO IMPORTACAO E EXPORTACAO DE SOFTWARE, COMERCIO DE EQUIPAMENTOS E SUPRIMENTOS DE INFORMATICA, AGENCIAMENTO, CORRETAGEM OU INTERMEDIACAO DE TITULOS, VALORES MOBILIARIOS E CONTRATOS QUAISQUER OU AGENCIAMENTO, CORRETAGEM OU INTERMEDIACAO DE BENS MOVEIS OU IMOVEIS, NÃO ABRANGIDOS EM OUTROS ITENS OU SUBITENS, INCLUSIVE AQUELES REALIZADOS NO AMBITO DE BOLSAS DE MERCADORIA**.

Cláusula 4º: O capital social é de R$ 1.000.000,00 (um milhão de reais), representado por 1.000.000 (um milhão) quotas no valor nominal de R$ 1,00 (um real) cada, cuja integralização pelos sócios se dará em moeda corrente do país e da seguinte forma:

SÓCIO	QUOTAS	R$	%
PETAHOLD PARTICIPAÇÕES LTDA	1.000.000 quotas	R$ 1.000.000,00	100%
Total	**1.000.000 quotas**	**R$ 1.000.000,00**	**100%**

Cláusula 5º: As quotas da sociedade são indivisíveis e não poderão ser cedidas ou transferidas sem o expresso consentimento dos demais sócios, cabendo em igualdade de condições e preço, o direito de preferência ao sócio que queira adquiri-las. O sócio que pretenda ceder ou transferir toda ou parte de suas quotas deverá manifestar sua intenção por escrito aos outros sócios, assistindo a estes o prazo

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2932004 em 28/01/2026 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFN2543420151 - 22/12/2025. Autenticação: 60494231193B4F96449778EE842F87AB68E81C9. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 25/200.731-0 e o código de segurança HNdg Esta cópia foi autenticada digitalmente e assinada em 28/01/2026 por Fabianne Raissa da Fonseca Secretária-Geral.

de 30 (trinta) dias para que possam exercer o direito de preferência, ou ainda, optar pela dissolução da sociedade antes mesmo da cessão ou transferência das cotas.

Cláusula 6º: Das responsabilidades de cada sócio é restrita ao valor de suas quotas, mas todas respondem solidariamente pela integralização do capital social.

Cláusula 7º: A administração da sociedade é exercida por **JOSÉ ANDRÉ MENDES COIMBRA**, brasileiro, solteiro, estatístico, residente e domiciliado na SMPW QD 17 Conjunto 07 Lote 03, Núcleo Bandeirante, Brasília/DF CEP: 71.741-707, nascido em 26.01.1970, natural de Montes Claros/MG, filho de José André Coimbra e Terezinha Angelica Mendes Coimbra, portador da carteira de Identidade n°: 1.179.715 expedida pelo SSP/DF em 24.06.1987, e inscrito no CPF/MF sob o n°. 471.539.891-53; **ANDRÉ CASIMIRO COSTA**, brasileiro, empresário, casado sob o regime de comunhão parcial de bens, residente e domiciliado no Condomínio Solar de Brasília, 0 Quadra 03, Conjunto 20, Casa 20, Setor Habitacional Jardim Botânico, Brasília/DF CEP: 71.680-349, nascido em 03/06/1981, natural de Brasília/DF, filho de Herlandes Antônio da Costa e Maria do Socorro Casimiro Silva Costa, portador da carteira nacional de habilitação n° 007246677714, expedida pelo DETRAN/DF em 30/01/2020, e inscrito no CPF/MF sob o n° 923.876.321-68; e **GUILHERME LOPES MARANHÃO**, brasileiro, solteiro, empresário, residente e domiciliado no Q SHDB QL 32, Conjunto 20, QL 32, Casa 132, Setor de Habitações Individuais Sul, Brasília/DF CEP 71.676-200, nascido em 18/02/1975, natural do Rio de Janeiro/RJ, filho de Carlos Fernando dos Reis Maranhão e Tereza Cristina Lopes Maranhão, portador da carteira nacional de habilitação n° 05801102104, expedida pelo DETRAN/DF em 13/09/2018, e inscrito no CPF/MF sob o n° 029.485.647-19, que atuarão na qualidade de administradores não sócios, com poderes para representar a sociedade ativa e passivamente, em juízo ou fora dele, podendo praticar todos os atos necessários ao cumprimento de seu objeto social, sendo vedado, no entanto, em atividades estranhas ao interesse da sociedade, ou assumir obrigações seja em favor de qualquer dos quotistas ou de terceiros, bem como onerar ou alienar bens imóveis da sociedade, sem autorização do outro sócio.

Cláusula 8º: A sociedade iniciou suas atividades em **11/03/2016** e seu prazo de duração é por tempo indeterminado.

Cláusula 9º: Ao termino de cada exercício social, em 31 dezembro os, administradores, sócios ou não, prestarão contas justificadas de sua gestão, procedendo à elaboração do inventário, do balanço patrimonial e do balanço de resultado econômico, cabendo aos sócios, na proporção de suas cotas, os lucros ou perdas apuradas.

Parágrafo Único: Nos quatro meses seguintes ao término do exercício social, os sócios deliberarão sobre as contas e designarão administrador, quando for o caso.

Cláusula 10º: Os sócios poderão de comum acordo, fixar uma retirada mensal, a título de "pró-labore", observadas as disposições regulamentares pertinentes.

Cláusula 11º: Falecendo ou sendo interditado qualquer sócio(a), a sociedade continuará suas atividades com os herdeiros, sucessores e o incapaz. Não sendo possível ou inexistindo interesse destes ou do sócio remanescente, o valor de seus haveres será apurado e liquidado com base na situação patrimonial da sociedade, à data da resolução, verificada em balanço especialmente levantado.

Parágrafo Único: O mesmo procedimento será adotado em outros casos em que a sociedade se resolva em relação a seu sócio.

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2932004 em 28/01/2026 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFN2543420151 - 22/12/2025. Autenticação: 60494231193B4F96449778EE842F87AB68E81C9. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 25/200.731-0 e o código de segurança HNdg Esta cópia foi autenticada digitalmente e assinada em 28/01/2026 por Fabianne Raissa da Fonseca Secretária-Geral.

Cláusula 12º: Os administradores declaram, sob pena da lei, de que não estão impedidos de exercer a administração da sociedade, por lei especial, ou em virtude de condenação criminal, ou por se encontrar sob os efeitos dela, a pena que vede, ainda que temporariamente, o acesso a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato, ou contra a economia popular, contra o sistema financeiro nacional, contra normas de defesa da concorrência, contra as relações de consumo, fé pública, ou à propriedade.

Cláusula 13º: Fica eleito o foro de Brasília/DF para a solução de quaisquer dúvidas ou questões oriundas deste contrato, com desistência de qualquer outro, por parte dos sócios, por mais privilegiado que venha a ser.

Cláusula 14º: Os sócios se comprometem a proteger todos os dados oriundos da sociedade aqui formada, na forma da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

Parágrafo Primeiro - Se qualquer dos sócios for responsável pelo vazamento de dados, deverá esta arcar com as eventuais consequências previstas na mesma lei citada.

Parágrafo Segundo - O sócio responsável pelos vazamentos de dados deverá indenizar a sócia prejudicada no montante de R$ 100.000,00 (cem mil reais), fora as demais penalidades impostas pela Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) e apuração de perdas e danos.

Cláusula 15º: O presente instrumento será firmado através de assinatura eletrônica e/ou digital, certificada pelo Sistema Eletrônico de Informações do Ministério da Cidadania, garantida a eficácia das Cláusulas. As Partes envolvidas neste instrumento afirmam e declaram que esse poderá ser assinado eletronicamente através da plataforma "D4Sign", atualmente no endereço https://secure.d4sign.com.br, conformidade com o disposto § 1º do art. 10 da MPV 2.200-02/01, a assinatura deste termo pelo representante oficial da contratada, pressupõem declarada, de forma inequívoca, a sua a sua concordância, bem como o reconhecimento de validade e aceite do presente documento. Consigna-se no presente instrumento que a assinatura com Certificado Digital/eletrônica tem a mesma validade jurídica de um registro e autenticação feita em cartório, seja mediante utilização de certificados e-CPF, e-CNPJ.

Parágrafo Primeiro: A assinatura deste instrumento pelas partes, pressupõe declarada, de forma inequívoca, a sua concordância, bem como o reconhecimento da validade e do aceite ao presente documento.

Parágrafo Segundo: A sua autenticidade poderá ser atestada a qualquer tempo, seguindo os procedimentos da certificação digital, não podendo, desta forma, as partes se oporem a sua utilização.

Brasília/DF, 22 de dezembro de 2025.

JOSE ANDRE MENDES COIMBRA
Administrador JAMC

GUILHERME LOPES MARANHÃO
Administrador JAMC

ANDRE CASIMIRO COSTA
Administrador JAMC

PETAHOLD PARTICIPAÇÕES LTDA
Por seus sócios-administradores:
JOSÉ ANDRÉ MENDES COIMBRA
GUILHERME LOPES MARANHÃO
ANDRÉ CASIMIRO COSTA

FELIPE ORSETTI PRADO
Advogado
OAB 62782/DF

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 2932004 em 28/01/2026 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFN2543420151 - 22/12/2025. Autenticação: 60494231193B4F96449778EE842F87AB68E81C9. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 25/200.731-0 e o código de segurança HNdg Esta cópia foi autenticada digitalmente e assinada em 28/01/2026 por Fabianne Raissa da Fonseca Secretária-Geral.

Documento Principal

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
25/200.731-0	DFN2543420151	22/12/2025

Identificação do(s) Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	28/01/2026 08:44:49
Assinado utilizando assinatura qualificada		
019.610.441-61	FELIPE ORSETTI PRADO	28/01/2026 10:47:10
Assinado utilizando assinaturas avançadas gov.br		
029.485.647-19	GUILHERME LOPES MARANHAO	28/01/2026 08:43:46
Assinado utilizando assinatura qualificada		
471.539.891-53	JOSE ANDRE MENDES COIMBRA	28/01/2026 08:42:26
Assinado utilizando assinatura qualificada		

Junta Comercial, Industrial e Serviços do Distrito Federal

TERMO DE AUTENTICAÇÃO - REGISTRO DIGITAL

Certifico que o ato, assinado digitalmente, da empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, de CNPJ 24.425.034/0001-96 e protocolado sob o número 25/200.731-0 em 22/12/2025, encontra-se registrado na Junta Comercial sob o número 2932004, em 28/01/2026. O ato foi analisado pelo examinador MARX HUMBERTO DE FREITAS e deferido eletronicamente.

Certifica o registro, a Secretária-Geral, Fabianne Raissa da Fonseca. Para sua validação, deverá ser acessado o sitio eletrônico do Portal de Serviços / Validar Documentos (https://portalservicos.jucis.df.gov.br/Portal/pages/imagemProcesso/viaUnica.jsf) e informar o número de protocolo e chave de segurança.

Capa de Processo

Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	28/01/2026 08:44:50
Assinado utilizando assinatura qualificada	AC REDE IDEIA RFB	
029.485.647-19	GUILHERME LOPES MARANHAO	28/01/2026 08:43:47
Assinado utilizando assinatura qualificada	AC SEMPRE RFB v2	
471.539.891-53	JOSE ANDRE MENDES COIMBRA	28/01/2026 08:42:28
Assinado utilizando assinatura qualificada	AC SAFEWEB RFB v5	

Documento Principal

Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	28/01/2026 08:44:49
Assinado utilizando assinatura qualificada	AC REDE IDEIA RFB	
029.485.647-19	GUILHERME LOPES MARANHAO	28/01/2026 08:43:46
Assinado utilizando assinatura qualificada	AC SEMPRE RFB v2	
471.539.891-53	JOSE ANDRE MENDES COIMBRA	28/01/2026 08:42:26
Assinado utilizando assinatura qualificada	AC SAFEWEB RFB v5	
019.610.441-61	FELIPE ORSETTI PRADO	28/01/2026
Assinado utilizando assinaturas avançadas		

Data de início dos efeitos do registro (art. 36, Lei 8.934/1994): 28/01/2026

Documento assinado eletronicamente por FABIANNE RAISSA DA FONSECA, Servidor(a) Público(a), em 28/01/2026, às 16:25.

A autencidade desse documento pode ser conferida no portal de serviços da jucisdf informando o número do protocolo 25/200.731-0.

Junta Comercial, Industrial e Serviços do Distrito Federal

O ato foi assinado digitalmente por :

Identificação do(s) Assinante(s)	
CPF	Nome
017.057.021-55	FABIANNE RAISSA DA FONSECA

VENTVRIS VENTIS

Brasília. quarta-feira, 28 de janeiro de 2026

Ministério do Empreendedorismo, da Microempresa e da Empresa de Pequeno Porte
Secretaria Nacional de Microempresa e Empresa de Pequeno Porte
Diretoria Nacional de Registro Empresarial e Integração
Junta Comercial, Industrial e Serviços do Distrito Federal

Nº DO PROTOCOLO (Uso da Junta Comercial)

NIRE (da sede ou filial, quando a sede for em outra UF)	Código da Natureza Jurídica	Nº de Matrícula do Agente Auxiliar do Comércio
53202049896	2062	

1 - REQUERIMENTO

ILMO(A). SR.(A) PRESIDENTE DA Junta Comercial, Industrial e Serviços do Distrito Federal

Nome: JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA

(da Empresa ou do Agente Auxiliar do Comércio)

Nº FCN/REMP

DFE2600155529

requer a V.Sª o deferimento do seguinte ato:

Nº DE VIAS	CÓDIGO DO ATO	CÓDIGO DO EVENTO	QTDE	DESCRIÇÃO DO ATO / EVENTO
1	002			ALTERACAO
		051	1	CONSOLIDACAO DE CONTRATO/ESTATUTO
		021	1	ALTERACAO DE DADOS (EXCETO NOME EMPRESARIAL)
		028	1	EXTINCAO DE FILIAL EM OUTRA UF

BRASILIA
Local

1 Julho 2026
Data

Representante Legal da Empresa / Agente Auxiliar do Comércio:
Nome: _____
Assinatura: _____
Telefone de Contato: _____

2 - USO DA JUNTA COMERCIAL

☐ DECISÃO SINGULAR ☐ DECISÃO COLEGIADA

Nome(s) Empresarial(ais) igual(ais) ou semelhante(s):

☐ SIM ☐ SIM

_____ _____
_____ _____
_____ _____
_____ _____
_____ _____

☐ NÃO ___/___/_____ _____ ☐ NÃO ___/___/_____ _____
Data Responsável Data Responsável

Processo em Ordem
À decisão

___/___/_____
Data

_____
Responsável

DECISÃO SINGULAR

	2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência
☐ Processo em exigência. (Vide despacho em folha anexa)	☐	☐	☐	☐
☐ Processo deferido. Publique-se e arquive-se.				
☐ Processo indeferido. Publique-se.				

___/___/_____ _____
Data Responsável

DECISÃO COLEGIADA

	2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência
☐ Processo em exigência. (Vide despacho em folha anexa)	☐	☐	☐	☐
☐ Processo deferido. Publique-se e arquive-se.				
☐ Processo indeferido. Publique-se.				

___/___/_____ _____ _____ _____
Data Vogal Vogal Vogal

Presidente da _____ Turma

OBSERVAÇÕES

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 3134725 em 07/07/2026 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2600155529 - 18/06/2026. Autenticação: 3B4719BD16CB546426378626217ADFE6496142B. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 26/189.232-1 e o código de segurança pGUH Esta cópia foi autenticada digitalmente e assinada em 07/07/2026 por Fabianne Raissa da Fonseca – Secretária-Geral.

Capa de Processo

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
26/189.232-1	DFE2600155529	17/06/2026

Identificação do(s) Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	06/07/2026 16:45:03
Assinado utilizando assinatura qualificada		
029.485.647-19	GUILHERME LOPES MARANHAO	06/07/2026 16:47:07
Assinado utilizando assinatura qualificada		
471.539.891-53	JOSE ANDRE MENDES COIMBRA	06/07/2026 16:38:22
Assinado utilizando assinatura qualificada		

Junta Comercial, Industrial e Serviços do Distrito Federal
Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 3134725 em 07/07/2026 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2600155529 - 18/06/2026. Autenticação: 3B4719BD16CB546426378626217ADFE6496142B. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 26/189.232-1 e o código de segurança pGUH Esta cópia foi autenticada digitalmente e assinada em 07/07/2026 por Fabianne Raissa da Fonseca – Secretária-Geral.

DÉCIMA QUARTA ALTERAÇÃO DO CONTRATO SOCIAL
JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA
NIRE 53202049896
CNPJ 24.425.034/0001-96

PETAHOLD PARTICIPAÇÕES LTDA, pessoa jurídica de direito privado inscrita no CNPJ sob o nº 64.138.953/0001-01, com seu contrato social arquivado sob ire: 53203623855 por despacho em 18/12/2025, com sede no TR SCES Trecho 2, Centro de Lazer Beira Lago, SN, Conjunto 08, Loja 03, Asa Sul, Brasília/DF, CEP: 70.200-002, neste ato representada por seu sócio administrador JOSÉ ANDRÉ MENDES COIMBRA, brasileiro, solteiro, estatístico, residente e domiciliado na Quadra SMPW 17, Conjunto 07, Lote 03, Park Way, Brasília/DF CEP: 71.741-707, nascido em 26/01/1970, natural de Montes Claros/MG, filho de José André Coimbra e Terezinha Angelica Mendes Coimbra, portador da carteira de Identidade n°: 1.179.715 expedida pelo SSP/DF em 24/06/1987, e inscrito no CPF/MF sob o n°. 471.539.891-53;

Único sócio componente da sociedade limitada, JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA, estabelecida no TR SCES Trecho 2, Centro de Lazer Beira Lago, Conjunto 08, Loja 03; Asa Sul, Brasília/DF, CEP: 70.200-002, inscrita no CNPJ sob o nº. 24.425.034/0001-96, com seu contrato social arquivado na Junta Comercial do Distrito Federal sob o Nire: 53202049896, por despacho em 21/03/2016, filial 1: JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA estabelecida na Alameda Rio Negro n° 503, Conj. 2005, sala 02, Alphaville Centro Industrial e Empresarial/Alphav, Barueri/SP, CEP: 06.454-000, inscrita no CNPJ sob o n°. 24.425.034/0002-77, filial 2: JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA estabelecida na Rua Francisco Drumond, 41, Edif. Macedo, Andar 1, Sala 103, Centro Camaçari/Bahia, CEP: 42.800-063, inscrita no CNPJ sob o n°. 24.425.034/0003-58; filial 3: JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA estabelecida na Avenida Josué Di Bernardi 185, Sala 31P, Campinas, São Jose/Santa Catarina, CEP: 88.101-200 inscrita no CNPJ sob o n°. 24.425.034/0004-39, resolvem alterar e consolidar de pleno e comum acordo as disposições contratuais vigentes, conforme a cláusulas e condições seguintes:

1. DO ENCERRAMENTO DE FILIAL

A sociedade delibera pelo encerramento da filial inscrita no CNPJ nº 24.425.034/0003-58, localizada na Rua Francisco Drumond, nº 41, Edifício Macedo, Andar 1, Sala 103, Centro, Camaçari/BA, CEP: 42.800-063, promovendo-se a respectiva baixa perante os órgãos competentes.

2.DA CONSOLIDAÇÃO

Em face da alteração acordada, os sócios resolvem efetuar a Consolidação do Contrato Social, que passa a vigorar com a redação dada a seguir:

CONSOLIDAÇÃO DO CONTRATO SOCIAL
JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA

PETAHOLD PARTICIPAÇÕES LTDA, pessoa jurídica de direito privado inscrita no CNPJ sob o nº 64.138.953/0001-01, com seu contrato social arquivado sob ire: 53203623855 por despacho em 18/12/2025, com sede no TR SCES Trecho 2, Centro de Lazer Beira Lago, SN, Conjunto 08, Loja 03, Asa Sul, Brasília/DF, CEP: 70.200-002, neste ato representada por seu sócio administrador JOSÉ ANDRÉ MENDES COIMBRA, brasileiro, solteiro, estatístico, residente e domiciliado na Quadra SMPW 17, Conjunto 07, Lote 03, Park Way, Brasília/DF CEP: 71.741-707, nascido em 26/01/1970, natural de Montes Claros/MG, filho de José André Coimbra e Terezinha Angelica Mendes Coimbra, portador da carteira de Identidade n°: 1.179.715 expedida pelo SSP/DF em 24/06/1987, e inscrito no CPF/MF sob o n°. 471.539.891-53;

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 3134725 em 07/07/2026 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2600155529 - 18/06/2026. Autenticação: 3B4719BD16CB546426378626217ADFE6496142B. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 26/189.232-1 e o código de segurança pGUH Esta cópia foi autenticada digitalmente e assinada em 07/07/2026 por Fabianne Raissa da Fonseca – Secretária-Geral.

Cláusula 1º: A sócia decide, para incorporar a alteração expressamente mencionada no item, anterior, consolidar o ato de alteração da **JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA**, passando este a ter a seguinte, nova e integral redação:

Parágrafo Primeiro. A sociedade tem como nome de fantasia **PETA**

Cláusula 2º: A matriz tem sua sede no TR SCES Trecho 2, Centro de Lazer Beira Lago, Conjunto 08, Loja 03; Asa Sul, Brasília/DF, CEP: 70.200-002, e pode constituir filiais, sucursais, escritórios e franquias em qualquer parte do território nacional ou no exterior, por deliberação dos sócios e, mediante alteração contratual para o devido fim.

Parágrafo Primeiro: A Sociedade possui uma filial situada na Alameda Rio Negro n° 503, Sala 2005, Alphaville Centro Industrial e Empresarial/Alphav, Barueri/SP, CEP: 06.454-000, inscrita no CNPJ sob o n°. 24.425.034/0002-77.

Parágrafo Segundo: A Sociedade possui uma filial situada na Avenida Josué Di Bernardi 185, Sala 31p, Campinas, São Jose, Santa Catarina, CEP: 88.101-200, inscrita no CNPJ sob o n°. 24.425.034/0004-39.

Parágrafo Terceiro: As atividades empresariais da filial serão executadas, exclusivamente, de forma digital pela internet, salvo quando o contratante indicar local ou estabelecimento para tanto.

Parágrafo Quarto: Surgindo a necessidade de controle e manutenção de estoques, a Sociedade utilizará depósitos e ou armazéns de terceiros

Cláusula 3º: A sociedade tem como objetivo social: **COMERCIALIZACAO, CONSULTORIA, REPRESENTACAO IMPORTACAO E EXPORTACAO DE SOFTWARE, COMERCIO DE EQUIPAMENTOS E SUPRIMENTOS DE INFORMATICA, AGENCIAMENTO, CORRETAGEM OU INTERMEDIACAO DE TITULOS, VALORES MOBILIARIOS E CONTRATOS QUAISQUER OU AGENCIAMENTO, CORRETAGEM OU INTERMEDIACAO DE BENS MOVEIS OU IMOVEIS, NÃO ABRANGIDOS EM OUTROS ITENS OU SUBITENS, INCLUSIVE AQUELES REALIZADOS NO AMBITO DE BOLSAS DE MERCADORIA**.

Cláusula 4º: O capital social é de R$ 1.000.000,00 (um milhão de reais), representado por 1.000.000 (um milhão) de quotas no valor nominal de R$ 1,00 (um real) cada, cuja integralização pela sócia se deu em moeda corrente do país e da seguinte forma:

SÓCIO	QUOTAS	R$	%
PETAHOLD PARTICIPAÇÕES LTDA	1.000.000 quotas	R$ 1.000.000,00	100%
Total	**1.000.000 quotas**	**R$ 1.000.000,00**	**100%**

Cláusula 5º: As quotas da sociedade são indivisíveis e não poderão ser cedidas ou transferidas sem o expresso consentimento dos demais sócios, cabendo em igualdade de condições e preço, o direito de preferência ao sócio que queira adquiri-las. O sócio que pretenda ceder ou transferir toda ou parte de suas quotas deverá manifestar sua intenção por escrito aos outros sócios, assistindo a estes o prazo de 30 (trinta) dias para que possam exercer o direito de preferência, ou ainda, optar pela dissolução da sociedade antes mesmo da cessão ou transferência das cotas.

Cláusula 6º: Das responsabilidades de cada sócio é restrita ao valor de suas quotas, mas todas respondem solidariamente pela integralização do capital social.

Cláusula 7º: A administração da sociedade é exercida por **JOSÉ ANDRÉ MENDES COIMBRA**, brasileiro, solteiro, estatístico, residente e domiciliado na Quadra SMPW 17, Conjunto 07, Lote 03, Park Way, Brasília/DF CEP: 71.741-707, nascido em 26/01/1970, natural de Montes Claros/MG, filho de José André Coimbra e Terezinha Angelica Mendes Coimbra, portador da carteira de Identidade n°: 1.179.715 expedida pelo SSP/DF em 24/06/1987, e inscrito no CPF/MF sob o n°. 471.539.891-53;

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 3134725 em 07/07/2026 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2600155529 - 18/06/2026. Autenticação: 3B4719BD16CB546426378626217ADFE6496142B. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 26/189.232-1 e o código de segurança pGUH Esta cópia foi autenticada digitalmente e assinada em 07/07/2026 por Fabianne Raissa da Fonseca – Secretária-Geral.

ANDRÉ CASIMIRO COSTA, brasileiro, empresário, casado sob o regime de comunhão parcial de bens, residente e domiciliado no Condomínio Solar de Brasília, Quadra 03, Conjunto 20, Casa 20, Setor Habitacional Jardim Botânico, Brasília/DF CEP: 71.680-349, nascido em 03/06/1981, natural de Brasília/DF, filho de Herlandes Antônio da Costa e Maria do Socorro Casimiro Silva Costa, portador da carteira nacional de habilitação n° 007246677714, expedida pelo DETRAN/DF em 30/01/2020, e inscrito no CPF/MF sob o n° 923.876.321-68; e GUILHERME LOPES MARANHÃO, brasileiro, solteiro, empresário, residente e domiciliado na Quadra SHDB QL 32, Conjunto 20, Casa 132, Setor de Habitações Individuais Sul, Brasília/DF CEP: 71.676-200, nascido em 18/02/1975, natural do Rio de Janeiro/RJ, filho de Carlos Fernando dos Reis Maranhão e Tereza Cristina Lopes Maranhão, portador da carteira nacional de habilitação n° 05801102104, expedida pelo DETRAN/DF em 13/09/2018, e inscrito no CPF/MF sob o n° 029.485.647-19. Que atuam na qualidade de administradores não sócios, com poderes para representar a sociedade ativa e passivamente, em juízo ou fora dele, podendo praticar todos os atos necessários ao cumprimento de seu objeto social, sendo vedado, no entanto, em atividades estranhas ao interesse da sociedade, ou assumir obrigações seja em favor de qualquer dos quotistas ou de terceiros, bem como onerar ou alienar bens imóveis da sociedade, sem autorização do outro sócio.

Cláusula 8º: A sociedade iniciou suas atividades em 11/03/2016 e seu prazo de duração é por tempo indeterminado.

Cláusula 9º: Ao termino de cada exercício social, em 31 dezembro os, administradores, sócios ou não, prestarão contas justificadas de sua gestão, procedendo à elaboração do inventário, do balanço patrimonial e do balanço de resultado econômico, cabendo aos sócios, na proporção de suas cotas, os lucros ou perdas apuradas.

Parágrafo Único: Nos quatro meses seguintes ao término do exercício social, os sócios deliberarão sobre as contas e designarão administrador, quando for o caso.

Cláusula 10º: Os sócios poderão de comum acordo, fixar uma retirada mensal, a título de “pró-labore”, observadas as disposições regulamentares pertinentes.

Cláusula 11º: Falecendo ou sendo interditado qualquer sócio(a), a sociedade continuará suas atividades com os herdeiros, sucessores e o incapaz. Não sendo possível ou inexistindo interesse destes ou do sócio remanescente, o valor de seus haveres será apurado e liquidado com base na situação patrimonial da sociedade, à data da resolução, verificada em balanço especialmente levantado.

Parágrafo Único: O mesmo procedimento será adotado em outros casos em que a sociedade se resolva em relação a seu sócio.

Cláusula 12º: Os administradores declaram, sob pena da lei, de que não estão impedidos de exercer a administração da sociedade, por lei especial, ou em virtude de condenação criminal, ou por se encontrar sob os efeitos dela, a pena que vede, ainda que temporariamente, o acesso a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato, ou contra a economia popular, contra o sistema financeiro nacional, contra normas de defesa da concorrência, contra as relações de consumo, fé pública, ou à propriedade.

Cláusula 13º: Fica eleito o foro de Brasília/DF para a solução de quaisquer dúvidas ou questões oriundas deste contrato, com desistência de qualquer outro, por parte dos sócios, por mais privilegiado que venha a ser.

Cláusula 14º: Os sócios se comprometem a proteger todos os dados oriundos da sociedade aqui formada, na forma da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 3134725 em 07/07/2026 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2600155529 - 18/06/2026. Autenticação: 3B4719BD16CB546426378626217ADFE6496142B. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 26/189.232-1 e o código de segurança pGUH Esta cópia foi autenticada digitalmente e assinada em 07/07/2026 por Fabianne Raissa da Fonseca – Secretária-Geral.

Parágrafo Primeiro - Se qualquer dos sócios for responsável pelo vazamento de dados, deverá esta arcar com as eventuais consequências previstas na mesma lei citada.

Parágrafo Segundo - O sócio responsável pelos vazamentos de dados deverá indenizar a sócia prejudicada no montante de R$ 100.000,00 (cem mil reais), fora as demais penalidades impostas pela Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) e apuração de perdas e danos.

Cláusula 15º: O presente instrumento será firmado através de assinatura eletrônica e/ou digital, certificada pelo Sistema Eletrônico de Informações do Ministério da Cidadania, garantida a eficácia das Cláusulas. As Partes envolvidas neste instrumento afirmam e declaram que esse poderá ser assinado eletronicamente através da plataforma "D4Sign", atualmente no endereço https://secure.d4sign.com.br, conformidade com o disposto § 1º do art. 10 da MPV 2.200-02/01, a assinatura deste termo pelo representante oficial da contratada, pressupõem declarada, de forma inequívoca, a sua a sua concordância, bem como o reconhecimento de validade e aceite do presente documento. Consigna-se no presente instrumento que a assinatura com Certificado Digital/eletrônica tem a mesma validade jurídica de um registro e autenticação feita em cartório, seja mediante utilização de certificados e-CPF, e-CNPJ.

Parágrafo Primeiro: A assinatura deste instrumento pelas partes, pressupõe declarada, de forma inequívoca, a sua concordância, bem como o reconhecimento da validade e do aceite ao presente documento.

Parágrafo Segundo: A sua autenticidade poderá ser atestada a qualquer tempo, seguindo os procedimentos da certificação digital, não podendo, desta forma, as partes se oporem a sua utilização.

Brasília/DF, 10 de junho de 2026.

JOSE ANDRE MENDES COIMBRA
Administrador JAMC

GUILHERME LOPES MARANHÃO
Administrador JAMC

ANDRE CASIMIRO COSTA
Administrador JAMC

PETAHOLD PARTICIPAÇÕES LTDA
Por seus sócios-administradores:
JOSÉ ANDRÉ MENDES COIMBRA
GUILHERME LOPES MARANHÃO
ANDRÉ CASIMIRO COSTA

FELIPE ORSETTI PRADO
Advogado
OAB 62782/DF

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 3134725 em 07/07/2026 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2600155529 - 18/06/2026. Autenticação: 3B4719BD16CB546426378626217ADFE6496142B. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 26/189.232-1 e o código de segurança pGUH Esta cópia foi autenticada digitalmente e assinada em 07/07/2026 por Fabianne Raissa da Fonseca – Secretária-Geral.

Documento Principal

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
26/189.232-1	DFE2600155529	17/06/2026

Identificação do(s) Assinante(s)		
CPF	Nome	Data Assinatura
923.876.321-68	ANDRE CASIMIRO COSTA	06/07/2026 16:45:02
Assinado utilizando assinatura qualificada		
019.610.441-61	FELIPE ORSETTI PRADO	06/07/2026 17:53:55
Assinado utilizando assinatura qualificada		
029.485.647-19	GUILHERME LOPES MARANHAO	06/07/2026 16:47:05
Assinado utilizando assinatura qualificada		
471.539.891-53	JOSE ANDRE MENDES COIMBRA	06/07/2026 16:38:21
Assinado utilizando assinatura qualificada		

Junta Comercial, Industrial e Serviços do Distrito Federal

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 3134725 em 07/07/2026 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2600155529 - 18/06/2026. Autenticação: 3B4719BD16CB546426378626217ADFE6496142B. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 26/189.232-1 e o código de segurança pGUH Esta cópia foi autenticada digitalmente e assinada em 07/07/2026 por Fabianne Raissa da Fonseca – Secretária-Geral.

TERMO DE AUTENTICAÇÃO - REGISTRO DIGITAL

Certifico que o ato, assinado digitalmente, da empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, de CNPJ 24.425.034/0001-96 e protocolado sob o número 26/189.232-1 em 18/06/2026, encontra-se registrado na Junta Comercial sob o número 3134725, em 07/07/2026. O ato foi deferido eletronicamente pelo examinador GABRIELA DOS ANJOS TORRACCA.

Certifica o registro, a Secretária-Geral, Fabianne Raissa da Fonseca. Para sua validação, deverá ser acessado o sitio eletrônico do Portal de Serviços / Validar Documentos (https://portalservicos.jucis.df.gov.br/Portal/pages/imagemProcesso/viaUnica.jsf) e informar o número de protocolo e chave de segurança.

Capa de Processo

Assinante(s)		
CPF	Nome	Data Assinatura
471.539.891-53	JOSE ANDRE MENDES COIMBRA	06/07/2026 16:38:22
Assinado utilizando assinatura qualificada	AC SAFEWEB RFB v5	
029.485.647-19	GUILHERME LOPES MARANHAO	06/07/2026 16:47:07
Assinado utilizando assinatura qualificada	AC SAFEWEB RFB v5	
923.876.321-68	ANDRE CASIMIRO COSTA	06/07/2026 16:45:03
Assinado utilizando assinatura qualificada	AC REDE IDEIA RFB	

Documento Principal

Assinante(s)		
CPF	Nome	Data Assinatura
471.539.891-53	JOSE ANDRE MENDES COIMBRA	06/07/2026 16:38:21
Assinado utilizando assinatura qualificada	AC SAFEWEB RFB v5	
029.485.647-19	GUILHERME LOPES MARANHAO	06/07/2026 16:47:05
Assinado utilizando assinatura qualificada	AC SAFEWEB RFB v5	
923.876.321-68	ANDRE CASIMIRO COSTA	06/07/2026 16:45:02
Assinado utilizando assinatura qualificada	AC REDE IDEIA RFB	
019.610.441-61	FELIPE ORSETTI PRADO	06/07/2026 17:53:55
Assinado utilizando assinatura qualificada	AC VALID RFB v5	

Data de início dos efeitos do registro (art. 36, Lei 8.934/1994): 10/06/2026

Documento assinado eletronicamente por GABRIELA DOS ANJOS TORRACCA, Servidor(a) Público(a), em 07/07/2026, às 10:21.

A autencidade desse documento pode ser conferida no portal de serviços da jucisdf informando o número do protocolo 26/189.232-1.

O ato foi assinado digitalmente por :

Identificação do(s) Assinante(s)	
CPF	Nome
017.057.021-55	FABIANNE RAISSA DA FONSECA

Brasília. terça-feira, 07 de julho de 2026

Junta Comercial, Industrial e Serviços do Distrito Federal
Certifico registro sob o nº 3134725 em 07/07/2026 da Empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, CNPJ 24425034000196 e protocolo DFE2600155529 - 18/06/2026. Autenticação: 3B4719BD16CB546426378626217ADFE6496142B. Fabianne Raissa da Fonseca - Secretária-Geral. Para validar este documento, acesse http://jucis.df.gov.br e informe nº do protocolo 26/189.232-1 e o código de segurança pGUH Esta cópia foi autenticada digitalmente e assinada em 07/07/2026 por Fabianne Raissa da Fonseca – Secretária-Geral.

REPUBLICA FEDERATIVA DO BRASIL

DISTRITO FEDERAL

SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA

POLÍCIA CIVIL

DPT - INSTITUTO DE IDENTIFICAÇÃO

NOME JOSÉ ANDRÉ MENDES COIMBRA



FILIAÇÃO
JOSÉ ANDRÉ COIMBRA

TEREZINHA ANGÉLICA MENDES COIMBRA

DATA NASCIMENTO
26/01/1970

TIPO SANGUÍNEO
A+

NATURALIDADE
MONTES CLAROS / MG

OBSERVAÇÃO
*****

CARTEIRA DE IDENTIDADE

LEI Nº 7.116, DE 29 DE AGOSTO DE 1983

CPF 471.539.891-53 DNI *****

RG 1.179.715 2ª VIA

DATA DE EXPEDIÇÃO 15/03/2022

REGISTRO CIVIL
C.C.RS AV.DIV. 9885, FL 154, LV BA-20, 1º OF. (31/05/2005) NÚCLEO BANDEIRANTE-DF

T. ELEITOR
007551962070

OSPB
85785

SÉRIE
00008

UF
DF

NIS/PIS/PASEP
*****

IDENTIDADE PROFISSIONAL
*****

CERT. MILITAR
RA 072022296676

CNH
*****

CNS
*****

POLEGAR DIREITO



4538744

VÁLIDA EM TODO O TERRITÓRIO NACIONAL







QR-CODE

Documento assinado com certificado digital em conformidade com a Medida Provisória nº 2200-2/2001. Sua validade poderá ser confirmada por meio do programa Assinador Serpro.

As orientações para instalar o Assinador Serpro e realizar a validação do documento digital estão disponíveis em: https://www.serpro.gov.br/assinador-digital.

SERPRO / SENATRAN







QR-CODE

Documento assinado com certificado digital em conformidade com a Medida Provisória nº 2200-2/2001. Sua validade poderá ser confirmada por meio do programa Assinador Serpro.

As orientações para instalar o Assinador Serpro e realizar a validação do documento digital estão disponíveis em: https://www.serpro.gov.br/assinador-digital.

SERPRO / SENATRAN

Sistema de Cadastramento Unificado de Fornecedores - SICAF

Declaração

Declaramos para os fins exigidos na legislação, conforme documentação registrada no SICAF, que a situação do fornecedor no momento é a seguinte:

Dados do Fornecedor

CNPJ:	**24.425.034/0001-96**	DUNS®:	**94*****86**
Razão Social:	**JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA**		
Nome Fantasia:	**PETA**		
Situação do Fornecedor:	**Credenciado**	Data de Vencimento do Cadastro:	**02/08/2027**
Natureza Jurídica:	**SOCIEDADE EMPRESÁRIA LIMITADA**		
MEI:	**Não**		
Porte da Empresa:	**Demais**		

Ocorrências e Impedimentos

Ocorrência:

Impedimento de Licitar: **Nada Consta**

Níveis cadastrados:

Documento(s) assinalado(s) com "*" está(ão) com prazo(s) vencido(s).

Automática: a certidão foi obtida através de integração direta com o sistema emissor. Manual: a certidão foi inserida manualmente pelo fornecedor.

I - Credenciamento

II - Habilitação Juridica

III - Regularidade Fiscal e Trabalhista Federal

Receita Federal e PGFN		Validade:	**23/03/2027**	**Automática**
FGTS		Validade:	**02/11/2026**	**Automática**
Trabalhista	**(http://www.tst.jus.br/certidao)**	Validade:	**03/04/2027**	**Automática**

IV - Regularidade Fiscal Estadual/Distrital e Municipal

Receita Estadual/Distrital	Validade:	**13/12/2026**	
Receita Municipal	(Isento)		

V - Qualificação Técnica

VI - Qualificação Econômico-Financeira

Validade: **30/06/2027**

Esta declaração é uma simples consulta e não tem efeito legal

CPF: 471.XXX.XXX-53 Nome: JOSE ANDRE MENDES COIMBRA

Ass: _____

CONTROLADORIA-GERAL DA UNIÃO

Certidão Negativa Correcional - Entes Privados (ePAD, CGU-PJ, CEIS, CNEP e CEPIM)

Consultado: **JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA**

CPF/CNPJ: **24.425.034/0001-96**

Certifica-se que, em consulta aos sistemas ePAD e CGU-PJ e aos cadastros CEIS, CNEP e CEPIM, mantidos pela Corregedoria-Geral da União, **NÃO CONSTAM** registros de penalidades vigentes ou de procedimentos acusatórios em andamento, relativos ao CPF/CNPJ consultado.

Destaca-se que, nos termos da legislação vigente, os referidos cadastros consolidam informações prestadas pelos entes públicos, de todos os Poderes e esferas de governo.

Os Sistemas ePAD e CGU-PJ consolidam os dados sobre o andamento dos processos administrativos de responsabilização de entes privados no Poder Executivo Federal.

O Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) apresenta a relação de empresas e pessoas físicas que sofreram sanções que implicaram a restrição de participar de licitações ou de celebrar contratos com a Administração Pública.

O Cadastro Nacional de Empresas Punidas (CNEP) apresenta a relação de empresas que sofreram quaisquer das punições previstas na Lei nº 12.846/2013 (Lei Anticorrupção).

O Cadastro de Entidades Privadas sem Fins Lucrativos Impedidas (CEPIM) apresenta a relação de entidades privadas sem fins lucrativos que estão impedidas de celebrar novos convênios, contratos de repasse ou termos de parceria com a Administração Pública Federal, em função de irregularidades não resolvidas em convênios, contratos de repasse ou termos de parceria firmados anteriormente.

Certidão emitida às 00:29:21 do dia 14/10/2026 , com validade até o dia 13/11/2026.

Link para consulta da verificação da certidão https://certidoes.cgu.gov.br/

Código de controle da certidão: jdJdgHZac65IzHDGDj3p

Qualquer rasura ou emenda invalidará este documento.

CONTROLADORIA-GERAL DA UNIÃO

Certidão Negativa Correcional - Entes Privados (ePAD, CGU-PJ, CEIS, CNEP e CEPIM)

Consultado: **ANDRE CASIMIRO COSTA**

CPF/CNPJ: **923.876.321-68**

Certifica-se que, em consulta aos sistemas ePAD e CGU-PJ e aos cadastros CEIS, CNEP e CEPIM, mantidos pela Corregedoria-Geral da União, **NÃO CONSTAM** registros de penalidades vigentes ou de procedimentos acusatórios em andamento, relativos ao CPF/CNPJ consultado.

Destaca-se que, nos termos da legislação vigente, os referidos cadastros consolidam informações prestadas pelos entes públicos, de todos os Poderes e esferas de governo.

Os Sistemas ePAD e CGU-PJ consolidam os dados sobre o andamento dos processos administrativos de responsabilização de entes privados no Poder Executivo Federal.

O Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) apresenta a relação de empresas e pessoas físicas que sofreram sanções que implicaram a restrição de participar de licitações ou de celebrar contratos com a Administração Pública.

O Cadastro Nacional de Empresas Punidas (CNEP) apresenta a relação de empresas que sofreram quaisquer das punições previstas na Lei nº 12.846/2013 (Lei Anticorrupção).

O Cadastro de Entidades Privadas sem Fins Lucrativos Impedidas (CEPIM) apresenta a relação de entidades privadas sem fins lucrativos que estão impedidas de celebrar novos convênios, contratos de repasse ou termos de parceria com a Administração Pública Federal, em função de irregularidades não resolvidas em convênios, contratos de repasse ou termos de parceria firmados anteriormente.

Certidão emitida às 10:46:37 do dia 19/10/2026 , com validade até o dia 18/11/2026.

Link para consulta da verificação da certidão https://certidoes.cgu.gov.br/

Código de controle da certidão: 3xqPlGlSFZXa9OmPBYTv

Qualquer rasura ou emenda invalidará este documento.

MINISTÉRIO DA FAZENDA
Secretaria da Receita Federal do Brasil
Procuradoria-Geral da Fazenda Nacional

CERTIDÃO POSITIVA COM EFEITOS DE NEGATIVA DE DÉBITOS RELATIVOS AOS TRIBUTOS FEDERAIS E À DÍVIDA ATIVA DA UNIÃO

Nome: JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA
CNPJ: 24.425.034/0001-96

Ressalvado o direito de a Fazenda Nacional cobrar e inscrever quaisquer dívidas de responsabilidade do sujeito passivo acima identificado que vierem a ser apuradas, é certificado que:

1. constam débitos administrados pela Secretaria da Receita Federal do Brasil (RFB) com exigibilidade suspensa nos termos do art. 151 da Lei nº 5.172, de 25 de outubro de 1966 - Código Tributário Nacional (CTN), ou objeto de decisão judicial que determina sua desconsideração para fins de certificação da regularidade fiscal, ou ainda não vencidos; e

2. não constam inscrições em Dívida Ativa da União (DAU) na Procuradoria-Geral da Fazenda Nacional (PGFN).

Conforme disposto nos arts. 205 e 206 do CTN, este documento tem os mesmos efeitos da certidão negativa.

Esta certidão é válida para o estabelecimento matriz e suas filiais e, no caso de ente federativo, para todos os órgãos e fundos públicos da administração direta a ele vinculados. Refere-se à situação do sujeito passivo no âmbito da RFB e da PGFN e abrange inclusive as contribuições sociais previstas nas alíneas 'a' a 'd' do parágrafo único do art. 11 da Lei nº 8.212, de 24 de julho de 1991.

A aceitação desta certidão está condicionada à verificação de sua autenticidade na Internet, nos endereços <http://rfb.gov.br> ou <http://www.pgfn.gov.br>.

Certidão emitida gratuitamente com base na Portaria Conjunta RFB/PGFN nº 1.751, de 2/10/2014.
Emitida às 08:25:07 do dia 17/09/2026 <hora e data de Brasília>.
Válida até 16/03/2027.
Código de controle da certidão: **321D.E8E6.D1E1.2D18**
Qualquer rasura ou emenda invalidará este documento.

CAIXA ECONÔMICA FEDERAL

Certificado de Regularidade do FGTS - CRF

Inscrição: 24.425.034/0001-96
Razão social: JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA
Endereço: TR SCES TRECHO 2 03 CONJ 08/ ASA SUL / BRASILIA / DF / 70200-002

A Caixa Econômica Federal, no uso da atribuição que lhe confere o Art. 7, da Lei 8.036, de 11 de maio de 1990, certifica que, nesta data, a empresa acima identificada encontra-se em situação regular perante o Fundo de Garantia do Tempo de Servico - FGTS.

O presente Certificado não servirá de prova contra cobrança de quaisquer débitos referentes a contribuições e/ou encargos devidos, decorrentes das obrigações com o FGTS.

Validade: 04/10/2026 a 02/11/2026

Certificação Número: 2026100403172990891168

Informação obtida em 16/10/2026 00:40:33

A utilização deste Certificado para os fins previstos em Lei esta condicionada a verificação de autenticidade no site da Caixa: **www.caixa.gov.br**

GOVERNO DO DISTRITO FEDERAL
SECRETARIA DE ESTADO DE ECONOMIA
SUBSECRETARIA DA RECEITA

CERTIDÃO NEGATIVA DE DÉBITOS

CERTIDÃO Nº: 305195014522026
NOME: JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA
ENDEREÇO: SCES TRECHO 2, CENTRO DE LAZER BEIRA LAGO CONJ 08 LOJA 03 03
CIDADE: ASA SUL
CNPJ: 24.425.034/0001-96
CF/DF 0776048100140
FINALIDADE: Verificação de Débitos

_____ CERTIFICAMOS QUE _____

Até esta data não constam débitos de tributos de competência do Distrito Federal, inclusive os relativos à Divida Ativa, para o contribuinte acima. Fica ressalvado o direito de a Fazenda Pública do Distrito Federal cobrar, a qualquer tempo, débitos que venham a ser apurados.

Certidão expedida conforme Decreto Distrital nº 23.873 de 04/07/2003, gratuitamente.
Válida até 09 de janeiro de 2027. *

Certidão emitida via internet em 11/10/2026 às 00:16:49 e deve ser validada no endereço https://www.receita.fazenda.df.gov.br.



Improbidade Administrativa e Inelegibilidade

Certidão Negativa

Certifico que nesta data (19/10/2026 às 11:48) NÃO CONSTA no Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade registros de condenação com trânsito em julgado ou sanção ativa quanto ao CPF nº 923.876.321-68.

A condenação por atos de improbidade administrativa não implica automático e necessário reconhecimento da inelegibilidade do condenado.
Para consultas sobre inelegibilidade acesse portal do TSE em http://divulgacandcontas.tse.jus.br/

Esta certidão é expedida gratuitamente. Sua autenticidade pode ser por meio do número de controle PORP.PFQ2.LYZY.T3LM no seguinte endereço: https://www.cnj.jus.br/improbidade_adm/autenticar_certidao.php

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO

CERTIDÃO NEGATIVA DE DÉBITOS TRABALHISTAS

Nome: JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA (MATRIZ E FILIAIS)
CNPJ: 24.425.034/0001-96
Certidão nº: 87368121/2026
Expedição: 16/10/2026, às 01:01:59
Validade: 14/04/2027 - 180 (cento e oitenta) dias, contados da data de sua expedição.

Certifica-se que **JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA (MATRIZ E FILIAIS)**, inscrito(a) no CNPJ sob o nº **24.425.034/0001-96**, **NÃO CONSTA** como inadimplente no Banco Nacional de Devedores Trabalhistas.
Certidão emitida com base nos arts. 642-A e 883-A da Consolidação das Leis do Trabalho, acrescentados pelas Leis ns.° 12.440/2011 e 13.467/2017, e no Ato 01/2022 da CGJT, de 21 de janeiro de 2022.
Os dados constantes desta Certidão são de responsabilidade dos Tribunais do Trabalho.
No caso de pessoa jurídica, a Certidão atesta a empresa em relação a todos os seus estabelecimentos, agências ou filiais.
A aceitação desta certidão condiciona-se à verificação de sua autenticidade no portal do Tribunal Superior do Trabalho na Internet (http://www.tst.jus.br).
Certidão emitida gratuitamente.

INFORMAÇÃO IMPORTANTE
Do Banco Nacional de Devedores Trabalhistas constam os dados necessários à identificação das pessoas naturais e jurídicas inadimplentes perante a Justiça do Trabalho quanto às obrigações estabelecidas em sentença condenatória transitada em julgado ou em acordos judiciais trabalhistas, inclusive no concernente aos recolhimentos previdenciários, a honorários, a custas, a emolumentos ou a recolhimentos determinados em lei; ou decorrentes de execução de acordos firmados perante o Ministério Público do Trabalho, Comissão de Conciliação Prévia ou demais títulos que, por disposição legal, contiver força executiva.

CERTIDÃO NEGATIVA DE LICITANTES INIDÔNEOS

O Tribunal de Contas da União certifica, em 19/10/2026 às 10:49, que **ANDRE CASIMIRO COSTA**, CPF: **923.876.321-68**, **NÃO CONSTA** no cadastro de responsáveis declarados inidôneos para participar de licitação na Administração Pública.

O que significa não constar nesse cadastro?

Significa que não há decisões do TCU que impeçam a pessoa de participar de licitações no âmbito da Administração Pública.

O cadastro não inclui:

- Responsáveis ainda não notificados sobre a decisão;
- Decisões ainda não transitadas em julgado; e
- Decisões anuladas ou suspensas pelo TCU ou pela Justiça.

Base legal:

Artigo 46 da Lei 8.443/1992 (Lei Orgânica do TCU)

- O trânsito em julgado marca uma decisão como não mais sujeita a recursos com efeitos suspensivos.

Certidão valida até **18/11/2026**
Quer confirmar os dados? Acesse https://certidoes.apps.tcu.gov.br
com o código GDVB20261019104911
https://portal.tcu.gov.br/carta-de-servicos/certidoes

CERTIDÃO NEGATIVA DE LICITANTES INIDÔNEOS

O Tribunal de Contas da União certifica, em 15/10/2026 às 01:12, que **JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA**, CNPJ: **24.425.034/0001-96**, **NÃO CONSTA** no cadastro de responsáveis declarados inidôneos para participar de licitação na Administração Pública.

O que significa não constar nesse cadastro?

Significa que não há decisões do TCU que impeçam a pessoa de participar de licitações no âmbito da Administração Pública.

O cadastro não inclui:

- Responsáveis ainda não notificados sobre a decisão;
- Decisões ainda não transitadas em julgado; e
- Decisões anuladas ou suspensas pelo TCU ou pela Justiça.

Base legal:

Artigo 46 da Lei 8.443/1992 (Lei Orgânica do TCU)

- O trânsito em julgado marca uma decisão como não mais sujeita a recursos com efeitos suspensivos.

Certidão valida até **14/11/2026**
Quer confirmar os dados? Acesse https://certidoes.apps.tcu.gov.br com o código NYYE20261015011225
https://portal.tcu.gov.br/carta-de-servicos/certidoes



Certidão Negativa

Certifico que nesta data (16/10/2026 às 00:29) NÃO CONSTA no Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade registros de condenação com trânsito em julgado ou sanção ativa quanto ao CNPJ nº 24.425.034/0001-96.

A condenação por atos de improbidade administrativa não implica automático e necessário reconhecimento da inelegibilidade do condenado.
Para consultas sobre inelegibilidade acesse portal do TSE em http://divulgacandcontas.tse.jus.br/

Esta certidão é expedida gratuitamente. Sua autenticidade pode ser por meio do número de controle W8WV.NHW6.CXCK.766Y no seguinte endereço: https://www.cnj.jus.br/improbidade_adm/autenticar_certidao.php

COORDENAÇÃO DE APERFEIÇOAMENTO DE PESSOAL DE NÍVEL SUPERIOR
Setor Bancário Norte (SBN), Quadra 2, Bloco L, Lote 06, Edifício Capes, SOBRELOJA - Bairro Asa Norte, Brasília/DF, CEP 70040-020
Telefone: (61) 2022-6103 - www.capes.gov.br

ATESTADO DE CAPACIDADE TÉCNICA

Processo nº 23038.008491/2023-18

Interessado: Coordenação-Geral de Segurança e Infraestrutura de Informática, JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA

A **Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES**, inscrita no CNPJ sob o nº 00.889.834/0001-08**,** com sede no Setor Bancário Norte Quadra 02, Bloco L, Lote 06, Brasília/DF, declara a pedido da interessada, empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, inscrita no CNPJ nº 24.425.034/0001-96, situada em Al. Rio Negro, nº 500, 5º Andar, Sala 501 a 508, Torre B, Alphaville Centro Industrial e Empresarial | Barueri – SP, que mantém contrato de prestação de serviços de Tecnologia da Informação, com as características abaixo relacionadas:

1. **DADOS DO CONTRATO**

- Contrato: 45/2022 e 46/2022.
- Vigência: 21/12/2022 a 21/12/2023
- Processo administrativo: 23038.008732/2021-59
- Local da Prestação dos Serviços: nas instalações da Contratante
- Objeto: Aquisição de soluções de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados, endpoint e proteção e controle de acesso de usuários privilegiados (PAM), incluindo garantia, serviço de instalação e treinamento, nos termos e condições constantes no contrato, seus anexos e edital.

2. **ATIVIDADES DESEMPENHADAS**

Fornecimento, execução de maneira satisfatória do fornecimento, instalação, parametrização e suporte no ambiente da CAPES, das seguintes ferramentas:

- 1.200 Licenças de uso de software e garantia por 12 meses para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint.
- 1.200 Licenças de uso de software e garantia por 12 meses para funcionalidade de auditoria para disco em nuvem para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados.
- 01 Serviço de instalação para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint.
- 01 Treinamento para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint.

Atestamos ainda, cumprimento das obrigações assumidas, a qualidade dos serviços prestados em nível satisfatório, nada havendo em nossos arquivos que desabone a conduta da empresa na execução do objeto do Contrato nº 45/2022 e 46/2022 até a presente data.

Francisco Araújo de Almeida Neto
Coordenador-Geral de Segurança e Infraestrutura de Informática
E-mail: francisco.neto@capes.gov.br
Tel. (61)2022-6103

Documento assinado eletronicamente por **Francisco Araujo de Almeida Neto**, **Coordenador(a)-Geral de Segurança e Infraestrutura de Informática**, em 06/09/2023, às 11:59, conforme horário oficial de Brasília, com fundamento no art. 54, inciso II, da Portaria nº 06/2021 da Capes.

A autenticidade deste documento pode ser conferida no site http://sei.capes.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2043174** e o código CRC **2B2E442B**.

CONSELHO FEDERAL DE MEDICINA
ATESTADO DE CAPACIDADE TÉCNICA

ATESTADO DE CAPACIDADE TÉCNICA

O CONSELHO FEDERAL DE MEDICINA**,** entidade de fiscalização da profissão médica, instituída pela Lei nº 3.268, de 30 de setembro de 1957, regulamentada pelo Decreto nº 44.045, de 19 de julho de 1958, com sede no SGAS 616, Conjunto D, Lote 115, L2 Sul – Brasília–DF, CNPJ sob o nº 33.583.550/0001-30, por intermédio de seu representante legal, consoante delegação de competência conferida pela lei nº 3.268/57, neste ato representado pelo seu Presidente **Dr. JOSÉ HIRAN DA SILVA GALLO,** nomeado pela Ata de Reunião de Plenária do Conselho Federal de Medicina, publicada no DOU nº 66, seção 3, no dia 06 de abril de 2022, atesta para os devidos fins que a empresa **JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA,** devidamente inscrita no CNPJ sob o nº 24.425.34/0001-96, estabelecida no SCES Trecho 2, Centro de Lazer Beira do Lago, conjunto 08, loja 3, Asa Sul – Brasília-DF, CEP: 70200-002, presta ao CONSELHO FEDERAL DE MEDICINA serviços de renovação da Solução de Auditoria e de Gerenciamento de Controlador de Domínio e de Servidor de Arquivo, com garantia (manutenção e suporte técnico) das licenças por 36 meses, conforme as características, condições, obrigações e requisitos técnicos contidos no Termo de Referência e demais anexos do Edital do Pregão nº 026/2022.

Declaramos que a citada empresa atende satisfatoriamente todas as obrigações do contrato, não havendo fatos que desabonem sua conduta ou a qualidade dos serviços prestados.

De acordo com o Processo Administrativo
PREGÃO ELETRÔNICO Nº 026/2022

Dra DILZA AMBRÓS RIBEIRO
SECRETÁRIA-GERAL DO CFM

Dr. JOSÉ HIRAN DA SILVA GALLO
PRESIDENTE DO CFM

Brasília, 21 de março de 2024

Documento assinado eletronicamente por **Dilza Teresinha Ambrós Ribeiro**, **Secretária-geral**, em 21/03/2024, às 17:55, com fundamento no art. 5º da RESOLUÇÃO CFM nº2.308/2022, de 28 de março de 2022.

Documento assinado eletronicamente por **José Hiran da Silva Gallo**, **Presidente**, em 22/03/2024, às 08:23, com fundamento no art. 5º da RESOLUÇÃO CFM nº2.308/2022, de 28 de março de 2022.

A autenticidade do documento pode ser conferida no site https://sei.cfm.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0893687** e o código CRC **73BE401D**.

SGAS, Qd. 616 Conjunto D, lote 115, L2 Sul - Bairro Asa Sul | CEP 70.200-760 | Brasília/DF - https://portal.cfm.org.br

Referência: Processo SEI nº 29.0.000001974-3 | data de inclusão: 21/03/2024

MINISTÉRIO DAS CIDADES

Secretaria Executiva
Subsecretaria de Planejamento, Orçamento e Administração
Coordenação-Geral de Tecnologia da Informação

ATESTADO DE CAPACIDADE TÉCNICA Nº 1/2024

Atestamos que a empresa **JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA**, inscrita no CNPJ/MF sob n° 24.425.034/0001-96, sediada no CJ SRTVN Quadra 701, Conjunto C, Ala B, Parte V, Nº 124, Asa Norte, Brasília-DF, CEP: 70.719-903, por meio do Contrato Administrativo nº 170/2022, forneceu Solução de Segurança, Auditoria e Governança, contemplando instalação e garantia da proteção dos dados do Ministério das Cidades, assim como os Serviços de Monitoramento, Detecção e Resposta aos Incidentes em regime 24x7 (vinte e quatro horas e sete dias por semana), no período de **20/12/2022 a 20/12/2023**, conforme especificações no quadro abaixo:

OBJETO DA CONTRATAÇÃO

ITEM	DESCRIÇÃO	MÉTRICA	QUANTIDADE
1	Solução de segurança, auditoria e prevenção de ameaças	Contas do AD/Usuários	3190
2	Serviço de instalação para solução de segurança, auditoria e prevenção de ameaças	Serviço	1

Informo também que o supracitado contrato foi renovado por mais 12 (doze) meses, de 21/12/2023 a 20/12/2024, por intermédio do Termo Aditivo nº 93/2023.

Declaramos, ainda, que os compromissos assumidos pela empresa foram cumpridos satisfatoriamente, nada constando em nossos arquivos que o desabone comercial ou tecnicamente.

Brasília, na data da assinatura.

Atenciosamente,

[assinado eletronicamente]

ARNALDO LESSA SANCHES

Gestor do Contrato

Documento assinado eletronicamente por **Arnaldo Lessa Sanches**, **Coordenador-Geral**, em 19/03/2024, às 11:53, com fundamento no art. 4º, § 3º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida no site https://sei.mi.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **4943338** e o código CRC **E10F8648**.

ATESTADO

O **TRIBUNAL REGIONAL DO TRABALHO DA 1ª REGIÃO** inscrito no CNPJ sob número 02.578.421/0001-20, situado na Av. Presidente Antônio Carlos, 251, Centro, Rio de Janeiro, RJ, **atesta** para os devidos fins que a empresa JAMC – Consultoria e Representação de Software LTDA, sob CNPJ n° 24.425.034/0001-96, sediada no Centro de Lazer Beira Lago, SCES Trecho 2, Lote 8, Loja 3, forneceu, executou e executa de maneira satisfatória o fornecimento, instalação, parametrização e suporte técnico para as seguintes soluções, no ambiente do **TRIBUNAL REGIONAL DO TRABALHO DA 1ª REGIÃO**:

- Solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint para 4170 usuários;

- Ferramenta de proteção e controle de acesso de usuários privilegiados (PAM) nos seguintes quantitativos:

    - 1224 credenciais privilegiadas;
    - 866 servidores;
    - 294 dispositivos de rede;
    - 18 aplicações;
    - 18 bases de dados;
    - 115 IoT.

EDUARDO PEREIRA BORGES:95338

Assinado de forma digital por EDUARDO PEREIRA BORGES:95338
Dados: 2023.06.02 15:17:41 -03'00'

Eduardo Pereira Borges
Titular da unidade gestora do contrato no TRT/RJ

Coordenadoria de Governança e Segurança de TIC - CGOV
Secretaria de Tecnologia da Informação e Comunicação
Tribunal Regional do Trabalho da 1ª Região
Tel (021) 2380-7405

TRIBUNAL REGIONAL DO TRABALHO DA 10ª REGIÃO
SAS Quadra 1 Bloco D - Bairro Asa Sul - CEP 70097-900 - Brasília - DF - www.trt10.jus.br
Praça dos Tribunais Superiores

ATESTADO DE CAPACIDADE TÉCNICA

Declaramos, para fins de participação em licitação no âmbito da Administração Pública, que a empresa abaixo identificada prestou para este Tribunal os seguinte serviços e fornecimentos:

<table>
<tr><td>Empresa:
JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA</td><td colspan="2">CNPJ:
24.425.034/0001-96</td></tr>
<tr><td>Endereço:
São Paulo:Al. Rio Negro, nº 500, 5º Andar, Sala 501 a 508, Torre B, Alphaville Centro Industrial e Empresarial|Barueri –SP | CEP: 06.454-000
Brasília: SCES Trecho 2, Centro de Lazer Beira Lago, Conjunto08, Loja 03, Asa Sul| Brasília-DF | CEP 70.200-002
Site:www.petacorp.com.br|</td><td colspan="2">Telefone / Fax / E-mail:
E-mail:comercial@petacorp.com.br
Telefones:(61) 2017-0771 / (11) 3136-0190-</td></tr>
<tr><td>Objeto:
• 1 Cluster para prover recursos para solução de acesso a usuários privilegiados
• 10 Licenças para contas para acesso privilegiados simultâneos (admin segurança/rede/Root/DomainAdmin/DBadmin/SysDBA, VMadmin, helpdesk)
• 400 Licenças para servidores físicos e virtuais (Linux, Windows e Storages)
• 200 Licenças para estações de trabalho Windows
• 40 Licençaspara instancias de Banco de Dados (Oracle, Postgres, MSSQL e MySQL)
• 1 Serviço de instalação para solução de controle de acesso de usuários privilegiados.
• 1 Treinamento para solução de controle de acesso de usuários privilegiados</td><td>Processo Administrativo:

0009115-34.2022.5.10.8000</td><td>Contrato/Vigência:

nº 204/2022
Vigência: dez/2023</td></tr>
</table>

A Responsabilidade Técnica do serviço ficou a cargo do senhor Emerson de Sousa Albino - gerente técnico - CPF nº 01480140112

Declaramos que a contratada forneceu, executou e executa o fornecimento, instalação, parametrização e suporte no ambiente deste Tribunal da ferramenta contratada: software Senha Segura.

Declaramos, ainda, que os compromissos assumidos foram cumpridos satisfatoriamente, nada constando em nossos registros, que desabone comercialmente ou tecnicamente, até o momento.

FRANCISCO ROGÉRIO CAVALCANTE DA PONTE FILHO
Chefe da Divisão de Segurança Cibernética

Documento assinado eletronicamente por **FRANCISCO ROGERIO C. DA PONTE FILHO**, **Chefe de Divisão**, em 26/07/2023, às 15:02, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://www.trt10.jus.br/validadorsei.htm informando o código verificador **2275493** e o código CRC **D6D7A573**.

ATESTADO DE CAPACIDADE TÉCNICA

Atestamos para os devidos fins que a empresa JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, inscrita no CNPJ nº 24.425.034/0001-96, estabelecida na Al. Rio Negro, no 500, 5o Andar, Sala 501 a 508, Torre B, Alphaville Centro Industrial e Empresarial, Barueri/SP, Telefone/Fax: (11) 3136-0190 CEP: 06.454-000, presta de maneira satisfatória os serviços abaixo discriminados ao Tribunal Regional do Trabalho da 11ª Região, sito Rua Visconde de Porto Alegre, 1265, 4º andar - Manaus/AM, inscrito no CNPJ sob nº 01.671.187/0001-18:

Serviços de Monitoramento, Detecção e Resposta aos Incidentes em regime 24x7 (vinte e quatro horas e sete dias por semana), assim como o fornecimento, instalação, parametrização e suporte no ambiente deste Tribunal, das seguintes ferramentas:

• 1.600 Licenças de uso de software e garantia por 12 meses para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint.

• 1.600 Licenças de uso de software e garantia por 12 meses para funcionalidade de auditoria para disco em nuvem para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados.

• 1 Serviço de instalação para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint.

• 1 Treinamento para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint.

• 1 Cluster para prover recursos para solução de acesso a usuários privilegiados

• 12 Licenças para contas para acesso privilegiados simultâneos (admin segurança/rede/Root/DomainAdm in/DBadmin/SysDBA, VMadmin, helpdesk)

• 375 Licenças para servidores físicos e virtuais (Linux, Windows e Storages)

• 2.100 Licenças para estações de trabalho Windows

• 300 Licenças para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP)

• 35 Licenças para aplicações conteinerizadas com secrets

Av. Tefé, 930 – Praça 14 de Janeiro
Sede Administrativa – 3º Andar
Manaus/AM – 69020-090
Telefone: (92) 3621-7480 / 7474
e-mail: gestaotic@trt11.jus.br

- 40 Licenças para aplicações não-conteinerizadas com senha embutida (hard coded)
- 10 Licenças para instâncias de Banco de Dados (Oracle, Postgres, MSSQL e MySQL)
- 1 Serviço de instalação para solução de controle de acesso de usuários privilegiados
- 1 Treinamento para solução de controle de acesso de usuários privilegiados
- 12 Meses de serviço e suporte técnico especializado

Manaus/AM, 28 de junho de 2023.

RONANIO CINTRA DA SILVA:308110480
Assinado de forma digital por RONANIO CINTRA DA SILVA:308110480
Dados: 2023.06.28 13:39:59 -04'00'

Assinado eletronicamente

Ronanio Cintra da Silva
Diretor da Coordenadoria de Operação e Suporte

ARILDO DISARO FILHO
29/08/2023 15:34

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 12ª REGIÃO - SANTA CATARINA

ATESTADO DE CAPACIDADE TÉCNICA nº 25/2023

Atesto, para todos os fins, que a empresa JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA, localizada no endereço SCES Trecho 2, Centro de Lazer Beira Lago, Conjunto 08, Loja 03, Asa Sul, Brasília-DF, CEP 70.200-002, inscrita no CNPJ sob o nº 24.425.034/0001-96, prestou ao Tribunal Regional do Trabalho da 12ª Região, localizado no endereço Rua Esteves Júnior, nº 395, centro, Florianópolis, SC, CEP: 88.015-905, inscrito no CNPJ sob o nº 02.482.005/0001-23, por meio do contrato Registro de Preços nº 10470/2022.

Serviços de auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados, endpoint e proteção e controle de acesso de usuários privilegiados (PAM), incluindo garantia, serviço de instalação e treinamento, parametrização e suporte no ambiente deste Tribunal, das seguintes ferramentas:

- 1 Cluster para prover recursos para solução de acesso a usuários privilegiados
- 30 Licenças para contas para acesso privilegiados simultâneos (admin segurança/rede/Root/DomainAdm in/DBadmin/SysDBA, VMadmin, helpdesk)
- 500 Licenças para servidores físicos e virtuais (Linux, Windows e Storages)
- 2.700 Licenças para estações de trabalho Windows
- 10 Licenças para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP)
- 50 Licenças para aplicações conteinerizadas com secrets
- 100 Licenças para aplicações não-conteinerizadas com senha embutida (hard coded)
- 8 Licenças para instancias de Banco de Dados (Oracle, Postgres, MSSQL e MySQL)
- 1 Serviço de instalação para solução de controle de acesso de usuários privilegiados
- 1 Treinamento para solução de controle de acesso de usuários privilegiados
- 12 Meses de serviço e suporte técnico especializado

Período: 24 de dezembro de 2022 até a presente data.

Local da prestação: Coordenadoria Segurança da Informação e Proteção de Dados, Tribunal Regional do Trabalho 12ª Região, Rua Esteves Júnior 395, centro, Florianópolis, CEP 88015-905, fones: (048) 3216-4240. E-mail de contato: segtic@trt12.jus.br.

PROAD 10470/2022. DOC 122. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2023.VMZZ.RTGB:
https://proad.trt12.jus.br/proad/pages/consultadocumento.xhtml

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 12ª REGIÃO - SANTA CATARINA

Conforme manifestação formal do gestor do contrato, o objeto deste contrato atingiu os objetivos e resultados acordados, não havendo nenhum tipo de conduta passível de desabonar os serviços prestados pela empresa.

Florianópolis, 29 de agosto de 2023.

Documento assinado digitalmente,
validado pelo QR Code na origem.

Arildo Disaró Filho
Assistente Chefe do Setor de Registro
de Preços e Cadastro de Fornecedores
Serviço de Licitações e Compras
TRT – 12ª Região

PROAD 10470/2022. DOC 122. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2023.VMZZ.RTGB:
https://proad.trt12.jus.br/proad/pages/consultadocumento.xhtml

PODER JUDICIÁRIO FEDERAL – JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 15ª REGIÃO

ATESTADO DE CAPACIDADE TÉCNICA

ATESTAMOS, para os devidos fins, que a empresa **JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA,** com sede na SRTVN Quadra 701, conjunto C, Ala B, Parte V, nº 124, Asa Norte, Brasília-DF, inscrita no CNPJ 24.425.034/0001-96, forneceu ao **TRIBUNAL REGIONAL DO TRABALHO DA 15ª REGIÃO**, por meio do contrato nº 116/2022, os itens relacionados abaixo:

- 1 Cluster para prover recursos para solução de acesso a usuários privilegiados.
- 46 Licenças para contas para acessos privilegiados simultâneos (admin segurança/rede/Root/DomainAdm in/DBadmin/SysDBA, VMadmin, helpdesk).
- 700 Licenças para servidores físicos e virtuais (Linux, Windows e Storages).
- 252 Licenças para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP).
- 12 Licenças para aplicações conteinerizadas com secrets.
- 60 Licenças para instâncias de Banco de Dados (Oracle, Postgres, MSSQL e MySQL).
- 1 Serviço de instalação para solução de controle de acesso de usuários privilegiados.
- 2 Treinamentos para solução de controle de acesso de usuários privilegiados.
- 12 Meses de serviço e suporte técnico especializado.

Atestamos ainda que, o fornecimento dos equipamentos, licenças e entrega dos serviços e suporte técnico foram executados satisfatoriamente, não existindo em nossos registros, até a presente data, fatos que desabonem sua conduta e responsabilidade com as obrigações assumidas.

PODER JUDICIÁRIO FEDERAL – JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 15ª REGIÃO

Campinas, 22 de março de 2023.

Andre Luis da Silva
andresilva@trt15.jus.br
(19) 3231-9500
Gestor do Contrato
Coordenador de Segurança da Informação de TIC

gov.br Documento assinado digitalmente
ANDRE LUIS DA SILVA
Data: 22/03/2023 16:50:37-0300
Verifique em https://validar.iti.gov.br

Bruno Tobias Stella
brunostella@trt15.jus.br
(19) 3231-9500
Gestor Suplente do Contrato
Coordenador de Infraestrutura de TIC

gov.br Documento assinado digitalmente
BRUNO TOBIAS STELLA
Data: 22/03/2023 18:49:38-0300
Verifique em https://validar.iti.gov.br

TRT-16ª REGIÃO
Sec. de Tecnologia da Informação e Comunicação

ATESTADO DE CAPACIDADE TÉCNICA Nº 1/2023

Referência: Adesão ARP TST 58/2021 - Processo TST Nº 6001640/2021-00

Instrumento de Contrato: Contrato nº 27/2022

Contratada: JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA, inscrita no CNPJ sob o no 24.425.034/0001-96.

Objeto: Aquisição de soluções de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados, endpoint e proteção e controle de acesso de usuários privilegiados (PAM), incluindo garantia, serviço de instalação e treinamento.

Data de assinatura do contrato: 28/10/2022
Vigência do contrato: 12 meses.
Produtos fornecidos:

Item	Qtde.	Descrição
1	880	Licença de uso de software e garantia por 12 meses para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*.
2	880	Licença de uso de software e garantia por 12 meses para funcionalidade de auditoria para disco em nuvem para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados.
3	1	Serviço de instalação para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*.
4	1	Treinamento para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint.*
5	1	*Cluster* para prover recursos para solução de acesso a usuários privilegiados.
6	1	Garantia do fabricante por período de 12 meses para *cluster* para prover recursos para solução de acesso a usuários privilegiados
7	45	Licença para contas para acesso privilegiado simultâneos (admin

		segurança/rede/Root/DomainAdm in/DBadmin/SysDBA, VMadmin, helpdesk).
8	45	Garantia do fabricante por período de 12 meses para licença para contas para acesso privilegiados simultâneos (admin segurança/rede/Root/DomainAdm in/DBadmin/SysDBA, VMadmin, helpdesk).
9	100	Licença para servidores físicos e virtuais (Linux, Windows e Storages).
10	100	Garantia do fabricante por período de 12 meses para licença para servidores físicos e virtuais (Linux, Windows e Storages).
11	750	Licença para estações de trabalho Windows.
12	750	Garantia do fabricante por período de 12 meses para licença para estações de trabalho Windows.
13	200	Licença para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP)
14	200	Garantia do fabricante por período de 12 meses para licença para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP).
15	34	Licença para aplicações conteinerizadas com secrets.
16	34	Garantia do fabricante por período de 12 meses para licença para aplicações conteinerizadas com secrets.
17	26	Licença para aplicações não- conteinerizadas com senha embutida (hard coded).
18	26	Garantia do fabricante por período de 12 meses para licença para aplicações não-conteinerizadas com senha embutida (hard coded).
19	34	Licença para instâncias de Banco de Dados (Oracle, Postgres, MSSQL e MySQL).
20	34	Garantia do fabricante por período de 12 meses para licença para instâncias de Banco de Dados (Oracle, Postgres,MSSQL e MySQL).

TRT-16ª REGIÃO
Sec. de Tecnologia da Informação e Comunicação

21	1	Serviço de instalação para solução de controle de acesso de usuários privilegiados.
22	1	Treinamento para solução de controle de acesso de usuários privilegiados.
23	12	Serviço e suporte técnico especializado

ATESTAMOS que os produtos foram entregues com qualidade satisfatória, cumprindo plenamente as exigências contratuais e que não constam em nossos arquivos, até a presente data, fatos a reportar que desabonem a conduta desta empresa.

Ressalvamos que o presente atestado não exime a contratada das responsabilidades futuras previstas em contrato.

Por ser verdade, firmamos o presente.

São Luís, 01/06/2023.

RODRIGO SILVEIRA ALEXANDRE:30816202

Assinado digitalmente por RODRIGO SILVEIRA ALEXANDRE:308162002
ND: C=BR, O=ICP-Brasil, OU=Autoridade Certificadora da Justica - AC-JUS, OU=21308480000122, OU=Videoconferencia, OU=Cert-JUS Institucional - A3, OU=Tribunal Regional do Trabalho da 16 Regiao - TRT16, OU=SERVIDOR, CN=RODRIGO SILVEIRA ALEXANDRE:308162002
Razão: Eu sou o autor deste documento
Localização:
Data: 2023.06.01 14:07:06-03'00'
Foxit PDF Reader Versão: 12.1.0

(datado e assinado digitalmente)
RODRIGO SILVA ALEXANDRE
Divisão de Infraestrutura e Segurança da Informação

TRT-16ª REGIÃO
Maranhão

Assinado de forma digital por RAFAEL ROBINSON DE SOUSA NETO:308161473
Dados: 2023.06.02 11:03:47 -03'00'

(datado e assinado digitalmente)
RAFAEL ROBINSON DE SOUSA NETO
Secretário de Tecnologia da Informação e Comunicação

PODER JUDICIÁRIO FEDERAL
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 17ª REGIÃO
Diretoria-Geral - DIGER
diger@trtes.jus.br - Tel: (27) 3321 2467

ATESTADO DE CAPACIDADE TÉCNICA

ATESTAMOS, para os devidos fins, que a empresa **JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA,** inscrita no CNPJ/MF sob n° 24.425.034/0001-96, com sede na SRTVN Quadra 701, conjunto C, Ala B, Parte V, n.º 124, Asa Norte, Brasília/DF, CEP: 70719-903, encontra-se prestando para este **TRIBUNAL REGIONAL DO TRABALHO DA 17ª REGIÃO**, CNPJ: 02.488.507/0001-61, com sede na Avenida Nossa Senhora dos Navegantes, 1245, Enseada do Suá, CEP: 29050-335, Vitória – ES, os serviços relacionados abaixo:

Termo de Contrato n.º 41/2022, assinado em 28/10/2022.

Vigência: 12 (doze) meses (atualmente, em estágio de prorrogação contratual).

DESCRIÇÃO DOS SERVIÇOS

Aquisição de soluções de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados, endpoint e proteção e controle de acesso de usuários privilegiados (PAM), incluindo garantia, serviço de instalação e treinamento.

Tabela demonstrativa da prestação do serviço:

GRUPO	ITEM	DESCRITIVO	UNIDADE	QUANTITATIVO
1	1	Licença de uso de software e garantia por 12 meses para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint.	Usuários	1.200
	2	Licença de uso de software e garantia por 12 meses para funcionalidade de auditoria para disco em nuvem para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados.	Usuários	1.200
	3	Serviço de instalação para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint.	Serviço	1
	4	Treinamento para solução de segurança, auditoria e prevenção de ameaças à base de	Turmas	1

		dados não estruturados, abrangendo centro de dados e endpoint. (30 horas)	(10 alunos)	

Atestamos ainda que a empresa contratada vem cumprindo as cláusulas contratuais, atuando com responsabilidade e conhecimento das obrigações, inexistindo qualquer fato que desabone a sua conduta.

Johnathan Marques Silveira Carioca
Secretário de Tecnologia da Informação e Comunicação (SETIC)
setic@trt17.jus.br

Carlos Tadeu Goulart
Diretor-Geral (DIGER)
diger@trt17.jus.br

Assinado digitalmente por:
CARLOS TADEU GOULART
Data: 06/10/2023

Assinado digitalmente por:
JOHNATHAN MARQUES SILVEIRA CARIOCA
Data: 05/10/2023

DOCUMENTO ASSINADO DIGITALMENTE
A autenticidade deste documento pode ser verificada abaixo ou no QR code
https://www.trt17.jus.br/principal/publicacoes/leitor/946430269?Formato=PDF&securityCode=TO8ivz+GHFpW6jX/dcTO4rkzBg9Afp5Kfg9K

PODER JUDICIÁRIO DA UNIÃO
TRIBUNAL REGIONAL DO TRABALHO DA 18ª REGIÃO
SECRETARIA-GERAL DA PRESIDÊNCIA
COORDENADORIA DE SEGURANÇA DA INFORMAÇÃO

VINÍCIUS GRACIANO ELIAS
02/06/2023 14:37

ATESTADO DE CAPACIDADE TÉCNICA

A Coordenadoria de Segurança da Informação do Tribunal Regional do Trabalho da 18ª Região, inscrito no CNPJ/MF n.º 02.395.868/0001-63**,** ATESTA, para fins de **comprovação de capacidade técnica**, que a empresa **JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA**, CNPJ/MF n.º 24.425.034/0001-96, sediada à SCES Trecho 2, Centro de Lazer Beira Lago, Conjunto 08, Loja 03, Asa Sul – Brasília - DF, CEP: 70.200-002, forneceu à declarante os produtos abaixo relacionados, conforme previsto no Contrato: **SLC-SEC Contrato nº 034/2022**

Objeto: Solução de controle de acesso de usuários privilegiados (PAM), incluindo garantia, serviço de instalação e treinamento, conforme especificações constantes no edital do "Pregão EletrônicO/SRP/TST Nº 58/2021"

Item	Descrição/Produtos	Qtde.
5	Cluster para prover recursos para solução de acesso a usuários privilegiados	1
7	Licença para contas para acesso privilegiados simultâneos (admin segurança /rede /Root /DomainAdmin /DBadmin /SysDBA, VMadmin, helpdesk)	45
9	Licença para servidores físicos e virtuais (Linux, Windows e Storages)	326
13	Licença para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch,Roteadores, Firewall e Controladoras WIFI, VOIP)	68
15	Licença para aplicações conteinerizadas com secrets	5
17	Licença para aplicações não conteinerizadas com senha embutida (hard coded)	20
19	Licença para instancias de Banco de Dados (Oracle, Postgres, MSSQL e MySQL)	11
21	Serviço de instalação para solução de controle de acesso de usuários privilegiados.	1
22	Treinamento para solução de controle de acesso de usuários privilegiados.	1

Informamos que os itens: 5, 7, 9, 13, 15, 17 e 19 foram contratados com garantia de 12 meses do fabricante, conforme itens de garantia constantes do contrato. Por fim atestamos, que a entrega dos produtos e a prestação dos serviços ocorreu de acordo com as expectativas e obrigações contratuais assumidas pela empresa.

Goiânia/GO, data da assinatura eletrônica.

[Assinado Eletronicamente]
VINICIUS GRACIANO ELIAS
Diretor da Coordenadoria de Segurança da Informação

JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 20ª REGIÃO

NEO VEDDER COSTA MARQUES
01/03/2023 10:15

LAURO AUGUSTO HOLANDA PEREIRA
01/03/2023 10:28

MARCOS XAVIER DE ALMEIDA BARRETTO
02/03/2023 10:30

ATESTADO DE CAPACIDADE TÉCNICA

PREÂMBULO

O Tribunal Regional do Trabalho da 20ª Região, inscrita no CNPJ sob o nº 01.445.033/0001-08, com sede na Av. Dr. Carlos Rodrigues da Cruz, s/nº - Centro Administrativo Governador Augusto Franco - Aracaju - SE, para fins de comprovação, que a empresa JAMC – Consultoria e Representação de Software LTDA , sob CNPJ n° 24.425.034/0001-96, sediada no Centro de Lazer Beira Lago, SCES Trecho 2, Lote 8, Loja 3, forneceu, executou e executa de maneira satisfatória Serviços de Monitoramento, Detecção e Resposta a Incidentes em regime 24x7 (vinte e quatro horas e sete dias por semana), com vigência de 19/09/2022 até o presente momento, assim como o fornecimento, instalação e parametrização das seguintes ferramentas:

- Fornecimento de solução de Auditoria, Monitoramento, Detecção e Resposta a Incidentes de ambiente centralizados para 700 usuários;
- Fornecimento de solução de Auditoria, Monitoramento, Detecção e Resposta a Incidentes de ambiente em nuvem para 721 usuários;
- Fornecimento de solução de Auditoria, Monitoramento, Detecção e Resposta a Incidentes de ativos de TI para 700 ativos;
- Fornecimento de ferramenta e serviço de operação especializada para solução de proteção a ativos de TI e credenciais privilegiadas nos seguintes quantitativos:
  - 30 credenciais privilegiadas;
  - 155 servidores;
  - 974 estações de trabalho;
  - 31 dispositivos de rede;
  - 10 aplicações;
  - 35 bases de dados.

Dados do Contrato	
Processo nº	4274/2021
Contrato nº	12/2022
Data de início da vigência	19/09/2022
Data de término da vigência	18/09/2023

PROAD 4274/2021. DOC 156. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2023.TJSD.ZGVJ:
https://proad.trt20.jus.br/proad/pages/consultadocumento.xhtml

JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 20ª REGIÃO

DECLARAÇÃO

ATESTA que os serviços foram / têm sido prestados de forma satisfatória, não havendo em nossos registros nenhum fato que desabone a conduta da empresa e sua responsabilidade em relação às tarefas assumidas.

Aracaju, 01 de março de 2023.

Neo Vedder
Fiscal Demandante e Técnico

Lauro A. Holanda Pereira
Fiscal Administrativo

Marcos Xavier de A. Barretto
Gestor do Contrato

Portaria DG nº 153/2022.

PROAD 4274/2021. DOC 156. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2023.TJSD.ZGVJ:
https://proad.trt20.jus.br/proad/pages/consultadocumento.xhtml

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 22ª REGIÃO

ATESTADO DE CAPACIDADE TÉCNICA

Declaramos, para os devidos fins, que a empresa **JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA,** CNPJ: 24.425.034/0001-96, situada na SRTVN Quadra 701, Conjunto C, Ala B, Parte V, nº 124, Asa Norte, Brasília-DF, CEP 70.719-903, forneceu sistema de controle de acesso de usuários privilegiados (PAM) e prestou serviços de instalação e capacitação de forma satisfatória, conforme dados especificados abaixo:

DADOS DA CONTRATANTE:
Denominação: TRIBUNAL REGIONAL DO TRABALHO 22ª REGIÃO – TERESINA – PIAUÍ - PI
CNPJ: 03.458.141/0001-40
Endereço: Av. João XXIII, 1460, bairro dos Noivos, CEP 64045-000, Teresina-PI
Contrato nº 26/2022 – Pregão Eletrônico Nº 58/2021 – TST
Objeto: Aquisição controle de acesso de usuários privilegiados (PAM), incluindo garantia, serviço de instalação e treinamento, conforme tabela abaixo:
Escopo do Fornecimento:

Item	Descrição detalhada	QT
5	Cluster para prover recursos para solução de acesso a usuários privilegiados	1
6	Garantia do fabricante por período de 12 meses para cluster para prover recursos para solução de acesso a usuários privilegiados	1
7	Licença para contas para acesso privilegiados simultâneos (admin segurança/rede/Root/DomainAdm in/DBadmin/SysDBA, VMadmin, helpdesk)	15
8	Garantia do fabricante por período de 12 meses para licença para contas para acesso privilegiadossimultâneos (admin segurança/rede/Root/DomainAdmin/DBadmin/SysDBA, VMadmin, helpdesk)	15
9	Licença para servidores físicos e virtuais (Linux, Windows e Storages)	200
10	Garantia do fabricante por período de 12 meses para licença para servidores físicos e virtuais (Linux, Windows e Storages)	200
11	Licença para estações de trabalho Windows	1200
12	Garantia do fabricante por período de 12 meses para licença para estações de trabalho Windows	1200
13	Licença para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP)	120
14	Garantia do fabricante por período de 12 meses para licença para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP)	120
17	Licença para aplicações não-conteinerizadas com senha embutida (hard coded)	65
18	Garantia do fabricante por período de 12 meses para licença para aplicações não-conteinerizadas com senha embutida (hard coded)	65
19	Licença para instâncias de Banco de Dados(Oracle,Postgres, MSSQL e MySQL)	15
20	Garantia do fabricante por período de 12 meses para licença para instâncias de Banco de Dados (Oracle, Postgres, MSSQL e MySQL)	15
21	Serviço de instalação para solução de controle de acesso de usuários privilegiados.	1
22	Treinamento para solução de controle de acesso de usuários privilegiados.	1

Teresina/PI, 25 de agosto de 2023.

(Assinado Digitalmente)
Leonardo de Oliveira Rafael
ASSISTENTE-CHEFE DA SEÇÃO DE SEGURANÇA DA INFORMAÇÃO

LEONARDO DE OLIVEIRA RAFAEL:87116740325

Digitally signed by LEONARDO DE OLIVEIRA RAFAEL:87116740325
DN: c=BR, o=ICP-Brasil, ou=Secretaria da Receita Federal do Brasil - RFB, ou=RFB e-CPF A3, ou=VALID, ou=AR SOLIMOES CERTIFICADORA, ou=Presencial, ou=22759531000103, cn=LEONARDO DE OLIVEIRA RAFAEL:87116740325
Date: 2023.08.25 12:28:46 -03'00'

JUSTIÇA DO TRABALHO

Tribunal Regional do Trabalho da 24ª Região
Secretaria de Tecnologia da Informação e Comunicações

GESLAINE PEREZ MAQUERT
11/04/2023 10:05

ATESTADO DE CAPACIDADE TÉCNICA

Atestamos para os devidos fins que a empresa **JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA EPP**, CNPJ/MF n.º 24.425.034/0001-96, sediada à SRTVN Quadra 701, conjunto C, Ala B, Parte V, Nº 124, Asa Norte, Brasília-DF, CEP 70.719-903, mantém contrato com o **TRIBUNAL REGIONAL DO TRABALHO DA 24ª REGIÃO (TRT24)**, conforme detalhamento a seguir:

Processo Administrativo: PROAD TRT24 nº 19.874/2022
Contrato nº: 24/2022

Objeto: soluções de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados, endpoint e proteção e controle de acesso de usuários privilegiados (PAM), abrangendo garantia, serviço de instalação e treinamento., de acordo com os quadros abaixo, conforme especificações constantes do "Anexo I do Edital do Pregão Eletrônico 058/2021 – TST", ao qual este TRT24 aderiu à contratação.

Data de assinatura do contrato: 28/10/2022.
Vigência do contrato: 12 (doze) meses.
Produtos Fornecidos:

Item	Qtde.	Descrição
1	1300	Licença de uso de software e garantia por 12 meses para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint
2	1300	Licença de uso de software e garantia por 12 meses para funcionalidade de auditoria para disco em nuvem para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados
3	1	Serviço de instalação para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint
4	1	Treinamento para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint
5	1	Cluster para prover recursos para solução de acesso a usuários privilegiados
6	1	Garantia do fabricante por período de 12 meses para cluster para prover recursos para solução de acesso a usuários privilegiados
7	42	Licença para contas para acesso privilegiados simultâneos (admin segurança/rede/Root/DomainAdm in/DBadmin/SysDBA, VMadmin, helpdesk)
8	42	Garantia do fabricante por período de 12 meses para licença para contas para acesso privilegiados simultâneos (admin segurança/rede/Root/DomainAdm in/DBadmin/SysDBA, VMadmin, helpdesk)
9	420	Licença para servidores físicos e virtuais (Linux, Windows e Storages)
10	420	Garantia do fabricante por período de 12 meses para licença para servidores físicos e virtuais (Linux, Windows e Storages)
11	1500	Licença para estações de trabalho Windows
12	1500	Garantia do fabricante por período de 12 meses para licença para estações de trabalho Windows
13	170	Licença para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP)

JUSTIÇA DO TRABALHO

Tribunal Regional do Trabalho da 24ª Região
Secretaria de Tecnologia da Informação e Comunicações

14	170	Garantia do fabricante por período de 12 meses para licença para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP)
15	25	Licença para aplicações conteinerizadas com secrets
16	25	Garantia do fabricante por período de 12 meses para licença para aplicações conteinerizadas com secrets
17	45	Licença para aplicações nãoconteinerizadas com senha embutida (hard coded)
18	45	Garantia do fabricante por período de 12 meses para licença para aplicações não-conteinerizadas com senha embutida (hard coded)
19	30	Licença para instancias de Banco de Dados (Oracle, Postgres, MSSQL e MySQL)
20	30	Garantia do fabricante por período de 12 meses para licença para instancias de Banco de Dados (Oracle, Postgres, MSSQL e MySQL)
21	1	Serviço de instalação para solução de controle de acesso de usuários privilegiados
22	1	Treinamento para solução de controle de acesso de usuários privilegiados
23	12	Serviço e suporte técnico especializado

Declaramos que os produtos foram entregues com qualidade satisfatória, cumprindo plenamente as exigências contratuais e que não constam em nossos arquivos, até a presente data, fatos a reportar que desabonem a conduta desta empresa.

Ressalvamos que o presente atestado não exime a contratada das responsabilidades futuras previstas em contrato.

Por ser verdade, firmamos o presente.

Campo Grande, 11 de abril de 2023.

(Assinado Eletronicamente)

Geslaine Perez Maquerte
Chefe da Divisão de Proteção de Dados e Segurança da Informação
Gestora do Contrato no TRT24 conforme Portaria TRT/DG 086/2023
Matrícula: 30824201
Telefone: (67) 99206-1013

ATESTADO DE CAPACIDADE TÉCNICA

Atestamos para os devidos fins que a empresa **JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA**, inscrita no CNPJ nº 24.425.034/0001-96, estabelecida na Alamenda Rio Negro, nº 500, 5º Andar, Sala 501 a 508, Torre B, Alphaville Centro Industrial e Empresarial, cidade de Barueri/SP, Telefone/Fax: (11) 3136-0190 CEP: 06.454-000, presta de maneira satisfatória os serviços abaixo discriminados ao Tribunal Regional do Trabalho da 11ª Região, sito Rua Visconde de Porto Alegre, 1265, 4º andar - Manaus/AM, inscrito no CNPJ sob nº 01.671.187/0001-18:

Em relação ao Contrato nº 31/2022/TRT11 que têm por objeto os serviços de Monitoramento, Detecção e Resposta aos Incidentes em regime 24x7 (vinte e quatro horas e sete dias por semana), assim como o fornecimento, instalação, parametrização e suporte no ambiente deste Tribunal, das seguintes ferramentas:

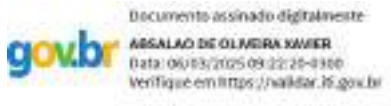
- **1.600** Licenças de uso de software e garantia por **12** meses para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint.
- **1.600** Licenças de uso de software e garantia por **12 meses** para funcionalidade de auditoria para disco em nuvem para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados.
- **1** Serviço de instalação para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint.
- **1** Treinamento para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint.
- **1** Cluster para prover recursos para solução de acesso a usuários privilegiados
- **12** Licenças para contas para acesso privilegiados simultâneos (admin segurança/rede/Root/DomainAdm in/DBadmin/SysDBA, VMadmin, helpdesk)
- **375** Licenças para servidores físicos e virtuais (Linux, Windows e Storages)
- **2.100** Licenças para estações de trabalho Windows
- **300** Licenças para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, APE WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP)
- **35** Licenças para aplicações conteinerizadas com secrets

- **40** Licenças para aplicações não-conteinerizadas com senha embutida (hard coded)
- **10** Licenças para instâncias de Banco de Dados (Oracle, Postgres, MSSQL e MySQL)
- **1** Serviço de instalação para solução de controle de acesso de usuários privilegiados
- **1** Treinamento para solução de controle de acesso de usuários privilegiados
- **12 Meses** de serviço e suporte técnico especializado

Em relação ao 1º Termo Aditivo que prorrogou o prazo da vigência do Contrato nº 31/2022/TRT11, por mais **12 (doze) meses**, referente às soluções de segurança, auditoria e prevenção de ameaças, pelo **período de 07/10/2023 a 06/10/2024**, ficando ratificadas as demais cláusulas e condições do contrato originário.

Em relação ao 2º Termo Aditivo que prorrogou o prazo da vigência do Contrato nº 31/2022/TRT11, por mais **12 (doze) meses**, referente às soluções de segurança, auditoria e prevenção de ameaças, pelo **período de 07/10/2024 a 06/10/2025**, bem como suprimiu em 25% o quantitativo de serviços do Item 1 e em 6,25% o quantitativo de serviços Item 2, os quais passaram a operar da seguinte maneira:

- **Item 1: 1.200** Licenças de uso de software e garantia por **12 meses** para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint.
- **Item 2: 1.500** Licenças de uso de software e garantia por **12 meses** para funcionalidade de auditoria para disco em nuvem para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados.



_____

Absalao de Oliveira Xavier

Chefe da SEMOSE/ DISEGINF/ SETIC – TRT 11ª Regiao

Av. Tefé, 930 – Praça 14 de Janeiro
Sede Administrativa – 3º Andar
Manaus/AM – 69020-090
Telefone: (92) 3621-7480 / 7474
e-mail: ti.seguranca@trt11.jus.br

À

JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA

A VARONIS SYSTEMS INC. (Varonis), DECLARA que a empresa JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA (PETA) inscrita no CNPJ/MF sob o nº 24.425.034/0001-96, sediada na SCES Trecho 02, Lote 08, Loja 03, BRASÍLIA-DF, CEP: 70.200-002, está autorizada a ofertar, comercializar, instalar, configurar e fornecer suporte técnico para provimento da solução de detecção e resposta à incidentes, auditoria e proteção de dados, detecção e resposta a ameaças baseadas em dados, coleta de fluxos de metadados, e análise constante de dados e de seus repositórios de dados corporativos, plataforma de compartilhamento colaborativo, a ser adquirida pela COMPANHIA DE SANEAMENTO DE SERGIPE (DESO), objeto do Pregão Eletrônico nº 044/2026.

Sem mais para o momento.

Atenciosamente,

gov.br Documento assinado digitalmente
RICARTE DE LIMA BERNARDES NETO
Data: 14/05/2026 13:45:32-0300
Verifique em https://validar.iti.gov.br

ATESTADO DE CAPACIDADE TÉCNICA

Atestamos para os devidos fins que a empresa **JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA**, inscrita no CNPJ nº. 24.425.034/0001-96, sediada em Brasília/DF, SRTVN Quadra 701, Conjunto C, Ala B, Parte V, nº 124, Sala 421, Asa Norte, CEP: 70.712-900, firmou com o **BANCO REGIONAL DE DESENVOLVIMENTO DO EXTREMO SUL - BRDE**, instituição financeira pública, com sede em Porto Alegre/RS, na Rua Uruguai, nº 155, 4º andar, inscrito no CNPJ sob o nº 92.816.560/0001-37, o Contrato nº 2022101 para o seguinte objeto: *"contratação de subscrição para uso de Solução de Auditoria e Gerenciamento de Serviços On-Premises (Microsoft Active Directory – AD, Microsoft File Server e de análise de comportamento e alarme em tempo real) e na Nuvem (Microsoft Office 365), bem como de prestação de serviços técnicos de implantação, garantia, correção/atualização de software, suporte técnico e treinamento na solução adquirida".* O referido contrato, oriundo do Processo de Licitação Eletrônica BRDE nº 2022/000193, dispõe, até o momento, das seguintes características e informações:

- **Contrato (início vigência em 23/01/2023):**

ITEM	DESCRIÇÃO	QUANTIDADE MÁXIMA
01	Subscrição dos Módulos da Solução – Serviços On-Premisses	Faixa de Usuários 1001 a 1050
02	Subscrição dos Módulos da Solução – Serviços em Nuvem	Faixa de Usuários 651 a 700
03	Serviço de implantação	Único
04	Hora técnica de suporte técnico	250 horas
05	Serviço de treinamento	40 horas

- **Aditivo nº 01 (assinatura 22/12/2023):** acréscimo de objeto/ampliação faixa usuários item 02

ITEM	DESCRIÇÃO	QUANTIDADE MÁXIMA
02	Subscrição dos Módulos da Solução – Serviços em Nuvem	Faixa de Usuários 801 a 850

- **Aditivo nº 02 (assinatura 02/01/2024):** prorrogação da vigência contratual por mais 12 (doze) meses, a partir de 23/01/2024, tendo seu término previsto para 22/01/2025.

Atestamos ainda que os serviços foram prestados satisfatoriamente, no que diz respeito às informações discriminadas acima, não havendo em nossos registros fatos que desabonem sua conduta e desempenho.

Porto Alegre/RS, 19 de março de 2024.

VITORIA ALMEIDA LUNARDELLI:04513481927

Assinado de forma digital por VITORIA ALMEIDA LUNARDELLI:04513481927
Dados: 2024.03.19 16:20:06 -03'00'

Vitória Almeida Lunardelli
Chefe do Departamento Administrativo
E-mail: vitoria.lunardelli@brde.com.br – Telef.: 51 3215-4977
BANCO REGIONAL DE DESENVOLVIMENTO DO EXTREMO SUL – BRDE

VARONIS

Microsoft OneDrive

Proteja seus dados confidenciais contra exposição excessiva e ataques cibernéticos.

Desafio

O OneDrive permite que os usuários do Microsoft 365 armazenem e compartilhem grandes quantidades de dados para colaboração remota na nuvem em tempo real.Os recursos de sincronização e compartilhamento do OneDrive tornam praticamente impossível identificar e proteger arquivos confidenciais entre milhares de usuários e petabytes de dados com as funções de segurança integradas da Microsoft.

Soluções

Com a Varonis, você pode visualizar automaticamente onde seus dados confidenciais estão em risco nos bilhões de arquivos armazenados e compartilhados no OneDrive e reduzir de forma proativa a exposição excessiva. Monitore a atividade dos dados de maneira transparente e registre uma trilha de auditoria completa dos eventos para entender como os usuários compartilham, acessam e utilizam dados, a fim de poder detectar os primeiros sinais de ameaças e mitigar os riscos.

> "A Varonis nos dá a visibilidade necessária em nossos ambientes Exchange Online e OneDrive. Saber que melhoramos a visibilidade na nossa nuvem pública e infra-estrutura on-premises nos dá uma tranquilidade enorme."
>
> CTO, Prospect Capital Management

Leia o estudo de caso →

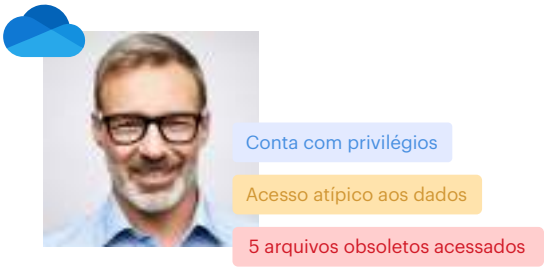
Arquivos compartilhados com usuários externos	Arquivos confidenciais	Arquivos compartilhados publicamente	Tamanho das pastas com dados obsoletos
46%	433 Arquivos	73%	184 GB

Classifique e bloqueie seus dados confidenciais.

Classifique de forma automática e precisa os dados confidenciais compartilhados e armazenados no OneDrive para alcançar a conformidade e priorizar seus esforços de remediação.Mapeie permissões para acessar e eliminar a exposição de dados confidenciais por meio de links compartilhados, grupos ou permissões diretas.

Diretório	Acesso	Classificação
CORPFS02		
C:\PERSONAL		
CC_NUMBERS.XLSX	EVERYONE	PCI, PHI, PII
HR_ONBOARDING.DOC	TODOS	PII, LGPD, CCPA
CUSTOMER_ORDERS.XLSX	TODOS	PCI

Quantidade irregular de dados confidenciais inativos acessados



Detecte e responda à ameaças rapidamente.

Combata ransomware e ameaças internas com alertas baseados em comportamento. A Varonis envia alertas de forma proativa sobre ameaças aos seus dados do OneDrive, como acesso incomum à dados confidenciais, presença de ferramentas de hacking ou atividades de compartilhamento suspeitas. As respostas automatizadas podem ajudar você à impedir ameaças antes que elas se instalem.

Investigue incidentes com agilidade.

A Varonis cria um registro normalizado de ações de compartilhamento de arquivos, pastas e links no OneDrive, incluindo ações realizadas pelo Microsoft Teams. Investigue rapidamente um incidente de segurança com um log de investigação detalhado. Pesquise e filtre por usuário, servidor de arquivos, tipo de evento etc. Correlacione eventos do OneDrive a outros eventos de sistemas como SharePoint, servidores de dados on-premises, Active Directory e muito mais.

Agente: (contém) Adam Nelson

Serviço	Tipo	Objeto
	Arquivo aberto	M&A Due Diligence.docx
	Arquivo aberto	G&A Legal Budget.xlsx
	Arquivo aberto	Interesting.txt

Experimente a Varonis gratuitamente.

Todos os produtos da Varonis podem ser testados gratuitamente e são acompanhadas de uma avaliação de riscos preparada por engenheiros. A maneira mais fácil de começar é com uma breve demonstração e uma conversa individual.

Contato

SharePoint e SharePoint Online

Proteja seus dados do SharePoint contra exposição excessiva e ataques cibernéticos.

Desafio

O SharePoint pode ser uma ferramenta de colaboração poderosa, mas é extremamente difícil de proteger em grande escala. Com centenas (ou milhares) de sites/subsites/bibliotecas, níveis de permissão personalizáveis, compartilhamento de links e usuários/grupos locais que podem conter grupos AD, responder à uma pergunta simples como "Quais dados uma pessoa pode acessar?" torna-se um projeto arqueológico.

Soluções

A Varonis permite visualizar e quantificar instantaneamente os riscos em todo o ambiente do SharePoint, independentemente do tamanho e da complexidade, além de reduzir a exposição de forma proativa.

A Varonis detecta e classifica informações confidenciais, mostra exatamente quem tem acesso aos dados e captura cada ação em uma trilha de auditoria detalhada (sem auditoria nativa) para que você possa detectar ameaças avançadas e investigar incidentes com rapidez.

> "Sem a Varonis, todas as decisões são reativas. As ferramentas da Microsoft não oferecem o mesmo nível de visibilidade. Com a Varonis, podemos tomar decisões estratégicas para proteger nossos dados de forma proativa. A Varonis nos dá uma vantagem competitiva."
>
> CISO, U.S. Commodities Trader

Leia o estudo de caso →

Arquivos compartilhados com usuários externos	Arquivos confidenciais compartilhados externamente	Pastas compartilhadas publicamente	Tamanho das pastas com dados obsoletos
42%	38%	7%	0.64 GB

Limite o raio de exposição do SharePoint.

A Varonis mostra onde os dados confidenciais são expostos externamente, para usuários convidados ou para todos os funcionários, assim você elimina com rapidez os riscos mais críticos. Além disso, oferece uma visão intuitiva das permissões efetivas para qualquer usuário ou grupo, independentemente da origem das permissões. Nossa tecnologia de machine learning analisa as permissões e o comportamento do usuário para destacar onde os usuários têm acesso aos dados que não utilizam ou necessitam.





Classifique e bloqueie os dados em grande escala.

Classifique dados confidenciais e regulamentados em seu ambiente SharePoint de maneira automática e precisa com centenas de políticas integradas, dicionários e regras de validação. Painéis e relatórios específicos do SharePoint fornecem conhecimento em tempo real da sua abordagem de risco e ajudam a garantir a conformidade com as regras e os regulamentos relevantes. Use nosso mecanismo de rotulagem para aplicar etiquetas MIP persistentes à arquivos sensíveis para criptografia, DRM e muito mais.

Monitore e investigue atividades suspeitas.

A Varonis amplia seu campo de visão incorporando atividades do SharePoint e do SharePoint Online ao contexto de outros aplicativos M365 e sistemas de telemetria on-premises e de perímetro. Nossas detecções baseadas no comportamento correlacionam a atividade no SharePoint com o comportamento de login, acesso aos dados on-premises e atividade de e-mail para gerar alertas precisos com poucos falsos positivos.



Experimente a Varonis gratuitamente.

Todos os produtos da Varonis podem ser testados gratuitamente e vêm com uma avaliação de riscos preparada por engenheiros. A maneira mais fácil de começar é com uma breve demonstração e uma conversa individual.

Contato

DatAdvantage Cloud

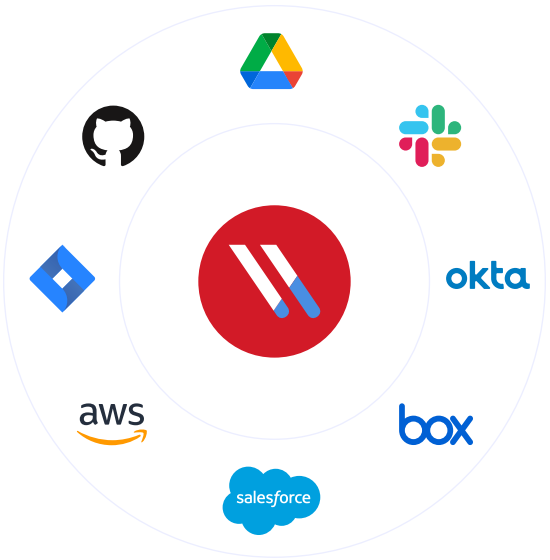
Conheça o novo padrão de segurança na nuvem

Desafio

À medida que as empresas tornam-se mais dependentes dos serviços em nuvem, a proteção de dados confidenciais contra ataques cibernéticos e superexposição acidental fica cada vez mais complexa. Cada serviço em nuvem isolado tem seus próprios tipos de dados, modelos de permissões e formatos de logs de atividades. A falta de visibilidade e controle unificados sobre os dados nos serviços SaaS e IaaS deixa as empresas vulneráveis a violações graves.

Soluções

O DatAdvantage Cloud correlaciona identidades entre nuvens com privilégios e atividades com AWS, Google Drive, Box, Salesforce, Zoom, Okta, GitHub, Slack e Jira. Com isso, as empresas finalmente podem ver **e priorizar seus maiores riscos na nuvem, reduzir** proativamente **o raio de destruição** e realizar **investigações mais rápidas entre nuvens.**



Informações sobre risco na nuvem

43%

dos usuários de nuvem

são alvos fáceis e desamparados de invasores

20%

dos usuários de nuvem

podem acessar dados corporativos confidenciais

15%

dos funcionários

transferem dados da empresa para contas pessoais na nuvem[1]

> "A capacidade de dimensionar o acesso corretamente e detectar o uso indevido na **mesma plataforma** facilita o gerenciamento do processo de segurança e oferece proteção quando ocorrem incidentes."
>
> CISO e DPO
> Apps Flyer

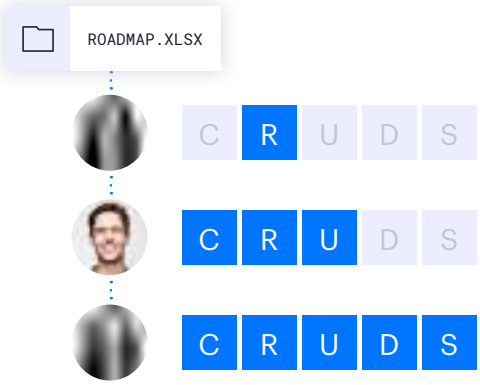
Leia o estudo de caso →

[1] Varonis 2021 SaaS Risk Report

Reduza o raio de exposição

O DatAdvantage Cloud mapeia e normaliza as permissões em um modelo simples de criação, leitura, atualização, exclusão e compartilhamento (CRUDS), para que seja possível reduzir o raio de exposição de maneira proativa. Responda a perguntas de vital importância em segundos:

- Quem tem acesso ao nosso roteiro confidencial de produtos?
- Como estão conseguindo acesso?
- O que fazem com ele?



Agente	Serviço	Tipo
	Jira	Autenticação
	aws	Acesso
	okta	Gerenciamento de usuários

Conduza investigações rápidas entre nuvens

Nós padronizamos e enriquecemos os eventos em nuvem de todos os seus serviços em nuvem, apresentando respostas simples para perguntas complexas:

- Quais usuários externos têm permissões em qualquer aplicativo SaaS?
- Algum administrador está acessando sem MFA?
- Quais alterações na configuração os usuários da lista de observação fizeram em todos os nossos aplicativos?

Alerta sobre atividades suspeitas e violações de políticas

Impeça sequestros de contas na nuvem, ameaças internas e violações de políticas involuntárias com auditoria e alertas entre nuvens. Utilize alertas prontos para uso ou crie seus próprios alertas



Experimente a Varonis gratuitamente

Todos os produtos Varonis podem ser experimentados gratuitamente e são fornecidos com uma avaliação de riscos realizada por engenheiros. A maneira mais fácil de começar é com uma breve demonstração e uma conversa individual.

Contato

VARONIS

A PLATAFORMA DE SEGURANÇA DE DADOS PROJETADA PARA A ERA DA IA

Descubra e classifique continuamente os dados confidenciais, remova as exposições e bloqueie as ameaças em tempo real com a automação baseada em IA.

Nem todas as soluções são iguais.

O mercado de segurança de dados está repleto de soluções pontuais e projetos que falham com frequência e lentamente. Os provedores de soluções de classificação de dados tentam catalogar dados confidenciais, mas não conseguem dizer se esses dados estão expostos ou sob ataque. Os provedores de DSPM baseados exclusivamente no modelo IaaS só podem verificar parte dos seus dados, o que fragmenta a visibilidade dos dados e das políticas de segurança. A Varonis é a única plataforma de segurança de dados (DSP) totalmente automatizada que reduz a probabilidade de violação de dados enquanto você dorme.

OS PONTOS FORTES DA NOSSA AUTOMAÇÃO

Visibilidade em tempo real

- Análises abrangentes em enormes repositórios de dados. Sem pontos cegos
- Descubra se dados confidenciais estão expostos, rotulados ou sob ataque
- Monitore todas as atividades de dados. Visibilidade sempre atualizada

Prevenção automatizada

- Garanta que os usuários e copilots de IA possam acessar apenas os dados corretos
- Corrija erros de configuração e remova usuários fantasmas
- Aplique políticas de rotulagem, DLP e residência de dados

Detecção proativa

- Centenas de modelos de ameaças UEBA alimentados por IA
- Alertas em tempo real e resposta automatizada à ameaças
- Serviço MDDR 24x7x365 e busca à ameaças

Uma plataforma. Todos os seus dados.

O Varonis protege dados corporativos onde quer que eles estejam — nos maiores e mais importantes repositórios de dados e aplicativos em nuvem e atrás do seu firewall.

- SaaS
- IaaS
- Compartilhamentos de arquivos
- Banco de dados
- E-mail
- NAS híbrido

VARONIS

Faça parceria com a empresa líder em segurança de dados.

Gartner

Provedora nº 1 de DSPM no Gartner Insights

FORRESTER

Líder no Forrester Wave™: Plataforma de Segurança de Dados, 1.º trimestre de 2023

GIGAOM

Líder em radar GigaOm para plataformas de segurança de dados (DSP)

Automatize centenas de casos de uso.

Sua plataforma unificada para encontrar automaticamente dados confidenciais, remover exposições e impedir ameaças. A Varonis reduz significativamente a probabilidade de vazamento de dados em tempo recorde.

- DSPM
- Descoberta e Classificação de Dados
- dlp na nuvem
- Segurança de IA
- UEBA
- Gerenciamento de Detecção e Resposta de Dados (MDDR)
- Automação de Políticas
- SSPM
- Governança de acesso aos dados
- Gestão de conformidade
- Segurança de e-mail
- Segurança do Active Directory

Reduza os riscos sem se arriscar.

Nossa avaliação gratuita de risco de dados leva minutos para ser configurada e oferece valor imediato. Em menos de 24 horas, terá uma visão clara e baseada no risco dos dados mais importantes e um caminho assertivo para a segurança desses dados.

Comece em www.varonis.com/demo.



GETTING STARTED WITH VARONIS SAAS

Publishing Information

Software Version	
Publication date	December 5, 2024

Copyright © 2005 -2024 Varonis Systems Inc.
All rights reserved.
This information shall only be used in conjunction with services contracted for with Varonis Systems, Inc. and shall not be used to the detriment of Varonis Systems, Inc. in any manner. User agrees not to copy, reproduce, sell, license, or transfer this information without prior written consent of Varonis Systems, Inc.
Other brands and products are trademarks of their respective holders.

Contents

Chapter 1: Welcome to Varonis SaaS. 4
About Data Security Platform in Varonis SaaS. 5
Varonis SaaS Architecture. 5
Varonis SaaS High-Level Deployment Flow. 8
Chapter 2: Requirements. 11
Varonis SaaS Deployment Prerequisites. 12
Monitored Data Source Requirements. 13
Varonis SaaS Prerequisite Checker Tool. 13
Running the Varonis Installation Cleaner. 24
Data Labeling Prerequisites. 24
Privacy Automation Prerequisites. 27
File Types Supported for Classification. 29
File Types Supported for Data Labeling. 36
Chapter 3: Installation and Configuration. 37
Installing a Collector. 38
Requirements for a Certificate Issued by an Enterprise Certificate Authority 44
Adding an Active Directory Data Source. 46
Adding Monitored Data Sources. 48
Configuring Federated Authentication (SSO). 53
Using Entra ID for the New Relying Trust. 61
Using Active Directory Federation Services (AD FS) for the New Relying Trust. 68
Using Okta for the New Relying Trust. 71
Configuring Varonis SaaS Security Roles. 77
Chapter 4: Upgrade the Collectors. 85
On-Premises Component Upgrade/Update – Architecture and Security Measures. 87
Chapter 5: Configuring Live Update for the (Deprecated) Deployment Hub. . . . 89
Chapter 6: Tour the Varonis SaaS Web Interface. 93
Chapter 7: Product Trust and Security. 109

1 WELCOME TO VARONIS SAAS

This guide tells you everything you need to know about getting up and running with Varonis SaaS. Here, you'll find information about the Varonis SaaS architecture, deployment plan, trust and security, and instructions for registering and activating your license. You'll also find instructions for installing the Collectors as well as adding an Active Directory (AD) data source. Finally, we'll show you how to configure your monitored data sources and offer you a tour of the Varonis Web Interface.

Before you dive in, click here to read more about the Data Security Platform in Varonis SaaS.

About Data Security Platform In Varonis SaaS

Data Security Platform

The Varonis Data Security Platform is an analytic software-based solution for data usage management.

With the Data Security Platform, organizations can see, understand, and manage who is using data, to control data access and enforce compliance with data usage policies to meet business needs.

The Data Security Platform addresses the growing need for regulating data usage within organizations, enabling full visibility and accountability of data usage across legal, financial, data security, intellectual property, and data privacy requirements.

Varonis SaaS

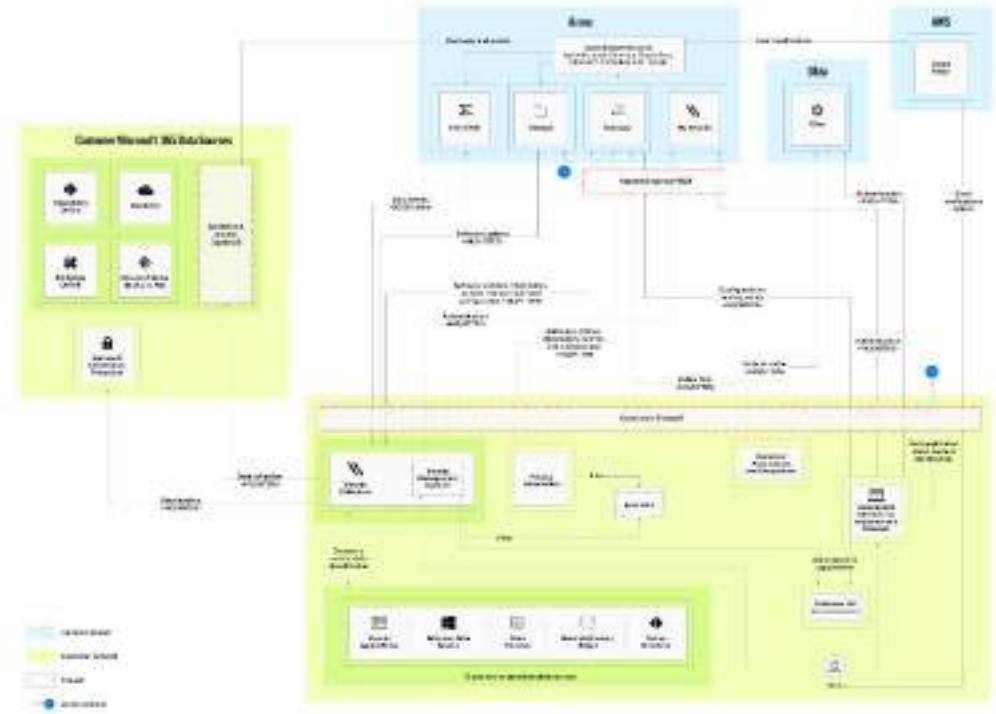
Varonis SaaS offers the Data Security Platform as a service in the cloud, leveraging continuous value with reduced capital expenses, time to value, and maintenance. Varonis products are provided as a SaaS solution, and the Varonis Collector is located near the monitored data sources. Cloud maintenance is handled by Varonis; upgrades are automatic and transparent, and bug fixes and new capabilities are provided directly in the product.

Take a look at Varonis SaaS Architecture to learn more about the system and its components.

Varonis SaaS Architecture

Varonis SaaS architecture is secure, scalable, and flexible, enabling you to monitor your organization's data with ease.

The following diagram showcases the Varonis SaaS architecture.



To download the architecture diagram, click the paper clip icon in the top right corner. Then select the PNG file and click Download.

- Varonis SaaS - The area in which all cloud infrastructure services and application services are hosted and running.
- My Varonis (my.varonis.com) and Okta - The identity manager for Varonis SaaS users. A login page through which users connect to the system. Users are authenticated via either accounts that they create in MyVaronis or are redirected to their Identity Provider (IdP) via SAML federation.
- Customer IdP – Customer Identity Provider (IdP) service, used when SAML federation is enabled for the tenant
- Varonis SaaS Services - Cloud services that scan data sources and calculate user security posture; Varonis SaaS stores only metadata (file, folder, and user names) but not document contents.
- Gateway - Varonis web gateway that acts as the front end for Varonis SaaS services.
- Event Hubs - Real-time data ingestion cloud services; used by Varonis to receive data from the Collector so that other Varonis SaaS services can consume the data in the cloud.
- Storage - Access stored reports.
- Email Relay - Send system and applicative emails.
- Varonis Management Console - For environment configuration.
- Varonis Web Interface - For query and data analysis.
- Privacy Automation - A server that retrieves files from the Sync Unit and indexes them to enable data subject requests and data archival.
- Sync Unit - A shared folder to which all Collectors write files for indexing by Privacy Automation.
- Customer Automations and Integrations – Customer scripts or applications that directly interact with Varonis SaaS APIs using API keys.
- Varonis Collectors - Collect and audit user activity events and data source metadata, and send data to Varonis SaaS for analysis and processing; Varonis Collectors are installed near the monitored data sources, publish threat detection alerts through syslog, and execute response scripts.

  Note: All changes conducted by Varonis automations are executed by the Collector (including changes applied to Entra ID, SharePoint Online, and OneDrive data sources).

For a further detailed explanation about the architecture, see Varonis in the Cloud: Building a Secure and Scalable Data Security Platform.

Now that you understand the architecture of Varonis SaaS, click here to see an overview of the deployment flow.

Varonis SaaS High-Level Deployment Flow

This high-level deployment walkthrough teaches you how to set up everything you need to monitor and protect data in your organization. We'll take you through the steps needed to finalize your registration, install on-premises components, and enroll monitored servers.

To work with Varonis, you need at least one Collector and one data source in your environment. You must also add an Active Directory (AD) data source; it is required to resolve the AD users and groups who have permissions to the data stored in other monitored data sources.

Next, read on to learn how to deploy Varonis SaaS.

> Note: Varonis Sales Engineers will assist with the installation.

1. Activate your Varonis Community account

Once you are registered with Varonis, before you can download the files required for installation, you must first be invited into the Varonis Community page by your Varonis contact. Once invited, you will receive an email that outlines the required activation steps to finalize your account. Varonis recommends establishing federation between My Varonis and your Identity Provider.

> Note: If you're already part of the Varonis community and you already have an active account, you can skip this step.

2. Install your first Collector

The Collector is a Varonis service that monitors and collects data from data sources in your organization. Every data source monitored by Varonis is assigned to a Collector, so monitoring your first data source starts with setting up a Collector.

Consult your Varonis account team for the recommended topology and server requirements. On the server where the Collector is to be installed, access the Varonis Web Interface, and from the Management menu, select System Topology, then on the Collectors tab, click + New Collector. Download the installer, double-click it, and proceed with the installation. Click here to view the full installation procedure.

3. Add an Active Directory data source

Once your first Collector is set up, you'll need to add an Active Directory data source for Varonis to monitor. Information about the users and groups will be collected from this data source and used to enrich the data collected from monitored data sources. To configure, open the Management Console, go to Management > Components > Root and start by switching to the Domains tab and clicking the Add button. You'll be prompted to fill in the data source type; specify Active Directory.

Click here to view the full installation procedure. Once you click Install, you'll be returned to the Domains tab, where you can follow the installation progress.

4. Monitor your first data source

Once your first Collector and Active Directory data source are set up, you can monitor your first data source. This may be a data source, such as Windows or NetApp, an application, or even a cloud application. To begin, switch to the File Servers tab and click the Add button. You'll be prompted to fill in your data source's details.

Click here to find the instructions in Working with Monitored Data Sources for adding data sources for configuration specific to your platform. Next, you'll need to assign the monitored data source to the Collector added in the previous step. Once you click Install, you'll be returned to the File Servers tab, where you can follow the installation progress.

5. Review monitored data in the Varonis Web Interface

> Note: The data collected in Varonis is private; your data is accessible only to you.

Once the data source setup is complete, Varonis will start gathering events and data structure from the monitored data sources. This data will be sent from the Collector to the Varonis servers in the cloud. You can review our analysis of your data security in the Varonis Web Interface. When you open it, the Varonis Web Interface displays the Dashboards screen, showing you an analysis of the data gathered so far from the monitored data sources.

You can monitor additional data sources to get a more complete picture and better protection of your organization's data. You will need to purchase the relevant licenses. Then, just follow the steps above to enroll more data sources to monitor. If you're adding data sources in remote networks, it is recommended to add Collectors in close proximity to them; consult your Varonis account team on the recommended monitoring topology.

Additionally, you can remediate permission issues and risks using policies defined and implemented through the Varonis Web Interface, classify sensitive data using Data Classification Engine, and detect cybersecurity issues and vulnerabilities using the DatAlert Suite.

Now that you've learned how to deploy Varonis SaaS, let's do it! Before you begin, make sure you fulfill the Firewall, Proxy, and Certificate Requirements and Varonis SaaS Deployment Prerequisites.

2 REQUIREMENTS

Before you begin to deploy Varonis SaaS, verify you comply with our network and access requirements to ensure your system is secure and configured properly. For details, see Firewall, Proxy, and Certificate Requirements, Collector-to-Cloud Bandwidth Requirements, Varonis SaaS EDR/Antivirus Allow List, and Varonis SaaS Data Centers.

> Important: To receive your user credentials and log in to the system, verify emails from no-reply@varonis.io are not blocked or sent to your spam folder.

Also check out our deployment prerequisites.

Varonis SaaS Deployment Prerequisites

Varonis SaaS includes various requirements for its on-premises system components to ensure proper functioning.

> Important: To receive your user credentials and log in to the system, verify emails from no-reply@varonis.io are not blocked or sent to your spam folder.

Before installing a new Collector, and after fulfilling the below requirements to ensure that your environment is compliant, you must run the Varonis SaaS Prerequisite Checker tool within two weeks prior to the actual installation. The tool must run on your actual tenant URL without errors (warnings are allowed). For more information about the tool, see Prerequisite Checker tool.

Collector Requirements

- A minimum of 8 cores for data classification and 12 cores for data labeling
- Minimum Windows version - Windows Server 2016 Standard or Datacenter (x64)
- Server OS should be updated with the latest security updates and hotfixes
- .NET Framework - 4.7.2, 4.8, or 4.8.1
- .NET 8
- Microsoft Message Queuing (MSMQ) enabled
- PowerShell 5.1 or higher
- Minimum disk space required - 250GB
- Enabled services:
  - RemoteRegistry
  - LanmanServer
- Make sure that the Windows RPC dynamic port range is 49152 through 65535 for TCP and UDP.
  - To verify that the start port is 49152 and the number of ports is 16384, run the following commands:
    - `netsh int ipv4 show dynamicport tcp`
    - `netsh int ipv4 show dynamicport udp`
  - If the ranges aren't correct, run the following commands:
    - `netsh int ipv4 set dynamicport tcp start=49152 num=16384`

- `netsh int ipv4 set dynamicport udp start=49152 num=16384`

For more information, see this Microsoft article.

- Internet connectivity to all of the Varonis SaaS outbound targets, see Firewall, Proxy, and Certificate Requirements
- Windows proxy configured (WinINET and WinHTTP for current user and LocalSystem account) if required for internet connectivity, see Varonis SaaS Web Proxies - Additional Details
- At least one of the following TLS 1.2 ciphers must be enabled:
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Note: If you have third-party (non-Microsoft) security software installed on the Collector, contact Varonis Support for additional instructions.

Supported Browsers

The supported browser versions and screen resolutions for the Varonis Web Interface include:

- Google Chrome (recommended)
  - 78.x and higher
- Microsoft Edge
  - 79.x and higher
- Screen resolution
  - 1920 x 1080 (recommended)

As mentioned above, to help ensure that everything is in place, we recommend to run the Varonis SaaS Prerequisite Checker Tool and follow the tool results.

Monitored Data Source Requirements

For monitored data source requirements, see Working with Monitored Data Sources.

Varonis SaaS Prerequisite Checker Tool

The Prerequisite Checker tool helps you successfully prepare your environment for Varonis SaaS installation. It runs tests that verify whether your system meets all the requirements, and provides remediation steps for noncompliant prerequisites.

Running the Prerequisite Checker Tool

Run the Prerequisites Checker tool on each server that is designated for the Deployment Hub and Collectors. The tool examines the required hardware, software, configuration, connectivity, and sizing.

To run the Prerequisites Checker Tool:

1. Download the tool from the Varonis Community site:
   a. From the Manage menu, select My Downloads, or go to My Downloads.
   b. In the My Downloads page, locate the SaaS Prerequisites Checker Tool tile, and click its Download button.



2. Copy the ZIP file to the servers designated as Deployment Hub and Collectors, and extract the VaronisPrereqCheckerTool.zip file to the relevant folder.

   Note: To ensure the files are not blocked prior to extraction, right-click the ZIP file and select Unblock.

3. Double-click PrereqChecker.exe and follow the on-screen instructions, as described below.
4. Click I Agree to agree to the terms and conditions.

The tool's main menu is displayed.



5. Select your region and type your company name.
   Varonis SaaS cloud infrastructure and services are hosted in multiple regions. Select the most suitable region for your environment considering factors such as distance, latency, regulations and so on.
6. Select the components you want to check:
   - Standalone Collector (distributed deployment) - Select this option to verify the readiness of the servers that will host the Collectors.
     Application URL - If the tenant was created and the Web UI address is known, clear the I don't have an application URL checkbox, and type the Web UI name to complete the URL; otherwise, keep the I don't have an application URL checkbox selected.
   - Deployment Hub and Collector - Select this option to verify the readiness of the server that will host the Deployment Hub and Collectors.
     Application URL - If the tenant was created and the Web UI address is known, clear the I don't have an application URL checkbox, and type the Web UI name

to complete the URL; otherwise, keep the I don't have an application URL checkbox selected.

- Standalone Deployment Hub - Select this option to verify the readiness of the server that will host the Deployment Hub.
  - Application URL - If the tenant was created and the Web UI address is known, clear the I don't have an application URL checkbox, and type the Web UI name to complete the URL; otherwise, keep the I don't have an application URL checkbox selected.
  - Remote Collector machine hostname - Enter the name of the server where the Collectors are to be installed to enable communication with the Deployment Hub server and installation of the Collectors, and click Validate to validate that the server exists.
- Standalone Collector - Select this option to verify the readiness of the servers that will host the Collectors.
  - Application URL - If the tenant was created and the Web UI address is known, clear the I don't have an application URL checkbox, and type the Web UI name to complete the URL; otherwise, keep the I don't have an application URL checkbox selected.
  - Remote Deployment Hub machine hostname – Enter the name of the Deployment Hub server to enable communication with the Collectors and click Validate to validate that the server exists.

7. Click Next.



8. Select the monitored data sources you want to check:
   - Directory Services - Select this option to verify the readiness of the environment for monitoring directory services monitoring. Under Monitored domain controllers, define which domain controllers should be checked.
     - Select domain controllers – Use this option to select specific domain controllers to be checked. To make the Select domain controllers button available, clear the Check all domain DC servers and Include all trusted domains checkboxes; then click the Select domain controllers button. In the dialog box that opens, type the server's name and click Add for each server you want to be checked. The tool will first verify if the server exists and is managed in the local Active Directory and if so, will add the server to the list.

When you finish adding the required servers, list is done, click OK.



- Check all domain DC servers – Select this option to automatically check all domain controllers under the same forest.
- Include all trusted domains – Select this option to automatically include all child domains under the same forest.
- Use single credentials for all servers – Select this checkbox to use the same credentials for executing directory services prerequisite checks in all servers. Then select Logged-in user, or select Other user account and click Enter Credentials to enter the username and password of the required

account.



Note: When the Check all domain DC servers and Include all trusted domains checkboxes are selected, the logged-in user account is used for credentials.

- Windows - Select this option to verify the readiness for monitoring Windows file servers. Under Windows servers, define which Windows file servers should be checked.
  - Select Windows file servers – Use this option to select specific Windows file servers to be checked. Click the Select Windows file servers button, and in the dialog box that opens, type the server's name and click Add for each file server you want to be checked. The tool will first verify if the file server exists and is managed in the local Active Directory and if so, will add the server to

the list. When you finish adding the required servers, list is done, click OK.



- Use single credentials for all servers - Select this checkbox to use the same credentials for executing prerequisite checks in all Windows file servers. Then select Logged-in user, or select Other user account and click Enter

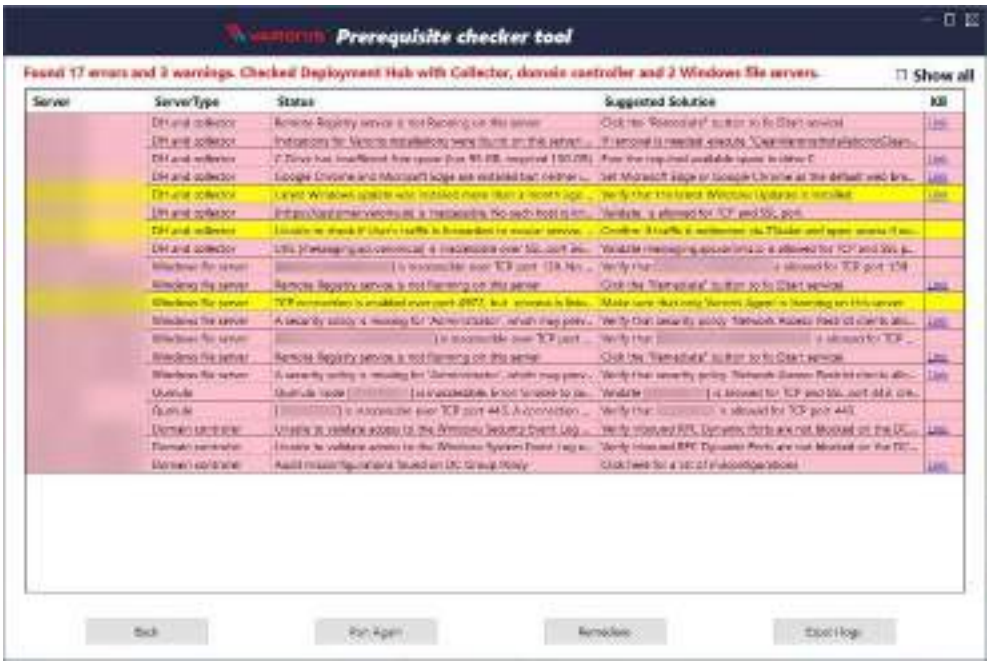
Credentials to enter the username and password of the required account.



- M365 - Select this checkbox to add the required checks if M365 data sources such as SharePoint Online, OneDrive or Exchange Online are to be monitored.
- Edge - Select this checkbox to add the required checks if an Edge component is to be installed.
- Data labeling - Select this checkbox to add the required checks if a data labeling component is to be installed.
- Qumulo - Select this checkbox to add the required checks if Qumulo data sources are to be monitored.
  - Cluster node IP - Type the IP address of the Qumulo cluster and click Enter Credentials to enter the username and password of the required account.
  - Middleware Name/IP - Type the name or IP address of the Qumulo Broker (middleware) server.

9. Click Next.

All defined prerequisite checks start running. When the runs are completed the tool's result window displays the noncompliant prerequisites.



10. Select the Show all checkbox to see all results including the compliant prerequisites (displayed in green rows).



11. The window features several buttons that you can use:
    - Back – Go back to previous window. This button is unavailable when the tool is running the checks.
    - Run Again – Run the same checks again for the selected component type.
    - Remediate – Trigger the prerequisite checker tool to remediate the issues that have `Click Remediate` in their Action column.
    - Export Logs – Export logs and summary reports to a zip file.

      Note: The tool's log is stored in the Logs folder. Summary reports are HTML-based reports, which summarize every set of checks including all statuses and exceptions, and are generated after every run of the tool.

12. Proceed as follows:
    - If the results display all prerequisites as compliant, proceed with Installing the Varonis Deployment Hub.

- If the results display noncompliant prerequisites, the issues that include `Click Remediate` in their Action column can be remediated by the Prerequisite checker tool by clicking the Remediate button at the bottom of the results window. Other issues will need to be remediated manually. Click the Remediate button and when the tool completes to remediate the relevant issues, it will run the checks again automatically.

  Note: If the results display indications of Varonis items from previous installations and a recommendation to clean them, run the Varonis Installation Cleaner.

Now that you've fulfilled the requirements, let's install the Collector.

Running the Varonis Installation Cleaner

The Varonis Installation Cleaner tool is intended to run on a clean environment that may have items remaining from previous Varonis installations. Do not run this tool on a server that has an existing Varonis installation.

1. In the VaronisPrereqCheckerTool folder, open the CleanVaronisInstallations folder and double-click Cleaner.exe.
   The tool starts searching for Varonis installation items.
2. If Varonis installation items are found, review the list of remaining items in the displayed message, and click Yes to approve the cleanup.
   The removal process starts running. Logs are displayed in the tool window and are saved in the CleanVaronisInstallations\Logs folder.

   Once the removal process is completed, the tool looks for any remaining items again.
3. If Varonis installation items are found, a message is displayed listing the items. In the message, click OK. Then, restart the server and run the tool again.
4. If the server restart did not remove the remaining items, remove them manually.

Data Labeling Prerequisites

The following prerequisites are required for Varonis data labeling.

License Prerequisites

A Microsoft 365 (formerly called Office 365 or O365) tenant license, of type E3/A3/G3, and above

Important: A single E3/P1 license is sufficient for managing labels in Azure, publishing a labeling policy, and providing Azure admin consent to the labeling application for automatically labeling files via the MIP SDK.

Note: If a file is not protected, a Microsoft license is not required to access it. If labels with encryption are applied to a file, you must have at least one of the Microsoft license types mentioned above to access the file.

Hardware and Setup Requirements

- A minimum of 12 cores in the Collector.
- Performing one of the following actions:
  - Connect Collectors to the internet.
  - Use a web proxy to have a single point of connection to the internet.

    Note: If you use a web proxy that requires authentication, you must configure the proxy to use integrated Windows authentication with the user's Active Directory logon credentials.

  - Provide all Collectors with access to the following domains (proxy include list) over HTTPS (TCP 443): *.protection.outlook.com, *.aadrm.com, login.microsoftonline.com, aadcdn.msftauth.net, graph.microsoft.com, portal.azure.com, *substrate.office.com, *.events.data.microsoft.com

    For GCCH tenants only, access to these domains is required: login.microsoftonline.com, login.microsoftonline.us, aadcdn.msauth.net, graph.microsoft.us, portal.azure.us, *.protection.office365.us, *.aadrm.us, *substrate.office365.us, *.events.data.microsoft.com

    Note: Follow the Microsoft guidelines in 'Azure Information Protection requirements' on how to set firewalls and network infrastructure.

Varonis User Configurations

To perform labeling, you can either:

- Use the existing Varonis Service Account with additional permissions to modify, remove, and create files
- Create a domain user with the following permissions:

- Read all files (administrator or backup operator and power user)
- Modify, create, and remove files

The minimum permissions/roles needed for labeling in NetApp CM servers:

- Within the NetApp command line interface:
  - Backup Operator and Power User roles assigned to the service account in use
  - The service account needs access-control share to have Full Control permissions for the required user.
- On the Windows side, confirm the NTFS permissions of the share allow the service account modify, create, and remove files.

Microsoft User Configurations for Unified Labeling

A Microsoft 365 User with an E3 license or higher is required for your organization to manage the sensitivity labels in Microsoft Information Protection. Such user should have (at least) one of the following roles - Compliance administrator, Compliance data administrator, or Security administrator.

Data Labeling Application Permissions

When configuring data labeling, an application is created to support the labeling functionality. The application needs to read labeling policies, read protected content, and create protected content.

These permissions are mapped to the following Microsoft Azure application permissions:

- UnifiedPolicy.Tenant.Read is required to download unified labeling policies from a tenant:
  - Mandatory permission
  - Without this permission the labeling functionality will not work
- Content.SuperUser is required to decrypt all content protected for a specific tenant:
  - Not a mandatory permission
  - Without this permission protected content with restricted user/group permissions will not be classified and will not be relabled

> Note: If the user does not require classification of protected (encrypted) content, the Content.SuperUser permission can be removed by the Entra ID administrator.

- Content.Writer is required to list templates and encrypt content in order to create protected content:
  - Not a mandatory permission
  - Without this permission, protected content (labeling content with encryption) cannot be created

> Note: If the user does not need to create protected (encrypted) content, the Content.Writer permission can be removed by the Entra ID administrator.

Microsoft Azure permissions can be updated in the API permissions screen in the Microsoft Azure portal.

Labels and Policies Configuration and Migration in Microsoft Azure

Perform one of the following prerequisites:

- If you have any existing labeling policies defined by Azure Information Protection Center–migrate them to the Office 365 Security & Compliance Center.
- If you do not have existing labels and policies in Azure–create, configure and publish labels and policies (at least one label and policy) by following the Microsoft 365 Compliance guidelines.

For labeling best practices, see this article.

Privacy Automation Prerequisites

The following prerequisites are required for Varonis Privacy Automation.
Before installing Privacy Automation, contact your Varonis representative to perform a sizing assessment. This process is critical for providing the suitable environment for your needs.

We also provide a Prerequisite Checker tool. We recommend to run this tool after fulfilling the below requirements to ensure that your environment is compliant.

General Requirements

- The Collector version must be 9.0.399 or higher.

User Requirements

- The Privacy Automation user must be a domain user.

Sync Unit Requirements

- The Sync Unit folder must be a shared network folder with share permissions.
- “Full control” access must be granted to the Privacy Automation user.
- All Varonis Collectors and Privacy Automation Servers should be able to access this shared folder.

Server Requirements

Privacy Automation installation requires a dedicated server (a “search node” server):

- Minimum Windows version - Windows Server 2016 Standard or Datacenter (x64)
- Server operating system updated with the latest security updates and hotfixes
- .NET Framework - 4.7.2, 4.8, or 4.8.1
- Microsoft Message Queuing (MSMQ) enabled
- PowerShell 5.1 or higher
- Java versions between 17.0 to 19.9
- Environment variables:
  - Add the "JAVA_HOME" environment variable that will hold the Java install location
  - Java bin location in the "Path" environment variable
- Minimum disk space (according to the sizing process):
  - Under 50TB data: 8 core/32GB RAM/1.5TB disk
  - 50TB to 100TB data: 8 core/64GB RAM/3TB disk
- Enabled services:
  - LanmanServer
- Firewall requirements: Make sure all the relevant firewall rules described in Firewall, Proxy, and Certificate Requirements are configured.
- Windows RPC dynamic port range 49152 through 65535 for TCP and UDP:

- To verify that the start port is 49152 and the number of ports is 16384, run the following commands:
  - `netsh int ipv4 show dynamicport tcp`
  - `netsh int ipv4 show dynamicport udp`
- If the ranges aren't correct, run the following commands:
  - `netsh int ipv4 set dynamicport tcp start=49152 num=16384`
  - `netsh int ipv4 set dynamicport udp start=49152 num=16384`

> Note: For more information, refer to the Microsoft article The default dynamic port range for TCP/IP has changed since Windows Vista and in Windows Server 2008

- For details about Varonis Certificates, see Varonis SaaS Certificates - Additional Details.

> Note: If you have third-party (non-Microsoft) security software installed on the Collector, see Varonis SaaS Deployment Prerequisites.

Supported Browsers and Screen Resolution

- Google Chrome (recommended) - 78.x and higher
- Microsoft Edge - 79.x and higher
- Screen resolution - 1920 x 1080 (recommended)

File Types Supported For Classification

The following file types can be classified by Varonis:

> Note: PDF and image files are supported for Optical Character Recognition (OCR).

Note: Image file types (bmp, jpg, jpeg, png, tif, tiff, gif, pjpg, ptif, ppng, pbmp, pgif, pjpeg, and ptiff) are cleared by default. To include any of them in the scan, select the required file type in the File Types tab. If image file types are selected, the scan will take longer to complete since more files will be scanned and also because image files are processed through Optical Character Recognition (OCR). Processing through OCR takes significantly more time to process compared to regular document text extraction.

Note: Microsoft owner files are not scanned by Varonis. A Microsoft owner file is a temporary file created when you open an Office file, and deleted when you save your file and exit the Office application. The owner file contains your logon name and lets Office know that you have this file open so that other users trying to open the file will not be able to do so until you close the file. A Microsoft owner file has a prefix of a tilde (~) followed by a dollar sign ($) and an Office file extension, for example ~$test.doc. Since such files are temporary files that Office will eventually delete, Varonis does not scan them.

Note: Symbolic links are treated as files and are detected according to their file extension.

File Extension	Description
.vsd	Microsoft Visio Drawing
.vsdx	Microsoft Visio Open XML Drawing
.vsdm	Microsoft Visio Macro-Enabled-Drawing
.vssx	Microsoft Visio Stencil Adobe Acrobat
.vssm	Microsoft Visio Macro-Enabled-Stencil
.vss	Microsoft Visio Smart Shapes
.vst	Microsoft Visio Binary Document

File Extension	Description
.vstx	Microsoft Visio Template
.vstm	Microsoft Visio Macro-Enabled Template
.one	Microsoft OneNote
.onepkg	Microsoft OneNote Package
.dwg	AutoCad Drawing File
.dxf	AutoCad Drawing Exchange File
.dotx	Microsoft Word Open XML Template
.dot	Microsoft Word Template
.docm	Microsoft Word Open XML Macro-Enabled Document
.docx	Microsoft Word Open XML Document
.doc	Microsoft Word Document
.rtf	Rich Text Format File
.ptxt	Text File protected by Microsoft Information Protection (MIP) using Microsoft Rights Management Service (RMS)
.pxml	XML File protected by Microsoft Information Protection (MIP) using

File Extension	Description
	Microsoft Rights Management Service (RMS)
.pjpg	Joint Photographic Group File protected by Microsoft Information Protection (MIP) using Microsoft Rights Management Service (RMS)
.pjpeg	Joint Photographic Experts Group File protected by Microsoft Information Protection (MIP) using Microsoft Rights Management Service (RMS)
.ppng	Portable Network Graphics File protected by Microsoft Information Protection (MIP) using Microsoft Rights Management Service (RMS)
.ptif	Tagged Image File protected by Microsoft Information Protection (MIP) using Microsoft Rights Management Service (RMS)
.ptiff	Tagged Image File Format protected by Microsoft Information Protection (MIP) using Microsoft Rights Management Service (RMS)
.pbmp	Bitmap Image File protected by Microsoft Information Protection (MIP) using Microsoft Rights Management Service (RMS)
.pgif	Graphics Interchange Format protected by Microsoft Information Protection (MIP) using Microsoft Rights Management Service (RMS)

File Extension	Description
.pot	Microsoft PowerPoint Template
.potx	Microsoft PowerPoint Open XML Template
.pps	Microsoft PowerPoint Slide Show
.ppsx	Microsoft PowerPoint Open XML Show
.pptx	Microsoft PowerPoint Open XML Presentation
.ppt	Microsoft PowerPoint Presentation
.xlsb	Microsoft Excel Binary Spreadsheet
.xlsm	Microsoft Excel Macro-Enabled Spreadsheet
.xltx	Microsoft Excel Open XML Spreadsheet Template
.xlt	Microsoft Excel Spreadsheet Template
.xls	Microsoft Excel Spreadsheet
.xlsx	Microsoft Excel Open XML Spreadsheet
.csv	Comma Separated Values File
.pdf	Portable Document Format File

File Extension	Description
.txt	Text File
.xml	XML File
.sub	Subtitle Text File
.srt	Subtitle Text File
.sbv	YouTube Video Subtitles or Captions File
.vtt	Web Video Text Tracks and Transcripts File
.log	Log File
.sxw	OpenOffice Writer 1.x Document
.stw	OpenOffice Writer 1.x Document Template
.odt	OpenOffice Writer 2.x (and above) Document
.ott	OpenOffice Writer 2.x (and above) Document Template
.sxc	OpenOffice Calc 1.0 Spreadsheet
.stc	OpenOffice Calc 1.0 Spreadsheet Template
.ods	OpenOffice Writer 2.x (and above) Spreadsheet

File Extension	Description
.ots	OpenOffice Writer 2.x (and above) Spreadsheet Template
.sxi	OpenOffice Impress 1.x Presentation
.sti	OpenOffice Impress 1.x Presentation Template
.odp	OpenOffice Impress 2.x (and above) Presentation
.otp	OpenOffice Impress 2.x (and above) Presentation Template
.mdb	Microsoft Access (95-2003) Database
.accdb	Microsoft Access (2007 and above) Database
.eml	E-mail Message File Note: Including attachments
.msg	Message Format File Note: Including attachments
.jpg	Joint Photographic Group File
.jpeg	Joint Photographic Experts Group File
.bmp	Bitmap Image File

File Extension	Description
.tif	Tagged Image File
.tiff	Tagged Image File Format
.gif	Graphics Interchange Format
.png	Portable Network Graphics File
.rar	WinRAR Compressed Archive
.zip	Zipped File

File Types Supported For Data Labeling

The following file types are supported for data labeling:

Application	Supported File Type
Adobe Acrobat	.pdf
Microsoft Visio	.vsdx .vsdm .vssx .vssm .vstx .vstm
Microsoft Word	.docm, .dotx, .dot, .docx, .doc
Microsoft Excel	.xlsb, .xlsm, .xltx, .xlt, .xls, .xlsx
Microsoft PowerPoint	.pot, .potx, .pps, .ppsx, .pptx, .ppt

3

Installing A Collector

To start monitoring the on-premises environment, at least one Collector is required. You download and run an installer on the dedicated server for the Collector. Then you activate the Collector in the Varonis Web Interface. You can deploy and activate multiple Collectors at the same time. You can also use third-party distribution tools to install multiple Collectors automatically.

Install a Collector

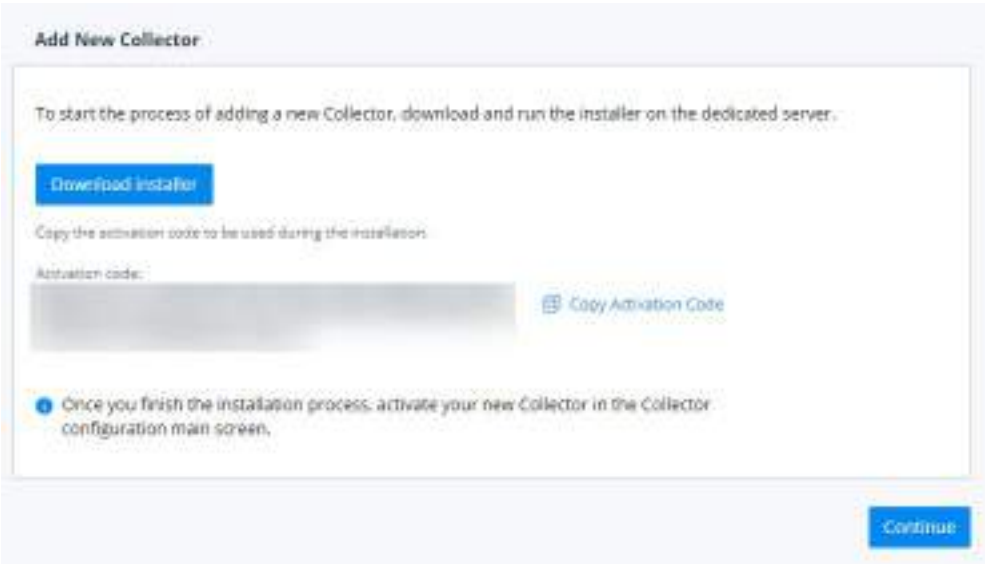
Before you begin to install, upgrade, or configure a Collector, you need to ensure several prerequisites have been met.

> Important: After you install a Collector, you need to install a domain. Afterward, you can add data sources.

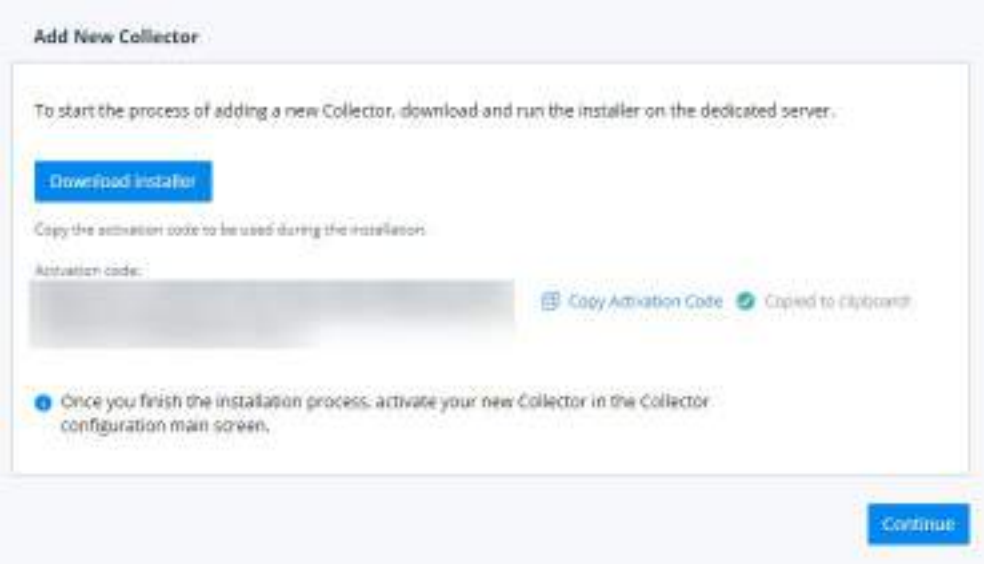
> Note: The Collector is installed on drive C.

Follow the steps below to perform a clean installation of a Collector. For instructions for upgrading an existing Collector, click here.

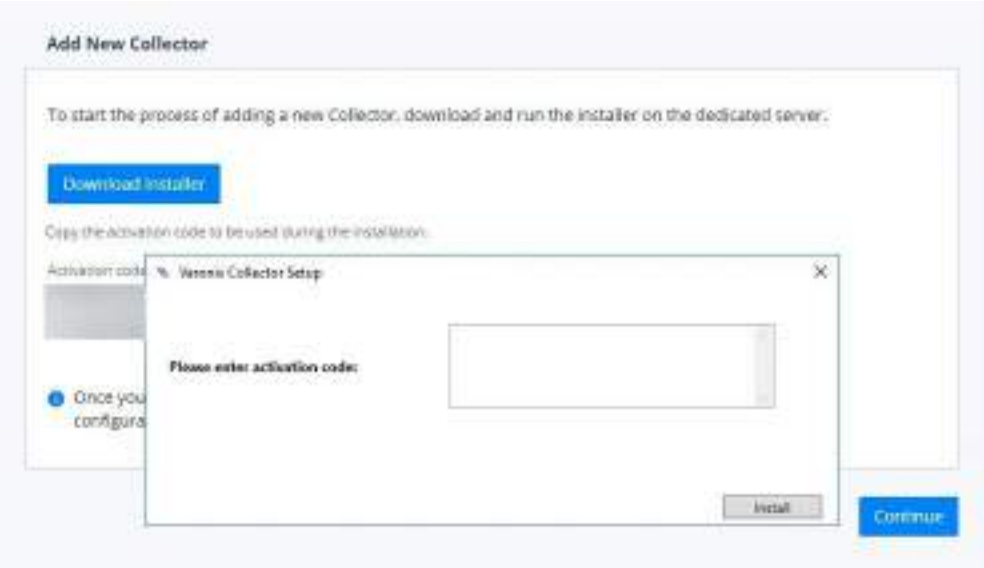
1. In the Varonis Web Interface, from the  Configuration menu, select System Topology.
2. On the Collectors tab, click + New Collector.
   The Add New Collector dialog box is displayed.



3. In the Add New Collector dialog box, click Copy Activation Code to copy the code to be used during the installation, then click Download installer.

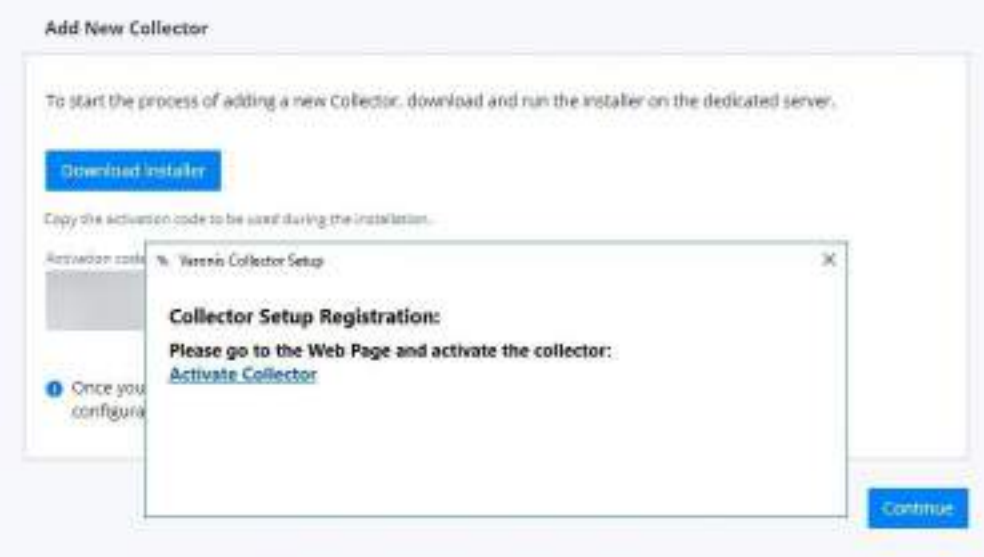


4. After the download has completed, copy the VaronisCollectorSetup.exe file to the server where the Collector is to be installed.
5. Double-click the VaronisCollectorSetup.exe file you downloaded.
   The Varonis Installer Setup wizard is displayed.



6. Paste the activation code you copied, and click Install.

When the installation is completed, the Collector Setup Registration dialog box is displayed.



7. Click the Activate Collector link.
   The Varonis Web Interface System Topology screen opens and the Collectors tab is displayed showing the newly installed Collector.
8. In the row of the newly installed Collector, from the Actions menu, select Activate.



The activation process starts. After it is completed, the Collector is displayed as Active.
After the Collector is activated, you can proceed to configure a certificate for it, if required.

> Note: To enable the Collector for network devices (Edge), select the Collector, and from its options menu, select Edit. Then, on the General tab in the right pane, select the Enable for Edge checkbox, and click Apply. For more information, click here.

Repair a Collector

You can repair a Collector when it is not functioning properly. The repairing process reinstalls the Collector, keeping its current configuration.

1. Select the row of the Collector you want to repair.
2. From the Actions menu, select Repair.
   The repairing process takes several minutes to complete. You can follow its progress in the Status column.

Remove a Collector

You cannot remove a Collector that is involved in a process or is monitoring any data sources or domains.

1. Select the row of the Collector you want to remove.
2. From the Actions menu, select Remove.
3. In the confirmation message that opens, click Yes.
   The status in the Status column changes to Removing until the Collector is removed.

Add a Certificate for a Collector

This topic describes adding a certificate to Collectors managed in the Varonis Web Interface.

> Important: You must add a certificate for the Collectors used for monitoring Nasuni, Panzura, Nutanix, Cohesity, CTERA, and Qumulo data sources. We recommend that you use a purchased certificate signed by an enterprise certificate authority (CA) rather than creating a self-signed certificate.

1. In the Varonis Web Interface, from the  Configuration menu, select System Topology.
2. On the Collectors tab, select the row of the Collector to which you want to add a certificate, and from its options menu, select Edit.

The Collector Settings pane is displayed.



3. On the Certificates tab, from the Select Certificate Source list, choose an option:
   - Certificate Store (recommended) - Select this option to use a certificate issued by an enterprise certificate authority.
     A list of available certificates is displayed. Select the required certificate.

     Make sure you've uploaded a valid CA certificate to the certificate store on the Collector. See Requirements for a Certificate Issued by an Enterprise Certificate Authority.
   - Self-signed Certificate - Use this option to create and use a new self-signed certificate.
4. Click Apply.
   The certificate is assigned to the Collector and its name and expiration date are displayed on the Certificates tab.
5. Close the Collector Settings pane.
   The Certificate column of the Collector to which you added the certificate, displays Active, and when you hover over it, the certificate name and its expiration date are displayed.



Replace a Certificate

> Important: Certificates are supported up until their defined expiration date. To avoid expiration, make sure to renew the certificate periodically and replace it in the Varonis Web Interface to keep it valid. Otherwise, Varonis will stop monitoring events for all the data sources that require the certificate and are deployed on this Collector.

When replacing a CA certificate, first make sure you've uploaded a valid CA certificate to the certificate store on the Collector.

1. Select the row of the Collector whose certificate you want to replace, and from its options menu, select Edit.
   The Collector Settings pane is displayed.
2. In the Collector settings pane, from the options menu, select Edit and continue to select a valid certificate from the Certificate Store or a new self-signed certificate.



Remove a Certificate

You can remove (unassign) a certificate from any Collector that is not used for monitoring a data source that requires the certificate.

1. Select the row of the Collector whose certificate you want to remove, and from its options menu, select Edit.
   The Collector Settings pane is displayed.

2. In the Collector settings pane, from the options menu, select Remove.



Now that you've installed a Collector, you need to associate it with an Active Directory data source.

Requirements for a Certificate Issued by an Enterprise Certificate Authority

When adding a certificate to your Collector, make sure that the certificate complies with the requirements below to pass validation by Varonis. CA-generated certificates must contain a full certificate chain, including Root CA and intermediate CA certificates. The certificate should include a private key.

Field	Description	Valid Values
Valid-From:	From when the certificate is valid	Any time in the past
Valid-To:	When the certificate will expire	At least 3 months, up to 2 years
Signature Algorithm	Type of signature used	rsa_pkcs1_sha256 sha-256WithRSAEncryption OID: 1.2.840.113549.1.1.11 rsa_pkcs1_sha384 sha-384WithRSAEncryption OID: 1.2.840.113549.1.1.12 rsa_pkcs1_sha512 sha-512WithRSAEncry

		ption OID: 1.2.840.113549.1.1.13 ecdsa_secp256r1_sha256 ecdsa-with-sha256 OID: 1.2.840.10045.4.3.2 ecdsa_secp384r1_sha384 ecdsa-with-sha384 OID: 1.2.840.10045.4.3.3 ecdsa_secp521r1_sha512 ecdsa-with-sha512 OID: 1.2.840.10045.4.3.4
Public key type	Private/public key type	RSA (rsaEncryption) = The length of the modulus n >= 2048-bit DSA (id-dsa) = The DSA domain parameter lengths: (2048, 224), (2048, 256) or (3072, 256) EC (id-ecPublicKey) = The length of the EC domain parameter n >= 224-bit
Key-Usage	Purpose of the certificate	Digital signature and certificate signing
Extended-Key-Usage	Purpose of the certificate continuation	Server authentication
Subject name	Name of the Collector server	Fully qualified domain name (FQDN) of the Collector server

Subject Alternative Name (SAN)	Alternative name	Optional - Collector IP

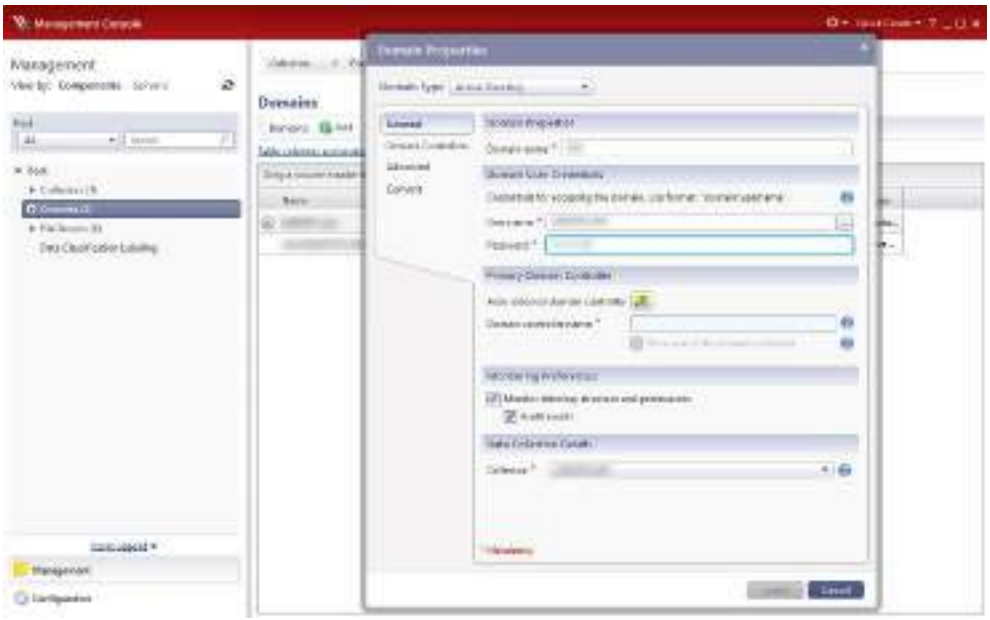
Adding An Active Directory Data Source

After the required Collectors are installed, you must add an Active Directory (AD) data source; it is required to resolve the AD users and groups who have permissions to the data stored in other monitored data sources. For Entra ID instructions, see Entra ID Data Sources.

> Note: Each AD data source represents a monitored AD domain. In some cases, the Varonis UI displays the term Domain instead of Data Source. To monitor multiple AD domains, add an AD data source per AD domain.

To add and configure an AD data source:

1. In the Management Console, select Management > Components > Root > Domains, and on the toolbar, click Add.
   The Domain Properties window is displayed, showing the General pane.



2. Select Active Directory as the Domain Type if it is not already selected.
3. In the Domain Properties area, set the following parameters:
   - Domain name - Type the name of the AD domain you want to monitor.

     > Note:

- This option is read-only if you are editing an existing AD data source.

4. Specify the Domain User Credentials:
   - User name - Set the name of the user that can access the AD domain. Use the format domain\username.This is the VaronisAdmin user described in Required User Accounts in AD Requirements.

     Note:
     - To monitor accounts, the user must be a member of the Domain Users security group.
     - To monitor directory structure and permissions, the user must have permission to read all OUs and the system access control list (SACL), or be a member of the Account Operators security group.

   - Password - Type the user's password.
5. Set the Primary Domain Controller to be used for monitoring the domain's accounts, directory structure, and permissions:
   - Auto-discover domain controller - Click the button to automatically discover the domain controller.
   - Domain controller name - If you didn't click the Auto-discover domain controller button, type the AD domain controller server name. Alternatively, enter the user credentials described above, then fill in any computer name in the AD domain and click the Auto-discover domain controller button to auto-discover the domain controller.
   - Force use of this domain controller - Select this checkbox to force Varonis to connect only to the domain controller specified above. When selected, only this domain controller will be used to monitor the domain's accounts, directory structure, and permissions. If the connection to the primary domain controller fails, the respective data will not be monitored. If cleared, Varonis will try to connect to other available DCs.
6. In the Monitoring Preferences area, choose whether to monitor the AD structure and permissions and audit AD events (these are selected by default for licensed users, otherwise they are unselected). Set the following options:
   - Monitor directory structure and permissions - Select this checkbox to enable monitoring the AD structure and permissions.
   - Audit Events - Select this checkbox to audit AD events. This option is only available if the Monitor directory structure and permissions option is selected. Event auditing can be enabled only if DCs are configured, so make sure to configure at least one DC in the Domain Controllers tab.

7. In the Data Collection Details area, select the Collector from the dropdown list.
   Now that you've completed the general settings, you can proceed to configure configure the domain controllers and AD auditing (if licensed). For instructions, see Configure domain controllers in Adding an AD Data Source and Event Auditing Requirements in AD Requirements.

After configuration is complete, click Install to add the AD data source.

A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the Domains pane. When the installation completes, the status shows "Installed 100%".

Now that you've added an AD data source, you can proceed to add additional data sources for monitoring.

Adding Monitored Data Sources

Now that you have installed the Varonis Collector and an Active Directory (AD) data source, you can install and configure the data sources (file servers) that the Collector monitors, per machine, and define the related shares.

1. Set common data source parameters

1. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.
   The Resource Wizard is opened to the Common pane, where you can specify the data source and set the relevant parameters. The left menu options and settings

vary per specified data source.



2. In the Common pane, set the following parameters:
   a. Resource Details - Specify the data source name.
   b. Data Collection Details - Select the relevant Collector from the dropdown list.
   c. FileWalk Credentials - Enter the credentials for running directory structure monitoring. File System operations include directory structure monitoring, event auditing (if set) and account enumeration on local accounts (if set).

      Important: You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.

   d. Resource Type - Select the data source type from the dropdown list.
      - Connect and verify - Click this link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

Note:

- The Connect and verify link is displayed only when all relevant data is entered.
- A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

e. Monitored Shares - Select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source installed and share detection is completed.

- Automatically monitor detected shares - Select this option to automate monitoring for all detected shares. Share monitoring will automatically start after the data source installation is completed. Varonis will monitor all shares that aren't marked as "ignored".
- Monitor selected shares - This option is selected by default. You can manually select the shares to be monitored only after the data source is installed and share detection is completed. You'll need to open the Edit window for the installed data source and select the shares. For more information, see Post-installation share detection and registration.

Once the above settings are configured, you can proceed to review and adjust configuration settings.

2. Review and adjust configuration settings

1. On the left menu, click Configuration and confirm the information.
   The general configuration settings are displayed.
2. In the Local Accounts area, review the options:
   - Collect information regarding local accounts from this file server - Select this checkbox to collect user accounts from this file system.
3. In the FileWalk Settings area, review the options:
   - Identify actual unique folders and file system inconsistencies - Select this checkbox (if it not already selected) to detect broken permissions in NTFS file systems.
   - FileWalk Method - Select the method to be used for directory structure monitoring. If you change the method, you will need to rescan the shares.
     - Select the supported option per platform:

- CIFS - Uses the Common Internet File System (CIFS) protocol. The Varonis FileWalk agent need not be installed if CIFS is selected, since it uses the UNC path.
- NFS - (Relevant for Unix) Uses the Network File System (NFS) protocol.

- Varonis - A method of running directory structure monitoring through the agent. This method only works if the agent is installed.
  - An error will occur if this option is selected but there is no agent installed.
  - Cluster installation - If the Varonis FileWalk method is selected, the agent must be installed on all nodes.

4. In the Event Auditing Parameters area, review the options:

- Port in use - The port through which the Varonis agent on the data source communicates with the Collector.
- Filter out false "File Opened" events - Open events may be triggered unintentionally for a variety of reasons, resulting in inaccurate analysis of file system access. Select this option to filter such unintentional Open events and gather Open events only if enough file content is actually read. Small files and certain operations may still trigger Read events.
- Collect Access Denied events - Select this checkbox to audit events in which an attempt was made to access an entity by a user with insufficient credentials.
  - Include denied attempts to open folders - Select if preferred.

    CAUTION: Selecting this option may result in the creation of a large number of false access denied events.

Note:
Servers may have duplicate SIDs. This is common when the machine you are adding has been cloned from another machine and was not system-prepared (via the `Sysprep` command) prior to deployment. It might have been cloned from a machine already being monitored, or perhaps both servers were cloned from an original one and neither of them was system-prepared.

You can add the data source with the duplicated SID. You will be able to audit events and crawl the server for directory structure and permissions. However, you cannot collect local account information on any machines that have matching SIDs in Varonis.

By default, the option to Collect information regarding local accounts from this file server will b be cleared if there is already a machine with that SID being monitored; when two machines have duplicate SIDs, there is no way for Varonis to identify the machine from which those local accounts came.

The duplicate machine will have a fake SID entry in the Varonis Domain database. It is possible to switch which machine has the fake entry and the real entry by enabling advanced features in the Management Console. Contact Varonis Support for assistance.

3. Install the data source

After configuration is complete, click Install to install the data source.

A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the File Servers pane. When the installation completes, the status shows "Installed 100%".

4. Post-installation share detection and registration

After the data source installation and share detection are completed, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. The following procedure describes the manual registration and automatic share detection flows.

Important: If after the data source is installed, share detection fails for any reason, the Share Detection Status column will remain "In Progress" until the issue is fixed, and share detection completes successfully at least once.

After the data source is installed, the Shares pane is enabled, and you can view the share settings.

1. On the left menu, click Shares.
   The share settings are displayed. The pane's heading indicates the option you selected when adding a data source.
2. Do one of the following:
   - If you chose to monitor selected shares, in the Available Shares area, select the required shares and click the down arrow. The selected shares are moved to the Registered Shares area. (The registered shares list is empty until you make your selections.)
   - If you chose to automatically monitor detected shares, Varonis will monitor all shares that aren't marked as "ignored". The automated share detection runs every few hours. The Registered Shares area is autopopulated with the shares to be monitored.
3. For each share, review and set the following information as required:

- Ignore Detection - Select the shares to be ignored (and not be the subject of automatic detection and notifications) by the data source monitor.
- Events - Select this checkbox to audit events for the share.
- Crawl - To enable or disable monitoring for the share, in the Crawl column, select the relevant option.

  Note: You can also right-click the grid and select the required options for event auditing and crawling.

4. In the Additional Share Settings area, review the options:
   - Remove deleted shares - Select this checkbox to remove deleted shares. Shares that were deleted from the data source will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the data source is unavailable, the shares will not be removed.
   - Enable event auditing - Select this checkbox to audit events from all shares added from this data source.

   After share detection and registration are completed, the status and number of registered volumes are respectively displayed in the Share Detection Status and Registered Shares columns in the File Servers pane.

Now that you've added your monitored data sources, it's time to set up federated authentication.

Configuring Federated Authentication (SSO)

It's a simple process to set up single sign-on for Varonis SaaS through federated authentication with your organization’s Active Directory.

Note: If the steps below are not completed accurately, users may experience SSO 400 errors during authentication.

Federation Flow

The federation flow always starts with the user. The browser (or Management Console) is redirected among multiple URLs to complete the login flow.
1. The user accesses the tenant.

2 & 3. The user is redirected to My Varonis.

4 & 5. The user is redirected to Varonis Okta.

6. The user is redirected to their identity provider (IdP).

7. The user enters their credentials and meets other security requirements (multifactor authentication, IP restrictions, etc.).

8 & 9. The user is now authenticated and is redirected back to the tenant.

Prerequisites

Varonis supports SAML-based identity providers (IdP).

> Note: Varonis supports only service provider-initiated SSO, not IdP-initiated SSO. With IdP-initiated SSO, the user attempts to access Varonis through the IdP's application portal or page. Since this is not supported, users may only navigate to Varonis through the address bar.

The IdP must be configured before you begin configuring federation, so that you can have the following ready:

- The IdP's Login URL
- The IdP's Issuer Identifier
- The IdP's Signing Certificate

Varonis supports all SAML-based IdPs. If you use an IdP for which we do not provide instructions, consult the IdP's documentation.

The following claims must be configured for any IdP you use:

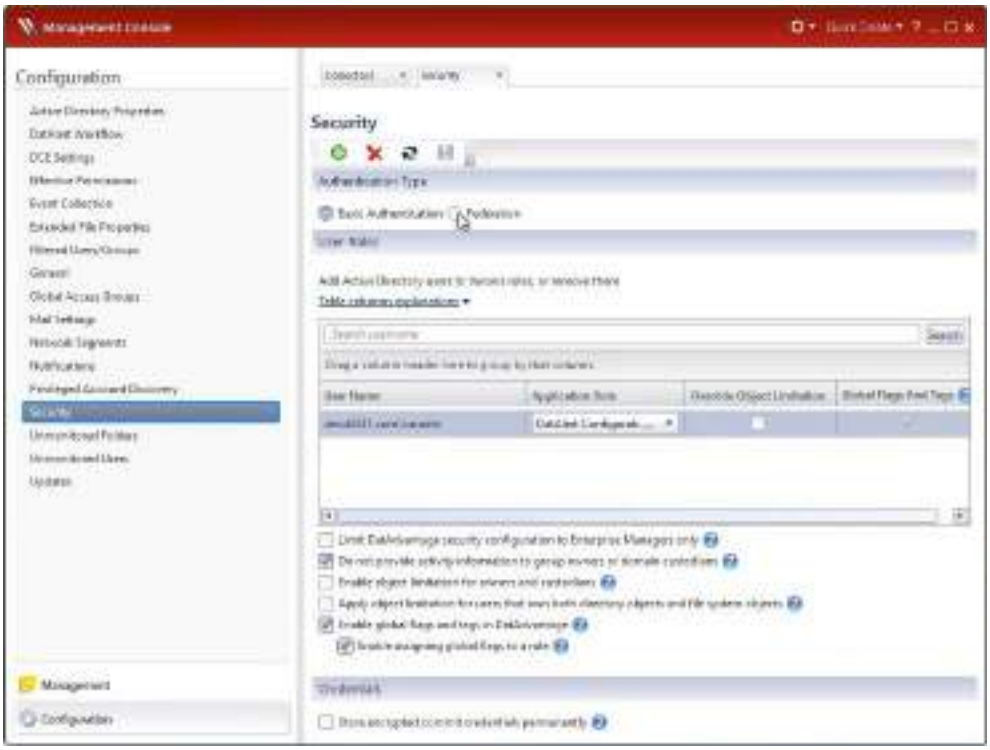
- email
- firstname
- lastname
- username
- Unique User Identifier
- varonisUserId

> Note: It is recommended to log in to Varonis SaaS using multifactor authentication (MFA). To enable MFA, consult your identity provider's settings.

Open the Federation Configuration Window in the Management Console

1. Log in to the Varonis Management Console with the Varonis SaaS user.
2. From the menu in the left pane, select Configuration > Security.

3. In the Authentication Type section, select Federation.

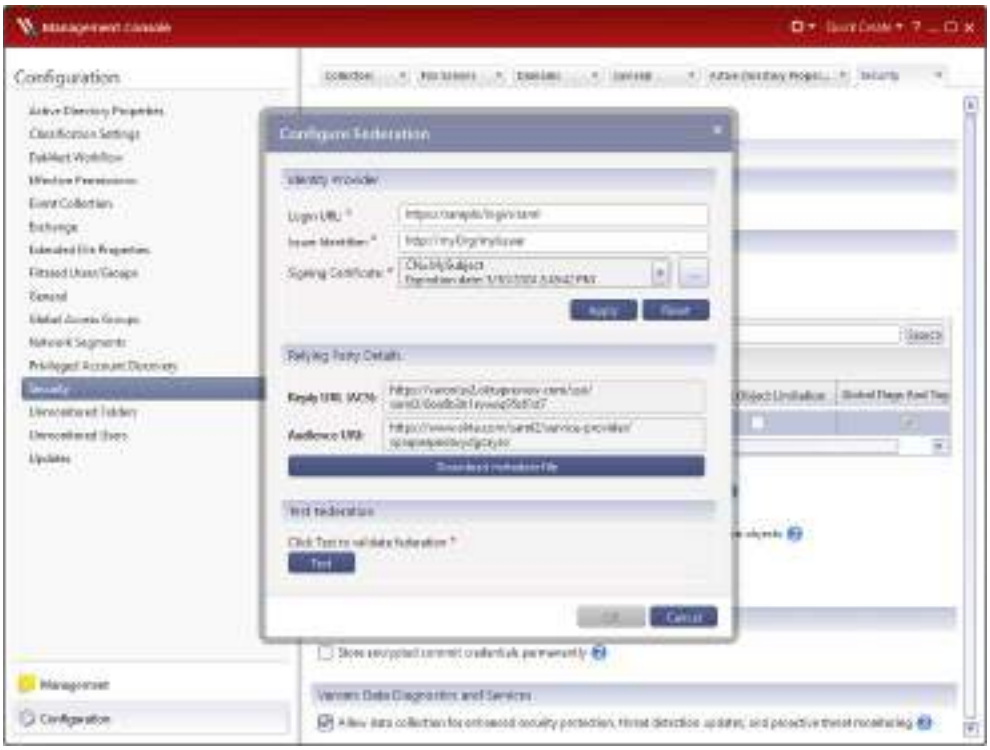


The Configure Federation dialog box is displayed.

Set the IdP's Configuration to Federation

Note: While we demonstrate configuration of AD FS and Entra ID, Varonis supports all SAML-based IdPs.

1. In the Configure Federation dialog box, set the IdP's configuration parameters and signing certificate.
   - Login URL. Example: https://devd4531dc.devd4531.com/adfs/ls
   - Issuer Identifier. Example: http://devd4531dc.devd4531.com/adfs/services/trust
   - Signing Certificate - a Base-64 encoded PEM certificate
2. Click Apply and see the Relying Party details.



Set the New Relying Trust in the IdP

Now set the new relying trust in the IdP. See the relevant topic below.

- Using Entra ID for the New Relying Trust
- Using Active Directory Federation Services (AD FS) for the New Relying Trust
- Using Okta for the New Relying Trust

If you are using an IdP that is not listed above, consult its documentation for instructions. You will need to map the following claims:

- firstname
- lastname
- username
- email
- Unique User Identifier (Name ID) - This must be identical to username.
- varonisUserId - If you are using data access governance, this additional claim is required for federated authentication.

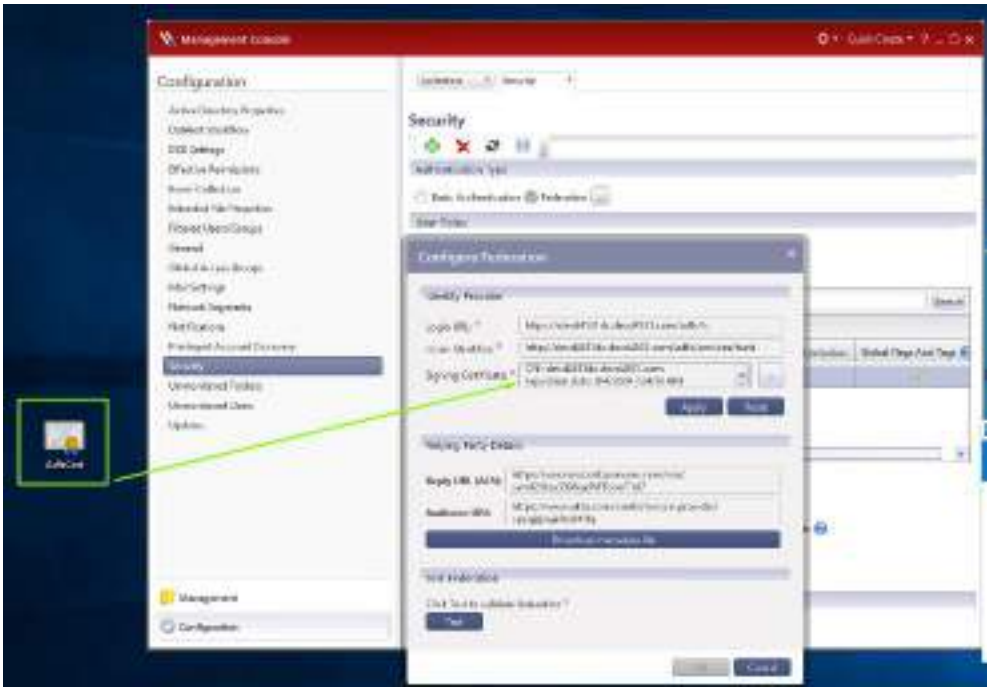
Come back here when you're done setting up the relying trust to test your federation configuration.

Test Federation

Now it's time to test the federation you configured.

1. In the Varonis Management Console, select Configuration > Security
2. In the Authentication Type section, select Federation.
3. In the Configure Federation window, click Test.

The configured federation is validated.



Activate Federation

If the federation test was successful, click OK in the same window to activate federation in Varonis SaaS.

> Note: If the test fails, the Activate button remains disabled.

Verify Federation Login Using SSO

1. To test SSO in the Varonis Management Console, try to log in without entering credentials.
2. To test SSO in Chrome or Edge, go to the user WebDA account without entering credentials.

Now let's take a look at how to configure Varonis SaaS security roles.

Using Entra ID for the New Relying Trust

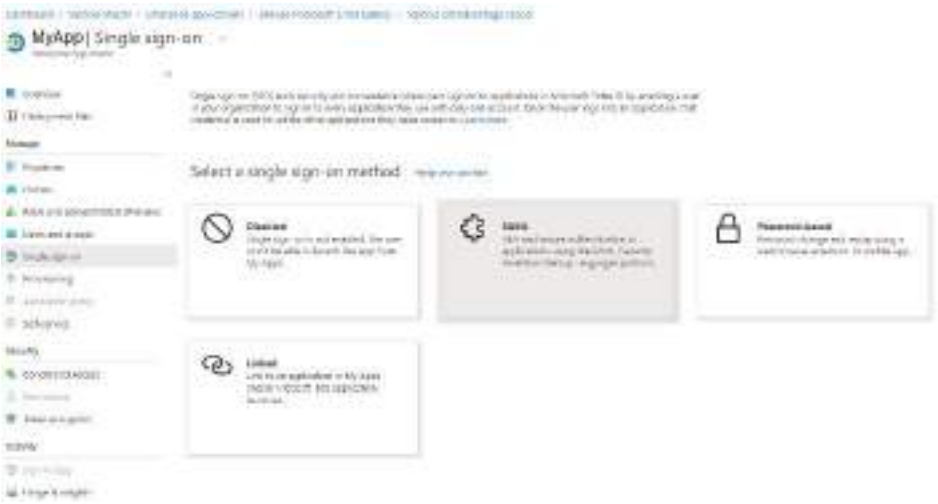
To create an application in Entra ID:

1. Create a new enterprise application in Entra ID. In the examples here, we'll call the application "MyApp," but you can give your application any name you want.
   a. Go to the Microsoft Azure portal.
   b. Navigate to Microsoft Entra ID > Enterprise Applications.
   c. Click New Application > Create your own application.
   d. Type the name of your application (for example, MyApp), select the Integrate any other application you don't find in the gallery (Non-gallery) option, and click Create.



e. Go to the newly created application and then to Single sign-on.

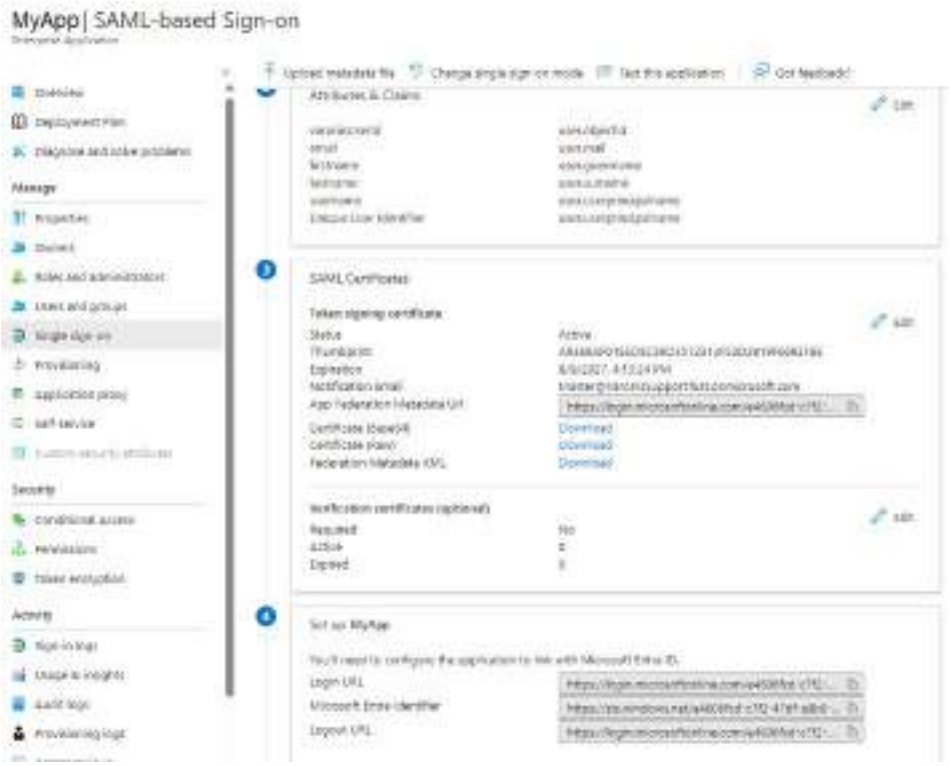
f. In the Select a single sign-on method panel, select SAML.



g. Enter temporary (dummy) values for Identifier (Entity ID) and Reply URL (Assertion Consumer Service URL) to generate the certificate for download.

Important:

- After you have made Entra ID an identity provider in the next section, you need to update the values for Identifier (Entity ID) and Reply URL (Assertion Consumer Service URL) here, using the values that were returned from Okta in the Management Console.
- The URL must use the HTTPS protocol.



h. In the Attributes & Claims panel, map the Entra ID attributes to the relevant Okta attributes:

Claim Name	Value (SAML)	Comments
email	user.mail	Ex: johnsmith@email.com
firstname	user.givenname	Ex: John

Claim Name	Value (SAML)	Comments
lastname	user.surname	Ex: Smith
username	user.userprincipalname	The User Principal Name as defined by your organization. Note this field is case-sensitive.
Unique User Identifier	user.userprincipalname	The User Principal Name as defined by your organization. Note this field is case-sensitive.
varonisUserId	user.objectid	The user's Windows Security Identifier (SID) or Entra ID Object ID. This unique identifier enables Varonis SaaS to map the federated user account to a Windows user account for data access governance. Set to enable federation for data access governance. Ex: S-1-5-21-8417586931-6147815714-526114273-5211

Important:

- These Okta claims are case-sensitive and must be added exactly as shown above. If they are not configured properly, new users who are added after federation has been configured may experience issues signing in. If this happens, the workaround is to go to the Security tab of the Management Console and remove the affected users. Then resolve the issue and add the users back.
- The claim values in the Entra ID user profile must not be null or empty. If the values of the user.givenname, user.surname and user.mail attributes don't exist in the user profile, the login will fail because the user will not be created in Okta.
- The Namespace field must be empty when you're adding a new claim or editing an existing one. Values in this field will alter the claim name that is sent and cause issues for newly added users.

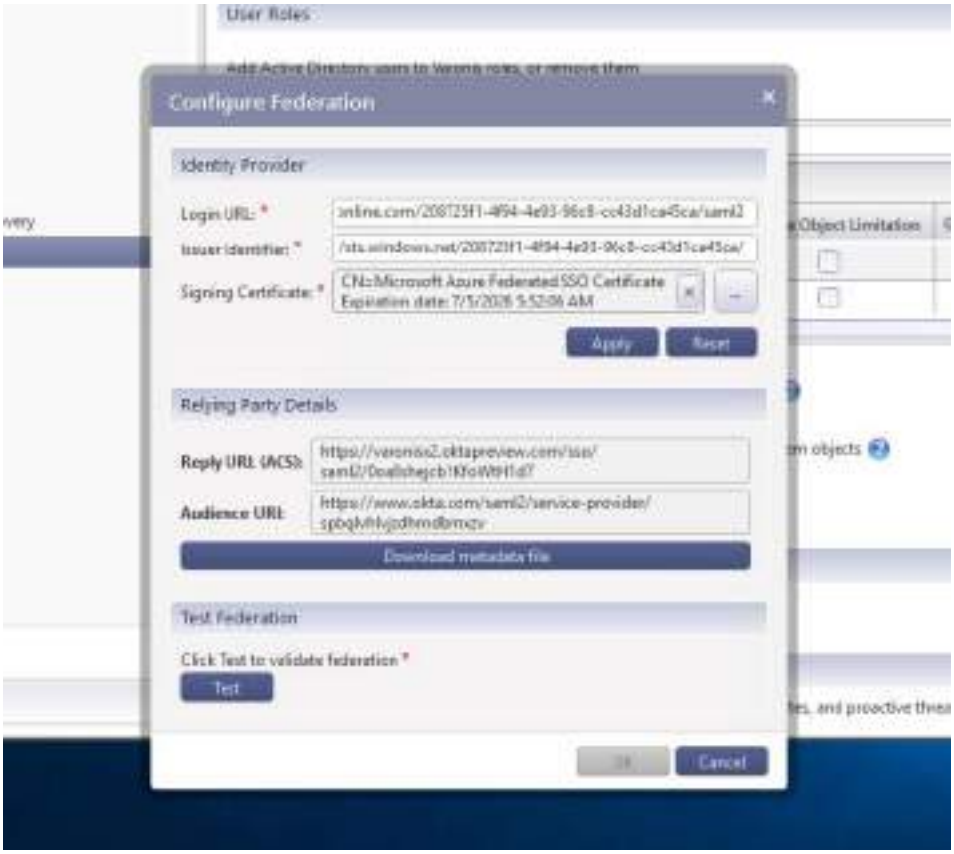


i. Download the certificate. You'll need to upload it to the Management Console in Step 2a below.

j. Assign users to the MyApp application on Entra ID's Users and Groups tab.



2. In the Varonis Management Console, add Entra ID as an Identity Provider on the Security tab.
   a. Use the following input values from Step 1 to configure the IdP in the Management Console:
      - Login URL - Defined in Entra ID, in MyApp > Single sign-on > Set up MyApp.
      - Entra ID Identifier - Defined in Entra ID, in MyApp > Single sign-on > Set up MyApp.
      - The SAML Signing Certificate (base 64) that you downloaded in Step 1i.



b. Click Apply to receive the metadata configuration.

3. Update the MyApp configuration in Entra ID:
   a. Get the following relying party details from the Management Console (the details are returned when you click Apply in the previous step.)
      - Audience URI
      - Reply URL
   b. In Entra ID, go to Single Sign-on > Basic SAML Configuration.
   c. Edit the following fields with the information from the Management Console:
      - Identifier (Entity ID) - This is the Audience URI value in the Management Console

- Reply URL (Assertion Consumer Service URL)



4. When you're done, return to Configuring Federated Authentication (SSO) to test your configuration. After your test is successful, you'll be able to activate the federation for your app.

> Important: If your Entra ID is configured to use Windows credentials for sign-in, be aware of which user account is attempting to sign in when the SSO window is opened.

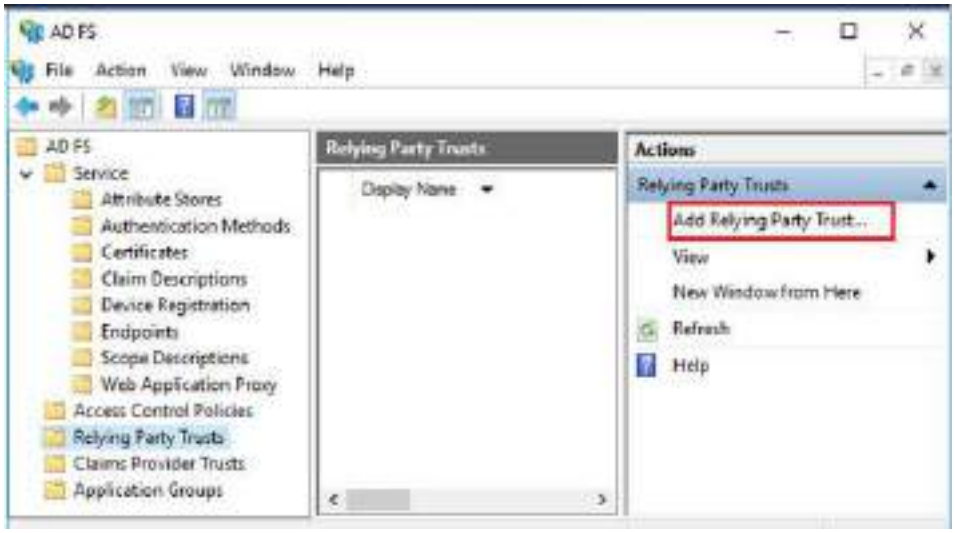
Using Active Directory Federation Services (AD FS) for the New Relying Trust

1. Obtain the IdP configuration prerequisites from AD FS by running the following PowerShell scripts on the domain controller:
   - Login URL (must use the HTTPS protocol)
     ```
     Write-Host "https://$(($adfsProps = Get-
     AdfsProperties).HostName)$
     ($adfsProps.FederationPassiveAddress)"
     ```
   - Issuer Identifier (must use the HTTP protocol)
     ```
     Write-Host (Get-AdfsProperties).Iden/0 v(
     ```
2. Obtain the signing certificate from AD FS Management:
   a. Select AD FS > Service > Certificates.
   b. Right-click the Token-signing certificate and select View Certificate.
   c. On the Details tab, select the following:

- Copy to File
- Export without private key
- Base-64 encoded

3. Now set the new relying trust in the IdP using the metadata.xml file. Download the metadata.xml file from the Management Console and copy it to the Active Directory Federation Services (AD FS) server location.
4. In the AD FS Management Console, add a new relying trust with the claims rule using the returned metadata file.
   a. Set the new relying party trust as follows:
      i. Select AD FS > Relying Party Trusts > Add Relying Party Trust.
      ii. Select Claims aware and Start.
      iii. Select the metadata.xml file as the data source (select Import data about the relying party from the file).
      iv. Specify the display name.
      v. Choose Permit everyone as the Access Control Policy.

      The relying party trust configuration is shown in the Ready to Add Trust section.



   b. Edit the Claim Policy for the new relying party trust:
      i. Right-click Edit Claim Issuance Policy and select Add Rule.
      ii. Select the Send LDAP Attributes as Claims template.
      iii. Set the rule name.
      iv. Select Active Directory from the Attribute store dropdown list.
      v. Set the parameters as follows:

Claim Name	LDAP Attribute	Comments
email	E-Mail-Addresses	Ex: johnsmith@email.com
firstname	Given-Name	Ex: John
lastname	Surname	Ex: Smith
username	User-Principal-Name	The User Principal Name as defined by your organization. Note this field is case-sensitive.
Name ID	User-Principal-Name	The User Principal Name as defined by your organization. Note this field is case-sensitive.
varonisUserId	objectSid	The user's Windows Security Identifier (SID) or Entra ID Object ID. This unique identifier enables Varonis SaaS to map the federated user account to a Windows user account for data access governance. Ex: S-1-5-21-8417586931-6147815714-526114273-5211

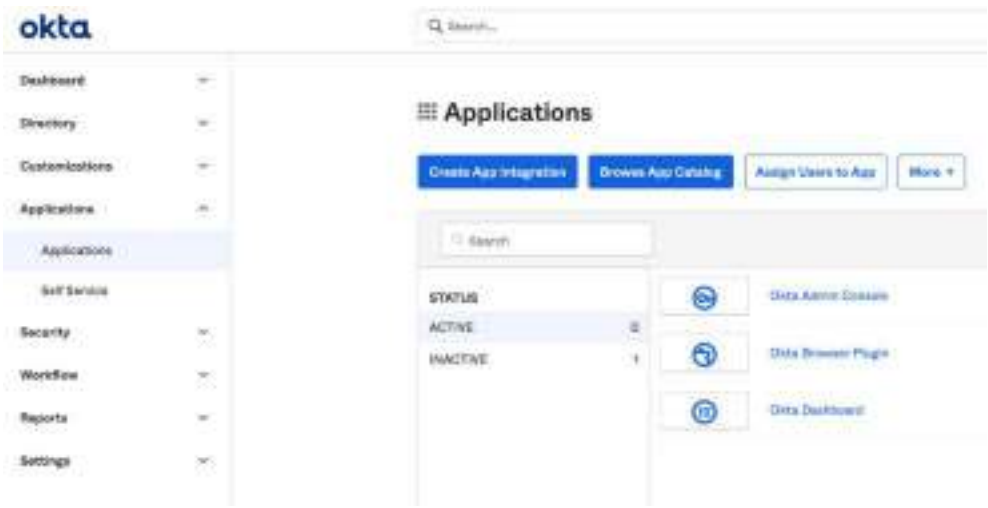
5. When you're done, return to Configuring Federated Authentication (SSO) to test your configuration.

Using Okta for the New Relying Trust

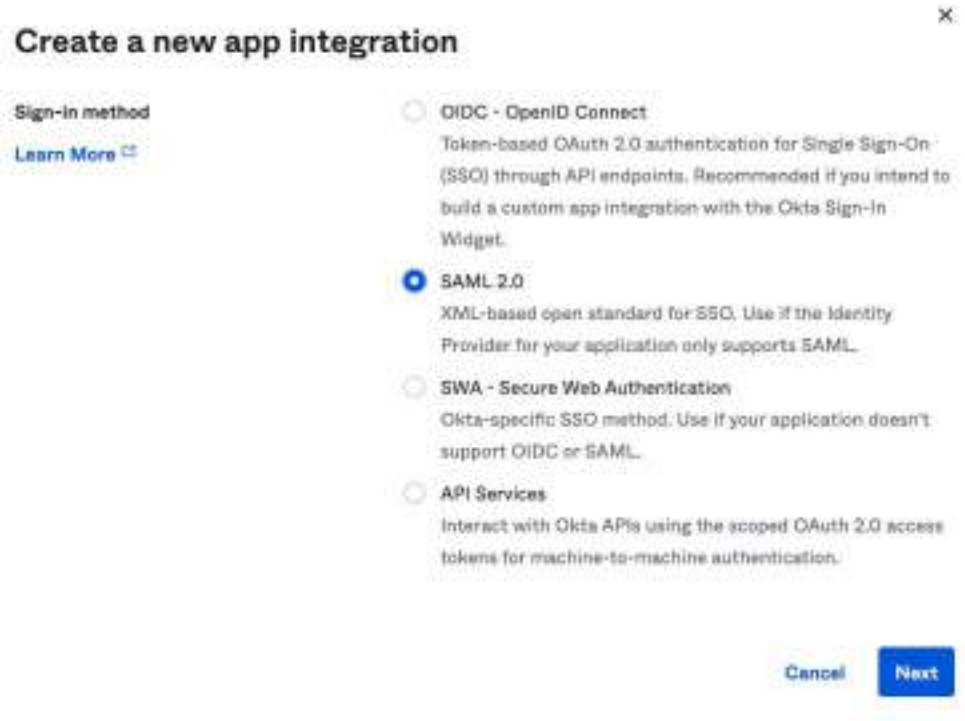
If you want to use your Okta instance as the identity provider for SSO, you need to create an application on your Okta to configure the trust between Varonis and your Okta. This means authentication will be carried out against your Okta, but the users being authenticated will still have an entity in Varonis Okta.

To accomplish this, you need to create an app integration of SAML 2.0 in your Okta with the attributes that Varonis requires. Then set the app registration data on the Management Console Security tab and set the relying party data back in the app registration to enable federation.

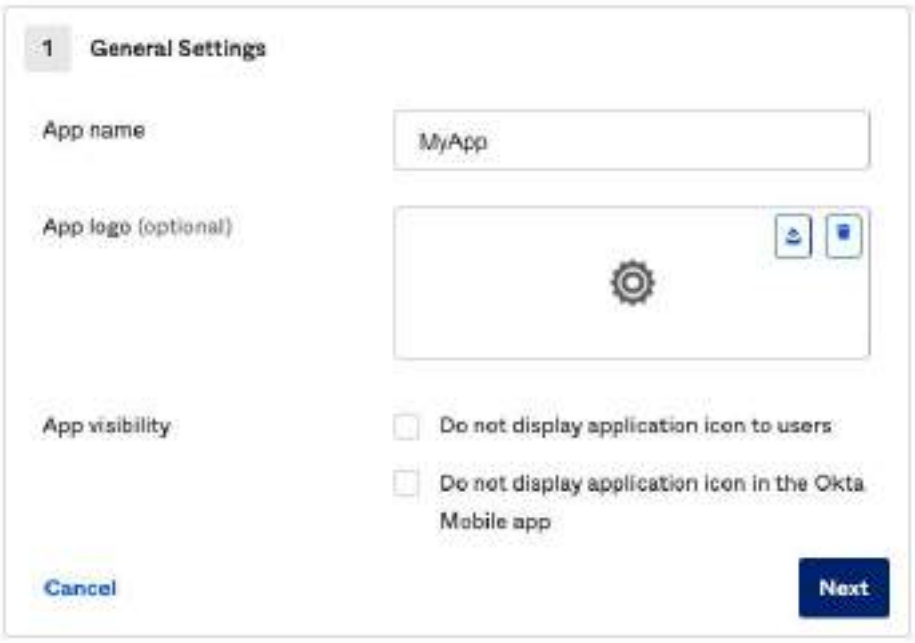
1. In your Okta Admin console, navigate to Applications > Applications and then click Create App Integration.



2. In the Create a new app integration panel, select SAML 2.0 and click Next.

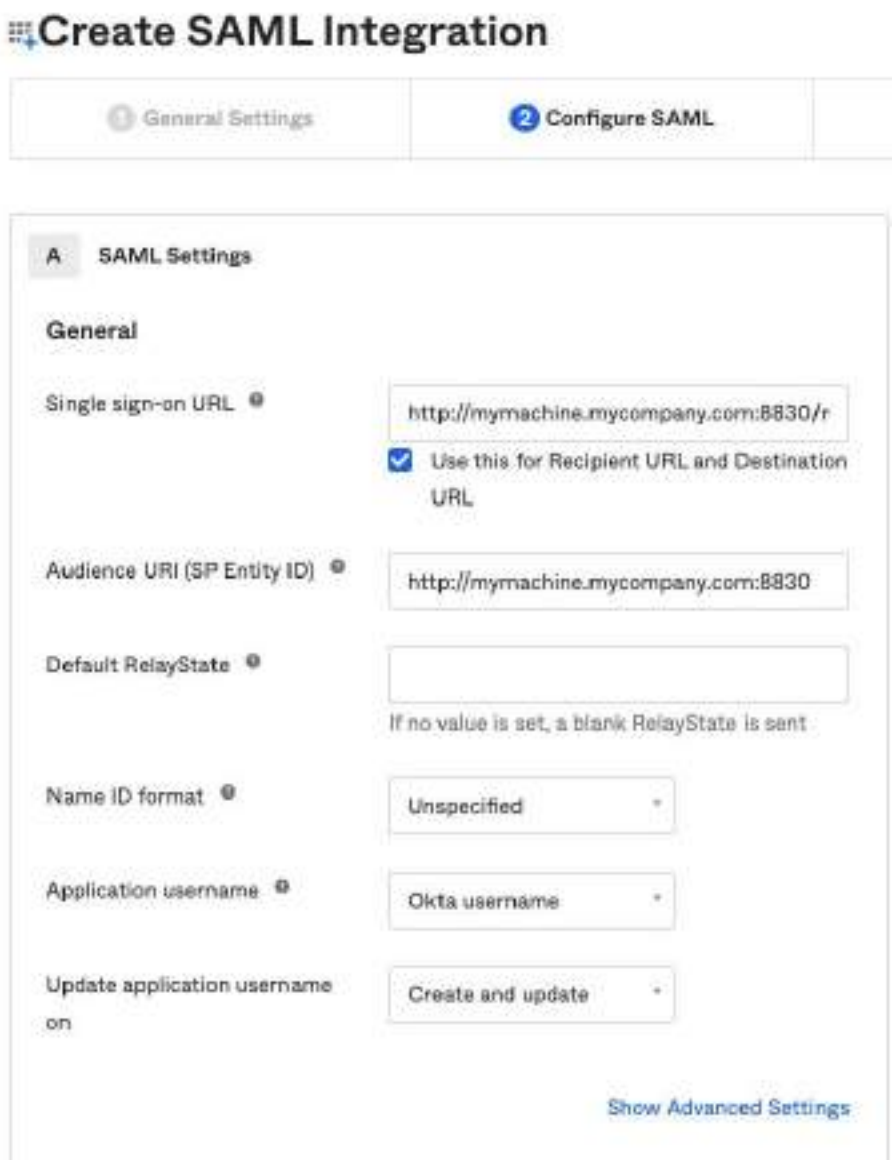


3. On the General Settings tab, enter the name of your application and click Next. For this example, we'll call it "MyApp," but you can call the app whatever you want.



4. On the Configure SAML tab, enter temporary (dummy) values for the following mandatory fields (they'll be updated later):
   - General

- Single sign-on URL - The location to send the SAML assertion.
- Audience URI (SP Entity ID) - The audience of the SAML assertion. This is usually the Entity ID of your application.
- Default RelayState - Optional. The URL of the resource to direct users after they successfully sign in using SAML.
- Name ID format - The username format to send in the SAML response.
- Application username - The default value to use for a user's application username.
- Update application username on - Choose when to update the application username.



- Attribute Statements - Set the attributes as follows:

Name	Value
email	user.email
firstName	user.firstName
lastName	user.lastName

Note: The values in the Value field are case-sensitive

5. Click Next, and then click Finish.
   You are redirected to the newly created application.

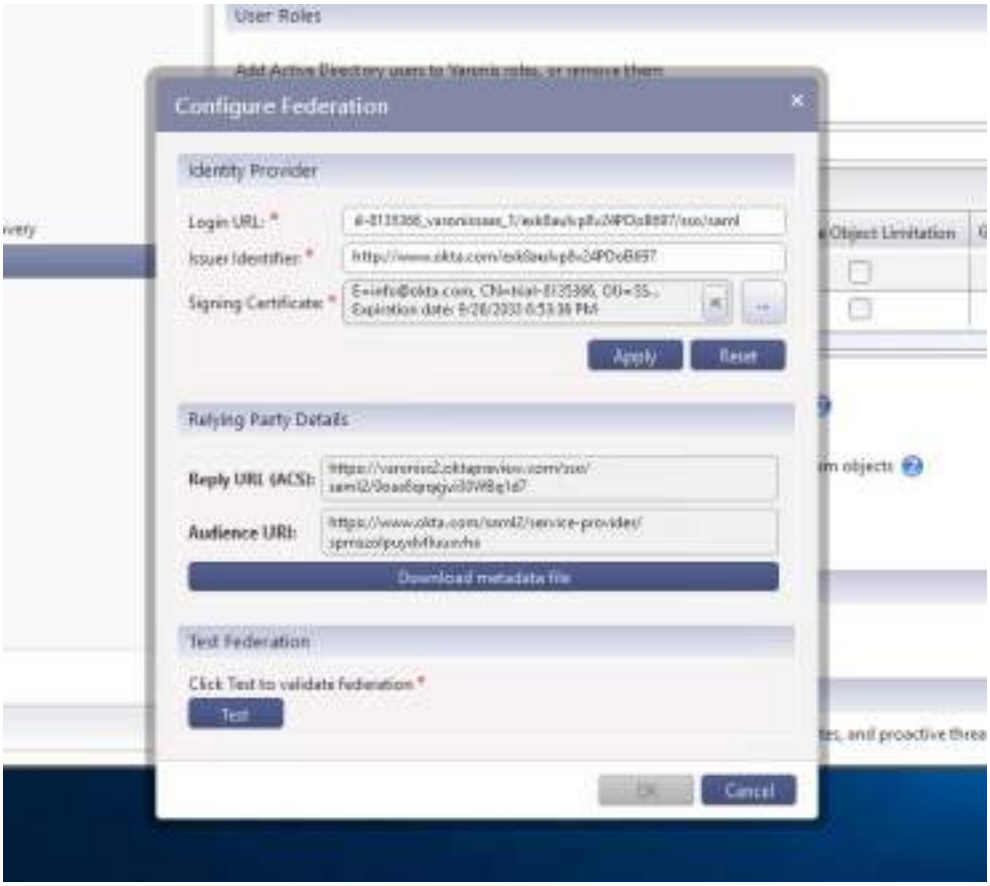


6. Click View SAML setup instructions.
7. Copy the following information from the corresponding fields to the Management Console Configuration Federation dialog box:
   - Identity Provider Single Sign-On URL - Copy to Login URL
   - Identity Provider Issuer - Copy to Issuer Identifier
   - X.509 Certificate - Click the button to download it and save it to your hard drive. Then, on the Management Console Federation configuration screen, click the Browse button to upload it in the Signing Certificate field.

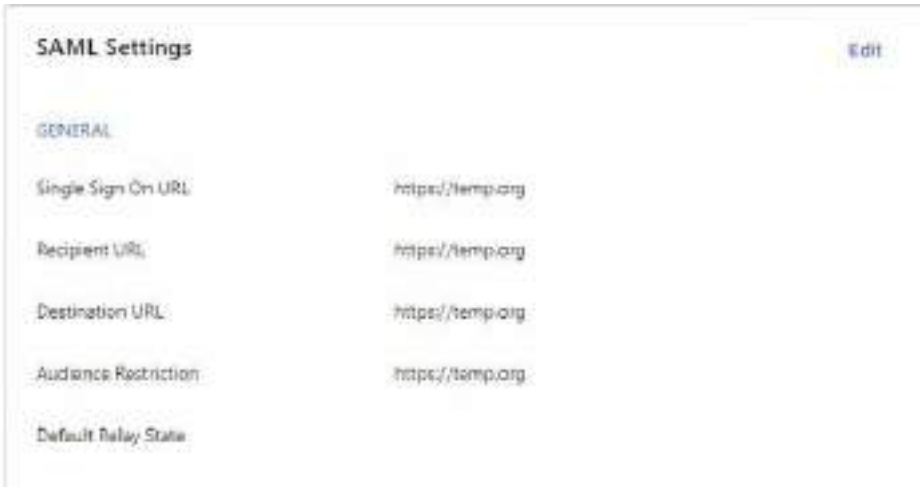


8. Click Apply.

The extended Configure Federation dialog box is displayed, which now includes the relying party details: Reply URL (ACS) and Audience URI.

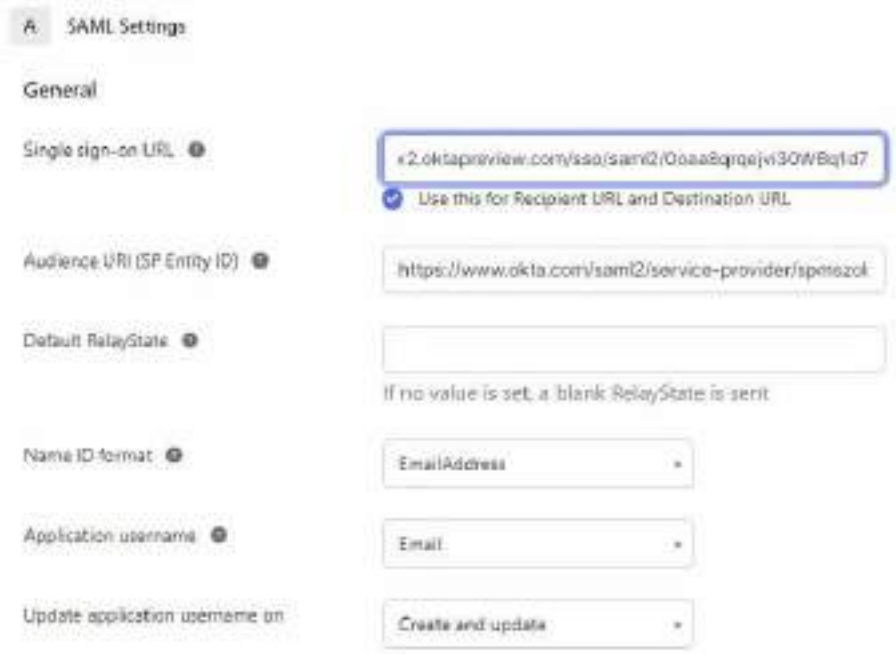


9. Go back to the newly created Okta application.
10. Navigate to SAML Settings and click Edit.



11. Use the relying party details from the Management Console to edit the following:
    - Single sign-on URL - Enter the Reply URL (ACS)

- Audience URI - Enter the Audience URI



12. Click Next, and then click Finish.
13. When you're done, return to Configuring Federated Authentication (SSO) to test your configuration.

Configuring Varonis SaaS Security Roles

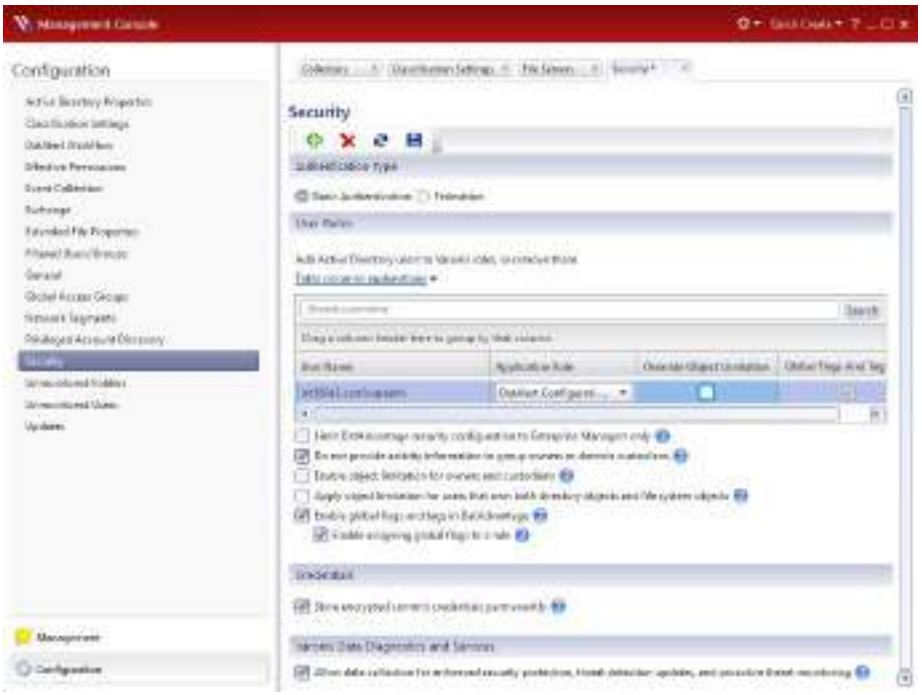
This section walks you through the steps to set up user access using security roles in Varonis SaaS. It provides instructions for configuring security settings and describes the predefined security roles.

Adding New Users to Varonis SaaS Security Roles

The Security settings enable you to add AD users to Varonis SaaS roles (or remove them from roles).

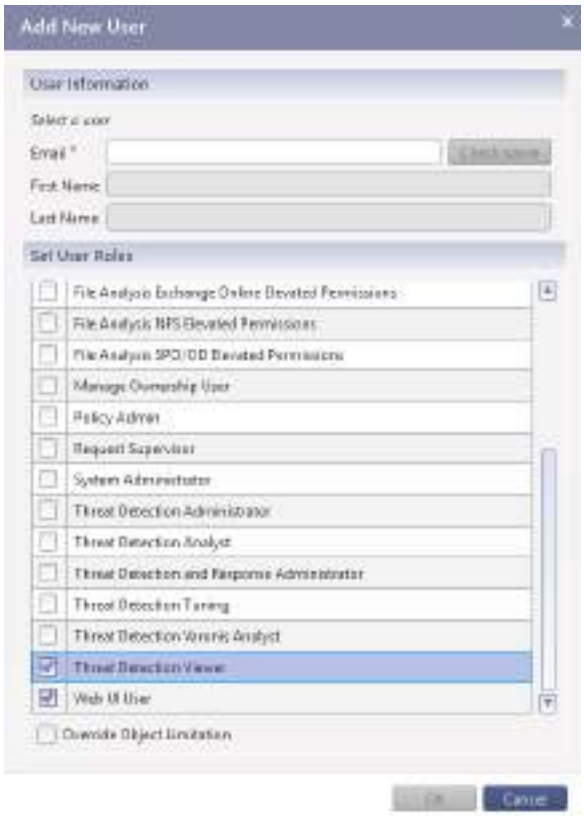
1. In the Management Console, from the menu in the left pane, select Configuration > Security.

The Security settings are displayed.



2. In the Authentication Type area, specify the authentication mode:
   - Basic Authentication - The default option.
   - Federation - For more information, see Configuring Federated Authentication (SSO).
3. To add users to a role:
   a. In the Security Settings pane, click Add on the toolbar.

The Add New User dialog box is displayed.



b. (Mandatory) In the User Information area, enter the user's Email and click Find. The First Name and Last Name fields will be populated.

> Note: The email setting is a unique identifier and cannot be changed, regardless of the authentication method (basic or federation). If there is a need to update the email for the account, the new email should be added as a new user.

c. (Mandatory) In the Set User Roles area, assign one or more user roles.

d. To change a user's role, click that user's Application Role field and select the required roles from the dropdown list. Users may belong to more than one role.

4. When adding or editing a user, you can select the Override Object Limitation checkbox to override the Enable object limitation for owners and custodians setting for the user. The Override Object Limitation checkbox is located at the bottom of the Add New User dialog box, and for editing the user in the main Security Settings pane, it's located in the User Roles grid.

5. Select the relevant option for each user:

   - Limit DatAdvantage security configuration to Enterprise Managers only - Select this option to limit Varonis SaaS security configuration to Enterprise Manager and exclude users with the Configuration role.

- Do not provide activity information to group owners or domain custodians - This option is selected by default. When enabled, it prevents group owners and domain custodians from viewing activity information regarding group members. Regarding reports, this option affects only results displayed in the user interface and data-driven subscriptions. It does not affect regular subscriptions. These must be deleted manually to prevent owners from viewing them.
  - Activity-based reports (report categories 1 and 2) are not available to group owners or custodians
  - Group owners who are also data owners have access to all relevant information as usual
- Enable object limitation for owners and custodians - Select to limit owners and custodians to view only the object hierarchy each one owns.
- Apply object limitation for users that own both directory objects and file system objects - Select to restrict users from owning both directory objects and file system objects.
- Enable global flags and tags in DatAdvantage - This option is selected by default. When enabled, it determines whether global flags and tags can be used in Varonis SaaS.
  - Enable assigning global flags to a rule - This option is selected by default when the Enable global flags and tags in Varonis SaaS is selected. When activated, it enables assigning global flags to a file based on Data Classification rule criteria. The global flags can be assigned to files only.

6. To remove users:
   a. Select the relevant users in the User Roles area.
   b. Click Remove.
7. Click Save.

Varonis SaaS Security Roles

Varonis provides several basic predefined application roles that can be assigned through the Management Console.

The predefined application roles include:

Role	Description
Classification and Privacy Automation Configuration User	Edit classification rules and policies; access and edit the Privacy Automation Setup section in the Management Console.

Role	Description
Classification Results View	View the results of data classification in the Varonis Web Interface.
Commit/Edit User	Access the Action Center. View, edit and manage operations and actions.
Configuration User	View and configure objects.
Dictionary and Content View User	View and edit the Dictionaries window.
Edit memberships and permissions	Can edit changes but cannot commit.
Enterprise Manager	Has full control over the Varonis SaaS environment, including all required operations. Note: File analysis and access to data discovery and classification policies require additional roles as specified in the relevant documentation.
File Analysis Exchange Online Elevated Permissions	View the classification analysis of all sensitive items on an Exchange Online data source in the Access Intelligence screen. Important: This role allows the user to access the files regardless of the user's permissions.
File Analysis NFS Elevated Permissions	View the classification analysis of all sensitive documents on an NFS data

Role	Description
	source in the Access Intelligence screen. Important: This role allows the user to access the files regardless of the user's permissions.
File Analysis SPO/OD Elevated Permissions	View the classification analysis of all sensitive documents on a SharePoint Online or OneDrive data source in the Access Intelligence screen. Important: This role allows the user to access the files regardless of the user's permissions.
Manage Ownership User	Access the Manage Ownership window. Assign ownership and custodianship without having access to the configuration screens in the Management Console.
Policy Admin	Access the Automations tab in the Policies page, create new automations and edit existing automations.
Privacy Automation User	Access and use Privacy Automation
Request Supervisor	View all Data Access Governance requests with a status of Pending
System Administrator	Maintain Varonis SaaS through its configuration window.
	Cannot edit or commit changes on the actual data.

Role	Description
Threat Detection Administrator (previously "DatAlert Configuration User")	"Threat Detection Tuning" permissions plus the ability to edit the Alerts dashboard, create and edit Threat Detection policies.
Threat Detection Analyst	"Threat Detection Viewer" permissions plus the ability to manage alerts (change alert status).
Threat Detection and Response Administrator	"Threat Detection Administrator" permissions plus the ability to change script execution configuration. If a user doesn't have this role, the ability to edit script execution settings is not permitted.
Threat Detection Tuning	"Threat Detection Analyst" permissions plus the ability to change Privileged Account type, add and edit exclusions (from the Policy or Alert page).
Threat Detection Viewer	Basic "Web UI User" permissions plus the ability to view Threat Detection policies.
Web UI User	View most pages of the Varonis Web Interface (such as the Dashboards and Analytics pages, including Alerts), but cannot access pages and actions that require a more elevated role (such as policies, certain configurations, file analysis etc.).
AI Prompt Auditor	View collected Copilot prompts and responses.

Role	Description
Note: Private Preview.	

You're well on your way to Varonis SaaS! Now let's get familiar with the web interface.

4 UPGRADE THE COLLECTORS

To benefit from the newest features and enhancements available in the latest version, you must upgrade your Collectors.

> Note: Cloud services are updated by Varonis while the Collectors are updated by the following procedure.

To upgrade the Collectors:

1. In the Varonis Web Interface, from the Configuration menu, select System Topology.
2. Select the Update Settings tab.
   The System Updates page is displayed.
3. To receive automatic updates, set a schedule for the updates to be installed.
4. If you want to limit the time you allow for an upgrade, select the Limit execution duration to checkbox and type the number of hours an upgrade can take.

If you select manual updates, make sure you look at your Collectors page to see if they need to be updated. If an Update button is displayed in the Status column instead of Active, click the Update button to perform the upgrade.



> Note:
> When you upgrade a Collector, the Management Console installed on the Collector is upgraded as well.
>
> To install or upgrade the Management Console on a different machine, in the Varonis Community (help.varonis.com), go to Manage > My Downloads and download the latest SaaS Management Console installer.

Collector Updates

Sometimes, a security hotfix or small functionality updates will be delivered to the Collector. These updates will not change the Collector version but will remediate specific issues until the next version is released.

The updates will be deployed over the same scheduling settings as the Collector upgrades.

Once an upgrade is available, it will render all previous updates obsolete.

On-Premises Component Upgrade/Update – Architecture And Security Measures

The Varonis on-premises components (such as the “Collector”) can be automatically or manually upgraded. This process undergoes various security measures for protection.
There are two tracks for updating the on-premises component:

- Full upgrade - moving to a newer major version
- Applying an update – updating the current version with a hotfix

Processes and Procedures

- All software developed by Varonis adheres to the company's Secure Software Development Life Cycle (SSDLC) processes. The SSDLC processes include a review of the defined scope of the changes, the components within the application stack, control testing, binary signing during the release phase, and more.
- Varonis is ISO27001 certified with multi-year compliance maintenance. Processes and procedures undergo review and verification; the processes are continuously optimized. Varonis believes that improvement is constant, and strives to improve its platforms, internal tools, and related processes.
- All Varonis binaries are signed as part of the build process.
- All deployment packages themselves are also signed as part of the build process.
- Varonis has a secure CI/CD, which ensures that only hardened build servers can build, sign and publish deployment packages.
- Once a package is published, it is gradually rolled out to customers. If issues are detected during the gradual rollout, further rollout is halted, and a fix is re-released.
- The Varonis agent downloads deployment packages and verifies their integrity signature.
- Actual deployment occurs based on maintenance windows defined by the customer.

The Path to an Upgrade / Update Delivery

Varonis Engineering

- The build/upgrade? (entire version) or update (single package) is generated from internal official repository, by release managers.

- The build passes automatic acceptance tests and other inspections
- Once approved, the build or package becomes an official version and is uploaded to the CDN.
- The build is deployed to Varonis production environment. Varonis is always the first customer to get the new version / upgrade.
- From this point there is a controlled rollout to selected customers until the upgrade is released for full rollout.

Server Side (cloud)

- Release managers grant access to the new version in CDN based on rings/tenant id?
- Cloud distribution services enforce this settings? and generate instructions for self-hosted/on-premises? Agents?.

Client side

- Distribution agents in the self hosted/on premises? part – such as the Collector – poll the cloud distribution services for new instructions.
- Once the agent receives new instructions, the agent downloads the new version from the CDN.
- The local agent verifies the content of the upgrade/update and the signature, ensuring the source of the files is Varonis and files were? not intact in the delivery process.
- Based on the maintenance window (either immediately / Scheduled/ Manual), the new version is deployed.
- Deployment status / success / failure is reflected in the WEB UIwhere? and in internal Varonis health dashboards.

5 CONFIGURING LIVE UPDATE FOR THE (DEPRECATED) DEPLOYMENT HUB

The Live Update functionality enables you to automatically keep your Varonis on-premises components up to date with content, security updates, and bug fixes. You can choose whether to deploy the updates automatically or manually.

About Live Update

- No user data is sent or exposed when Live Update is enabled. Live Update receives updates and sends only deployment status and installed updates.
- Live Update will not cause any data loss or system downtime.
- The Varonis Live Update service is enabled by default to ensure that Varonis applications run efficiently and stay protected, to enhance system stability, reliability, and security. Live Update can be disabled during installation or at any time through the Management Console.
- The download time for live updates depends on Internet connectivity and update size; the typical update package size is less than 100MB.
- You can view installed updates in the Management Console Update Manager tab.

Live Update Requirements

- Internet connectivity is required to receive live updates. If Internet connectivity is disrupted, once the connectivity is restored, Live Update will query the server and provide the new update.

Security

- All updates that are downloaded via Live Update are signed using cryptographic keys and verified by Varonis. The update creation process prevents the injection of malicious code into these packages.

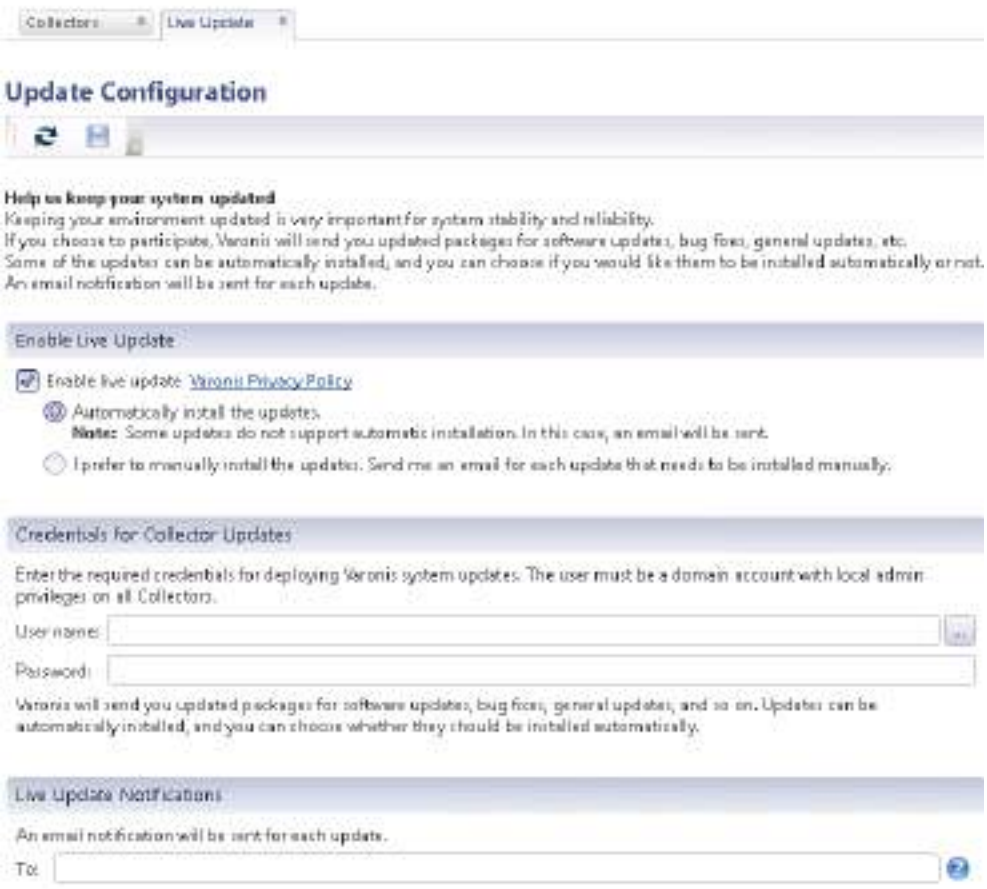
Limitations

- Live Update is not supported when run via a proxy that requires authentication. As a workaround, add the following Live Update endpoints to the Allow List (to skip authentication):
  - Live Update external service: https://liveupdate.varonis.com/
  - Live Update blob storage: https://azeu2prdlveupdsa.blob.core.windows.net/

Configuring Live Update

To configure Live Update:

1. In the Management Console, from the menu in the left pane, select Configuration > Updates. The Live Update tab is displayed.



2. Enable live update is selected by default. You can clear this option to disable it, to prevent updates from being automatically downloaded to your system; however, it is not recommended to do so.
3. Select your desired installation mode:
   - Automatically install the updates - Select this option for automatic update installation. A notification will be sent about the deployment.
   - I prefer to manually install the updates - Select this option to receive an email notification for each update that needs to be installed manually. Downloaded updates can be deployed through the Management Console Update Manager tab, accessed via Management > Components > Root.
4. In the Credentials for Collector Updates area, enter the credentials that will be used for Collectors.

   Note: The user will be used to automatically deploy updates; therefore, the user must be a local administrator in the environment.
5. To configure the Web proxy server for Live Update:
   a. Go to the Deployment Hub installation location. By default, it is C:\Program Files (x86)\Varonis\DatAdvantage\.
   b. Go to the LiveUpdate\ subfolder.
   c. Open the `Varonis.LiveUpdate.Service.exe.con x` file in Notepad. (You may need to open Notepad with "Run As Administrator" if User Account Control (UAC) is configured.)
   d. Find the section named `<defaultProxy>` under `<system.net>`. For more information about this section, see Microsoft Docs.
   e. If the section is commented out, uncomment it.
   f. If the section does not exist, add it (see the example provided at the end of this procedure).
   g. Change the `<proxyaddress>` to the address of your proxy server.
   The following is an example of the proxy section in textual format.

```
<system.net>
     <defaultProxy>
       <proxy
           usesystemdefault="true"
           proxyaddress="http://10.10.4.160:998"
           bypassonlocal="true"
```

```
      uvwr"3/d(6-$
)$)/v4 net>
```

6. Click Save.
7. Restart the Live Update Client service to effect immediate configuration changes.

Live Update Email Notifications

With each Live Update deployment, an email notification is sent, indicating whether the update has been published and deployed, or is waiting to be deployed on your system.

> Note: Emails are sent to users defined in the Live Update Notifications area of the Live Update tab. To access the tab, go to the Management Console > Configuration > Updates.

Varonis Update Notification messages vary per Live Update deployment type and outcome:

- Successful deployment - "No further action is required on your part."
- Manual deployment - User action is required; "To install the update, see the Update Manager tab in your Management Console."
- Failed deployment - User action is required, "Due to system limitations, the update was not completely installed. Contact Varonis Support for assistance."

6 TOUR THE VARONIS SAAS WEB INTERFACE

The Varonis Web Interface provides several ways to narrow your focus and pinpoint the events and alerts that most require your attention, enabling you to review high-level summarized data via metrics in dashboards and perform investigation flows based on the collected data.

The Varonis Web Interface enables investigations flows, such as alerts and events investigations. These flows are based on an intuitive search mechanism that eases and simplifies investigation flows. In addition, predefined saved searches representing valuable use cases are provided, and additional saved searches can be defined. Investigation results can be exported from the Varonis Web Interface and scheduled searches can be easily configured.

The Varonis Web Interface comprises three main sections (pages): Dashboards, Analytics, and Management (advanced user roles such as administrators have access to additional sections, for example Configuration and Account). The main sections and functionalities are described below.

> Note: For contextual help and self-service articles, click the search icon at the bottom right corner: 

Dashboards

The Varonis Web Interface dashboards display important risk indicators and other metrics through widgets that enable you to view information at a glance.



The Dashboards page includes the following components:

- Navigation bar (1) - Used to access the main sections of the Varonis Web Interface. By default, this bar is collapsed, showing only the icons of the main menus. Use this bar to navigate as follows:
  - Hover over the Dashboards or Management icons to view the menu options.

- To expand the navigation bar and display the menu names, click the Varonis arrow at the top:



- Dashboards panel (2) - Lists a range of dashboards that offer at-a-glance visibility into critical exposures and concerns regarding your key data stores and Active Directory (the Alerts dashboard is displayed by default).
- Filters panel (3) - Dashboard-specific, predefined filters for running a search query and displaying data. These filters include:
  - File server or Domain - Narrow down the search to a subset of these entities (default is All).
  - Alert date - Set the date and time range over which to run your search query (default is Today).
- A variety of widgets within each dashboard (4) - Show the query results, providing drill-down context and explanations of security risks and vulnerabilities: From vulnerable user accounts to at-risk cloud data to potential compliance violations.

Widgets Types and Elements

The available widget types include:

- Single-metric Widgets - Show a single data point, such as the number of sensitive files, or the number of folders with open access.
- Percentage Widgets - Compare two metrics.
- Horizontal Bar Chart Widgets - Are useful for comparing related metrics at a glance by displaying statistics from multiple metrics at the same time side by side.
- Stacked Vertical Bar Chart Widgets - Display statistics from multiple widgets at the same time stacked one on top of the other.
- Overlay Bar Chart Widgets - Display series as subsets of others, unlike horizontal bar chart widgets that display statistics from multiple metrics side by side.

- Timeline Chart Widgets - Display statistics over time.
- List Widgets - Display individual values from a single set.
- Geo Widgets - Display the number and severity of alerts in a pop-up for a geolocation selected on a map.

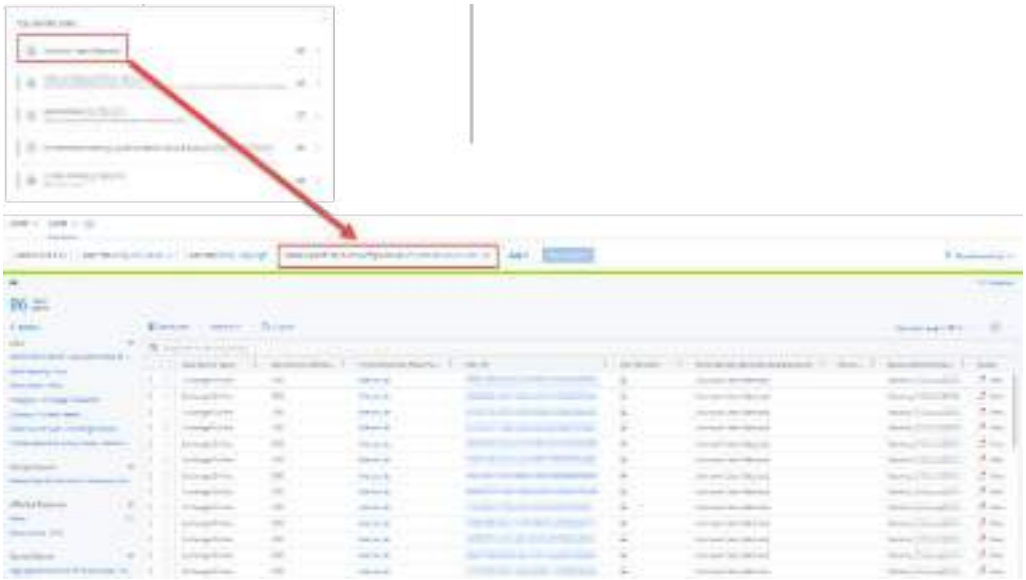
Note: For a description of a specific widget, click its menu at the top right corner and then select Information:

The widget elements (titles, categories, and series) are context-sensitive, so you can click a specific element to view its filtered data on the Analytics page:

- At the Dashboard level - The filters you set on the Dashboards page are applied to the data on the Analytics page.
- At the widget level - Click a specific element (title, category or series), or click the View Items menu option to jump to the corresponding filtered data.

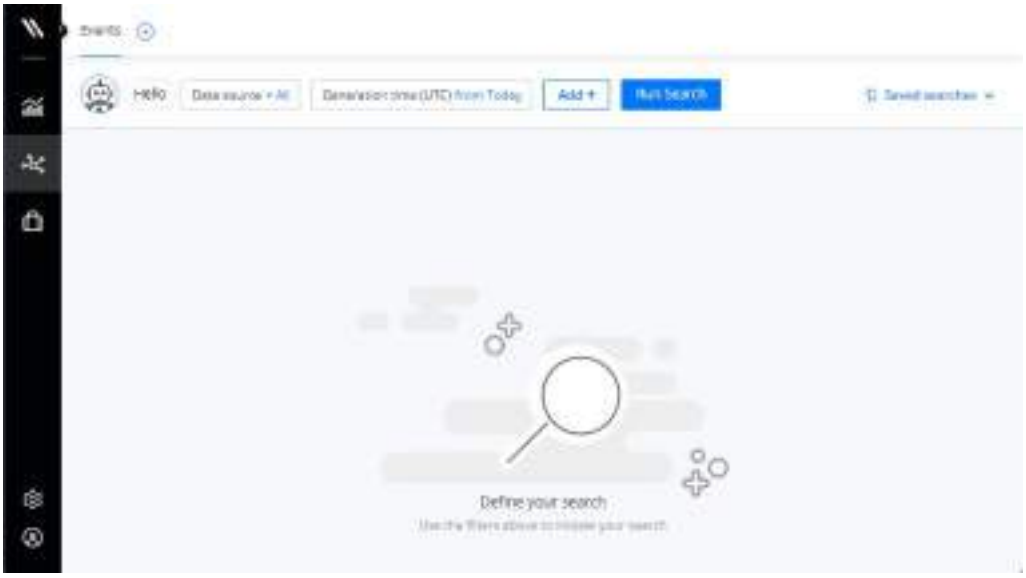
The following example shows the Alerts dashboard's Top alerted users widget. You can click the top alerted user, in this case: Unknown User, to jump to its filtered data

on the Analytics page.



Analytics

The Analytics page provides deep data visibility: Drill down to specific data in the Events, Alerts, Resources, Permissions or Accounts tabs. You can also go to the Access Intelligence tab to view your network's resource tree.



The page has two main areas: The top area defines the search and the bottom area shows the results.

Search Area

The search area defines the query context and criteria using the following components:

- Tabs - Determine the search context by the type of objects to be searched: Alerts, events, resources etc. The Events tab is displayed by default and a plus sign ⊕ allows you to add new tabs.
- Filters panel - The work area for building and running search queries.

Tabs

Click the plus sign ⊕ to launch one or more of the following tabs and then search for specific analytics:

- Events (the default tab) - Displays a line chart illustrating the dispersion of events (for example, creating or removing a site, folder, file, or permission on the platform you are monitoring) over the specified time line, as well as event information in table form. You can use this information to view and search the activity log of your data sources and domains, identify risky activities, and investigate alerts.
- Alerts - Displays the alerts triggered by DatAlert. You can use this information to review alerts and search for alerts by a specific user, threat model and so on to understand the overall threats detected, manage them, and investigate a specific alert.

- Access Intelligence - Displays the resources in your network in a hierarchical tree that allows you to see which users have access to each resource, and the permissions granted to each resource. You can also access insights per resource.
- Resources - Displays a tabular view of a resource's properties, based on the criteria you define in the search query. Resources include the sites, folders, or files on the platform you are monitoring.
- Permissions:
  - Physical Permissions - Granted directly to users and/or groups on a resource (shown by default).
  - Effective Permissions - Click the Switch to effective permissions link to display permissions that users (or groups) inherited via membership of groups with permissions on the resource.
- Accounts:
  - Accounts - Displays a tabular view of the retrieved data for all types of accounts (User, Computer or Group). You can use this information to analyze the accounts that triggered the alerts. Shown by default.
  - Memberships - Click the Switch to memberships link to display groups and their membership details.

  Displays a tabular view of the retrieved data for all types of accounts, including groups and their membership details. You can use this information to analyze the accounts that triggered the alerts.

Filters Panel

The search query is built using filters. A filter is an event attribute that is registered as a database column, for example; "Account Type", "Authentication Method", "Status" etc. Each filter has a set of supported values, for example: The "Account Type" filter may have one of the following values: "User", "Computer" or "Group".

When you create a query, you can add as many filters as needed to pinpoint the relevant data: Narrow down your search by setting your filters to specific values of interest (in the above example, you can set the "Account Type" filter to the "User" value).

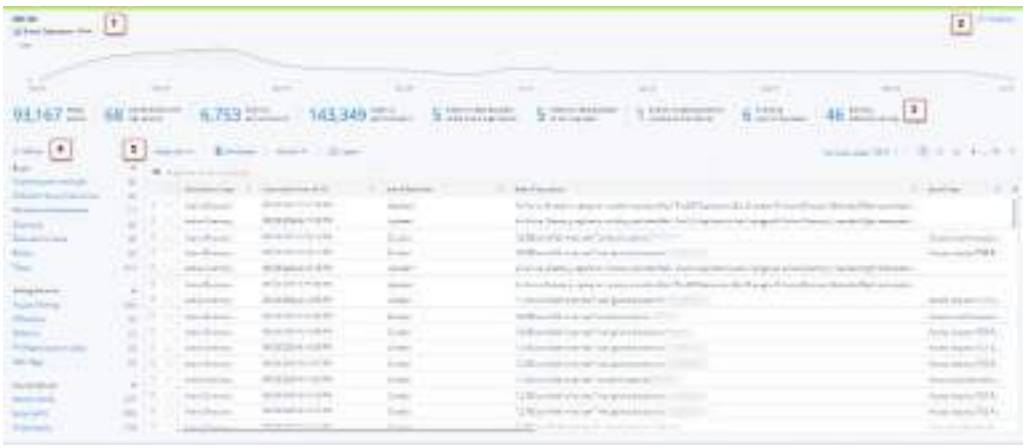
The query filters and values are defined using the following components:

- AI functionality  - Use natural language search to conduct in-depth investigations and analysis. Click the robot icon to replace the filters with a text box and enter your query. For details, go to Athena AI.
- Default search filters:

  - Data Source filter - Narrow down the search to a subset of your servers (default is All)
  - Generation time (UTC) filter - Set the time range over which to run your search query (default is Today).
- Add + - Launch a free text search box to get auto-complete filter suggestions: When you begin to type a word or phrase, the area below the search box automatically shows suggestions for filters and values that contain your text. Select one or more of these suggestions to add them to the search bar.
- Run Search - Click this button to execute your query against the database and view the search results below the progress line.
- Saved searches (on the right of the search area):
  - Save search (or Save search as) - Save your current search for reuse at any time.
  - Available searches - Select from a list of predefined, commonly-used queries. You can further customize these existing queries to pinpoint the data you need.

Results Area

Varonis creates a record of every important action on your data. The search Results area (1) shows the total number of records that match your query. In addition, you are presented with a variety of components that highlight important findings: Timeline (2), Insights (3) and a Refine pane (4).



To understand your results and identify where you are at risk, customize the display and perform additional actions using the following components:

- Table view (5, Events tab only) - Lists all records that match your query. The table columns correspond to your search filters and to additional relevant attributes that are included by default.

  Note: To view the complete set of results available for an event, switch the view from the default Table View to the optional List View. This view provides the option to show all attributes with populated data, to fine-tune your analytics.

- Attributes - The table displays commonly-used default attributes. Use this option to add other attributes of interest to your results.
- Actions - Use this context-sensitive menu for actions that are relevant to the tab that is currently active and the entries you select from the search results. For example, use the View related action to jump to the related alerts, events, accounts, permissions, or resources: The relevant page opens and the search

query is automatically updated, enabling you to easily see your data in a narrower context for further investigation.

- Export - Download the search results as a CSV, Excel or PDF file.
- Each table entry (row) has a more options button for running relevant actions on the selected table entry, such as opening its context card or managing ownership (available in the Resources and Access Intelligence tabs).
- Timeline (4) - When working in the Events tab, you can click the expand arrows to view a line chart illustrating the changes in the alerted events over the specified period of time.
- Insights (5) - A quick way to spot meaningful information. When you click an insight, the insight criteria are added to your search query, and the query is executed again.
- Refine pane (6) - Includes facets: Search statistics that can also be used to refine the scope of your search (Event, Acting Account, Source Device etc.). By default, all facets are expanded to show the distribution of their attributes in your search results.
  The Refine pane also provides a quick, easy way to drill down and analyze the results per facet. For example, you select the User name facet to view information about the users who performed the events and the number and percentage of alerts generated per user.

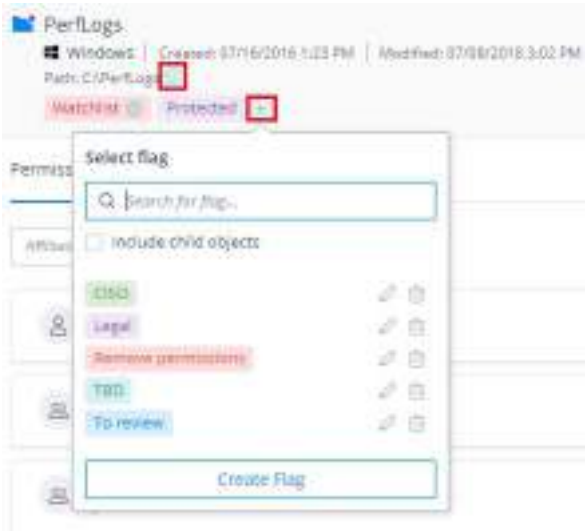
Resource Side Pane

If your search results include resource paths, you can click the path of a specific resource of interest to launch its side pane. This pane allows you to easily view all of the resource data at a glance, detect risks, and drill down to perform your investigations.

The side pane includes a header with brief metadata about the resource (such as its name, tags, and so on), as well as commonly used functions:

- Copy path - Click the copy icon (at the end of the path) to copy and paste the path either inside the Varonis system or into your external applications.
- Manage flags - Click the plus icon (at the end of the attached flags list) to create, edit or delete flags. Attach flags to a resource to mark it with your own insights, and then filter or group search results by their flags.

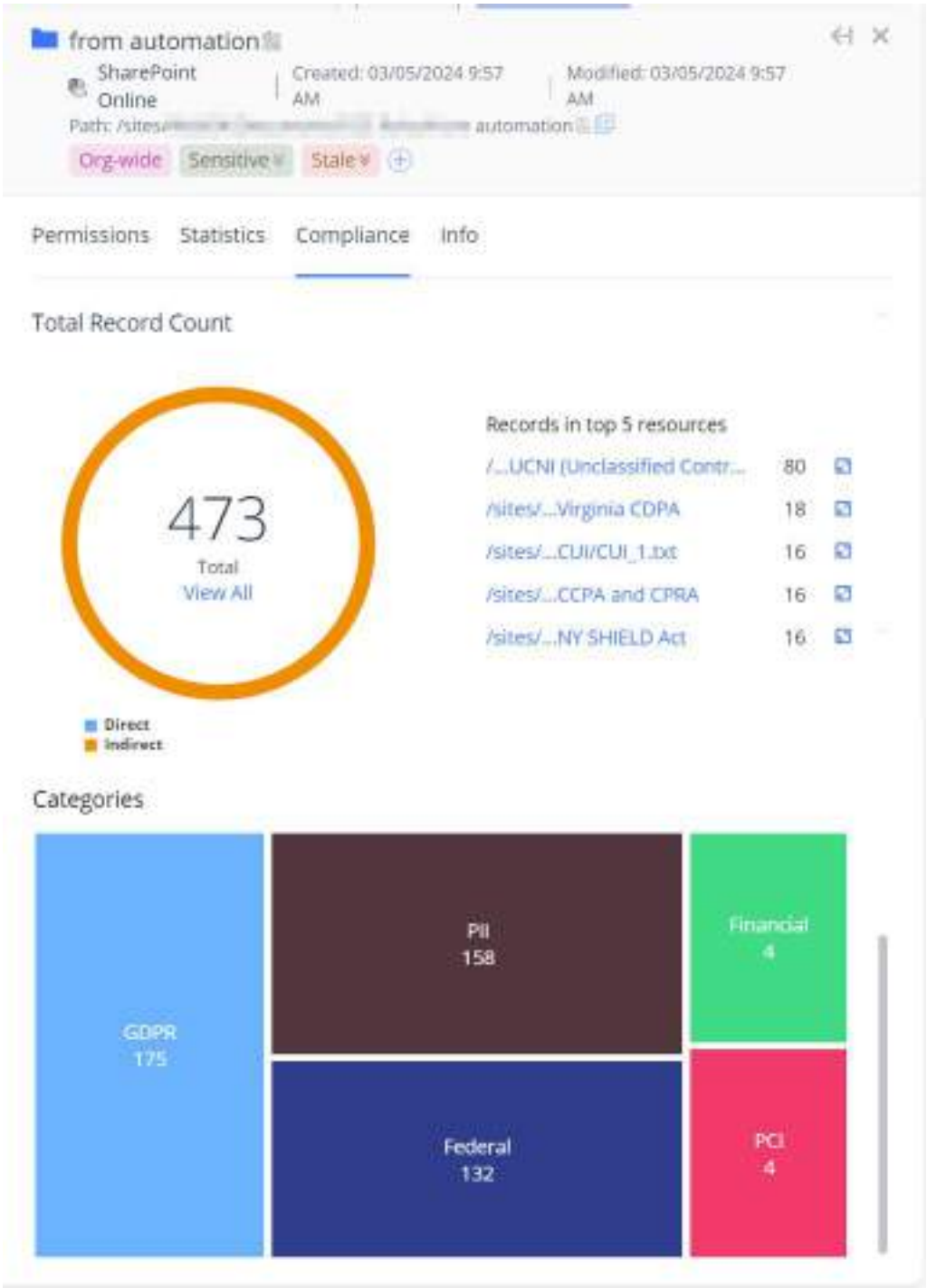
  Note: In addition to these custom, user-defined flags, there are system flags that are managed by Varonis and automatically detect important insights (for example: Whether this resource is stale, protected, unique etc.).



The resource data is presented in the following tabs (the available tabs depend on the available information):

- Permissions - All the permissions on the resource.
- Statistics - An aggregated view of the accounts with the most events on the selected resource.
- Compliance - An overview of all the classified data on the resource and its subfolders.
- Info - All the metadata for the resource, a notes component, and a list of owners.

The following image shows an example side pane of an example resource, displaying its Compliance tab.

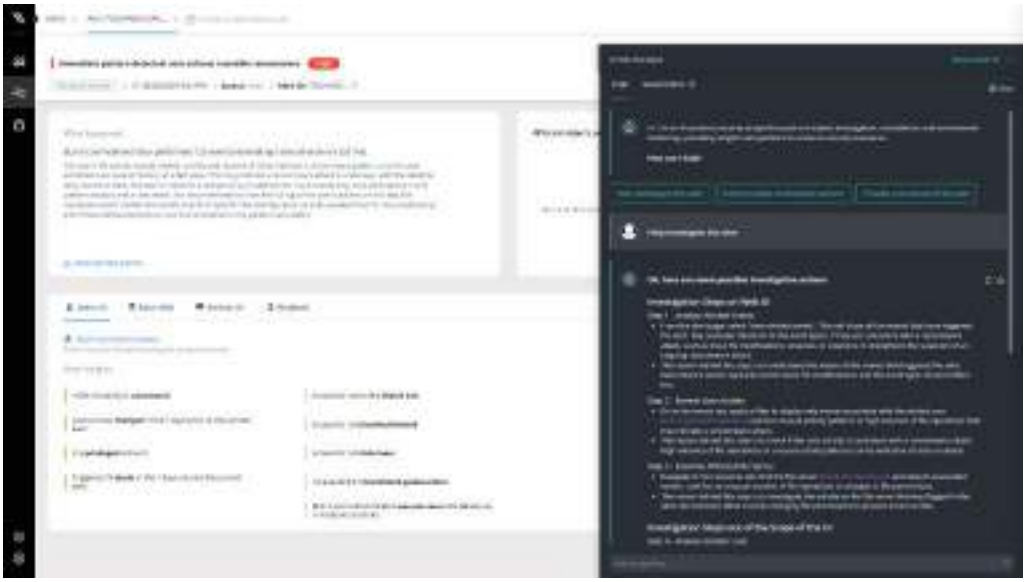

from automation
SharePoint Online
Created: 03/05/2024 9:57 AM
Modified: 03/05/2024 9:57 AM
Org-wide
Sensitive
Stale
Permissions
Statistics
Compliance
Info
Total Record Count
473
Total
View All
Direct
Indirect
Records in top 5 resources
/...UCNI (Unclassified Contr... 80
/sites/...Virginia CDPA 18
/sites/...CUI/CUI_1.txt 16
/sites/...CCPA and CPRA 16
/sites/...NY SHIELD Act 16
Categories
GDPR
175
PII
158
Federal
132
Financial
4
PCI
4

Athena AI

Athena AI provides two powerful generative AI capabilities: AI SOC Analyst and Natural Language Search for conducting in-depth investigations and analysis more efficiently, decreasing time to resolution, and getting to the root cause of alerts faster. This transforms users of all skill levels into formidable defenders.

In the Alert page, you can click the robot icon 

on the right to use the AI chat pane.



In Events and Resources Analytics, you can click the robot  icon for natural language search.



After clicking Send , the filters successfully resolved by the AI engine will be displayed and will part of the coming search.



Management

The Management options include:

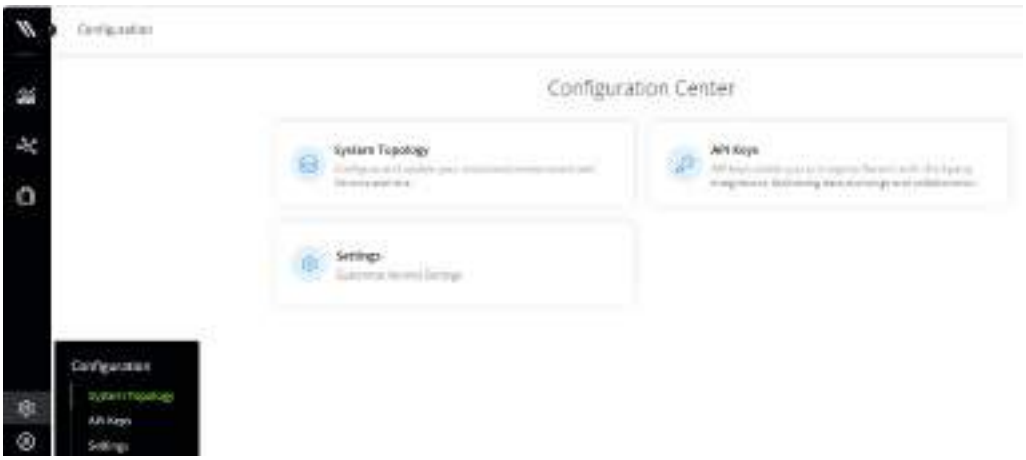
- Policies - For automatic remediation of risk in your environment. See Threat Detection Policies and Working with Automations.
- Action Center - For viewing and tracking the execution progress of actions generated by your policies. This includes operations waiting for review and approval, operations waiting to be performed, operations currently running, and operations that have completed their run.
- Scheduled Searches - For viewing existing scheduled searches, creating new scheduled searches, and performing actions on single or multiple scheduled searches.
- Flags - For assigning flags that can be used to filter searches or to group results.
- System Health - For viewing up-to-date information about your system's health and monitoring the classification and labeling coverage in your scanned environment.



Configuration

The Configuration Center page includes the following options:

- System Topology - For installing your Collectors and scheduling their upgrade.
- API Keys - For configuring Varonis integrations, starting with Palo Alto Cortex XSOAR Integration.
- Settings - Allow you to configure additional product areas:
  - Staleness Threshold - Customize the staleness threshold period of resources and accounts.
  - Response Scripts - Configure the dedicated directory for storing all scripts for Varonis threat detection policy script execution.
  - Generative AI - For enabling Athena AI, you need to agree to the Generative AI Terms and Conditions. Before initial use, you can also enable Athena AI through the features (Alert page for AI Assisted SOC and Events and Resources Analytics for Search AI).
  - Notifications - Choose whether to allow email notifications for system health issues, which are enabled by default and sent to your enterprise admin. You can also customize the notification recipients.



7 PRODUCT TRUST AND SECURITY

Organizations are adopting cloud solutions for the flexibility and productivity gains they offer. The increased efficiency can bear increased risk. At Varonis, we take our software development and security practices seriously. We refine and share our security practices so that customers can trust in our solutions and practices. Varonis is a pioneer in data security and analytics specializing in data protection, threat detection and response, and compliance. Varonis adopts a risk-based approach for its information security management system (ISMS). This approach requires identifying, assessing, and appropriately mitigating vulnerabilities and threats to information assets. Deploying an ISMS reduces the risk of unauthorized, accidental, or intentional information disclosure, modification, or destruction.

The Varonis security program is based on industry-leading best practices. Along with third-party penetration tests, Varonis uses dynamic application testing and automated scanning to continually validate our software's security.

For more information, visit the Varonis Trust & Security website.

CERTIFICATE

This is to certify that the Security Techniques Cloud Services of

VARONIS SYSTEMS INC.

1250 Broadway, New York, NY, USA 10001

Has been assessed and complies with the requirements of :

ISO/IEC 27017:2015 Best Practices

This Certificate is Applicable to

Development, research, delivery of software support and professional services, delivery of cloud-based software solutions, sales, training, project management, design and planning of risk assessment, protection of information systems, security of corporate and cloud networks.

Initial Approval:	22/05/2018		
Valid From:	22/05/2024	**Revised:**	21/05/2024
Valid Until:	22/05/2027	**Certificate No.:**	97592

SII-QCD assumes no liability to any party other than the client, and then only in accordance with the agreed upon Certification Agreement.
This certificate's validity is subject to the organization maintaining their system in accordance with SII-QCD requirements for system certification. The continued validity may be verified via scanning the code with a smartphone, or via website www.sii.org.il. This certificate remains the property of SII-QCD.

Dr. Gilad Golub
CEO

Avital Weinberg
Director, Quality & Certification Division

THE STANDARDS INSTITUTION OF ISRAEL

The standards institution of Israel
42 Chaim Levanon St.
Tel-Aviv 6997701

Annex to Certificate of Registration no. 97592

VARONIS SYSTEMS INC.

1250 Broadway, New York, NY, USA 10001

With Additional Sites At:

North Carolina - Varonis Systems Inc.
3300 Paramount Parkway, Suite 300, Morrisville NC 27560

Portland
2175 NW Raleigh St., Suite 110 Office 2029 Portland, OR 97210

Arizona
4343 N Scottsdale Rd Suite 180 Scottsdale, AZ 85251

Federal Sales (US)
Two Fountain Square, 11921 Freedom Drive, Reston VA 20190

France
LE Colisee Gardens, Bariment C, 9eme etage 8-14 Avenue de l'Arche, 92400 Courbevoie, France

United Kingdom
Salisbury House, 29 Finsbury Circus, London UK C2M 7AQ

Germany
Kronstadter Str. 4, Munich Bayern 81677 Germany

Israel
5 Arie Shenkar Street, Gav-Yam Bldg 1, Herzliya Israel 4672505

Initial Approval:	22/05/2018		
Valid From:	22/05/2024	**Revised:**	21/05/2024
Valid Until:	22/05/2027	**Certificate No.:**	97592

Dr. Gilad Golub
CEO

Avital Weinberg
Director, Quality & Certification Division

October 20, 2026 11:32 UTC

The standards institution of Israel
42 Chaim Levanon St.
Tel-Aviv 6997701

Ireland
Penrose Two, Penrose Dock Cork T23 YY09, Ireland

Netherlands
Saturnusstraat 46-62, 2132 HB Hoofddorp, The Netherlands

Luxembourg
Livange, Luxembourg sud 1, Rue de Turi, L3378 Livange, Luxembourg

Australia
276 Flinders Street, level 7 Melbourne, VIC 3000 Australia

October 20, 2026 11:32 UTC

Initial Approval:	22/05/2018		
Valid From:	22/05/2024	**Revised:**	21/05/2024
Valid Until:	22/05/2027	**Certificate No.:**	97592

Dr. Gilad Golub
CEO

Avital Weinberg
Director, Quality & Certification Division

The standards institution of Israel
42 Chaim Levanon St.
Tel-Aviv 6997701

CERTIFICATE

This is to certify that the
ISMS which supports the protecting of PII in public clouds of

VARONIS SYSTEMS INC.

1250 Broadway, New York, NY, USA 10001

Has been assessed and complies with the requirements of :

ISO/IEC 27018:2019 Best Practices

This Certificate is Applicable to

Development, research, delivery of software support and professional services, delivery of cloud-based software solutions, sales, training, project management, design and planning of risk assessment, protection of information systems, security of corporate and cloud networks.

Initial Approval:	16/04/2019		
Valid From:	22/05/2024	**Revised:**	21/05/2024
Valid Until:	22/05/2027	**Certificate No.:**	113358

SII-QCD assumes no liability to any party other than the client, and then only in accordance with the agreed upon Certification Agreement.
This certificate's validity is subject to the organization maintaining their system in accordance with SII-QCD requirements for system certification. The continued validity may be verified via scanning the code with a smartphone, or via website www.sii.org.il. This certificate remains the property of SII-QCD.

Dr. Gilad Golub
CEO

Avital Weinberg
Director, Quality & Certification Division

THE STANDARDS INSTITUTION OF ISRAEL

The standards institution of Israel
42 Chaim Levanon St.
Tel-Aviv 6997701

Annex to Certificate of Registration no. 113358

VARONIS SYSTEMS INC.

1250 Broadway, New York, NY, USA 10001

With Additional Sites At:

North Carolina - Varonis Systems Inc.
3300 Paramount Parkway, Suite 300, Morrisville NC 27560

Portland
2175 NW Raleigh St., Suite 110 Office 2029 Portland, OR 97210

Arizona
4343 N Scottsdale Rd Suite 180 Scottsdale, AZ 85251

Federal Sales (US)
Two Fountain Square, 11921 Freedom Drive, Reston VA 20190

France
LE Colisee Gardens, Bariment C, 9eme etage 8-14 Avenue de l'Arche, 92400 Courbevoie, France

United Kingdom
Salisbury House, 29 Finsbury Circus, London UK C2M 7AQ

Germany
Kronstadter Str. 4, Munich Bayern 81677 Germany

Israel
5 Arie Shenkar Street, Gav-Yam Bldg 1, Herzliya Israel 4672505

Initial Approval:	16/04/2019		
Valid From:	22/05/2024	**Revised:**	21/05/2024
Valid Until:	22/05/2027	**Certificate No.:**	113358

Dr. Gilad Golub
CEO

Avital Weinberg
Director, Quality & Certification Division

October 20, 2026 1:33 UTC

The standards institution of Israel
42 Chaim Levanon St.
Tel-Aviv 6997701

THE STANDARDS INSTITUTION OF ISRAEL

Ireland
Penrose Two, Penrose Dock Cork T23 YY09, Ireland

Netherlands
Saturnusstraat 46-62, 2132 HB Hoofddorp, The Netherlands

Luxembourg
Livange, Luxembourg sud 1, Rue de Turi, L3378 Livange, Luxembourg

Australia
276 Flinders Street, level 7 Melbourne, VIC 3000 Australia

October 20, 2026 11:33 UTC

Initial Approval:	16/04/2019		
Valid From:	22/05/2024	**Revised:**	21/05/2024
Valid Until:	22/05/2027	**Certificate No.:**	113358

Dr. Gilad Golub
CEO

Avital Weinberg
Director, Quality & Certification Division

The standards institution of Israel
42 Chaim Levanon St.
Tel-Aviv 6997701

CERTIFICATE

This is to certify that the Privacy information management system of

VARONIS SYSTEMS INC.

1250 Broadway, New York, NY, USA 10001

Has been assessed and complies with the requirements of :

ISO/IEC 27701:2019

This Certificate is Applicable to

Development, research, delivery of software support and professional services, delivery of cloud-based software solutions, sales, training, project management, design and planning of risk assessment, protection of information systems, security of corporate and cloud networks.

Initial Approval:	11/07/2021		
Valid From:	22/05/2024	**Revised:**	21/05/2024
Valid Until:	22/05/2027	**Certificate No.:**	115022

SII-QCD assumes no liability to any party other than the client, and then only in accordance with the agreed upon Certification Agreement.
This certificate's validity is subject to the organization maintaining their system in accordance with SII-QCD requirements for system certification. The continued validity may be verified via scanning the code with a smartphone, or via website www.sii.org.il. This certificate remains the property of SII-QCD.

Dr. Gilad Golub
CEO

Avital Weinberg
Director, Quality & Certification Division

THE STANDARDS INSTITUTION OF ISRAEL

The standards institution of Israel
42 Chaim Levanon St.
Tel-Aviv 6997701

Annex to Certificate of Registration no. 115022

VARONIS SYSTEMS INC.

1250 Broadway, New York, NY, USA 10001

With Additional Sites At:

North Carolina - Varonis Systems Inc.
3300 Paramount Parkway, Suite 300, Morrisville NC 27560

Portland
2175 NW Raleigh St., Suite 110 Office 2029 Portland, OR 97210

Arizona
4343 N Scottsdale Rd Suite 180 Scottsdale, AZ 85251

Federal Sales (US)
Two Fountain Square, 11921 Freedom Drive, Reston VA 20190

France
LE Colisee Gardens, Bariment C, 9eme etage 8-14 Avenue de l'Arche, 92400 Courbevoie, France

United Kingdom
Salisbury House, 29 Finsbury Circus, London UK C2M 7AQ

Germany
Kronstadter Str. 4, Munich Bayern 81677 Germany

Israel
5 Arie Shenkar Street, Gav-Yam Bldg 1, Herzliya Israel 4672505

Initial Approval:	11/07/2021		
Valid From:	22/05/2024	**Revised:**	21/05/2024
Valid Until:	22/05/2027	**Certificate No.:**	115022

Dr. Gilad Golub
CEO

Avital Weinberg
Director, Quality & Certification Division

October 20, 2026 1:35 UTC

THE STANDARDS INSTITUTION OF ISRAEL
The standards institution of Israel
42 Chaim Levanon St.
Tel-Aviv 6997701

THE STANDARDS INSTITUTION OF ISRAEL

Ireland
Penrose Two, Penrose Dock Cork T23 YY09, Ireland

Netherlands
Saturnusstraat 46-62, 2132 HB Hoofddorp, The Netherlands

Luxembourg
Livange, Luxembourg sud 1, Rue de Turi, L3378 Livange, Luxembourg

Australia
276 Flinders Street, level 7 Melbourne, VIC 3000 Australia

October 20, 2026 11:35 UTC

Initial Approval:	11/07/2021		
Valid From:	22/05/2024	**Revised:**	21/05/2024
Valid Until:	22/05/2027	**Certificate No.:**	115022

Dr. Gilad Golub
CEO

Avital Weinberg
Director, Quality & Certification Division

The standards institution of Israel
42 Chaim Levanon St.
Tel-Aviv 6997701

Nº ITEM
6 –
6.1 –
6.1.1 –
6.1.2 –
6.1.3 –
6.1.4 –
6.1.5 –
6.1.6 –
6.1.7 –
6.1.8 –
6.1.9 –
6.1.10 –
6.1.11 –
6.1.12 –
6.1.13 –
6.2 –

6.2.1 –
6.2.2 –
6.2.3 –
6.2.4 –
6.2.5 –
6.2.6 –
6.2.7 –
6.2.8 –
6.2.9 –
6.2.9.1 –
6.2.9.2 –
6.2.9.3 –
6.2.9.4 –
6.2.9.5 –
6.2.9.6 –
6.2.9.7 –

6.2.9.8 –
6.2.9.9 –
6.2.9.10 –
6.2.9.11 –
6.2.9.12 –
6.2.9.13 –
6.2.9.14 –
6.2.9.15 –
6.2.10 –
6.2.10.1 –
6.2.10.2 –
6.2.10.3 –
6.2.10.4 –
6.2.10.5 –
6.2.10.6 –
6.2.10.7 –
6.2.10.8 –
6.2.10.9 –
6.2.10.10 –
6.2.10.11 –
6.2.10.12 –
6.2.10.13 –
6.2.10.14 –

6.2.10.15 –
6.2.10.16 –
6.2.10.17 –
6.2.10.18 –
6.2.11 –
6.2.12 –
6.2.13 –
6.2.14 –
6.2.15 –
6.2.16 –
6.2.17 –
6.2.18 –
6.2.19 –

6.2.20 –
6.2.21 –
6.2.22 –
6.2.23 –
6.2.24 –
6.2.25 –
6.2.26 –
6.2.27 –
6.2.28 –
6.2.29 –
6.2.30 –

6.2.31 –
6.2.32 –
6.2.33 –
6.2.34 –
6.2.35 –
6.2.35.1 –
6.2.35.2 –
6.2.35.3 –
6.2.35.4 –
6.2.35.5 –
6.2.35.6 –
6.2.35.7 –
6.2.35.8 –
6.2.35.9 –
6.2.35.10 –
6.2.35.11 –
6.2.36 –
6.2.37 –
6.2.38 –

6.2.39 –
6.2.40 –
6.2.41 –
6.2.42 –
6.2.43 –
6.2.44 –
6.2.45 –
6.2.46 –
6.2.47 –
6.2.48 –
6.2.49 –
6.2.50 –
6.2.51 –
6.2.52 –
6.2.53 –
6.2.54 –

6.2.55 –
6.2.56 –
6.2.57 –
6.2.58 –
6.2.59 –
6.2.60 –
6.2.61 –
6.2.62 –
6.2.63 –
6.2.64 –
6.2.65 –
6.2.66 –
6.2.67 –
6.2.68 –
6.2.69 –
6.3 –
6.3.1 –
6.3.2 –
6.3.3 –
6.3.3.1 –

6.3.3.2 –
6.3.3.3 –
6.3.3.4 –
6.3.3.5 –
6.3.3.6 –
6.3.3.7 –
6.3.3.8 –
6.3.3.9 –
6.3.3.10 –
6.3.3.11 –
6.3.3.12 –
6.3.3.13 –
6.3.3.14 –
6.3.3.15 –
6.3.3.16 –
6.3.3.17 –
6.3.3.18 –
6.3.3.19 –
6.3.3.20 –
6.3.3.21 –
6.3.3.22 –
6.3.3.23 –
6.3.3.24 –

6.3.3.25 –
6.3.3.26 –
6.3.3.27 –
6.3.3.28 –
6.3.3.29 –
6.3.3.30 –
6.3.3.31 –
6.3.4 –
6.3.4.1 –
6.3.4.2 –
6.3.4.3 –
6.3.4.4 –
6.3.4.5 –
6.3.4.6 –
6.3.4.7 –
6.3.4.8 –
6.3.4.9 –
6.3.4.10 –
6.3.4.11 –

6.3.4.12 –
6.3.4.13 –
6.3.4.14 –
6.3.4.15 –
6.3.4.16 –
6.3.4.17 –
6.3.4.18 –
6.3.4.19 –
6.3.4.20 –
6.3.4.21 –
6.3.4.22 –
6.3.4.23 –
6.3.4.24 –
6.3.4.25 –
6.3.4.26 –
6.3.4.27 –

6.3.4.28 –
6.3.4.29 –
6.3.4.30 –
6.3.4.31 –
6.3.4.32 –
6.3.4.33 –
6.3.4.34 –
6.3.4.35 –
6.3.4.36 –
6.3.4.37 –
6.3.4.38 –
6.3.4.39 –
6.3.4.40 –
6.3.4.41 –
6.3.4.42 –
6.3.4.43 –

6.3.4.44 –
6.3.4.45 –
6.3.4.46 –
6.3.4.47 –
6.3.4.48 –
6.3.5 –
6.3.6 –
6.3.7 –
6.3.8 –
6.3.9 –
6.3.10 –
6.3.11 –
6.3.12 –
6.3.13 –

6.3.14 –
6.3.15 –
6.3.16 –
6.3.17 –
6.3.18 –
6.3.19 –
6.3.20 –
6.3.21 –
6.3.22 –
6.3.23 –
6.3.24 –
6.3.24.1 –
6.3.24.2 –

6.3.24.3 –
6.3.24.4 –
6.3.24.5 –
6.3.24.6 –
6.3.25 –
6.3.26 –
6.3.27 –
6.3.28 –
6.3.29 –
6.3.30 –
6.3.31 –
6.3.32 –

6.3.33 –
6.3.34 –
6.3.35 –
6.3.36 –
6.3.37 –
6.3.38 –
6.3.39 –

ITEM
ESPECIFICAÇÕES TÉCNICAS
Considerações Gerais
Visando preservar harmonia entre todos os elementos da solução, a total interoperabilidade de componentes e a facilidade de uso e operação, a solução de auditoria deverá ser de um único fabricante;
A solução deve disponibilizar console web ou cliente que poderá ser acessada através do servidor de aplicação e estações de trabalho dos usuários com acesso autorizado;
A solução deverá possibilitar integração, de forma direta ou indireta, de suas informações com sistemas de DLP (Data Lost Prevention) e SIEM.
Caso seja necessária instalação de qualquer agente nos servidores a serem monitorados, o processo não deve impactar na disponibilidade dos servidores ou serviços;
O agente deve possuir um mecanismo de monitoramento de desempenho dos servidores onde atua, de modo a não permitir que o nível de consumo de recursos ultrapasse limites definidos e configuráveis;
A solução deve oferecer a possibilidade de configurações de diferentes níveis de segurança às suas funcionalidades, podendo, desta forma, ser utilizada por diferentes equipes com variadas demandas de atividades e com acesso restrito a diferentes funções;
Devido às características e criticidade das informações coletadas, armazenadas e processadas, com o intuito de garantir integridade e confiabilidade jurídica, contratual e regulatória, e pela possibilidade das informações serem utilizadas para perícia forense inclusive como provas judiciais, a solução deverá ter certificação utilizada pela administração pública como parâmetro para definição de requisitos de sistema de gerenciamento de segurança da informação como a ISO/IEC 27001 ou similares;
A solução deve suportar a utilização de servidores virtualizados para os componentes;
A solução deve possibilitar a configuração de credencial diferente para cada servidor/serviço a ser monitorado;
A solução deverá fazer recomendações de melhores práticas a serem aplicadas no ambiente;
A solução deverá ser entregue como serviço na nuvem, sendo toda infraestrutura disponibilizada pelo fabricante. Caso a solução necessite de uma probe/coletor de dados no ambiente local, deve ser compatível com o ambiente virtualizado do órgão;
Toda a infraestrutura da nuvem deve ser gerenciada pelo fabricante, incluindo, mas não se limitando a: Manutenção do ambiente, atualizações aplicadas de forma transparente, pacotes de correções e novas features aplicadas direto no produto e sem nenhum tipo de impacto;
O fabricante deverá disponibilizar um time de resposta a incidentes para auxiliar em caso de investigação de algum incidente ou alguma suspeita de um alerta crítico que possa ter sido gerado no ambiente;
Estrutura LOCAL (on-premise)

A solução deverá monitorar múltiplos domínios do Active Directory e servidores de arquivos Windows e NAS (Network Attached Storage) e Linux do ambiente, incluindo: Contas, estruturas de diretórios, permissões e eventos;
A solução deverá suportar no mínimo, para servidores de arquivos, Windows server 2012 ou superior e Linux para no mínimo as seguintes distribuições: Red Hat Enterprise Linux em todas as suas versões ativas, SUSE Linux Enterprise Server Versão 15 SP2 LTSS e 15 SP3.
A solução deve permitir uma pré-visualização das alterações de permissionamento pretendidas de maneira gráfica antes da aplicação em produção. Esta pré-visualização deve demonstrar os impactos nos grupos e usuários em relação a suas permissões nos diretórios monitorados;
A solução deve fornecer a visibilidade sobre aplicações de alteração que estão pendentes e o histórico das alterações aplicadas através da console;
Caso a solução necessite da instalação de agente para o monitoramento dos eventos do Active Directory e servidores de arquivos, os agentes não devem gerar nenhuma queda de performance nos servidores;
O gerenciamento da solução deverá ser centralizado para todos os módulos;
A solução deverá monitorar todos os domain controllers instalados em qualquer versão do Windows Server 2003 ou superior;
A solução deverá monitorar todos os servidores de arquivos instalados em Windows Server 2012 ou superior;
A solução deverá monitorar no mínimo, os seguintes eventos do Microsoft Active Directory:
Conta habilitada e desabilitada ;
Autenticação de conta (TGT) ;
Renovação de acesso (TGS) ;
Replicação de AD ;
Logon de conta no DC;
Criação, deleção, renomeação, modificação, remoção e adição de membros no objeto do DS;
Requisição de acesso NTLM;

Alteração de senha de usuário;
Conta de usuário bloqueada;
Conta de usuário desbloqueada;
Netlogon vulnerável;
Criação, deleção e modificação de GPO;
Tentativa de reset de senha;
Criação, atualização, deleção, habilitação e desabilitação de tarefa agendada dentro do DC;
Alteração de política de kerberos.
A solução deverá monitorar no mínimo, os seguintes eventos do servidor de Arquivos Windows:
Arquivo criado;
Arquivo deletado;
Arquivo aberto;
Arquivo renomeado;
Arquivo modificado;
Mudança de proprietário do arquivo;
Permissões adicionadas no arquivo;
Permissões removidas no arquivo;
Proteção adicionado no arquivo;
Proteção removida no arquivo;
Pasta criada;
Pasta deletada;
Pasta renomeada;
Mudança de proprietário da pasta;

Permissões adicionadas na pasta;
Permissões removidas na pasta;
Proteção adicionada na pasta;
Proteção removida na pasta;
Deverá ser possível definir os proprietários das pastas através da console;
A solução deverá exibir uma lista com todas as contas de usuários monitoradas, indicando no mínimo, o tipo de conta (seviço, executiva ou administrativa) e grupos que fazem parte;
A solução deverá exibir o repositório monitorado em formato hierarquico, expandindo as pastas e sub-pastas até o nível do arquivo, permitindo a visualização de quais usuários tem acesso a cada recurso e as permissões concedidas;
A solução deverá possuir uma visão bi-direcional indicando através de uma visualização gráfica e interativa, todas as permissões dos usuários e grupos, e quais as permissões aplicadas nos objetos (arquivos e pastas);
A solução deverá disponibilizar a visibilidade de permissões, sejam elas NTFS ou share;
A solução deverá realizar a classificação do conteúdo do arquivo, fornecendo visibilidade sobre onde residem os dados confidenciais e sensíveis no sistema de arquivos;
A solução deverá utilizar múltiplos fatores para realizar a classificação do conteúdo do arquivo, incluindo: Metadados, padrões, dicionários, palavras-chave e expressão regular;
A solução deverá indicar para qualquer arquivo e pasta no servidor monitorado, uma visualização gráfica contendo o nível de exposição e indicando se o arquivo é sensível ou não a partir da classificação realizada;
A solução deverá fornecer filtros para visualizar apenas determinados objetos de dados em exibição gráfica interativa, incluindo pastas protegidas e pastas únicas;

A solução deverá incluir informações de classificação de dados na tela das permissões, incluindo: nome da regra classificada, e quantidade de instâncias sensíveis encontradas no arquivo;
A solução deverá fornecer para as permissões, tipos de exibição diferentes, incluindo exibições hierárquicas e de lista;
A solução deverá realizar a classificação de imagens através de OCR ou tecnologia similar;
A solução deverá possibilitar a criação de regras customizadas para que os administradores possam definir o que deve ser encontrado dentro do conteúdo do arquivo, de acordo com a necessidade organizacional;
Deve ser possível exportar eventos e informações apenas referente aos dados classificados como sensíveis;
Deve ser possível definir o escopo do ambiente que vai ser classificado, podendo definir: repositório, arquivo, pasta, tipo de arquivo, quantidade mínima de hits e outros;
A solução deverá permitir a análise dos arquivos classificados, indicando dentro do conteúdo do arquivo exatamente o que foi encontrado de dado sensível e confidencial;
A solução deverá auxiliar na conformidade com a LGPD, identificando aonde os dados pessoais (CPF,RG,CNH e outros) são armazenados, quem tem acesso aos dados e quais são as atividades em cima destes dados;
A solução deverá escanear e classificar no mínimo os seguintes tipos de arquivos: doc, docx, dwg, rtf, ppt, xls, txt, csv, pdf, xml, log, eml, jpg, jpeg, gif, png, rar e zip;
A solução deverá encontrar em arquivos com formato tabular, palavras-chave em cabeçalhos e colunas;
A solução deverá indicar no painel de diretórios: o nome da regra, a quantidade de hits do termo sensível encontrado nos arquivos e pastas e a quantidade de hits incluindo sub-pastas;

A solução deverá notificar os administradores através de alertas para qualquer tipo de atividade incomum e comportamentos suspeitos de usuários;
Os alertas da solução deverão ser encaminhados via SMTP e SNMP;
A solução deverá suportar a configuração de respostas automáticas para os alertas gerados, possibilitando a execução automática de scripts ou comandos pré-configurados;
A solução deverá realizar a análise comportamental dos usuários de forma automática, através de machine learning, entendendo o comportamento e rotina de todos os usuários, o que acessam, quando acessam e onde;
A solução deverá contemplar a assinatura de uma base de conhecimentos do fornecedor com mais de 150 modelos de alertas pré-configurados de eventos suspeitos tais como:
Ataques de sequestro de dados (ransomware);
Detecção de ferramentas nocivas ao ambiente;
Ações com acessos negados;
Ações de escalações de privilégios;
Excesso de tentativas de autenticação ou contas bloqueadas;
Atividades suspeitas em dados parados e/ou inativos;
Alterações anormais em GPO;
Ataques de golden ticket;
Ataques de injeção de códigos maliciosos;
Ataques de decoberta de contas com NTLM e Kerkeros;
Ataques de força bruta.
Os modelos de alertas devem ser atualizados de forma automática;
A solução deverá detectar ameaças em todos os estágios de um ataque cibernético, incluindo dashboard que indica algumas categorias como: Reconhecimento, intrusão, exploração, escalação de privilégio, movimento lateral, negação de serviço e exfiltração de dados;
A solução deverá monitorar a atividade do usuário para construir perfis de comportamento e usar os modelos de ameaça baseados em comportamento para alertar quando uma atividade anormal no Active Directory é detectada;

A solução deverá construir perfis de comportamento comparando as atividades dos usuários e entidades e identificando a relação entre eles;
A solução deverá possuir um período de aprendizado, para que seja feito a coleta de eventos e identificação do comportamento dos usuários para a criação do perfil comportamental;
A solução deverá realizar a descoberta de contas privilegiadas de forma automática, identificando contas executivas, contas de serviço e contas administrativas baseado no seu comportamento e nos grupos de segurança que a conta está inserida;
A solução deverá possuir dashboard de alertas indicando os usuários mais alertados, dispositivos e modelos de alertas gerados;
A solução deverá possuir política de automação para remediação de exposição de dados para toda a organização, removendo as permissões globais das pastas e arquivos;
A solução deverá possuir política de automação para remediar permissões inconsistentes, garantindo que não exista permissão quebrada e aplicando as entradas de permissão corretamente para as sub-pastas e arquivos;
As políticas de automação para remediação devem ser executadas de forma manual e automática;
A solução deverá suportar na busca dos eventos a utilização de operadores relativos, auxiliando na investigação e nos resultados esperados;
Deve ser possível salvar uma pesquisa customizada, agendando para que ela possa ser executada de forma automática e que os administradores recebam as informações necessárias de forma periódica;
A solução deverá suportar a criação e utilização de flags para serem aplicadas as contas de usuários e aos recursos monitorados, essas flags podem ser utilizadas nos filtros e na aba de eventos;
A solução deverá identificar dados que não foram acessados por um período de tempo, podendo especificar a quantidade de dias desejado;
A solução deverá disponibilizar dashboard das informações correlacionadas dos dados do Active Directory, com painéis, indicando no mínimo: Usuários com senha que nunca expira, contas de usuários obsoletas, contas executivas, contas desabilitadas e contas habilitadas com a senha expirada;
A solução deverá disponibilizar dashboard com painéis dos dados correlacionados dos servidores de arquivos Windows, indicando no mínimo: Arquivos sensíveis expostos para toda organização, pastas expostas, permissões obsoletas, permissões direta nas pastas, pastas com permissões inconsistentes e pastas com dados obsoletos;
Deve ser possível comparar os gráficos do dashboard através da console, indicando a diferença dos valores atuais com o período anterior;
Os widgets devem ser configuráveis e customizáveis, podendo alterar o modo de visualização, para alguns tipos, como: widgets de métrica única, widgets de porcentagem e widgets com linha do tempo;
A solução deverá possuir Widget de geolocalização com mapa indicando a origem da ação para os alertas gerados;

A solução deverá possuir uma tela de visualização de eventos, podendo realizar pesquisas e filtros à cerca de todas as atividades e dados do ambiente.
Todos os eventos podem ser filtrados e organizados no mínimo por: tipo de evento, ID do evento, operação, status e plataforma;
Deve ser possível definir uma data e horário para busca dos eventos;
A solução deverá possuir filtro para última atividade registrada do usuário,facilitando a busca de contas que estão atualmente inativas;
A solução deverá fornecer relatório dos níveis de exposição das permissões, no contexto de dados sensíveis para qualquer pasta e arquivo;
A solução deverá fornecer relatório das permissões, incluindo dados da classificação;
A solução deverá fornecer relatório das atividades de acesso dos usuários aos arquivos e pastas;
A solução deverá fornecer relatório dos resultados da classificação dos dados, incluindo o número de hit e regra classificada;
A solução deverá fornecer relatório dos dados que estão com permissões de grupos globais e quem está utilizando estas permissões para acessar as informações;
A solução deverá fornecer relatório para SID não resolvido em ACLs;
A solução deverá fornecer relatório sobre grupos de segurança não utilizados ou vazios;
A solução deverá fornecer relatório para usuários desabilitados;
Deve ser possível exportar o relatório em no mínimo 3 tipos de formatos: CSV,Excel e PDF;
Deverá ser possível realizar o agendamento de relatórios;
Deverá ser possível encaminhar o relatório apenas para o propietário do dado;
Estrutura em NUVEM
A solução deverá contemplar o monitoramento de repositórios em nuvem Google Workspace OU Microsoft Sharepoint Online e OneDrive, devendo a CONTRATANTE definir qual módulo irá adquirir no momento do pedido de entrega.
Para ambientes Microsoft, a solução deverá suportar todas as funcionalidades descritas no item 2 para os repositórios de nuvem corporativa: Microsoft Sharepoint Online e OneDrive, correlacionando identidades com privilégios, atividades, reduzindo riscos e acelerando investigações;
A solução deverá monitorar, no mínimo, os seguintes eventos do Entra ID:
Conta desativada;

Conta ativada;
Aplicativo adicionado;
Consentimento do aplicativo aprovado;
Consentimento do aplicativo removido;
Proprietário do aplicativo adicionado;
Proprietário do aplicativo removido;
Aplicativo removido;
Aplicativo atualizado;
Dispositivo adicionado;
Proprietário do dispositivo adicionado;
Proprietário do dispositivo removido;
Usuário registrado do dispositivo adicionado;
Usuário registrado do dispositivo removido;
Dispositivo removido;
Dispositivo atualizado;
Grupo adicionado;
Grupo excluído;
Conjunto de licenças de grupo;
Membro do grupo adicionado;
Membro do grupo removido;
Proprietário do grupo adicionado;
Proprietário do grupo removido;
Grupo atualizado login;

Função do membro adicionada;
Função do membro removida;
Usuário adicionado;
Usuário excluído;
Usuário convidado para a organização;
Licença de usuário alterada;
Usuário restaurado e Usuário atualizado;
A solução deverá monitorar, no mínimo, os seguintes eventos do Sharepoint Online e OneDrive:
Malware detectado no arquivo;
Solicitação de acesso a arquivos aprovada;
Arquivo copiado;
Arquivo excluído;
Arquivo baixado para uma pasta local sincronizada;
Arquivo baixado;
Convite de arquivo aceito;
Convite de arquivo cancelado;
Convite de arquivo criado;
Convite de arquivo atualizado;
Arquivo modificado;

Arquivo movido;
Arquivo aberto;
Arquivo renomeado;
Arquivo restaurado;
Link compartilhado de arquivo criado;
Link compartilhado do arquivo removido;
Link compartilhado do arquivo atualizado;
Link compartilhado do arquivo usado;
Arquivo enviado;
Arquivo enviado de uma pasta local sincronizada;
Solicitação de acesso à pasta aprovada;
Pasta copiada;
Pasta criada;
Pasta excluída;
Convite de pasta aceito;
Convite de pasta cancelado;

Convite de pasta criado;
Convite de pasta atualizado;
Pasta movida;
Pasta renomeada;
Pasta restaurada;
Link compartilhado da pasta criado;
Link compartilhado da pasta removido;
Link compartilhado da pasta atualizado;
Link compartilhado da pasta usado;
Grupo adicionado;
Grupo excluído;
Membro do grupo adicionado;
Membro do grupo removido;
Permissões adicionadas;
Herança de permissão quebrada;
Herança de permissão restaurada;

Permissões removidas;
Administrador do conjunto de sites adicionado;
Administrador do conjunto de sites removido;
Mudança geográfica do site agendada;
Mudança geográfica do site concluída;
A solução deverá possuir uma visão bidirecional das permissões dos repositórios de nuvem, podendo clicar em um recurso para ver quem tem acesso a ele ou filtrar um usuário/grupo e validar todo o seu acesso de acordo com os repositórios monitorados;
A solução deverá fornecer uma visão gráfica interativa dos níveis de exposição de permissões (interna, externa, convidado, em toda a organização, qualquer pessoa) no contexto com dados confidenciais para qualquer arquivo, pasta e site no SharePoint Online e OneDrive ou Google Workspace;
A solução deverá monitorar e detectar quando um usuário realizar o login no M365 ou Google Workspace de um país novo ou país incomum;
A solução deverá suportar a configuração de gatilhos pré-definidos para incidentes de segurança e alertas com base em políticas definidas para links de compartilhamento público e em toda a organização que expõe dados confidenciais;
A solução deverá monitorar e normalizar a atividade do usuário, criando um perfil comportamental, baseado nas suas atividades, gerando alertas para acessos anormais à dados sensíveis e dados parados;
A solução deverá monitorar a atividade do usuário para construir perfis de comportamento e usar os modelos de ameaça baseados em comportamento para alertar atividades em risco ou incomuns no M365 ou Google Workspace;
A solução deverá fornecer alerta para links de compartilhamento público e em toda a organização que expõe dados sensíveis;
A solução deverá fornecer alerta para atividades suspeita em pastas e arquivos;
A solução deverá fornecer alerta para mudanças de membros em grupos privilegiados;

A solução deverá detectar e alertar de forma automática, atividades que correspondem a possíveis ameaças cibernéticas e padrões de ataques comuns;
A solução deverá fornecer alerta para acessos anormais a dados sensíveis baseado no comportamento do usuário;
A solução deverá fornecer uma visão gráfica e interativa dos links de compartilhamento do Microsoft 365 ou Google Workspace em contexto com sensibilidade e desatualização;
A solução deverá realizar a classificação dos arquivos hospedados nos repositórios de nuvem suportados;
A solução deverá auxiliar na conformidade com a LGPD, identificando aonde os dados pessoais (CPF,RG,CNH e outros) são armazenados, quem tem acesso aos dados e quais são as atividades em cima destes dados;
A solução deverá permitir a configuração dos tipos de arquivos que serão escaneados e a definição do tamanho do arquivo;
A varredura para classificação dos arquivos deve acontecer de forma contínua para qualquer tipo de dado armazenado nos repositórios monitorados na nuvem;
A solução deverá permitir a análise dos arquivos classificados, indicando dentro do conteúdo do arquivo exatamente o que foi encontrado de dado sensível e confidencial;
A solução deverá realizar a varredura de classificação de forma incremental, monitorando as atividades dos arquivos e executando a varredura apenas para os dados que foram atualizados ou tiveram alguma alteração;
A solução deverá possibilitar a revisão das políticas de automação antes de serem aplicadas, com fluxo de aprovação, para que os usuários que tenham permissão, possam aprovar a execução da política;
A solução deverá remediar de forma automatizada:
Links de colaboração que expõe dados sensíveis;
links de colaboração que expõe dados externamente ou publicamente;

links de colaboração que expõe dados para toda a organização;
links de colaboração obsoletos;
permissões diretas;
permissões diretas obsoletas.
A solução deverá permitir a customização das políticas de remediação, podendo ser agendadas ou executadas de forma manual, baseado em sensibilidade, utilização, tipo de link e outros;
A solução deverá disponibilizar dashboard de informações dos alertas verificados, com gráficos e painéis de usuários desatualizados com funções administrativas, associações desatualizadas em grupos, grupos públicos e muito mais;
A solução deverá disponibilizar dashboard do SharePoint Online, com painéis para visualização de permissões obsoletas, exposição de sites, exposição de arquivos, exposição de pastas e membros de grupos obsoletos;
A solução deverá disponibilizar dashboard do OneDrive, com painéis para visualizar arquivos expostos, arquivos sensíveis obsoletos, permissões obsoletas, links de colaboração;
A solução deverá fornecer relatórios e painéis que mostram onde os dados confidenciais estão concentrados e expostos na nuvem, e onde você pode remover o acesso desnecessário para obter conformidade e manter os riscos baixos;
A solução deverá fornecer relatório de permissões, incluindo informação da classificação dos arquivos;
A solução deverá fornecer relatório referente aos níveis de exposição dos dados na nuvem, para qualquer tipo de site, pasta ou arquivo;
A solução deverá fornecer relatório dos níveis de exposição das permissões, no contexto de dados sensíveis para qualquer pasta e arquivo;

A solução deverá fornecer relatório das atividades de acesso dos usuários aos arquivos e pastas;
A solução deverá fornecer relatório dos resultados da classificação dos dados, incluindo o número de hits e regra classificada;
A solução deverá fornecer relatório de dados obsoletos, que não estão sendo acessados por um certo período de tempo;
A solução deverá fornecer relatório para usuários desabilitados;
Deve ser possível exportar o relatório em no mínimo 3 tipos de formatos: CSV, Excel e PDF;
Deverá ser possível realizar o agendamento de relatórios;
Deverá ser possível encaminhar o relatório apenas para o proprietário do dado.

Documento	Trecho
De acordo	De acordo
Getting Started with Varonis SaaS.pdf	The Varonis Web Interface provides several ways to narrow your focus and pinpoint the events and alerts that most require your attention, enabling you to review high-level summarized data via metrics in dashboards and perform investigation flows based on the collected data.
Varonis SaaS Web Interface User Guide.pdf Working with Monitored Data Sources in Varonis SaaS.pdf	Splunk SIEM Integration Remove DLP policy
Working with Monitored Data Sources in Varonis SaaS.pdf	Installation Requirements
Working with Monitored Data Sources in Varonis SaaS.pdf	MemoryThreshold - The threshold for the monitored service's memory usage. If the monitored service passes this threshold, the monitor terminates the service. The default is 32M.
Getting Started with Varonis SaaS.pdf	Adding New Users to Varonis SaaS Security Roles
https://www.varonis.com/trust	ISO/IEC 27001:2022
Getting Started with Varonis SaaS.pdf	To start monitoring the on-premises environment, at least one Collector is required. You download and run an installer on the dedicated server for the Collector. You can deploy and activate multiple Collectors at the same time. You can also use third-party distribution tools to install multiple Collectors automatically
Working with Monitored Data Sources in Varonis SaaS.pdf	Varonis Service Account
https://www.varonis.com/coverage/saas	Detect and fix SaaS misconfigurations
Getting Started with Varonis SaaS.pdf	Varonis SaaS Architecture
Getting Started with Varonis SaaS.pdf	loud services that scan data sources and calculate user security posture; Varonis SaaS stores only metadata (file, folder, and user names) but not document contents.
Varonis SaaS Web Interface User Guide.pdf	How MDDR Works
ok	ok

Working with Monitored Data Sources in Varonis SaaS	Each AD data source represents a monitored AD domain. In some cases, the Varonis UI displays the term Domain instead of Data Source. To monitor multiple AD domains, add an AD data source per AD domain.
Working with Monitored Data Sources in Varonis SaaS	Each AD data source represents a monitored AD domain. In some cases, the Varonis UI displays the term Domain instead of Data Source. To monitor multiple AD domains, add an AD data source per AD domain.
Varonis SaaS Supported Data Sources.pdf	Windows Linux
Varonis SaaS Web Interface User Guide	Working with the Action Center
Varonis SaaS Web Interface User Guide.pdf	Reviewing an Operation and Approving its Actions
Working with Monitored Data Sources in Varonis SaaS.pdf	A mini-filter driver (VrnsFilter) that transparently intercepts IRP (I/O Request Packet) packets occurring on the Windows Server and forwards them to a queue in memory. The driver is completely nonintrusive and transparent to ongoing Windows Server operations, with zero service degradation. • A service (VrnsCifsQueue) that continuously reads the events from the queue in memory and empties it. The service filters and aggregates the events and accumulates them in memory until they are read by the event collection service that runs on the Collector (Forwarder).
Varonis SaaS Web Interface User Guide.pdf	The Management tab includes the following options:
Varonis SaaS Supported Data Sources.pdf	Active Directory
Varonis SaaS Supported Data Sources.pdf	Windows
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported AD Events
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported AD Events
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported AD Events
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported AD Events
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported AD Events
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported AD Events

Working with Monitored Data Sources in Varonis SaaS.pdf	Supported AD Events
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported AD Events
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported AD Events
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported AD Events
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported AD Events
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported AD Events
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported AD Events
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported AD Events
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported AD Events
Working with Monitored Data Sources in Varonis SaaS	Supported Events for Windows Data Sources
Working with Monitored Data Sources in Varonis SaaS	Supported Events for Windows Data Sources
Working with Monitored Data Sources in Varonis SaaS	Supported Events for Windows Data Sources
Working with Monitored Data Sources in Varonis SaaS	Supported Events for Windows Data Sources
Working with Monitored Data Sources in Varonis SaaS	Supported Events for Windows Data Sources
Working with Monitored Data Sources in Varonis SaaS	Supported Events for Windows Data Sources
Working with Monitored Data Sources in Varonis SaaS	Supported Events for Windows Data Sources
Working with Monitored Data Sources in Varonis SaaS	Supported Events for Windows Data Sources
Working with Monitored Data Sources in Varonis SaaS	Supported Events for Windows Data Sources
Working with Monitored Data Sources in Varonis SaaS	Supported Events for Windows Data Sources
Working with Monitored Data Sources in Varonis SaaS	Supported Events for Windows Data Sources
Working with Monitored Data Sources in Varonis SaaS	Supported Events for Windows Data Sources
Working with Monitored Data Sources in Varonis SaaS	Supported Events for Windows Data Sources

Working with Monitored Data Sources in Varonis SaaS	Supported Events for Windows Data Sources
Working with Monitored Data Sources in Varonis SaaS	Supported Events for Windows Data Sources
Working with Monitored Data Sources in Varonis SaaS	Supported Events for Windows Data Sources
Working with Monitored Data Sources in Varonis SaaS	Supported Events for Windows Data Sources
Working with Monitored Data Sources in Varonis SaaS	Supported Events for Windows Data Sources
https://help.varonis.com/s/document-item?bundleId=ami1661784208197&topicId=brm1689522682243.html&_LANG=enus	The automation review phase also enables you to view active accounts whose access cannot be preserved, if such exist, before you decide to execute the automation. To view these accounts, click the link in the Lost Access column.
https://help.varonis.com/s/document-item?bundleId=nmc1648373836582&topicId=ecp1648376864325.html&_LANG=enus	Resources - Displays a tabular view of a resource's properties, based on the criteria you define in the search query. Resources include the sites, folders, or files on the platform you are monitoring.
https://help.varonis.com/s/document-item?bundleId=nmc1648373836582&topicId=ecp1648376864325.html&_LANG=enus	Resources - Displays a tabular view of a resource's properties, based on the criteria you define in the search query. Resources include the sites, folders, or files on the platform you are monitoring.
https://help.varonis.com/s/document-item?bundleId=ami1661784208197&topicId=hra1709205345147.html&_LANG=enus	CISF Platform Org-Wide Exposure
https://help.varonis.com/s/document-item?bundleId=nmc1648373836582&topicId=iyt1689602733608.html&_LANG=enus	View the classification analysis of all sensitive documents on an NFS data source in the Access Intelligence screen.
https://help.varonis.com/s/document-item?bundleId=otn1613070384298&topicId=qze1715766655181.html&_LANG=enus	Data Discovery and Classification VIP 20.0 Release Summary
Varonis SaaS Web Interface User Guide.pdf	Analyzing Data Classification Results Of A File
Varonis SaaS Web Interface User Guide.pdf	n addition to these custom, user-defined flags, there are system flags that are managed by Varonis and automatically detect important insights (for example: Whether this resource is stale, protected, unique etc.).

Varonis SaaS Web Interface User Guide.pdf	Data discovery policies (previously known as classification rules) are now available in the Varonis Web Interface in Management > Policies, on the Data Discovery
Varonis SaaS Web Interface User Guide.pdf	Displays the resources in your network in a hierarchical tree that allows you to see which users have access to each resource, and the permissions granted to each resource.
https://help.varonis.com/s/document-item?bundleId=nmc1648373836582&topicId=xti1713092191090.html&_LANG=enus	image files are processed through Optical Character Recognition (OCR)
Varonis SaaS Web Interface User Guide.pdf	Analyzing Data Classification Results Of A File
Varonis SaaS Web Interface User Guide.pdf	you can download all the dashboards or just the dashboard you are currently viewing as a CSV or Excel file at any time.
Varonis SaaS Web Interface User Guide.pdf	Analyzing Data Classification Results Of A File
Varonis SaaS Web Interface User Guide.pdf	Analyzing Data Classification Results Of A File
Varonis SaaS Web Interface User Guide.pdf	The right pane, named Document Text, displays the text of the document, with the results underlined in the color of each of the conditions they matched, and the condition names displayed below them. The rule names are displayed above the results.
https://help.varonis.com/s/document-item?bundleId=nmc1648373836582&topicId=xti1713092191090.html&_LANG=enus	File Types Supported for Classification
Getting Started with Varonis SaaS.pdf	The Events tab displays a line chart illustrating the dispersion of events (for example, creating or removing a site, folder, file, or permission on the platform you are monitoring) over the specified timeline, as well as event information in table form. You can use this information to view and search the activity log of your data sources and domains, identify risky activities, and investigate alerts.
https://help.varonis.com/s/document-item?bundleId=fvn1651844569092&topicId=dfw1639306202667.html&_LANG=enus	Files with classification hits - Files and list items with classification hits are collected according to the Data Classification Engine license and configuration.

Varonis SaaS Web Interface User Guide.pdf	Threat Detection - Varonis detects anomalous behavior and triggers an alert.
https://help.varonis.com/s/document-item?bundleId=fvn1651844569092&topicId=esf1634580209837.html&_LANG=enus	SMTP - The SMTP server.
Varonis SaaS Web Interface User Guide.pdf	Threat Detection Policies
Varonis SaaS Web Interface User Guide.pdf	Threat Detection - Varonis detects anomalous behavior and triggers an alert.
ok	ok
Varonis SaaS Web Interface User Guide.pdf	Threat Detection Policies
Varonis SaaS Web Interface User Guide.pdf	Threat Detection Policies
Varonis SaaS Web Interface User Guide.pdf	Threat Detection Policies
Varonis SaaS Web Interface User Guide.pdf	Threat Detection Policies
Varonis SaaS Web Interface User Guide.pdf	Threat Detection Policies
Varonis SaaS Web Interface User Guide.pdf	Threat Detection Policies
Varonis SaaS Web Interface User Guide.pdf	Threat Detection Policies
Varonis SaaS Web Interface User Guide.pdf	Threat Detection Policies
Varonis SaaS Web Interface User Guide.pdf	Threat Detection Policies
Varonis SaaS Web Interface User Guide.pdf	Threat Detection Policies
Varonis SaaS Web Interface User Guide.pdf	Threat Detection Policies
Varonis SaaS Web Interface User Guide.pdf	• MITRE ATT&CK - Varonis out-of-the-box policies are all mapped to the MITRE framework reflecting the Tactics and Techniques per policy.
Varonis SaaS Web Interface User Guide.pdf	Threat Detection - Varonis detects anomalous behavior and triggers an alert.

Varonis SaaS Web Interface User Guide.pdf	As such, they require a minimum 30-day learning period to gather data and analyze your users' behavior.
Varonis SaaS Web Interface User Guide.pdf	As such, they require a minimum 30-day learning period to gather data and analyze your users' behavior.
Varonis SaaS Web Interface User Guide.pdf	You can use this information to analyze the accounts that triggered the alerts or that have access to the data
Varonis SaaS Web Interface User Guide.pdf	The default dashboard view is the Alerts dashboard:
Varonis SaaS Web Interface User Guide.pdf	Working with Automations
Varonis SaaS Web Interface User Guide.pdf	Working with Automations
Varonis SaaS Web Interface User Guide.pdf	Working with Automations
Varonis SaaS Web Interface User Guide.pdf	Boolean operators allow terms to be combined through logic operators to form more complex queries. Varonis supports OR, AND, "+" and "-" as Boolean operators.
Varonis SaaS Web Interface User Guide.pdf	Working With Saved Searches
Varonis SaaS Web Interface User Guide.pdf	Varonis enables you to assign flags to accounts and resources. Use these flags to filter searches in the Accounts and Resources analytics tabs or to group search results.
Varonis SaaS Web Interface User Guide.pdf	Staleness Threshold
Varonis SaaS Web Interface User Guide.pdf	Dashboards display statistics through widgets that enable you view information at a glance
Varonis SaaS Web Interface User Guide.pdf	Dashboards display statistics through widgets that enable you view information at a glance
Varonis SaaS Web Interface User Guide.pdf	You can also compare the dashboard widgets over time by selecting the Compare over time button and then setting the period you want to compare.
Varonis SaaS Web Interface User	Dashboards display statistics through widgets that enable you view information at a glance. The following sections describe different types of widgets used to present your data:
Varonis SaaS Web Interface User	Geo

Varonis SaaS Web Interface User	In the Analytics page, you can run an out-of-the-box saved search, or create and run your own search query on specified data sources in your environment.
Varonis SaaS Web Interface User	In the Analytics page, you can run an out-of-the-box saved search, or create and run your own search query on specified data sources in your environment.
Varonis SaaS Web Interface User	In the Analytics page, you can run an out-of-the-box saved search, or create and run your own search query on specified data sources in your environment.
Varonis SaaS Web Interface User	In the Analytics page, you can run an out-of-the-box saved search, or create and run your own search query on specified data sources in your environment.
Varonis SaaS Web Interface User	In the Analytics page, you can run an out-of-the-box saved search, or create and run your own search query on specified data sources in your environment.
Varonis SaaS Web Interface User	In the Analytics page, you can run an out-of-the-box saved search, or create and run your own search query on specified data sources in your environment.
Varonis SaaS Web Interface User	In the Analytics page, you can run an out-of-the-box saved search, or create and run your own search query on specified data sources in your environment.
Varonis SaaS Web Interface User	In the Analytics page, you can run an out-of-the-box saved search, or create and run your own search query on specified data sources in your environment.
Varonis SaaS Web Interface User	In the Analytics page, you can run an out-of-the-box saved search, or create and run your own search query on specified data sources in your environment.
Varonis SaaS Web Interface User	In the Analytics page, you can run an out-of-the-box saved search, or create and run your own search query on specified data sources in your environment.
Varonis SaaS Web Interface User	In the Analytics page, you can run an out-of-the-box saved search, or create and run your own search query on specified data sources in your environment.
Varonis SaaS Web Interface User	In the Analytics page, you can run an out-of-the-box saved search, or create and run your own search query on specified data sources in your environment.
Varonis SaaS Web Interface User	In the Analytics page, you can run an out-of-the-box saved search, or create and run your own search query on specified data sources in your environment.
Varonis SaaS Web Interface User	In the Analytics page, you can run an out-of-the-box saved search, or create and run your own search query on specified data sources in your environment.
Varonis SaaS Web Interface User	In the Analytics page, you can run an out-of-the-box saved search, or create and run your own search query on specified data sources in your environment.
ok	ok
De acordo	De acordo
De acordo	De acordo
ok	ok
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources

Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources

Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for Entra ID Data Sources
ok	ok
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources

Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources

Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources

Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
About DatAdvantage.pdf	Bidirectional Clustering
Getting Started with Varonis SaaS.pdf	About Data Security Platform in Varonis SaaS
Working with Monitored Data Sources in Varonis SaaS.pdf	Supported Events for SharePoint Online Data Sources Supported Events for OneDrive Data Sources
Working with DatAdvantage Cloud.pdf	Varonis maps, analyzes, and normalizes relationships between users and data so you can easily answer critical security and compliance questions like, "Which sensitive files containing personal identifiable information (PII) are exposed via sharing links?" or "Which external users have granted permissions in any of our SaaS apps
Varonis SaaS Web Interface User Guide.pdf	This information is helpful for compliance and legal purposes and provides insights into your Varonis users' behavior.
Varonis SaaS Web Interface User Guide.pdf	Most Copilot alerts are based on behavioral learning. As such, they require a minimum 30-day learning period to gather data and analyze your users' behavior.
Working with Monitored Data Sources in Varonis SaaS.pdf	Folder shared link created • Folder shared link removed • Folder shared link updated • Folder shared link used
Getting Started with Varonis SaaS.pdf	Show a single data point, such as the number of sensitive files, or the number of folders with open access.
Working with DatAdvantage Cloud.pdf	Investigating Group Membership

Working with DatAdvantage Cloud.pdf	The Threat Detection policies page shows all the policies that are defined for each tenant, categorized by service. The services are listed on the right.
Working with DatAdvantage Cloud.pdf	Investigate high-fidelity alerts on sharing sensitive data, abnormal logins, suspicious administrator activity, and many other unusual events through predefined activity policies
Working with DatAdvantage Cloud.pdf	Similar to remediation of public links in Google Workspace and Box, you will now find under the “Remediate Public Links” report, Salesforce content documents that have public links. Using the same flow in the system as for Google Workspace and Box, you will now be able to select the ones that you wish to remediate.
Working with Monitored Data Sources in Varonis SaaS.pdf	To analyze data classification results of a file in OneDrive data sources, you should have the File Analysis Elevated Permissions role.
Working with DatAdvantage Cloud.pdf	Varonis maps, analyzes, and normalizes relationships between users and data so you can easily answer critical security and compliance questions like, "Which sensitive files containing personal identifiable information (PII) are exposed via sharing links?"
Getting Started with Varonis SaaS.pdf	File Types Supported For Classification
Working with DatAdvantage Cloud.pdf	DatAdvantage Cloud Architecture with a Private Cloud Data Collector Deployed
Getting Started with Varonis SaaS.pdf	View the classification analysis of all sensitive documents on a SharePoint Online or OneDrive data source in the Access Intelligence screen. Important: This role allows the user to access the files regardless of the user's permissions
https://www.varonis.com/blog/data-classification-buyers-guide	A big reason why Varonis can scan the largest data environments is our incremental approach.
Varonis SaaS Web Interface User Guide.pdf	Rolling Back Actions of an Automation
ok	ok
Working with DatAdvantage Cloud.pdf	Revoking Public Sharing
Working with DatAdvantage Cloud.pdf	Revoking Public Sharing

Working with DatAdvantage Cloud.pdf	Revoking Public Sharing
Working with DatAdvantage Cloud.pdf	Revoking Public Sharing
Working with DatAdvantage Cloud.pdf	Remediate Stale Direct Permissions - Identify users that have stale, recently unused, direct permissions on data
Working with DatAdvantage Cloud.pdf	Remediate Stale Direct Permissions - Identify users that have stale, recently unused, direct permissions on data
Working with DatAdvantage Cloud.pdf	Remediation within Varonis is supported via two different workflows: Manual item selection for Remediation and Automated Remediation
Varonis SaaS Web Interface User Guide.pdf	What is a stale resource? The dashboards in the Varonis Web Interface provide you with a fast understanding of your risk situation and enhanced control over your data.
Varonis SaaS Web Interface User Guide.pdf	What is a stale resource? The dashboards in the Varonis Web Interface provide you with a fast understanding of your risk situation and enhanced control over your data.
Varonis SaaS Web Interface User Guide.pdf	What is a stale resource? The dashboards in the Varonis Web Interface provide you with a fast understanding of your risk situation and enhanced control over your data.
Varonis SaaS Web Interface User Guide.pdf	The Compliance dashboard default view provides key metrics at a glance at classification category and rule level, focusing on the potential risk of sensitive, stale, or over-exposed data.
Varonis SaaS Web Interface User Guide.pdf	In the Analytics page, you can run searches on specified data sources in your environment for different entities (events, alerts, permissions, accounts and memberships, and resources) ... Searches create reports which include types of data relevant to the entity being searched
Varonis SaaS Web Interface User Guide.pdf	Displays a tabular view of a resource's properties, based on the criteria you define in the search query. Resources include the sites, folders, or files on the platform you are monitoring.
Varonis SaaS Web Interface User Guide.pdf	Click the Switch to effective permissions link to display the permissions granting access to users or groups as a result of their membership of wider groups which themselves have access to the resource.

Varonis SaaS Web Interface User Guide.pdf	Displays a line chart illustrating the dispersion of events (for example, creating or removing a site, folder, file, or permission on the platform you are monitoring) over the specified time line, as well as event information in table form
Varonis SaaS Web Interface User Guide.pdf	The side pane includes a header with brief metadata about the resource (such as its name, tags, and so on), as well as commonly used actions:
Varonis SaaS Web Interface User Guide.pdf	Varonis monitors activity on resources over time. If no activity has been detected over a predefined period of time, known as the “staleness threshold”, the resource is considered “stale”.
Working with Monitored Data Sources in Varonis SaaS.pdf	Account disabled Account enabled
Varonis SaaS Web Interface User Guide.pdf	When exporting data (as a CSV, Excel or PDF file)
Varonis SaaS Web Interface User Guide.pdf	Working With Scheduled Searches
Varonis SaaS Web Interface User Guide.pdf	Data-Driven - A sub-set of the scheduled search, customized per-owner: When selected, each owner receives only relevant information based on their managed objects.

VARONIS

Active Directory e Azure AD

Tenha uma visão geral da sua estrutura local e do Azure AD, identifique as vulnerabilidades e detecte ataques como Kerberoasting e pass-the-hash.

Desafio

O Active Directory (AD) e o Azure AD são destinos comuns para hackers, pois têm as chaves para acessar dados confidenciais: as credenciais. É difícil para os administradores proteger as estruturas complexas do AD, mas os invasores as exploram com facilidade, abrindo a porta para conjuntos valiosos de informações confidenciais. As ferramentas de auditoria nativas do AD, por si só, não oferecem visibilidade nem contexto suficientes para dar eficiência à defesa contra ataques avançados.

Soluções

A plataforma de segurança de dados Varonis ajuda a oferecer uma visão geral da sua estrutura local e do Azure AD, a identificar as vulnerabilidades e a detectar ataques como Kerberoasting e pass-the-hash. Monitoramos todas as atividades do AD (acessos, alterações de usuários e grupos, eventos de GPO) e usamos modelos de ameaças baseados em comportamento como maneira proativa de impedir os ataques. Ao combinar a atividade do AD com eventos de acesso a dados e atividade de rede, a Varonis pode detectar, por exemplo, usuários obsoletos que acessam dados confidenciais, o que poderia facilmente passar despercebido de outra forma. Informe-se em tempo real sobre os principais riscos do AD e tenha as ferramentas necessárias para desembaraçar seus domínios, fechar as lacunas e reduzir os riscos com eficácia.



▲ Os painéis do Active Directory ajudam a priorizar os maiores riscose a demonstrar o progresso ao longo do tempo.

Sucesso do cliente

"Seria quase impossível realizar a difícil tarefa de proteger os dados sem a Varonis. **Com a Varonis, posso ter uma imagem clara dentro de alguns minutos."**

Gerente de infraestrutura,
Grande fabricante americano

LEIA O ESTUDO DE CASO ›

Informações de risco do AD

61% das empresas
têm mais de 500 usuários com senhas que nunca vão expirar[1]

50% das contas dos usuários
são obsoletas ou estão inativas[1]

38% dos usuários
tinham senhas que nunca expiram (mais de 10% no ano passado)[1]

1. Relatório Global de Risco de Dados da Varonis, 2019



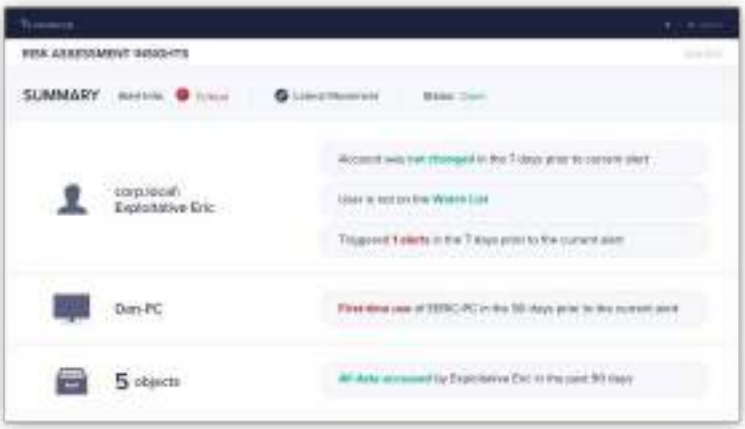
Desembarace os seus domínios

Tenha uma visão geral sobre todos os seus domínios e usuários, grupos e objetos locais em uma interface intuitiva e responda rapidamente a perguntas como “quem pode alterar configurações críticas, como adicionar usuários a grupos privilegiados?”

Pesquise uma trilha de auditoria de atividades unificada

Saiba quem está fazendo o que no Active Directory, além dos arquivos confidenciais abertos, dos envios de email, das solicitações da web e do acessoa à VPN, com apenas alguns cliques.





Investigue incidentes rapidamente e de forma conclusiva

Faça com que analistas pareçam equipes muito experientes, com ferramentas intuitivas para perícia e resposta a incidentes. A Varonis faz todo o trabalho para normalizar, enriquecer e correlacionar registros para facilitar os alertas para análise e ação.

Experimente a Varonis gratuitamente

Todos os produtos Varonis podem ser experimentados gratuitamente e são fornecidos com uma avaliação de riscos realizada por engenheiros. A maneira mais fácil de começar é com uma breve demonstração e uma conversa individual.

CONTATO

Proactive Incident Response

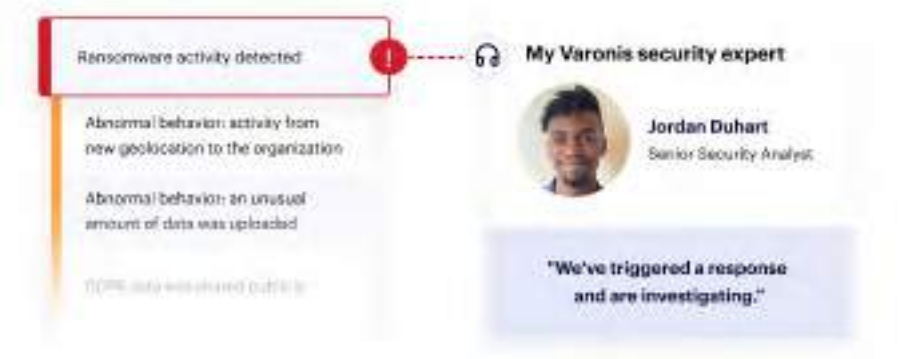
The brightest minds in offensive and defensive security, watching your data for threats

Challenge

Security teams are stretched thin. They're responsible for sifting through mountains of alerts — many of which are false positives — to find attacks before they take hold. Many times, this means managing multiple systems and spending hours on investigations to separate the signal from the noise.

Solution

Varonis' Proactive Incident Response team watches your Varonis alerts for you and notifies you of true incidents. We investigate suspicious behavior and call you if we see a problem. This means that instead of more alerts, you get outcomes — without even needing to log in.
In the background, we develop custom threat models specific to your environment and configure automated responses to stop threats like ransomware in its tracks.



Key benefits

- Proactive alert monitoring and threat investigation
- Threat model development tailored to your organization
- Automatic response configuration to stop an attack in its tracks
- Regular check-ins to review security findings

"The investment we've made in Varonis has been immeasurable in finding and stopping cyberattacks. The Varonis team proactively reaches out to me with true incidents, rather than just surfacing more alerts for my team to manage."

Scott Mercer
Director, Cybersecurity and Technical Services, KU Endowment

What you can expect



Proactive monitoring and investigation

Our team of cybersecurity experts watches your data for threats, investigates alerts, and only surfaces true incidents that require your attention. Varonis saves your team time and hardens your security defenses — all without you even needing to log in.



A resilient security infrastructure

Our dedicated engineers will do all the heavy lifting for you, including creating custom threat models designed for your specific environment, data, and organization and configuring automated alert responses. Use our team's industry and product expertise to enhance proactive threat detection efforts.



Consistent, expert help

We meet regularly with our customers to ensure Varonis delivers maximum value to each organization. Our engineers will sit down with your team to review security findings and explain each result, providing you with personalized recommendations for where you can improve your security posture.

Learn more about our incident response services.

The Varonis experience includes more than just software. Our customers have access to a host of services designed to drive effortless security outcomes.

Learn more

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

Varonis Systems, Inc

DatAdvantage Cloud Platform

ISAE 3000 (SOC 2) Type II

Service Auditor's Assurance Report

For the period

January 1, 2025 to December 31, 2025

roberto.recordato@petacorp.com.br
October 20, 2026 11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

Contents

Section I - Management Assertion Provided by Varonis Systems, Inc 5

Section II – Independent Service Auditor's Assurance Report 7

Scope 7

Description of Tests of Controls 9

Opinion 9

Restricted Use 9

Section III - 11

Description of Varonis Systems Inc's DatAdvantage Cloud Platform System 11

Company Overview and Background 11

Description of the Services Provided 11

Principal Service Commitment and System Requirements 12

Organizational Structure 13

Functional areas of operations are listed below: 13

Description of the Control Environment, Information Communication, Monitoring and Risk Management Process 13

Control Environment 14
Authority and Responsibility 14
Management Philosophy and Operating Style 14
Integrity and Ethical Values 14
Whistleblower Program 15
Commitment to Competence 15
Accountability 15
Control Activities 15
Information and Communication 15
Risk Management 17
Enterprise Risk Management Program 17
Cyber Risk Assessments 17
Third-Party Risk Management 18

Components of the DatAdvantage Cloud Platform 18

Infrastructure 18
System Boundaries 18

Infrastructure and Software 19

Third-Party Cloud Services 20

Varonis DatAdvantage Cloud relies on third-party services as part of its operations. 20

Data 20

Data Processing 20

robert.rezende@petacorp.com.br October 20, 2026 11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

Description of the Information Systems Controls 21
Separation of Environments 21
Access Authentication and Authorization 21
Authentication 21
Authorization 21
Varonis DatAdvantage Cloud Platform Access 21
Customer Access 22
Password Policy 22
Privileged Access 22
Encryption 22
Network Security 22
Security Testing 22
Vulnerability Scanning and Monitoring 23
Asset Management 23
Secure Software Development Lifecycle (SSDLC) 23
Software Testing and Validation Process 23
Change Management 24
Change Documentation 24
Emergency Changes 25
Change Monitoring 25
Human Resource Policies and Procedures 25
New Hire Process 25
During Employment 26
Access Provisioning/De-provisioning 26
Performance Evaluation 26
Physical Access 27
Facilities Physical Security 27
Incident Response 27
Endpoint Security 27
Anti-Malware 27
Software Approval and Monitoring Process 27
Other Endpoint Security Controls 28
Business Continuity and Disaster Recovery 28
Backup and Restore 28
Additional Criteria for Availability 29
Support Services 29
Support 29
Ticketing and Management 29
Escalation Process 29
Internal Audits 29

roberto.revoredo@petacorp.com.br
October 20 2026 11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

External Audits 29

Complementary User Entity Controls 30

Subservice Organizations carved-out controls: 30

Section IV - Trust Services Criteria, Related Controls and Tests of Controls ***32***

Overview 32

Testing Performed and Results of Tests of Entity-Level Controls 32

Testing Methods 33

Security Principle and Criteria 34

Control Environment 34
Risk Assessment 42
Monitoring Activities 45
Control Activities 46
Logical and Physical Access Controls 48
System Operations 55
Change Management 59
Risk Mitigation 60

Availability 61

Confidentiality 63

roberto.revoredo@petacorp.com.br
October 20, 2026 11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

Section I - Management Assertion Provided by Varonis Systems, Inc

We have prepared the accompanying description in Section III of Varonis Systems, Inc's titled "Management of Varonis Systems, Inc's Description of its DatAdvantage Cloud Platform system" throughout the period January 1, 2025 to December 31, 2025 (the Description), based on the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report, (the Description Criteria). The Description is intended to provide report users with information about the DatAdvantage Cloud Platform that may be useful when assessing the risks arising from interactions with system, particularly information about system controls that has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security ,Confidentiality and Availability (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

Varonis Systems, Inc uses Amazon Web Services (AWS) as a carved-out subservice organization to provide cloud infrastructure, hosting services, and related platform capabilities. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at, Varonis Systems, Inc, to achieve Varonis Systems, Inc's service commitments and system requirements based on the applicable trust services criteria. The Description presents Varonis Systems, Inc's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Varonis Systems, Inc's controls. The Description does not disclose the actual controls at the subservice organization.

The Description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Varonis Systems, Inc , to achieve Varonis Systems, Inc's service commitments and system requirements based on the applicable trust services criteria. The Description presents Varonis Systems, Inc's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Varonis Systems, Inc's controls.

We confirm, to the best of our knowledge and belief, that:

a. The Description presents Varonis Systems, Inc's DatAdvantage Cloud Platform that was designed and implemented throughout the period January 1, 2025, to December 31, 2025, in accordance with the Description Criteria
.

b. The controls stated in the Description were suitably designed throughout the period January 1, 2025 to December 31, 2025 to provide reasonable assurance that Varonis Systems, Inc's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and AWS subservice organization and user entities applied the complementary controls assumed in the design of Varonis Systems, Inc's controls throughout the period January 1, 2025 to December 31, 2025.

c. The controls stated in the Description operated effectively throughout the period January 1, 2025 to December 31, 2025 to provide reasonable assurance that Varonis Systems, Inc's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary

Copia para revisão@petecorp.com.br October 20, 2026 11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

subservice organization controls and complementary user entity controls, assumed in the design of Varonis Systems, Inc's controls, operated effectively throughout the period January 1, 2025 to December 31, 2025.

Varonis Systems, Inc
March 16, 2026

Gilad Raz	DocuSigned by: EC1D2A0F14EA468...	CIO	March 18, 2026 | 15:48:06 EDT
Dror Shemesh	Signed by: Dror Shemesh 835689DDD5E94F9...	Chief Information Security Officer	March 18, 2026 | 15:46:17 EDT
John Neystadt	Signed by: 4D88EB5E32CA40A...	Chief Architect	March 19, 2026 | 04:11:47 EDT

roberto revoredo@petacorp.com.br October 20, 2026 11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

Somekh Chaikin
17 Ha'arba'a Street, PO Box 609
KPMG Millennium Tower
Tel Aviv 6100601, Israel
+972 3 684 8000

TEL +972 3 684 8000
Fax +972 3 684 8444
Website www.kpmg.co.il

Section II – Independent Service Auditor's Assurance Report

To: Management of Varonis Systems, Inc:

Scope

We have been engaged to report on Varonis Systems, Inc's accompanying description of its system titled "Management of Varonis Systems, Inc's Description of its DatAdvantage Cloud Platform system" throughout the period January 1, 2025 to December 31, 2025 (the Description), based on the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report, in AICPA Description Criteria (the Description Criteria), and the suitability of the design and operating effectiveness of controls stated in the Description throughout the period January 1, 2025 to December 31, 2025 to provide reasonable assurance that service commitments and system requirements were achieved based on the trust services criteria relevant to *Security ,Confidentiality and Availability* (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria.

Varonis Systems, Inc uses AWS as a carved-out subservice organization to provide cloud infrastructure and hosting services The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Varonis Systems, Inc, to achieve Varonis Systems, Inc's service commitments and system requirements based on the applicable trust services criteria. The Description presents controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of controls. The Description does not disclose the actual controls at the subservice organization. Our engagement did not include the services provided by the subservice organization(s), and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The Description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at, to achieve Varonis Systems, Inc's service commitments and system requirements based on the applicable trust services criteria. The Description presents Varonis Systems, Inc's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Varonis Systems, Inc's controls. Our engagement did not include such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

Varonis Systems, Inc is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Varonis Systems Inc's service commitments and system requirements were achieved. Management of has provided the accompanying statement titled "Management of Varonis Systems Inc's Statement" (the Management Statement) about the Description and the suitability of design and operating effectiveness of controls stated therein. Varonis Systems, Inc is also responsible for preparing the Description and Statement, including the completeness, accuracy, and method of presentation of the Description and Statement; providing the services covered by the Description; selecting the applicable trust services criteria and stating the related controls in the Description; and identifying the risks that threaten the achievement of Varonis Systems Inc's service commitments and system requirements.

Roberto Evgi Datacorp.com.pr
October 29, 2026 11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

Somekh Chaikin
17 Ha'arba'a Street, PO Box 609
KPMG Millennium Tower
Tel Aviv 6100601, Israel
+972 3 684 8000

TEL +972 3 684 8000
Fax +972 3 684 8444
Website www.kpmg.co.il

Our independence and quality management

We have complied with the independence and other ethical requirements of the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants (including International Independence Standards) (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

The firm applies to International Standard on Quality Management 1, Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements, which requires the firm to design, implement and operate a system of quality management including documented policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the Description and on the suitability of the design and operating effectiveness of the controls stated in the Description based on the evidence we have obtained in our engagement.

Our engagement was conducted in accordance with International Standard on Assurance Engagements 3000 (Revised), Assurance Engagements Other than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board. That standard requires that we plan and perform our engagement to obtain reasonable assurance about whether, in all material respects, the Description is presented in accordance with the Description Criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

A reasonable assurance engagement to report on the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization would achieve its service commitments and system requirements based on the applicable trust services criteria if those controls operated effectively.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description; and
- Performing such other procedures as we considered necessary in the circumstances.

KPMG Storeupdate.storeupdategroup.com.br October 20, 2023 14:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

Somekh Chaikin
17 Ha'arba'a Street, PO Box 609
KPMG Millennium Tower
Tel Aviv 6100601, Israel
+972 3 684 8000

TEL +972 3 684 8000
Fax +972 3 684 8444
Website www.kpmg.co.il

Inherent Limitations

The Description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that each individual report user may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are listed in Section four (IV)

Opinion

In our opinion, in all material respects,

a. The Description presents Varonis Systems, Inc's DatAdvantage Cloud Platform that was designed and implemented throughout the period January 1, 2025, to December 31, 2025, in accordance with the Description Criteria
b. The controls stated in the Description were suitably designed throughout the period January 1, 2025, to December 31, 2025, to provide reasonable assurance that Varonis Systems, Inc's service commitments and system requirements would be achieved based on the applicable trust services criteria if the controls operated effectively throughout that period.
c. The controls stated in the Description operated effectively throughout the period January 1, 2025, to December 31, 2025, to provide reasonable assurance that Varonis Systems, Inc's service commitments and system requirements were achieved based on the applicable trust services criteria.

Restricted Use

This report, including the description of tests of controls and results thereof in Section four (IV), is intended solely for the information and use of and user entities of Varonis Systems Inc's DatAdvantage Cloud Platform during some or all of the period January 1, 2025, to December 31, 2025, who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

roberto.revoredo@peteco.com.br
October 20, 2026 11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

Somekh Chaikin
17 Ha'arba'a Street, PO Box 609
KPMG Millennium Tower
Tel Aviv 6100601, Israel
+972 3 684 8000

TEL +972 3 684 8000
Fax +972 3 684 8444
Website www.kpmg.co.il

- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria, and
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be and should not be used by anyone other than these specified parties.



March 16, 2026

17 Ha'arba'ah St. Tel Aviv 6473917, Israel

roberto.revoredo@petacorp.com.br
October 20, 2026 11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

Section III -
Description of Varonis Systems Inc's DatAdvantage Cloud Platform System

Company Overview and Background

Varonis Systems, Inc started operations in 2005 and services numerous leading firms in the financial services, public, healthcare, industrial, insurance, energy and utilities, technology, consumer and retail, media and entertainment, and education sectors.

Varonis Systems, Inc (Nasdaq: VRNS) is the leader in data security, fighting a different battle than conventional cybersecurity companies. Varonis Systems, Inc is a pioneer in data security and analytics, fighting a different battle than conventional cybersecurity companies. Varonis Systems, Inc focuses on protecting enterprise data, which includes sensitive files and emails, as well as confidential customer, patient, and employee data. Our services also protect financial records, strategic product plans, and other intellectual property from unauthorized access by nefarious actors.

The Varonis Systems, Inc's DatAdvantage Cloud Platform system detects cyberthreats from both internal and external actors by continuously analyzing cloud configurations, data permissions, account activity, and user behavior across SaaS and IaaS platforms. The platform helps prevent and contain potential breaches by automatically locking down access to sensitive and stale data and maintains a least-privilege posture through intelligent automation and policy enforcement.

Varonis Systems, Inc products address important use cases including data protection, data governance, zero trust, compliance, data privacy, classification, and threat detection and response.

Description of the Services Provided

Varonis Systems, Inc's DatAdvantage Cloud Platform is a cloud-hosted data security platform for protecting and governing enterprise data. Companies use Varonis Systems, Inc's DatAdvantage Cloud Platform to discover mission-critical data, ensure only the right people have access, and detect threats before they come. Varonis Systems, Inc integrates with a wide array of data repositories, SaaS applications, and infrastructure to give customers a holistic view of their data. Varonis can be used to address these important use cases:

- **Detecting insider threats and cyberattacks**: Varonis Systems, Inc's DatAdvantage Cloud Platform detects threats to data, including insider threats and external cyberattacks with a live-updating library of pre-built threat models based on attack techniques and vulnerabilities used by real-world adversaries.
- **Limiting the blast radius of an attack:** Varonis Systems, Inc's DatAdvantage Cloud Platform analyzes where there is unnecessary access to data and can eliminate excessive access at scale, drastically reducing the damage from insider threats and cyberattacks.
- **Preventing data exposure:** Varonis Systems, Inc's DatAdvantage Cloud Platform's Data Security Posture Management (DSPM) capabilities help teams automatically classify sensitive data, find where information is exposed externally or internally, and help teams continually prioritize remediation efforts to improve security posture.
- **Fixing misconfigurations:** Varonis Systems, Inc's DatAdvantage Cloud Platform provides SSPM capabilities to analyze and fix misconfigured Software as a Service (SaaS) application, discovering shadow instances, and spotting vulnerabilities that could put data at risk.
- **Achieving compliance:** Varonis Systems, Inc's vast library of classification rules policies can discover sensitive data related to GDPR, CCPA, HIPAA, and more. The permissions analysis and continual monitoring Varonis provides gives auditors a real-time pulse on compliance.

Prepared for peterschrup.com by Coalfire on 10/26/2021 11:15 EDT

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

Principal Service Commitment and System Requirements

Varonis Systems, Inc's DatAdvantage Cloud Platform offers security teams a single point of control for identifying sensitive data and where it is exposed, reducing risk by understanding and rightsizing privileges, and monitoring for suspicious or inappropriate behavior across SaaS apps.

Varonis Systems, Inc's DatAdvantage Cloud Platform's infrastructure is deployed on Amazon Web Services (AWS) (utilizing both SaaS and PaaS solutions) for hosting and operating the production, staging, and development environments. Varonis Systems, Inc's commitment to customers and other third parties include *security, availability and confidentiality.* This is communicated and documented as part of the supplier relationship process. Our commitment for our customers includes but is not limited to:

- An established global risk management process to identify, monitor and manage risks for the entire organization, business units and supplier relationships.
- Physical, logical, and remote access to sensitive information that is controlled to reduce the likelihood of a security incident. Varonis Systems, Inc has established and follows specific access control practices to protect information and information systems from unauthorized access, modification, disclosure, or destruction.
- Secure data transmission protocols to encrypt data when transmitting over public networks. Encryption is also enabled on databases, data at rest, data backups and communication between segmented boundaries.
- Network segregation to enforce separation between production, staging, testing, and other cloud-based and internal infrastructure environments.
- Minimum standards of security for the development, provision, and use of Varonis Systems, Inc cloud services require that the *security, availability and confidentiality* of assets within Varonis cloud services are protected. Cloud services provided, and risks to the services and to customers are subject to risk assessment and application of suitable technical and organizational controls.
- Data centers which host, store, and/or process customer data comply with industry's best practices. This includes protecting information system equipment and cabling, entrance controlled by access card, surveillance cameras, providing emergency power, shutoff, and lighting, fire alarms, protection from water and fire, and maintaining temperature and humidity controls.
- A retention policy that complies with applicable legal, regulatory, and contractual requirements. This includes deleting customer data upon request or automatically based on lifecycle policies that are communicated to the customer.
- The Human Resources Department (HR) ensures successful operations and delivery of effective security controls. This includes implementing security measures prior to employment, during employment, at termination and any other changes in employment, as well as ongoing cybersecurity awareness training.
- Backup procedures to ensure the continued availability and accessibility of information and minimize the cost of a disruption (e.g., operational error, disaster, or sabotage that causes damage to, or destruction of, information).
- Maintaining contractual agreement between Varonis and customer wherein the customer requirements are specified, and Varonis states the level of service responsibilities and guarantees regarding availability, performance, handling of availability incidents and support levels.
- Implementing privacy by design within the systems and processes in such a way as to minimize risks to privacy and aims to process personally identifiable information (PII) in line with regulatory requirements.

Powered by Edgewise Networks.com
October 20, 2021 1:51 PM PDT

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

Organizational Structure

Varonis Systems, Inc has an established organization structure with defined roles and responsibilities. Roles and responsibilities are segregated based on functional requirements. Varonis Systems, Inc has an organization chart that outlines lines of reporting. The organization chart is updated in real time to reflect any changes.

Functional areas of operations are listed below:

- **Executive Management** – responsible for overseeing company-wide initiatives and activities, establishing, and accomplishing goals, overseeing objectives, and ensuring appropriate resource levels are available to meet business objectives.
- **DevOps** – Responsible for a diverse Varonis DatAdvantage Cloud environment. Design and development of DevOps tools and features, CI/CD pipelines and automation processes for configuration, deployment, monitoring, and maintenance of complex cloud environments.
- **Product Management (PM**) – Responsible for product planning and execution throughout the product life cycle. The PM gathers and prioritizes product requirements by conducting market research supported by visits and interaction with customers, prospects, and partners, as well as perform analysis of market trends and competitive landscape.
- **Information Security** – Provides leadership in developing, reviewing, and recommending direction for the Information Security Policy, Standards, and Guidelines, as well as responsible for the security monitoring, architecture, testing, governance, risk, and compliance.
- **Security Operations Center (SOC)** – The team is a part of the Global Information Security team, and responsible for monitoring systems and investigating cybersecurity incidents, as well as developing operational playbooks and suggest alert enhancements to improve threat detection capabilities.
- **Product Security** – Responsible for the secure software development lifecycle, secure design, security testing and the security of the cloud-based production environments.
- **Human Resources** - Responsible for HR policies, practices, and processes including but not limited to talent acquisition, recruitment, Employee on boarding, Training and development, benefits, compensation, resignation process, and performance review.
- **Support** – Managing, monitoring, and supporting users for the cloud services environment.
- **Software Engineers** – Responsible for programming high-performance core applications, which are responsible to collect and move large amounts of data. Design, features, and modules of ownership in all aspects.
- **Architecture Team** – Responsible for designing software systems aligned with industry best practices and ensures that the threat model for the software and services is conducted and mitigated.
- **Internal Audit** – Independent, objective assurance and consulting activity designed to add value and improve an organization's operations. The team supports the organization to accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

Description of the Control Environment, Information Communication, Monitoring and Risk Management Process

A company's internal control is a process – affected by the entity's boards of directors, management, and other personnel – designed to enable the achievement of objectives in the following categories: (a) reliability of Product Development, (b) effectiveness and efficiency of operations, and (c) compliance with applicable laws and regulations. The following section is a description of the components of internal control for Varonis.

Prepared for: kennedy@peaccorp.com.ph
October 20, 2026 11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its employees. It reflects the overall attitude, awareness, and actions of management and others concerning the importance of controls and the emphasis given to controls in the entity's policies, procedures, methods, and organizational structure. Varonis executive management recognizes its responsibility for directing and controlling operations and for establishing, communicating, and monitoring control policies and procedures. Policy and procedures documents for significant processes that address system requirements and relevant updates are available on the internal shared drive.

Authority and Responsibility

Lines of authority and responsibility are clearly established throughout. The Varonis' Board of Directors (The Board) meets periodically to review committee charters and corporate governance, which define their roles, responsibilities, member qualifications, meeting frequency, and other discussion topics. Meeting minutes of the annual meetings are recorded, which include participants and date the meeting occurred.

Each member of the Board possesses adequate, relevant experience, and is recognized as an individual of high integrity and good stature. The Board is actively involved in and scrutinizes the activities of Varonis' functional groups and acts with respect to its fiduciary responsibilities. The Board is responsible for overseeing Varonis' corporate governance and has discretion to delegate a broad range of powers and decisions to the Management Committee to manage the entity and its daily business.

The Audit Committee is responsible for, among other things, overseeing and monitoring the integrity of Varonis' consolidated financial statements, the entity's compliance with legal and regulatory requirements as they relate to financial reporting or accounting matters, and the organization's internal accounting and financial controls; overseeing and monitoring Varonis' independent auditor's qualifications, independence, and performance; providing the Board with the results of its monitoring and recommendations; providing the Board with additional information and materials as it deems necessary to make the Board aware of significant financial matters that require the attention of the Board; and overseeing the Varonis' internal audit function.

Management Philosophy and Operating Style

The control environment at Varonis entails the involvement and ongoing engagement of Executive and Senior Management (Management Team), chaired by the Chief Executive Officer ("CEO"), who has been delegated by the Board the responsibility to manage Varonis and its daily business. In its role, the Management Team assigns authority and responsibility for operating activities and establishes reporting relationships and authorization hierarchies. The Management Team designs policies and communications so that personnel understand Varonis' objectives, know how their individual actions interrelate and contribute to those objectives and recognize how and for what they will be held accountable. Communication exists between Executive and Senior Management so that both have information needed to fulfill their roles.

Integrity and Ethical Values

Integrity and ethical values are essential elements of the control environment, affecting the design, administration, and monitoring of key processes. Integrity and ethical behavior are the products of Varonis' ethical and behavioral standards, how they are communicated, and how they are monitored and enforced in its business activities. They include management's actions to remove or reduce incentives/pressures, and opportunities that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of the entity's values and behavioral standards to personnel through policy statements and codes of conduct, and by the examples the executives set.

Varonis Board of Directors (the Board) and management recognize their responsibility to foster a strong ethical environment within Varonis to determine that its business affairs are conducted with integrity, and in accordance

Robert Half Forensic & Litigation Consulting
October 29 2026 1:01 PM UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

with high standards of personal and corporate conduct. This responsibility is characterized and reflected in the Varonis Code of Business Conduct and Ethics (the Code of Conduct), which is distributed to all employees. Specifically, employees and their immediate families are prohibited from using their positions with Varonis for personal or private gain, disclosing confidential information regarding clients, or taking any action that is not in the best interest of clients. Employees' personal securities transactions are governed by corporate policy and employee account trades are reviewed to monitor adherence to Varonis policy. All employees are required to maintain ongoing compliance with all policies, standards, and procedures of the Code of Conduct and with lawful and ethical business practices, whether they are specifically mentioned in the Code of Conduct. Each employee is required to affirm periodically that he or she received, read, understood, and complied with the requirements set forth in the Code of Conduct and the Employee Handbook. Employee recertification status is monitored periodically for compliance.

Whistleblower Program

Varonis has an anonymous whistle-blower program in place for employees to report any violations without fear of dismissal or retaliation. Reported issues are investigated and acted on in a timely manner. Information regarding how to report any violations is outlined in Varonis' Code of Business Conduct and Ethics policy.

Commitment to Competence

Varonis management defines competence as the necessary knowledge and skills required by employees to fulfil and accomplish tasks that define their roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

Accountability

Varonis employees and contractors are accountable for understanding and adhering to the guidance contained in the security policies, and any applicable supporting procedures.

Control Activities

Control activities are the policies and procedures that enable management directives to be conducted to address risks to the achievement of the entity's objectives. Varonis operating and functional units are required to implement control activities that help achieve business objectives associated with:

1. The reliability of financial reporting,
2. The effectiveness and efficiency of operations and
3. Compliance with applicable laws and regulations**.**

The controls activities are designed to address specific risks associated with Varonis operations and are reviewed as part of the risk assessment process. Varonis has developed formal policies and procedures covering various operational matters to document the requirements for performance of control activities. Controls are in place to put the policies into action in a timely manner. Competent personnel with sufficient authority perform the control activities with diligence and continuing focus. Policies and procedures are documented, reviewed, and approved on an annual basis by the management team and available to Varonis' employees within the Varonis internal portal. In addition, Responsibility, and accountability for developing and maintaining the policies are assigned to the relevant personnel and approved on an annual basis by the management team.

Information and Communication

Information and communication are integral components of Varonis' internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Varonis, information

roberto.revoredo@petacorp.com.br
October 20 2020 21:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

The Varonis Community Portal offers detailed product information. Varonis' customers may access detailed service plans in the Community Portal

Internally, Varonis offers their employees several methods for communication. All policies and procedures are available via the internal employee portal. Employees are informed regularly of service updates, delays as well as new products and services once they are made available.

With communication being critical to the provision of cloud services, Varonis ensures that customers are informed of all critical information in a timely manner. This includes information about changes to services or availability, and to security incidents relating to either their services or their account. Methods of communication with Cloud service customers are set out in contracts.

To support this, Varonis provides customers with key information before agreeing to contracts, during the exchange of contracts and throughout the lifecycle of the relationship. Varonis also established a Privacy Policy which discloses its confidentiality practices for customer data. The privacy policy is available on Varonis website to all customers. Customers are notified of material updates to the privacy policy.

Varonis communicates its commitment that security is a top priority for its customers and Varonis internal users through Varonis Systems, Inc's portal. In addition, customers and Varonis Systems, Inc internal users are offered multiple methods for contacting Varonis. Customers and internal users can contact Varonis via various methods to report issues on bugs, defects, security, availability and confidentiality:

Varonis Systems, Inc also communicates security, availability and confidentiality principles to the internal users through the on-boarding process and policies and procedures available in the internal website and shared folders. Varonis communicates commitments of Security, Availability, Confidentiality and Privacy principles to external audience via Trust & Security | Varonis.

Varonis Systems, Inc has established Information Security Policies that ensure that its community of users are properly informed of their role and responsibilities based upon their level(s) of access to Varonis Systems. This policy also defines the role of each end-user in helping to safeguard sensitive and confidential information systems from internal and external threats. These following security policies apply to everyone, and enhance Varonis' security posture:

- Acceptable-Use of Assets
- Asset Management
- Backup and Restore
- Business Continuity
- Change Management
- Cloud Security
- Compliance
- Cryptography
- Data Classification
- Data Disposal
- Endpoint Security
- Human Resources Security

Roberto Revoredo Neto@petacorp.com.br
October 20 2026 11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

- Identity and Access Management
- Incident Response
- Information Security Awareness, education, and Training
- Information Transfer
- Logging and Monitoring
- Mobile Device Management
- Network Security
- Passwords
- Physical and Environmental Security
- Privacy Management
- Records Retention and Data Disposal
- Risk Management
- Secure Software Development Lifecycle
- Supplier Relationships
- Teleworking and Remote Access
- Vulnerability and Threat Management

Powered by Concierto.revored@datacenter.com on October 20, 2026 11:51 UTC

Varonis Systems, Inc is committed to and conducts its business activities lawfully and in a manner that is consistent with its compliance obligations. This includes legislative obligations, regulations, security standards, intellectual property rights, protection of records, independent review of information security, compliance with security policies and standards, contractual requirements, applicable privacy regulations industry codes and standards, as well as Varonis internal policies, standards, and procedures.

Risk Management

Varonis Systems, Inc has a risk management policy that includes risk identification, analysis, communication and reporting, treatment, and monitoring. The risk management program implements a structured security plan. Each risk is evaluated by the likelihood and impact it may cause, and the treatment plan is an ongoing effort by all Varonis Systems, Inc departments.

Enterprise Risk Management Program

The security and privacy risk management program has several levels and is conducted periodically by external and internal auditors. Company-wide risks are covered during the semi-annual enterprise risk assessment, assessed performed by the Internal Auditor, and presented to senior management and the Audit Committee of the Board of Directors. As part of the risk management program, mitigation activities to reduce the risk levels are reviewed. The CISO conveys cyberthreats, and a mitigation plan is decided and followed.

Cyber Risk Assessments

Varonis performs regular technical risk assessments for software development, Varonis DatAdvantage Cloud Platform, and corporate and cloud infrastructure (more details in the Security Testing' section). Expert third-party consultants also perform ongoing assessments. The Information Security Department led by the CISO monitors the progress of such efforts until all substantial risks are remediated. The CISO and senior management propose remediation plans, and the security steering committees decide the treatment plan.

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

Third-Party Risk Management

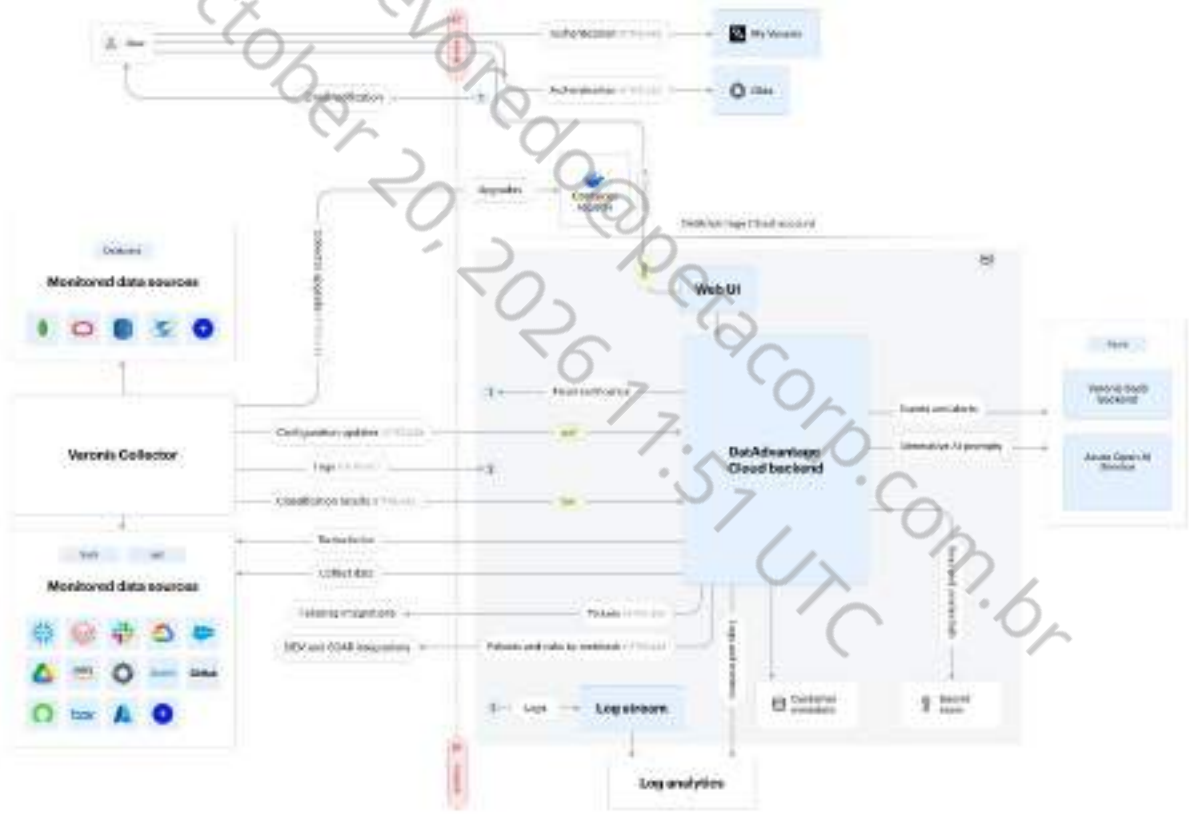
Engagements with third-party suppliers undergo a security risk assessment. It is incumbent upon Varonis Systems, Inc to ensure that vendors are capable of delivery and aware of inherent security risks. The vendor is thoroughly vetted for security and posture. We assure customers, and their data are protected and evaluate the risk by thoroughly reviewing third parties' security, compliance, and privacy practices. Whenever customer data is shared with a new third party, customers are notified, and the vendor list is updated. High-risk third parties that hold customer data undergo periodic reviews. Each engagement with potential disclosure of PII requires a Privacy assessment and signing of a mutual Data Processing Addendum. We also require a Non-Disclosure Agreement (NDA) and security agreements.

Components of the DatAdvantage Cloud Platform

Infrastructure

Varonis DatAdvantage Cloud services utilize Amazon AWS for cloud operations. Varonis Systems, Inc provides software installations of Collector services, which the customer installs on its servers inside its data center.

System Boundaries



roberto.revoredo@petacorp.com.br October 20, 2026 11:51 UTC

Varonis DatAdvantage Cloud infrastructure is deployed on Amazon AWS for hosting and operating the production, staging, and development environments. Varonis leverages the experience, resilience, and reliability of Amazon AWS to scale quickly and securely to meet our current and future demands.

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the system. Varonis Systems, Inc DatAdvantage Cloud Platform monitors various cloud platforms, such as Box, Salesforce, and AWS.

Infrastructure and Software

Varonis DatAdvantage Cloud Platform relies on several third-party services and software as part of its operations.

Varonis DatAdvantage Cloud Applications	Business Function
AWS Aurora RDS	PostgreSQL-compatible relational database used for configuration and alerts storage.
AWS Key Management System (KMS) AWS Secrets Manager AWS Certificate Manager	Create and manage cryptographic keys and secrets, used by DatAdvantage Cloud Platform for internal and external authentication.
AWS Simple Storage Service (S3)	Storage - used for operations and events data.
AWS EKS (Kubernetes)	Automated deployment, scaling, and management of containerized applications.
AWS MSK (Kafka)	Used for communication between services.
AWS ElastiCache	Caching service.
AWS SES	E-mail delivery service, used for sending DatAdvantage Cloude-mails to customers.
Neo4J	Graph database, used for storing and processing events.
Apache Tika	Detects and extracts metadata and text from over a thousand different file types.
Jenkins	Build and deploy automation.
Prometheus and Grafana	Metrics collection and visualization. Provides charts, graphs, and alerts for the DatAdvantage Cloud Platform.

roberto.revoredo@pstacorp.com.br October 29, 2025 11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

Third-Party Cloud Services

Varonis DatAdvantage Cloud relies on third-party services as part of its operations.

Varonis DatAdvantage Cloud Applications	Business Function
AWS (Amazon Web Services)	Cloud Service Provider hosting DatAdvantage Cloud Platform. Various AWS services are used as infrastructure – listed in the table above.
Datadog	Centralized observability platform. Ingest logs and metrics of DatAdvantage Cloud Platform to facilitate real-time monitoring, visualization, and alerting.
PagerDuty	Incident Management platform. Used for on-call notifications and escalations.
Twilio	Integrated with Okta to send MFA SMS messages.
Palo Alto Prisma	Cloud security platform – monitoring AWS configuration, running EKS pods.
Imperva Cloud WAF	Web application firewall.
Okta	Authentication and identity management, handling user logins and federation to customer IdP.

roberto.revoredo@petacorp.com.br October 20, 2026 11:51 UTC

Data

The customer configures what platforms will be monitored by DatAdvantage Cloud Platform. Customer metadata and data are accessed from DatAdvantage Cloud services or from Local Collector in the customer's on-prem environment. Varonis has deployed secure data transmission protocols to encrypt data when transmitting over public networks. Encryption is also enabled on databases at rest and on data backups.

Metadata and data classifications are uploaded for further analysis to Varonis DatAdvantage Cloud Platform. The data is gathered and stored in protected storage for further analysis and to identify immediate or potential risks in the customer's environment. This information is easily viewed on the Varonis DatAdvantage Cloud dashboard, including any alerts that are produced. All customer data is stored and transferred in encrypted form.

Data Processing

Customer metadata is managed, processed, and stored in accordance with the relevant data protection and other regulatory requirements. This data is managed and stored in a range of database technologies, and procedures are in place to manage separate access among tenants, periodic backups, and access control.

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

Description of the Information Systems Controls

Separation of Environments

All secrets, such as tokens for connecting to customer databases, are stored in AWS Secrets Manager. Tokens that are the responsibility of Varonis, e.g., the password for tenant databases, are periodically rotated.

Employee access to the DatAdvantage Cloud Platform is restricted and fully audited and is only allowed on demand to certain employees for a short period of time with manager approval, as described in the Access Authentication and Authorization section.

The Varonis DatAdvantage Cloud Platform is completely separated from the staging and development environments with separate access control and a segmented network. Logical segregation is performed for each customer's data and tenant.

Access Authentication and Authorization

Varonis has established and follows specific access control practices to protect information and information systems from unauthorized access, modification, disclosure, or destruction. Access to Varonis information systems is controlled by a centralized authentication, authorization, and accounting system. All staff are given network access in accordance with business access control procedures and requirements for access as defined by their roles.

A formal user registration and deregistration procedure for granting and revoking access to all information systems and services has been developed. The procedure includes an onboarding procedure and a procedure for terminating an employee's access, as part of the employee termination process.

Users are assigned to groups. When a user from that group requests access to the DatAdvantage Cloud Platform, the request requires justification and needs to be approved by the business owner for each session. Access is limited by time, and is documented, logged, and monitored by the SOC.

Physical access to Varonis' facilities is granted by the authority of the facility manager and applied on a strict need-to-know basis.

Authentication

Individuals are positively authenticated and authorized before being granted access to any Varonis information and information assets. Varonis personnel access to the corporate network and remote access to the Varonis corporate networks and the Varonis DatAdvantage Cloud Platform requires a virtual private network (VPN) or connection from the Varonis offices. Remote access sessions also require two-factor authentication. Separate accounts are used for corporate and production functions.

Authorization

No account is granted access unless the account holders and their access have been approved. Access is based on the individual's roles and responsibilities and is limited to the minimum access right necessary to perform an assigned job function (the principles of least privilege and need-to-know).

Access is reviewed on a quarterly basis and approved by the business owners to ensure that the level of access is current, necessary, and appropriate. Such access reviews are documented.

Varonis DatAdvantage Cloud Platform Access

Access to cloud production is limited based on the principles described in the sections above. The access is approved per request, is regularly monitored by Varonis' Security Operations, and is restricted to a minimal number of users.

roberto.revoredo@etacorp.com.br
October 29, 2025 11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

Customer Access

Customer employees authenticate to cloud services through the Internet using their web browser. All connections are protected using TLS. Customers authenticate using their corporate Identity Provider (federation - SSO) or using their DatAdvantage Cloud username and password.

Password Policy

When using federation with an Identity Provider, the authentication security requirements (e.g. password length and complexity, MFA, smart card, password change, failed attempts rate limit, inactivity timeout, re-login requirements) are governed and enforced by the customer.

When using DatAdvantage Cloud authentication these security requirements are enforced by DatAdvantage Cloud Platform, following industry standard practices. Password entry is masked, and users are required to change password upon initial sign-on.

Privileged Access

Privileged user accounts are strictly controlled. Their use is logged, monitored, approved, and regularly reviewed. The use of group identities is only permitted where they are suitable for the work carried out (e.g., service accounts).

Encryption

Data is encrypted at rest and in transit. Varonis uses strong ciphers with longer keys and FIPS-compliant ciphers where possible. Used ciphers and algorithms are regularly monitored to ensure deprecated versions are not used.

- Data at rest - databases and virtual machines are encrypted at rest.
- Data in transit sent over public networks is encrypted using TLS.

Network Security

Network security controls are implemented to ensure the isolation of different zones and prevent unauthorized attempts to penetrate Varonis' internal cloud security infrastructure. Similar controls are also in place for third-party cloud service vendors. The Varonis DatAdvantage Cloud environment is also protected by a web application firewall.

Security Testing

Varonis conducts rigorous security testing using various tools, techniques, and methods.

- A security design review is conducted for features involving security aspects.
- A peer programmer, who is not responsible for the change, conducts a code review on each change. Once the code review has been completed, the change is submitted to Quality Assurance (QA) for testing.
- Changes are tested in an isolated and controlled environment prior to deployment to minimize the effect on the relevant business process, to assess its impact on operations and security, and to verify that only intended and approved changes were made.
- Development changes are tested based on documented test plans, which are developed by a Business Analyst and/or Quality Assurance personnel.
- Assessment and remediation (according to the policy) are conducted on third-party, open-source, and other components identified as vulnerable.
- Automated security tests are continuously run as part of the CI/CD process.
- External and internal penetration testing is conducted on the software solution, including the OWASP Top 10 controls, at least once a year, or prior to any major version release.

Property of revolutionpetcorp.com.br
October 20, 2022 11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

- Functional security testing in the QA phase (manual or automated) that covers the designed controls and aligns with the application security verification processes (ASVS).
- Automated network and application vulnerability testing is conducted by third-party vendor software.
- Automated and manual reviews of product logs and telemetries are conducted to detect functional and security issues.

Vulnerability Scanning and Monitoring

Varonis Systems, Inc DatAdvantage Cloud Platform is periodically scanned for vulnerabilities by the following solutions:

1. Vulnerability management software.
2. Software Composition Analysis (SCA) tool to detect components with found vulnerabilities.
3. Dynamic Application Testing (DAST) tool.

Findings are handled according to a well-defined service level agreement (SLA), which is in line with industry best practices and standards.

Asset Management

Company assets are tracked and managed throughout the asset lifecycle. Each Asset has an owner assigned to it to ensure there is an individual responsible for securing the asset. The tracked assets include production components as well as employee devices that may contain personal data. When assets reach end of lifetime, they are securely destroyed to ensure that data is not recoverable.

Secure Software Development Lifecycle (SSDLC)

Varonis Systems, Inc is committed to information security at every level of the organization. It is based on industry-leading best practices and adopts a thorough secured software development lifecycle policy (SSDLC).

Our policy includes:

1. SCA - Software composition scanning for vulnerable components.
2. Security design and threat modeling reviews.
3. Secured code reviews—Performed by developers to detect and remediate security issues.
4. Secured development training—Performed annually for most developers in R&D.
5. Automated security testing—Part of the CI/CD process.
6. Security vulnerability handling procedure and SLA.
7. Periodic internal penetration testing—Performed by security experts.
8. Periodic external penetration testing—Performed by an external certified company.
9. Identification and tracking of application security issues and threat mapping and developing appropriate mitigations.
10. New features with security impact go through security architecture review, which includes threat mapping. Applicable controls are included in the feature design and development.

Software Testing and Validation Process

Varonis Systems, Inc has established Secure Software Development Lifecycle (SSDLC) process. Varonis DatAdvantage Cloud Platform applies both automatic and manual validation and quality assurance (QA) from the early stages of development. Each code change must first pass code review. Then, automatic tests are performed

roberto.revoredo@betacorp.com.br
October 20, 2026 14:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

on the code change: Each change passes unit testing and component testing. Then a set of automatic system tests are run to verify all major flows are functioning well. In addition, functionality is constantly tested manually where automation does not exist. Once all relevant tests pass (automatic and manual), there is another round of end-to-end (E2E) testing on the overall system to verify and approve deployment to production.

Change Management

Software development and change management at Varonis include development and production changes to Varonis DatAdvantage Cloud solutions.

Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are documented and approved by the management team within the change management solution.

Varonis Systems, Inc's management establishes direction and high-level objectives for change management and control. By implementing a defined change management process and policy, Varonis demonstrates increased agility in responding predictably and reliably to new business demands. The process ensures that proposed changes are reviewed, authorized, evaluated, and released in a controlled manner, and that the status of each proposed change is monitored. To fulfill this, the processes below are followed:

1. **Risk Management** - Risks related to changes are evaluated before the change is made. Proper precautions are taken to reduce the probability of the related risks.
2. **Approval** - All changes are approved by the business owner prior to deployment to production. Approval of changes is based on formal acceptance criteria, i.e., the change request was made by an authorized user, the impact assessment was performed, and the proposed changes were evaluated.
3. **Testing** - Where technically possible, changes are tested in an isolated and controlled environment prior to deployment to minimize the effect on the relevant business process, to assess its impact on operations and security, and to verify that only the intended and approved changes were made. The testing includes peer review.
4. **Deployment** - Deployment is only undertaken after appropriate testing and approval by stakeholders.
5. **Roll back** - Where applicable, procedures for aborting and recovering from unsuccessful changes are documented.

rogerio.rocha@petacorp.com.br October 29, 2026 11:51 UTC

Change Documentation

The change control process is formally defined and documented. At a minimum, the change control documentation includes the following:

- Submission date
- Start date and end date
- Description of the change
- Change requester
- Change urgency
- Impacted components
- Change approvers
- Change implementer
- Change status

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

Emergency Changes

An emergency change is usually a response to an outage or failure that needs an urgent fix. Due to the nature and urgency of these emergency changes, documentation of such changes can be done after the change has already been made. Emergency changes still require business owner approval prior to implementation.

Change Monitoring

All changes to Varonis Systems, Inc's services follow a structured process to ensure appropriate planning and execution. This structured process requires communication, documentation of important process workflows and personnel roles, and alignment of automation tools where appropriate.

The changes are monitored once they are rolled out to the production environment. Deviations from design specifications and test results are documented and escalated to the solution owner for verification.

Human Resource Policies and Procedures

Human resource (HR) policies and practices relate to hiring, onboarding, orienting, training, evaluating, counseling, promoting and compensating employees, and termination procedures. The competence and integrity of employees are essential elements of its control environment. The organization's ability to recruit and retain enough competent and responsible employees is dependent to a great extent on its HR policies and processes.

The HR policies and processes of Varonis are designed to: identify and hire competent employees, provide employees with the training and information they need to perform their jobs, evaluate the performance of employees to verify their ability to perform job assignments, and through performance evaluation, identify opportunities for growth and job performance improvement.

Formal written job descriptions are developed and maintained for each position. Each job description is reviewed and updated as needed by a manager responsible for overseeing employees with that description. Changes to formal written job descriptions are submitted to HR for review and approval. Formal written job descriptions are also prepared for contractors who work under the direct supervision of Varonis' management.

Occupational descriptions clearly articulate the job qualifications, required degrees/certifications, responsibilities, and placement in the chain of command with respect to supervisors and subordinates. Varonis' Human Resource (HR) department plays a key role in the development of its information security program by staff hiring and termination, formulating policies and procedures, and facilitating employees, awareness, training, education, and professional development.

New Hire Process

Managers within the respective functional groups of the organization determine the need for additional resources and submit formal job requisitions to senior management for approval. Once requisitions have been approved by the appropriate individual(s), HR begins sourcing for the available position. HR screens potential candidates and sends selected résumés to the respective managers. The relevant manager and HR conduct interviews and potential offers are submitted to the appropriate authority within the organization for approval.

Individuals offered a position at Varonis are subject to background checks (as appropriate for each country with respect to local laws and regulations) as a condition to their employment in the company. The background check for employees includes substantiation of educational credentials, previous employment, and criminal record, as applicable. Prospective employees complete an employment application and sign waivers to release information for the background check. In addition, it is the policy of Varonis to request employment references to determine whether the candidate is well-qualified and has the potential to be productive and successful during his or her tenure.

robert.rexford@pactera.com by October 28, 2026 11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

In each location, employees receive data packages containing an overview of Varonis' HR policies and procedures. These offer packages include the offer letter or employment contract, and the Code of Conduct. Employees are asked to sign their offer/employment contract to confirm that they have read these materials.

Vendor employees and non-employee personnel must sign an access and use agreement, the terms being like the Code of Conduct, prior to being granted access to Varonis assets or facilities.

Varonis Systems, Inc conducts background verification checks on all candidates for employment, contractors, and third-party users in accordance with relevant laws, regulations, and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

Verification checks are subject to all relevant privacy, protection of personal data and/or employment-based legislation, and where permitted, may include the following:

- Availability of satisfactory character references, e.g., one business and one personal.
- A check (for completeness and accuracy) of the applicant's resume.
- Confirmation of claimed academic and professional qualifications.
- Independent identity verification (passport or similar document).
- Additional detailed checks, such as credit checks or checks of criminal records.

Employees are obligated to agree and sign the terms of their employment contract, which states the employees' and the company's responsibilities for information security, privacy, and confidentiality.

During Employment

All employees receive appropriate Information Security and Privacy Awareness Training and regular updates in related statutes and organizational policies and procedures relevant for their role. All employees are required to complete security and privacy awareness training on an annual basis.

Varonis Systems, Inc Information Security department works with HR to provide periodic security awareness newsletters to Varonis Systems, Inc employees through emails and posters, as well as announcements on significant changes to security, availability and confidentiality. Other awareness training materials include phishing campaigns. Varonis has established a sanction policy to address non-compliance with Varonis' security policies, and disciplinary actions are taken in the event of violation.

Access Provisioning/De-provisioning

Upon hire, employees are assigned to a position in the HR management system. Prior to the employees' start date, Employees are required to sign Varonis confidentiality agreement. New hire signs an additional privacy addendum and if background checks are not permitted in their country of employment, they also undergo reliability tests. Terminated employees' access is revoked as soon as possible. Quarterly access reviews are conducted as an additional layer of access control to make sure only active employees are granted access.

Performance Evaluation

Varonis Systems, Inc has a continuous performance management process, which provides feedback for employees and managers through regular 1:1 meeting as well as Goal Plans within the Human Resources Information System (HRIS). Varonis also has an annual performance review process in place to review annual accomplishments, provide constructive feedback, identify opportunities for improvement, and development for all Varonis employees. The annual performance reviews allow managers to provide ratings for the direct reports on their team, employees to provide self-evaluations, and end with a year-end conversation between the managers and employees. This process supports alignment between employee efforts and the organization's goals.

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

Physical Access

Varonis Systems, Inc recognizes the significance of physical security controls as a key component in its overall security program.

Facilities Physical Security

Physical access protection mechanisms include entrances controlled by access cards and surveillance cameras as well as environmental security controls. Employees must have ID badges on their person when in Varonis premises, and badges are not to be shared with anyone else. Access rights are granted according to a least privileged model. Access rights are promptly removed for terminated and transferred personnel, or for personnel no longer requiring access to the facility where the information system resides. Access rights are reviewed and approved periodically by the facility manager, and guests are always accompanied by an employee when in Varonis physical areas. Varonis facilities are monitored using surveillance cameras and notification systems, such as intrusion detection sensors, locks, identification cards, and physical presence (guards and company personnel).

Incident Response

Varonis Systems, Inc has implemented incident response policies and procedures to detect, investigate, and respond to security incidents. These procedures guide Varonis' personnel in reporting and responding to information technology incidents. Additionally, these implemented procedures help Varonis to identify, response, and report on system, security, and privacy breaches. The organization's incident response phases are aligned with industry best practices and are as follows:

- Preparation - establishes policies and procedures to effectively manage incidents and enables efficient communication methods both before and after an incident.
- Detection and Analysis – Identifies and validates security incidents.
- Containment, Eradication, and Recovery - These phases addresses:
  - How to isolate systems that have been affected.
  - Restoration of services.
- Lesson Learned – Recommendations on how to handle future incidents and if necessary, what process needs to be revised.

The Incident Response plan contains procedures to address various cyber-security scenarios that may occur. Furthermore, the plan includes a communication process for stakeholders at each phase. Varonis also has cyber insurance in place and remains up to date to cover any business liability for data breaches and loss of availability in the event of a cyber incident.

Endpoint Security

Anti-Malware

Anti-malware solutions are installed on employees' endpoints to detect and prevent infection of unauthorized or malicious software. Antivirus reports are sent to relevant stakeholders on a regular basis. Additionally, Varonis uses a real-time anti-malware solution to protect its servers located at the external data centers and its private computers against viruses, worms and other forms of malicious code that may cause damage.

Software Approval and Monitoring Process

The installation of applications and software is restricted to authorized individuals. Software is fully controlled before it is implemented on the network. Processes are in place to detect changes to software and configuration parameters that may indicate unauthorized or malicious software. Antimalware software is implemented and maintained to provide for the interception or detection and remediation of malware. Software that is noncompliant with the company standards is detected and identified. Detection policies and procedures are defined. Detection tools are implemented on infrastructure and software to identify anomalies in operation or

roberto.prado@petacorp.com.br
October 26 2026 11:31 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

unusual activity on systems. Procedures include a defined governance process for security event detection and management, including the provision of resources, use of intelligence sources to identify newly discovered threats and vulnerabilities, and logging of unusual system activities. Anomalies are identified and handled by the relevant Varonis team.

Other Endpoint Security Controls

- Patch Management – The vulnerability and Threat management policy requires security patches to be installed in a timely manner. All devices are scanned for vulnerabilities, and then patches are deployed by the IT department.
- Configuration Management – Hardening policy is developed for servers and network devices.
- Mobile Device Management – A Mobile Device Management (MDM) solution is deployed for all Varonis' corporate and authenticated devices, which includes encryption, password protection, session time out, auditing and more production data is not accessible via smartphones or IoT devices.
- Restrictions on the use of removable media – Media such as USB drives are restricted of being used and monitored by the SOC.

Business Continuity and Disaster Recovery

Varonis Systems, Inc Business Continuity Plan outlines measures to avoid disruptions to customers and partners. The business continuity plan includes impact analysis and risk assessment to help identify critical functions and processes. Customer support and resiliency are top priorities. The plan includes a strategic continuity plan for the DatAdvantage Cloud Platform and customer support and cloud-based solutions, including all systems, suppliers, and users.

The business continuity plan also includes the following topics:

- Cloud production infrastructure.
- Corporate infrastructure.
- Critical suppliers.
- Cyber Incident Response.
- Pandemic Preparedness.

Backup and Restore

Varonis Systems, Inc has documented policies in place to guide personnel in system backup. The organization ensures availability and integrity of customer data by conducting regular periodic backups and restore tests.

The backup policy also contains provisions on backup systems and configurations, and all necessary data required to maintain continual operation.

- Backups are stored encrypted.
- Backup data is stored in a location at a distance from the data's principal storage location.
- Access to backups is restricted to a minimal number of authorized employees.
- Varonis uses at least daily differential backup and a weekly full backup for Varonis DatAdvantage Cloud application database.
- Varonis transactional log backups are performed based on business needs to meet its objectives.
- All data is retained according to Varonis' Privacy Policy.

roberto.revoredo@petacorp.com.br October 20 2026 11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

- Backup monitoring:
  - Varonis monitors backups and infrastructure capacity within the Varonis DatAdvantage Cloud environment.
  - Alerts are triggered to the cloud operation team when capacity reaches a defined threshold.

Additional Criteria for Availability

High availability eliminates single points of failure and helps to ensure continuous operations or uptime for an extended period. Load balancing is used to distribute traffic across multiple servers. High availability and load balanced arrays are in place for production systems to help mitigate the effect of a system error. Additionally, Varonis implemented a web application firewall to protect against denial-of-service attacks and reduce the risk of web application threats.

Support Services

Support

Varonis Systems, Inc's customer support procedures are designed to handle and resolve issues and requests in a timely manner. This includes issues that are internally identified, and issues submitted by customers. Varonis' support is provided via the support platform and support hotline. Response time to customers' issues is defined in the SLA agreement. The agreement is communicated to the customers as part of the contract.

Ticketing and Management

Varonis Systems, Inc opens a ticket when an issue is raised by a customer or when an issue is proactively identified. Varonis uses an application to manage, classify, and ticket the customer support-related issues. Tickets are classified by level of urgency and assigned to the appropriate support tier for resolution.

Escalation Process

Varonis Systems, Inc goal is to resolve issues efficiently. Issues are tracked and updated in the ticket system. The escalation process is defined and documented by Customer Support. Tickets are escalated as deemed necessary to the Infrastructure or Engineering teams. Service interruptions are communicated to clients using email based on the escalation procedures and SLA notification thresholds.

Internal Audits

Varonis has an independent internal audit team which performs audits and assessments to evaluate information systems controls on an ongoing basis. Issues that are identified are reported to management and corrective actions are taken when necessary. Preventative strategies are put in place to limit the recurrence of identified deficiencies.

External Audits

Varonis Systems, Inc is committed to ensuring compliance with industry standards including but not limited to:

1. ISO/IEC 27001:2022
2. ISO/IEC 27017:2015
3. ISO/IEC 27018:2019
4. ISO/IEC 27701:2019
5. NIST 800-53

Varonis Systems, Inc verifies compliance with this standard through various methods, including but not limited to, periodic security assessments, business tool reports, internal and external audits, and feedback to the standard owner.

roberto.oreste@petrocorp.com.br October 20, 2025 11:54 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

Complementary User Entity Controls

Varonis Systems, Inc controls related to the Varonis DatAdvantage Cloud Platform cover only a portion of the overall internal controls for each user entity of this platform. It is not feasible for the trust services criteria related to Varonis DatAdvantage Cloud Platform to be achieved solely by Varonis. Therefore, each user entity's internal control must be evaluated in conjunction with Varonis controls described in this report, taking into consideration the related complementary user entity controls expected to be implemented and operating effectively, and shown in the table below:

#	User Entity Responsibilities	Related Complemented Criteria Ref. Number
1	Ensure strong password policy.	CC6.1
2	Ensure multi-factor Authentication.	CC6.1
3	Ensure timely removal of user accounts for employees when user access is no longer required.	CC6.2
4	Configure roles and authorization – configure access to be based on the individual's roles and responsibilities and be limited to the minimum access right necessary to perform an assigned job function.	CC6.3
5	Integrating with monitored platforms/applications in a secure manner and according to necessary compliance requirements.	CC6.1, CC6.7
6	Notify Varonis of unauthorized use of any account or other breaches related to the security, availability, and confidentiality in service usage.	CC4.2, CC7.2, CC7.4
7	Tenant geolocation selection during the deployment phase.	CC2.3, A1.2

roberto.revoredo@netacorp.com.br
October 29, 2026 11:51 UTC

Subservice Organizations carved-out controls:

The following table presents the applicable Trust Services criteria that are intended to be met by controls at Amazon AWS, alone or in combination with controls at Varonis, and the types of controls expected to be implemented at Amazon AWS to meet those criteria. The subservice organization is SOC 2 certified and is not included in the scope of this report.

#	Control Activity Expected to be Implemented by Amazon AWS	Applicable Trust Service Criteria
1	Subservice organizations are responsible for managing logical access to the underlying network, virtualization management, and storage devices for their infrastructure as a Service (IaaS) cloud hosting services where Information systems reside.	CC6.1 – CC6.4, CC6.6
2	Subservice organizations are responsible for the secure disposal of end of life and decommissioned physical devices which hold Varonis data.	C1.2

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

3	Subservice organizations are responsible for implementing controls to detect and address vulnerabilities impacting the infrastructure components supporting the cloud services utilized by Varonis.	CC 7.1
4	Subservice organizations are responsible for implementing and maintaining environmental protection.	A1.2
5	Subservice organizations are responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.	CC6.4
6	Subservice organizations are responsible for providing and maintaining the environmental security systems (fire detection and suppression systems, UPS systems, generators, air conditioning units, and CCTV Monitoring) at the data center facilities.	A1.2
7	Subservice organizations are responsible for revoking access to the scoped data centers in a timely manner of employee or vendor record being deactivated.	CC6.2
8	Subservice organizations are responsible for periodically reviewing access to the scoped data center by appropriate personnel.	CC6.2
9	Subservice organizations are responsible for monitoring and maintaining processing capacity on an ongoing basis.	A1.1
10	Subservice organizations are responsible for notifying Varonis of unauthorized use of any account or other breaches related to the security, availability, confidentiality, and Privacy in service usage.	CC7.1 - CC7.5
11	Subservice organizations are responsible for installing anti-malware solutions to detect or prevent unauthorized or malicious software on hosted systems managed by the subservice organizations.	CC6.8
12	Subservice organizations are responsible for implementing strong authentication mechanisms.	CC6.1
13	Subservice organizations are responsible for monitoring backup operations impacting the infrastructure components and alerting backup failures.	A1.2

Roberto.rezende@etrcorp.com.br
October 20 2026 11:51 EDT

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

Section IV - Trust Services Criteria, Related Controls and Tests of Controls

Overview

This section describes, for the Security, Availability and Confidentiality principles – from the criteria in the 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy. We have included the recommended controls implemented in order to meet those criteria including mapping to the relevant criteria:

The security principle, defined as the system being protected against unauthorized access, use, or modification, refers to the protection of the system resources through logical and physical access control measures in order to support the achievement of management's commitments and requirements related to security, availability, processing integrity, and confidentiality. Controls over the security of a system prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of data or system resources, misuse of software, and improper access to, or use of, alteration, destruction, or disclosure of information.

The confidentiality principle, defined as Information designated as confidential is protected as committed or agreed, addresses the system's ability to protect information designated as confidential in accordance with the organization's commitments and requirements through its final disposition and removal from the system. Information is confidential if the custodian of the information, either by law or regulation, the custodian's own assertion, commitment, or other agreement, is obligated to limit its access, use, and retention, and restrict its disclosure to a specified set of persons or organizations (including those that may otherwise have authorized access within the boundaries of the system). The need for information to be confidential may arise for many different reasons. For example, the information is proprietary information, information intended only for company personnel, personal information, or merely embarrassing information.

The availability principle, defined as the system, is available for operation and use as committed or agreed, refers to the accessibility of the system, products, or services as committed by contract, service level agreement, or other agreements. This principle does not set a minimum acceptable performance level for system availability. The availability principle does not address system functionality (the specific functions a system performs) and system usability (the ability of users to apply system functions to the performance of specific tasks or problems) but does address whether the system includes controls to support system accessibility for operation, monitoring, and redundancy.

Testing Performed and Results of Tests of Entity-Level Controls

In Planning the nature, timing, and extent of its testing of the controls specified by company - KPMG considered the aspects of the company's control environment, risk assessment processes, information and communication and management monitoring procedures and performed such procedures as considered necessary in the circumstances.

Property of edoc@stacorp.com.br October 20, 2020 11:24 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

Testing Methods

Various testing methods are used to assess the operating effectiveness of controls during the Specified Period. The table below describes the optional various methods in testing the operating effectiveness of controls that are in place at the Company.

TYPE	DESCRIPTION
Inquiry	Inquired of appropriate personnel seeking relevant information or representation including, among other things: • Knowledge and additional information regarding the policy or procedure. • Corroborating evidence of the policy or procedure. As inquiries were performed for substantially all controls, the test was not listed individually for every control shown in the accompanying matrices.
Observation	Observation consists of looking at a process or procedure being performed by others. Observation can provide audit evidence about the performance of a process or procedure, but the evidence is limited to the point in time at which the observation takes place and is limited by the fact that the act of being observed may affect how the process or procedure is performed Observed the application or existence of specific controls as represented.
Inspection	Inspection involves examining records or documents, whether internal or external, in paper form, electronic form, or other media, or physically examining an asset. Inspection of records and documents provides audit evidence of varying degrees of reliability, depending on their nature and source and, in the case of internal records and documents, on the effectiveness of the controls over their production. An example of inspection used as a test of controls is inspection of records for evidence of authorization.
Re-performance	Re-performance involves the independent execution of procedures or controls that were originally performed by company personnel.

roberto.resendo@pecegroup.com.br
October 20 2020 11:54 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

Security Principle and Criteria

Control Environment

CC1.1 / COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
1	Varonis has established a Conduct and Ethics (hereafter "Code of Conduct") which refers to the following issues. 1. Compliance with laws, rules, and regulations. 2. Conflicts of interest. 3. Insider trading. 4. Corporate opportunities. 5. Competition and fair dealing. 6. Discrimination and harassment. 7. Health and safety. 8. Record-keeping. 9. Confidentiality. 10. Protection and proper use of company assets. 11. Payments to government personnel. 12. Waivers of the code of business conduct and ethics. 13. Reporting any illegal or unethical behavior. 14. Compliance procedures.	Inspected Varonis' Code of Business Conduct and determined that all topics mentioned are included.	No deviations noted.
2	The Code of Conduct is accessible on Varonis' website and is approved by the Board of Directors.	Inspected documentation to ascertain that Varonis' Code of Business Conduct is accessible on the company's website.	No deviations noted.
		Inspected documentation to ascertain that Varonis' Code of Business Conduct was approved by the Board of Directors.	No deviations noted.
3	Once a year, the Chief Human Resources Officer (CHRO) distributes the Code of Conduct to all Varonis' employees via e-mail.	Inspected an email sent by the CHRO during the audit period and ascertain that the Code of Conduct was communicated to all employees.	No deviations noted.

roberto.revoredo@petacorp.com.br October 20, 2026 14:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
4	Varonis Whistleblower Hotline is in place for employees to report violations anonymously.	Inspected whistleblower system to ascertain that Varonis Whistleblower Hotline is in place.	No deviations noted.
5	Deviations or suspicion from the Varonis expected standards of conduct can be reported anonymously to the Audit Committee. The Audit Committee is responsible for investigating those incidents and tracks matters through resolution.	Inspected documentation to verify that deviations from Varonis expected standards of conduct can be reported anonymously to the Audit Committee.	No deviations noted.
		Inspected the whistleblower system and management meeting summary and determined that no deviations were reported within the audit period.	No deviations noted.
6	According to Varonis "Code of Business Conduct and Ethics," for each case of violation of the Code of Conduct, management response is based on the event severity. Those who violate the standards in the Code of Conduct may be subject to disciplinary action, up to and including termination of employment.	Inspected Varonis' Code of Business Conduct and determined that violating Varonis' standards may be subject to disciplinary action up to and including termination of employment.	No deviations noted.
		Obtained written confirmation from the company's legal counsel stating that there are no violations of the Code of Business Conduct and Ethics occurred during the audit period.	No deviations noted.
7	Cases of deviation from integrity and ethical values, if any, are treated promptly and communicated to the relevant levels within the company and reported as needed to the Audit Committee. In addition, and for some cases and as needed, the case of violation is communicated to the Company's employees.	Inspected Varonis' Code of Business Conduct to ascertain that deviation cases are treated promptly and communicated to relevant levels within the organization and as needed, to the Audit Committee and employees.	No deviations noted.
		Observed the relevant reporting mechanisms and inspected management and Audit Committee meeting summaries to determine whether any deviation cases occurred and were communicated during the audit period.	No deviations noted.

CC1.2 / COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
8	The Board of Directors reviews and approves the company's annual business plan and budget.	Inspected Board meeting minutes and determined that annual business plan and budget were approved by the board.	No deviations noted.

Document received by eSignGlobal.com.br
October 20, 2021 6:11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
9	The Board of Directors reviews, on a quarterly basis, the company's performance, including actual financial results in relation to budgets and business plans. Board members raise questions and receive information during the Board meeting from the CEO/CFO.	Obtained a list of Board meetings held during the audit period and verified the completeness of the list.	No deviations noted.
		For a sample of meetings, inspected protocols and determined that (1) the Board of Directors reviews the company's performance on a quarterly basis, including actual financial results in relation to budgets and business plans, and (2) Board members raise questions and receive information from the CEO/CFO during the meeting, as documented in the meeting minutes.	No deviations noted.
10	The Board of Directors includes adequate number of directors with different skills and expertise that allow them to ask probing questions of management and to take appropriate actions.	Obtained a list of Varonis Board members and verified its completeness.	No deviations noted.
		For a sample of Board members, inspected documentation to ascertain that the selected Board members are independent and possess Relevant professional expertise.	No deviations noted.
11	The Board of Directors includes at least one financial expert according to the Securities and Exchange Commission (SEC) requirements.	Obtained a list of Varonis Board members and verified its completeness.	No deviations noted.
		Inspected documentation to ascertain that at least one board member is a financial expert.	
12	The Board of Directors includes at least two independent directors according to the independence definition of applicable laws (under the listing rules of NASDAQ).	Obtained the list of Board members and verified its completeness.	No deviations noted.
		Inspected supporting documentation to ascertain that at least two directors meet the independence definition under NASDAQ listing rules during the audit period.	No deviations noted.

Roberto Prevedello Peterson 20:26:51 UTC October 2021

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

CC1.3 / COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
13	Varonis has developed an organizational chart which sets forth roles and respective reporting lines for all units of function.	Inspected documentation to ascertain that an organizational chart is in place and includes roles and reporting lines.	No deviations noted.
		For a sample of units, inspected documentation to ascertain that an organizational chart is in place and clearly defines roles and reporting lines.	No deviations noted.
14	Policies and procedures, relevant to security, availability, processing integrity, confidentiality, and privacy, are documented, timely updated, and communicated to staff.	Inspected documentation to ascertain those policies and procedures relevant to security, availability, processing integrity, confidentiality, and privacy are documented and updated in a timely manner.	No deviations noted.
		Inspected the company's portal and determined that policies and procedures are communicated to staff.	No deviations noted.

CC1.4 / COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
15	Information Technology Policies and Procedures for IT security and computer operations are documented, timely updated, and communicated to staff.	Inspected Information Technology Policies and Procedures for IT security and computer operations to ascertain that they are documented and updated in a timely manner.	No deviations noted.
		Inspected the company portal and/or related communications to determine that the policies and procedures are communicated and available to relevant staff.	No deviations noted.

roberto.revoredo@etacorp.com.br October 20, 2026 11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
16	Background verification checks on all candidates for employment, contractors, and third-party users are carried out where applicable and in accordance with relevant laws, regulations, and ethics, and proportional to the business requirements, and the perceived risks.	Obtained a list of candidates, contractors, and third-party users and verified its completeness.	No deviations noted.
		For a sample of candidates, contractors, and third-party users, inspected background check evidence to determine that screening was completed in accordance with company policy.	No deviations noted.

CC1.5 / COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
17	Varonis has defined roles and responsibilities for all positions to increase accountability.	Inspected documentation to ascertain that roles and responsibilities are defined within the Security and Privacy Policies	No deviations noted.
18	Varonis established a regular schedule for conducting employee performance evaluations, ensuring that evaluations are performed at defined intervals.	Obtained a list of employees and verified its completeness.	No deviations noted.
		For a sample of employees, inspected documentation to ascertain that the selected employees undergo annual and mid-year performance review.	No deviations noted.

Communication and Information

CC2.1 / COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
19	Varonis has established a set of Information Security and privacy policies.	Inspected documentation to ascertain that Varonis has established a set of policies relevant to information security and privacy.	No deviations noted.

roberto.revoredo@pfeiffercorp.com.br October 2020 11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
20	Threat Intelligence and other external scanning resources are used to scan Varonis' external assets and accounts. This information is reviewed by the SOC and action items are taken place, based on the severity.	Observed threat intelligence and external scanning resources used to scan external assets/accounts and inspected SOC procedures.	No deviations noted.
		For a sample of findings/alerts, inspected evidence of review by the SOC and related action items to determine that items were triaged and handled based on severity during the audit period.	No deviations noted.
21	Varonis uses various sources to capture external data relevant to internal controls including, but not limited to penetration testing, and external scanning.	Inspected documentation and systems to ascertain that Varonis uses multiple external sources to capture data relevant to internal controls.	No deviations noted.
		Inspected penetration test reports and observed external scanning tool evidence to determine that external scanning activities were performed during the audit period.	No deviations noted.
22	Acceptance Test Plan is defined. Manual and automated testing are performed on new candidate production builds by the system QA team.	Obtained a list of tests performed on new production builds and verified its completeness.	No deviations noted.
		For a sample of tests, inspected documentation to ascertain that manual and automated testing performed by the system QA team are in place.	No deviations noted.

Roberto.revoredo@petacorp.com.br
October 20, 2020 11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

CC2.2 / COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
23	Each employment agreement is signed by both the employee and Company's representative. All employees are required to sign Varonis' Non-Disclosure agreement (NDA). The NDA includes provisions regarding keeping client's data private and policies kit that includes, inter alia, Code of Conduct and Anti-Bribery and Corruption Policy.	Obtained a list of employees and verified its completeness.	No deviations noted.
		For a sample of employees, inspected signed employment agreements and Non-Disclosure Agreements (NDAs) to ascertain that the agreements were executed by both the employee and an authorized company representative, and that the NDAs include confidentiality obligations related to client data and reference to the company's policies, including the Code of Conduct and Anti-Bribery and Corruption Policy.	No deviations noted.
		For the same sample, inspected signed privacy addendums to confirm acknowledgment of data privacy obligations by employees.	No deviations noted.
24	Employees with access to the cloud production environment are required to sign additional privacy addendum and successfully pass reliability test.	Obtained a list of employees with access to the cloud production environment and verified its completeness	No deviations noted.
		For a sample of employees, inspected the following: a. Signed privacy and confidentiality undertaking (including the additional privacy addendum). b. Evidence of successfully passing the reliability/background check.	No deviations noted.
25	Varonis Whistleblower Hotline is in place for employees to report violations anonymously.	Inspected documentation to ascertain that a whistleblower hotline is in place.	No deviations noted.
26	Employees are provided with training on how to report security incidents to the Security Operations Center.	Inspected documentation to ascertain that employees are provided with information on how to report security incidents.	No deviations noted.

roberto.rezende@peteca.com.br October 20, 2026 11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
27	Varonis' has established a security awareness training program.	Inspected a Security Awareness curriculum to ascertain that Varonis has established a security awareness training program.	No deviations noted.
		Obtained a list of employees and verified completeness.	No deviations noted.
		For a sample of employees who did not complete the training, inspected evidence of follow-up notifications.	No deviations noted.
28	The security awareness program includes annual training modules, monthly newsletters, and periodic phishing campaigns. Follow-up notifications are sent to personnel who have not completed the training.	Inspected documentation to ascertain that the security awareness program includes annual training modules, monthly newsletters, and periodic phishing campaigns.	No deviations noted.
		For a sample of users who did not complete the awareness training, inspected evidence of follow-up notifications and tracking of completion status.	No deviations noted.
29	Varonis provides annual privacy training to all employees. The training covers the organization's privacy policies and procedures, applicable laws and regulations, and best practices for protecting customer data.	Inspected documentation to ascertain that training covers the organization's privacy policies and procedures, applicable laws and regulations, and best practices for protecting customer data.	No deviations noted.
		Obtained a list of employees and verified its completeness.	No deviations noted.
		For a sample of employees, inspected documentation to ascertain those employees completed annual privacy training.	No deviations noted.

CC2.3 / COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
30	Varonis Whistleblower Hotline is in place for employees to report violations anonymously.	Inspected documentation to ascertain that Whistleblower Hotline is in place	No deviations noted.

roberto.revoredo@etacorp.com.br October 20 2026 1:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
31	Varonis' security and availability commitments and the associated system requirements are documented in customer agreements.	Inspected documentation to ascertain that Varonis' security and availability commitments and the associated system requirements are documented.	No deviations noted.

Risk Assessment

CC3.1 / COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
32	The Board of Directors reviews, on a quarterly basis, the company's performance, including actual financial results in relation to budgets and business plans. Board members raise questions and receive information during the Board meeting from the CEO/CFO.	Obtained a list of Board meetings held during the audit period and verified its completeness.	No deviations noted.
		For a sample of meetings, inspected protocols and determined that (1) the Board of Directors reviews the company's performance on a quarterly basis, including actual financial results in relation to budgets and business plans, and (2) Board members raise questions and receive information from the CEO/CFO during the meeting, as documented in the meeting minutes.	No deviations noted.

CC3.2 / COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
33	The Audit Committee appointed an internal auditor to provide independent and objective evaluations of financial and operational business activities.	Inspected formal appointment documentation to ascertain that the internal auditor was appointed by the Audit Committee, is independent from management, and operates under the direct oversight of the Audit Committee	No deviations noted.

Roberto Revoredo Contacorp.com.br
October 2026 15:51 ART

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
34	The internal auditor performs audits according to the Audit Committee instructions and presents to them his findings and recommendations for improvement. Follow-up reviews are performed as necessary.	Inspected documentation to ascertain that internal audit was performed, presented, and tracked.	No deviations noted.
		Inspected documentation to ascertain that follow-up reviews were performed within the audit period.	No deviations noted.
35	Based on results of the Risk Assessment and Fraud Risk Assessment, the company performs mitigations which presented to the Audit Committee.	Inspected documentation to ascertain that risk assessment and fraud risk assessment have been performed.	No deviations noted.
		Inspected documentation to ascertain that mitigation plan is in place and is based on the risk assessment and the fraud risk assessment.	No deviations noted.
36	Risk identification considers internal and external factors and their impact.	Inspected documentation to ascertain that internal and external factors and their impact are considered in the internal audit report.	No deviations noted.
37	Risk assessment process includes the following: - Interviews with management members - Assigning risk rating - Assessing the risk likelihood - Assessing the risk impact -Identification of mitigating activities to reduce risk	Inspected documentation to ascertain that risk assessment methodology is in place and includes the mentioned elements.	No deviations noted.
38	Vendor risk assessments are conducted during the engagement phase.	Inspected documentation to ascertain that Vendors Policy is in place and includes clauses related to risk analysis phase before entering a contract with a supplier.	No deviations noted.
		Obtained a list of vendors and verified its completeness.	No deviations noted.
		For a sample of vendors, observed the vendors management system to ascertain that risk assessments were conducted during the engagement phase.	No deviations noted.
39	Annual assessment is performed for high-risk and cloud production services.	Obtained a list of high-risk and cloud production services and verified its completeness.	No deviations noted.
		For a sample of services, inspected documentation evidencing annual assessments, including review of ISO 27001 and SOC 2 reports.	No deviations noted.

Roberto.reis@metacorp.com.br
October 20, 2026 11:51 ART

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
40	Varonis has established a Third-Party Risk Management Policy.	Inspected Information Security and Privacy Policies and determined that the Third-Party Risk Management Policy is included	No deviations noted.

CC3.3 / COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
41	The Board of Directors reviews and approves the company's annual business plan and budget, presented by the Chief Executive Officer (CEO)/Chief Financial Officer (CFO).	Inspected Board meeting minutes and supporting documentation to determine that the annual business plan and budget presented by the CEO/CFO were reviewed and approved by the Board of Directors during the audit period.	No deviations noted.

CC3.4 / COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
42	Varonis has established a change control policy. Changes related to DatAdvantage Cloud Platform undergo the change control process and changes are documented.	Inspected the Change Management Policy to verify that it is formally documented and addresses key elements of the change control process, including review, approval, and documentation requirements.	No deviations noted.
43	Varonis' Change Management Policy includes the procedure for emergency changes.	Inspected documentation to ascertain that emergency Change procedures are included within the Change Management Policy.	No deviations noted.

roberto.revoredo@preacorp.com.br
October 20, 2026 15:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

Monitoring Activities

CC4.1 / COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
44	Varonis uses both technical and non-technical evaluations as well as internal and external audits, including penetration testing, vulnerability scanning and internal audits.	Inspected a penetration test report to ascertain that penetration test was performed by an external party within the audit period.	No deviations noted.
		Inspected documentation to ascertain that internal audit took place within the audit period by relevant personnel.	
		Obtained a list of reports and scan-results and verified its completeness. For a sample of vulnerability scan results, inspected documentation to ascertain that they were logged, assigned an owner, triaged by the information security team and addressed by relevant personnel.	No deviations noted.

CC4.2 / COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
45	The results of the internal audit are reported to management, which decides on the action items deriving from the results.	Inspected internal audit reports and evidence of reporting results to management.	No deviations noted.
		For a sample of audits, inspected documentation evidencing that management defined action items resulting from the audit results	No deviations noted.

roberto.revoredo@etacorp.com.br October 20 2020 11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
46	Deficiencies from the internal audit are communicated to senior management and business owners, which decides on the corrective actions.	Inspected documentation related to internal audit deficiencies to ascertain that identified deficiencies are communicated to senior management and relevant business owners.	No deviations noted.
		Inspected documentation evidencing management review of identified deficiencies and decisions regarding corrective actions taken in response to the internal audit findings during the audit period.	No deviations noted.
47	Internal control deficiencies are tracked by the Internal auditor and business owners until remediation is complete.	Inspected documentation to ascertain that mitigation plan is in place.	No deviations noted.
		Inspected documentation to ascertain that internal control deficiencies are tracked, monitored and communicated.	No deviations noted.

Control Activities

CC5.1 / COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
48	Risk assessment is conducted annually and reported to senior management.	Inspected the annual risk assessment documentation and management communications to ascertain that the risk assessment was conducted and its results were reported to and reviewed by senior management during the audit period.	No deviations noted.

roberto.vedoato@petacorp.com.br
October 20, 2026 11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

CC5.2 / COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
49	Varonis uses both technical and non-technical evaluations as well as internal and external audits, including penetration testing, vulnerability scanning and internal audits.	Inspected a penetration test report to ascertain that penetration test was performed within the audit period by an external party.	No deviations noted.
		Inspected documentation to ascertain that internal audit took place within the audit period by relevant personnel.	No deviations noted.
		Obtained a list of reports and scan-results and verified its completeness. For a sample of vulnerability scan results, inspected documentation to ascertain that they were logged, assigned an owner, triaged by the information security team and addressed by relevant personnel.	

CC5.3 / COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
50	Security Policies were established and published in the company portal.	Inspected documentation to ascertain that policies and procedures are in place.	No deviations noted.
		Inspected Varonis' portal and determined that security policies are published in the company portal.	No deviations noted.

roberto.evora@petacorp.com.br October 20, 2020 11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
51	Policies are reviewed and approved by CISO and Senior Management once a year.	Inspected a list of policies and procedures. For a sample of policies and procedures, inspected documentation to ascertain that they were reviewed and approved by the CISO and senior management within the audit period.	No deviations noted.
52	Responsibilities are documented within each policy.	Inspected a list of policies and procedures and verified its completeness. For a sample of policies inspected, clauses relevant for roles and responsibilities.	No deviations noted.

Logical and Physical Access Controls

CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
53	Inventory of Varonis' internal assets are identified and managed within asset inventory system.	Observed the asset inventory system to ascertain that Varonis' internal assets are identified and managed within the system.	No deviations noted.
54	Strong password configuration settings are enabled on DatAdvantage Cloud Platform and Varonis corporate environments using Group Policies. These settings include: 1. Forced password change at defined intervals. 2. A minimum password length. 3. A limit on the number of unsuccessful attempts to enter a password before the user ID is suspended. 4. Password complexity requirements. 5. Maximum and Minimum Password Age. 6. Password History.	Inspected DatAdvantage Cloud Platform password configuration settings and observed access process to Varonis DatAdvantage Cloud Platform and Varonis corporate environments and determined that passwords are enabled with the mentioned settings and enforced.	No deviations noted.

roberto.revoredo@ppeacorp.com.br
October 20, 2020 11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
55	The DatAdvantage Cloud Platform network is segmented using VPCs to protect computing resources, and prevent unauthorized access to customer's data, keys and/or internal resources.	Inspected documentation to ascertain that security zones are documented, and network segmentation is in place.	No deviations noted.
56	An architecture diagram with all points of access is developed, maintained, and reviewed periodically by the system architecture. All points of access are identified, inventoried, and managed.	Inspected documentation to ascertain that the architecture diagram is in place and approved by the system architect.	No deviations noted.
		Inspected documentation to ascertain that access points are identified, inventoried, and managed.	No deviations noted.
57	Access Control policy to the DatAdvantage Cloud Platform infrastructure is documented, and includes, but not limited to: • Limited access based on the principals of least privilege and need-to-know. • Approved per access. • Restricted to a minimal number of users. • multi-factor authentication (MFA). • Limited by time.	Inspected documentation and system configurations to ascertain that an Access Control Policy for the DatAdvantage Cloud Platform infrastructure is in place and includes access restrictions based on the principles of least privilege and need-to-know, requires approval for each access, limits access to a minimal number of users, enforces multi-factor authentication (MFA), and restricts access by time through session-based activation and periodic reauthentication mechanisms.	No deviations noted.
58	System servers and databases are encrypted at rest with industry standard ciphers.	Observed encryption-at-rest configurations and inspected documentation to ascertain that system servers and databases are encrypted at rest using industry standard ciphers.	No deviations noted.
59	Encryption keys are rotated once a year.	Inspected key management configurations and related system evidence to ascertain that encryption keys are configured to rotate once a year.	No deviations noted.
60	Varonis Security Operation Center (SOC) team configures and monitors alerts from various information security systems related to DatAdvantage Cloud Platform. Alerts are triaged and resolved in a timely manner.	Inspected documentation to ascertain that DatAdvantage Cloud Platform is monitored.	No deviations noted.
		Observed SOC alerting configurations to ascertain that alerts are configured and enforced.	
		For a sample of dates, inspected incident tickets to ascertain that alerts are triaged and resolved in a timely manner.	No deviations noted.

Report generated by A-LIGN.com.br October 2020 Version 1.0

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
61	Audit logs of Varonis DatAdvantage Cloud Platform are collected and monitored by the Security Operation Center (SOC).	Observed log collection and monitoring solutions to ascertain that audit logs are collected and actively monitored by the SOC	No deviations noted.

CC6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
62	Access to DatAdvantage Cloud Platform is provided to new employees after completion of screening process.	Obtained a list of new employees granted access to the DatAdvantage Cloud Platform during the audit period and verified its completeness.	No deviations noted.
		For a sample of new hires, inspected evidence of completed screening prior to access provisioning and inspected provisioning records to confirm access was granted after screening completion.	No deviations noted.
63	Termination process is in place and documented. Terminated employees' access is revoked following HR notification.	Inspected documentation to ascertain that termination process is in place.	No deviations noted.
		Obtained a list of employees terminated during the audit period and verified its completeness.	No deviations noted.
		For a sample of terminated employees, inspected documentation to ascertain that terminated employees' access was revoked following HR notification.	No deviations noted.
64	DatAdvantage Cloud Platform access reviews are performed and documented on quarterly basis.	Inspected documentation and determined that user access reviews were performed and documented on a quarterly basis by relevant personnel.	No deviations noted.
		For a sample of quarters, inspected evidence of access review and determined that user access review was performed and approved by relevant personnel.	No deviations noted.

Report Generated for Roberto Fevereiro Corretor de Seguros - 01/10/2021 to 31/10/2021 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

CC6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, considering the concepts of least privilege and segregation of duties, to meet the entity's objectives.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
65	Logical and Physical Access is removed when no longer needed during termination process - Employees are restricted from accessing using conditional access rules.	Obtained a list of terminated employees during the audit period and verified its completeness.	No deviations noted.
		For a sample of terminated employees, inspected evidence to confirm that their logical and physical access was removed in a timely manner as part of the termination process. Additionally, observed that conditional access rules and determined that they are enforced to restrict access when it is no longer required.	No deviations noted.

CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
66	As part of the global termination process, automation is in place to disable accounts which are terminated in the physical access system.	Observed the automated termination process within the physical access management system to ascertain that user accounts are automatically disabled upon employee termination.	No deviations noted.
		Obtained a list of terminated employees to verified its completeness.	No deviations noted.
		Inspected system evidence to determine that physical access accounts associated with terminated employees were disabled as part of the automated termination process.	No deviations noted.

roberto.revoredo@petacorp.com.br October 20, 2020 15:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
67	The physical access management system is maintained through automated processes. Reviews of system administrators and global physical access cards are performed on a semi-annual basis to ensure that access is restricted to authorized personnel only.	Inspected documentation related to the physical access management system to ascertain that reviews of system administrators and global physical access cards are performed on a semi-annual basis.	No deviations noted.

CC6.5: The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
68	Varonis has implemented a procedure for the deletion of customer data upon the conclusion of the subscription period.	Inspected documentation to ascertain that a procedure for deletion of customer data upon subscription termination is documented and implemented.	No deviations noted.
69	Varonis established and maintained a documented asset disposal policy that includes procedures for the secure disposal of corporate physical assets, ensuring that all data stored on the assets are completely wiped or destroyed prior to disposal.	Inspected documentation to ascertain that a documented asset disposal policy is in place and includes procedures for secure disposal of corporate physical assets.	No deviations noted.

CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
70	Remote access to the corporate and DatAdvantage Cloud Platform networks requires Virtual Private Network (VPN) and Multi Factor Authentication (MFA).	Inspected configuration to ascertain that access to corporate and Varonis DatAdvantage Cloud Platform environments requires VPN and MFA.	No deviations noted.

Powered by reveregeneta corp.com.br
October 20, 2026 1:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
71	Varonis DatAdvantage Cloud Platform maintains logical segregation between customer's data.	Inspected system architecture and configuration, including tenant isolation mechanisms, to ascertain that logical segregation between customers' data within the DatAdvantage Cloud Platform is implemented.	No deviations noted.
72	A firewall is in place to segregate internal and external resources, controlling network traffic and preventing unauthorized access to protect the organization's systems and data.	Inspected documentation to ascertain that the firewall segregates internal and external resources.	No deviations noted.
73	Varonis has implemented a Web Application Firewall (WAF) to provide protection against denial-of-service attacks and web application attacks	Inspected documentation to ascertain that the architecture of Varonis DatAdvantage Cloud Platform is in place and includes a WAF.	No deviations noted.
		Inspected WAF configuration and determined that WAF is configured to protect the external boundary from application vulnerabilities and attacks	No deviations noted.

CC6.7: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
74	Encryption in transit is performed to secure transmission of data. Data is encrypted using TLS 1.2 or higher.	Inspected documentation to ascertain that data transmitted by the DatAdvantage Cloud Platform is encrypted in transit using TLS 1.2 or higher.	No deviations noted.

Roberto.Reyes@peracorp.com.br
October 20 2023 11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
75	The use of removable media on Varonis issued devices is prohibited and restriction is enforced by the security policy.	Inspected documentation to ascertain that Removal Media Policy is in place.	No deviations noted.
		Inspected system configuration to ascertain that the use of removable media on Varonis-issued devices is restricted and enforced by the security policy.	No deviations noted.
76	The Varonis Mobile Device Policy includes security measures to protect company data on mobile devices. This includes password protection, prohibition of rooted or jailbroken devices, and remote wipe.	Inspected documentation to ascertain that Mobile Device Management Policy is in place.	No deviations noted.
		Inspected documentation to ascertain that a Mobile Device Management (MDM) policy has been configured.	No deviations noted.

CC6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
77	Varonis has implemented a tool to limit user's permissions to install applications and software.	Inspected system configuration to ascertain that a dedicated tool is implemented to restrict user's permissions to install applications and software.	No deviations noted.
78	A software approval process has been established and requires Legal and IT Security department's approval for each new software.	Inspected documentation and observed the software approval workflow to ascertain that Legal and IT Security approvals are required prior to installation.	No deviations noted.
		For a sample of software requests, inspected evidence of Legal and IT Security approvals.	No deviations noted.
79	Changes to software at endpoints require administrative accounts and can only be performed by IT Help Desk after security and legal department's approval.	Inspected system configuration and endpoint management documentation to ascertain that software changes on endpoints require administrative accounts and are performed by IT Help Desk following Legal and Security approval.	No deviations noted.

roberto.reboredo@peteorp.com.br October 20, 2023 11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
80	Varonis monitors issued laptops and workstations for compliance with policies for: 1. Full disk encryption. 2. Antimalware and Endpoint Detection and Response (EDR) software installation and continuous monitoring. 3. Session timeout. 4. Other endpoint security solutions as specified by Varonis internal security policies.	Inspected system and documentation to ascertain that Varonis monitors issued laptops and workstations for compliance with the following policies: 1. Full disk encryption. 2. Antimalware and EDR software installation and continuous monitoring. 3. Session timeout.	No deviations noted.
		Inspected documentation to ascertain that noncompliance with the endpoint security policy is addressed by the IT department.	No deviations noted.

System Operations

CC7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
81	A baseline and hardening Configuration policy that is aligned with the Center for Internet Security (CIS) Configuration recommendation is configured consistently and documented for Varonis DatAdvantage Cloud Platform assets.	Inspected documentation to ascertain that a Baseline and Hardening Configuration Policy have been developed and documented for Varonis DatAdvantage Cloud Platform assets.	No deviations noted.
82	Secure system hardening policy for Varonis' end points is in place to facilitate the configuration process and maintain consistency.	Inspected documentation to ascertain that a secure system hardening policy for Varonis' endpoints is documented and implemented to support consistent configuration.	No deviations noted.
83	Varonis has implemented a tool to limit user's permissions to install applications and software.	Inspected system configuration to ascertain that a dedicated tool is implemented to restrict users' permissions to install applications and software.	No deviations noted.
84	A Software approval process is established and requires legal and security department's approval for each new software.	Inspected documentation to ascertain that a software approval process is established and requires Legal and IT Security department approval prior to installation.	No deviations noted.
		For a sample of software requests, inspected evidence of Legal and IT Security approvals.	No deviations noted.

roberto.revoredo@pelacon.com.br October 20, 2020 11:31 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
85	Vulnerability scans of DatAdvantage Cloud Platform are performed to identify threats and assess their potential impact to system confidentiality, integrity, and availability. Security vulnerabilities are triaged by the information security team and remediated according to the security policy.	Inspected reports to confirm that vulnerability scans were performed during the audit period.	No deviations noted.
		Obtained a list of reports and scan-results and verified its completeness. For a sample of vulnerability scan results, inspected documentation to ascertain that they were logged, assigned an owner, triaged by the information security team and addressed by relevant personnel.	No deviations noted.
86	Varonis' security incident response is tested annually to ensure its effectiveness and alignment with industry's best practices. The results of the testing are documented, reviewed, and used to improve the incident response capabilities and processes.	Inspected documentation to ascertain that the security incident response process was assessed during the audit period and that the results of the testing were documented, reviewed, and used to improve incident response capabilities and processes.	No deviations noted.

CC7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
87	Security monitoring tools are configured to alert the Security Operations Center for possible or actual security incidents and breaches.	Inspected monitoring systems and system configurations of the DatAdvantage Cloud Platform to ascertain that security monitoring tools are configured to generate alerts to the Security Operations Center for possible or actual security incidents and breaches.	No deviations noted.

Roberta Fávero - Interaction Corp.com.br
October 29, 2026 11:24 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

CC7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
88	Varonis' management is performing a monthly review of closed incidents. Monthly team meetings are held to review alerts and improve capabilities.	Inspected meeting documentation and schedules to ascertain that monthly meetings are held to review security incidents and alerts.	No deviations noted.
		For a sample of months, inspected meeting minutes evidencing review of incidents and improvement actions.	No deviations noted.
89	Varonis Incident Response Plan includes internal and external communication protocols for reporting security incidents.	Inspected Varonis' Incident Response Plan to confirm inclusion of internal and external communication protocols for reporting security incidents.	No deviations noted.
90	Customer Support cases are tracked in a support platform from initiation to closure. Tickets are assigned to a severity level to prioritize the urgency of each support case.	Obtained a list of customer support cases and verified its completeness.	No deviations noted.
		For a sample of cases, inspected documentation to ascertain that cases are tracked from initiation to closure in a support platform and are assigned severity levels to prioritize urgency.	No deviations noted.

CC7.4: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
91	A restore test is performed semi-annually.	Inspected documentation to ascertain that restore tests were performed on a semi-annual basis during the audit period.	No deviations noted.
92	A monthly evaluation of the Security Operations Center is performed to evaluate and improve the effectiveness of the incident response.	Inspected documentation to ascertain that periodic evaluations of the Security Operations Center are performed.	No deviations noted.
		For a sample of evaluations, inspected meeting minutes and documentation evidencing review of rules, alerts, and response effectiveness.	No deviations noted.

roberto.reboucas@petacorp.com.br October 20, 2026 11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
93	Monthly team meetings are held to review alerts and improve capabilities.	Inspected documentation to ascertain that monthly team meetings are held to review alerts and improve detection and response capabilities.	No deviations noted.
94	Varonis SOC team regularly add rules to the SIEM solution for new threat detection capabilities.	Inspected documentation and determined that the Varonis SOC team constantly adds rules to the SIEM solution to support new threat detection capabilities.	No deviations noted.
95	Varonis' management is performing a monthly review of closed incidents. Monthly team meetings are held to review alerts and improve capabilities.	Inspected meeting documentation and schedules to ascertain that monthly meetings are held to review security incidents and alerts.	No deviations noted.
		For a sample of months, inspected meeting minutes evidencing review of incidents and improvement actions	No deviations noted.
96	Varonis Incident Response Plan includes internal and external communication protocols for reporting security incidents.	Inspected Varonis' Incident Response Plan to confirm inclusion of internal and external communication protocols for reporting security incidents.	No deviations noted.
97	Varonis has established a sanction policy to address non-compliance with Varonis' security policies, and disciplinary actions are taken in the event of violation.	Inspected documentation to verify that Varonis has a formal sanction policy addressing noncompliance with security policies and outlining applicable disciplines actions.	No deviations noted.

CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
98	Varonis established lesson learned process.	Inspected the Incident Response Policy and post-incident review documentation to ascertain that a lesson-learned process is defined.	No deviations noted.
99	Root cause analysis is documented within the summary of critical severity incidents.	Inspected documentation to ascertain that root cause analysis (RCA) is documented within the summary of critical severity incidents	No deviations noted.

roberto.revoredo@petacorp.com.br October 2020 11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

Change Management

CC8.1: The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
100	Varonis has established a change control policy. Changes related to DatAdvantage Cloud Platform undergo the change control process and changes are documented.	Inspected the Change Management Policy to verify that it is formally documented and addresses key elements of the change control process, including review, approval, and documentation requirements.	No deviations noted.
101	Changes related to DatAdvantage Cloud Platform are tested, in an isolated and controlled environment prior to implementation, to minimize the effect on the relevant business process, to assess its impact on operations and security and to verify that only intended and approved changes were made. Approval is required from relevant personnel prior to migration to the production environment.	Obtained a list of changes uploaded to the Varonis DatAdvantage Cloud Platform and verified its completeness.	No deviations noted.
		For a sample of changes, inspected documentation to ascertain that (1) changes were tested in an isolated environment prior to implementation and (2) changes are approved prior to migration to the production environment	No deviations noted.
102	Peer approval is required for DatAdvantage Cloud Platform before merging any infrastructure or application code into the main branch of the code repository. Modifications to configuration or code are restricted to the Engineering Production Team.	Obtained a list of changes and verified its completeness.	No deviations noted.
		For a sample of changes, inspected documentation to ascertain that approval is required before merging infrastructure and application code to main branch within the code repository tool.	No deviations noted.
103	Varonis' Change Management Policy includes the procedure for emergency changes.	Inspected documentation to ascertain that an emergency changes procedure is included in the Change Management Policy.	No deviations noted.
104	Cloud DatAdvantage data Confidential information is protected with encryption at rest and in transit.	Observed system configuration and inspected documentation to ascertain that DatAdvantage Cloud Platform confidential data is encrypted at rest using industry standard ciphers.	No deviations noted.
		Inspected documentation and configuration to ascertain that data in transit is encrypted (minimum TLS version is defined and tested under CC6.7).	No deviations noted.

robert.revoredo@petacorp.com.br October 20, 2021 5:51 EDT

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

Risk Mitigation

CC9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
105	Cyber Insurance coverage exists and renewed annually.	Inspected documentation to ascertain that cyber insurance coverage was in place and valid throughout the audit period and was renewed on an annual basis.	No deviations noted.

CC9.2: The entity assesses and manages risks associated with vendors and business partners.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
106	A security annex is added to new agreement with third parties.	Inspected documentation to ascertain that a Security Annex is in place and is required to be added to agreements with third-party vendors and business partners.	No deviations noted.
		For a sample of new third-party agreements executed during the audit period, documentation inspected to determine that the Security Annex was added to the agreements.	No deviations noted.
107	Each third party undergoes risk assessment.	Obtained a list of vendors and verified its completeness.	No deviations noted.
		For a sample of vendors, inspected documentation to ascertain that risk assessment took place.	No deviations noted.
108	CISO Team approval is required when software is installed on endpoints.	Inspected documentation and approval records to ascertain that CISO team approval is required prior to installation of software on endpoints.	No deviations noted.

roberto.revoredo@petratorp.com.br
October 20 2020 11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
109	Roles and responsibilities related to managing vendors are documented in the Supplier Relationships Security Policy.	Inspected the Vendor Security Policy to confirm that roles and responsibilities related to vendor management are clearly documented.	No deviations noted.
110	Varonis has risk assessment process to evaluate new and existing third parties. Minimum criteria are defined for risk assessment approval. The criteria are defined within a procedure	Inspected the risk assessment procedure to confirm minimum criteria for approval are defined.	No deviations noted.
		Obtained a list of third parties and verified completeness.	No deviations noted.
		For a sample of third parties, inspected risk assessment documentation to confirm assessments were performed according to procedure.	No deviations noted.
111	Varonis has established a Supplier Relationship Security Policy, which specifies the minimum requirements for each vendor to comply with.	Inspected the Supplier Relationship Security Policy to ascertain that minimum security requirements for vendors are defined and documented.	No deviations noted.
112	Termination clauses which include, but not limit to, data deletion requirements are included in Varonis' agreements with third parties and business partners.	Obtained a list of suppliers and verified its completeness	No deviations noted.
		For a sample of supplier agreements, inspected documentation to ascertain that termination clauses, including data deletion requirements, are included.	No deviations noted.
113	The Data Processing Addendum is mutually signed with the relevant vendors to obtain privacy commitments.	Inspected documentation to ascertain that Data Processing Addendums (DPAs) are in place with relevant vendors and business partners.	No deviations noted.
		For a sample of vendors, inspected executed agreements to confirm that the DPAs were mutually signed by both parties.	No deviations noted.

Report Generated on October 2021 at 14:51 UTC

Availability

A1.1: The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
114	Varonis monitors backups and infrastructure capacity within the DatAdvantage Cloud Platform environment.	Inspected monitoring notifications and system-generated alerts to ascertain that infrastructure capacity and backups are monitored within the DatAdvantage Cloud Platform environment.	No deviations noted.
115	Alerts are triggered to the cloud operation team when capacity reaches a defined threshold.	Obtained a list of alerts and verified its completeness.	No deviations noted.
		For a sample of alerts, inspected configuration to ascertain that alerts are triggered to the cloud operation team when capacity reaches a defined threshold.	No deviations noted.

A1.2: The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
116	High availability and load balanced arrays are in place for DatAdvantage Cloud Platform systems to help mitigate the effect of a system error.	Inspected documentation to ascertain that high availability and load-balanced configurations are in place for DatAdvantage Cloud Platform systems to help mitigate the effect of a system error.	No deviations noted.
117	Varonis uses daily backup for the DatAdvantage Cloud Platform's application database.	Observed system configuration to ascertain that a daily backup mechanism for the DatAdvantage Cloud Platform application database is configured.	No deviations noted.
		Inspected backup execution logs to determine that the configured daily backups were performed during the audit period.	No deviations noted.
118	All data is retained according to the Varonis Software Privacy policy.	Varonis' Software Privacy Policy inspected to ascertain that data retention requirements are defined.	No deviations noted.
		Inspected documentation to determine that data is retained in accordance with the documented retention policy	No deviations noted.
119	Varonis has implemented web application firewall (WAF) to provide protection against denial-of-service attacks and other web application attacks.	Inspected documentation to ascertain that the architecture of the DatAdvantage Cloud Platform includes a web application firewall (WAF).	No deviations noted.

Roberto Fevereiro Netto Corp. - CPF 015.[illegible].151-[illegible]
October 20, 2021 | 11:51 UTC

Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
		Inspected WAF configuration and determined that the WAF is configured to protect the external boundary from application vulnerabilities and attacks.	No deviations noted.

A1.3: The entity tests recovery plan procedures supporting system recovery to meet its objectives.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
120	Varonis has established a Business Continuity Plan (BCP), which includes: 1. Business impact analysis 2. Continuity plans 3. Cyberattack response plan. 4. Pandemic recovery plan 5. Recovery Time Objective (RTO) and Recovery Point Objective (RPO).	Inspected the Business Continuity Plan (BCP) to verify that it is formally documented and includes a business impact analysis, continuity plans, cyberattack response plan, pandemic recovery plan, and defined RTO and RPO.	No deviations noted.
121	The Business Continuity Plan is reviewed and approved on an annual basis.	Inspected documentation to verify that the Business Continuity Plan (BCP) is reviewed and formally approved on an annual basis.	No deviations noted.

Confidentiality

C1.1: The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
122	Varonis' security and availability commitments and the associated system requirements are documented in customer agreements.	Inspected customer agreements to ascertain that security and availability commitments and associated system requirements are documented.	No deviations noted.
123		Obtained a list of third-party vendors and verified its completeness.	No deviations noted.

roberto.revoredo@etacorp.com.br October 20, 2026 11:51 UTC

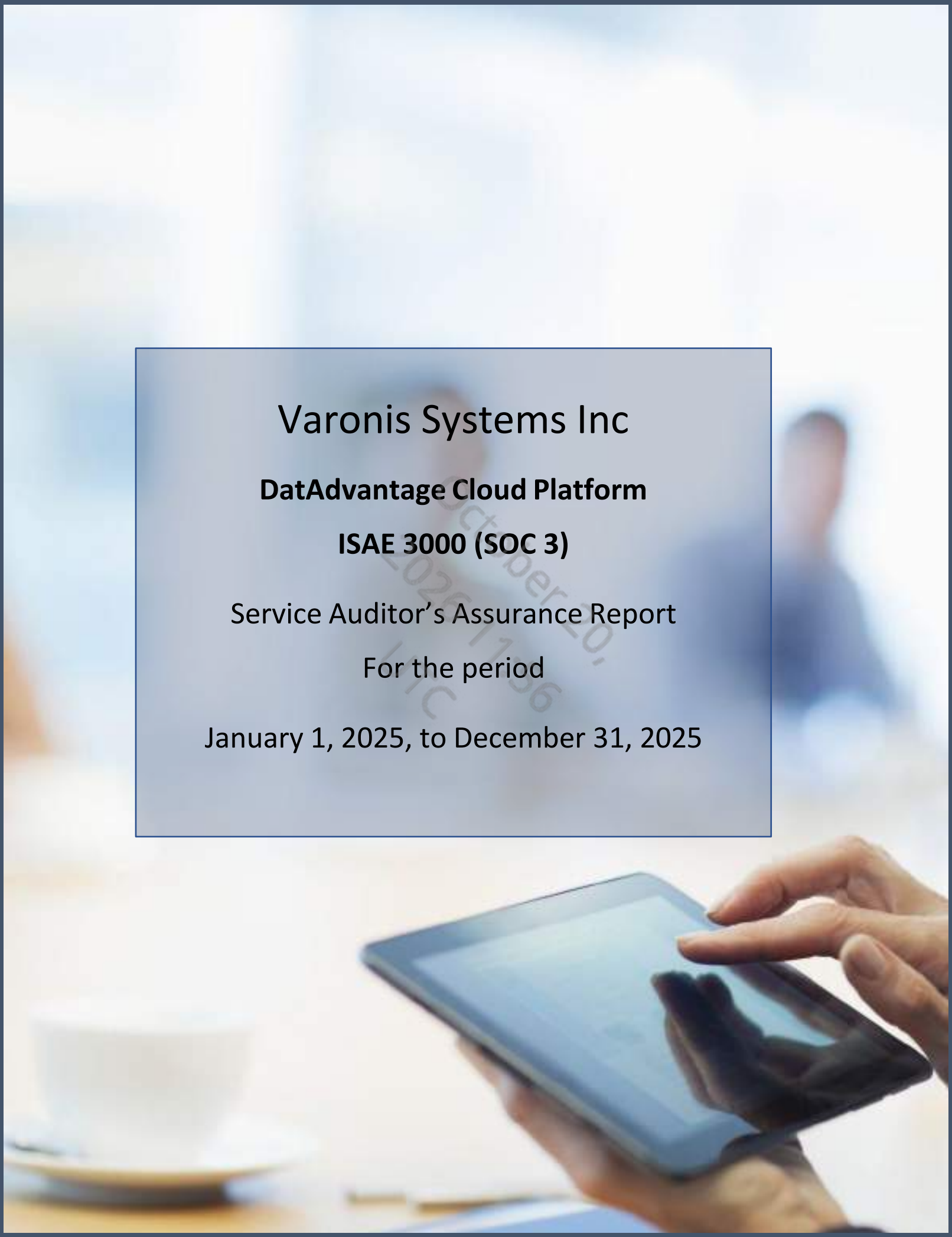
Docusign Envelope ID: 8E04B688-302E-4968-8331-F3DED7EC6BFF

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
	Termination clauses which include, but not limit to, data deletion requirements are included in Varonis' agreements with vendors and business partners.	For a sample of third-party agreements, inspected documentation to confirm that termination clauses include data deletion requirements	No deviations noted.

C1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.

#	Controls specified by the company	Testing performed by the auditor	Results of Testing
124	The retention policy for customer data is documented within Varonis' Privacy policy.	Inspected Varonis' Privacy Policy to ascertain that customer data retention periods are documented.	No deviations noted.

roberto.revoredo@petacorp.com.br
October 20, 2026 11:51 UTC



Varonis Systems Inc

DatAdvantage Cloud Platform

ISAE 3000 (SOC 3)

Service Auditor's Assurance Report

For the period

January 1, 2025, to December 31, 2025

Contents

Section I - Management Assertion Provided by Varonis Systems, Inc _____

Section II – Independent Service Auditor's Assurance Report _____ *5*

Section III - Description of Varonis DatAdvantage Cloud Platform _____

Company Overview and Background _____ **6**

Description of the Services Provided _____ **6**

Infrastructure _____ **7**

System Boundaries _____ **7**

Separation of environments _____ **7**

Network Infrastructure _____ **8**

Security and Architecture _____ **8**

Data Center Security _____ **8**

Software _____ **8**

Physical Security _____ **9**

Access Control and User and Permissions Management _____ **9**

Quality Testing _____ **9**

Data _____ **9**

People _____ **9**

Change Management _____ **10**

Security Testing _____ 10

Encryption _____ **10**

Human Resources processes _____ **10**

New Hire _____ 10

Performance Evaluation _____ 10

Whistleblower Program _____ 11

Organizational Structure _____ **11**

Authority and Responsibilities _____ **11**

Audit Committee _____ **11**

Communication _____ **11**

Risk Management _____ **12**

Enterprise Risk Management Program _____ 12

Cyber Risk Assessments _____ 12

Third-Party Risk Management _____ 12

October 20, 2026 11:56 UTC

Privacy Management 12
Security and Privacy Awareness Training 12
Company Information Security Policies 13
Availability Procedures 13
Business Continuity Plan 13
Backup 14
Incident Response 14
Asset Management 14
Endpoint Security 14
Monitoring 14
Principal Service Commitment and System Requirements 14

October 20, 2026 11:56 UTC

Section I - Management Assertion Provided by Varonis Systems, Inc

We, as management of, Varonis Systems, Inc ("the Company or Varonis") are responsible for:

- Identifying the Varonis Systems, Inc SaaS Platform named Varonis DatAdvantage Cloud (“the system”) and describing the boundaries of the system.
- Identifying our principal service commitments and system requirements.
- Identifying the risks that would threaten the achievement of the principal service commitments and service requirements that are the objectives of our system.
- Identifying, designing, implementing, operating, and monitoring effective controls over the Varonis Systems, Inc platform (system), to mitigate risks that threaten the achievement of the principal service commitments and system requirements.
- Selecting the trust services categories that are the basis of our assertion.

We assert that the controls over the system were effective throughout the period January 1, 2025, to December 31, 2025, to provide reasonable assurance that the principal service commitments and system requirements were achieved, based on the criteria relevant to security, availability and confidentiality set forth in the AICPA’s TSP Section 100 2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (with Revised Points of Focus – 2022).

October 20, 2026 11:56 UTC

Varonis Systems, Inc

April 13, 2026

Somekh Chaikin
17 Ha'arba'a Street, PO Box 609
KPMG Millennium Tower
Tel Aviv 6100601, Israel
+972 3 684 8000

TEL +972 3 684 8000
Fax +972 3 684 8444
Website www.kpmg.co.il

Section II – Independent Service Auditor's Assurance Report

We have examined management's assertion that Varonis Systems, Inc, during the period January 1, 2025, to December 31, 2025, maintained effective controls to provide reasonable assurance that:

- The System was protected against unauthorized access, use, or modification.
- The System was available for operation and use, as committed or agreed.
- Information within the System designated as confidential is protected as committed or agreed.

Based on the criteria for security, availability, and confidentiality in the American Institute of Certified Public Accountants' TSP Section 100 2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (with Revised Points of Focus – 2022). This assertion is the responsibility of Varonis Systems, Inc' management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included:

(1) Obtaining an understanding of Varonis Systems, Inc ' relevant to security, availability, confidentiality, and Privacy controls.

(2) Testing and evaluating the operating effectiveness of the controls.

(3) Performing such other procedures as we considered necessary in the circumstances.

October 29, 2026 11:56 UTC

We believe that our examination provides a reasonable basis for our opinion.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls or a deterioration in the degree of effectiveness of the controls.

In our opinion, Varonis Systems, Inc management's assertion referred to above is fairly stated, in all material respects, based on the criteria mentioned for security, availability and confidentiality.

Yours faithfully,



KPMG

Tel Aviv, Israel

May 6, 2026

Section III - Description of Varonis DatAdvantage Cloud Platform

Company Overview and Background

Varonis Systems Inc. started operations in 2005 and services numerous leading firms in the financial services, public, healthcare, industrial, insurance, energy and utilities, technology, consumer and retail, media and entertainment, and education sectors.

Varonis Systems Inc. (Nasdaq: VRNS) is the leader in data security, fighting a different battle than conventional cybersecurity companies. Varonis Systems Inc. is a pioneer in data security and analytics, fighting a different battle than conventional cybersecurity companies. Varonis Systems Inc. focuses on protecting enterprise data, which includes sensitive files and emails, as well as confidential customer, patient, and employee data. Our services also protect financial records, strategic product plans, and other intellectual property from unauthorized access by nefarious actors.

The Varonis Systems Inc.'s DatAdvantage Cloud Platform system detects cyberthreats from both internal and external actors by continuously analyzing cloud configurations, data permissions, account activity, and user behavior across SaaS and IaaS platforms. The platform helps prevent and contain potential breaches by automatically locking down access to sensitive and stale data and maintains a least-privilege posture through intelligent automation and policy enforcement.

Varonis Systems Inc. products address important use cases including data protection, data governance, zero trust, compliance, data privacy, classification, and threat detection and response.

October 20 2021 1:56 UTC

Description of the Services Provided

The Varonis DatAdvantage Cloud a cloud-hosted data security platform for protecting and governing enterprise data. Companies use Varonis DatAdvantage Cloud to discover mission-critical data, ensure only the right people have access, and detect threats before they come breaches. Varonis integrates with a wide array of data repositories, applications, and infrastructure to give customers a holistic view of their data. Varonis can be used to address these important use cases:

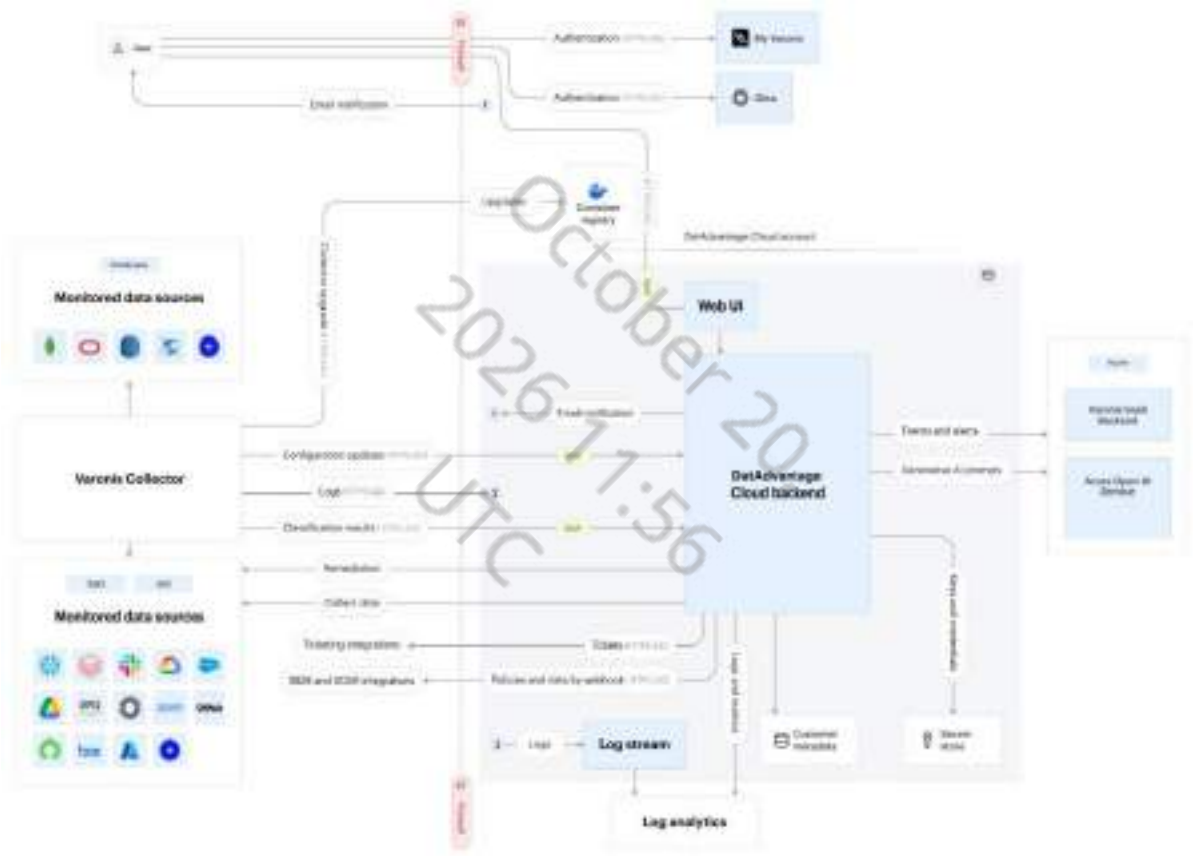
- **Detecting insider threats and cyberattacks**: Varonis DatAdvantage Cloud detects threats to data, including insider threats and external cyberattacks with a live-updating library of pre-built threat models based on attack techniques and vulnerabilities used by real-world adversaries.
- **Pinpointing data exposure**: Varonis DatAdvantage Cloud automatically classifies sensitive data, highlights where information is exposed externally or internally and helps teams prioritize remediation efforts.
- **Limiting the blast radius of an attack**: Varonis DatAdvantage Cloud analyzes where there is unnecessary access to data and drastically reduces the damage from insider threats and cyberattacks.
- **Fixing misconfigurations**: Varonis DatAdvantage Cloud provides SSPM capabilities to analyze and fix misconfigured SaaS applications, discovering shadow instances, or spotting vulnerabilities that could put data at risk.
- **Achieving compliance**: Varonis' vast library of classification rules can discover sensitive data related to GDPR, CCPA, HIPAA, and more. The permissions analysis and continual monitoring Varonis provides gives auditors a real-time pulse on compliance.

Infrastructure

Varonis' DatAdvantage Cloud infrastructure is deployed on Amazon AWS (utilizing both SaaS and Platform as a Service [PaaS] solutions) for hosting and operating production, staging, and development environments. Varonis leverages the experience, resilience, and reliability of AWS to scale quickly and securely to meet the current and future demands of its customers.

Each boundary of the system has specific security controls. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the system.

System Boundaries



October 20 2026 11:56 UTC

Varonis' DatAdvantage Cloud infrastructure is implemented in Amazon AWS and uses Okta as the identity provider for customer access and authentication. The Varonis solution leverages the capabilities, resilience, and reliability of Amazon AWS to scale quickly and securely to meet our customers' current and future demands.

Separation of environments

The production environment is separated from the staging and development environments with separate access control and segmented network.

Network Infrastructure

Robust network infrastructure is essential for reliable and secure real-time data communication between the various Varonis cloud service components. To provide sufficient capacity, Varonis' network infrastructure relies on platforms provided by Amazon AWS and other software providers. To ensure appropriate network security levels, security standards and practices are backed by a multi-layered approach aimed at preventing security breaches and ensuring confidentiality and availability.

Security and Architecture

Varonis provides a secure, reliable, and resilient SaaS platform that has been designed from the ground up based on industry best practices. All secrets, such as tokens for connecting to customer databases, are stored in the Amazon AWS Secrets Manager. Varonis uses. Varonis has multiple security zones to differentiate services of various sensitivities and different service principles to isolate secrets. The keys that are under Varonis' responsibility (e.g., the password for tenant databases) are periodically rotated.

The sections below describe the network and hardware infrastructure, software, and information security elements that Varonis delivers as part of the platform, database management system security, and application controls.

Data Center Security

Varonis relies on Amazon AWS's global infrastructure, including the facilities, network, hardware, and operational software, all of which support the provisioning and use of basic computing resources and storage. These facilities comply with industry standards of security and reliability, thereby enabling Varonis to provide its services in an efficient and stable manner.

October 20, 2026 11:56 UTC

Software

The Varonis application includes the following primary service components:

- Virtual machines, Kubernetes, Logging, and monitoring
- Firewall and web application firewall
- Change management tool
- Storage service
- Key management system
- Identity and security management
- Programmable communication application program interfaces (APIs) for messaging
- Database applications
- Simple Mail Transfer Protocol (SMTP) provider
- Security information and event management
- Incident management platform
- Certificate management solution
- Managing observability platform
- Domain Name System (DNS) service
- Relational and graph databases
- Automated deployment, scaling, and management of containerized applications
- Build and deploy automation
- Caching service

- Event streaming platform
- Messaging service

Physical Security

Varonis maintains a physical security policy that aligns with industry best practices. The policy details procedures for securing offices globally, access restrictions to buildings and offices, badge access, periodic review of entry, and continuous workplace monitoring.

Our partner data center, Amazon AWS, is SOC 2 compliant. The SOC 2 report addresses various physical security and environmental controls that are tested annually, and the Varonis security team reviews certificates and attestation reports annually to ensure a consistent level of protection.

Access Control and User and Permissions Management

Varonis' users are provided with the minimal access rights required to carry out their duties (known as "least privilege" access). Employees are assigned to a specific group upon hire. Only employees who are assigned to the production group can request access to production. Their access is reviewed periodically by the business owners. When a user from that group requests access to production, the request must be approved by the business owner for each session. Access is limited by time and then documented, logged, and monitored by the security operations center. Employees accessing Varonis DatAdvantage Cloud Platform and the corporate network are required to use a two-factor authentication mechanism and a virtual private network (VPN). Logical and physical access is revoked from resigned employees upon termination.

Customer access is authenticated in the system either by logging in with username and password or federated by the customer through the customer's identity provider, which is supported by the system.

Quality Testing

Varonis' Validation and Quality Assurance (QA) team is involved from the early stages of development. Automatic tests are performed using a dedicated tool to validate the code quality. Code review is mandatory to continue the Secure Software Development Lifecycle (SSDLC) process. Successful test status is mandatory to continue in the SSDLC process and deploy a version to the production environment.

Data

The customer defines and controls the data they load into and store in the Varonis production network. Such data contains access logs and configuration logs. Data is accessed remotely from the company's customer portal via the internet. Varonis has deployed secure data transmission protocols to encrypt data when transmitting over public networks. Encryption is also enabled on databases at rest and on data backups.

Metadata and data classifications are uploaded for further analysis to Varonis DatAdvantage Cloud. The data is gathered and stored in protected storage for further analysis and to identify immediate or potential risks in the customer's environment. This information is easily viewed on the Varonis DatAdvantage Cloud dashboard, including any alerts that are produced. All customer data is stored and transferred in encrypted form.

People

The Varonis employees involved in the development, operation, security, or support of the Varonis DatAdvantage Cloud platform are grouped in the following primary areas:

- Executive Management
- Product Management
- Product Security

- Software Engineers
- DevOps
- Information Security
- Human Resources
- Professional Services
- Support
- Internal Audit
- Legal

Change Management

All changes to Varonis' services follow a structured process to ensure appropriate planning and execution. This structured process requires communication, documentation of important process workflows and personnel roles, and the alignment of automation tools where appropriate.

Software changes are tested in the development environment, committed to a source code management system, and reviewed through automated testing and by peers. Releases are tested by QA before deployment.

Security Testing

Various sets of security testing are performed on the cloud infrastructure and applications. Testing includes, but is not limited to, penetration testing that is performed by both an internal red team and on an annual basis by a reputable third-party vendor, vulnerability scanning, software composition scanning, code reviews, and other automated scans.

Encryption

Varonis uses Transport Level Security (TLS) to encrypt and provide integrity to all data when transmitting data over public networks. Encryption is for data at rest stored on virtual machines, databases, data backups and all other storage types. Communication between the boundaries is encrypted.

Human Resources processes

e ire

Individuals offered a position at Varonis are subject to background checks (as appropriate for each country and taking into account local laws and regulations) as a condition to their employment in the company. In each location, employees receive data packages containing an overview of Varonis' Human Resources policies and procedures. These packages include the offer letter or employment contract, NDA, and the Varonis Code of Conduct. Employees are asked to sign their offer/employment contract to confirm that they have read these materials and agree to be bound by their terms. New hires are also required to sign a privacy addendum. If background checks are not permitted in their country of employment, they undergo a reliability test.

Performance valuation

Varonis has a continuous performance management process that provides feedback to employees and managers through regular 1:1 meetings and Goal Plans in HR. Varonis also has an annual performance review process in place to review accomplishments, provide constructive feedback, identify opportunities for improvement, and ensure the ongoing development of all Varonis employees. The annual performance reviews enable managers to provide ratings for the direct reports on their team, employees to provide self-evaluations, and end with a year-end conversation between the managers and employees. This process is designed to align the employee's efforts and the organization's goals.

istleblo er Program

Varonis has an anonymous whistleblower program in place for employees to report any violation without fear of dismissal or retaliation. Reported issues are investigated and acted on in a timely manner. Information regarding how to report any violation is outlined in the Varonis Code of Business Conduct and Ethics policy.

Organizational Structure

Varonis has an established organizational structure with defined roles and responsibilities that are segregated based on functional requirements. The organization chart delineates lines of reporting and is updated in real-time to reflect any changes.

Authority and Responsibilities

Lines of authority and responsibility are clearly established throughout the company. Varonis' Board of Directors meets periodically to review committee charters and corporate governance that define their roles, responsibilities, member qualifications, meeting frequency, and other discussion topics. Minutes of the annual meetings are recorded and include the names of the participants and the date the meeting occurred.

The Board of Directors and management recognize their responsibility to foster a strong ethical environment within Varonis to determine that its business affairs are conducted with integrity and in accordance with high standards of personal and corporate conduct. This responsibility is characterized and reflected in the Varonis Code of Business Conduct and Ethics, which is distributed to all employees. Specifically, employees are prohibited from using their positions at Varonis for personal or private gain, disclosing confidential information regarding customers or taking any action that is not in the best interest of the customers. Employees' personal securities transactions are governed by a corporate policy and employee account trades are reviewed to monitor adherence to Varonis' policy. All employees are required to maintain ongoing compliance with all policies, standards, and procedures of the Code of Conduct and with lawful and ethical business practices, whether they are specifically mentioned in the Code of Conduct or not. All employees are required to affirm annually that they received, read, understand, and comply with the requirements set forth in the Code of Conduct and the Employee Handbook. Employee recertification status is monitored periodically for compliance/

Audit Committee

The Audit Committee is responsible for overseeing and monitoring the integrity of Varonis' consolidated financial statements, the company's compliance with legal and regulatory requirements as they relate to financial reporting or accounting matters, and the company's internal accounting and financial controls. The Audit Committee also oversees and monitors Varonis' independent auditor's qualifications, independence, and performance; provides the Board of Directors with the results of its monitoring and recommendations; provides the Board of Directors with the additional information and materials it deems necessary to ensure the Board of Directors is aware of significant financial matters that require the Board's attention; and oversees Varonis' internal audit function.

Communication

Varonis values transparent communication—both internally and externally. Varonis communicates with prospects, customers, and employees through several methods including, without limitation, the corporate website, which includes our privacy policy and public ways to report product flaws or security issues, a customer portal, which contains product release notes and other critical product information, and an internal employee portal which offers information about policies and procedures.

Varonis' security approach and compliance certifications are documented and communicated to customers on the Trust & Security page, in the company's agreements, and as part of the description of services provided online.

Risk Management

Varonis has developed a risk management policy that includes risk identification, analysis, communication and reporting, treatment, and monitoring. The risk management program implements a structured security plan. Each risk is evaluated by the likelihood and impact it may cause, and the treatment plan is an ongoing effort by all Varonis departments.

nterprise Ris Management Program

The security and privacy risk management program has several levels and is conducted periodically by external and internal auditors. High-level risks are covered during the annual enterprise risk assessment performed by the internal auditor and are presented to the company's senior management. The Chief Information Security Officer (CISO) conveys cyber threats, and a mitigation plan is then decided upon and implemented.

Cyber Ris Assessments

Varonis performs routine technical risk assessments for software development, cloud production, and corporate and cloud infrastructure. Expert third-party consultants also perform ongoing assessments. The Information Security Department, led by the CISO, monitors the progress of such efforts until all substantial risks are remediated. The CISO and senior management propose remediation plans, and the security steering committees decide on the treatment plan to be adopted.

T ird-Party Ris Management

Engagements with third-party suppliers undergo a security risk assessment. It is incumbent upon Varonis to ensure that vendors are capable of delivery and aware of inherent security risks. The vendor is thoroughly vetted for security and posture. We assure our customers that their data is protected and evaluate the risk by thoroughly reviewing third parties' security, compliance, and privacy practices. Whenever customer data is shared with a new third party, our customers are notified, and the vendor list is updated. High-risk third parties that hold customer data undergo periodic reviews. Each engagement with potential disclosure of PII requires a privacy assessment and signing of a Data Processing Addendum. We also require a Non- Disclosure Agreement (NDA) and security agreements.

Privacy Management

Varonis is committed to complying with all applicable data protection laws and regulations and maintaining appropriate procedures and work instructions as part of its privacy information management system. The privacy program is aligned with global privacy standards, including the EU's GDPR.

Varonis implements a privacy-by-design strategy that limits the scope and scale of data collection and processing as much as possible to limit risks to sensitive data.

Varonis is committed to upholding contractual terms related to privacy and data protection in its agreements with its partners, subcontractors, and other relevant third parties (customers, suppliers, etc.). Varonis has a designated Data Protection Officer who guides Varonis on all data privacy concerns, risk management, and other related legal matters.

Security and Privacy A areness Training

Varonis' employees undergo information security and privacy awareness training upon joining the company, as well as annually thereafter, in conformance with the information security policy. The training ensures that each group of employees receives security training according to their technical knowledge and needs.

October 20, 2021 21:56 UTC

Company Information Security Policies

Varonis has established Information Security policies that ensure that its community of users are properly informed of their role and responsibilities based upon their level(s) of access to Varonis systems. This policy also defines the role of each end-user in helping to safeguard sensitive and confidential information systems from internal and external threats.

These policies include:

- Acceptable use of assets
- Access control
- Asset management
- Backup and restore
- Business continuity
- Change management
- Cloud security
- Compliance
- Cryptography
- Data classification
- Data disposal
- Endpoint security
- Human Resources security
- Incident response
- information security awareness, education, and training
- Information transfer
- Logging and monitoring
- Mobile device management
- Network security
- Passwords
- Physical and environmental security
- Privacy management
- Records retention and data disposal
- Risk management
- Secure software development lifecycle
- Supplier relationships
- Teleworking and remote access
- Vulnerability and Threat management

October 20, 2026 11:56 UTC

Availability Procedures

High availability eliminates single points of failure to ensure continuous operations and extended uptime. Load balancing is used to distribute traffic across multiple servers. High availability and load balanced arrays are in place for production systems to help mitigate the effect of a system error. Additionally, Varonis implemented a web application firewall to protect against denial-of-service attacks and reduce the risk of web application threats.

usiness Continuity Plan

Varonis' Business Continuity Plan outlines measures to avoid disruptions to customers and partners. The plan includes impact analysis and risk assessment to help identify critical functions and processes. Customer support and resiliency are top priorities. The plan includes a strategic continuity plan for customer support, including systems, suppliers, and users. The Business Continuity Plan also includes the following topics:

- DatAdvantage Cloud production infrastructure
- Corporate infrastructure
- Critical suppliers
- Cyber incident response
- Pandemic preparedness

ac up

The database and storage are hosted on Amazon AWS. A daily backup is performed using an automated application. In case of failure, a notification is sent to the operations team. Production databases utilize AWS availability zone capabilities. Additionally, a complete replica is stored at a separate region.

Incident Response

Varonis has implemented incident response policies and procedures to detect, investigate, and respond to security incidents. These procedures guide Varonis personnel in reporting and responding to information technology incidents that affect the security, availability, and confidentiality of the system. The Incident Response plan contains procedures to address various cybersecurity scenarios that may occur. Furthermore, the plan includes roles and responsibilities, and the communication process for stakeholders at each phase.

Asset Management

Company assets are tracked and managed throughout the asset lifecycle. Each asset has an owner assigned to it, to ensure there is an individual responsible for securing the asset. The tracked assets include production components as well as employee devices that may contain personal data. When assets reach end of life, they are securely destroyed to ensure that data is not recoverable.

Endpoint Security

Devices issued to company personnel must meet minimum security criteria, including full disk encryption, screen lockout policy, running antimalware and other security software, and being kept up to date with security patches.

Monitoring

Varonis uses a set of monitoring tools to monitor its service. Alerts are sent to relevant stakeholders by an internal communication tool based on predefined rules and are then reviewed and processed according to their level of urgency.

Principal Service Commitment and System Requirements

Varonis' commitments to customers include security, confidentiality, availability, and privacy. Commitments are communicated and documented within agreements, the Trust & Security page, and as part of the supplier relationship process. Our commitments to our customers include, but are not limited to:

- An established global risk management process to identify, monitor, and manage risks for the entire organization, business units, and all supplier relationships.
- Controlled physical, logical, and remote access to sensitive information to reduce the likelihood of a security incident. Varonis has established and follows specific access control practices to protect information and information systems from unauthorized access, modification, disclosure, or destruction.
- Secure data transmission protocols to encrypt data in transmission over public networks. Encryption is also enabled on databases, data at rest, data backups, and communication between segmented boundaries.
- Network segregation to enforce separation between production, staging, testing, and other cloud-based and internal infrastructure environments.
- Minimum standards of security for the development, provision, and use of Varonis cloud services require that the security, confidentiality, availability, and privacy of assets within Varonis cloud services are protected. Risks to the services and to customers are subject to a risk assessment and to the application of suitable technical and organizational controls.
- Data centers that host, store, and/or process customer production data must comply with industry best practices. This includes protecting information system equipment and cabling, entrance controlled by access card, surveillance cameras, providing emergency power, shutoff, lighting, fire alarms, protection from water and

October 20, 2026 11:56 UTC

fire, and maintaining temperature and humidity controls.

- A retention policy that complies with applicable legal, regulatory, and contractual requirements. This includes deleting customer data upon request or automatically based on lifecycle policies that are communicated to the customer.
- The Human Resources department (HR) ensures successful operations and delivery of effective security controls. This includes implementing security measures prior to employment, during employment, at termination, and as otherwise required during any other changes in employment status, as well as providing ongoing cybersecurity awareness training to the company's employees.
- Backup procedures designed to ensure the continued availability and accessibility of information and to minimize the cost of a disruption (e.g., operational error, disaster, or sabotage that causes damage to, or destruction of, information).
- Maintaining a service level agreement (SLA) between Varonis and its customers wherein Varonis' responsibilities and the customer's cooperation requirements are specified. Within such SLA, Varonis upholds certain obligations regarding the availability of its service, and maintaining support levels, depending on the severity of the error.
- Implementing privacy by design within the systems and processes, which is intended to minimize risks to privacy rights and to process personally identifiable information (PII), in keeping with regulatory requirements.
- An established business continuity and disaster recovery plan that provides an overview of the activities necessary to coordinate the recovery of critical business customer functions and managing and supporting recovery in the event of a disruption or disaster.

October 20, 2026 11:56 UTC



Software Version Publication date December 4, 2024

Copyright © 2005 - ©2024 Varonis Systems Inc

All rights reserved.

This information shall only be used in conjunction with services contracted for with Varonis Systems,Inc. and shall not be used to the detriment of Varonis Systems, Inc. in any manner. User agrees not to copy, reproduce, sell,license,or transfer this information without prior written consent of Varonis Systems,Inc. Other brands and products are trademarks of their respective holders.

SUPPORTED DATA SOURCES

Different components of the platform support different data sources. Take a look at the matrices below to see which data sources are supported for which functionalities. Varonis products support the following data sources:

- Data Sources
- Network devices

Important:

- To fully understand all aspects of support for a particular data source, the information in the tables below is intended to be used in conjunction with the relevant deployment guide.
- To learn more about the network firewall and certificate requirements, click here.

Data Sources

Click the relevant link to view the supported data source versions for each Varonis SaaS product:

- Active Directory
- Amazon FSx for Windows
- Azure Files
- Cohesity

- CTERA
- Dell CEE Framework
- Dell PowerScale OneFS (Isilon)
- Dell Unity
- Generic Data Source
- Hitachi HCP Anywhere Enterprise (HCP-AWE)
- Hitachi HCP Gateway
- Hitachi NAS
- IBM AIX
- Linux
- Microsoft 365:
  - Entra ID
  - Exchange Online
  - OneDrive
  - SharePoint Online
- Nasuni
- NetApp ONTAP Cluster Mode
- Nutanix
- Panzura
- Pure Storage FlashArray

- Pure Storage FlashBlade
- Qumulo
- Unix Directory Services
- VAST
- Windows

Active Directory

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies
Active Directory on Windows 2003	√	√	N/A	N/A	√
Active Directory on Windows 2003 R2	√	√	N/A	N/A	√
Active Directory on Windows 2008 R2	√	√	N/A	N/A	√

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies
Active Directory on Windows 2012, 2012 R2✣	√	√	N/A	N/A	√
Active Directory on Windows 2016 (Standard, Core Standard)✣	√	√	N/A	N/A	√
Active Directory on Windows 2019 (Standard, Core Standard)✣	√	√	N/A	N/A	√
Active Directory on Windows 2022 (Standard, Core Standard)✣	√	√	N/A	N/A	√
Entra ID Domain Services	√		N/A	N/A	N/A

✣Note the following:

- Installing an AD proxy on a Windows 2003 or Windows 2003 R2 domain controller is not supported. To monitor domain controllers running on Windows 2003 or Windows 2003 R2, install the AD proxy on another Windows Server running a higher Windows version.
- If the AD proxy is installed on a Windows Server Core operating system, GPO change events will not be audited.
- If you're not using a Directory Services proxy, when event monitoring is enabled, events are audited directly from the Collector.

For more information, see the Installation Requirements section in AD Requirements.

Amazon FSx for Windows

Note: Private Preview. If you'd like to use Amazon FSx for Windows, contact your Sales Engineer.

Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)
√	√	√	√		√

For more information, see Amazon FSx for Windows Requirements.

Azure Files

Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)	NFS
√	√	√		√✣	√	

✣The following policies are not supported for Azure Files:

- Remediate org-wide exposure
- Remove stale memberships
- Remove stale direct permissions

For more information, see Azure Files Requirements.

Cohesity

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)	NFS
6.6.b	√	√	√	√	√	√	
6.6.0d	√	√	√	√	√	√	
6.8.x	√	√	√	√	√	√	
7.0	√	√	√	√	√	√	
7.1	√	√	√	√	√	√	

✥The supported Cohesity-Varonis connector app versions are 1.0 and 1.0.3.

For more information, see Cohesity Requirements.

CTERA

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)	NFS
7.8.x✣	√	√	√	√	√	√	

✣Due to a change in CTERA functionality, older versions are no longer supported.

For more information, see CTERA Requirements.

Dell CEE Framework

The supported versions include:

Version	SMB (CIFS)	NFS
4.5.1.x	√	√
4.6.7.x	√	√

Version	SMB (CIFS)	NFS
6.x	√	√
7.x	√	√
8.x[a, b]	√	√

a. Dell CEE Framework version 8.7.8.1 is not supported.

b. Up to version 8.9.10.0 is supported.

For more information, see Dell PowerScale OneFS (Isilon) Monitoring Overview.

Dell PowerScale OneFS (Isilon)

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)		NFS
8.0.x	√	√	√	√	√	√		√
8.1	√	√	√	√	√	√		√
8.2.x	√	√	√	√	√	√		√
9.0	√	√	√	√	√	√		√
9.1	√	√	√	√	√	√		√
9.2.1	√	√	√	√	√	√		√

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)		NFS
9.3	√	√	√	√	√	√		√
9.4	√	√	√	√	√	√		√
9.5	√	√	√	√	√	√		√
9.7.x	√	√	√	√	√	√		√
9.8.x	√	√	√	√	√	√		√

a. Varonis supports monitoring of Dell PowerScale OneFS (Isilon) data sources that are configured with Edit ACL Policy settings set to Balanced, Unix only, or Windows only. Dell PowerScale OneFS (Isilon) data sources set to Custom environment are not supported.

b. For Isilon version 8.2.0 and higher, Varonis supports monitoring the System Zone or a zone with a unique, dedicated IP. For lower Isilon versions, Varonis supports monitoring the System Zone. Simultaneous monitoring of multiple zones is not supported.

c. Dell PowerScale OneFS (Isilon) CloudPools is not supported.

d. Events are collected from Dell CEE.

e. Dell PowerScale OneFS (Isilon) version 9.6.x was not validated by Varonis.

For more information, see PowerScale OneFS (Isilon) Requirements.

Dell Unity

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)	NFS
4.1	√		√	√	√	√	√
4.2	√		√	√	√	√	√
4.3	√		√	√	√	√	√
4.4	√	√	√	√	√	√	√

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)	NFS
4.5	√	√	√	√	√	√	√
5.0.x	√	√	√	√	√	√	√
5.1.x	√	√	√	√	√	√	√
5.2	√	√	√	√	√	√	√
5.2.2	√	√	√	√	√	√	√
5.3	√	√	√	√	√	√	√
5.4	√	√	√	√	√	√	√

✥Events are collected from Dell CEE.

For more information, see Dell Unity Requirements.

Generic Data Source

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)	NFS
N/A[a, b]	√		√			√	

a. IMPORTANT: Generic data sources can only be used for data sources that support SMB and WINAPI.

b. Event auditing is not supported.

For more information, see Generic Data Source Requirements.

Hitachi Content Platform Anywhere Enterprise (HCP-AWE)

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)	NFS
7.5 ✣	√	√	√		√	√	

✣Hitachi HCP Anywhere Enterprise (HCP-AWE) should be deployed as a CTERA data source.

Hitachi Content Platform (HCP) Gateway

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)	NFS
4.3.1✣	√					√	

✣Hitachi HCP Gateway should be deployed as a Windows Server, including installation of a Windows agent to audit events.

Hitachi NAS

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)	NFS
14.2✣	√	√	√	√	√	√	
14.5✣	√	√	√	√	√	√	
14.6✣	√	√	√	√	√	√	

✣Access denied events are not supported.

For more information, see Hitachi NAS Requirements.

IBM AIX

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)	NFS
AIX-5300-powerpc-64	√	√	√				√
AIX-6100-powerpc-64	√	√	√				√
AIX-7100-powerpc-64	√	√	√				√
AIX 7.2	√	√	√				

For more information, see Unix Requirements.

Linux

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)	NFS
Linux kernels✣	√	√	√		N/A		√

✣Only Red Hat Enterprise Linux (RHEL) is supported.

For a complete list of supported kernel versions, see Supported Linux Versions and Requirements.

Microsoft 365

To monitor multiple M365 tenants, create an Entra ID data source for each tenant.

Entra ID

Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies
√	√	N/A	N/A	

For more information, see M365 > Entra ID Requirements.

Exchange Online

Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies
√	√	√		

For more information, see M365 > Exchange Online Requirements.

OneDrive

Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies
√	√	√	√	√

For more information, see M365 > OneDrive Requirements.

SharePoint Online

Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies
√	√	√	√	√

For more information, see M365 > SharePoint Online Requirements.

Nasuni

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)	NFS
8.5	√	√	√	√	√	√	
8.7	√	√	√	√	√	√	
8.8	√	√	√	√	√	√	
9.0	√	√	√	√	√	√	
9.3	√	√	√	√	√	√	
NEA 9.5	√	√	√	√	√	√	
NMC 21.2	√	√	√	√	√	√	

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)	NFS
9.7	√	√	√	√	√	√	
9.8	√	√	√	√	√	√	
9.9	√	√	√	√	√	√	
9.10	√	√	√	√	√	√	
NMC 23.1	√	√	√	√	√	√	
9.12	√	√	√	√	√	√	
NMC 23.2	√	√	√	√	√	√	
9.14	√	√	√	√	√	√	
NMC 23.3	√	√	√	√	√	√	

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)	NFS
9.15	√	√	√	√	√	√	
NMC 24.1	√	√	√	√	√	√	

✣ Starting from Nasuni release 9.5, the NMC can be released independently from the Nasuni Edge Appliance, so a new NMC versioning system was introduced to reflect this change. From this version onwards, NMC versions will be listed in this matrix in addition to NEA (Nasuni Edge Appliance) versions.

For more information, see Nasuni Requirements.

NetApp ONTAP Cluster Mode

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)[c]	NFS
Cloud Volumes ONTAP[a, b]	√	√	√		√	√	√
Amazon FSx for NetApp ONTAP[c]	√	√	√	√ (CIFS only)	√	√	√
8.2.x	√	√	√	√ (CIFS only)	√	√	√

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)[c]	NFS
8.3.x	√	√	√	√ (CIFS only)	√	√	√
9.0 RC	√	√	√	√ (CIFS only)	√	√	√
9.1	√	√	√	√ (CIFS only)	√	√	√
9.2	√	√	√	√ (CIF	√	√	√

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)[c]	NFS
				S only)			
9.3	√	√	√	√ (CIFS only)	√	√	√
9.4	√	√	√	√ (CIFS only)	√	√	√
9.5	√	√	√	√ (CIF	√	√	√

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)[c]	NFS
				S only)			
9.6	√	√	√	√ (CIFS only)	√	√	√
9.7[e]	√	√	√	√ (CIFS only)	√	√	√
9.8[e]	√	√	√	√ (CIF	√	√	√

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)[c]	NFS
				S only)			
9.9.1x[e]	√	√	√	√ (CIFS only)	√	√	√
9.10.1x[e]	√	√	√	√ (CIFS only)	√	√	√
9.11.1x[e]	√	√	√	√ (CIF	√	√	√

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)[c]	NFS
				S only)			
9.12.1x[e]	√	√	√	√ (CIFS only)	√	√	√
9.13.1x[e]	√	√	√	√ (CIFS only)	√[f]	√	√
9.14.1x[e]	√	√	√	√ (CIF	√[f]	√	√

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)[c]	NFS
				S only)			
9.15.1x[e, g]	√	√	√	√ (CIFS only)	√	√	√

a. Cloud Volumes ONTAP (CVO) High Availability (HA) is supported.

b. To monitor events, a Collector or proxy should be installed in the same cloud network close to the CVO shares.

c. The firewall rules for Amazon FSx for NetApp ONTAP are identical to those for NetApp ONTAP.

d. SMBv3 is supported for NetApp clusters.

e. For ONTAP versions 9.7 and higher, depending on the ONTAP version, Windows Updates for CVE-2022-38023 on domain controllers starting June 13, 2023 will cause NTLM authentication for our API calls to ONTAPI to fail. NTLM will only be used as a fallback in environments where Kerberos authentication fails. To resolve this issue, you need to upgrade the ONTAP version. For more information, see this KB article.

f. ONTAP version 9.14.1 is not currently supported for the Remediate org-wide exposure policy.

g. Starting from ONTAP version 9.15.1, REST API permissions are required.

For more information, see NetApp Requirements.

Nutanix

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)	NFS
3.7.1[a]	√	√	√	√	√	√	
3.8.1[a]	√	√	√	√	√	√	
4.0.0.2[a, b]	√	√	√	√	√	√	
4.0.3[a, b]	√	√	√	√	√	√	
4.1.01[a, b]	√	√	√	√	√	√	

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)	NFS
4.2.1[a, b]	√	√	√	√	√	√	
4.3.x[a]	√	√	√	√	√	√	
4.4.x[a]	√	√	√	√	√	√	
5.0.0.3[a, b]	√	√	√	√	√	√	

a. Varonis supports only Nutanix Acropolis File Services (AFS).

b. Nutanix versions 4.2 and 5.0.0.2 are not supported.

For more information, see Nutanix Requirements.

Panzura

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)	NFS
PZOS 8.0.2	√	√	√	√	√	√✣	
PZOS 8.2.2	√	√	√	√	√	√✣	
PZOS 8.2.4	√	√	√	√	√	√✣	
PZOS 8.2.5	√	√	√	√	√	√✣	
PZOS 8.3.1	√	√	√	√	√	√✣	

✣Access Denied events are not supported.

For more information, see Panzura Requirements.

Pure Storage FlashArray Data Sources

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)	NFS
6.6.11	√	√	√	√		√	

For more information, see Pure Storage FlashArray Requirements.

Pure Storage FlashBlade Data Sources

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)	NFS
4.4.1	√	√	√	√		√	

For more information, see Pure Storage FlashBlade Requirements Requirements.

Qumulo

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)	NFS
6.0.x	√	√	√	√	√	√	
6.1.x	√	√	√	√	√	√	
6.2.x	√	√	√	√	√	√	
6.3.0.1	√	√	√	√	√	√	
7.2.1	√	√	√	√	√	√	

✥Qumulo version 7.13 is not supported.

For more information, see Qumulo Requirements.

Unix Directory Services

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)	NFS
LDAP	√				N/A		
NIS	√				N/A		
Samba AD	√				N/A		

For more information, see Unix Directory Services Requirements.

VAST

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)	NFS
5.2.x	√	√	√	√		√	

For more information, see VAST Requirements.

Windows

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)
2008 64-bit with SP2[a, c, d]	√	√	√	√	√	√
2008 R2 64-bit with SP1 or SP2[b, c, d]	√	√	√	√	√	√
2012 64-bit[e], 2012 R2 64-bit[f]	√	√	√	√	√	√
2016 (Standard, Core Standard, Datacenter)	√	√	√	√	√	√

Version	Data Access Intelligence	Threat Detection and Response (UEBA)	Data Discovery and Classification	Data Labeling	Automated Remediation Policies	SMB (CIFS)
2019 (Standard, Core Standard, Datacenter)	√	√	√	√	√	√
2022 (Standard, Core Standard, Datacenter)	√	√	√	√	√	√
Amazon FSx for Windows[g]	√	√	√	√	√	√

a. Windows 2008 must be installed with SP2. For Windows 2008 SP2, install Microsoft KB 4039648, KB 4493730, and KB 4474419.

b. For Windows 2008 R2 SP1, install Microsoft KB 4490628 and KB 4474419.

c. For Windows 2008/2008 R2, you need to manually install the agent. Download the Windows agent from My Downloads on varonis.com (located under EventsCollection > Varonis.Agent.Setup.2008.x64) and install it on your Windows data source.

d. Windows 2008/2008 R2 are not supported for the Collector installation.

e. Windows 2012 Dynamic Access Control is not supported.

f. For Windows 2012 R2, install Microsoft KB 4345424.

g. The firewall rules for Amazon FSx for Windows are identical to those for Windows.

For more information, see Windows Requirements.

Network Devices

Network devices include the following. Click the relevant link to view which network device is supported for which functionalities.

- VPN
- Web Proxy
- DNS

VPN

Version	Data Access Intelligence	Threat Detection and Response (UEBA)
Check Point versions R77.x, 80.x, or 81.x	√	√
Cisco ASA version 9.x (AnyConnect)	√	√
Cisco Firepower Threat Defense (FTD) version 6.x or 7.x	√	√

Version	Data Access Intelligence	Threat Detection and Response (UEBA)
Citrix ADC (Netscaler) version 12.x, 13.x, 14.x, or 15.x	√	√
F5 BIG-IP APM version 12.x, 13.x, 14.x, 15.x, or 16.x	√	√
Fortinet FortiGate (with or without FortiAnalyzer) running FortiOS version 5.x, 6.x, or 7.x	√	√
Microsoft Always On VPN	√	√
Palo Alto firewalls running PAN-OS 8.x, 9.x, 10.x, or 11.x	√	√
Pulse Secure version 8.xR.x or 9.x	√	√
SonicWall SonicOS version 6.x or 7.x	√	√
Sophos XG VPN version 18.x or 20.x	√	√

For more information, see Network Device Data Sources.

Web Proxy

Version	Data Access Intelligence	Threat Detection and Response (UEBA)
Apache HTTP Server version 2.x	√	√
Barracuda Web Security Gateway version 14.x or 15.x	√	√
Cisco Firepower Threat Defense (FTD) versions 6.x or 7.x	√	√
Cisco (IronPort) Web Security Appliances AsyncOS 10.x-14.x	√	√
Cisco Umbrella	√	√
Forcepoint (WebSense) Web Security 8.x	√	√
Fortinet FortiGate (with or without FortiAnalyzer) running FortiOS version 6.x or 7.x	√	√

Version	Data Access Intelligence	Threat Detection and Response (UEBA)
McAfee Web Gateway 7.x or 10x; Skyhigh Secure Web Gateway (On Prem) version 10.x (previously McAfee Web Gateway)	√	√
Palo Alto firewalls running PAN-OS 7.x, 8.x, 9.x, 10.x, or 11.x	√	√
Sophos XG Proxy version 18.x or 20.x	√	√
Squid versions 3.x, 4.x, and 5.x	√	√
Symantec (Bluecoat) ProxySG 6.x	√	√
Zscaler Proxy version 5.x and 6.x	√	√

For more information, see Network Device Data Sources.

DNS

Version	Data Access Intelligence	Threat Detection and Response (UEBA)
BlueCat 9.3.0 and 9.4.0	√	√
Cisco Umbrella	√	√
Infoblox version 8.x	√	√
Microsoft Windows Server 2012 R2, 2016, 2019, and 2022	√	√

For more information, see Network Device Data Sources.

VARONIS SAAS WEB INTERFACE USER GUIDE

Publishing Information

Software Version

Publication date November 19, 2024

Copyright © 2005 -2024 Varonis Systems Inc.
All rights reserved.
This information shall only be used in conjunction with services contracted for with Varonis Systems, Inc. and shall not be used to the detriment of Varonis Systems, Inc. in any manner. User agrees not to copy, reproduce, sell, license, or transfer this information without prior written consent of Varonis Systems, Inc.
Other brands and products are trademarks of their respective holders.

Contents

Chapter 1: Working with the Varonis SaaS Web Interface. 5
Basic Functionality. 6
Chapter 2: Logging In to the Varonis SaaS Web Interface. 7
Chapter 3: Dashboards. 12
Working with Dashboards. 16
Exporting Dashboards. 16
Working with Widgets. 18
Widget Types. 19
Available Widget Menu Actions. 26
Adding and Removing Widgets. 37
Jumping from Dashboard Widgets to their Filtered Analytics. 39
Specific Dashboards. 40
Classification on the Exchange Online Dashboard. 40
Chapter 4: Analytics. 46
Running Your First Search Query. 51
Refining Your Search. 53
Resource Side Pane. 59
Saving Your Searches. 61
Working with Saved Searches. 63
Analyzing Data Classification Results of a File. 64
Chapter 5: Varonis Managed Data Detection and Response (MDDR). 69
Chapter 6: Athena AI. 74
Enabling Athena AI. 75
AI SOC Analyst. 76
Natural Language Search. 78
Chapter 7: Management. 80
Policies. 81
Working with Automations. 81
Threat Detection Policies. 93
Data Discovery Policies. 102
Working with the Action Center. 107

Downloading a CSV Approval File. 109
Rolling Back Actions of an Automation. 111
Working with Scheduled Searches. 112
System Health. 114
Discovery Monitor. 116
Labeling Monitor. 117
Chapter 8: Securing Copilot for Microsoft 365. 119
Chapter 9: Configuration. 124
System Topology. 125
API Keys. 126
Third-Party Integrations. 128
EDR Integration. 139
Settings. 148
Staleness Threshold. 148
Response Scripts. 149
Generative AI. 150
AI Conversation Auditing. 150
Flags. 151
Notifications. 152
Administrative Tools. 153
Collector Dumps. 153
Audit Log. 154
Chapter 10: Account. 156
License Information. 157
Chapter 11: Understanding Risk Indicators. 159
Organization-Wide Exposure. 160
Staleness. 162
Resource Staleness FAQs. 162
Account Staleness FAQs. 164
Permission and Membership Staleness FAQs. 164
Chapter 12: Appendix. 167
Privacy Automation Search Syntax. 168

1 WORKING WITH THE VARONIS SAAS WEB INTERFACE

The Varonis Web Interface provides several ways to narrow your focus and pinpoint the events and alerts that most require your attention, enabling you to review high-level summarized data via metrics in dashboards and perform investigation flows based on the collected data.

The Varonis Web Interface enables investigations flows, such as alerts and events investigations. These flows are based on an intuitive search mechanism that eases and simplifies investigation flows. In addition, predefined saved searches representing valuable use cases are provided, and additional saved searches can be defined. Investigation results can be exported from the Varonis Web Interface and scheduled searches can be easily configured.

Basic Functionality

The following table introduces the icons that perform the basic functions of the Varonis Web Interface.

Icon	Description
	Expands and collapses menus.
	Adds new tabs in the Analytics tab.
	Opens a list of options for displaying information and jumping to the results of a search query in the Analytics tab from where you can refine your search results.
	Opens a list of options for jumping to related alerts, events, accounts, permissions, or resources (depending on the tab that is currently active). The relevant page opens and the query is automatically updated, enabling you to easily see your data in a narrower context for further investigation.

2 LOGGING IN TO THE VARONIS SAAS WEB INTERFACE

As of March 2023, the Varonis Web Interface supports single sign-on authentication through the MyVaronis Portal. If your organization has configured federated authentication, you will no longer be able to log in using a username and password. If your organization does not use federated authentication, follow the steps below to authenticate via Varonis Okta.

Workflow for Logging In

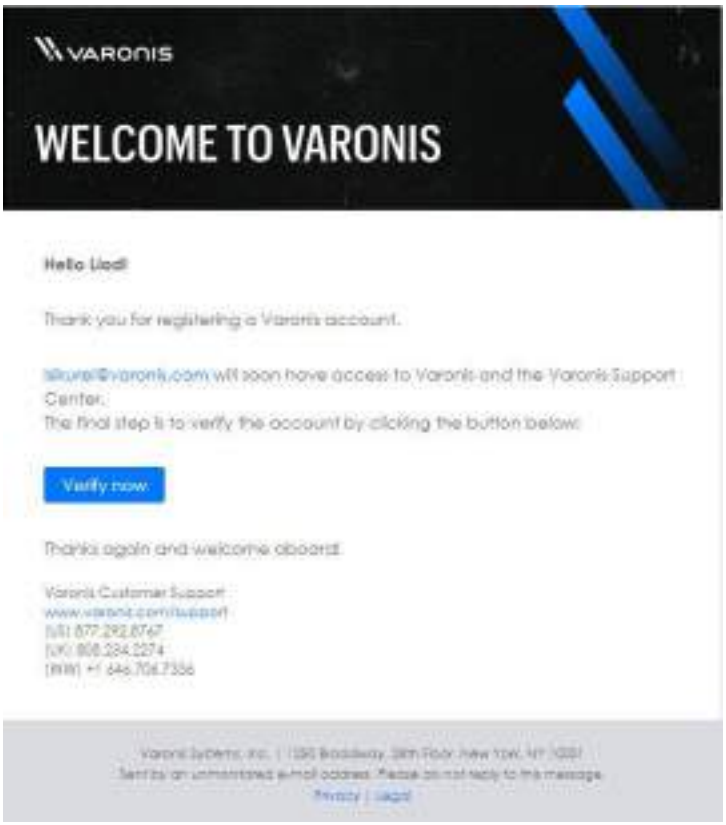
1. Your organization administrator registers you as a Varonis user.
2. Varonis sends you an account activation email.
3. Follow the steps to start using single sign-in (SS0).
4. Log in using SS0.

To easily access the Varonis Web Interface, make sure to bookmark the tenant URL (and not the URL that is available after you login, since it includes the session details).

> Note: If you haven't activated your account yet, click here to regenerate the activation email or check your mailbox's spam folder for the activation email.

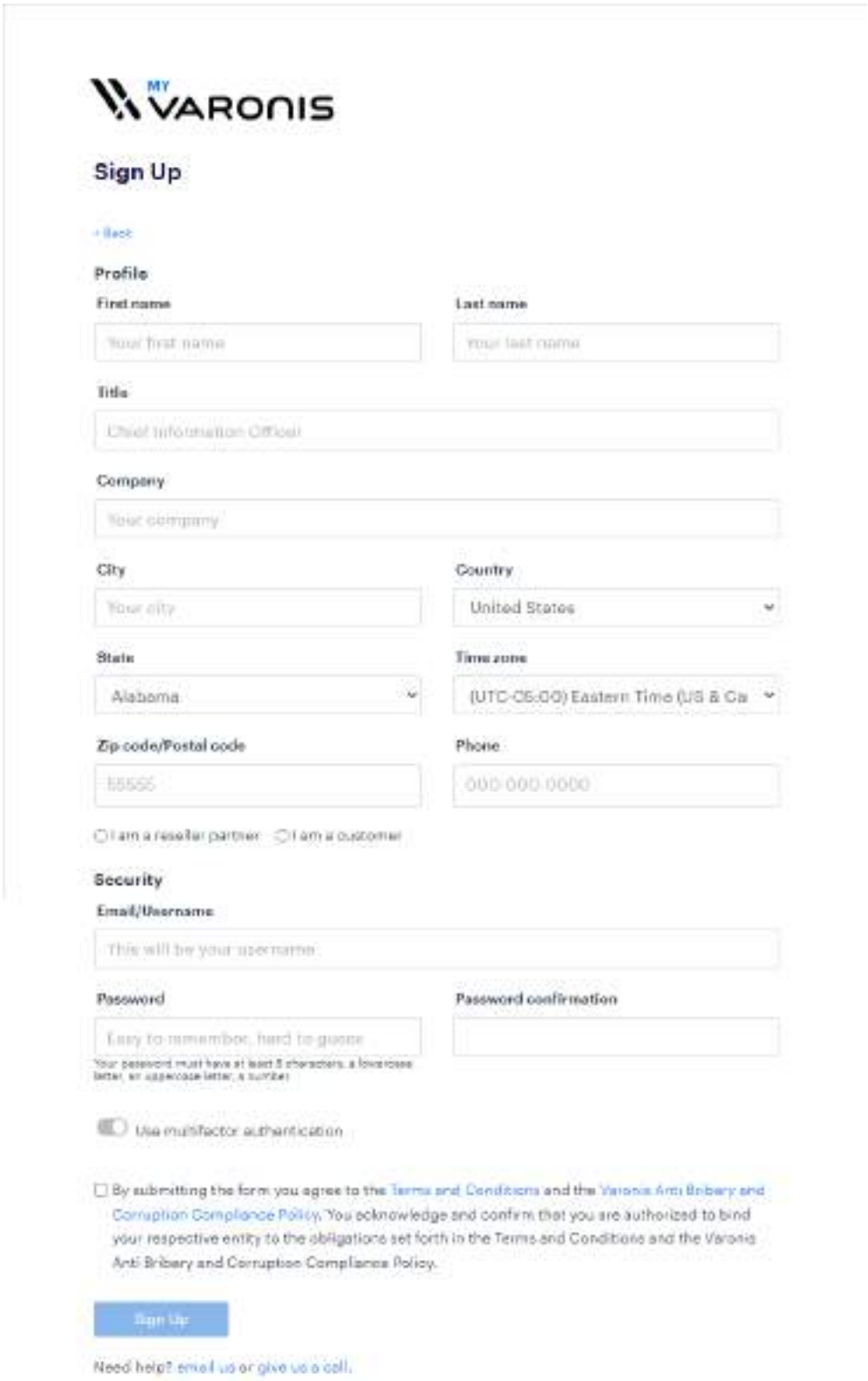
Start Using Single Sign-On

1. Once your account is registered in Varonis by your organization's account owner, you will receive an email to verify and activate your account.



Note: If your organization has its own single sign-on provider, you will not receive a setup email, but will instead be redirected to your organization's identity provider to log in.

2. Click Verify Now. You'll be redirected to the MyVaronis portal, where you can finish setting up your profile.


MY VARONIS
Sign Up
‹ Back
Profile
First name
Last name
Your first name
Your last name
Title
Chief Information Officer
Company
Your company
City
Country
Your city
United States
State
Time zone
Alabama
(UTC-05:00) Eastern Time (US & Ca
Zip code/Postal code
Phone
55555
000 000 0000
I am a reseller partner
I am a customer
Security
Email/Username
This will be your username
Password
Password confirmation
Easy to remember, hard to guess
Use multifactor authentication
By submitting the form you agree to the Terms and Conditions and the Varonis Anti Bribery and Corruption Compliance Policy. You acknowledge and confirm that you are authorized to bind your respective entity to the obligations set forth in the Terms and Conditions and the Varonis Anti Bribery and Corruption Compliance Policy.
Sign Up
Need help? email us or give us a call.

3. (Recommended) Enable Use multifactor authentication (MFA) for your account.

   Note: After multifactor authentication is configured on your account, it cannot be removed.

4. Click Update.
5. On the next screen, set a password for your Varonis account.

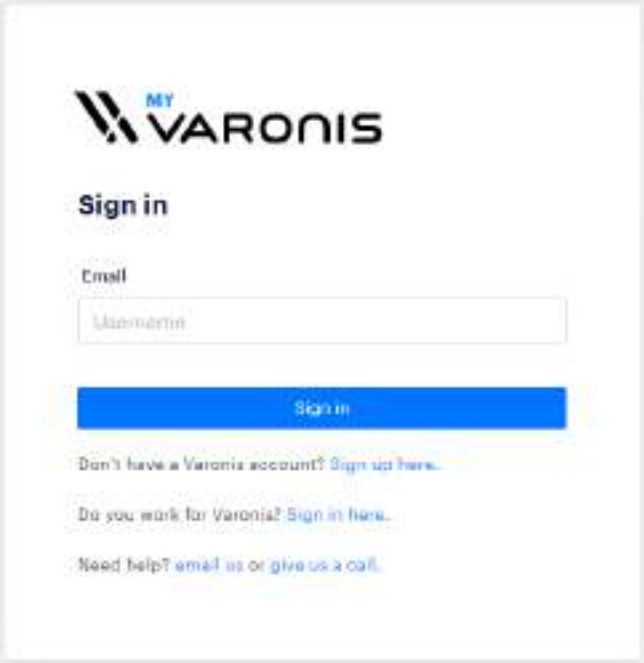


6. Click Apply. You are redirected to the Varonis login page.
7. Log in to the Varonis Web Interface with your username and password.

Logging In Using SSO

1. Click the login link provided in the email.
   The Varonis Web Interface Login page is displayed.
2. Click Continue With SSO.

The MyVaronis Sign In page is displayed.

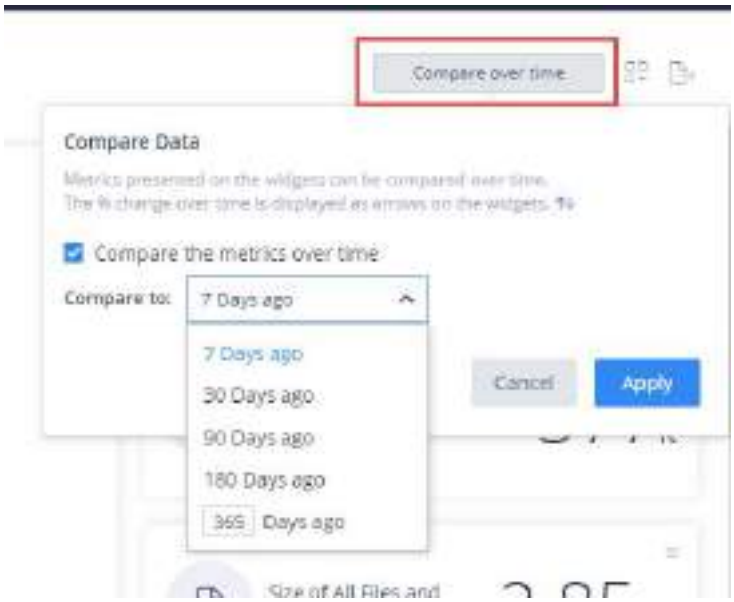


3. Enter your email, and click Sign In. The relevant login page is displayed, depending on whether your organization uses Varonis Okta or a different identity provider. Once the login process has been completed, you'll be redirected and logged into the Varonis Web Interface.

3 DASHBOARDS

The dashboards in the Varonis Web Interface provide you with a fast understanding of your risk situation and enhanced control over your data. The dashboards display statistics through widgets that enable you view information at a glance. You can easily customize any dashboard to display the widgets that are most useful to you by using the widget picker. You can also compare the dashboard widgets over time by selecting the Compare over time button and then setting the period you want to compare.

Note: Dashboard widgets are updated once a day (via the metrics job), while Analytics queries run on the latest data in the database. Please expect some discrepancies between high-level widget data and drill-down Analytics results.



Note: The Compare over time option is not relevant to the Alerts dashboard.

The default dashboard view is the Alerts dashboard:



The following dashboards are available:

Dashboard	Description
Alerts	Displays alert information retrieved for a specified time period, enabling you to quickly view and detect suspicious activity for further analysis. This view also presents the top five alerted users, assets, devices, and threat models as well as a kill chain analysis. For platforms enriched with geolocation, including SharePoint Online, Exchange Online, OneDrive,

Dashboard	Description
	and VPN, the dashboard displays a map with geolocation information, enabling you to view the locations from which the alerts were generated.
Compliance	Provides insights to help decision-makers identify compliance trends and to spot compliance problems before they become a real threat. The Compliance dashboard default view provides key metrics at a glance at classification category and rule level, focusing on the potential risk of sensitive, stale, or over-exposed data. Additional metrics are available in the widget picker of the Compliance dashboard.
File Servers	Displays aggregated file system statistics for selected data sources.
Active Directory	Displays aggregated directory service statistics for selected domains.
Entra ID	Provides visibility into your Entra ID environment and highlights potential risks. Using the dashboard you can easily understand your Cloud directory and identify risks, such as over-privileged users.
Copilot	Provides a clear view of how your organization uses Copilot and whether your data is at risk. This dashboard provides live stats on Copilot usage, including daily counters of Copilot

Dashboard	Description
	interactions (prompts) and the sensitive files referenced. In addition, you can get general information on your organization's Copilot usage, like the exposure level and sensitivity of the referenced files and the state of data exposure in your M365 environment.
Network Devices	Displays aggregated statistics for selected VPN, Web Proxy, and DNS sources.
Exchange Online	Displays aggregated statistics for selected Exchange Online data sources.
SharePoint Online	Displays aggregated statistics for selected SharePoint Online data sources.
OneDrive	Displays aggregated statistics for selected OneDrive data sources.

Working With Dashboards

The dashboards in the Varonis Web Interface display statistics through a range of different widgets.

Read Working with Widgets to learn about the different types of widgets available and how to work with them.

Exporting Dashboards

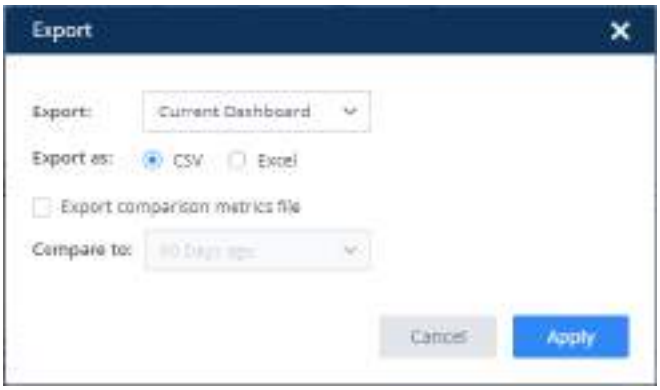
If you want to download and analyze the data behind the widget in a separate file, you can download all the dashboards or just the dashboard you are currently viewing as a CSV or Excel file at any time.

1. From a dashboard, click the Export icon in the top-right corner of the screen.



> Note: The Export icon is not available for the Alerts and Network Devices dashboards.

2. In the Export dialog box, set the following:



   a. From the Export dropdown list, select Current Dashboard or All Dashboards.

   > Note: To export data about decommissioned file servers, use the Current Dashboard option.

   b. In the Export as field, select the format in which to export the dashboard statistics.

   c. To export a comparison of the current dashboard statistics with past statistics, select the Export comparison metrics file checkbox, then from the Compare to

dropdown list, select the point in the past with which to compare current dashboard statistics.

3. Click Apply to download the selected file format.

If you chose to export a comparison, two files are downloaded: one with current metrics and one with historical metrics.

- Files with current metrics are named in the format SharePoint_Online_Current_202209111317.xlsx (or .csv), where:
  - SharePoint_Online is the name of the selected dashboard, if you selected Current Dashboard from the Export dropdown list. If you selected All Dashboards from the Export dropdown list, All_Dashboards appears here.
  - 20220911 indicates the year, month, and day of the download.
  - 1317 indicates the time of the download.
- Files with historical metrics are named in the format SharePoint_Online_Compared_202209111317.xlsx (or .csv), where:
  - SharePoint_Online is the name of the selected dashboard, if you selected Current Dashboard from the Export dropdown list. If you selected All Dashboards from the Export dropdown list, All_Dashboards appears here.
  - 20220911 indicates the year, month, and day of the download.
  - 1317 indicates the time of the download.

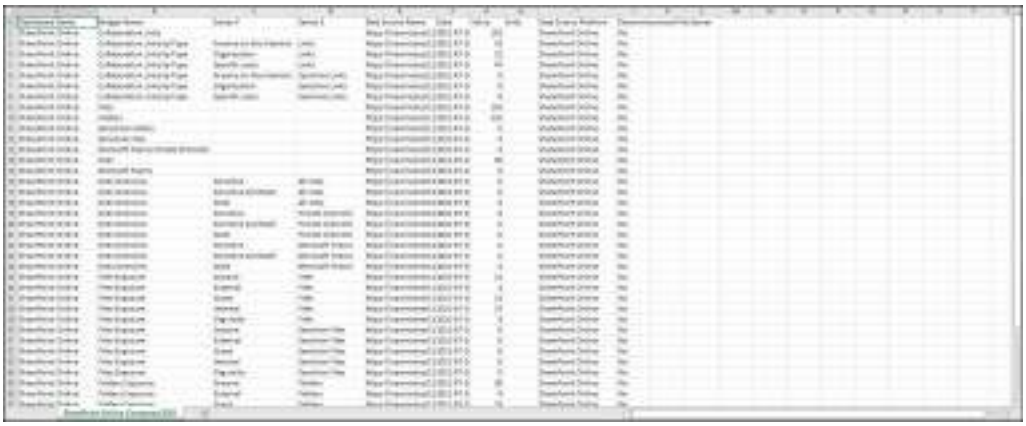
Note: Chrome may block the download of these files for security reasons. Before downloading, enable multiple downloads for your Chrome browser.

Downloaded files contain the following information:

- Dashboard Name – The name of the dashboard.
- Widget Name – The name of the widget.
- Series Y – The categories listed on the vertical Y axis of the chart.
- Series X – The series for which the categories are measured.
- Data Source Name – The name of the file server or domain name from which the data is taken.
- Date – The date from which the metric is calculated.
- Value – The total number of records collected by the metric.
- Units – The unit of the value presented, where relevant. For example, bytes.
- Data Source Platform – The data source as defined for the dashboard.

- Decommissioned File Server – An indication of whether the file server is decommissioned. Decommissioned file servers are available only when you export the current dashboard.

Here are examples of downloaded CSV file:



Working With Widgets

Read this section to learn about the different Widget Types available, and how to work with them.

You can easily customize the dashboards to display the information you need. For example, you can add or remove widgets, or return to the default display for your dashboard, as required. You can also organize widgets according to your needs by dragging and dropping them around the dashboard. Up to four single-metric widgets can be moved to the top of the dashboard for simultaneous convenient viewing.

The changes that you make in the dashboards are personal and only visible to you. All customizations are saved and displayed upon future log-ins. You can also print your personalized dashboard or revert to the default widget view at any time.

Each widget presents aggregated metric data for the selected scope, calculated at the time the search query was last run. If no data is retrieved for a widget, ensure that you have sufficient permissions and that the Trend job is running.

Widget Types

Dashboards display statistics through widgets that enable you view information at a glance. The following sections describe different types of widgets used to present your data:

- Single-statistic metric
- Percentage
- Horizontal bar chart
- Stacked vertical bar chart
- Overlay bar chart
- Timeline chart
- List
- Geo

Note: For a description of a specific widget, go to the additional actions menu icon in the top-right corner and select Information.

Single-statistic Metric Widgets



- Single-metric widgets show a single data point. These widgets are useful for monitoring data that remains relatively stable over time. For example, the total size of all files and folders, or aggregate count of files or folders.

Percentage Widgets



- Percentage widgets compare two metrics. By default, they display a number and that number as a percentage of another number. For example, the number of sensitive folders as a percentage of all folders.

Horizontal Bar Chart Widgets



- Horizontal bar chart widgets allow you to compare different metrics side by side. For example, you can see cloud users and synced users for both internal and guest users at the same time.
- Hover over a bar to view statistics in a pop-up (1). Click the pop-up to jump to the Analytics page to drill down to more details.
- Click on a series to hide it and focus on other data (2). This might change the chart's scale. Click again to show the series.

Stacked Vertical Bar Chart Widgets



- Stacked vertical bar chart widgets display statistics from multiple widgets at the same time stacked one on top of the other. They display multiple series of statistics that are measured for defined categories.
- Hover over a bar to view statistics in a pop-up (1). Click the pop-up to jump to the Analytics page to drill down to more details.
- Click on a series to hide it and focus on other data (2). This might change the chart's scale. Click again to show the series.

Overlay Bar Chart Widgets



- Overlay bar chart widgets display series as subsets of others, unlike horizontal bar chart widgets that display statistics from multiple metrics side by side. It's ideal for visualizing large data sets and making comparisons, such as the total number of applications versus those from unverified publishers.
- Hover over a bar to view statistics in a pop-up (1). Click the pop-up to jump to the Analytics page to drill down to more details.
- Click on a series to hide it and focus on other data (2). This might change the chart's scale. Click again to show the series.

Timeline Chart Widgets



- Timeline chart widgets are single-category or multiple-category widgets that display statistics over time. Multiple-category widgets display multiple series of statistics, each corresponding to a specific category.
- Some Timeline chart widgets provide a dropdown list for filtering options (1). For example, Stale Permissions and Sensitive Stale Permissions.
- Hover over a bar to view statistics in a pop-up (2). Click the pop-up to jump to the Analytics page to drill down to more details.
- Click on a series to hide it and focus on other data (3). This might change the chart's scale. Click again to show the series.
- Any single-metric widget or percentage widget can be become a timeline chart widget.

List Widgets



- List widgets display individual values from a single set. For example, they can show a list of the top alerted users along with the number of alerts for each user.
- This list is arranged in descending order, highlighting the most-alerted users based on factors such as data sources, time period, severity, and status.
- A set of actions can be performed on each entry in the list.
- Hover over the account text to view a full description in a pop-up.

Geo Widgets



- Geo widgets display the number and severity of alerts in a pop-up for a geolocation selected on a map.
- Hover over an indicated location to view statistics in a pop-up. Click the indicated location to jump to the Analytics page to drill down to more details.

Available Widget Menu Actions

Read this section to learn about how to take full advantage of all the actions that can be performed on widgets.

To perform any of these actions, click the widget menu icon in the top-right corner of any widget and select one of the following options from the dropdown list.

> Note: Available actions vary according to widget type.



Action	Description	Example (click an image to enlarge)
Information	Presents an explanation of the statistics that the widget displays.	Compliance 
See all alerts on <category displayed by widget>	Jumps from the Alerts dashboard to the Analytics tab and displays alerts by the category of data displayed by the widget. For example, by threat detection policies, users, devices, Watch List users, or by geolocation. For more information, see Analytics.	Alerts 

Action	Description	Example (click an image to enlarge)

Action	Description	Example (click an image to enlarge)
View Items	Jumps to the relevant tab in the Analytics tab and presents the statistics displayed by the widget in the form of the results of a search. For more information, see Analytics.	SharePoint Online 

Action	Description	Example (click an image to enlarge)
View Automation	Jumps to the Automations tab of the Policies area and presents the statistics displayed by the widget in the form of the results of a search. For more information, see	SharePoint Online 

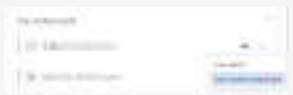
Action	Description	Example (click an image to enlarge)
	Working with Automations.	
Show as Number	Changes the display to a single-metric widget.	SharePoint Online  
Show as Timeline	Changes the display to a timeline chart widget.	SharePoint Online 

Action	Description	Example (click an image to enlarge)
		
Show as Percentage	Changes the display to a percentage widget.	 

Action	Description	Example (click an image to enlarge)
Remove	Removes the widget from the dashboard display. You can add it again if you wish.	SharePoint Online 
View alerts (from list widgets in the Alerts dashboard)	Jumps from the Alerts dashboard to the Analytics tab and presents the alerts displayed by the widget by alert category in the form of the results of a search. For more information, see Analytics.	
Open Device context card (from list widgets in the Alerts dashboard)	Displays the device context card showing information about the device and the alerts on it.	

Action	Description	Example (click an image to enlarge)
		
Open account context card (from list widgets in the Alerts dashboard)	Displays the account context card showing information about the account and the alerts on it.	

Action	Description	Example (click an image to enlarge)
		 

Action	Description	Example (click an image to enlarge)
		
Open asset context card (from list widgets in the Alerts dashboard)	Displays the asset context card showing information about the asset and the alerts on it.	

Action	Description	Example (click an image to enlarge)
		

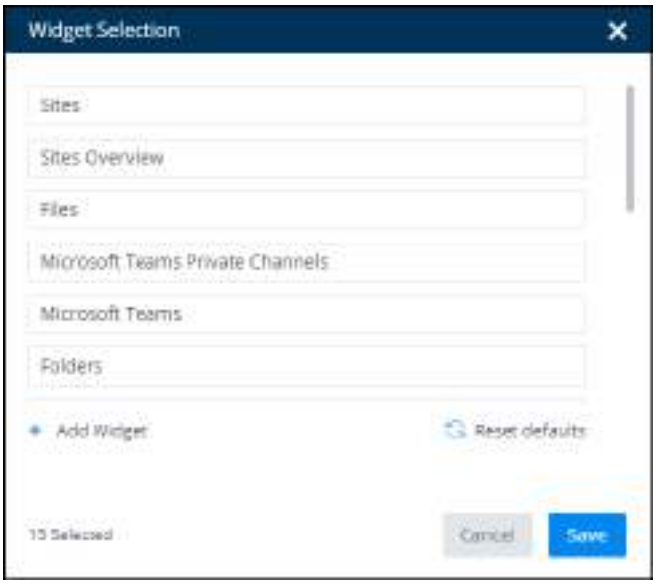
Adding and Removing Widgets

If you want to change the widgets that are currently displayed in a dashboard, you can add and remove widgets, or return to the default display for your dashboard, using the widget picker.

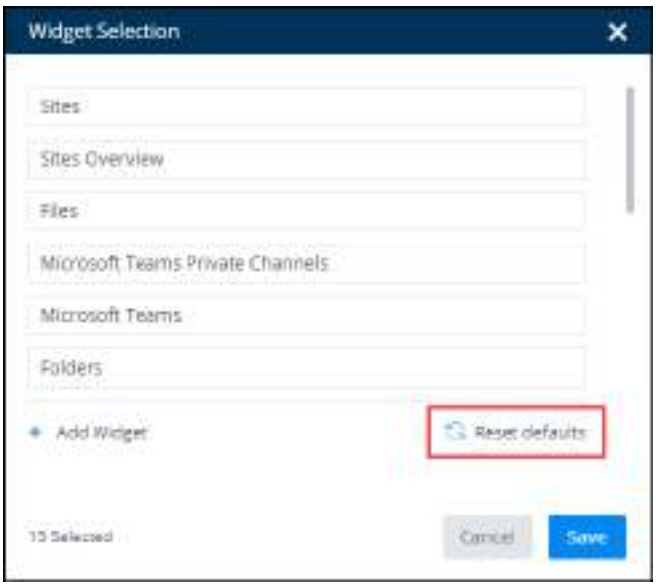
1. From any dashboard, click the Select Widgets icon in the top-right corner of the screen.



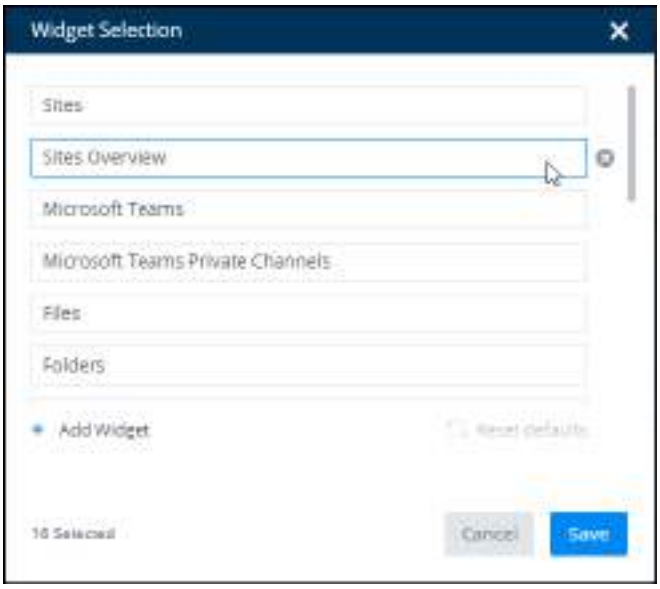
The Widget Selection dialog box displays a list of all the widgets currently showing in the dashboard you are viewing.



2. Configure the Widget Selection dialog box as follows:
   - To add a widget, click Add Widget and select the widget you want from the alphabetical list (or start typing the name of the widget in the search box and select he required widget from the list). Then click Save.
   - To return your dashboard to its default display, click Reset defaults. Then click Save.



   - To remove a widget from your dashboard, place your cursor over the widget in the list and click the "X" that appears next to the widget name. The click Save.



You can add the deleted widget to your dashboard at any time.

The dashboard updates automatically.

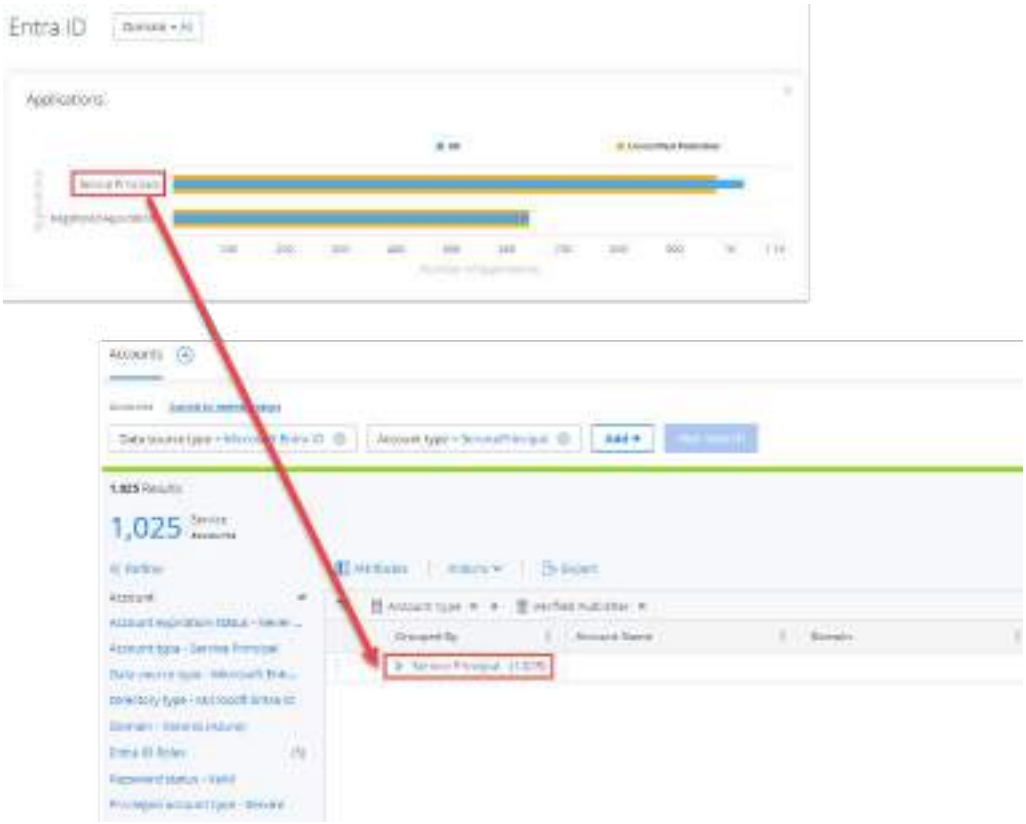
Jumping from Dashboard Widgets to their Filtered Analytics

The Dashboards page's widget elements (titles, categories, and series) are context-sensitive, so you can click a specific element to view its filtered data on the Analytics page:

- At the Dashboard level - The filters you set on the Dashboards page are applied to the data on the Analytics page.
- At the widget level - Click a specific title, category label, or series, or the View Items menu option to jump to the corresponding filtered data.

Note: Dashboard widgets are updated once a day (via the metrics job), while Analytics queries run on the latest data in the database. Please expect some discrepancies between high-level widget data and drill-down Analytics results.

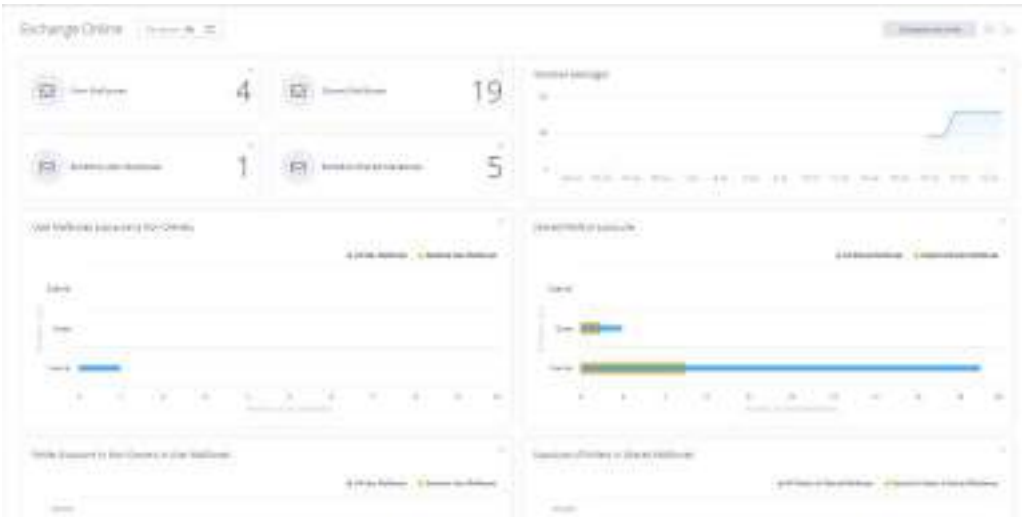
The following example shows a jump from a specific category (Service Principles) in the Applications widget to its filtered data on the Analytics page.



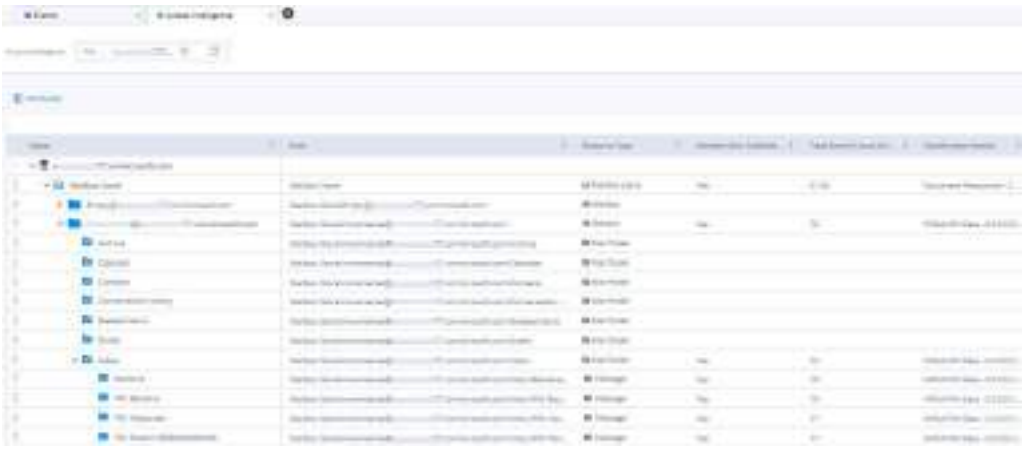
Classification on the Exchange Online Dashboard

The Exchange Online dashboard displays aggregated statistics for Exchange Online data sources. The dashboard displays a variety of widgets for various factors:

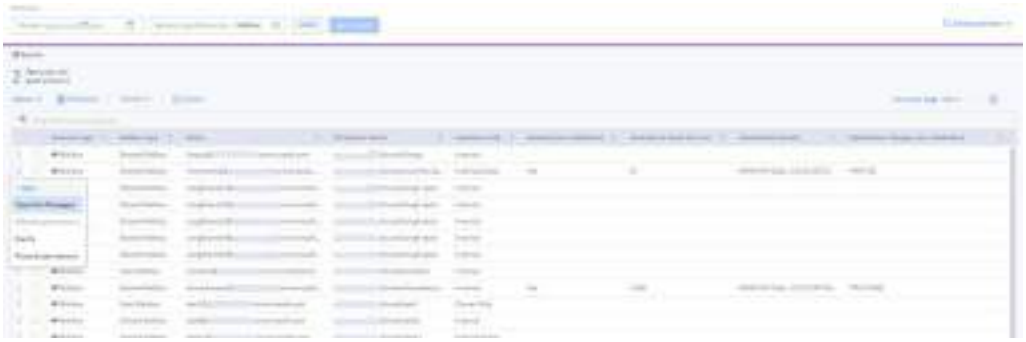
- Inventory-related widgets such as User Mailboxes and Shared Mailboxes
- Sensitivity-related widgets such as Sensitive Shared Mailboxes and Messages by Rule
- Exposure level widgets such as Folder Exposure to Non-Owners in User Mailboxes



Exchange Online messages and their attachments are scanned for data classification (not including link attachments). The classification results for the message and its attachments are aggregated in a single Message resource, available on the Resources and Access Intelligence tabs under Analytics. Mail folders, Mailboxes, and Mailbox Store aggregate classification results for all Messages they contain.



To examine all classified messages under a Mailbox or Mail folder, from the options menu, click View related > Classified Messages.



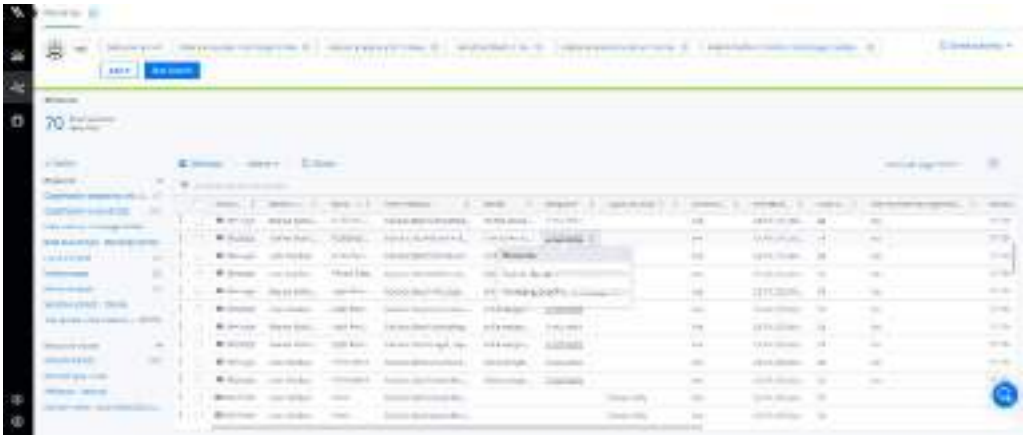
Note: A Mailbox contains Mail folders and does not contain Messages directly. To view classification results of a Mailbox, use attributes that include Incl. Subfolders.

Exchange Online Attributes

Attribute Name	Description	Filterable
Message Subject	The message subject without a prefix (such as RE, FW).	Yes
Sender	The mailbox address of the sender	Yes
Recipients	The mailbox addresses of all the recipients.	Yes

Attribute Name	Description	Filterable
	Note: Distribution lists cannot be expanded.	
Sent Outside the Organization	Indicate if at least one of the recipients is outside the organization	Yes
Parent Mailbox	The name of the parent mailbox	Yes
Message ID	The Message ID as provided by Microsoft API	Yes
Conversation ID	The Conversation ID as provided by Microsoft API	Yes
Delivery Time	The time the message was delivered or created	No

Note: See below an example of using the Recipients attribute.



Note:

- Data labeling is not supported.
- File analysis for attachments is not supported.
- Jumping from the Resources or Access Intelligence tabs to the Events tab is not supported for messages.
- The Events tab does not display classification results for messages.
- Group mailboxes and resource mailboxes are not monitored.
- Email-related items such as, calendar items, notes, and contacts, are not supported.

4 ANALYTICS

In the Analytics page, you can run searches on specified data sources in your environment for different entities (events, alerts, permissions, accounts and memberships, and resources), and view your network as a resource tree. There is a dedicated tab in the Varonis Web Interface for each of these entities.

Searches create reports which include types of data relevant to the entity being searched. For example, running a search in the Resources tab produces a report including data about the files, folders, and sites on the servers in your network that you have specified.

To help you refine your search, insights appear at the top of the grid of results, and facets are displayed on the left side in the Refine pane.

You can also save your searches for future use.

By default, the Analytics page displays the Events tab.



The Analytics page includes the following components:

- A plus sign ⊕ (1) for adding new tabs. Options are:

Entity	Description
Events	Displays a line chart illustrating the dispersion of events (for example, creating or removing a site, folder, file, or permission on the platform you are monitoring) over the specified time line, as well as event information in table form. You can use this information to view and

Entity	Description
	search the activity log of your data sources and domains, identify risky activities, and investigate alerts. Note: All event attributes are logged at the time of the event ingestion. Please be aware that these attributes are immutable: They are not live and are not updated.
Alerts	Displays the alerts triggered by DatAlert. You can use this information to review alerts and search for alerts by a specific user, threat detection policy, and so on to understand the overall threats detected, manage them, and investigate a specific alert.
Permissions	Displays the physical permissions granted directly to users and groups on a resource. Click the Switch to effective permissions link to display the permissions granting access to users or groups as a result of their membership of wider groups which themselves have access to the resource.
Accounts	Displays a tabular view of the retrieved data for all types of accounts. You can use this information to analyze the accounts that triggered the alerts or that have access to the data.

Entity	Description
	Click the Switch to memberships link to display the connections between individual member accounts and the groups to which they belong.
Resources	Displays a tabular view of a resource's properties, based on the criteria you define in the search query. Resources include the sites, folders, or files on the platform you are monitoring.
Access Intelligence	Displays the resources in your network in a hierarchical tree that allows you to see which users have access to each resource, and the permissions granted to each resource. You can also access insights per resource, and view the classification results of an individual file.

- A Saved Searches menu where you can save your searches for reuse at any time (2).
- Default data source and date filters for selecting the data sources and time range over which to run a query (3). The default filters vary according to the entity tab you have selected.
- An Add + button for adding additional filters and values with auto complete suggestions (4). When you begin to type a word or phrase in the search box, auto complete suggestions for filters and filter values that contain the typed text are displayed in the area below the search box. Selecting a filter in this area enables viewing and setting filter values. The selected filter values are automatically added to the search query.
- A Run Search button (5). Click to perform the search.
- An Event Operation dropdown list (6) for selecting the types of events to display in the search results. (Available only in the Events tab.)

- A line chart (in the Events tab) illustrating the dispersion of results matching the defined timeline and search criteria (7).
- A popup displaying the search results at a specific point in the timeline (8) that appears when you place your mouse over the required point.
- Insights (9) are displayed after a search providing a quick way to reach meaningful information. When you click an insight, the insight criteria are added to your search query.
- A Refine pane (10) that presents the number of distinct values retrieved per facet and enables you to refine the scope of your search according to one or more values for a specific facet.
  Facets show the distribution of attributes in the results of your search.

  The Refine pane provides a quick and easy way to drill down and analyze the results per facet. For example, you can select the User name facet in the Refine pane to view information about the users who performed the events which triggered the alert. You can also view the number and percentage of alerts generated per user.

  Click the Refine link to hide or show the Refine pane.
- A grid displaying the results matching the defined timeline and search criteria (11).
- An Actions dropdown list (12) for jumping to the related alerts, events, accounts, permissions, or resources (depending on the tab that is currently active) after selecting multiple entries from the search query results table. The relevant page opens and the query is automatically updated, enabling you to easily see your data in a narrower context for further investigation.

  Alternatively, click the more options button (13) to display the same options as the Actions dropdown list selecting a single entry from the search query results table.

Running Your First Search Query

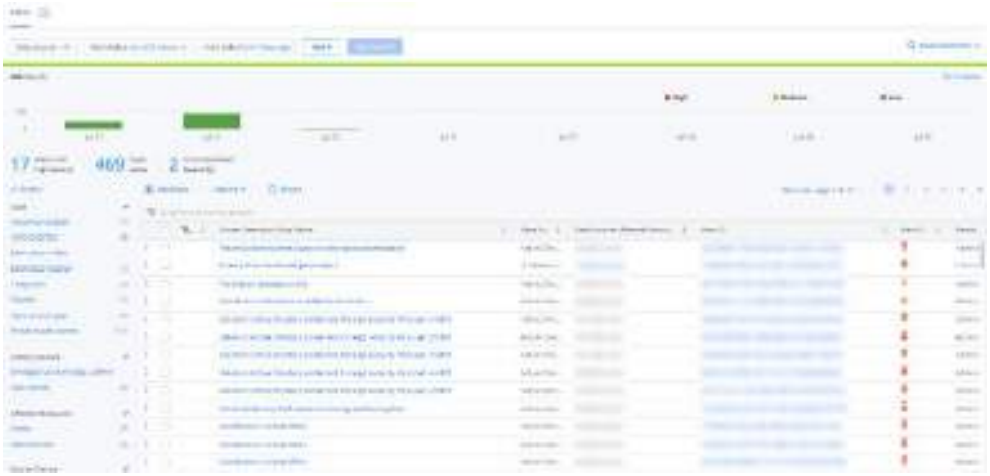
In the Analytics page, you can run an out-of-the-box saved search, or create and run your own search query on specified data sources in your environment.

To configure and run your own search query:

1. In the Varonis Web Interface, select Analytics, and then select the entity (Events, Alerts, Permissions, Accounts and Memberships, or Resources) on which you want to run your search query.
2. Select the values for the default filters of the entity you selected. The default filters vary according to the entity tab you have selected. For example, the Alerts entity includes filters for data sources, alert status, and time range.

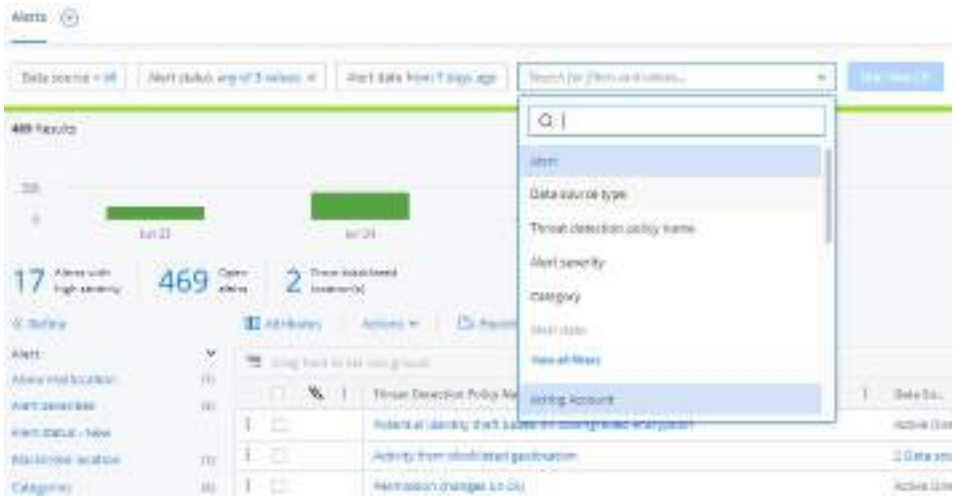


Your preliminary results are displayed.



3. To add additional filters for refining your preliminary search results, do the following:
   a. Click the Add + button.
      A filter search box opens displaying below it a list of available filters organized under filter categories. The listed filters and their categories vary according to the entity tab you have selected. Select a filter or use the search box to look for

your required filters or values.



Note: When you begin to type a word or phrase in the filter search box, auto-complete suggestions for filters and values that contain the typed text are displayed in the area below the search box.

b. If you selected a filter, continue by selecting its required value. You can add additional values to the filter if required.

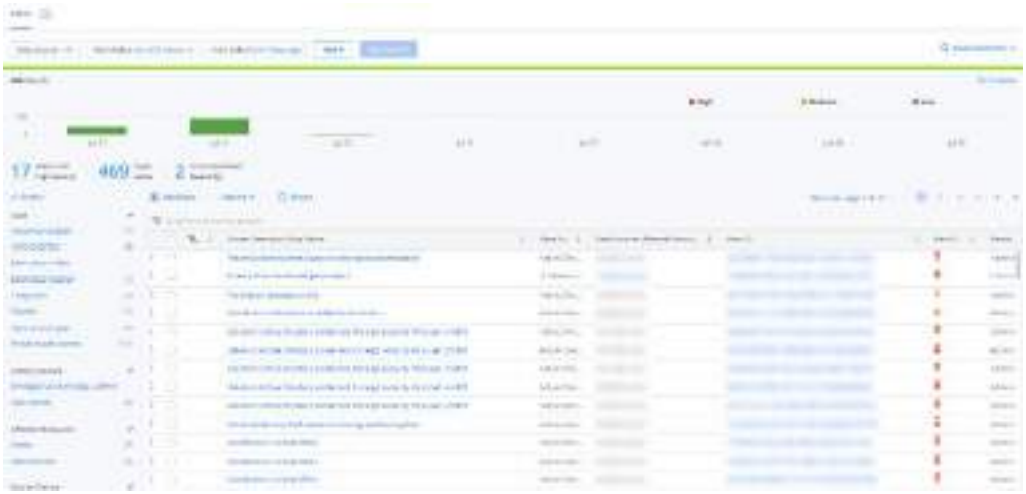


4. When you have finished adding the required filters, click Run Search to run your search query.

Now you can further refine your search results, or save your search for future use.

Refining Your Search

Once you have run your search, your preliminary results will look similar to this:

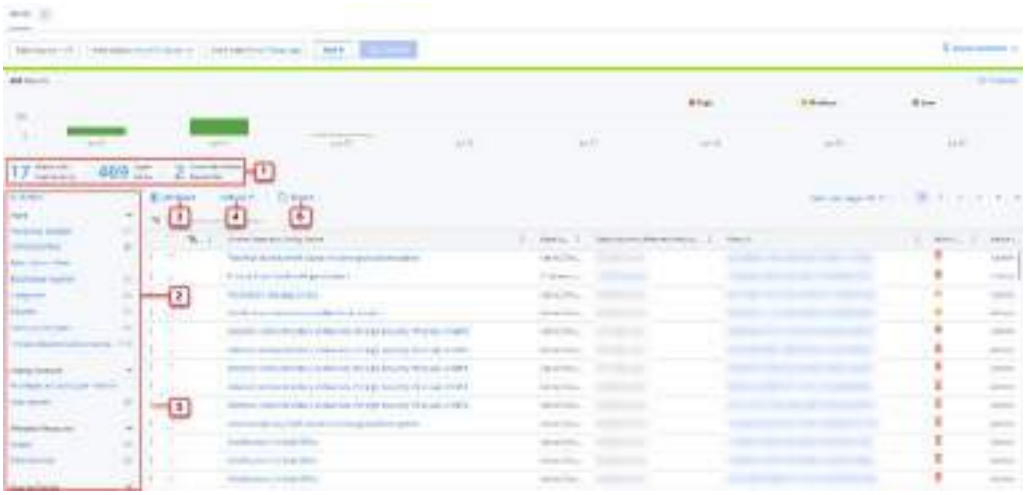


Note: You can add, remove, and change the order of columns in the results tables, and group results by attribute (column).

You can refine your preliminary search results using any of the following tools:

- Insights (1).
- A collapsible Refine pane (2)
- An Attributes button (3)
- An Actions menu (4)
- A More Options ⋮ menu (5)
- An Export button (6)

You can also save your search for future use.



Insights

The insights displayed at the top of the screen (1) show data which enables you to refine your preliminary search results by drawing your attention to important information.

Click the insight to add the insight criteria to your search query.

Refine

The Refine pane (2) presents the number of distinct values retrieved per facet and enables you to refine the scope of your search according to one or more values for a specific facet. Clicking a facet displays the distribution of values in the results of your search.

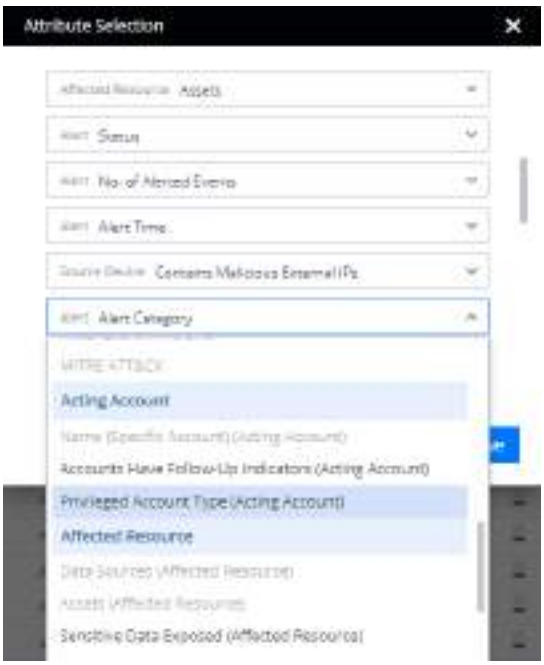
The Refine pane also provides a quick and easy way to drill down and analyze the results per facet. For example, you can select the User name facet in the Refine pane to view information about the users who performed the events which triggered the alert. You can also view the number and percentage of alerts generated per user.

Attributes

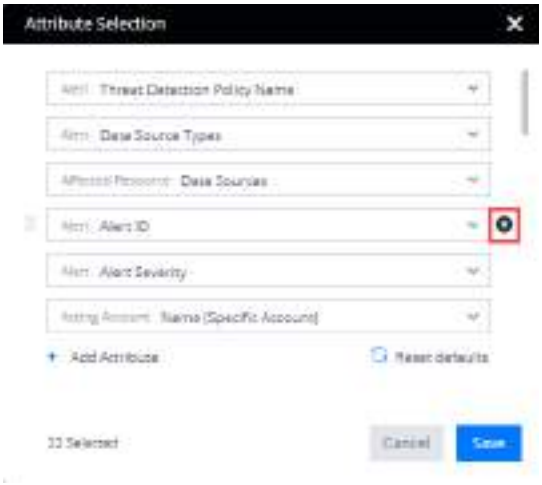
Click the Attributes button (3) to open the Attribute Selection dialog box that shows the attributes currently used as columns in the results grid.



To add an attribute (column) to the grid, click + Add Attribute and in the search box that opens, select or search for the required attribute.



To remove an attribute from the grid, hover over it and click the icon.



Click Reset defaults to reset the Attribute Selection dialog box and results grid to their default attribute list.

List View

When you search for events in the Analytics page's Events tab, you can view the complete set of results as a list view. This view provides the option to show all attributes with populated data, and use these additional data to fine-tune your analytics.

To view all data available for an event, go to the search results and switch the view from the default Table View to List View:



- By default, the list shows the same attributes that were displayed as table columns, separated by the "|" delimiter (this is the Show Less option).



- Click Show All to show the complete list of available, populated attributes: A horizontal divider is displayed, followed by all other available attributes that have values (attributes with no values are excluded).

To add relevant attributes to your analytics display, click Show All and then click the attribute value and choose one of these options:

- Click Add to search to include this attribute as a filter with a specific value in your query.
- Click Add column to add this attribute as a column in the search results, showing all available values (without adding it as a filter).

Actions

The Actions dropdown list (4) allows you to jump to the related alerts, events, accounts, permissions, or resources (depending on the tab that is currently active). The relevant page opens and the search query is automatically updated, enabling you to easily see your data in a wider context for further investigation and pivot between entities.

You can select multiple table rows and run an action on all of them at the same time, or use the more options button to run an action on a single table row.

More Options

Select a single table row and click the more options button ⋮ (5) to display options for running an action on the selected table entry, such as opening context cards and managing ownership (available in the Resources and Access Intelligence tabs).

Export

You can export your search results as a CSV, Excel or PDF file, by clicking the Export button (6).

> Note: When exporting data (as a CSV, Excel or PDF file), the maximum number of results is limited to 50,000 (Results that exceed the limit are not included in the exported file).

Resource Side Pane

The Analytics page features a resource path side pane, containing important data available for a selected resource throughout the Varonis system. Use this pane to easily view all resource information at a glance, detect risks, and drill down to perform your investigations.

To launch the resource side pane:

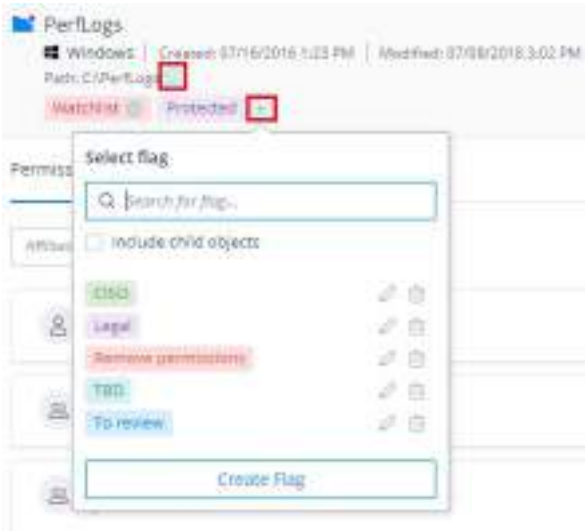
If your search results include resource paths, you can click the path of a specific resource of interest to launch its side pane.

Resource side pane actions

The side pane includes a header with brief metadata about the resource (such as its name, tags, and so on), as well as commonly used actions:

- Copy path - Click the copy icon (at the end of the path) to copy and paste the path either inside the Varonis system or into your external applications.
- Manage flags - Click the plus icon (at the end of the attached flags list) to create, edit or delete flags. Attach flags to a resource to mark it with your own insights, and then filter or group search results by their flags.

  > Note: In addition to these custom, user-defined flags, there are system flags that are managed by Varonis and automatically detect important insights (for example: Whether this resource is stale, protected, unique etc.).

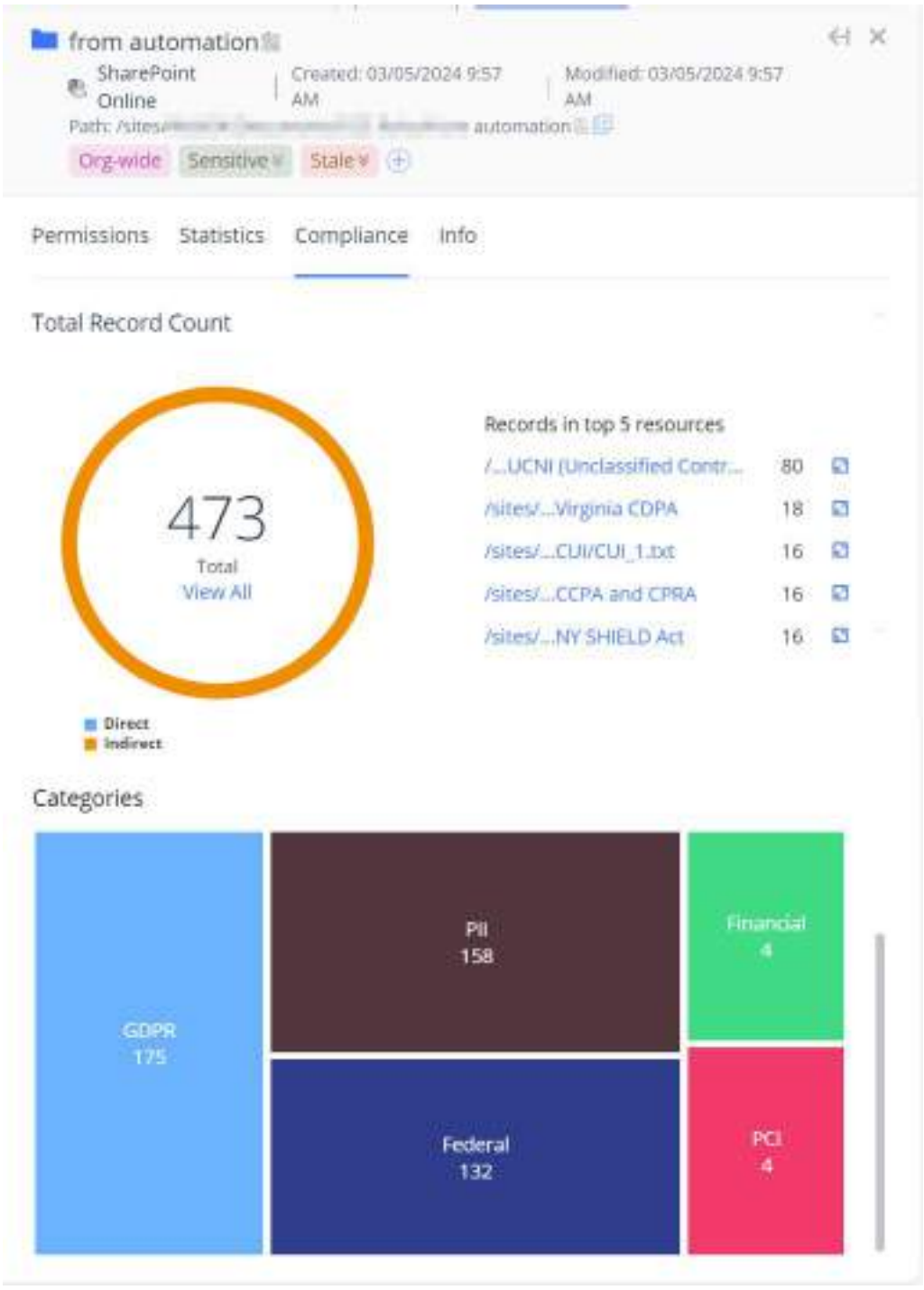


Resource side pane tabs

The resource data is presented in the following tabs (the available tabs depend on the available information):

- Permissions - All the permissions on the resource
- Statistics - An aggregated view of the accounts with the most events on the selected resource
- Compliance - An overview of all the classified data on the resource and its subfolders
- Info - All the metadata for the resource, a notes component, and a list of owners.

The following image shows an example side pane of an example resource, displaying its Compliance tab.



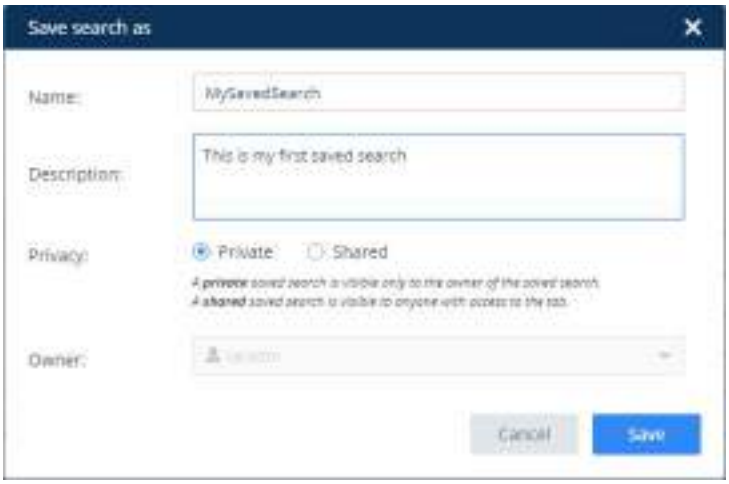
Saving Your Searches

After running a search query, you can save it for future use, as follows:

1. From the Saved searches menu in the top-right corner of the screen, select Save search as.

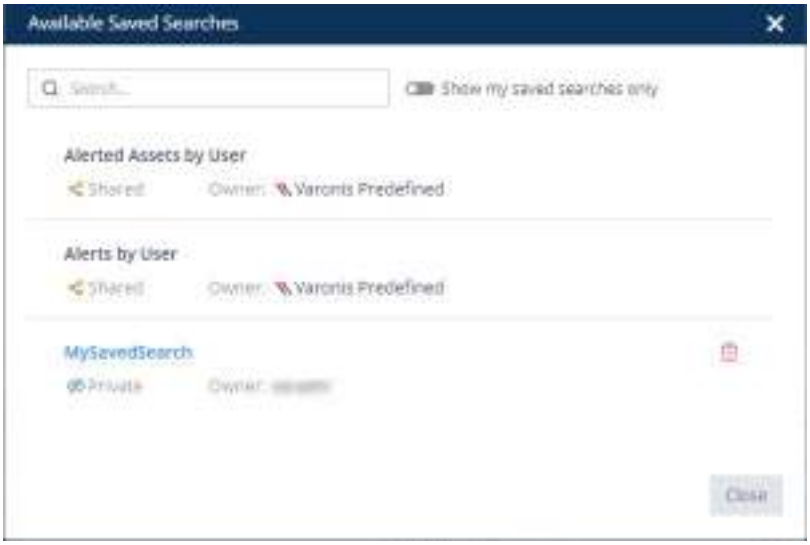


2. In the Save search as dialog box, type a name and an optional description for the search.



3. Select a Privacy option for the saved search.
   Your Private saved searches are available only to you. Shared saved searches are available to anyone who has access to the entity tab in which you saved the search.
4. Click Save.

Your saved search is added to the list of available searches in the Available Saved Searches dialog box for future use.



To access this list, from the Saved searches menu, select Available searches.



You can also perform multiple actions on your saved search at any time.

Working With Saved Searches

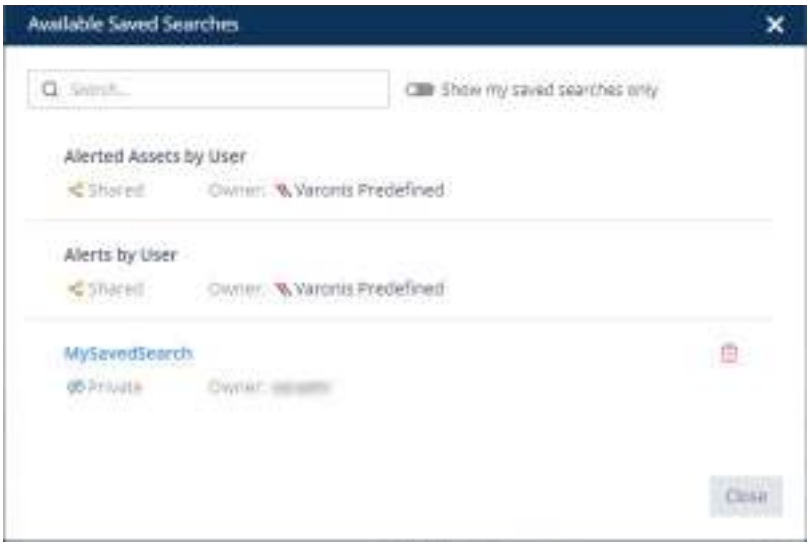
A good way to start searching is to use one of the saved searches that the Varonis Web Interface provides out-of-the-box, each representing valuable use cases such as Enabled but Stale Users or Non-Org Users.

To access the list of saved searches:

1. In the Analytics tab of the Varonis Web Interface, from the Saved searches menu in the top-right corner of the screen, select Available searches.



The Available Saved Searches dialog box for the selected entity tab is displayed.



Note: The list of visible saved searches depends on the entity tab you have selected so make sure you are in the correct tab.

2. You can now perform any of the following actions.
   - Search for a saved search by name or description.
   - Display only your own saved searches.
   - Run a saved search by clicking its row.
   - Delete any of your own saved searches by hovering over its row and clicking its Delete icon.

Analyzing Data Classification Results Of A File

You can display the contents of a file that has classification results and analyze the text that matched a specified rule.

Keep the following in mind:

- File content is not stored in the Varonis database.
- The query is performed in real time so it may take a few minutes to complete.
- You cannot analyze more than five files at the same time.
- The Document Text pane will not display the text for documents that contain more than 5,000 records.
- The results displayed in the File Information screen may differ from those displayed in the Access Intelligence screen if the file has been modified, or a dictionary used by the classification rule has been changed.

To analyze classification results of a file:

1. In the Varonis Web Interface, in Analytics, click the plus sign ⊕, and select Access Intelligence.

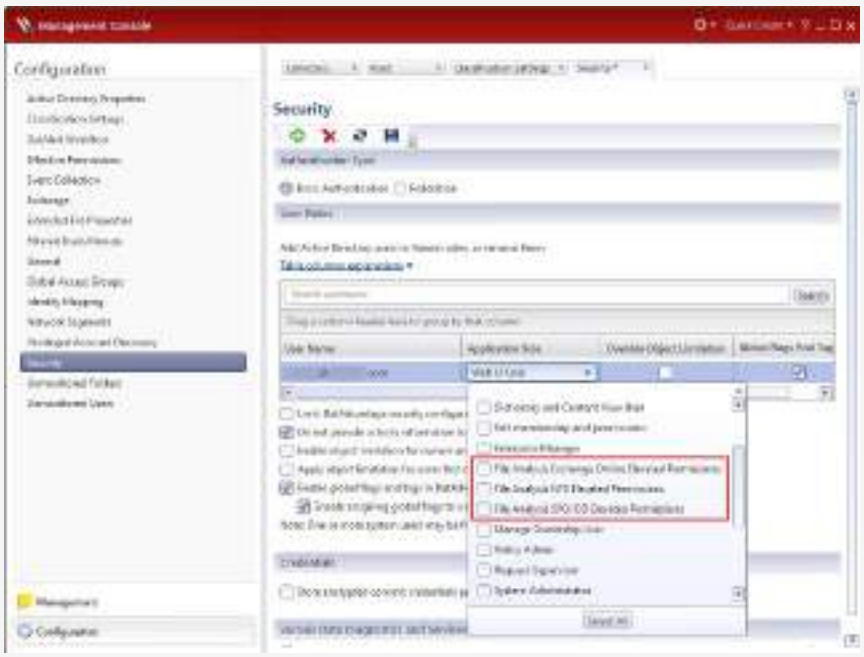
   Note: Alternatively, click the plus sign ⊕, and select Resources.

2. Browse to the file you want to analyze, and from the options menu, select Analyze file.
   A login dialog box is displayed to ensure only authorized users can view the classification analysis.
3. In the Login dialog box, enter the required credentials.

   Note:

   - To perform analysis with user credentials:
     - For SharePoint Online and OneDrive, you should also grant Global Administrator consent to the Varonis DCE application in Microsoft Azure. To do so, go to the Configuration tab of the relevant data source in the Management Console.
     - For CIFS, you should also grant share permissions and directory permissions for the required file.
     - For NFS and Exchange Online, you cannot perform file analysis with user credentials.
   - To perform analysis without user credentials:
     - For Exchange Online items, you should have the File Analysis Exchange Online Elevated Permissions role.
     - For NFS documents, you should have the File Analysis NFS Elevated Permissions role.
     - For SharePoint Online and OneDrive documents, you should have the File Analysis SPO/OD Elevated Permissions role.

Note: To add the role to the user, in the Management Console, go to Configuration > Security.



File analysis starts running. When the analysis is completed, the results are displayed in the File Information screen.



(1) Rule name and its number of total records on the rule level.

(2) Rule categories

(3) Rule conditions and their number of records and matches.

A match is considered per every condition (there can be multiple matches per condition).

A record indication could be based on a set of conditions that generate a match.

For example, only if condition Data Security Platform and condition Varonis pattern, have a match, it indicates a record. So for each condition we have the number of matches it generated, and how many records it contributed.

The left pane displays the classification rules that were matched, their conditions, and their categories. The right pane, named Document Text, displays the text of the document, with the results underlined in the color of each of the conditions they matched, and the condition names displayed below them. The rule names are displayed above the results.

Note: Each type of condition (string, pattern, dictionary and so on) is associated with a different color.



When analyzing files that contain tables, table rows are displayed in a single line (limited by the width of the text pane) and a double pipe || separator is placed between table cells so that table columns are easier to follow.



4. To show records and matches of a specific rule including all its conditions, in the left pane, select the rule's checkbox and clear the rest of the rules' checkboxes.
5. To show records and matches of specific rule conditions:
   a. In the left pane, expand the rule name to view its conditions.
   b. Select the checkboxes of the conditions whose results you want to view in the Document Text pane.
6. Use the Next and Previous buttons to jump from one record or match to another, depending on the option selected in the show only records checkbox.
7. To view only records in the Document Text pane, select the Show only records checkbox. If you clear the checkbox, the results will show both records and matches.
8. To view the Document Text pane across the screen and hide the left pane, click Hide Rules.

5 VARONIS MANAGED DATA DETECTION AND RESPONSE (MDDR)

Important: To get your MDDR license, contact your Sales Engineer.

Varonis Managed Data Detection and Response (MDDR) is the world's first managed service for monitoring and protecting critical data with a 24x7x365 SLA. MDDR combines Varonis' industry-leading threat detection technology with a world-class team of elite threat hunters, forensics analysts, and incident responders. Our team triages, investigates, and responds to every Varonis alert, so you don't have to.

How MDDR Works

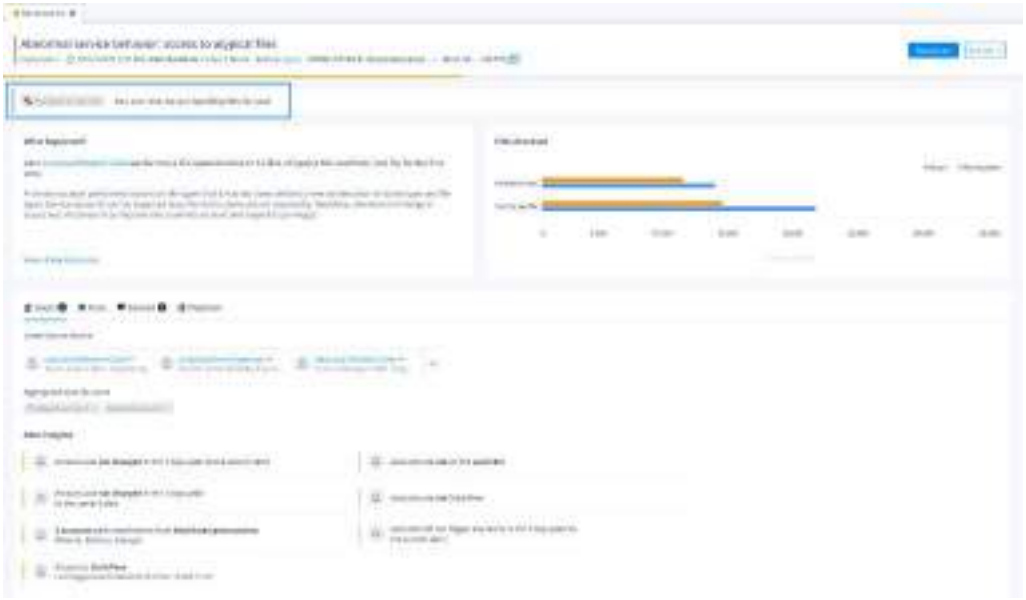
- Threat Detection - Varonis detects anomalous behavior and triggers an alert.
- Automated analysis - Varonis runs additional automatic analysis on an alert.
- MDDR Expert Analysts - Varonis expert investigates and responds to the alert and reports findings to keep you in the loop.
- Action and Next Steps - Varonis mitigates the threat, resolves the alert, and escalates it to you only when needed.

MDDR SLA

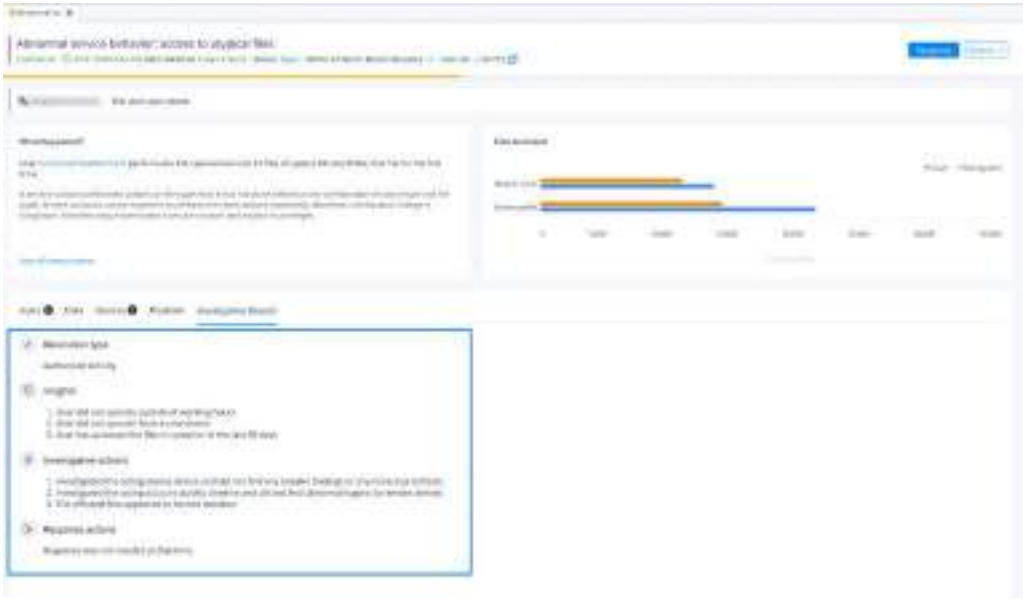
Varonis MDDR offers a 30-minute response for ransomware attacks and a 120-minute response for all other alerts.

User Experience

Clear indication of alerts managed by Varonis:



Detailed investigation analysis:

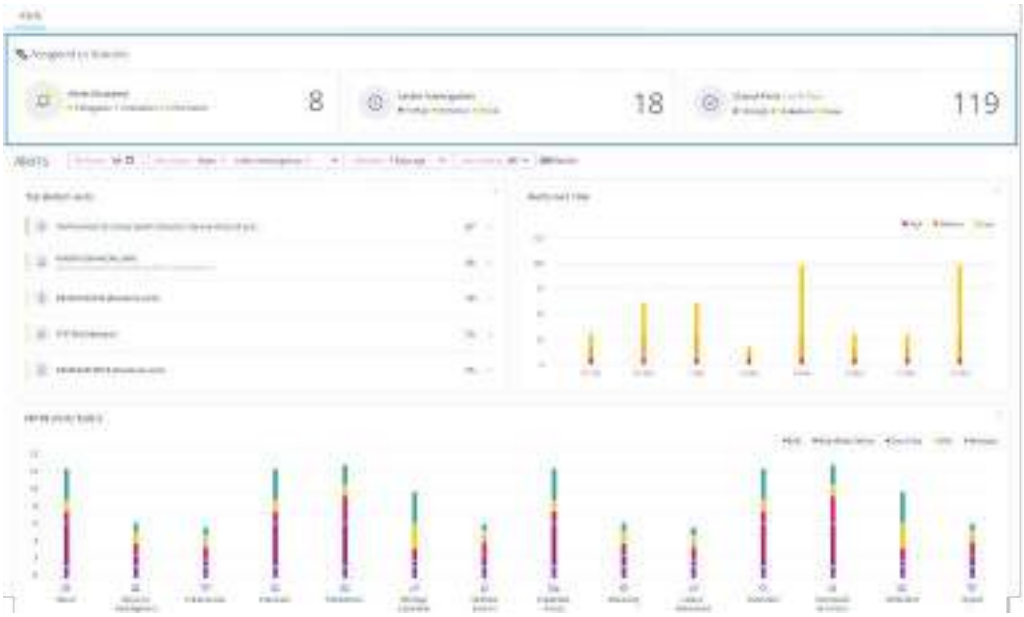


New columns in Alerts analytics - Is the alert assigned to Varonis ( ) and Closed By:



You can now see who closed the alert, whether Varonis, your SOC team member, or a third-party vendor that you use to close the alert from within the integration app using an API Key (preconfigured in the API Keys page in the Varonis Web Interface).

New MDDR widgets in Alerts Dashboard:



- Alerts Escalated – Quick view into alerts that need your attention for mitigation or additional investigation. This is only for awareness; Varonis will reach out to you as needed.
- Under Investigation – Snapshot of alerts currently being investigated by Varonis.
- Closed Alerts – Alerts that Varonis MDDR handled and closed in the past 90 days.

MDDR Dashboard

Use the MDDR dashboard to review and track important MDDR performance metrics.

The dashboard includes the following metrics:

- Number of alerts MDDR closed on your behalf

- Number of confirmed threats (True Positive alerts)
- Time saved for you by MDDR
- Median time to start and complete alert investigations



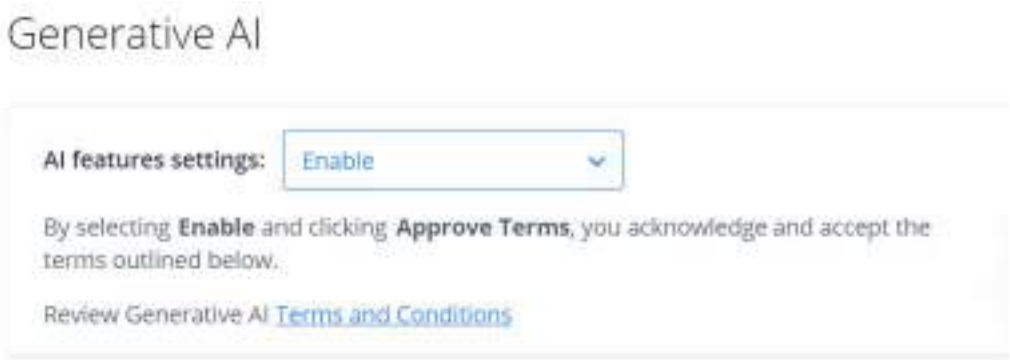
6

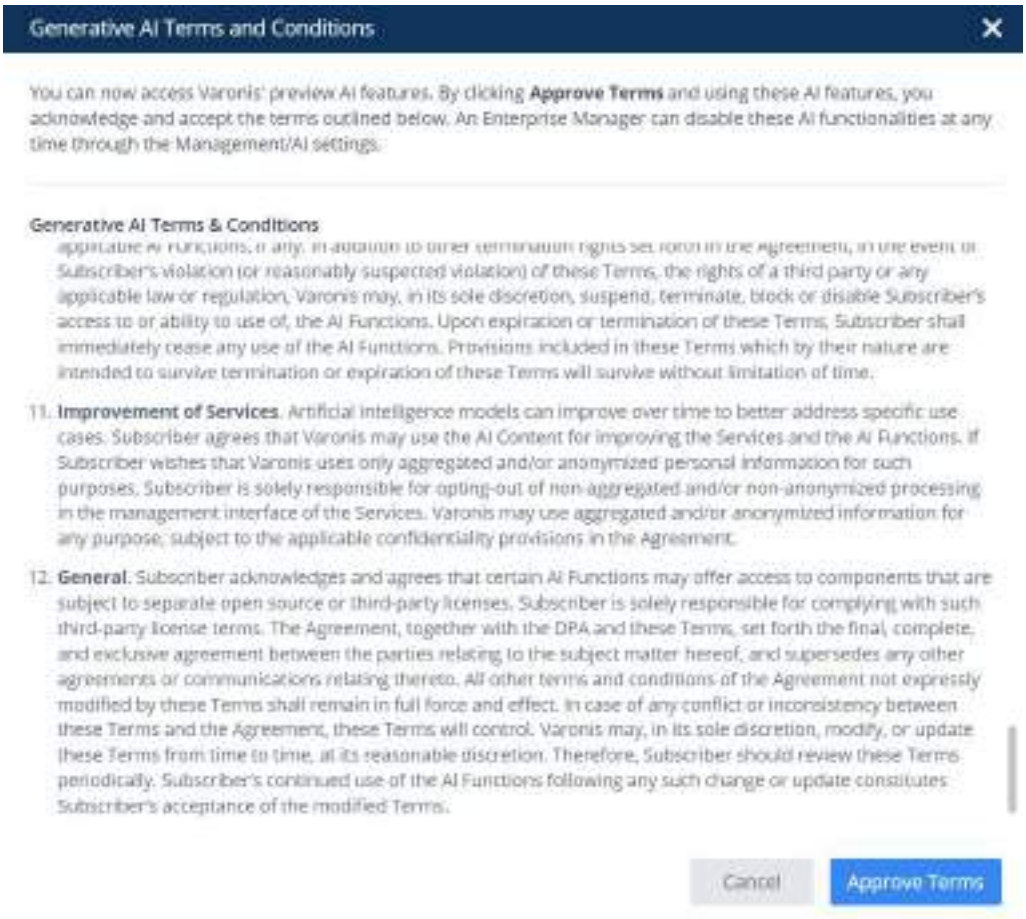
Enabling Athena AI

Important:
Varonis uses public LLM models that are provided via Azure OpenAI platform. We have a written contract with Microsoft, which ensures they are compliant with our security policies and are not retaining our customer data or using it to train models. For more details on data, privacy, and security for Azure OpenAI Service, see the "Important" note in this article.

To enable Athena AI in Varonis, you need to agree to the Generative AI Terms and Conditions, available in both the Configuration Center > Settings > Generative AI and through the features (Alert page for AI Assistant SOC and Events and Resources Analytics for Search AI) before initial use.

An Enterprise Manager can opt in or opt out of Athena AI through Configuration Center > Settings > Generative AI at any time.



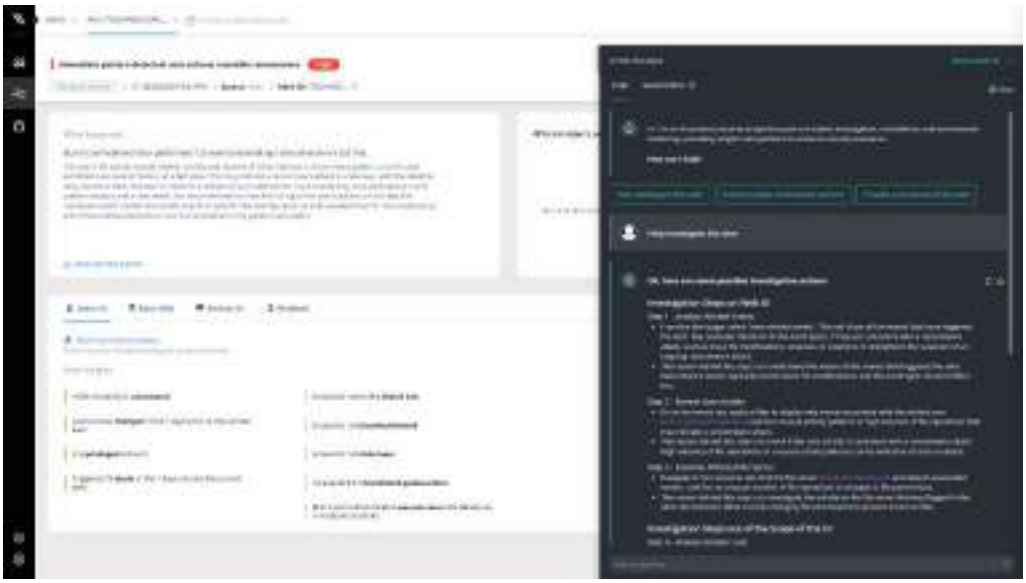


AI SOC Analyst

Varonis' AI-powered SOC assistant utilizes large language models (LLMs) with our unique context about your organization's data, identities, and devices to generate instant, tailored alert response playbooks. You can open the Alert page (for alerts triggered by a Threat Detection policy), click the AI robot icon 

on the right, and use the AI chat pane to ask the AI SOC Analyst to help you investigate and remediate the alert, provide a summary of the alert, or answer your free-text

question.



Advanced features that were added to the AI SOC Analyst:

- Streaming AI results - To improve your user experience and reduce the waiting time for the AI response, we now support streaming, where we serve message parts as soon as the AI model generates them.
- Copy AI chat response - You can copy an AI chat response to the clipboard using the copy icon to the right of the response.

- Extend the list of supported Threat Detection policies - We extended the list of Threat Detection policies supported for the AI SOC Analyst.
- Jump from AI-Assisted SOC to Analytics - To streamline alert investigations using AI-assisted SOC, you can now jump from the AI chat on the Alert page to Analytics, eliminating the need to navigate to a different area of the product and construct a query for your investigation.



Natural Language Search

Enables users of all skill levels to use natural language to quickly retrieve analytics data and resolve the text into query filters.

Events and Resources Analytics support natural language search via the robot icon.



Right after you approve the generative AI legal terms and conditions (see section below for details), a text box is displayed where you can enter free text to be processed by Athena AI. Several examples of free text will be displayed. If you've previously approved terms and conditions, click the robot icon on the Analytics page to open a text box where you can enter free text to be processed by Athena AI.

After clicking Send , the filters successfully resolved by the AI engine will be displayed and will part of the coming search.



7 MANAGEMENT

The Management tab includes the following options:

- Policies - For automatic remediation of risk in your environment.
- Action Center - For viewing and tracking the execution progress of actions generated by your automations. This includes operations waiting for review and approval, operations waiting to be performed, operations currently running, and operations that have completed their run.
- Scheduled Searches - For viewing existing scheduled searches, creating new scheduled searches, and performing actions on single or multiple scheduled searches.
- Flags - For assigning flags that can be used to filter searches or to group results.
- System Health - For viewing up-to-date information about your system's health and monitoring the classification and data labeling coverage in your scanned environment.

Working with Automations

Overview

The Automations tab of the Policies area in the Varonis Web Interface is where you create security automations that scan your environment and provide recommended actions for remediating a variety of issues and reducing risk. Each automation is defined to search for a specific risk and then remediate it.
Varonis provides some out-of-the-box automations, such as the automations listed below. Use any of these automations, or create your own.

- Remove collaboration links that over-expose sensitive data (related to the Collaboration Links by Type widget)
- Remove stale permissions (related to the Stale Permissions widget)
- Remove stale collaboration links (related to the Stale Permissions widget)
- Remove stale memberships in collaboration links (related to the Stale Memberships In Groups widget)

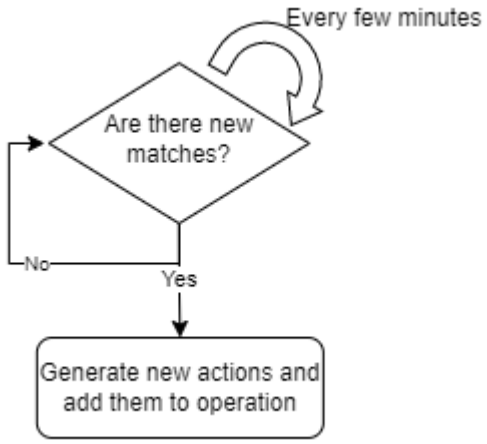
Note:
You can find detailed information about all available automations in the Varonis SaaS Automation Details spreadsheet. To download it, click the paper clip  icon in the top right corner. Then select the Excel file and click Download.

Key Terminology

- Matching process - where actions are created for each permission that meets the automation conditions
- Action - a recommended action, for example, Remove permission
- Operation - a container for multiple actions which are executed together

When an automation is enabled, it starts the matching process. Once it finds a match, an action is created along with an operation that contains this action. As the automation continues to find matches, additional actions are created and added to the

operation.



You can monitor the execution progress of actions created by your automations in the Action Center where actions are listed in six tabs according to their current status. For more information, see Working with the Action Center.

Note: To avoid unnecessary duplication of actions, actions with these statuses will not be recreated in the seven days which follow their execution: Completed, , Completed with Error, and Failed.

Note: Some actions with the Not executed status are not executed because we know in advance that those actions will fail.

Configuring the Learning Period for Automations

The following configuration options control the learning period for automations. You'll find them in the Management Console under Configuration > General:

- Show data in stale permission and stale membership widgets after a learning period of ____ days
  - The default value is 14 days for new installations. For upgrades, the value from the previous version is kept.
  - The system starts calculating data and presents it in stale permission and stale membership widgets in the Varonis Web Interface dashboards after this learning period ends.
- Generate actions for activity-based automations after a learning period of ____ days
  - The default value is 120 days for new installations. For upgrades, the value from the previous version is kept.

- The system starts generating actions for activity-based automations after this learning period ends.

Accessing the Automations Screen

In the relevant widget, click , or from the side menu bar, select Management > Policies > Automations tab. The Automations screen opens, displaying a list of all available automations.

Enabling or Disabling an Automation

To enable or disable an automation, in the list of automations, click the relevant option in the State column of the relevant automation.

You can also enable a new automation while you are creating it so that it starts running as soon as it is created

Creating a New Automation

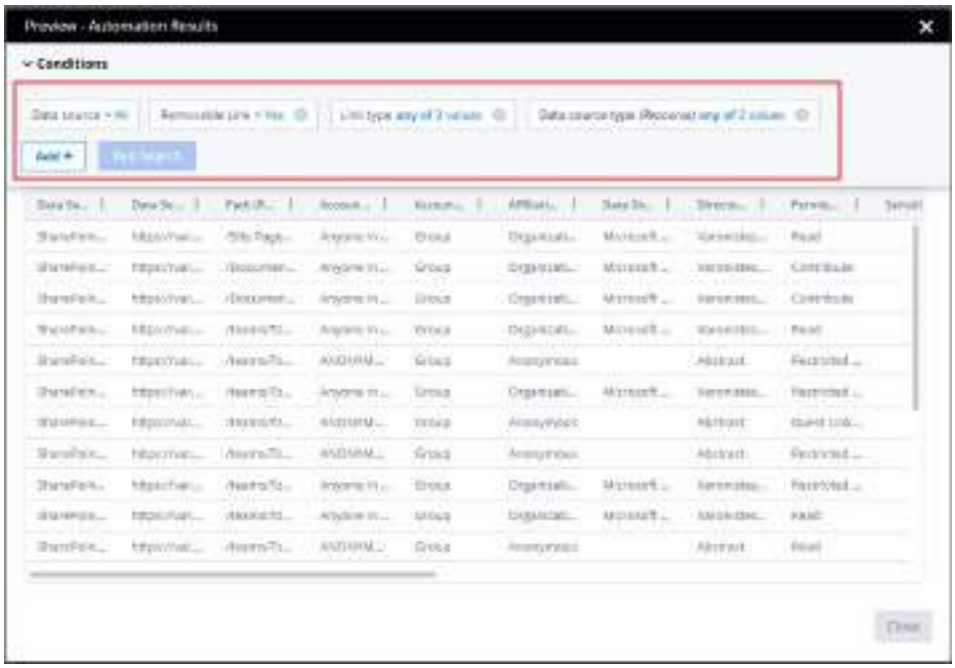
1. Click + New Automation.
2. Set the automation type, and add a name and description.
3. In the State setting, choose whether to enable the automation to run as soon as it is created or keep it disabled for now.
4. In the Conditions area, set the conditions for the automation scope:

   Note: Each automation type might feature predefined conditions which must be a part of the condition set of the automation and cannot be edited or removed.

   a. By default, the automation searches all data sources. To limit the scope to specific data sources, select the required data sources in the Select Servers dialog box, then click Save.

   b. To add additional conditions, click Add Filter, and set the required criteria.

   c. To preview the results based on the defined conditions, click Preview Scope. You can add, remove, and edit filters in the Preview - Automation Results dialog box allowing you to experiment and understand how the filters impact the scope of the remediation. The changes you make in this dialog box are for preview only and will not affect the actual scope.

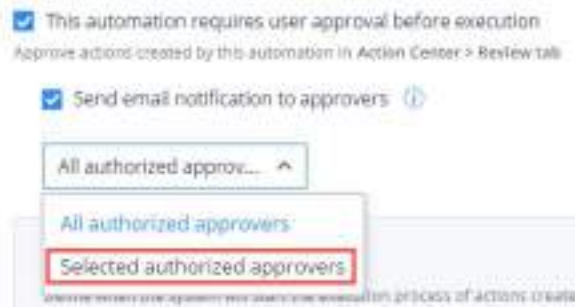


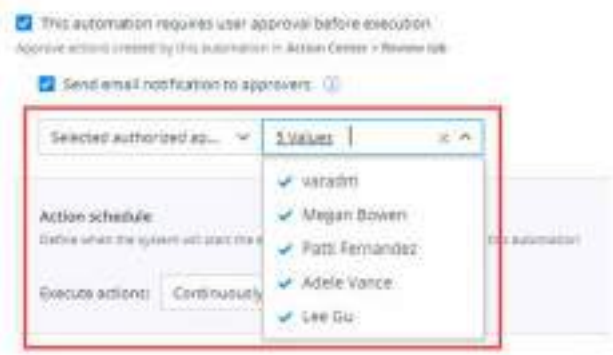
Note: The Preview - Automation Results dialog box may display only some of the results.

5. The Actions area displays the actions that this automation will apply on each of the permissions that met the conditions. It also lets you define whether an approval process is required before actions created by the automation will run, and lets you define a schedule to run the actions generated by the automation, if required.

   Note: These two settings do not affect the automation matching process. They will affect the run of the actions created by the automation.

   a. This automation requires user approval before execution – Select this check box to activate an approval process of the actual results in the Action Center before the actions created by the automation are run. New operations generated by the automation will remain in Pending Review status until they are approved.
   To send an email notification to authorized approvers, select the Send email notification to approvers checkbox. By default, all authorized approvers will receive the notification. To select only specific approvers, in the list of approvers, select Selected authorized approvers, then from the menu that appears on the right, select the names of the approvers that will receive the notification.





Note:
The approvers will receive an email notification with a Review Now button that will take them directly to the Action Center where they can review the operations that require their approval.

Authorized users are users with an Enterprise Manager, Power User, or Commit/Edit user role.

b. Action schedule – Define a schedule for the run of the actions created by the automation or keep the default option to immediately run the actions created by the automation.

6. Click Save.
   The new automation is saved and added to the list of automations on the Automations tab.

Remediate Org-Wide Exposure Automation

The "Remediate org-wide exposure" automation for Windows replaces Global Access Group permissions with permissions for dedicated security groups, which include users who accessed resources via the removed Global Access Group permissions during the defined learning period.

Note:

The "Remediate org-wide exposure" automation remediates protected and unique permissions of Global Access Groups and their inherited permissions. It does not remediate inherited permissions of Global Access Groups if the scope does not include the parent folders in which the permissions were defined.

For more information about org-wide exposure, see Organization-Wide Exposure.

The automation review phase enables you to view the active accounts whose access will be preserved when you execute the automation. To view these accounts, click the action name and in the context card that appears, under Add Members, click the View members link.



The automation review phase also enables you to view active accounts whose access cannot be preserved, if such exist, before you decide to execute the automation. To view these accounts, click the link in the Lost Access column.

Note: The Lost Access column contains data only when there is a user that will lose access as a result of the remediation.



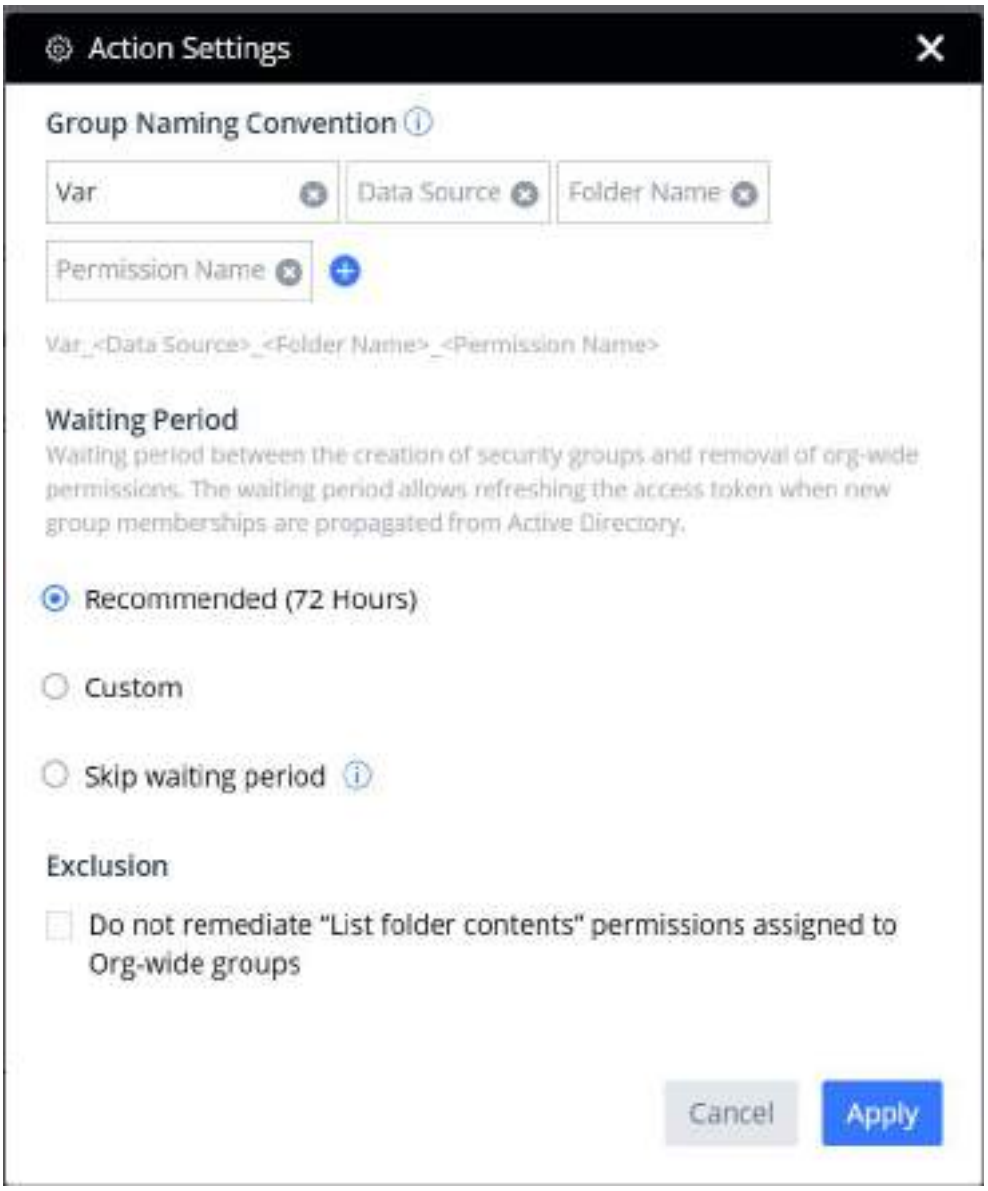
You can also export the actions of a "Remediate org-wide exposure" automation for review outside the Action Center. The resulting Excel file displays detailed information including the new group that is created, the new memberships, the new permission, the accounts that lose access, and which permissions are removed. The Excel file includes separate sheets for each type of information, so that you can view the changes by type:

- Actions
- New Groups
- New Memberships
- New Permissions
- Lost Access
- Removed Org-Wide Permissions

When creating or editing the automation, use the Action Settings dialog box to change the default waiting period between the creation of the replacement security groups in Active Directory and the removal of the org-wide permissions. You can also define a naming convention for the newly created groups, as well as choose to exclude “List folder contents” permissions (applying only to “This folder and subfolders” in the file system) assigned to Org-wide groups from remediation.

To access the Action Settings dialog box, click Manage action settings in the Actions area.





Note: When a new group is created, if a group with this name already exists, a suffix _x will be added to the new group name.

When a group (for example group A) contains a Global Access Group as a member, the automation preserves all members with events on the resource (including such members of the Global Access Group) by adding them to a new group, and group A's permission is removed.

In cases where the remediation involves removing all permissions from a resource, the automation will add a domain administrator permission to that resource.

To prevent token bloat, actions that result in users becoming members in more than 900 groups will be blocked from execution.

If required, you can also change the default organizational unit for the newly created groups in the Commit pane of the required data source in the Management Console.

The automation covers the following twelve groups defined by Varonis as Global Access Groups.

Group	Included Users
Everyone	All users
Dialup	All users who log on through a dial-up connection
Network	All users who log on through a network connection
Batch	All users who log on through a batch queue facility
Interactive	All users who log on interactively
Anonymous	All users who log on anonymously
Authenticated Users	All users whose identities were authenticated when they logged on
Terminal Server User	All users who log on to a Terminal Services server
Remote Interactive Logon	All users who log on through a terminal services logon
This Organization	All users from the same organization
Built-in Users	A built-in group. After the initial installation of the operating system,

Group	Included Users
	the only member is the Authenticated Users group. When a computer joins a domain, the Domain Users group is added to the Users group on the computer.
Domain Users	All user accounts in a domain

Rolling Back Actions of the “Remediate org-wide exposure” Automation

You can roll back completed actions of an operation created by a Remediate org-wide exposure automation. The operation must be in one of the following statuses: Completed, Completed with errors, Stopped, or Partial rollback completed.

Note: Rollback will fail if the groups created by the automation are renamed.

1. In the Action Center, go to the operation you want to roll back.
2. Click the operation name to view its actions.
3. Select the checkboxes of the completed actions you want to roll back.
4. From the Actions menu, select Roll back selected actions.



Remediate Inconsistent Permissions Automation

The “Remediate inconsistent permissions” automation enables system administrators and IT personnel to repair broken permissions quickly and easily in the organization's NTFS file system.
In NTFS file systems, each permission of a folder or a file can be either uniquely defined or inherited from the parent folder. However, if a folder is protected, it does not

inherit permissions from its parent. The permission set for the folder or file includes a flag indicating whether permissions are inherited.

A situation might arise in which the inheritance of a permission can be sometimes broken as a result of moving or copying folders or files from one location to another or due to manual changes of the permission sets.

If you have folders that should be inheriting permissions, but are not, some potentially damaging situations might occur:

- The first issue arises when you intend to grant permissions to an entire folder structure by adding the user or group to the parent folder's permission set. If inheritance is broken, this addition is not propagated to the child folders as it should be. This results in help desk calls from irritated users who can access certain folders but not others, even though you have followed the correct procedure to grant the appropriate permissions.
- The second issue is the reverse. If you intend to revoke permissions by removing a user or group from a parent folder's permission set, the change may not be propagated correctly to folders whose inheritance is broken. This could result in folders that are overly permissive, even after attempts to repair the permissions have been made.
- The Varonis Commit engine does not allow performing commit on folders with broken permissions - otherwise some users may lose their legitimate permissions.

The "Remediate inconsistent permissions" automation ensures that permissions are applied correctly on all folders and files which reside under the defined folders by making sure that permissions are ordered correctly, propagated to inheriting child folders, and structured according to the NFS specifications.

Note: Remediation of inconsistent permissions cannot be performed on a mount point and on any folders under a mount point. However, if the starting point of the scope is set to a folder underneath a mount point (does not include the mount point itself), remediation of inconsistent permissions can be performed on the folder and its subfolders.

The following table lists the inconsistent permissions types and their accompanying remediation:

Type #	Inconsistent Permission Types	Risk	After Repair by the Remediate Inconsistent Permissions Automation
1	The permissions in the permission set are not in the correct order, that is,. allow permissions are before deny.	The user that should have deny permissions will instead have allow permissions.	The permission set will be reordered correctly.
2	A permission on the parent folder is not inherited by one or more of its child folders.	The user that should have access permissions to the child folders will not have them.	The permission will be correctly propagated from the parent folder to all inheriting child folders and files.
3	The permissions of the creator owner are not inherited by the child folder.	• The owner of the child folder or file will not have permissions for it. • Creators of new child folders will not be granted with permissions for it.	The permissions will be correctly propagated from the parent folder to the child folder, and a dedicated permission will be created for the owner of the child folder or file.
4	The permissions of the owner of the child folder or file are missing.	The owner of the child folder or file will not have permissions for it.	The permissions of the owner of the child folder or file will be added.
5	A generic access right permission is	Users will not have the intended	The permission derived from the generic access right

Type #	Inconsistent Permission Types	Risk	After Repair by the Remediate Inconsistent Permissions Automation
	not correctly applied on the folder or file.	permissions on the folder or file.	will be correctly applied on the folder or file.
6	A permission exists on a child folder that is inherited from an unknown parent (orphan permission).	Any manual change to the folder's permission set will remove the orphan permission by default and may cause users to lose legitimate permissions.	Will be fixed based on the method selected in the repairing rule; the permission will be either removed according to Microsoft's best practices or preserved as a unique permission.

You can export the actions of a “Remediate inconsistent permissions” automation for review outside the Action Center. The resulting Excel file displays detailed information about each action, such as: Description, Data Source, Path, Exposure Level, Sensitive, Status, Status Details and Execution Results.

Threat Detection Policies

Threat detection policies provide you with the ability to customize configurations that will generate alerts and run automated responses to remediate threats.

In the Threat Detection policies page, you can view and manage your threat detection policies. For information about the required threat detection user roles, see Varonis Security Roles.

1. Navigate to Management > Policies > Threat Detection.
   The main Threat Detection policies page is displayed, where you can view a full list of your policies, and filter to view specific policies. It includes the following:
   - MITRE ATT&CK - Varonis out-of-the-box policies are all mapped to the MITRE framework reflecting the Tactics and Techniques per policy.

- Policy platforms - Only the installed platforms for the threat detection policies are displayed on the main Threat Detection policies page. You can view policy supported platforms (that are not yet installed) by opening the policy (as described below).
- Severity color - Each policy is marked with colored severity indicators (colored lines on the left of each policy).



2. Click a policy to drill down to view its details displayed in a side pane on the right. It contains a header area and several tabs where you can view policy details and perform related actions, as described in the following steps.
3. In the Header area, view the following information:
   - Policy Info - Policy name, severity, creator, category, last modified date
   - Enable/Disable Policy Toggle
   - Actions - Policy actions (including View policy alerts in Alerts Analytics)
   - MITRE ATT&CK - For out-of-the-box Varonis threat detection policies, you can see both the Tactics and Techniques to which the selected policy is mapped.

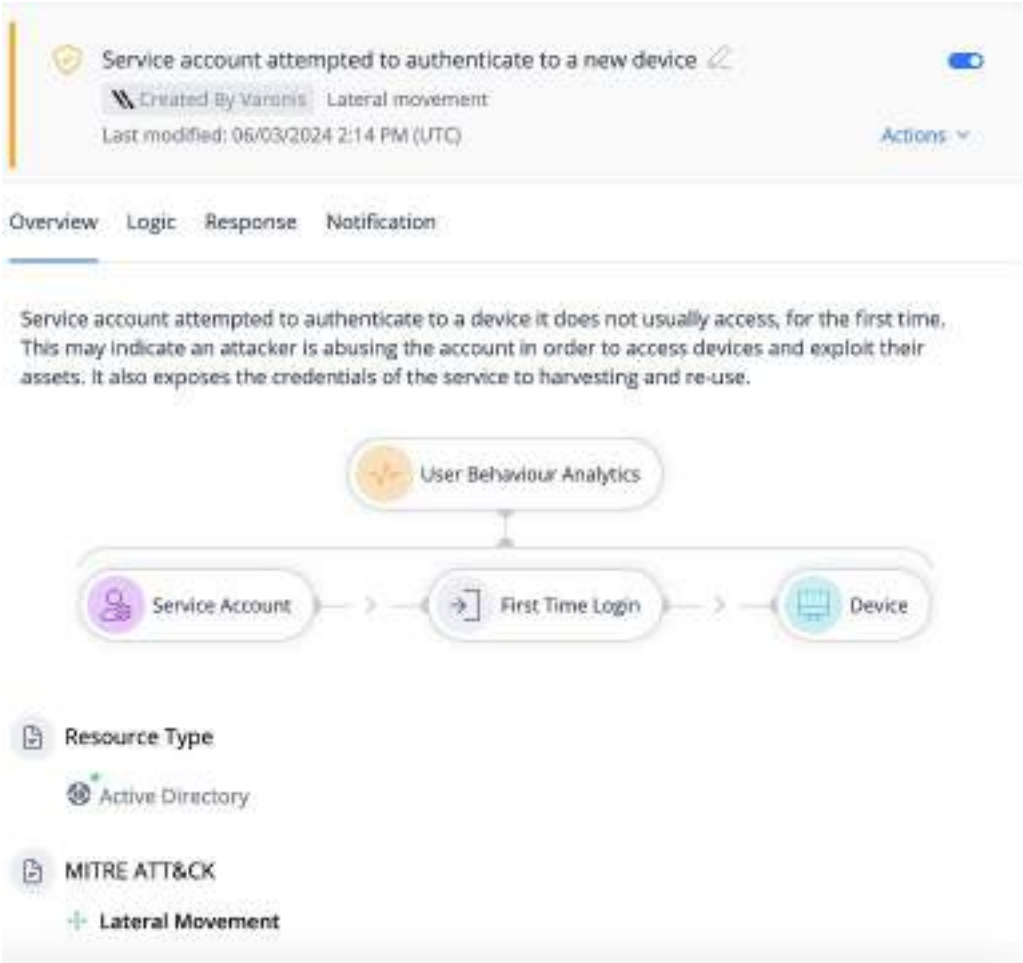
> Note: For user-defined polices, you can edit the policy header sections by clicking Edit (pencil icon) next to the policy name.



Overview - Policy Information

In the Overview tab, view policy information including:

- Policy Description
- Resource Type/Platforms - Installed platforms are marked with a green "Status online" icon (see Windows example below), supported (but not installed) platforms will appear after the installed platforms.


Service account attempted to authenticate to a new device
Created By Varonis
Lateral movement
Last modified: 06/03/2024 2:14 PM (UTC)
Actions
Overview
Logic
Response
Notification
Service account attempted to authenticate to a device it does not usually access, for the first time. This may indicate an attacker is abusing the account in order to access devices and exploit their assets. It also exposes the credentials of the service to harvesting and re-use.
User Behaviour Analytics
Service Account
First Time Login
Device
Resource Type
Active Directory
MITRE ATT&CK
Lateral Movement

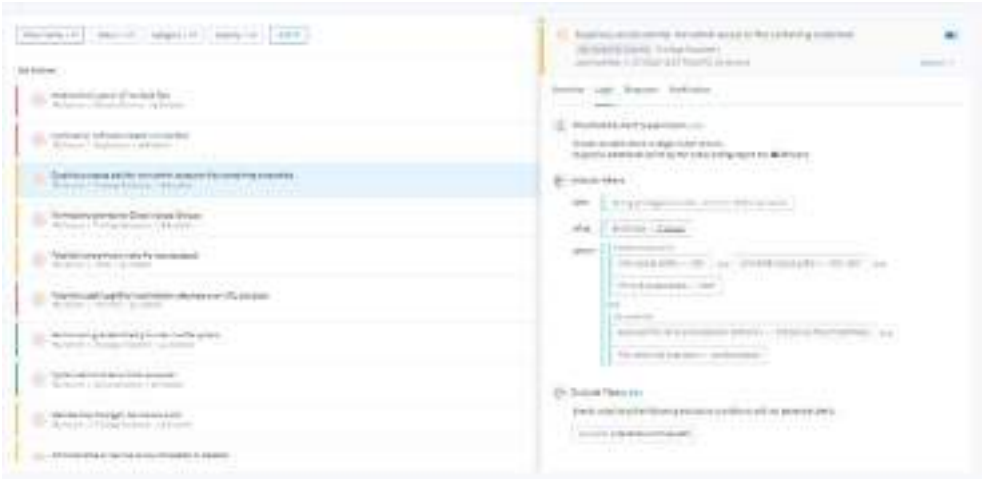
Logic Settings

In the Logic tab, view and set the following:

- Threshold and Suppression - Policies that support these settings allow you to view/edit directly from this section.
- Include Filters - Displays the policy filters (for non-behavioral policies) in the relevant scopes (Who, What, Where, When). This filter view displays the All of and Any of groups in the relevant colors (green or blue) to clarify which filters belong to which group, and the operators between these groups.

  Note: Coming soon - This release of threat detection policies in the Varonis Web Interface doesn't support the ability to edit policy filters. This capability will be supported as part of the following releases. In the meantime, you can still use the Rule Editor for such changes.

- Exclude Filters - Enable viewing/editing the policy exclusion conditions.



Response Script Settings

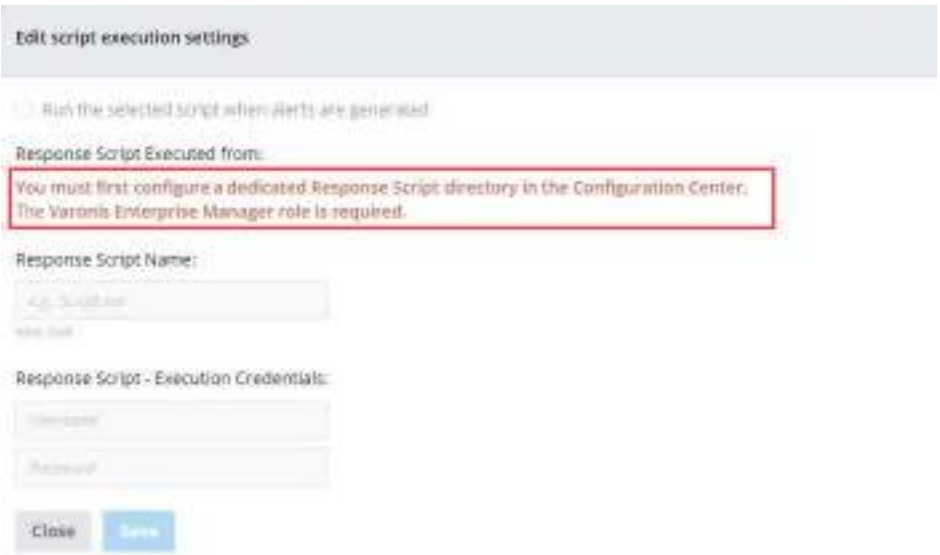
To edit response script settings:

> Note: The Edit option is only available for Varonis users with the Threat Detection and Response Administrator role.

1. In the Response tab, click Edit next to Script execution.



2. If this is the first time you're configuring script execution from the Varonis Web Interface, the Edit script settings pane will display a message prompting you to configure a dedicated Response Script directory.



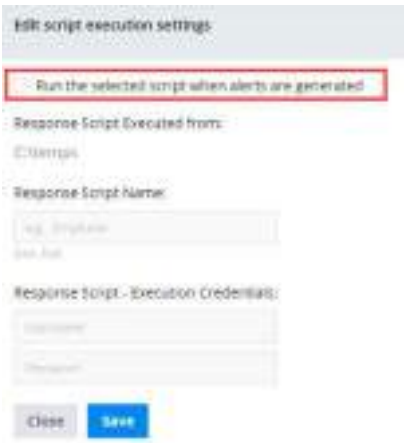
The Response Script directory stores all the scripts used for Varonis threat detection policy script execution, either locally or on a shared drive. It serves as a script execution repository and need only be configured once since it applies to all threat detection policies. Once configured, you'll only need to specify the name of the script from the dedicated directory for each policy for which you want to configure script execution.

> Note: Only users with the Varonis Enterprise Manager role (most elevated role) can configure a dedicated directory for script execution location.

To configure the dedicated directory for script execution, navigate to Configurations > > Settings > Response Script > Response Script directory. For more information, see Response Scripts.

Once you set the path for your Response Script directory, you can navigate back to the Threat Detection policies page to configure the script execution settings for a selected policy.

3. If you do not have a response script configured for the selected policy, or if you have a response script configured for this policy from the Management Console Rule Editor, do the following:
   a. Select Run the selected script when alerts are generated.



   b. Enter the Response Script Name (including the file extension) of the script you wish to execute, which is located inside the dedicated directory (for example, "Script.exe").
   c. Enter the Response Script - Execution Credentials that will be used to execute the script.
   d. When done, click Save to save the response script configurations.

> Important:

- Only the .exe and .bat extensions are supported from the Varonis Web Interface. If you want to execute a PowerShell script (with or without parameters), you can insert the PowerShell execution command into a ".bat" file.
- Policies for which the script execution configuration were configured in the Management Console Rule Editor will continue to run from the path configured in the Management Console Rule Editor. The dedicated directory configuration only applies to policies where the response script execution was configured from the Varonis Web Interface.
- After the response script executions are saved for a policy, you'll need to reenter the execution credentials if you want to modify the name of the execution script.
- Execution configurations set from the Management Console Rule Editor will not be displayed in the Script execution settings pane.
- The script execution settings in the Management Console Rule Editor are displayed in view-only mode. Any attempt to click them will generate a popup message explaining that they're configurable in the Varonis Web Interface.
- If the UNC/network path (\HOSTNAME\ScriptFolder) is used when configuring the script folder location, the local SYSTEM account must have Full Control permissions at the share level (not NTFS).

To automatically resolve policy alerts:

In the Autoresolve area of the Response tab, select Mark alert as autoresolved. When selected, all policy alerts will be created in Autoresolved status.

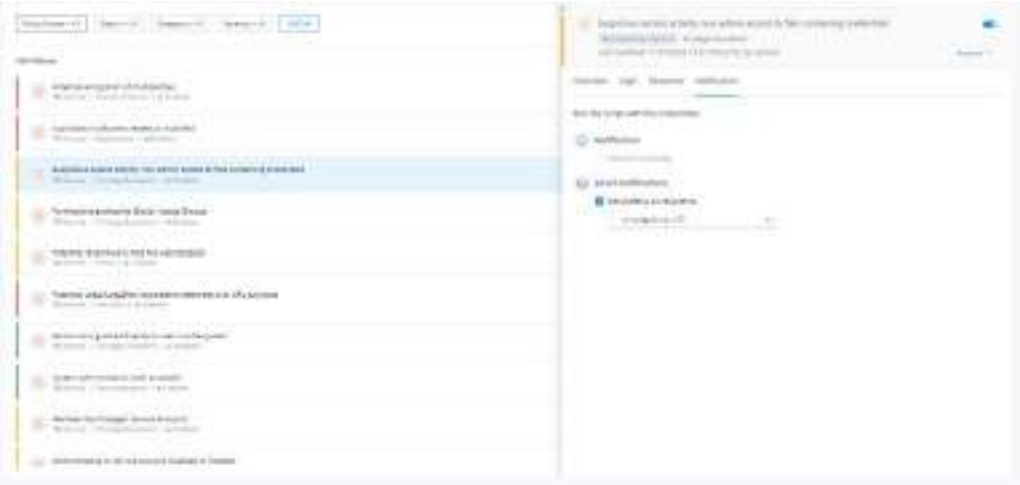
Note: This setting replaces the Display Alert in the UI option which was previously available in the Management Console Rule Editor (policies which previously had the Display Alert in the UI option unselected in the Management Console Rule Editor have been automatically configured with Autoresolve).

Notification Settings

In the Notification tab, view and set the following:

- Publish via Syslog - If a Syslog server is configured, you can select this option to have the policy alerts sent to your Syslog server.

- Email Notifications - You can view and edit the list of email recipients for alert notifications.



Note: Syslog server configurations and alert templates are not yet accessible in the Varonis Web Interface. You can still access these configurations via the Management Console.

Data Discovery Policies

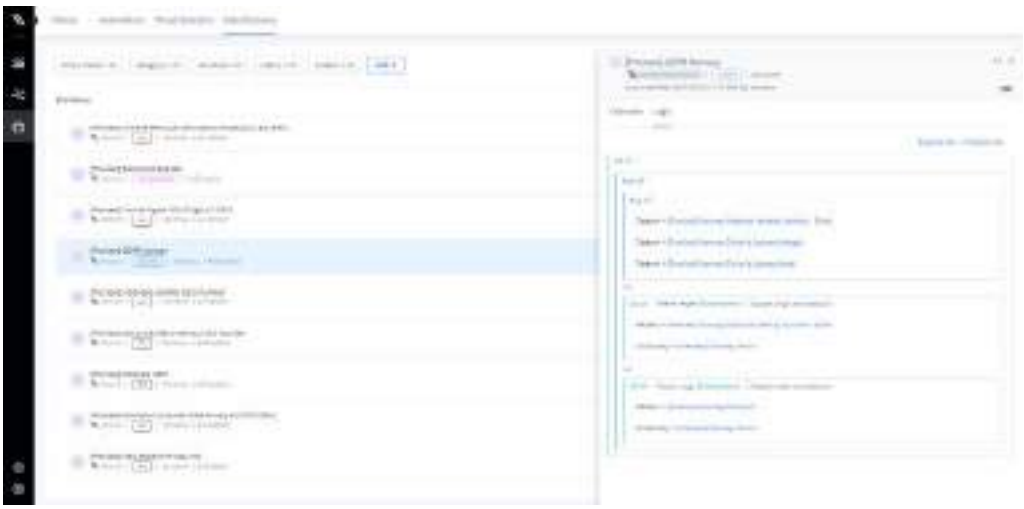
Data discovery policies (previously known as classification rules) are now available in the Varonis Web Interface in Management > Policies, on the Data Discovery tab.

You can view the full list of policies or filter the list to view specific policies.



When you click a policy, a pane opens on the right side, where you can view detailed information about the policy on the Overview tab, view the full structure of the policy including the defined conditions and filters on the Logic tab, and enable or disable the

policy based on your needs.



Note: To access the Data Discovery tab, you must have the relevant Varonis Web Interface roles: Policy Admin and Web UI User, and one of the following roles:

- Classification Configuration Edit User
- Enterprise Manager
- Configuration User
- System Administrator

Enabling or Disabling a Data Discovery Policy

1. In Management > Policies, select the Data Discovery tab.
2. Click the row of the policy you want to enable or disable.
3. In the side pane that opens on the right side, click the toggle.



Actions Initiating a Discovery Scan

The following list summarizes actions that will or will not initiate a discovery scan.

Note: As data discovery policies (previously known as classification rules) are in the process of being migrated from the Management Console to the Varonis Web Interface, the table below refers to a policy when describing actions performed in the Varonis Web Interface and refers to a rule (policy) when describing actions performed in the Management Console.

Action	Initiates a discovery scan?
Installing a new DCE VIP	No
Enabling a policy	Yes, for the scope of that policy
Disabling a policy	No
Editing a dictionary or pattern that is used by an enabled policy	Yes, for the scope of the affected policies
Adding or removing a condition of an enabled rule (policy)	Yes, for the scope of that rule/policy

Action	Initiates a discovery scan?
Adding a specific scope, such as a file server, to a rule (policy)	No
Removing a specific scope, such as a file server, from a rule (policy)	No
Removing all scopes from a rule (policy)	No
Editing a rule's (policy's) description	No
Renaming a rule (policy)	No
Assigning global flags to a rule (policy)	No
Changing the rule (policy) classification category or the state of the Files classified by this rule are considered sensitive checkbox.	No
Clicking the Rescan Rule button on the Classification Rules tab	Yes, for the scope of that rule
Creating a new rule (policy) without enabling it	No
Creating and enabling a new rule (policy)	Yes, for the scope of that rule
Enabling OCR	No
Disabling OCR	No

Action	Initiates a discovery scan?
Migrating the monitoring of a data source to a new Collector	No
Changing the scanning schedule	No
Adding a new file type	No
Changing file type text extractor on the File Types tab	No
Enabling/Disabling file type checkboxes (metadata/content) on the File Types tab	No
In Management Console, changing custom extended file properties used in an enabled rule	No
In Management Console, changing settings for file type detection	No
Changing maximum file size for scanning	No

Working With The Action Center

Overview

The Action Center allows you to view and track the execution progress of actions created by your automation. This includes actions waiting for review and approval, operations waiting to run, operations currently running, and operations that have completed their run.

Each operation includes multiple actions created by an automation. For example, for an automation that remediates stale permissions, the operation includes an action for each of the stale permissions identified by the automation.

Note: An operation can include up to 10,000 actions.

The operations are listed in six tabs according to their current status: Review, Pending, Running, Finished, Errors, and All. The lists in the tabs can be filtered according to a more detailed status, the automation type, the automation name, the date the operation was created, and the date the operation run was completed. For example, the Pending list can be filtered according to operations that are Pending and operations that are Scheduled and are awaiting execution per their defined schedule. The Review list can be filtered according to operations that are currently under review and operations that are awaiting review.

Viewing the Details and Actions of an Operation

1. Click an operation's link or the expand option to see its details.



2. Click View actions, to see a list of the operation's actions and their attributes.



Reviewing an Operation and Approving its Actions

The review and approval of actions is available for operations that were created by an automation in which the This automation requires user approval before running checkbox was selected.

1. From the options menu of the operation you want to review, select View.
   A list of all the actions in the operation is displayed.
2. Click Start Review.

   Note: The Start Review button is available only for operations in the Pending Review status.

   The operation is now locked–additional actions cannot be added to it–and is ready for review.
3. To approve all actions, from the Approval menu, select Approve all.

4. To approve only some of the actions, click the action's select icon.



> Note: Alternatively, you can download a CSV file of the actions and review them outside the Action Center. See Downloading a CSV Approval File.

5. Once you finish reviewing all the actions,click Execute to move the operation to the next phase in the process.

The operation moves to the Running list or to the Pending list if its automation has a defined schedule or if there is a queue of operations waiting to be executed.

> Note: Actions that were not completed will be included in an upcoming operation and will be reviewed again. Decisions about actions in previous approval processes are not kept.

Stopping an Operation's Execution

An operation can be stopped while its status is In progress. If stopped, the operation's actions, which were not executed yet, will not be executed. You cannot stop actions that were already executed.

To stop an operation's execution, click the operation's options menu, and select Stop.

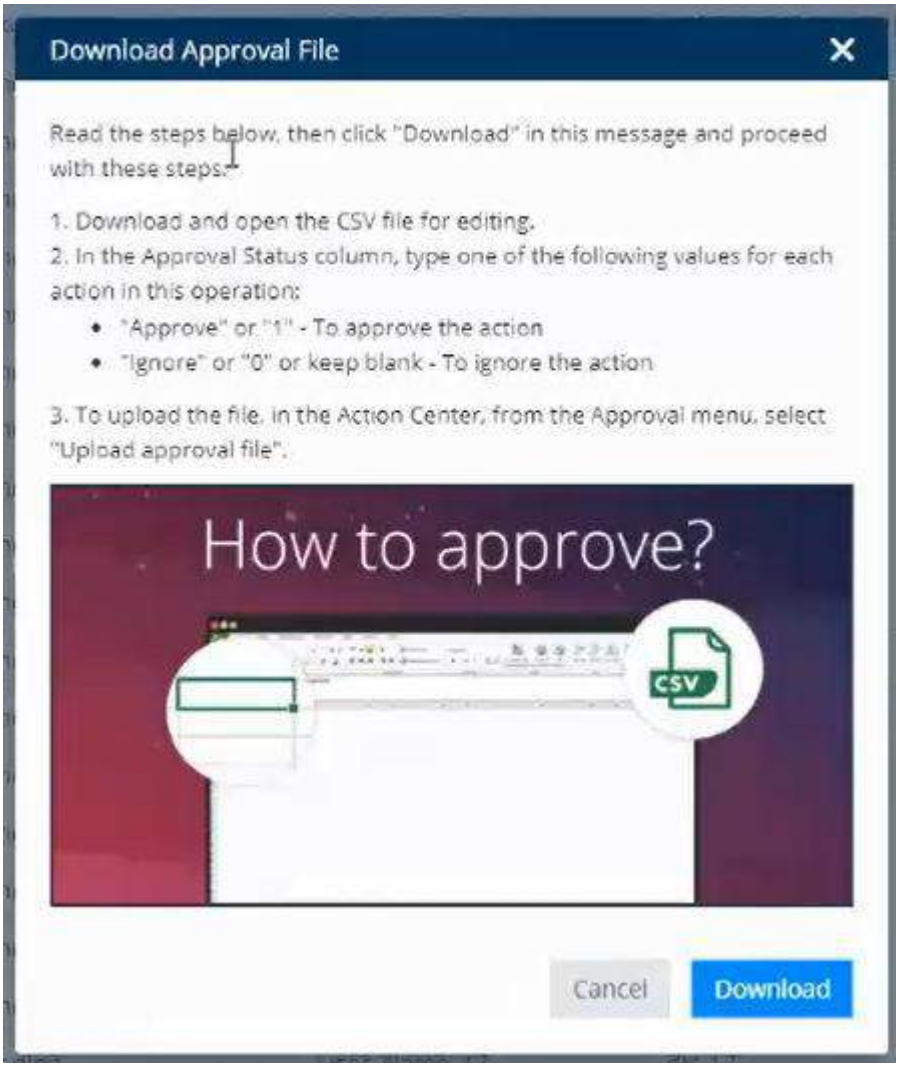


Downloading a CSV Approval File

You may want to share the automation's actions awaiting approval with users who do not have access to the Action Center. To do so, you can download a CSV file which lists all the actions for approval.

1. In the Action Center, click an operation's link or the expand option to see its details.

2. From the options menu of the operation you want to review, select View.
   A list of all the actions in the operation is displayed.
3. Click Start Review.
   The operation is now locked–additional actions cannot be added to it–and is ready for review.
4. From the Approval menu, select Download approval file.
   The Download Approval File dialog box is displayed.

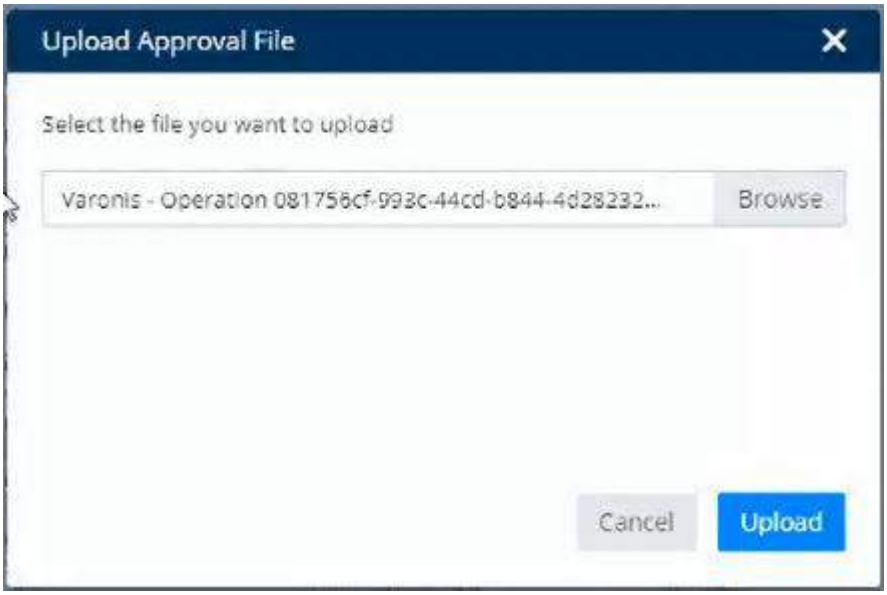


5. Read the instructions, and then click Download.
   The CSV file is downloaded to a destination folder.
6. Open the CSV file and in the Approval Status column, for each action, type one of the following:

> Note: Do not change the format of the CSV file as this might cause errors during upload.

- `Approve` or `1` – to approve the action
- `Ignore`, 0, or keep blank – to ignore the action for now and include it in the next list of actions.

7. After you finish reviewing and inserting a value for all actions, in the Action Center, from the Approvalmenu, select Upload approval file.
   The Upload Approval File dialog box is displayed.



8. Browse to the CSV file, and click Upload.
   The actions you approved in the CSV file are displayed as approved in the first column.
9. Click Execute to move the operation to the next phase in the process.

The operation moves to the Running list or to the Pending list if its automation has a defined schedule or if there is a queue of operations waiting to be executed.

Rolling Back Actions of an Automation

You can roll back completed actions of an operation created by some automations.

The operation must be in one of the following statuses: Completed, Completed with errors, Stopped, or Partial rollback completed.

> Note: An action can be rolled back only once.

1. In the Action Center, go to the operation you want to roll back.
2. Click the operation name to view its actions.
3. Select the checkboxes of the completed actions you want to roll back.

4. From the Actions menu, select Roll back selected actions.



> Note: The Roll back selected actions option is available only for actions that can be rolled back.

Working With Scheduled Searches

A scheduled search is a saved search that is run at a predetermined time or at specified intervals to enable you to periodically receive the information you need automatically.

Use a scheduled search to automate multiple saved searches per specified date, time, and recurrence frequency. An email that includes a link to the scheduled search results is sent to relevant recipients. If a recipient is external to the organization or is not defined as a Varonis user within Varonis Security for the organization, they are first authenticated via a one-time password (OTP) and are then redirected to the scheduled search download page.

> Note: When exporting data (as a CSV, Excel or PDF file), the maximum number of results is limited to 1,000,000 (Results that exceed the limit are not included in the exported file).

Go to Management and select Scheduled Searches. This page lets you see all scheduled searches, create new ones, and do actions on one or more scheduled searches at once. You can also include multiple saved searches within a single scheduled search.

The My Scheduled Searchespage includes the following components:



- A search box (1) for finding particular scheduled searches
- A clickable list of your scheduled searches (2). Click the scheduled search name to edit its settings.
- A more options button ⋮ (3) that displays a list of the actions you can perform on the scheduled search such as running the search, changing the owner of the search, or deleting the search.
- A Select action menu (4) for performing actions on selected scheduled searches in bulk
- A toggle button for enabling or disabling a scheduled search (5).
- A New Scheduled Search button (6) for creating a new scheduled search.

Note: To learn how to work with scheduled searches using the Varonis API, see Scheduled Search API.

Creating a Scheduled Search

1. Click New Scheduled Search at the top of the page.
2. In the General section, define the following options:
   - Name - The name of the scheduled search. You can click the search name later to view and edit the scheduled search settings.
   - Description - A brief description of the schedule search.

- Data-Driven - A sub-set of the scheduled search, customized per-owner: When selected, each owner receives only relevant information based on their managed objects.

  Note:
  - To enable data-driven scheduled searches: In the Management Console, go to Configuration > Security and select Apply object limitation.
  - The Specific Owners list is refreshed every eight hours. If you cannot find a newly set owner, wait for the list to be refreshed.
  - Data-driven reports are available for download for 30 days, after which they are removed.
  - The Data-Driven subscription feature does not include mailboxes.

- Export Format - Whether the scheduled search will be delivered as a CSV, Excel, or PDF file.
- You can also choose to send the search even if there are no results.

3. In the Linked Searches section, click Link Searches to link multiple saved searches to your scheduled search.
4. In the Recipients and Email Settings section, select who will receive your scheduled search email and other email-related settings.
5. In the Time Settings section, set the date, time, and recurrence frequency of the scheduled search.
6. Click Save to save your scheduled search for future use.

System Health

The System Health page provides up-to-date information on operational and configuration issues in your system, which you can resolve by implementing the recommended solutions.

The page consists of the following tabs: System Health, Discovery Monitor and Labeling Monitor.

System Health Tab

The System Health table displays a list of alerts. When you launch this page, it is refreshed with the live issues detected on the data sources monitored by Varonis. If an issue is fixed, the alert disappears after two days. The Last Update date and time of the page are indicated below the tab name.

Alert Table

The alert table consists of the following columns:

- Severity - Indicated by the alert color (on the left of its Description):
  - Red: High - Issues that prevent monitoring of the specified Collector, data source or domain controller. For example:
    - Events are not collected on the specified data sources. Auditing is disabled.
    - The specified Collectors reached high CPU in the last day.
    - Events are not collected on the specified data sources. There is no access to the data sources on Collector.
  - Orange: Medium - Issues that partially interrupt monitoring and should be addressed. For example:
    - User MFA information is not available due to a missing application permission in Entra ID.
  - Green: Low - Issues that don't interrupt monitoring, but should still be addressed. For example:
    - Executive accounts discovery failed to run because configuration is incomplete or incorrect.
- Description: Presents the issue to be resolved, including useful information such as the suspected cause and the consequences of the problem.
- Solution: Step-by-step instructions on how to resolve the issue. If the solution doesn't resolve the issue, contact Varonis Support for assistance.
- Data Source: The name of one or more Collectors, data sources or domain controllers in which the issue occurred.
- Data Source Type: The type of platform on which the issue occurred (Edge, SharePoint Online, Exchange, Active Directory, NetApp or Collector etc.).
- Last Updated: The date and time on which this issue was last updated.



System Health Notifications

To help you address issues in a timely fashion, your Enterprise Administrator is notified of alerts via a daily email. The Enterprise Administrator can manage the recipients list as needed.

Currently, system health notifications focus on high-severity alerts that may require your immediate attention.

The notification provides the complete information on each alert, as it appears in the System Health tab: Description, Solution and Data Source details.

Notifications are enabled by default. You can disable or re-enable these emails and manage the recipients list via Configuration > Settings > Notifications).

Note:

- System Health emails are sent once a day, informing you of issues in the past 24 hours. For live data (consisting of issues in the past 48 hours), go to the System Health page.
- Emails may include alerts about issues that you have already resolved. These issues are cleared after two days.

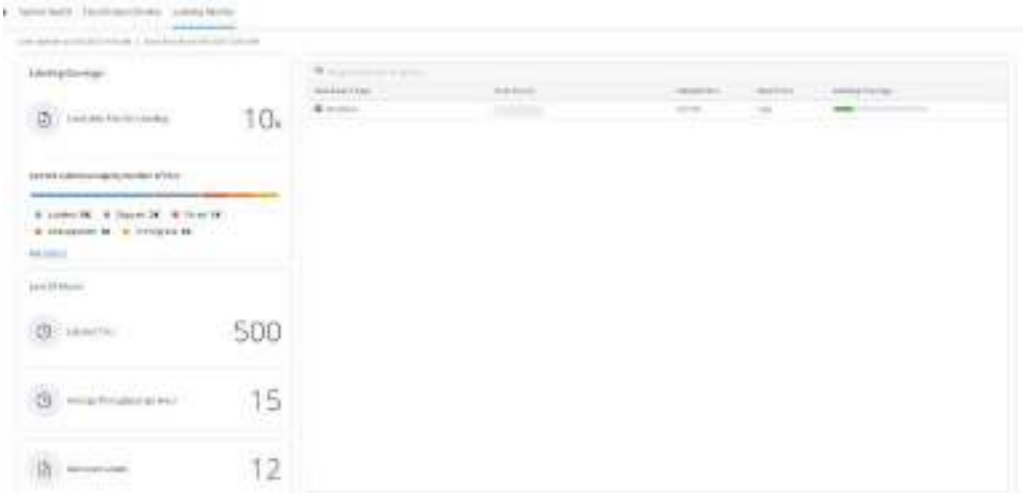
Discovery Monitor

The Discovery Monitor displays aggregated statistics that provide easy insight and confidence of the discovery coverage in your scanned environment. This includes information about the current scan and a drill down of the scanned file servers and their scan progress.

The Discovery Monitor is updated every three hours, reflecting the latest status in the database. The Last Update value indicates the specific time the monitor was last updated.

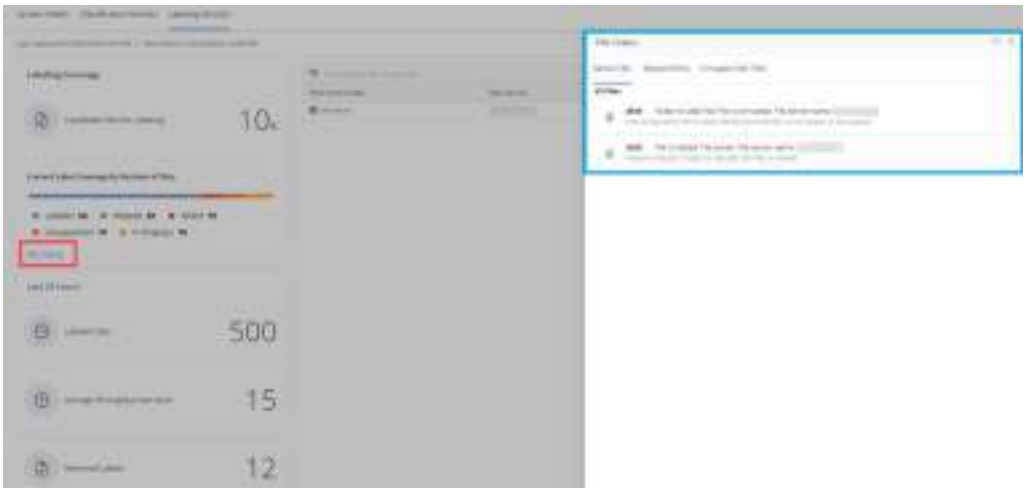
Labeling Monitor

The Labeling Monitor provides visibility into the labeling progress to ensure that classification labeling is running properly at all times.



The File Status side pane provides information about files that were not labeled or relabeled because labeling failed, or the file was skipped, or is not supported. To open the side pane, click File Status in the Current Label Coverage by Number of Files

widget.



8 SECURING COPILOT FOR MICROSOFT 365

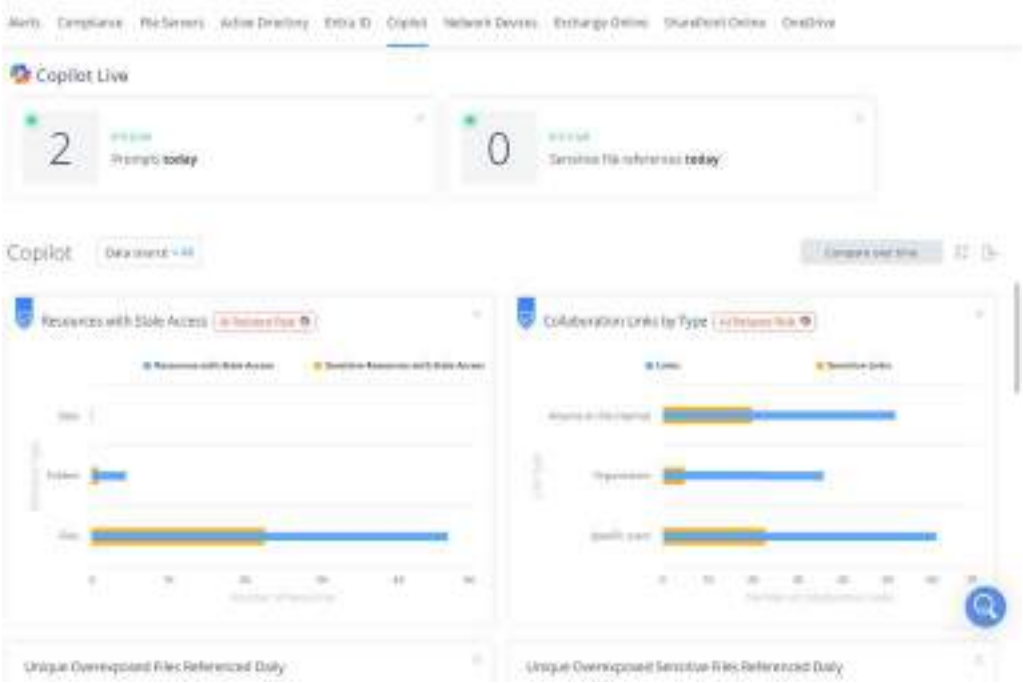
Built on the power of Large Language Models (LLMs) and generative AI, Copilot for Microsoft 365 can make your employees significantly more productive. But with great power comes great risk: If your organization lacks the required data protection, Copilot might expose your most sensitive data, putting you at risk for data leaks, theft, and misuse. Copilot uses your existing user permissions, so ensuring they are configured properly is critical. It is highly recommended that you do so before you enable Copilot and continue monitoring its activity to ensure your data is protected.

Through visibility and automation, Varonis provides the solution for securing your organization's data in M365 so you can safely deploy and benefit from Copilot. The Varonis Web Interface helps you secure Copilot using a Copilot dashboard and new Copilot analytics, including events and alerts.

Copilot Dashboard

The Copilot dashboard gives you a clear view of how your organization uses Copilot and whether your data is at risk. The dashboard widgets provide live stats on Copilot usage via live counters of Copilot interactions (prompts) and the sensitive files referenced. In addition, you can get general information on your organization's Copilot usage, like the exposure level and sensitivity of the referenced files and the state of data exposure in your M365 environment.

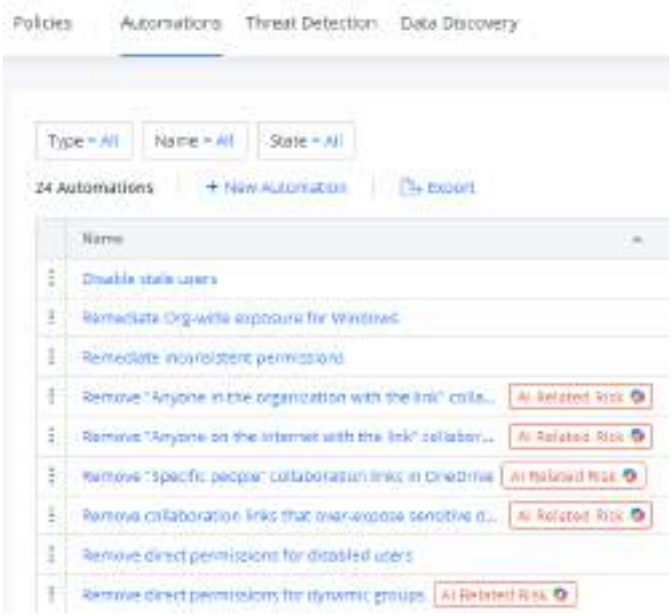
The following image shows an example Copilot dashboard. Note there are additional widgets that you can reorder as needed.



The widgets show Copilot-related events that took place in one of the following time frames:

- Widgets indicated by the “Live” icon are counters that query your data on demand, allowing them to be based on your local browser time (starting at midnight). At the beginning of each day, they restart and show 0 events until the first Copilot interaction is audited. They continue to show the accumulative number of audited events and are reset at midnight.
- Other “Daily” widgets summarize the total number of Copilot-related events until the previous day ended at midnight. They are recalculated and stored in UTC.

Note: The Copilot dashboard and related automations allow you to detect and remediate any overexposure. The relevant widgets and automations are easily identified by the new AI Related Risk icon: AI Related Risk



Copilot Events

Because Copilot makes it so easy to find and use sensitive information, once you’ve deployed it, you must ensure that your blast radius doesn’t grow and your data is still being used safely. Accordingly, event analytics now include two new event types:

- Interacted with Copilot - Monitors all user interactions with Copilot.
- File Referenced by Copilot Interaction - Monitors Copilot replies that reference files stored in SharePoint Online and OneDrive. This event includes information about

the file, its sensitivity, and its exposure.



Note: These events are collected from all Copilot users, whether they are licensed or not (e.g. Trial users). As a result, the number of users shown in the Events analytics page may be larger than the number of licensed users shown in the Copilot Licensed Users widget.

Copilot Alerts

Varonis uses this auditing of Copilot interactions to provide the following out-of-the-box alerts (available via the Management > Policies > Threat Detection page):

- Abnormal number of Copilot interactions
- Abnormal number of sensitive Copilot interactions
- Access to sensitive files using Copilot from a malicious IP
- Executive access to sensitive files using Copilot from a new geolocation
- First time service account interaction with Copilot

Note:

- Most Copilot alerts are based on behavioral learning. As such, they require a minimum 30-day learning period to gather data and analyze your users' behavior.
- Varonis securely stores your Copilot for M365 interactions: The Varonis SOC monitors the entire Varonis infrastructure and complies with ISO, HIPAA, PCI, and AICPA requirements. Varonis always stores data in the geography you select and never transfers any of your metadata outside that geography.

Contact your Varonis team to get access to these capabilities.

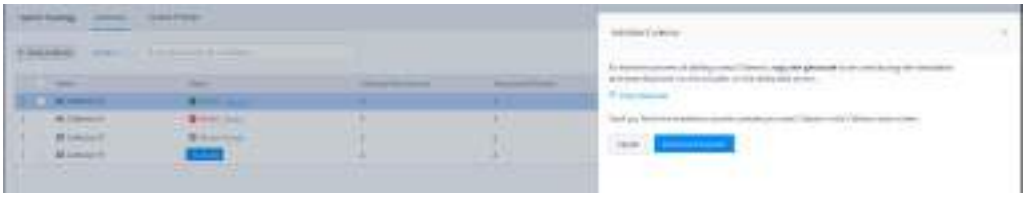
For more information on securing Copilot, see:

- Securing Microsoft Copilot Lab
- Is Your Org Ready for Microsoft Copilot?

9

System Topology

The System Topology page provides you with everything you need to know about your Collectors. This is where you install your Collectors and where you update them to a newer version.
Collectors are deployed and activated on the Collectors tab of the System Topology page. Collector installation is quick and simple. Click + New Collector to download and run an installer with short and easy instructions on the dedicated server for the Collector. For details, see Installing a Collector.



Once the installation is completed, the Collector is displayed on the Collectors tab and its status displays an Activate button. Click this button to activate the Collector.



You can deploy and activate multiple Collectors at the same time. You can also use third-party distribution tools to install multiple Collectors automatically.

You can repair a Collector when it is not functioning properly. Click the Repair button to reinstall the Collector, keeping its current configuration.



Collector updates are performed automatically, and you can set them to be performed during your maintenance window. You schedule Collector updates on the Update Settings tab of System Topology. For details, see Upgrade the Collectors.

API Keys

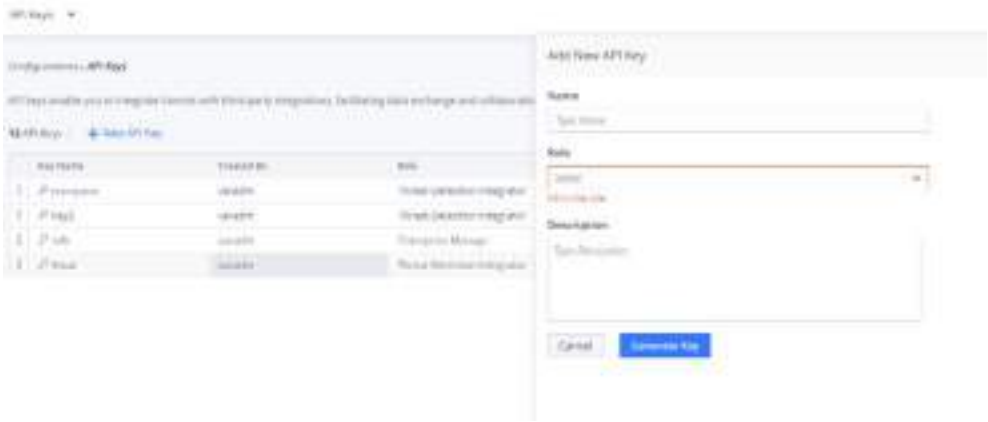
API keys enable you to integrate Varonis with third-party applications, facilitating data exchange and collaboration. You can control the permissions of an API key for specific API calls by assigning it a specific role.

Creating an API Key

Authenticate to the Varonis API by providing an API key token. You will need to create a new key with the relevant role required for your API call.

1. Navigate to Configuration > API Keys, and click + New API Key.

The Add New API Key settings are displayed on the right.



2. Fill in the required settings:
   - Name - (Mandatory) Enter the API key name.
   - Role - Select the relevant role from the dropdown list. For more information, see API Key Roles.
   - Description - Enter the API key description.
3. Click Generate Key.
4. Copy the API key secret and use it to authenticate API calls. For example, see Palo Alto Cortex XSOAR Integration.
5. From the options menu (three dots) next to each row, you can Rotate, and Revoke an API key. Rotating an API key will change its secret and you'll need to update the secret in the third-party application settings page. Revoking a key deletes it.

API Key Roles

Role	Description
Enterprise Manager	Use migration tools (such as Exporters, Uploader, and Deployer)

Role	Description
	for migration purposes. This role has full access to all operations in the Varonis system. Note: A key with an Enterprise Manager role expires seven days after creation.
Threat Detection Integrator	Integrate Varonis alerts with third-party applications. This role has permission to export and manage alerts.

Third-Party Integrations

API keys enable you to integrate Varonis with third-party integrations, facilitating data exchange and collaboration.

Note:

- As a security best practice, it is recommended to generate an API key per integration.
- The Threat Detection Integrator role is required for API keys for third-party integrations.
- For more information about creating API keys and assigning roles, see API Keys.

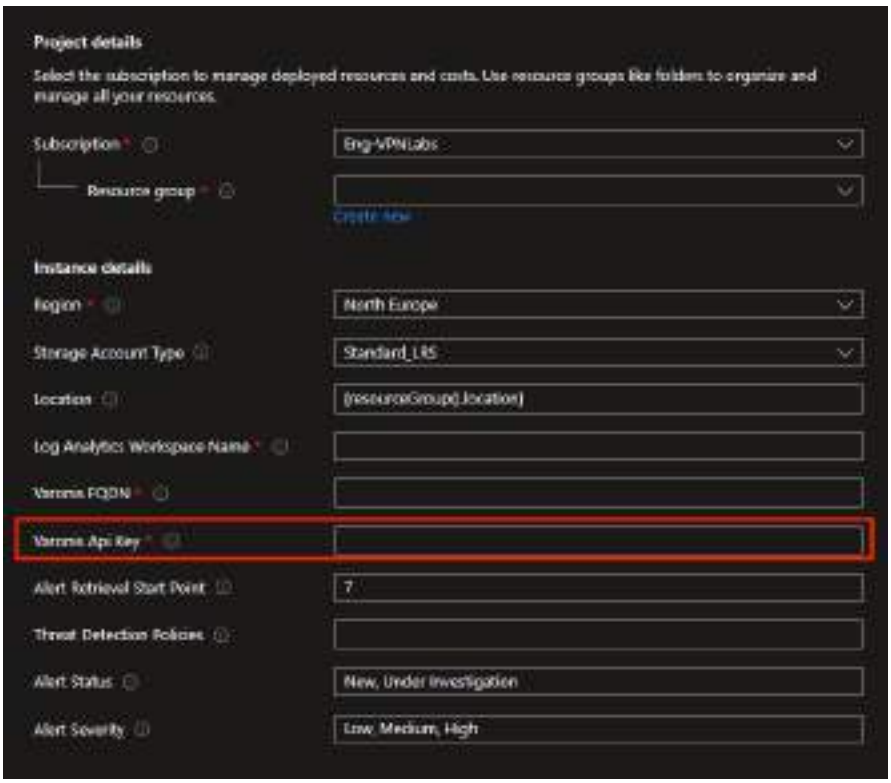
Microsoft Sentinel SIEM Integration

Varonis supports integration with Microsoft Sentinel SIEM. You can deploy the Varonis SaaS package from Microsoft's Marketplace to pull Varonis alerts into Microsoft Sentinel SIEM and manage them from there. After downloading the Varonis SaaS package from Microsoft's Marketplace, you'll need to authenticate to Varonis using an API key that you'll generate in the Varonis Web Interface.

Follow the steps in API Keys and the requirements in Third-Party Integrations to generate the API key needed for integration.

Configuration Page in Microsoft Sentinel SIEM

Paste the API key in the Varonis API Key field:



The rest of the alert retrieval configuration is on the same page.

Varonis License Agreement for Microsoft Sentinel SIEM

LICENSE AGREEMENT

IMPORTANT - READ CAREFULLY THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT (THIS "AGREEMENT") BEFORE USING THE SOFTWARE (AS DEFINED BELOW). THE SOFTWARE IS COPYRIGHTED AND LICENSED (NOT SOLD). CLICKING ‘AGREE’, OR DOWNLOADING, ACCESSING OR USING THE SOFTWARE INDICATES YOUR ACCEPTANCE OF THE TERMS SET FORTH BELOW AND CREATES A LEGAL AGREEMENT BETWEEN YOU AND VARONIS SYSTEMS, INC. ("LICENSOR"). IF YOU ARE NOT WILLING TO BE BOUND BY THE TERMS OF THIS AGREEMENT, YOU HAVE NO RIGHT TO USE THE SOFTWARE. In connection of your use of Microsoft Sentinel, and subject to the terms hereof, Licensor hereby grants you a limited right to use the Software. For the purposes of this Agreement, the term “Software” shall refer to the program, tool, plug-in, add-on,

application, library, content, data, solution, service or other item or material created and published by Licensor.

1. Grant of License. Subject to the terms and conditions of this Agreement, Licensor grants to you a personal, limited, non-exclusive, non-transferable, non-sublicensable, revocable license to use the Software, in executable form only, internally and solely in connection with the Microsoft Sentinel (the "License"). You may not, and may not permit or aid others to, translate, reverse engineer, decompile, disassemble, update, modify, reproduce, duplicate, copy, distribute or otherwise disseminate all or any part of the Software, or extract source code from the object code of the Software.
2. Proprietary Rights; Confidentiality. You acknowledge and agree that the Software is a proprietary productof Licensor or its licensors, protected under copyright laws and international treaties. You further acknowledge and agree that all right, title and interest in and to the Software and any derivatives thereof are and shall remain at all times with Licensor. All intellectual property rights (including, without limitation, copyrights, trade secrets, trademarks, etc.) evidenced by, embodied in or attached/ connected/related to the Software, including any revisions, corrections, modifications, enhancements, updates or upgrades thereof (to the extent provided by Licensor) are and shall remain exclusively owned by Licensor. Nothing in this Agreement constitutes a waiver of Licensor's intellectual property rights under any law. You shall maintain any non-public information provided to you by Licensor, including without limitation, the Software and documentation related thereto in strict confidence, and you shall not share the Software and the documentation related thereto with any third party. You shall ensure that only those of your employees and consultants that need access to the Software shall be able to access it, and you shall remain liable at all times for any breach of this Section by any such employees and consultants. This Section shall survive any expiration or termination of this Agreement.
3. Term and Termination. The License is effective until terminated by a party upon providing a written noticeto the other party. Your rights under the License will terminate automatically without notice from Licensor if you fail to comply with any term(s) of this Agreement. Upon termination, you shall cease all use of the Software and destroy all copies, full or partial, of the Software.
4. No Warranty. YOU USE THE SOFTWARE AT YOUR OWN RISK. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE SOFTWARE IS PROVIDED ON AN "AS IS" AND “AS AVAILABLE” BASIS, WITH ALL FAULTS AND WITHOUT WARRANTY OF ANY KIND, AND LICENSOR HEREBY DISCLAIMS ALL WARRANTIES AND CONDITIONS WITH RESPECT TO THE SOFTWARE, EITHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR

PURPOSE, ACCURACY, QUIET ENJOYMENT, AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS. SHOULD YOU DISCOVER ANY DEFECTS IN THE SOFTWARE, YOU ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION OF THE SOFTWARE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR LIMITATIONS ON APPLICABLE STATUTORY RIGHTS OF A CONSUMER, AND IN ANY SUCH CASE, THE ABOVE EXCLUSIONS AND LIMITATIONS SHALL NOT APPLY TO YOU.

5. Limitation of Liability. UNDER NO CIRCUMSTANCES WILL LICENSOR BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL OR EXEMPLARY DAMAGES, LOSS OF PROFITS, USE, REVENUE, OR DATA OR FOR BUSINESS INTERRUPTION (REGARDLESS OF THE LEGAL THEORY FOR SEEKING SUCH DAMAGES OR OTHER LIABILITY) ARISING OUT OF OR IN CONNECTION WITH USE OF THE SOFTWARE, WHETHER OR NOT LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ADDITION, THE LIABILITY OF LICENSOR ARISING OUT OF OR RELATING TO THE SOFTWARE WILL NOT EXCEED THE AMOUNT PAID OR PAYABLE BY YOU (IF ANY) FOR SUCH SOFTWARE.
6. Trade Compliance. You acknowledge that the Software is subject to the United States Financial Sanctions Regulations and the U.S. Export Administration Regulations. You further agree that you will comply with all financial sanctions and export control laws, regulations, and orders administered by the U.S.Government and/or, to the extent consistent with U.S. antiboycott law, comparable controls imposed by other governments having jurisdiction over activities under this Agreement (collectively, “Trade ControlLaws”) to assure that the Software is not exported, re-exported, transferred, installed or accessed, directly or indirectly, in violation of such Trade Control Laws. You warrant that neither you nor any party/ies that individually or in the aggregate own 50% or more of you, nor, to the best of your knowledge, any party authorized by you to use the Software, is subject to financial sanctions or other restriction on receipt of goods or services imposed by applicable Trade Control Laws (collectively, “RestrictedParties”) and agree that you shall be deemed a material breach if you violate Trade Control Laws in connection with activity under this Agreement, or becomes a Restricted Party, or otherwise becomes subject to applicable restrictions under Trade Control Laws, whether such restrictions apply to you or to the region in which you are located, including any restrictions that result in a requirement not to use License Exception ENC and to instead obtain an export license or similar government authorization to supply you with products or services. You agree to reasonably cooperate and assist Licensor or any of its representatives with an audit, review or investigation of your compliance with applicable laws and regulations as set forth in this Section. In connection with such review, audit or investigation, you will deliver to Licensor all

relevant records, information and documents reasonably requested by Licensor. You will immediately rectify non- compliance as requested by Licensor. The foregoing is without derogating from any other right or remedy Licensor may have under this Agreement or under any applicable law.

7. General.You may not assign this Agreement to any third party without the prior written consent of Licensor.This Agreement shall be governed by and construed in accordance with the laws of the State of New York, regardless of its conflict of laws rules. The federal and state courts located in the city of New York, New York shall have sole and exclusive jurisdiction over any dispute under this Agreement or otherwise related to the Software. This Agreement constitutes the entire agreement between Licensor and you with respect to your use of the Software and may not be modified except by a written instrument executed by an authorized representative of each of the parties. Should any term of this Agreement be declared void or unenforceable by any court of competent jurisdiction, such declaration shall have no effect on the remaining terms hereof. The application of the United Nations Convention of Contracts for the International Sale of Goods and the Uniform Computer Information Transactions Act are expressly excluded.

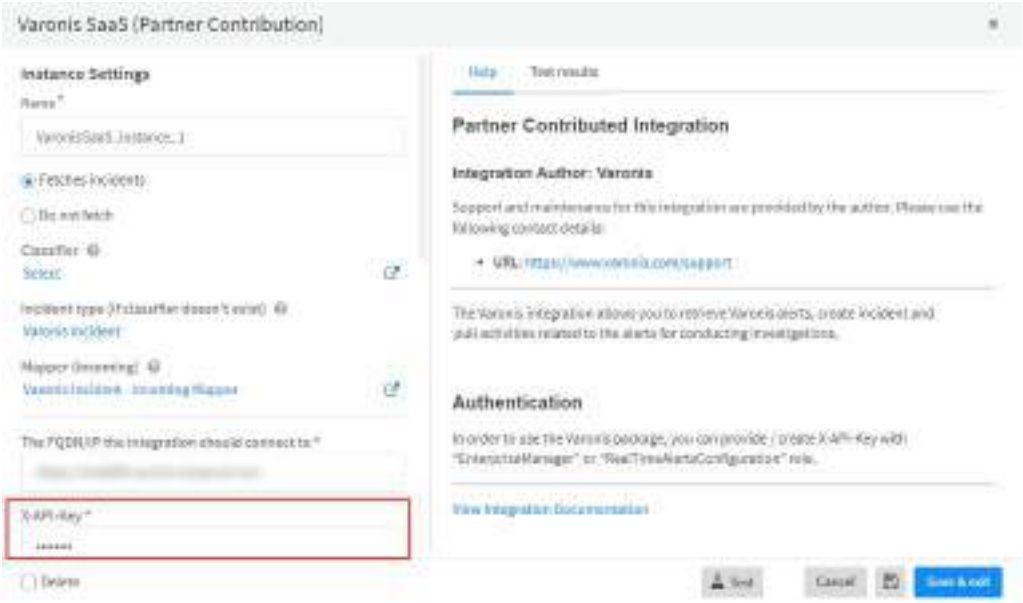
Palo Alto Cortex XSOAR Integration

Varonis supports integration with Palo Alto Cortex XSOAR. You can deploy the Varonis SaaS package from the Palo Alto Cortex Marketplace to pull Varonis alerts to Palo Alto Cortex XSOAR and manage them from there. After downloading XSOAR from the Palo Alto Cortex Marketplace, you'll need to authenticate to Varonis using an API key that you'll generate in the Varonis Web Interface.

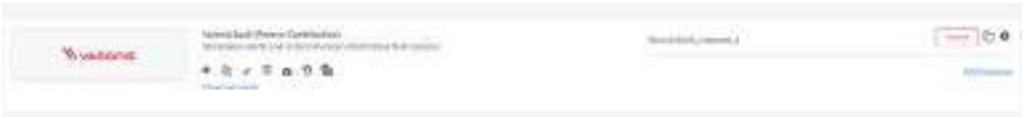
Follow the steps in API Keys and the requirements in Third-Party Integrations to generate the API key needed for integration.

Configuration Page in Palo Alto Cortex XSOAR Marketplace

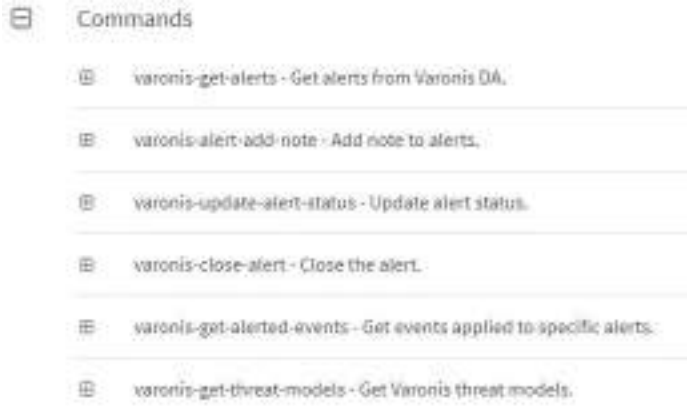
Paste the API key secret in the X-API-Key field:



Varonis Installed on Palo Alto Cortex XSOAR



Click Show commands to see the available actions for this integration.



Splunk SIEM Integration

Varonis supports integration with Splunk Enterprise SIEM. You can deploy the Varonis SaaS package from Splunk's Marketplace to pull Varonis alerts into Splunk Enterprise SIEM and manage them from there. After downloading the Varonis SaaS package from Splunk's Marketplace, you'll need to authenticate to Varonis using an API key that you'll generate in the Varonis Web Interface.

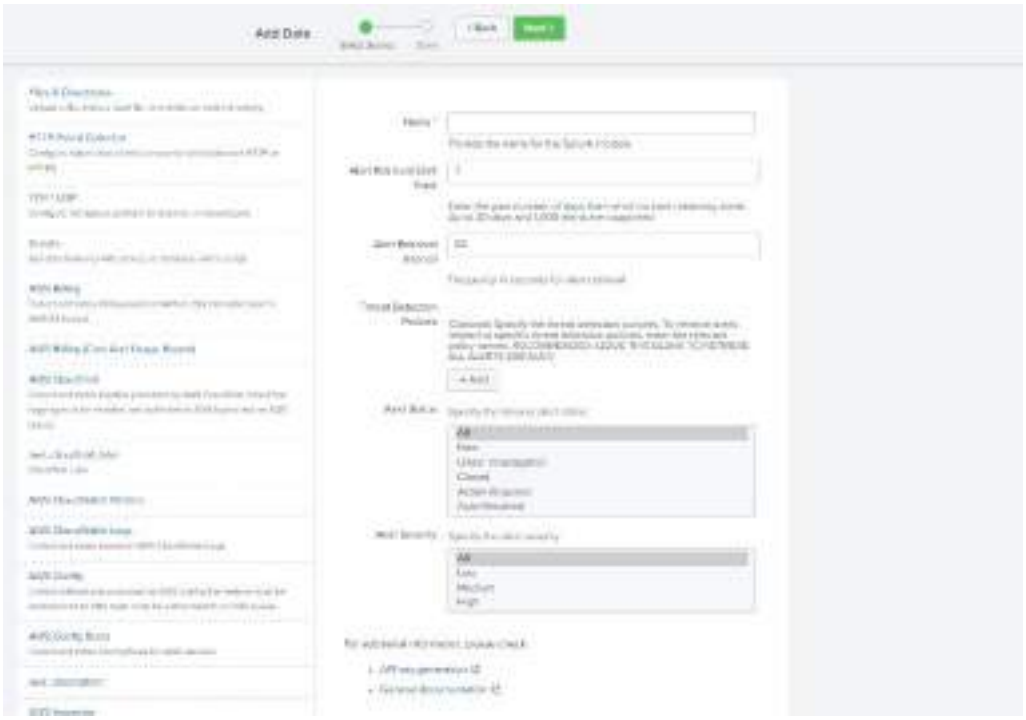
Follow the steps in API Keys and the requirements in Third-Party Integrations to generate the API key needed for integration.

Configuration Page in Splunk SIEM

Paste the API key in the Varonis API Key field:



Complete the required settings on the following page:



Varonis License Agreement for Splunk

LICENSE AGREEMENT

IMPORTANT - READ CAREFULLY THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT (THIS "AGREEMENT") BEFORE USING THE SOFTWARE (AS DEFINED BELOW). THE SOFTWARE IS COPYRIGHTED AND LICENSED (NOT SOLD). CLICKING ‘AGREE’, OR DOWNLOADING, ACCESSING OR USING THE SOFTWARE INDICATES YOUR ACCEPTANCE OF THE TERMS SET FORTH BELOW AND CREATES A LEGAL AGREEMENT BETWEEN YOU AND VARONIS SYSTEMS, INC. ("LICENSOR"). IF YOU ARE NOT WILLING TO BE BOUND BY THE TERMS OF THIS AGREEMENT, YOU HAVE NO RIGHT TO USE THE SOFTWARE. In connection of your use of Splunk Inc.’s or its affiliates products and/or services (the “Splunk Software”), and subject to the terms hereof, Licensor hereby grants you a limited right to use the Software. For the purposes of this Agreement, the term

“Software” shall refer to the program, tool, plug-in, add-on, application, library, content, data, solution, service or other item or material created and published by Licensor.

1. Grant of License. Subject to the terms and conditions of this Agreement, Licensor grants to you a personal, limited, non-exclusive, non-transferable, non-sublicensable, revocable license to use the Software, in executable form only, internally and solely in connection with the Splunk Software (the "License"). You may not, and may not permit or aid others to, translate, reverse engineer, decompile, disassemble, update, modify, reproduce, duplicate, copy, distribute or otherwise disseminate all or any part of the Software, or extract source code from the object code of the Software.
2. Proprietary Rights; Confidentiality. You acknowledge and agree that the Software is a proprietary product of Licensor or its licensors, protected under copyright laws and international treaties. You further acknowledge and agree that all right, title and interest in and to the Software and any derivatives thereof are and shall remain at all times with Licensor. All intellectual property rights (including, without limitation, copyrights, trade secrets, trademarks, etc.) evidenced by, embodied in or attached/connected/related to the Software, including any revisions, corrections, modifications, enhancements, updates or upgrades thereof (to the extent provided by Licensor) are and shall remain exclusively owned by Licensor. Nothing in this Agreement constitutes a waiver of Licensor's intellectual property rights under any law. You shall maintain any non-public information provided to you by Licensor, including without limitation, the Software and documentation related thereto in strict confidence, and you shall not share the Software and the documentation related thereto with any third party. You shall ensure that only those of your employees and consultants that need access to the Software shall be able to access it, and you shall remain liable at all times for any breach of this Section by any such employees and consultants. This Section shall survive any expiration or termination of this Agreement.
3. Term and Termination. The License is effective until terminated by a party upon providing a written notice to the other party. Your rights under the License will terminate automatically without notice from Licensor if you fail to comply with any term(s) of this Agreement. Upon termination, you shall cease all use of the Software and destroy all copies, full or partial, of the Software.
4. No Warranty. YOU USE THE SOFTWARE AT YOUR OWN RISK. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE SOFTWARE IS PROVIDED ON AN "AS IS" AND “AS AVAILABLE” BASIS, WITH ALL FAULTS AND WITHOUT WARRANTY OF ANY KIND, AND LICENSOR HEREBY DISCLAIMS ALL WARRANTIES AND CONDITIONS WITH RESPECT TO THE SOFTWARE, EITHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR

PURPOSE, ACCURACY, QUIET ENJOYMENT, AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS. SHOULD YOU DISCOVER ANY DEFECTS IN THE SOFTWARE, YOU ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION OF THE SOFTWARE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR LIMITATIONSON APPLICABLE STATUTORY RIGHTS OF A CONSUMER, AND IN ANY SUCH CASE, THE ABOVE EXCLUSIONS AND LIMITATIONS SHALL NOT APPLY TO YOU.

5. Limitation of Liability. UNDER NO CIRCUMSTANCES WILL LICENSOR BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL OR EXEMPLARY DAMAGES, LOSS OF PROFITS, USE, REVENUE, OR DATA OR FOR BUSINESS INTERRUPTION (REGARDLESS OF THE LEGAL THEORY FOR SEEKING SUCH DAMAGES OR OTHER LIABILITY) ARISING OUT OF OR IN CONNECTION WITH USE OF THE SOFTWARE, WHETHER OR NOT LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ADDITION, THE LIABILITY OF LICENSOR ARISING OUT OF OR RELATING TO THE SOFTWARE WILL NOT EXCEED THE AMOUNT PAID OR PAYABLE BY YOU (IF ANY) FOR SUCH SOFTWARE.
6. Trade Compliance. You acknowledge that the Software is subject to the United States Financial Sanctions Regulations and the U.S. Export Administration Regulations. You further agree that you will comply with all financial sanctions and export control laws, regulations, and orders administered by the U.S.Government and/or, to the extent consistent with U.S. antiboycott law, comparable controls imposed by other governments having jurisdiction over activities under this Agreement (collectively, “Trade ControlLaws”) to assure that the Software is not exported, re-exported, transferred, installed or accessed, directly or indirectly, in violation of such Trade Control Laws. You warrant that neither you nor any party/ies that individually or in the aggregate own 50% or more of you, nor, to the best of your knowledge, any party authorized by you to use the Software, is subject to financial sanctions or other restriction on receipt of goods or services imposed by applicable Trade Control Laws (collectively, “RestrictedParties”) and agree that you shall be deemed a material breach if you violate Trade Control Laws in connection with activity under this Agreement, or becomes a Restricted Party, or otherwise becomes subject to applicable restrictions under Trade Control Laws, whether such restrictions apply to you or to the region in which you are located, including any restrictions that result in a requirement not to use License Exception ENC and to instead obtain an export license or similar government authorization to supply you with products or services. You agree to reasonably cooperate and assist Licensor or any of its representatives with an audit, review or investigation of your compliance with applicable laws and regulations as set forth in this Section. In connection with such review, audit or investigation, you will deliver to Licensor all

relevant records, information and documents reasonably requested by Licensor. You will immediately rectify non- compliance as requested by Licensor. The foregoing is without derogating from any other right or remedy Licensor may have under this Agreement or under any applicable law.

7. General.You may not assign this Agreement to any third party without the prior written consent of Licensor. This Agreement shall be governed by and construed in accordance with the laws of the State of New York, regardless of its conflict of laws rules. The federal and state courts located in the city of New York, New York shall have sole and exclusive jurisdiction over any dispute under this Agreement or otherwise related to the Software. This Agreement constitutes the entire agreement between Licensor and you with respect to your use of the Software and may not be modified except by a written instrument executed by an authorized representative of each of the parties. Should any term of this Agreement be declared void or unenforceable by any court of competent jurisdiction, such declaration shall have no effect on the remaining terms hereof. The application of the United Nations Convention of Contracts for the International Sale of Goods and the Uniform Computer Information Transactions Act are expressly excluded.

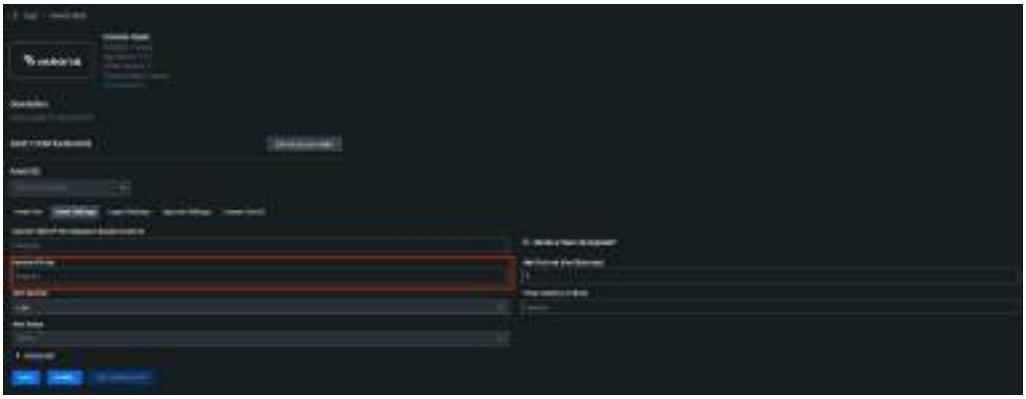
Splunk SOAR Integration

Varonis supports integration with Splunk Security Orchestration, Automation and Response (SOAR) . You can deploy the Varonis SaaS package from Splunk's Marketplace to pull Varonis alerts into Splunk SOAR, create workflows, and automate SOC tasks in mere seconds. After downloading the Varonis SaaS package from Splunk's Marketplace, you'll need to authenticate to Varonis using an API key that you'll generate in the Varonis Web Interface.

Follow the steps in API Keys and the requirements in Third-Party Integrations to generate the API key needed for integration.

Configuration Page in Splunk SOAR

Paste the API key in the Varonis API Key field:



The rest of the alert retrieval configuration is on the same page:

EDR Integration

Varonis supports integration with Endpoint Detection and Response (EDRs).

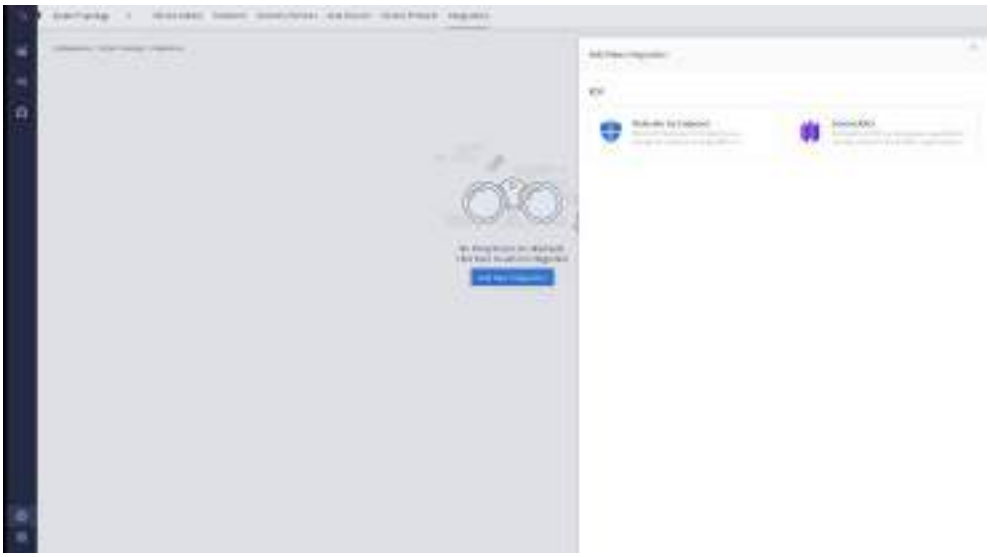
> Note: Private Preview. If you would like to integrate with EDR solutions, contact your Sales Engineer.

EDR integration significantly enhances Varonis' MDDR by leveraging telemetry data from EDR solutions. This data enriches Varonis alerting capabilities, provides additional context, reduces operational friction, and improves automated playbooks.

> Note: In the future, EDR alerts will be managed directly within MDDR.

To integrate an EDR solution:

1. Navigate to the Configuration > System Topology > Integrations tab. Here, you can easily configure your EDR settings to meet your specific needs.
2. Click Add New Integration and select the relevant EDR solution displayed on the right. Proceed to configure the relevant settings.



SentinelOne - Configuring a User Account for API

This section walks you through the process of configuring a user account for API access in the SentinelOne platform.

Note: Private Preview. If you would like to integrate with EDR solutions, contact your Sales Engineer.

User Roles

SentinelOne classifies users into unique types:

- Console Users:
  - Have access to the Management Console or API.
  - Are associated with a permanent email address.
- Service Users:
  - Can only interact with the API.
  - Receive an API token that is not tied to any individual user or email address.
  - Ideal for instances where a Console API token is needed for product integration.
- Management Users:
  - Have both an access level and a specific role within the system.

Service Users Overview

Service users enable the creation of API tokens that are not tied to a specific Console user or email address. They are ideal for scenarios such as integrating with Marketplace applications.

Characteristics of a Service User:

- API Access - Service users can interact with the API but are unable to log into the Management Console.
- Roles and Permissions - They inherit the same Role-Based Access Control (RBAC) and scopes as Console users, allowing them to perform permitted activities within their access level exclusively via the API.
- Identification - Each service user is assigned a name and an optional description. Once the name is set, it cannot be changed, but the description can be modified.

Unique naming is recommended for ease of tracking and auditing, although it is not mandatory within the scope or environment.

- Security - Two-Factor Authentication (2FA) and Single Sign-On (SSO) protocols are not applicable to service users.
- Token Expiration - The lifespan of the API token is selectable at the point of service user creation and is fixed thereafter.

Advantages of Service Users Over Console Users:

- Enhanced Security- As service users cannot log into the Management Console and are not associated with any personal identity or email, they are less susceptible to impersonation attacks.
- Customized Permissions- Unlike Console user tokens, which mirror the permissions of the user, service user permissions and scopes are defined individually. This allows for the allocation of only the necessary permissions for each service user's intended function, enhancing security by limiting unnecessary access.

Creating Service Users

To create a new service user:

1. On the Settings toolbar, click Users.



2. Select Service Users.



3. Click Actions and select Create New Service User.
   The Create New Service User page is displayed.





4. Fill in the following fields:
   - Name- Enter a unique identifier for the user. This name will be used for identification in the Management Console. Please note: Once set, the name cannot be changed. Avoid using equal sign (=) or angle brackets (<, >) in the name.
   - Description - (Optional) Provide a brief description that helps to identify the user or their function within the system.
   - Expiration Date - Set the expiration date of the API token. The default is 1 year. Click Custom to set a different date and time.
5. Click Next.
   The Select Scope of Access page is displayed.



6. Select the scope(s) that the user will have access to, and the role for each scope.

7. (Optional) To copy the scope from a different service user, click Copy The Scope From a Different User.



8. Click Select a Service User to copy their scopes and roles.
9. Click Create User.
   The API token is generated. The API Token for APIUser page is displayed, showing the token string and the message: This is the last time you can see this token.



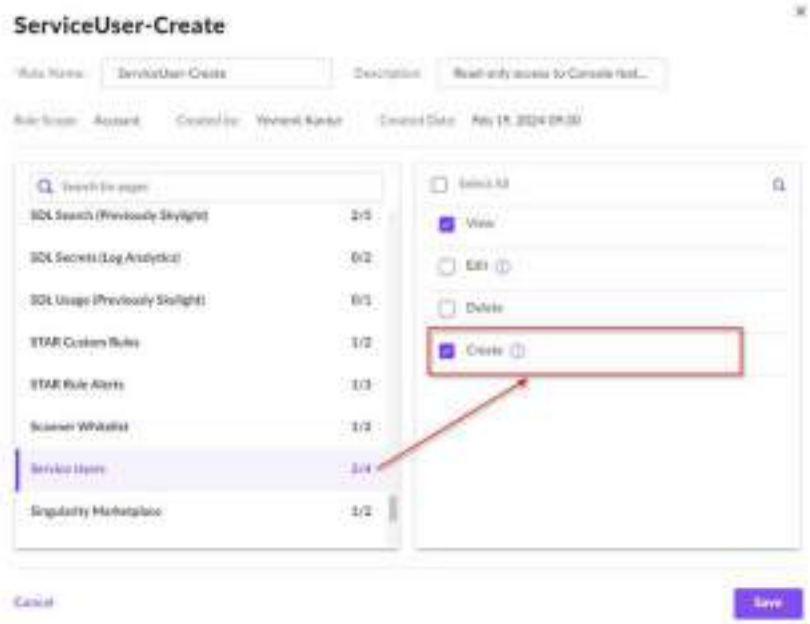
10. (Optional) Click Copy API Token and save the token string in a secured file.
11. Click Close.

Automating API Token Generation

It is best to create an API token for a script with a service user. If that is not possible, use a Console user API token.

Prerequisites for the Service User

The user must be granted the ServiceUser-Create RBAC role, along with the necessary permissions to execute the intended actions within the automation process.



To create a service user and delete a service user through the API:

1. Add the creation of a service user to the script: `/web/api/v2.1/service-users`.
   In the API doc, this is under Service Users > Create Service Users. For example:

```
headers = {
        "Authorization": f "ApiToken {API_TOKEN}",
        "Content-Type": "application/json",
        "Accept": "application/json, text/plain, */*"
    },
    json = {
        "data": {
            "name": "Service User Name",
            "description": "Service User Description",
            "expirationDate": f "{(datetime.datetime.utcn
ow() + datetime.timedelta(days=30)).isoformat()}Z",
            "scope": "account",
            "scopeRoles": [{
                "id": "426418030212073761",
                "roleId": "796941984887545597"
```

```
            }]
        }
    })
new_token = response.json().get('data').get('apiToken').g
et('value')
print(f 'New token: {new_token}')
```

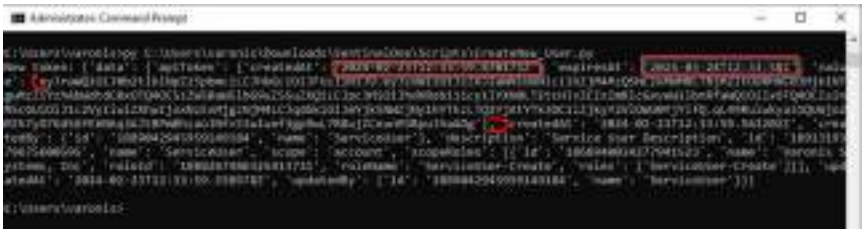
This example creates a service user that has the role ID 796941984887545597 in account ID 426418030212073761 that expires after 30 days. The response will contain the API token.

- `expirationDate` - Set the expiration time for the token in days. 30 days is the recommended expiration time. To define a different expiration time, change the value of days=30.
- `scope` - Set the user's scope to the minimum required access level: `site`, `account`, or `tenant for global`.
- `scopeRoles` - "`id`" is the ID of the site or account scope from the Console. "`roleId`" is the ID of the role assigned to the user, which defines its permissions.

The example that works in our lab:



2. Run the script and get the following results.



3. Verify that a new user was created.



Required Permissions for API Varonis Users

The following table describes the permissions required for API users in Varonis.

API Call Permissions	Identifier Role Name	Role Name	Title	Tyoe	Identifier	Value
/web/api/v2.1/user	users	Console Users	View	view	796870761852551000	TRUE
/web/api/v2.1/threats	threats	Endpoint Threats	View	view	796870763505107000	TRUE
/web/api/v2.1/agents	endpoints	Endpoints	View	view	796870762481697000	TRUE
/web/api/v2.1/threats/:threat_id/explore/events	threats	Endpoint Threats	View	view	796870763505107000	TRUE
/web/api/v2.1/cloud-detecti	custom Alerts	STAR Rule Alerts	View	view	1040438250645820000	TRUE

API Call Permissions	Identifier Role Name	Role Name	Title	Tyoe	Identifier	Value
on/alerts						
/web/api/v2.1/service-users	service Users	Service Users	View	view	1491839018456700000	TRUE
/web/api/v2.1/service-users	service Users	Service Users	Delete	delete	1491839018507030000	TRUE
/web/api/v2.1/service-users	service Users	Service Users	Create	create	1491839018473480000	TRUE

Staleness Threshold

The staleness threshold is defined for the following entities:

- Resources - Resources are considered "stale" if no activity is detected on them after the selected number of days (default is 180).
- Accounts - Accounts are considered "stale" if no activity is detected by them after the selected number of days (default is 120)

To customize these staleness thresholds, select another value from the list or enter a custom number of days.

Note: The changes you make here will take effect after the next calculation. This occurs once the next metrics jobs take place (FS job for stale resources and DS job for stale accounts). For more information on staleness, go to Staleness.



Response Scripts

The Response Script directory is where all the scripts used for Varonis threat detection policy script execution are stored, either locally or on a shared drive. It serves as a script execution repository and needs only to be configured once since it applies to all threat detection policies. Once configured, you'll only need to specify the name of the script from the dedicated directory for each policy you want to configure script execution.

> Note: Only users with the Varonis Enterprise Manager role (most elevated role) can configure a dedicated Response Script directory.

To configure the dedicated directory for script execution, navigate to Configurations > Settings > Response Script > Response Script directory.

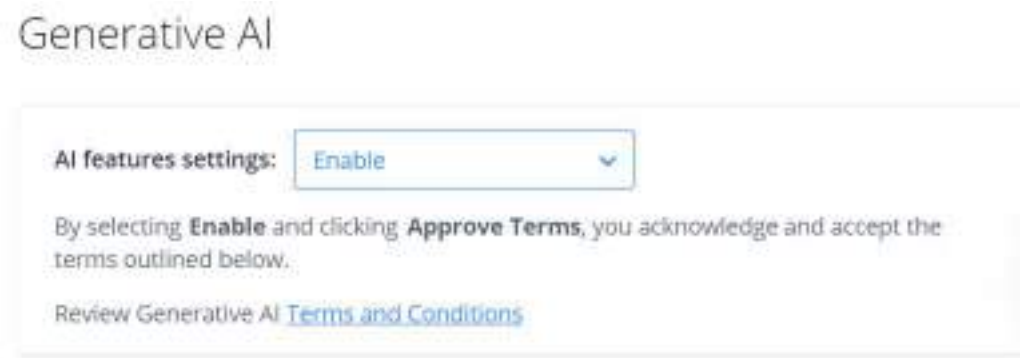
> Note: The selected AD account and network share/local folder need to be accessible from all Collectors.



For more information about configuring Response Script settings, see Threat Detection Policies.

Generative AI

For enabling Athena AI, you need to agree to the Generative AI Terms and Conditions. Before initial use, you can also enable Athena AI through the features (Alert page for AI Assistant SOC and Events and Resources Analytics for Search AI).



For more information, see Enabling Athena AI.

AI Conversation Auditing

> Note: Private Preview. If you'd like to use Conversation Investigation, contact your Sales Engineer.

By default, Varonis collects and presents metadata on Copilot conversations (for example, the names of the users who sent the prompts, the files referenced etc.).

You can enhance your analysis of Copilot interactions by monitoring and investigating Copilot conversation content. This information includes the complete text used in prompts and responses.

To activate the collection and analysis of Copilot prompts and responses, a user with an Enterprise Manager role is required to go to AI Conversation Auditing and set Audit AI conversations to Enable (disabled by default).



Note: To allow your Entra ID application to collect Copilot prompts, it must have a `Mail.Read` permission (see Allowing your Entra ID Application to Collect Copilot Prompts in the Working with Monitored Data Sources guide).

Flags

Varonis enables you to assign flags to accounts and resources. Use these flags to filter searches in the Accounts and Resources analytics tabs or to group search results.

There are two types of flags:

- System flags - Predefined flags that are managed by Varonis and cannot be edited by users. These flags indicate important insights that are automatically detected (for example: Whether a resource is stale, protected, unique etc.).
- User flags - Custom flags that you can manage via the Configuration menu. Use these flags to mark an account or a resource with your own insights.

To manage user flags:

1. Go to Configuration > Settings > Flags.



The Flags settings include:

- A search box for finding specific flags.
- A view of all user-defined flags.
- An + Add Flag button for creating new flags.

2. Manage your flags as follows:
   a. Create a new flag:
      i. Click + Add Flag to open the Create Flag window.
      ii. Enter a name and select a color for your new flag and then click Save.
   b. Edit a flag:
      i. Click the flag name to open the Edit Flag window.
      ii. Rename the flag or change its color and then click Save.
   c. Delete a flag:
      i. Click the X icon following the flag name.
      ii. In the Delete Flag confirmation window, click Delete.
      This operation removes the flag from any object it is attached to.

These flag settings control the flagging options available via the Accounts and Resources analytics tabs.

> Note: The flag management capabilities described here are also available via the Resource Side Pane.

Notifications

System Health alerts play a pivotal role in the smooth operation of your Varonis system. To help your team address high-severity alerts on time, you can configure push notifications of these critical analytics.

These notifications are enabled by default as emails that are sent to your Enterprise Administrator.

> Note:
>
> - System Health emails are sent once a day, informing you of issues in the past 24 hours. For live data (consisting of issues in the past 48 hours), go to the System Health page.
> - Emails may include alerts about issues that you have already resolved. These issues are cleared after two days.

Currently, the emails notify you of high-severity alerts, for example:

- Events are not collected on the specified data sources. Auditing is disabled.
- The specified Collectors reached high CPU in the last day.
- Events are not collected on the specified data sources. Varonis Audit Event Monitor Agent does not exist.

Each alert Description is followed by the recommended Solution: Step-by-step instructions for resolving the issue (as well as the data source details).

Set your system health notifications as follows:

- Toggle the feature on or off in the Allow notifications for system health issues field.
- Customize the notification mailing list by editing the emails defined in the Recipients field.



Collector Dumps

You can authorize Varonis Support to download process dumps from Varonis Collectors within your network to troubleshoot and address issues in your environment. Varonis Support can investigate issues in your environment without needing to connect to a Collector.

Note:

- Varonis Support can only download process dumps from Varonis Collectors version 11 and higher.
- Varonis does not collect dumps without consent.
- The memory dump includes the memory and stack of the faulty process on the Collector server.
- The dump may include excerpts of file contents classified by Varonis software.
- Upon consent, the dump file will be collected and stored inside the SaaS region chosen for your tenant.
- The dump will only be used to debug the problem by the Varonis Engineering Team.

- The file is stored in an encrypted form during the investigation and is discarded upon completion.

To grant approval:

1. Navigate to Configuration > Administrative Tools > Collector Dump.
2. Select Approve and set the duration (minimum of 3 days) or provide indefinite approval.



3. All dumps will be deleted when the investigation is complete.

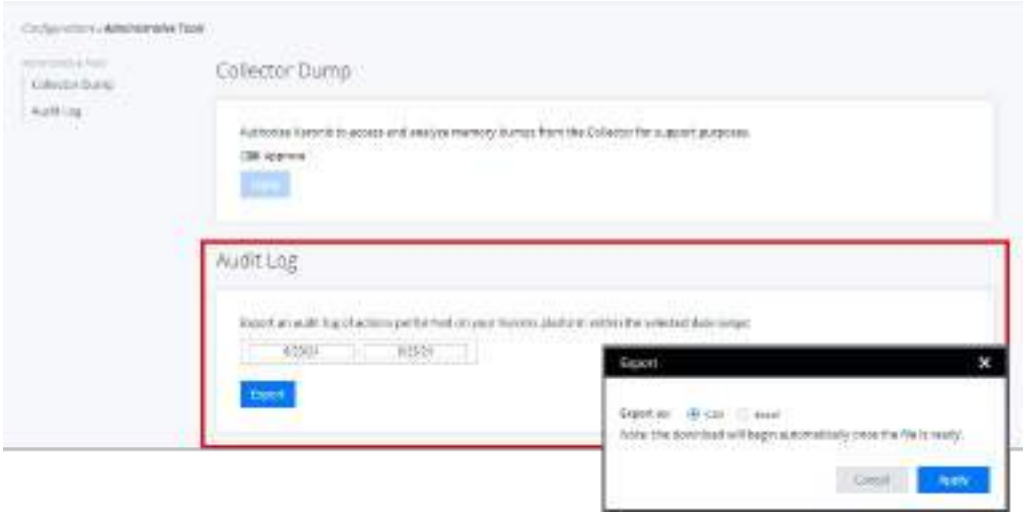
Audit Log

the Varonis Audit Log is an operational log of key actions (such as file analysis, log-ins, enabling or disabling policies, etc.) your organization's Varonis users perform on the Varonis platform.

This information is helpful for compliance and legal purposes and provides insights into your Varonis users' behavior.

To get this information, go to Configuration > Administrative Tools > Audit Log and click Export.

Note: This operation requires an Enterprise Manager role.



Audit log data is retained for seven years. Use the start and end date filters to pinpoint the relevant time span of your audit report.

Results are exported as either a CSV or an Excel file and are capped for 1,000,000 records.

10

License Information

The License Information page displays system license information and status including:

- License expiration date
- Licensed data source types
- Available quota for:
  - Events per day
  - Monitored resources

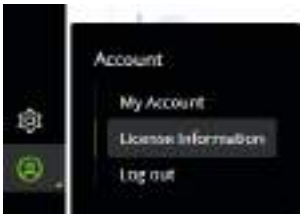
    Note: Resources may refer to folders, mailboxes, sites, directory structure and permissions (depending on the data source type), as well as classification results.
- Daily usage of monitored resources and number of events
- Indication of license violation

  Note: Exceeding the quota of events or resources for five days within a single calendar month is a considered a license violation.



Note: The data shown in the License Information page refers only to event and resource count in licensed data source types. Data collected from evaluation data source types is not included.

The License Information page is accessed from the Account menu and is available only to the Varonis Enterprise Manager and System Administrator user roles.



11

Organization-Wide Exposure

Here you'll learn what constitutes organization-wide exposure (org-wide, in short), how these metrics are calculated, and when these results are populated.

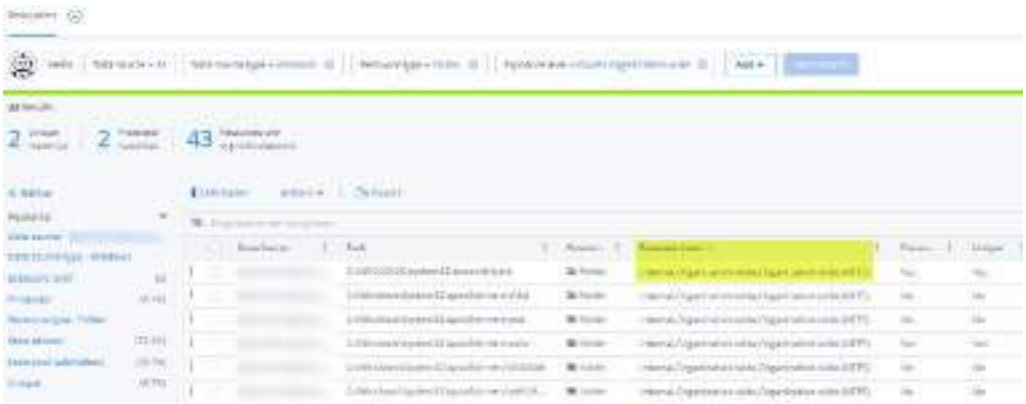
Org-wide exposure describes resources that are shared and can be accessed by global access groups (such as Everyone, Domain Users, Authenticated Users, and others).

CISF Platform Org-Wide Exposure

In CIFS platforms, global access groups have both Share and NTFS permissions to access the resource, either while logged into the server or remotely through Share.

In this CIFS case, the value of the exposure Level attribute is:

Internal, Organization-wide, Organization-wide (NTFS)

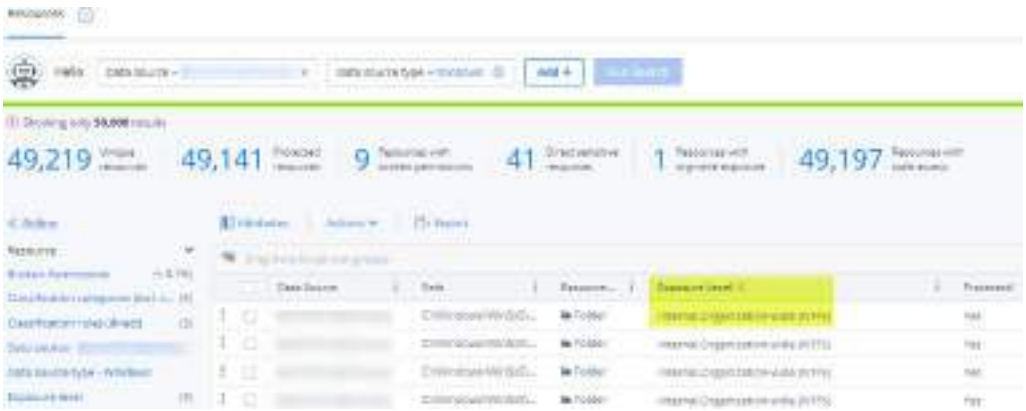


Note: Organization-wide exposure (NTFS) is relevant for CIFS platforms only.

The Organization-wide exposure (NTFS) value was introduced to indicate that the resource can be accessed by global access groups that are logged into the server, but they cannot access this resource through Share.

In this case, the value of the Exposure Level attribute is:

Internal, Organization-wide (NTFS).



Org-Wide Exposure Widgets in the File Servers Dashboard

The Dashboards menu's File Servers tab features several widgets that show the information breakdown of organization-wide access and exposure. These widgets include:

- Folders Exposed Org-wide - Counts only folders with both Share and NTFS permissions for global access groups.
- Folders Exposed Org-wide (NTFS) - Counts all the folders with NTFS permissions to global access groups, regardless of whether the global access groups have Share permissions for these resources.

  This widget is useful for monitoring the global access groups' remediation policies progress, since these policies remediate the NTFS permissions for resource global access groups, whether there are Share permissions for global access groups or not.



- Folders Exposed Org-wide by Permission (Incl. Inherited and Non-Inherited) - These two widgets provide a concise view of folders (with or without their inherited

folders), which are exposed org-wide with specific NTFS permissions: Full Control, Modify, Read & Execute, Special and List.

> Note: These widgets are not included in the default display (you can add them via the Widget Selection window).



To view the corresponding analytics, click these widgets to jump to their filtered data on the Resources page.

Staleness

This article explains the concept of staleness in the Varonis context. Varonis monitors several types of entities that might become stale (such as resources or accounts). The following sections describe how Varonis identifies each entity as stale, why such staleness is a security risk, and how to customize the entity's staleness threshold.

Resource Staleness FAQs

What is a stale resource?

Varonis monitors activity on resources over time. If no activity has been detected over a predefined period of time, known as the “staleness threshold”, the resource is considered “stale”.

The activity status of folders or files is applied to their parent resources, that is: If a child resource is identified as active, the parent resource is also considered active (even if there was no direct activity on the parent resource).

In addition, the staleness calculation considers the parent resource's Modify Date attribute, regardless of its child resources' activity: If the parent resource has been modified (for example, renamed), it is considered active.

Why are inactive resources considered risky?

An inactive resource that is kept beyond the required retention period can expose an organization to liability. It is often neglected when enforcing security measurements (like access control, permissions etc.). In addition, it might be easier for unauthorized users to access these resources under the radar. Also, it is expensive to maintain.

How does Varonis identify resource activity?

Varonis detects the resource activity using two sources of information:

- Events – Varonis monitors a predefined set of relevant events that platforms generate per-resource to determine if and when a resource was last active. This is the default source of information used to populate the resource's Last Event Date attribute.
- Resource attributes – Varonis also collects relevant resource attributes from the platform and uses them to determine the resource's activity status. This information is used when no event data is available, for example: During the onboarding period (right after installing the Varonis software). These resource attributes include:
  - File Modify Date – These two attributes capture the date different modifications were made on this resource or any of its sub resources. For example: The date on which this resource was created, renamed or removed, the date a file was created or changed in it, etc.
  - Last Activity Date– This attribute is currently only calculated for exchange online, where the definition of activity consists of a subset of relevant events. For example, Varonis does not consider the "Email Received" event as a relevant activity for calculating the Last Activity Date of a resource.

Varonis scans all of the above data, finds the latest date on which any activity took place on the resource or its sub resources by calculating the latest date between all of the relevant parameters described above, and uses it to determine whether the resource is stale.

How do I customize the Staleness Threshold of Resources?

By default, this staleness threshold is set as 180 days. If you need to change this threshold, to meet the requirements of your specific industry, regulations etc., go to

Configuration > Settings > Staleness Threshold and set the relevant number of days. This occurs once the next FS metrics job takes place.

Account Staleness FAQs

What is a stale account?

Varonis monitors activity on accounts over time. If no activity has been detected in your system over a predefined period of time, known as the “staleness threshold”, the account is considered “stale”.

Why are inactive accounts considered risky?

Having inactive accounts in your organization makes it harder to manage your accounts and to control their permissions. In addition, it might be easier for unauthorized users or attackers to target these accounts and use them to access your organization and even perform actions.

How does Varonis identify account activity?

Varonis detects the account activity using the following sources of information:

- Last Event Date: Varonis monitors a predefined set of relevant events per-account to determine if and when an account was last active.
- Last Logon Time: The last time this account has logged on to your system.
- Account Creation Date: The date and time on which this account was created.

Varonis uses the latest date out of these parameters to determine the value of the Last Activity Date attribute. This attribute is then compared to the staleness threshold, to determine whether the account is stale.

How do I customize the Staleness Threshold of Accounts?

By default, this staleness threshold is set as 120 days. If you need to change this threshold, to meet the requirements of your specific industry, regulations etc., go to Configuration > Settings > Staleness Threshold and set the relevant number of days. The changes you make here will take effect after the next calculation. This occurs once the next DS metrics job takes place.

Permission and Membership Staleness FAQs

What is a stale permission? What is a stale membership?

Access to resources is granted via permissions. Permissions can be given to individual users and to groups.

A membership in a group provides the member with the permissions of the group.

Varonis monitors access on resources over time. If no access has been detected over a predefined period, known as the “staleness threshold”, the permission or membership is considered “stale”:

- If a user with permission to a resource has not used this permission–accessed the resource over a predefined period–the permission is considered “stale”.
- If a member of a group has not used their membership–has not accessed any of the resources the group has permission to–over a predefined period, their membership is considered “stale".

Why are inactive permissions or memberships considered risky?

An inactive permission or membership that is kept beyond the required retention period can expose an organization to liability. It is often neglected when enforcing security measurements such as access control and permissions. In addition, it might be easier for unauthorized users to use this permission or membership under the radar. Also, handling stale permissions or memberships makes managing access more focused

How does Varonis identify permissions and membership staleness?

The Staleness Threshold of permissions and memberships is indicated by the "learning period" set for monitoring activity for automations. Once the learning period ends, permissions and memberships not used during this period are considered stale.

There are two configuration options for the learning period:

- Show data in stale permission and stale membership widgets after a learning period of ____ days
- Generate actions for activity-based automations after a learning period of ____ days

For details, see the Configuring the Learning Period for Automations section in Working with Automations.

How do I customize the Staleness Threshold (learning period) of permissions and memberships?

For stale permission and stale membership widgets, the default period is 14 days for new installations. For upgrades, the value from the previous version is kept.

For activity-based automations, the default period is 120 days for new installations. For upgrades, the value from the previous version is kept.

You can change the period, if required, in the Management Console under Configuration > General.

12

Privacy Automation Search Syntax

A search query can include terms or both terms and operators. Multiple terms can be combined with Boolean operators to produce more relevant results.

Note: Privacy Automation is available in a separate user interface.

Terms

There are two types of terms:

- Single Term - A single word such as "hello" or "world"
- Phrase - A group of words surrounded by double quotes such as "hello world"

Boolean Operators

Boolean operators allow terms to be combined through logic operators to form more complex queries. Varonis supports OR, AND, "+" and "-" as Boolean operators.

Note: Boolean operators must be typed in ALL CAPS (all capital letters).

- OR
  The OR operator links two terms and finds documents where either of the terms exist. The OR operator is the default conjunction operator, meaning that if there is no Boolean operator between two terms, the OR operator is used.

  Example: To search for documents that contain either "world" or "hello", use the search query `"hello" "world"` or `"hello" OR "world"`.
- AND
  The AND operator links two terms and finds documents where both terms exist anywhere in the text of a single document.

  Example: To search for documents that contain "hello world" and "good morning", use the search query `"hello world" AND "good morning"`.
- +
  The "+" operator requires that the term after the "+" symbol must exist somewhere in the text of a single document.

  Example: To search for documents that must contain "hello" and may contain "world", use the search query `+hello world`.
- -

The "-" operator excludes documents that contain the term after the "-" symbol.

> Note: If you are using special characters in a search, the - must have a space before the special character, but not after.

Example: To search for documents that contain "hello world" but not "good morning", use the search query `"hello world" -"good morning"`.

Proximity Searches

Varonis supports finding words that are within a specified distance away from each other. To perform a proximity search, use the tilde symbol "~" and a numeric value specifying the desired distance at the end of a search phrase.

Example: To search for "hello" and "world" within ten words of each other in a document, use the search query `"hello world"~10`

Wildcard Searches

Varonis supports single- and multiple-character wildcard searches within single terms (not within phrase queries).

- The single-character wildcard search looks for terms that match with the single character replaced. To perform a single character wildcard search, use the "?" symbol.

  Example: To search for "text" or "test" use the search query `te?t`.

- The multiple-character wildcard search looks for zero or more characters. To perform a multiple-character wildcard search, use the "*" symbol.

  Example: To search for test, tests or tester, use the search query `test*`

> Note: You can use the wildcard character (* or ?) in the middle of the search term or as the last character of the search term. You cannot use it as the first character of the search term.

File Names and Paths

- To find an exact file name, use the following syntax: `zs1o0s zs1o0s` . For example: `zs1o0s zsuoz 5s48w5s0s176`

Note: The results will include all files with the name you specified in the query, in all available file formats. To find a specific file, include the file extension. For example: `zs1o0s zsuoz 5s48w5s0s176 3rt`

- To find a string as part of a filename, use this syntax: `zs1o0s 675w1u`. For example: `zs1o0s zsuoz`
- To find a string as part of a file path, use this syntax: `zs3o7v 675w1u` . For example: `zs3o7v zsuoz`

WORKING WITH MONITORED DATA SOURCES IN VARONIS SAAS

Publishing Information

Software Version

Publication date December 3, 2024

Copyright © 2005 -2024 Varonis Systems Inc.
All rights reserved.
This information shall only be used in conjunction with services contracted for with Varonis Systems, Inc. and shall not be used to the detriment of Varonis Systems, Inc. in any manner. User agrees not to copy, reproduce, sell, license, or transfer this information without prior written consent of Varonis Systems, Inc.
Other brands and products are trademarks of their respective holders.

Contents

Chapter 1: Welcome to Deploying Monitored Data Sources. 12

Chapter 2: Active Directory Data Sources. 13

AD Monitoring Overview. 14

AD Requirements. 15

Deployment and Configuration. 31

Adding an AD Data Source. 31

Editing and Removing an AD Data Source. 40

Adding and Removing Organizational Units. 44

Supported AD Events. 46

Chapter 3: Windows Data Sources. 58

Windows Monitoring Overview. 59

Windows Requirements. 61

Deployment and Configuration. 70

Adding Windows Data Sources - Summary. 70

Adding Windows Data Sources - Detailed Procedure. 72

Configuring the Windows Data Source Following Deployment. 82

Supported Events for Windows Data Sources. 83

Chapter 4: Amazon FSx for Windows Data Sources. 87

Amazon FSx for Windows Monitoring Overview. 88

Amazon FSx for Windows Requirements. 88

Deployment and Configuration. 89

Configuring Event Auditing for Amazon FSx for Windows Data Source. . 89

(Optional) Manually Setting up Amazon FSx for Windows/Varonis Environment on AWS. 92

Adding Amazon FSx for Windows Data Sources - Detailed Procedure. 102

Supported Events for Amazon FSx for Windows Data Sources. 110

Chapter 5: M365 Data Sources. 113

Requirements for Monitoring M365 Data Sources. 114

Entra ID Data Sources. 130

Adding an Entra ID Data Source. 130

Supported Events for Entra ID Data Sources. 139

Allowing your Entra ID Application to Collect Copilot Prompts. 140
SharePoint Online Data Sources. 141
Adding a SharePoint Online Data Source - Summary. 141
Adding a SharePoint Online Data Source - Detailed Procedure. 143
Supported Events for SharePoint Online Data Sources. 158
OneDrive Data Sources. 160
Adding a OneDrive Data Source - Summary. 160
Adding a OneDrive Data Source - Detailed Procedure. 161
Supported Events for OneDrive Data Sources. 177
Exchange Online Data Sources. 179
Adding an Exchange Online Data Source. 179
Supported Events for Exchange Online Data Sources. 189
Supported Mailboxes for Exchange Online. 191
Improving Directory Structure Crawling for Large Exchange Online Environments. 191
Chapter 6: NetApp Data Sources. 193
NetApp Monitoring Overview. 194
NetApp Requirements. 194
Mixed Security Style in NetApp Data Sources. 200
Deployment and Configuration. 202
Amazon FSx for NetApp ONTAP. 202
NetApp Performance Recommendations. 202
Configuring FPolicies for NetApp Data Sources Operating in Cluster Mode 203
Adding a NetApp Data Source Operating in Cluster Mode - Summary. 221
Adding a NetApp Data Source Operating in Cluster Mode - Detailed Procedure. 223
Supported Events for NetApp Data Sources. 231
Chapter 7: Dell PowerScale OneFS (Isilon) Data Sources. 234
Dell PowerScale OneFS (Isilon) Monitoring Overview. 235
Dell PowerScale OneFS (Isilon) Requirements. 236
Monitoring Dell PowerScale OneFS (Isilon) with Mixed Security Style. 237
Deployment and Configuration. 237

Installing and Configuring the Dell CEE Framework. 237
Configuring Dell PowerScale OneFS (Isilon). 242
Configuring the Varonis Service Account and REST API User for Dell PowerScale OneFS (Isilon). 245
Adding a Dell PowerScale OneFS (Isilon) Data Source - Summary. . . . 247
Adding a Dell PowerScale OneFS (Isilon) Data Source - Detailed Procedure. 249
Supported Events for Dell PowerScale OneFS (Isilon) Data Sources 256
Chapter 8: Dell Unity Data Sources. 259
Dell Unity Monitoring Overview. 260
Dell Unity Requirements. 260
Monitoring Dell Unity with Mixed Security Style. 261
Deployment and Configuration. 262
Installing and Configuring the Dell CEE Framework. 262
Configuring Dell Unity. 266
Configuring the Dell Unity REST API Access User. 267
Adding a Dell Unity Data Source - Summary. 267
Adding a Dell Unity Data Source - Detailed Procedure. 269
Supported Events for Dell Unity Data Sources. 276
Chapter 9: Azure Files Data Sources. 280
Azure Files Monitoring Overview. 281
Azure Files Requirements. 283
Deployment and Configuration. 285
Configuring a User Access Administrator for Creating a New Entra ID Application. 285
Configuring Permissions for Direct Access SMB. 286
Adding an Azure Files Data Source - Summary. 287
Adding an Azure Files Data Source - Detailed Procedure. 288
Manual Installation Using an Existing Azure Application. 299
Manually Configuring an Event Hub and File Diagnostic Setting for Event Auditing. 302
Supported Events for Azure Files Data Sources. 304
Chapter 10: Hitachi NAS Data Sources. 306
Hitachi NAS Monitoring Overview. 307

Hitachi NAS Requirements. 308
Deployment and Configuration. 309
Configuring Event Auditing for Hitachi NAS. 309
Configuring Hitachi NAS Shares for Windows. 310
Adding a Hitachi NAS Data Source - Summary. 311
Adding a Hitachi NAS Data Source - Detailed Procedure. 312
Supported Events for Hitachi NAS Data Sources. 317
Chapter 11: Nasuni Data Sources. 319
Nasuni Monitoring Overview. 320
Nasuni Requirements. 320
Deployment and Configuration. 323
Configuring the Varonis Service Account for Nasuni. 323
Configuring the NMC User. 325
Adding a Nasuni Data Source - Summary. 326
Adding a Nasuni Data Source - Detailed Procedure. 328
Supported Events for Nasuni Data Sources. 334
Chapter 12: Panzura Data Sources. 335
Panzura Monitoring Overview. 336
Panzura Requirements. 336
Deployment and Configuration. 338
Configuring the Varonis Service Account for Panzura. 338
Configuring Event Auditing for Panzura. 339
Adding a Panzura Data Source - Summary. 340
Adding a Panzura Data Source - Detailed Procedure. 342
Supported Events for Panzura Data Sources. 348
Chapter 13: Nutanix Data Sources. 349
Nutanix Monitoring Overview. 350
Nutanix Requirements. 350
Deployment and Configuration. 351
Configuring the Varonis Service Account for Nutanix. 351
Configuring the Nutanix REST API Access User. 352
Adding a Nutanix Data Source - Summary. 353
Adding a Nutanix Data Source - Detailed Procedure. 355
Supported Events for Nutanix Data Sources. 361

Chapter 14: Cohesity Data Sources. 362
Cohesity Monitoring Overview. 363
Cohesity Requirements. 363
Deployment and Configuration. 365
Configuring the Varonis Service Account for Cohesity. 365
Configuring the Cohesity REST API Access User. 366
Installing the Cohesity Connector for Varonis App on the Cohesity Cluster. 367
Adding a Cohesity Data Source - Summary. 368
Adding a Cohesity Data Source - Detailed Procedure. 370
Supported Events for Cohesity Data Sources. 376
Chapter 15: CTERA Data Sources. 377
CTERA Monitoring Overview. 378
CTERA Requirements. 378
Deployment and Configuration. 380
Configuring the Varonis Service Account for CTERA. 380
Configuring the CTERA REST API Access User. 381
Configuring Event Auditing for CTERA. 382
Adding a CTERA Data Source - Summary. 382
Adding a CTERA Data Source - Detailed Procedure. 384
Supported Events for CTERA Data Sources. 389
Chapter 16: Qumulo Data Sources. 391
Qumulo Monitoring Overview. 392
Qumulo Requirements. 392
Deployment and Configuration. 393
Configuring the Varonis Service Account for Qumulo. 393
Configuring the Qumulo REST API Access User. 395
Adding a Qumulo Data Source - Summary. 396
Adding a Qumulo Data Source - Detailed Procedure. 398
Supported Events for Qumulo Data Sources. 404
Chapter 17: Pure Storage FlashBlade Data Sources. 406
Pure Storage FlashBlade Monitoring Overview. 407
Pure Storage FlashBlade Requirements. 407
Deployment and Configuration. 408

Configuring the Varonis Service Account for Pure Storage FlashBlade. 408
Adding a Pure Storage FlashBlade Data Source - Summary. 409
Adding a Pure Storage FlashBlade Data Source - Detailed Procedure. 411
Supported Events for Pure Storage FlashBlade Data Sources. 417
Chapter 18: Pure Storage FlashArray Data Sources. 418
Pure Storage FlashArray Monitoring Overview. 419
Pure Storage FlashArray Requirements. 420
Deployment and Configuration. 421
Configuring the Varonis Service Account for Pure Storage FlashArray. 421
Adding a Pure Storage FlashArray Data Source - Summary. 421
Adding a Pure Storage FlashArray Data Source - Detailed Procedure. 423
Supported Events for Pure Storage FlashArray Data Sources. 429
Chapter 19: VAST Data Sources. 431
VAST Monitoring Overview. 432
VAST Requirements. 433
Deployment and Configuration. 434
Configuring the Varonis Service Account for VAST. 434
Configuring the VAST REST API Access User. 434
Adding a VAST Data Source - Summary. 435
Adding a VAST Data Source - Detailed Procedure. 437
Supported Events for VAST Data Sources. 443
Chapter 20: Linux Data Sources. 445
Linux Monitoring Overview. 446
Supported Linux Versions and Requirements. 446
Deployment and Configuration. 454
Adding a Linux Data Source - Summary. 454
Adding a Linux Data Source - Detailed Procedure. 456
Installing the Varonis Unix Agent. 462
Configuring Unix Data Source Services. 471
Supported NFS Events for Linux Data Sources. 472
Chapter 21: Unix Data Sources. 474
Unix Monitoring Overview. 475
Unix Requirements. 475
Deployment and Configuration. 476

Adding a Unix Data Source - Summary. 476
Adding a Unix Data Source - Detailed Procedure. 478
Supported NFS Events for Unix Data Sources. 484
Chapter 22: Unix Directory Services. 486
Unix Directory Services Monitoring Overview. 487
Adding an LDAP Domain. 488
Adding a NIS Domain. 490
Adding a Samba AD Domain. 491
Chapter 23: Network Device (Varonis Edge) Data Sources. 495
Network Device (Varonis Edge) Deployment Overview. 496
Supported Source Products and Versions. 496
Network Devices (Varonis Edge) Requirements. 498
Configuring a Network Device (Edge) Data Source. 499
Configuring a Collector to Support Network Devices (Edge). 500
Adding a New Network Device (Edge) Data Source. 503
Configuring Advanced Filter IP Ranges for Proxy Data Sources. 516
Date and Time Format Notation. 517
Configuring VPN Sources to Send Events to Varonis. 519
F5 Big-IP Access Policy Manager (APM). 519
Palo Alto GlobalProtect. 524
Check Point VPN. 544
Fortinet Forticlient. 550
Cisco ASA. 556
Cisco Firepower Threat Defense (FTD). 562
Citrix ADC (Netscaler). 574
Pulse Secure. 580
SonicWall SonicOS. 584
Sophos XG VPN. 588
Microsoft Always On VPN. 592
Configuring Web Proxy Sources to Send Events to Varonis. 597
Symantec (Bluecoat) ProxySG. 597
Skyhigh Secure Web Gateway (Previously McAfee Web Gateway). . . 603
Forcepoint (Websense) Web Security. 610
Fortinet FortiGate. 611

Palo Alto Web Filtering. 617
Cisco Firepower Threat Defense (FTD) for Proxy. 649
Cisco (IronPort) Web Security. 655
Cisco Umbrella Proxy. 658
Squid Proxy. 671
Apache Proxy. 673
Zscaler Proxy. 676
Barracuda Web Security Gateway. 681
Sophos XG Proxy. 682
Configuring DNS Sources to Send Events to Varonis. 686
Microsoft DNS Servers. 686
Infoblox DNS Servers. 696
Cisco Umbrella DNS Servers. 704
BlueCat DNS Servers. 718
Filtering DNS Events per Specified Domains. 724
Configuring Firewall Sources to Send Events to Varonis. 726
Cisco Secure Firewall Threat Defense (formerly known as Cisco Firepower Threat Defense). 726
Supported Events for Network Device (Edge) Data Sources. 731
Changing Ports for Logstash. 735
Chapter 24: Generic Data Sources. 737
Generic Data Source Requirements. 738
Deployment and Configuration. 739
Adding a Generic Data Source - Summary. 739
Adding a Generic Data Source - Detailed Procedure. 740
Chapter 25: Appendix - Creating an Entra ID Application for Monitoring M365 via the Admin Center. 746
Creating an Entra ID Application for Monitoring Entra ID via the Admin Center. 747
Creating an Entra ID Application for Monitoring Entra ID - Summary. . . 747
Creating an Entra ID Application for Monitoring Entra ID - Detailed Procedure. 748
Creating an Entra ID Application for Monitoring SharePoint Online via the Admin Center. 765

Creating an Entra ID Application for Monitoring SharePoint Online - Summary. 766
Creating an Entra ID Application for Monitoring SharePoint Online - Detailed Procedure. 766
Creating an Entra ID Application for Monitoring OneDrive via the Admin Center. 778
Creating an Entra ID Application for Monitoring OneDrive - Summary. . 779
Creating an Entra ID Application for Monitoring OneDrive - Detailed Procedure. 779
Creating an Entra ID Application for Monitoring Exchange Online via the Admin Center. 792
Creating an Entra ID Application for Monitoring Exchange Online - Summary. 792
Creating an Entra ID Application for Monitoring Exchange Online - Detailed Procedure. 793
Chapter 26: Appendix - Renewing the Secret or Certificate of your Entra ID Applications. 812
Renewing the Secret of your Entra ID Application. 813
Renewing the Certificate of your Entra ID Application. 815
Chapter 27: Appendix - Additional Configurations and Operations. 818

1 WELCOME TO DEPLOYING MONITORED DATA SOURCES

What This Guide Contains

This guide walks you through the steps to deploy and configure your monitored data sources. Here, you'll find information about the requirements, deployment and configuration procedures, and supported events for each monitored data source. The last section in this guide describes additional configurations and operations, such as decommissioning and repairing data sources.

> Note: The term Data Source represents any source of data that Varonis monitors, such as an Active Directory Domain, an Entra ID tenant, a file storage server, system or service, or an M365 service such as SharePoint Online. In some cases, the Varonis UI displays the terms Domain, File Server, or Resource instead of Data Source.

Before You Begin

Make sure to follow the steps in Getting Started with Varonis SaaS to set up your first Collector. We recommend reading the Getting Started guide before you dive into this one.

What To Do Next

For file storage data sources, first add an Active Directory data source.

For M365 data sources, first add an Entra ID data source.

After that, you can add additional data sources to be monitored by Varonis.

2 ACTIVE DIRECTORY DATA SOURCES

What This Section Contains

This section describes how to deploy and monitor Active Directory (AD) data sources; the requirements, deployment and configuration steps, and supported events.

What To Do Next

Before you dive in, click here to learn more about how Varonis monitors AD accounts, directory structure and permissions, and events.

AD Monitoring Overview

Note: Each AD data source represents a monitored AD domain. In some cases, the Varonis UI displays the term Domain instead of Data Source. To monitor multiple AD domains, add an AD data source per AD domain.

Varonis monitors an AD domain via the following parallel data streams.

Accounts

- Varonis enumerates local account information remotely from the Collector with a dedicated service account. The service executes LDAP queries directly against the domain controllers (DCs).
- For user and group accounts synced from AD to Entra ID, Varonis maps the AD accounts to their corresponding Entra ID accounts based on the following AD attributes:
  - Users are mapped via objectGUID
  - Groups are mapped via objectNAME

  For this mapping to occur, both AD and Entra ID must be deployed and monitored.

Directory Structure and Permissions

- Varonis monitors the AD directory structure and permissions via a dedicated service for directory structure monitoring (FileWalk) which runs on the Collector server. This service leverages LDAP to enumerate the Active Directory structure.

Events

- Varonis monitors AD events by reading the Event Viewer logs on each monitored DC, using a dedicated event auditing service (Forwarder) which runs on the Collector server. The service can connect to the monitored DCs either directly, or via a AD proxy service which can be installed either on the DC servers or other Windows Servers.
- When a AD proxy is installed, the proxy service reads the events from the DC Event Viewer logs, filters and aggregates them, and queues them in memory. The event auditing service, which runs on the Collector server, then connects to the proxy service, reads the events, and empties the queue.

- When a AD proxy is not installed, the event auditing service on the Collector server connects to the DCs directly and reads the events from their Event Viewer logs. An proxy-less deployment is not recommended since it may result in increased network bandwidth consumption and reduced performance.
- When a AD proxy is installed, you will see the following services in Windows Services Manager on the Windows Server where the AD proxy is installed:
  - Varonis Audit Event Service – The service which monitors the AD events
  - Varonis Audit Event Monitor – The service which monitors the health of the Varonis Audit Event Service

  When the above services are running, you will see the following services in Windows Task Manager:
  - VrnsCifsQueue – The service which monitors the AD events
  - VrnsMon – The service which monitors the VrnsCifsQueue service health

What To Do Next

First, make sure you fulfill the AD requirements.

AD Requirements

Before you begin to deploy and monitor an Active Directory (AD) data source, make sure you fulfill the below requirements to ensure proper functioning.

License Prerequisites

Data Stream	Required License
AD accounts	No license is required
AD structure and permissions	Varonis for Active Directory
AD events	Varonis for Active Directory

Installation Requirements

The following Varonis components should be installed to deploy and monitor AD.

Data Stream	Required Installation
AD accounts	• A Collector must be installed. • No AD proxy installation is required.
AD structure and permissions	• A Collector must be installed. • No AD proxy installation is required.
AD events	• A Collector must be installed. • An AD proxy of version 11.x or higher is required. It is recommended to install an AD proxy on all monitored DCs. When not possible, the AD proxy can be installed on one or more monitored DCs or on other Windows Servers. At least one AD proxy should be installed per Active Directory site. For more information, see this KB article. • An AD proxy-less deployment is also supported but not recommended; it may result in increased network bandwidth consumption and reduced performance.

- Installing an AD proxy on a Windows 2003 or Windows 2003 R2 domain controller is not supported. To monitor domain controllers running on Windows 2003 or Windows 2003 R2, install the AD proxy on another Windows Server running a higher Windows version. For the list of supported operating systems, see Supported Data Sources.

- If you're using an AD proxy to audit Group Policy Object (GPO) change events, the Windows Server on which the AD proxy is installed needs to meet the following requirements:
  - Must have the Group Policy Management Console (GPMC) installed

  - Cannot run a Windows Server Core operating system
  - Must have English as the operating system's primary language (the GPMC HTML-generated report must be in English)
- If you're not using an AD proxy to audit GPO change events directly from the Collector server, the Windows Server on which the Collector is installed must meet the requirements listed above for a Windows Server on which the AD proxy is installed.

Note:

- Event auditing is supported on the default domain's partition (default naming context) only.
- Monitoring two domains with the same NetBIOS name is not supported.

Network Requirements

- Depending on your topology and preferences, the AD proxy can be installed on one or more DCs, or on other Windows Servers. The most effective way to reduce network traffic is to install the AD proxy on the DCs themselves, so that the only network traffic to the Collector would be the event data after filtering and aggregation.
- To optimize for low latency, if the AD proxy cannot be installed on the DCs themselves, the AD proxy should be installed on Windows Servers in LAN-proximity of the DCs so that the event log data transfer will be restricted to within the LANs.
- When no AD proxy is used, to optimize for low latency it is recommended to install the Collector in LAN-proximity of the monitored DCs.
- Different AD data sources may be monitored by different Collectors (using different containers). This can help in distributing network traffic.
- Access to certain ports and URLs is necessary from the servers running the various Varonis modules to monitor. For more information about the required ports, click here.
- If you are using Windows Firewall and an AD Proxy is not used or installed on a server other than the Domain Controller, the following Windows Firewall rules must be allowed on the Domain Controller:
  - Remote Event Log Management (RPC-EPMAP)
  - Remote Event Log Management (RPC)

Varonis Service Account

Varonis requires a dedicated service account. The service account can be reused for multiple data source installations and configurations.

- Service Account Read Operations:
  - Traverse and enumerate files, folders, directory structures, users, and groups.
  - Gather data source, user, and group metadata as part of normal system operations.
- Service Account Write Operations:
  - Used for executing Varonis Policies, if policies are defined.

Required User Accounts

The following user accounts are required for deploying and monitoring AD. You can use separate service accounts within AD or combined into a single account. Ensure that each user has all the required permissions to support the desired functionality.

The following table describes a two-service account implementation.

Service Account	Varonis Functionality	Required Permissions for the Service Account
Varonis Proxy Installer[1]	AD proxy installation and upgrade	• If the AD proxy is installed on the DC, the user must be a member of the Domain Admins group; DCs do not support local admin accounts, hence connecting the user to the local Administrators group is not sufficient. • If the AD proxy is installed on a

Service Account	Varonis Functionality	Required Permissions for the Service Account
		Windows Server that is not a DC, the user must be a member of Domain Admins group, or a member of the Administrators group on the local server where the AD proxy is installed.
Varonis service account for read operations[2]	Connection from the Collector to the monitored DCs, for continuous account retrieval	• The user must be a member of the Domain Users security group
	Connection from the Collector to the monitored DCs, required for continuous directory structure and permissions retrieval	• The user must have permission to read all OUs and all objects within the OUs; especially for foreign security principals. Enable List contents and Read all properties. • The user must have permission to the System access control list (SACL). OR • The user should be a member of the

Service Account	Varonis Functionality	Required Permissions for the Service Account
		Account Operators security group
	Connection from the Collector or AD proxy to the monitored DCs, required for continuous event retrieval	A user who is either: • Assigned with the "Manage auditing and security log" security policy • A member of the Event Log Readers group To collect GPO changed events: • The user and the computer accounts (of the Collector or AD proxy) that are used to monitor the events must have read access on each GPO. Using the default GPO permissions ensures, by default, that the Authenticated Users group has Read permissions on each GPO. If the Authenticated Users permission was removed intentionally, remediate by doing one of the following:

Service Account	Varonis Functionality	Required Permissions for the Service Account
		• Assign the user and the computer accounts Read permissions on each GPO. • Assign the user and the Domain Computers group Read permissions on each GPO. • Create a group of all the computer accounts and assign this group and the user Read permissions on each GPO. You may need to restart the servers to update the new group membership. To connect from the Collector to the AD proxy and retrieve events: • Use the same account for account enumeration and the Varonis service account. Make sure

Service Account	Varonis Functionality	Required Permissions for the Service Account

		the user has these permissions:
		• A member of the VaronisEventsRetrieval group with permissions to read status, interrogate, query status, pause/continue, start/stop services on the Windows Server where the AD proxy is installed; the VaronisEventsRetrieval group should be configured as a Domain local (group scope) Security group (group type)
		• A member in any of these local or domain groups:
		  • Administrators
		  • Backup Operators
		  • Power Users local group - This option is available only when the AD proxy is not

Service Account	Varonis Functionality	Required Permissions for the Service Account
		installed on the DC.

Varonis service account for write operations	Data protection automations	• In addition to the requirements for the read operations, the Varonis service account requires domain permissions to create groups, remove groups, and add members to a group.
		• To add, remove, or modify a group under organizational units, the following permissions are required for the specific OUs containing the groups you intend to manage:
		  • Create, delete, and manage groups
		  • Modify the membership of a group
		• Disabling a user requires permission to modify the userAccountControl attribute. The "create, delete, and manage user

Service Account	Varonis Functionality	Required Permissions for the Service Account
		accounts" delegation is required for the OUs.

Notes:

1. The Varonis Proxy Installer user is defined in Management Console > Domain Properties > Domain Controllers > Manage Proxies > Proxy Information > Installation Credentials. For more information, see Configure domain controllers in Adding an AD Data Source.

2. The Varonis Admin user is defined in Management Console > Domain Properties > General > Domain User Credentials. For more information, see Adding an AD Data Source.

Event Auditing Requirements

The following steps are mandatory to audit AD events:

1. Enable event auditing for everyone in the domain:
   a. Select Start > Administrative Tools > Active Directory Users and Computers.
   b. To ensure advanced features are enabled, select View > Advanced Features.
   c. Right-click the domain's root and select Properties. The Properties dialog box is displayed.
   d. In the Security tab, click Advanced. The Advanced Security Settings dialog box is displayed.
   e. In the Auditing tab, select the Everyone auditing entry and click Edit. The Auditing Entry dialog box is displayed.

      Note: If there is no such entry, you must add it.

   f. From the Type dropdown list, select All to audit both Success and Failure events.
   g. From the Applies to dropdown list, select This object and all descendant objects.
   h. In the Permissions area, select the Full Control checkbox.

> Important: This does NOT grant the Everyone group any permissions. Rather, it adds actions made by all users to the Windows audit log, thus enabling Varonis to read from the log.

i. In the Permissions area, clear the List contents, Read all properties, and Read checkboxes to reduce the number of events recorded in the event log.

j. In the Properties area, select Write all properties.

k. Clear the Only apply these auditing settings to objects and/or containers within this container checkbox.

2. Allow Varonis access to the security event log:

> Note: Once applying the configurations, additional events will be logged. Therefore, it is recommended to increase the security log size to at least 512 MB. Only this log should be increased.

a. For environments on which all the monitored DCs are on Windows Server 2008 and higher, add the Varonis user to the built-in Event Log Readers domain group.

b. For environments with at least one DC on Windows Server 2003, click here for instructions.

Verifying Audit Policy Requirements and Minimums

Varonis relies on the proper configuration of Active Directory audit policies for full functionality. Your environment will likely already have an audit policy being applied to domain controllers. Varonis recommends identifying this policy before moving forward to ensure you are making changes to the proper group policy object (GPO) and the proper setting hive (Local vs Advanced).

1. To best identify this, we recommend using the Group Policy Results Wizard tool remotely against a DC. This wizard is located within the Group Policy Management Console. For more information, see this KB article.
2. Once the policy result loads, inspect the Local Security Policy > Security Settings > Local Policies > Security Options > Audit: Force audit policy subcategory settings....
   a. Verify the "winning GPO". This is commonly the Default Domain Controllers Policy but it may have been changed at one point. All subsequent changes to the audit policies should only be done within this winning GPO.
   b. Verify the active Audit Policy hive. You only need to configure the relevant policy.

> Note: For more information about the differences between the two, see this Microsoft article.

i. If the above setting is set to Enabled, proceed to fulfill the Advanced Audit Policy Requirements and set the minimum parity.

ii. If the above setting is set to Disabled, proceed to fulfill the Local Audit Policy Requirements and set the minimum parity.

Advanced Audit Policy Requirements

Before you begin, ensure you have identified the active auditing hive. See Verifying Audit Policy Requirements and Minimums.

> Important: For the Audit: Force audit policy subcategory settings... setting:
>
> - Enabling Force Advanced Audit is strongly recommended. Failure to do so may lead to potential conflicts with other settings.
> - If this setting is enabled, Local Audit Policies will not work.

1. From within the Group Policy Object you identified earlier, go to Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration.
2. Ensure that the following configurations are set as a minimum:

Policy Path	Enable Success/Failure
Account Logon > Credential Validation	S + F
Account Logon > Kerberos Authentication Service	S + F
Account Logon > Kerberos Service Ticket Operations	S + F
Account Management > Audit Computer Account Management	S

Policy Path	Enable Success/Failure
Account Management > Audit Distribution Group Management	S
Account Management > Audit Security Group Management	S
Account Management > Other Account Management Events	S
Account Management > User Account Management	S + F
DS Access > Audit Directory Service Access	S
DS Access > Audit Directory Service Changes	S
Policy Change > Audit Policy Change	S
Policy Change > Authentication Policy Change	S
Policy Change > Authorization Policy Change	S
Policy Change > Other Policy Change Events	F
Policy Change > MPSSVC Rule-Level Policy Change	S
Object Access > Other Object Access Events	S

Policy Path	Enable Success/Failure
Object Access > Certification Services	S
Logon/Logoff > Audit Logoff	S
Logon/Logoff > Audit Logon	S
Logon/Logoff > Other Logon/Logoff Events	S
Logon/Logoff > Special Logon	S
System > Other System Events	S + F
System > Security State Change	S
System > Security System Extension	S
System > System Integrity	S + F

Local Audit Policy Requirements

Before you begin, ensure you have identified the active auditing hive. See Verifying Audit Policy Requirements and Minimums.

Important: For the Audit: Force audit policy subcategory settings... :

- If this setting is not enabled, Advanced Auditing will not apply. Failure to do so may lead to potential conflicts with other settings.
- If this setting is enabled, Local Audit Policies will not work.

1. From within the Group Policy Object you identified earlier, go to Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policies. The audit policies are displayed in the right pane.

2. Set the following policies to Success:
   - Audit logon events
3. Set the following policies to Success and Failure:
   - Audit account logon events
   - Audit account management
4. At the command prompt, execute the following on all monitored domain controllers to enable the Directory service changes audit events (5136, 5137, 5139, 5141):

   Note: The `auditpol` command enables you to implement changes to the granular audit policy, and set changes only to the specific subcategory instead of the entire category. Alternatively, you can set the parent category to "success" by using `gpmc.msc`, but pay attention that setting the entire category instead of the subcategory will add load to the security event log.

   Important: If you do not execute the `auditpol` command, some of the DS events and certain threat models will be missing from Varonis.

5. At the command prompt for all domain controllers, execute the following:

```
gpupdate /force
```

6. At the command prompt, execute the following on all monitored domain controllers:

```
auditpol /set  /subcategory:"Directory Service Changes","
Audit Policy Change","Authentication Policy Change","Auth
orization Policy Change","Other Object Access Gzirxw?$?Ei
vxm gation Services","Security State Change","Security Sy
stem Extension" /success:enable
```

```
auditpol /set /subcategory:"Other Policy Change Events","
User Account Management" /failure:enable
```

```
auditpol /set /subcategory:"Other System Events","System
Integrity" /success:enable /failure:enable
```

7. To enable domain and machine events, at the command prompt for all domain controllers, execute the following:

```
gpupdate /force
```

Operational NTLM Event Auditing

Follow the steps below to collect NTLM authentication events from the NTLM operational event log, located under: `Event Viewer (Local)\Applications And Services Logs\Microsoft\Windows\NTLM\Operational.` (To configure NTLM authentication event auditing from the security log, see step 3 above.)

Note:

- Microsoft NTLM Operational log events do not have any indication of failure or success. Nevertheless, these events are presented in Varonis with the status "success". The actual event status is reflected in the corresponding "Account authentication (TGT)" event based on Microsoft event ID 4776.
- It is recommended to increase the NTLM operational event log size to at least 512 MB to prevent event loss due to temporary service outage and increase robustness.

1. Go to Forest > Domains > <Domain Name> > Group Policy Objects > Edit Default Domain Controllers Policy > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options.
2. The following security policies support auditing NTLM. To enable the deepest level of auditing, including both workgroup and domain authentication attempts that use NTLM, set the following:
   a. Network security: Restrict NTLM: Audit NTLM authentication in this domain = Enable all
   b. Network security: Restrict NTLM: Audit Incoming NTLM Traffic = Enable auditing for all accounts

For Environments with At Least One DC on Windows Server 2003

1. Check the setting values:
   a. Open RSOP or export via `gpresult /h gpresult.html` on a DC machine, using administrator credentials.

b. Go to Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment and open the Manage auditing and security log setting. The list of the permitted users and groups is displayed.

> Note: All the users and groups which are currently defined must also be defined in the GPO you set.

2. Add the Varonis user.

> Note: If the Varonis user is already in the above list (or is member of a group in the list), then Varonis already has access to the event viewers and there is no need to continue this procedure to change the setting.

Do one of the following:

- Preferred option - Add the Varonis user to the GPO which defines the setting (see the Source GPO column in RSOP/gpresult.html – usually the Default Domain Controllers Policy).
- Add the Varonis user to another GPO. In this case, ensure the GPO you are defining actually takes effect (for each setting, only the strongest GPO which defines that setting takes effect; it overrides default or other GPO values for that setting):
  - Ensure it is at the highest level in the order of GPOs.
  - Verify that other GPOs are not enforced.

> Important: Be sure to add all the users listed in the RSOP or gpresult.html in step 1 above.

3. Recheck the setting values (using RSOP or gpresult.html):
   - Check the setting values to make sure that none of the previously defined users or groups were overridden.
   - Ensure that the Varonis user is present in the list.
4. Execute the `gpupdate /force` command on all the domain's global catalogs (GC) to apply the setting.
5. Ensure that the Collector has connected successfully to the domain's GC and events are gathered correctly.

What To Do Next

Now that you've fulfilled the requirements, proceed to add an AD data source.

Adding an AD Data Source

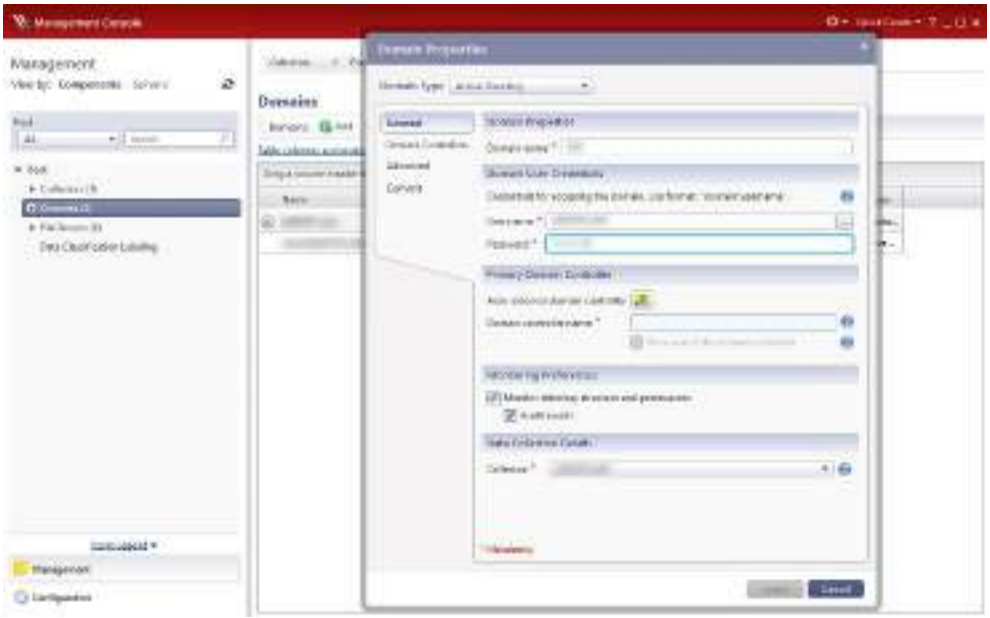
After the required Collectors are installed, you must add an Active Directory (AD) data source; it is required to resolve the AD users and groups who have permissions to the data stored in other monitored data sources.

Note: Each AD data source represents a monitored AD domain. In some cases, the Varonis UI displays the term Domain instead of Data Source. To monitor multiple AD domains, add an AD data source per AD domain.

1. Add an AD data source

You can add an AD data source and configure related settings, including properties, user credentials, and Collector details.

1. In the Management Console, select Management > Components > Root > Domains, and on the toolbar, click Add.
   The Domain Properties window is displayed, showing the General pane.



2. Select Active Directory as the Domain Type if it is not already selected.
3. In the Domain Properties area, set the following parameters:
   - Domain name - Type the name of the AD domain you want to monitor.

     Note:

- This option is read-only if you are editing an existing AD data source.

4. Specify the Domain User Credentials:
   - User name - Set the name of the user that can access the AD domain. Use the format domain\username. This is the VaronisAdmin user described in Required User Accounts in AD Requirements.

     Note:
     - To monitor accounts, the user must be a member of the Domain Users security group.
     - To monitor directory structure and permissions, the user must have permission to read all OUs and the system access control list (SACL), or be a member of the Account Operators security group.

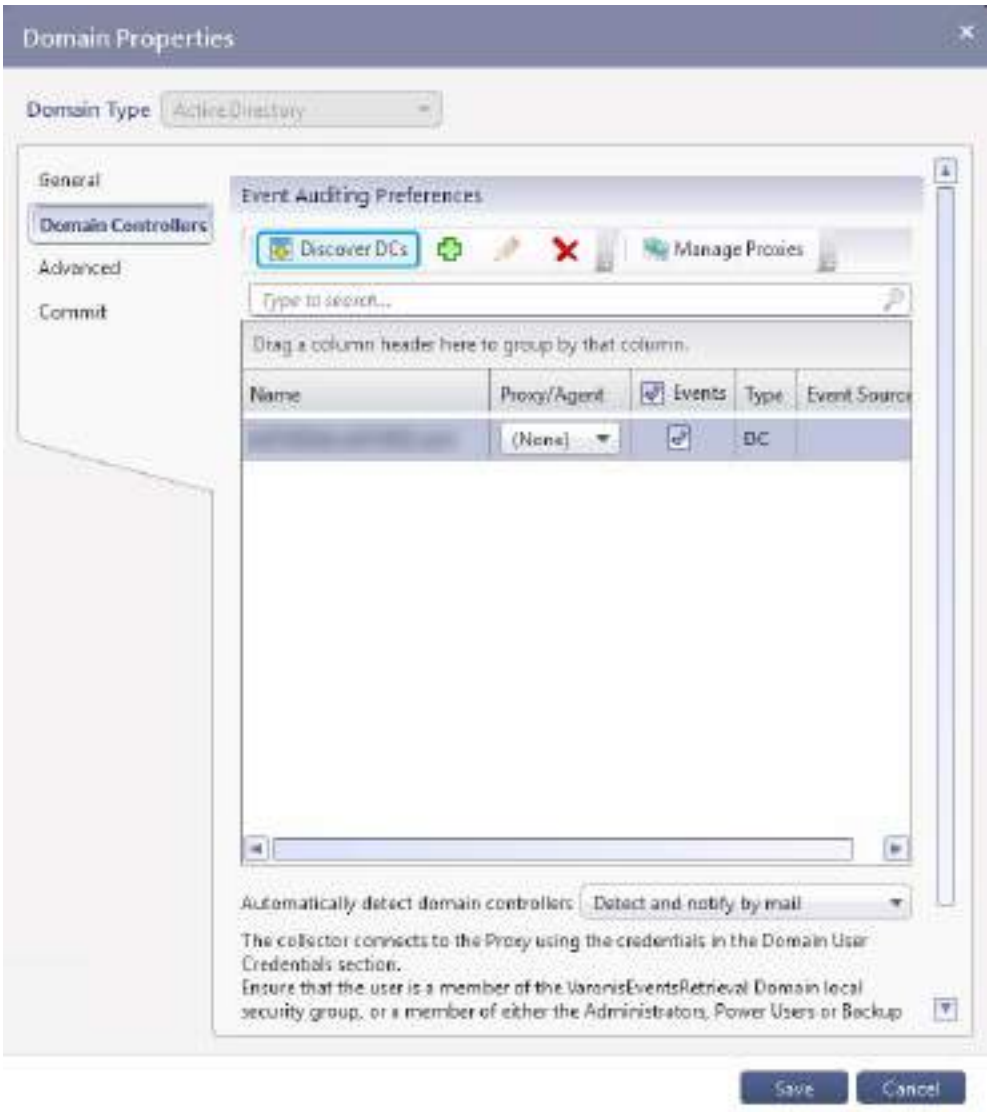
   - Password - Type the user's password.
5. Set the Primary Domain Controller to be used for monitoring the domain's accounts, directory structure, and permissions:
   - Auto-discover domain controller - Click the button to automatically discover the domain controller.
   - Domain controller name - If you didn't click the Auto-discover domain controller button, type the AD domain controller server name. Alternatively, enter the user credentials described above, then fill in any computer name in the AD domain and click the Auto-discover domain controller button to auto-discover the domain controller.
   - Force use of this domain controller - Select this checkbox to force Varonis to connect only to the domain controller specified above. When selected, only this domain controller will be used to monitor the domain's accounts, directory structure, and permissions. If the connection to the primary domain controller fails, the respective data will not be monitored. If cleared, Varonis will try to connect to other available DCs.
6. In the Monitoring Preferences area, choose whether to monitor the AD structure and permissions and audit AD events (these are selected by default for licensed users, otherwise they are unselected). Set the following options:
   - Monitor directory structure and permissions - Select this checkbox to enable monitoring the AD structure and permissions.
   - Audit Events - Select this checkbox to audit AD events. This option is only available if the Monitor directory structure and permissions option is selected. Event auditing can be enabled only if DCs are configured, so make sure to

configure at least one DC in the Domain Controllers tab (see Configure domain controllers).

7. In the Data Collection Details area, select the relevant Collector from the dropdown list.

2. Configure domain controllers

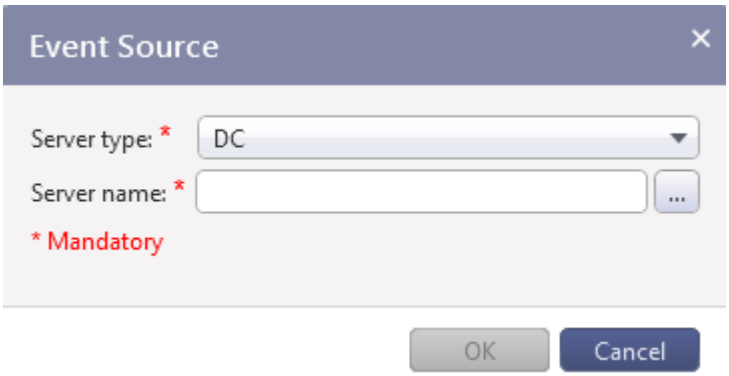
1. On the left menu, select Domain Controllers.
   The domain controller settings are displayed.



2. Do one of the following:
   - Click Discover DCs to auto-discover all the domain controllers in the domain.

Note: Events are not audited for domain controllers that are not listed in the table or have their Events checkbox cleared. To optimize for low latency and reduced network bandwidth consumption, make sure to assign AD proxy to each domain controller.

- Click Add to add additional domain controllers one by one. Any domain controller in the AD domain can be added.
  The Event Source dialog box is displayed, where you can choose which source to monitor. The options are DC (default) or WEF.



In the Server name field, you can browse to select an available server.
(Optional) Configure Windows Event Forwarding: If you want to monitor AD but do not allow Varonis direct access to the domain controller, you configure Windows Event Forwarding so that all the events are forwarded to one centralized Windows Server, the Windows Event Collector (WEC) server. The event auditing service on the Collector server will connect only to this Windows Server and monitor AD events there. For more information about Windows Event Forwarding, see this Microsoft article.

Note:

- Before you configure WEF, first remove all forwarding DCs from the list, if they appear. In the Domain Controllers grid, select the forwarding DC, and on the Domain Controllers toolbar, click Remove .
- There is no way to monitor part of the logs on the DC and another part on the WEC. If you decide to set up WEF on the DC, all monitored event sources such as security, system, NTLM, and monitored events will be forwarded.

Windows Event Forwarding deployment requires the following:

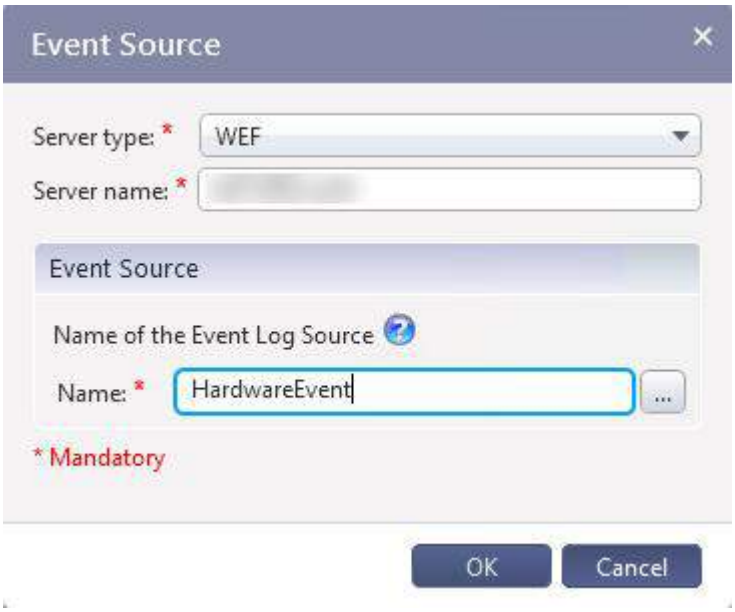
- WEF is configured on the Domain Controller (DC).

- The Windows Event Collector (WEC) is on the same domain as the monitored DCs.
- Each forwarding DC should forward the events to a WEC server on the same domain as the DC.
- Multiple WECs are supported; that is, different DCs may forward events to the different WECs on the same domain.
- There are sufficient permissions for successful event forwarding so that forwarded events appear on the WEC.
- The event log name key exists in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog` in the WEC registry.
- The service account needs to be a member of the Event Log Readers group on the WEC (not in "Active Directory Users and Computers").
- You will need to forward the security, system, and NTLM logs, preferably from each DC to a separate log (to reduce load). Do not forward logs from multiple domains into the same log.
- A minimum DC security log size is recommended.
- (Recommended) Set the content format of the WEF subscription to "Events" instead of the default "Rendered Text" to reduce the event size.

To configure Windows Event Forwarding, set the following parameters:

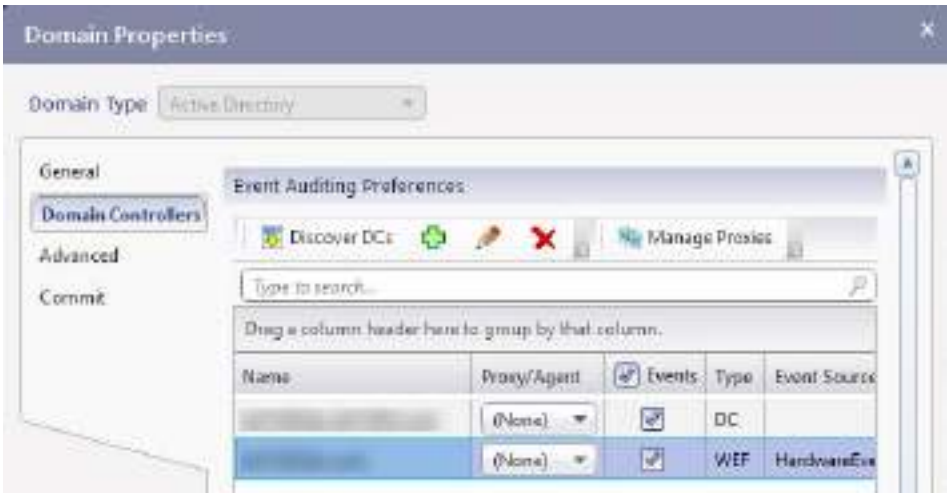
- Server type - Select WEF
- Server name - Type the WEC FQDN.
- Event Source Name - Click the Browse button (...) to select the name (If the event source does not appear in the list, check if the registry key exists on

the WEC), or type the Event Log Source name directly in the Name field.



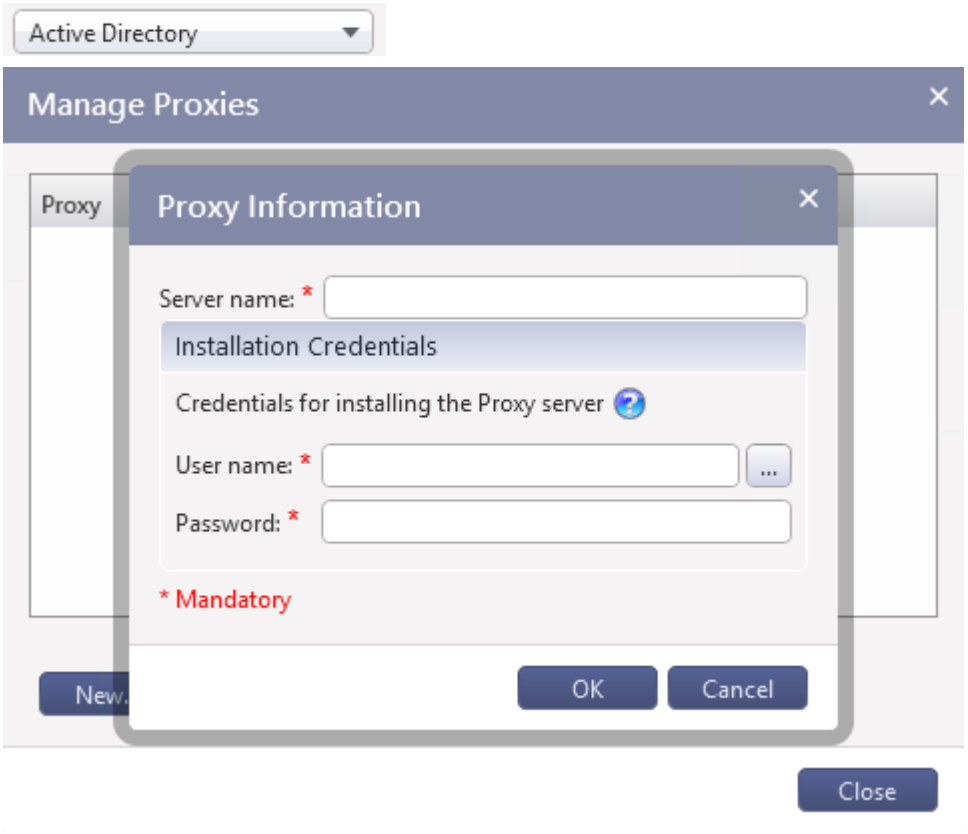
If the provided event log is not found in the WEC (either the event log is missing or there is an accessibility problem such as connectivity or insufficient permissions), a warning message will be displayed.

Upon configuration completion, the WEF hostname will be displayed in the DC grid.



The WEF can be monitored with an AD proxy. The configuration process is the same as for DCs. On the Collector and AD proxy, the relevant information regarding WEF will be displayed in the Varonis event log.

3. Click Manage Proxies on the toolbar to configure an AD proxy for AD event auditing.
   The Manage Proxies dialog box is displayed, where you can click New to add a new AD proxy. Set the relevant parameters in the Proxy Information dialog box.



For the required permissions for installing the AD proxy, see Required User Accounts in AD Requirements.

4. From the Automatically detect domain controllers dropdown list (located at the bottom of the Domain Controllers pane), select an option to set the system behavior when a domain controller is added to or removed from a domain. Options include:
   - Detect and notify by mail - New and deleted domain controllers are detected and email notifications are sent. This is selected by default.
   - Detect and monitor automatically - New and deleted domain controllers are detected and new domain controllers are automatically monitored by Varonis.
   - Detect, notify and monitor automatically - New and deleted domain controllers are detected, email notifications are sent, and new domain controllers are automatically monitored by Varonis.
   - Never - New and deleted domain controllers are not detected.

3. Configure advanced monitoring preferences

1. On the left menu, select Advanced.

The Advanced Monitoring Preferences are displayed.



2. Select the Enable RFC 2307 checkbox to enable using LDAP as a Network Information Service (NIS) for SID resolution, according to the RFC 2307 memorandum.
3. From the Group types dropdown list, select Only Security Groups to limit the group monitoring to only security groups, or select All (the default option) to monitor all groups, including distribution groups.

4. (Optional) Customize domain commit credentials

1. On the left menu, select Commit.
   The domain commit settings are displayed.

2. (Optional) Clear the Use domain user credentials checkbox to use different commit credentials than those defined for the domain user and enter the relevant username and password.

   Note:

   - If credentials were not entered but the checkbox was cleared, the domain user credentials in the General pane will be used instead.
   - If the Collector is in a lower version than 8, the domain user credentials will be used.

3. In the Group OU area, if required, choose a different OU from that defined in the data source's domain.

5. Install the data source

After configuration is complete, click Install to add the AD data source.

A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the Domains pane. When the installation completes, the status shows "Installed 100%".

What To Do Next

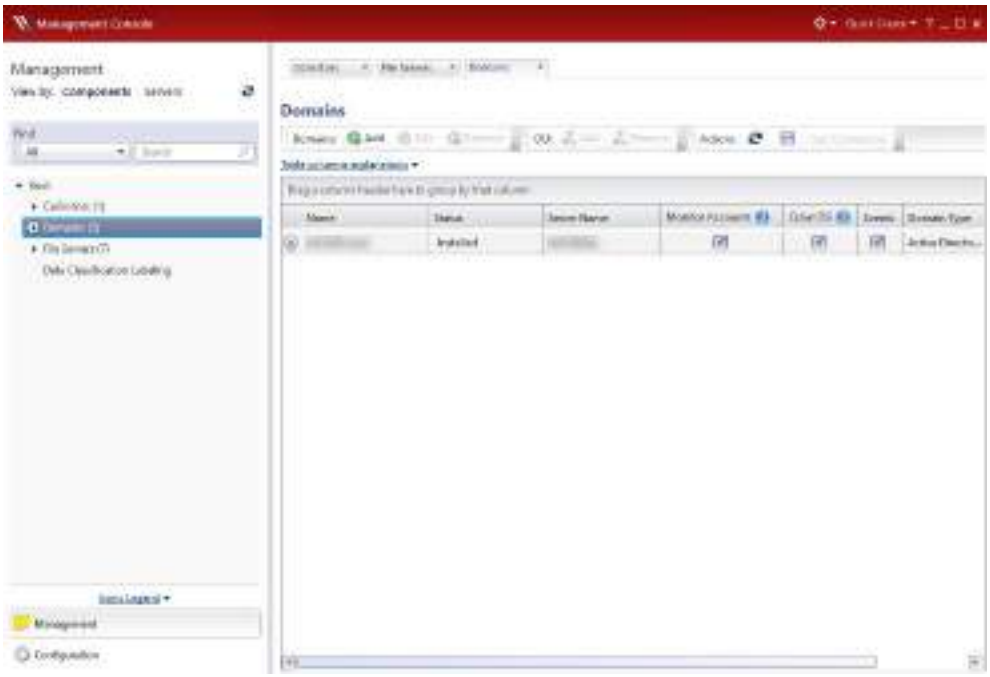
Now that you've added an AD data source, you can proceed to add additional data sources for monitoring. See the relevant monitored data source section for instructions.
Next, take a look at how to edit and remove an AD data source.

Editing and Removing an AD Data Source

You can edit and remove an AD data source and container.

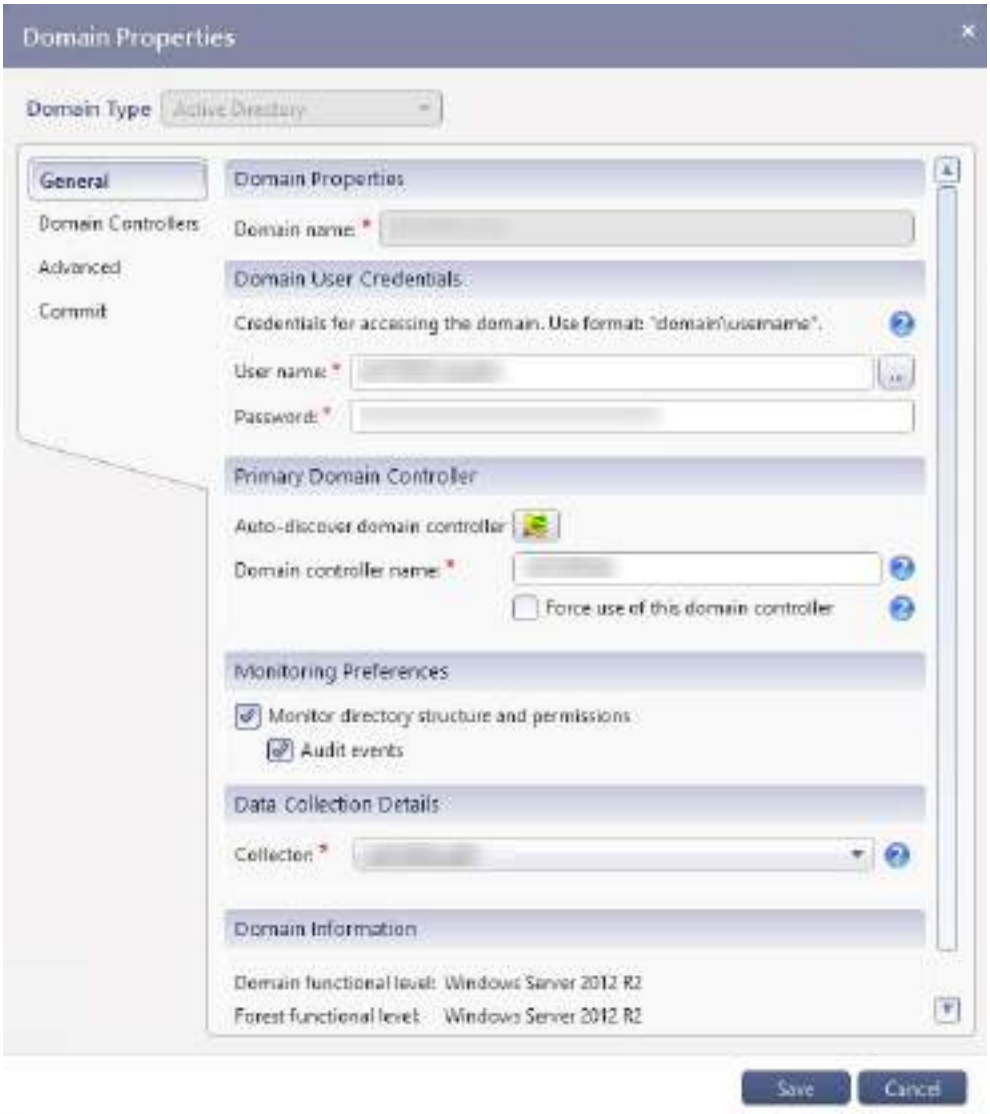
Editing an AD Data Source

1. In the Management Console, select Management > Components > Root > Domains.
   The Domains pane is displayed on the right.
2. In the grid, select the Monitor Accounts checkbox of the required AD data source to make sure Varonis monitors the user, group, and computer accounts from the specified AD data source.



3. To edit an AD data source, double-click its row, or select the AD data source and click Edit on the toolbar.

The Domain Properties window is displayed, where you can edit the AD data source as required.



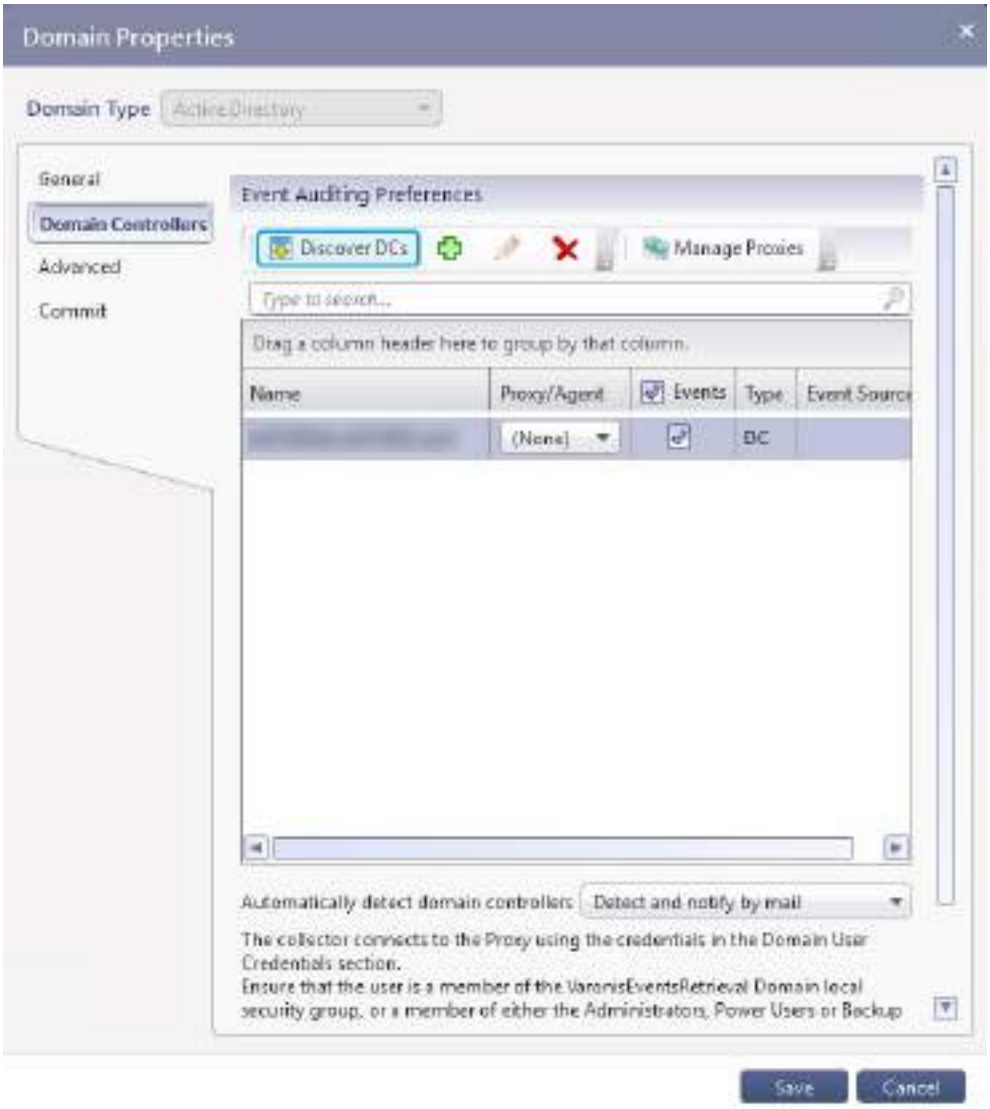
Removing an AD Data Source

1. In the Management Console, select Management > Components > Root > Domains.
   The Domains pane is displayed on the right.
2. In the grid, select the AD data source you want to remove, and on the Domains toolbar, click Remove .
   The Delete Domain confirmation window is displayed.
3. Click Yes.

The selected AD data source is removed.

Removing a Domain Controller

1. In the Management Console, select Management > Components > Root > Domains and on the toolbar, click Edit.
   The Domain Properties window is opened to the General pane.
2. On the left menu, select Domain Controllers. The domain controller settings are displayed.



3. In the grid, select the domain controller you want to remove, and on the Domain Controllers toolbar, click Remove .

A confirmation window is displayed.

4. Click Yes.
   The selected domain controller is removed.

What To Do Next

Now let's take a look at how to add and remove organizational units.

Adding and Removing Organizational Units

The addition of an OU allows you to limit the account monitoring service to a specific OU. If you define an OU, events that don't belong to the OU will be filtered out.

Adding Organizational Units

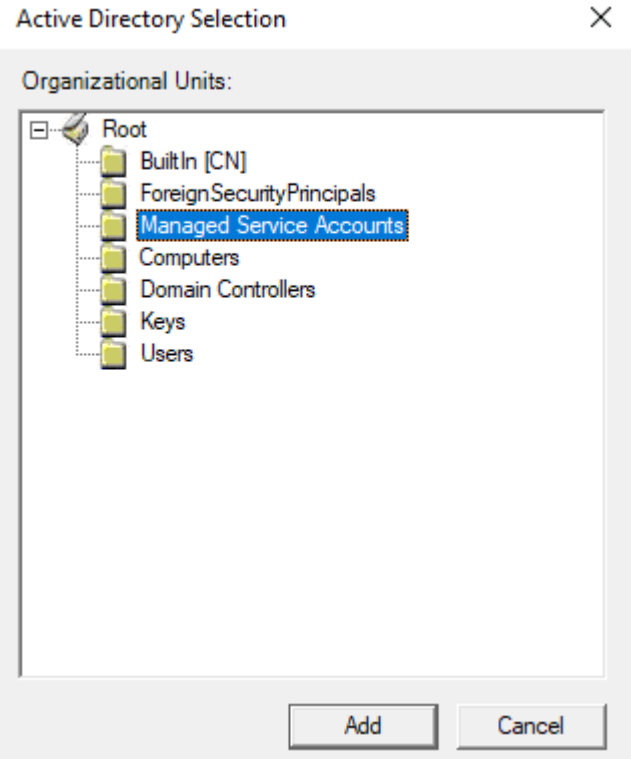
If you select an OU, only that OU is monitored. If you don't select an OU, the entire AD data source is monitored.

1. In the Management Console, select Management > Components > Root > Domains.
   The Domains pane is displayed on the right.
2. Select the AD data source on which you want to monitor specific OUs.
3. On the OU toolbar, click Add.
   The Domain User Credentials dialog box is displayed.

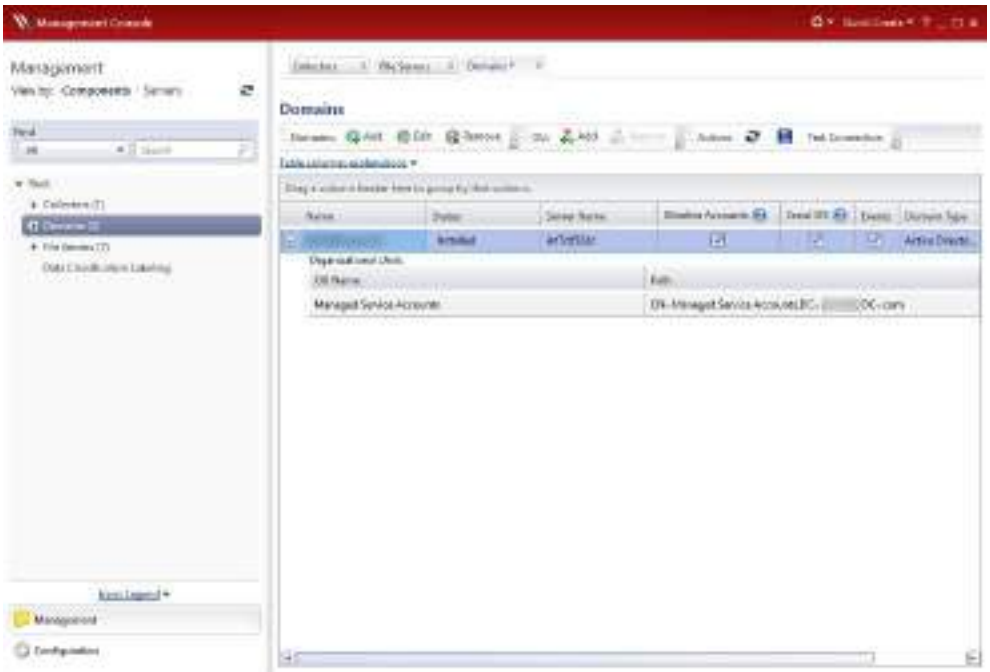


4. Enter the Varonis service account password, and click OK.

The Active Directory Selection dialog box is displayed.



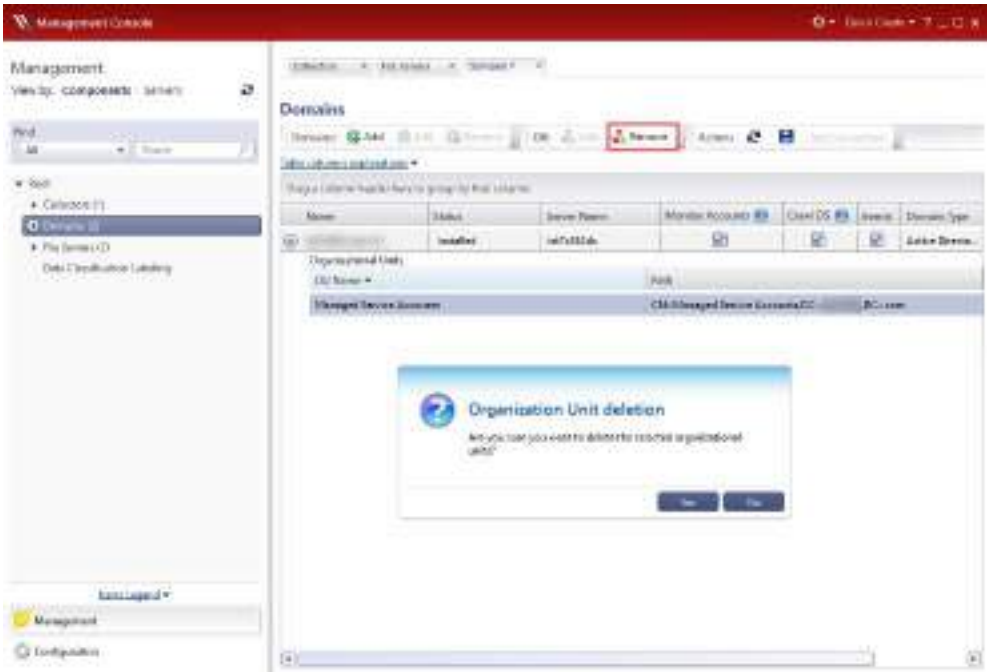
5. Select the required OU from the list, and click Add
   The OU is added to the AD data source and the dialog box is closed. In the grid, click the dropdown arrow in the Name column to view the OU.



Removing Organizational Units

The definition of an OU can be removed from Varonis without affecting the OU itself.

1. In the Management Console, select Management > Components > Root > Domains > <domain name>, where <domain name> is the name of data source from which you want to remove the OU.
   The <Domain Name> pane is displayed on the right.
2. In the Name column in the grid, click the dropdown arrow.
   All of the data source's OUs are listed.
3. Select the OU you want to remove, and on the OU toolbar, click Remove.
   The Organization Unit Deletion confirmation window is displayed.



4. Click Yes.
   The selected OU is removed.

What To Do Next

Now let's take a look at the supported AD events.

Supported AD Events

Mapping to Microsoft Event IDs

AD event auditing relies on Microsoft's event logs. The following table lists the mapping between the supported Varonis AD events and the corresponding Microsoft event IDs.

Note: Due to standard Microsoft behavior, Modified events may be recorded for all the fields in a modified object, not only those that were changed; also, when an AD object is created, many Created and Modified events are recorded on the object's fields.

Event	Microsoft Event ID	Notes
Access renewal (TGS renewal)	4770	
Access request (TGS request)	4769	
Account authentication (TGT)	4768, 4771,4776	
Account disabled	4738, 4742	
Account enabled	4738, 4742	
AD replication	4662	This event identifies an AD replication activity. The event is generated when one or more of the following AD Extended Rights attempted to be exercised: DS-Install-Replica, DS-Replication-Manage-Topology, DS-

Event	Microsoft Event ID	Notes
		Replication-Get-Changes-All.
DC account logon	4624	
DS object created	5137	
DS object deleted	4726, 5141	
DS object membership added	4728, 4732, 4746, 4751, 4756, 4761	
DS object membership removed	4729, 4733, 4747, 4752, 4757, 4762	
DS object modified	5136, 4742 (pwdLastSet)	
DS object moved	5139	
DS object renamed	5136	
NTLM Access Request	8004, 8006	
Ticket Without Requestor	5077	
Ticket Requestor Mismatch	5078	
User password changed	4723	
User locked out	4740	There may be duplicate lockout events, since

Event	Microsoft Event ID	Notes
		the lockout events may be registered in the Security log on one Primary Domain Controller (PDC) or on two domain controllers (on a PDC and on another domain controller) due to the nature of the authentication process. All failed logon attempts get forwarded to the PDC Emulator (PDC) in the domain. This means that whenever an account is locked out, a PDC of your domain registers an account lockout event in the Security log. For this reason, you might get two events on the same account lockout, generated from two different DCs. These two events will contain the same information, except for the Collection device host name that indicates the source DC.
User unlocked	4767	
Vulnerable Netlogon connection allowed by group policy	5830, 5831	

Event	Microsoft Event ID	Notes
Vulnerable Netlogon connection denied	5827, 5828	
Vulnerable Netlogon (deployment phase allowed)	5829	
GPO events		
GPO link created	5136	
GPO link deleted	5136	
GPO link modified	5136	
GPO settings modified	5136	
Permission events		
DS object permission added	5136	
DS object permission removed	5136	
Owner changed	5136	
Domain Events		
A replay attack was detected	4649	
A domain trust was created	4706	

Event	Microsoft Event ID	Notes
Domain trust was modified	4716	
DSRM administrator password was changed	4794	
Reset password attempt	4724	
SID History was added to an account	4765, 4766	
The password hash on an account was accessed	4782	
Trusted forest information entry was added	4865	
Trusted forest information entry was modified	4867	
Machine Events (related to the Domain Controller server only)		
Scheduled task was created	4698	
Scheduled task was updated	4702	
Scheduled task was deleted	4699	

Event	Microsoft Event ID	Notes
Scheduled task was enabled	4700	
Scheduled task was disabled	4701	
Audit Log was cleared	1102	
System time was changed	4616	
Service was installed	4697	
System audit policy was changed	4719	
Domain Policy was changed	4739	
Windows is starting up	4608	
Windows is shutting down	4609	
An authentication package has been loaded by the Local Security Authority	4610	
A notification package has been loaded by the Security Account Manager	4614	

Event	Microsoft Event ID	Notes
Auditing settings on an object were changed	4907	
Windows Firewall Service failed to start	5030	
Code integrity determined that the image hash of a file is not valid	5038	
GPO processing error	6145	
Monitored security event pattern has occurred	4618	
A user right was assigned	4704	
An account was mapped for logon	4774	
An account could not be mapped for logon	4775	
Special Groups Logon table was modified	4908	
Special groups have been assigned to a new logon	4964	
Role separation was enabled	4897	

Event	Microsoft Event ID	Notes
Kerberos policy was changed	4713	
A security setting was updated on the OCSP Responder Service	5124	
Admin object permission set was changed	4780	
An attempt was made to register a security event source	4904	Detects malicious activity on the Domain Controller involving volume shadow-copy.
A security package has been loaded by the local security authority	4622	Detects and notifies about potential attacks that involve adding a new Security Support Provider (SSP) to the Domain Controller, which could indicate an attempt to steal credentials.
A change has been made to Windows Firewall exception list. A rule was added.	4946	Detects and notifies about potential attacks involving firewall changes on the AD Domain Controllers.
A change has been made to Windows Firewall exception list. A rule was modified.	4947	Detects and notifies about potential attacks involving firewall

Event	Microsoft Event ID	Notes
		changes on the AD Domain Controllers.
A change has been made to Windows Firewall exception list. A rule was deleted.	4948	Detects and notifies about potential attacks involving firewall changes on the AD Domain Controllers.
Windows Firewall settings were restored to the default values	4949	Detects and notifies about potential attacks involving firewall changes on the AD Domain Controllers.
A Windows Firewall setting has changed	4950	Detects and notifies about potential attacks involving firewall changes on the AD Domain Controllers.

Note: Logoff events are not supported.

Domain and Machine Events

- Domain events:
  - Kerberos policy was changed
  - SID History was added to an account
  - User added to admin group
  - A replay attack was detected
  - Domain trust was created
  - Domain trust was modified
  - Attempt to add SID History to an account
  - The password hash on an account was accessed

  - DSRM administrator password change
  - Trusted forest information was added
  - Trusted forest information was modified
  - Kerberos service ticket was renewed

- Machine events (related to the domain controller server only):
  - Scheduled task was created
  - Scheduled task was updated
  - Scheduled task was deleted
  - Scheduled task was enabled
  - Scheduled task was disabled
  - Audit Log was cleared
  - System time was changed
  - Service was installed
  - System audit policy was changed
  - Domain Policy was changed
  - Windows is starting up
  - Windows is shutting down
  - Authentication package has been loaded
  - Notification package has been loaded
  - Auditing settings on an object were changed
  - Windows Firewall Service failed to start
  - Code integrity error
  - GPO processing error
  - Monitored security event pattern has occurred
  - A user right was assigned
  - An account was mapped for logon
  - An account could not be mapped for logon
  - Special Groups Logon table was modified
  - Special groups have been assigned to a new logon
  - Role separation was enabled
  - Cluster Shared Volume Functionality

Extended Properties

Extended properties are, in general, supported. However, the properties below are displayed as string data types and not dates. These properties can only be searched and sorted as strings:

- Account Expiration - The date on which the account expires
- Pwd Last Set - The date and time at which this account's password was last changed
- Last Logon - The last time the user logged on (this attribute is not replicated)
- Last Logon timestamp - The last time the user logged on (in the supported Windows Servers, this attribute is replicated; however, it is only updated when the user logs on if the old value is more than a configurable number of days in the past)
- Last logoff - The time at which the user last logged off

3 WINDOWS DATA SOURCES

What This Section Contains

This section describes how to deploy and monitor Windows sources; the requirements, deployment and configuration steps, and supported events.

What To Do Next

Before you dive in, click here to learn more about how Varonis monitors Windows accounts, directory structure and permissions, and events.

Windows Monitoring Overview

Note: Each Windows data source represents a monitored Windows Server. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source. To monitor multiple Windows Servers, add a Windows data source for each Windows Server.

Varonis monitors Windows Servers via the following parallel data streams.

Accounts

- Varonis enumerates local account information remotely from the Collector with a dedicated service account.

Directory Structure and Permissions

- Varonis collects folder structure, permissions, and metadata via a dedicated service for directory structure monitoring (FileWalk) that runs on the assigned Collector. The service can connect to the monitored Windows Servers directly or via a Windows agent service that is installed on the monitored Windows Server.
- When a Windows agent is installed, the directory structure and permissions monitoring service on the Collector connects to the agent service using Remote Procedure Call (RPC). The agent service, in turn, reads the directory structure and permissions locally from the Windows Server using WinAPI calls.
- When a Windows agent is not installed, the directory structure and permissions monitoring service on the Collector connects to the Windows Server directly and reads the directory structure and permissions data using Server Message Block (SMB). An agentless deployment is not recommended since it may result in increased network bandwidth consumption and reduced performance.
- When a Windows agent is installed, you will see the following services in Windows Services Manager on the monitored Windows Server:
  - Varonis FileWalk - The service that monitors the Windows directory structure and permissions
  - Varonis FileWalk Service Monitor - The service that monitors the agent's service health

  When the above services are running, you will see the following services in Windows Task Manager:
  - VrnsSvcFw - The agent service

- VrnsSvcFwMon - The service that monitors the agent's service health

For more information about the agent, see Configuring the Windows Data Source Following Deployment.

Data Classification and Labeling

- Varonis supports data classification and labeling on files that reside in the monitored data sources.

Events

- Varonis monitors Windows events using a dedicated event auditing service (Forwarder) that runs on the Collector. The service connects to a Windows agent installed on the monitored Windows Server.
- The Windows agent includes the following components, in addition to the abovementioned components used for monitoring directory structure and permissions:
  - A mini-filter driver (VrnsFilter) that transparently intercepts IRP (I/O Request Packet) packets occurring on the Windows Server and forwards them to a queue in memory. The driver is completely nonintrusive and transparent to ongoing Windows Server operations, with zero service degradation.
  - A service (VrnsCifsQueue) that continuously reads the events from the queue in memory and empties it. The service filters and aggregates the events and accumulates them in memory until they are read by the event collection service that runs on the Collector (Forwarder).
- When a Windows agent is installed, you will see the following services in Windows Services Manager on the monitored Windows Server:
  - Varonis Audit Event Service - The service that reads the events from the mini-filter driver
  - Varonis Audit Event Monitor - The service that monitors the health of the Varonis Audit Event Service

  When the above services are running, you will see the following services in Windows Task Manager:
  - VrnsCifsQueue - The service that reads the events from the mini-filter driver
  - VrnsMon - The service that monitors the VrnsCifsQueue service health

  Additionally, when running the `xqg` command, you will see `VrnsFilter` in the command output.

For more information about the agent, see Configuring the Windows Data Source Following Deployment.

What To Do Next

First, make sure you fulfill the Windows requirements.

Windows Requirements

License Requirements

Data Stream	Required License
Windows accounts	DatAdvantage for Windows
Windows directory structure and permissions	DatAdvantage for Windows
Windows events	DatAdvantage for Windows

Installation Requirements

The following Varonis components should be installed to deploy and monitor a Windows data source.

Data Stream	Required Installation
Accounts	• A Collector must be installed. • No Windows agent installation is required.
Directory structure and permissions	• A Collector must be installed. • A Windows agent of version 11.x or higher is required to be installed on the monitored Windows Server.

Data Stream	Required Installation
	• An agent-less deployment is also supported but not recommended; it may result in reduced performance.
Events	• A Collector must be installed. • A Windows agent of version 11.x or higher is required to be installed on the monitored Windows Server. • A Windows agent-less deployment is not supported.

- When a Windows agent is installed, it includes all components required to monitor both Windows directory structure and permissions, and Windows events.
- Each Windows data source can be monitored by both Varonis SaaS and Varonis self-hosted Data Security Platform simultaneously. That means that two types of Varonis Windows drivers are installed on the monitored Windows data source; a mini-filter driver (VrnsFilter) for the SaaS environment, and a legacy driver (sidfile) for the on-premises Data Security Platform environment. To facilitate such dual monitoring, an agent of version 11.x or higher must be installed on the monitored Windows Server. If one of the drivers had been removed manually (not recommended) and the second driver of the other environment (Varonis SaaS and Varonis self-hosted) had not been removed, the Windows data source will be monitored only by the environment of the corresponding installed driver. That means that even though a Windows agent is installed on the Windows Server, the Windows Server will be monitored only in one of the environments.
- To prevent Windows Agent issues on Windows Server 2012 R2, it is recommended to install Microsoft KB 4345424.
- Folder names are limited to 512 characters, just as in NTFS.
- Varonis monitors directory structure (folder hierarchy) and files identified as sensitive. For each folder and file, Varonis collects the name, creation, modification and access dates, size, and permissions. For folders, Varonis also collects the number of files. The data is enriched with additional insights such as the exposure level and last event time.

- Varonis requires domain-joined Windows data sources.

Network Requirements

- Access to certain ports and URLs is necessary from the servers running the various Varonis modules to monitor Windows. For more information about the required ports, click here.
- If you are using Windows Firewall, the following Windows Firewall rules must be allowed on the Windows data source:
  - Remote Scheduled Tasks Management (RPC)
  - Remote Scheduled Tasks Management (RPC-EPMAP)
  - File and Printer Sharing (SMB-In)

Varonis Service Account

Varonis requires a dedicated service account. The service account can be reused for multiple data source installations and configurations.

- Service Account Read Operations:
  - Traverse and enumerate files, folders, directory structures, users, and groups.
  - Gather data source, user, and group metadata as part of normal system operations.
- Service Account Write Operations:
  - Used for executing Varonis Policies, if policies are defined.

Requirements for Monitoring Local Service Accounts

Local service accounts are NT SERVICES that are defined on Windows Servers. Their SID starts with S-1-5-80, S-1-5-82 and S-1-15-3. Varonis collects local service accounts to resolve permissions and events associated with the accounts.

For monitoring local service accounts, the Varonis service account needs to be a local administrator or needs additional permissions. These can be added as follows:

1. From the Windows > Start menu, open the command prompt in Administrator mode.
2. Run the following command to get the user SID from the target system:

```
wmic useraccount where name="<FileWalk User>" get name,si
d
```

3. Store the user SID from step 2 in a handy location, for example:

```
S-1-5-21-3437249340-2515582971-2711699987-10114
```

4. Run the following command to get the current SDDL for the Service Control Manager:

```
sc sdshow scmanager > CurrentSDDL.txt
```

> Note: The above command will save the current SDDL for the SC Manager to the `CurrentSDDL.txt` file.

5. Store the current SDDL from step 4, for example:

```
D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCL
CRPWPRC;;;SY)(A;;KA;;;BA)(A;;CC;;;AC)(A;; CC;;;S-1-15-3-1
024-528118966-3876874398-709513571-1907873084-359 8227634
-3698730060-278077788-3990600205)S:(AU;FA;KA;;;WD)(AU;OII
 OFA;GA;;;WD)
```

6. Edit the following string to replace the new SDDL snippet using the SID you stored in step 3:

```
(A;; LCRC;;;<SID in step 3>)
```

   This includes Read and List children permissions. Add the SID in the above string to create a new SDDL snippet, for example:

```
(A;; LCRC;;;S-1-5-21-3437249340-2515582971-2711699987-101
1)
```

7. Add the above new SDDL snippet before word "S:" in the original SDDL that you stored in step 5, for example:

```
D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCL
CRPWPRC;;;SY)(A;;KA;;;BA)(A;;CC;;;AC)(A;; CC;;;S-1-15-3-1
```

```
024-528118966-3876874398-709513571-1907873084-359 8227634
-3698730060-278077788-3990600205)(A;; LCRC;;;S-1-5-21-343
7249340-2515582971-2711699987-1011)S:(AU;FA;KA;;;WD)(AU;O
II OFA;GA;;;WD)
```

8. Run the `sc sdset scmanager` with the updated SDDL that is created in step 7, for example:

```
:sc sdset scmanager D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;C
CLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)(A;;CC;;;AC)
(A;; CC;;;S-1-15-3-1024-528118966-3876874398-709513571-19
07873084-359 8227634-3698730060-278077788-3990600205)(A;;
 LCRC;;;S-1-5-21-3437249340-2515582971-2711699987-1011)S:
(AU;FA;KA;;;WD)(AU;OII OFA;GA;;;WD)
```

   Once the command in step 8 runs successfully, the below message will be displayed in the command prompt:

```
[SC] SetServiceObjectSecurity SUCCESS9
```

9. Delete the `CurrentSDDL.txt` file.

Varonis Service Account Required Permissions

The following service accounts are required for deploying and monitoring Windows. Ensure that each service account has all the required permissions to support the desired functionality.

User	Varonis Functionality	Required Permissions for the Varonis User
VaronisAgentInstaller[1]	Windows agent installation and upgrade	• A user who is a member of the Administrators group on the monitored Windows server

User	Varonis Functionality	Required Permissions for the Varonis User

Varonis service account for read operations[2]	Continuous retrieval of Windows accounts, directory structure and permissions, and event audit	• A user who is a member of either one of the following:
		  • Local Administrators group
		  • Local Power Users and Backup Operators groups[4]. In Windows Server 2022, the user should also be a member of the Access Control Assistance Operators group. Starting from Windows Server 2022, Power Users no longer have permission to view share metadata. Members of the Access Control Assistance Operators group can remotely query authorization attributes and permissions for data sources. The purpose of this group is to

User	Varonis Functionality	Required Permissions for the Varonis User

		grant non-administrators the option to query effective rights on files and shares.
		• For Windows Server 2016 and higher of Standard, Core, and Datacenter editions, do one of the following:
		  • (Recommended) Add the user to the local policy Network access: Restrict clients allowed to make remote calls to SAM.
		  • If the user is a member of the local Power Users and Backup Operators groups, add these groups to the local policy Network access: Restrict clients allowed to make remote calls to SAM.
		  • If the user is a member of the local Administrators

User	Varonis Functionality	Required Permissions for the Varonis User

		group, add this group to the local policy Network access: Restrict clients allowed to make remote calls to SAM.
		• If the Windows Server is also used as a domain controller:
		  • The user must be a member of the Server Operators and Backup Operators groups
		  • Automatic detection of Windows Servers 2016 and higher is possible only if the Active Directory Domain Services server role is installed on those Windows Servers
		• For Windows 2016 and higher Datacenter editions, additional permissions are required for the Varonis service

User	Varonis Functionality	Required Permissions for the Varonis User
		account. The user should be added also to the Access Control Assistance Operators or Print Operators groups. For more information, see NetShareEnum function (lmshare.h). • The Varonis service account requires Interactive Logon permissions on the Windows data sources being monitored.
Varonis service account for write operations[3]	Data protection automations	Same as the Varonis service account for read operations

1. The VaronisAgentInstaller user is defined in Management > Components > Root > File Servers > Common > Varonis Agent Installation > Agent Deployment Options > Agent Installation Credentials. For more information, see Adding Windows Data Sources - Detailed Procedure.

2. The Varonis service account for read operations is defined in Management > Components > Root > File Servers > Common > FileWalk Credentials. For more information, see Adding Windows Data Sources - Detailed Procedure.

3. The Varonis service account for write operations is defined in Management > Components > Root > File Servers > Commit > File Server Commit Credentials. For more information, see Adding Windows Data Sources - Detailed Procedure.

4. The Local Power Users and Backup Operators groups are required for monitoring Windows:

- Power Users group - Minimum mandatory requirement for Varonis to be able to perform share operations such as "netShareEnum" to retrieve the shares and their permissions, and to retrieve the volume cluster size for correct file sizing, and so on.
- Backup Operators group - Mandatory for directory structure monitoring, enabling read operations on files and folders to extract properties and permissions. This eliminates the need for explicit read ACE on all items in the data sources that Varonis monitors.

Event Auditing Requirements

- Some Windows events do not include an IP address. To enrich events that originate from a Windows Server with an IP address, ensure that the following Local Security Policy is set to Success on the Windows Server:
  - Audit logon events
- Windows Volume Shadow Copy Service (VSS) is supported for event auditing. The support for VSS is enabled by default and configurable. The configuration is preserved during upgrade.
- By default, the agent filters events done by well-known Security IDs (SIDs that have less than 10 characters). To turn off filtering, contact Varonis Support.
- When configuring a data source in the Management Console using an IP address, it is necessary for the Collector to resolve the IP address to a hostname. If the Collector can't resolve the IP to a hostname, add the IP-hostname mapping to the hosts file on the Collector (C:\Windows\System32\Drivers\etc\hosts).

Now that you've fulfilled the requirements, proceed to add a monitored Windows data source. First familiarize yourself with the deployment steps summary and then dive into the detailed procedure.

Adding Windows Data Sources - Summary

Now that you've fulfilled the requirements, you can deploy a Windows data source. This section summarizes the procedure for deploying Windows data sources in the Management Console.

1. Run the Management Console as an administrator.
2. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.

3. In the Resource Wizard's Common pane, specify the data source name, check the Collector selected by default and change it if needed, and enter the credentials for running directory structure monitoring (FileWalk).

   Important:

   - This account must have Backup Operator and Power User roles (Windows or NAS devices) on the data source during installation.
   - You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.

4. In the Resource Type area, select the data source type from the dropdown list. Then, click the Connect and verify link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

   Note:

   - The Connect and verify link is displayed only when all relevant data is entered.
   - A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

5. Select the relevant Varonis Agent Installation options, and click the Agent Deployment link to define the credentials used to install the agent on the data source.

   Note: The agent doesn't automatically update to new versions. If there's a new agent version, you have to update the agent manually on the Windows Server.

6. In the Monitored Shares area, select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source is installed and share detection is completed.
7. In the Configuration pane, review the Local Accounts, FileWalk Settings, and Event Auditing Parameters settings.

   Note:

   - If you change the FileWalk method, you will need to rescan the shares.

- The Varonis method runs the directory structure monitoring through the agent. This method only works if the agent is installed. An error will occur if this option is selected but there is no agent installed.
- The CIFS method uses the Common Internet File System (CIFS) protocol. The Varonis FileWalk agent need not be installed if CIFS is selected, since it uses the UNC path.

8. (Optional) In the Commit pane, clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials.

   Note:
   - If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
   - If the Collector is in a lower version than 8, the FileWalk credentials will be used.

   In the Group OU area, if required, select Uniquely defined to choose a different OU from that defined in the data source's domain.
9. After configuration is complete, click Install to add the data source.
10. (Optional) Enable SMB signing. Follow the steps described in Adding Windows Data Sources - Detailed Procedure.
11. After the data source installation and share detection are completed, in the Shares pane, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. If you chose to monitor selected shares, you can select and register the required shares.

What To Do Next

Now that you're familiar with the deployment steps, it's time to dive into the detailed procedure.

Adding Windows Data Sources - Detailed Procedure

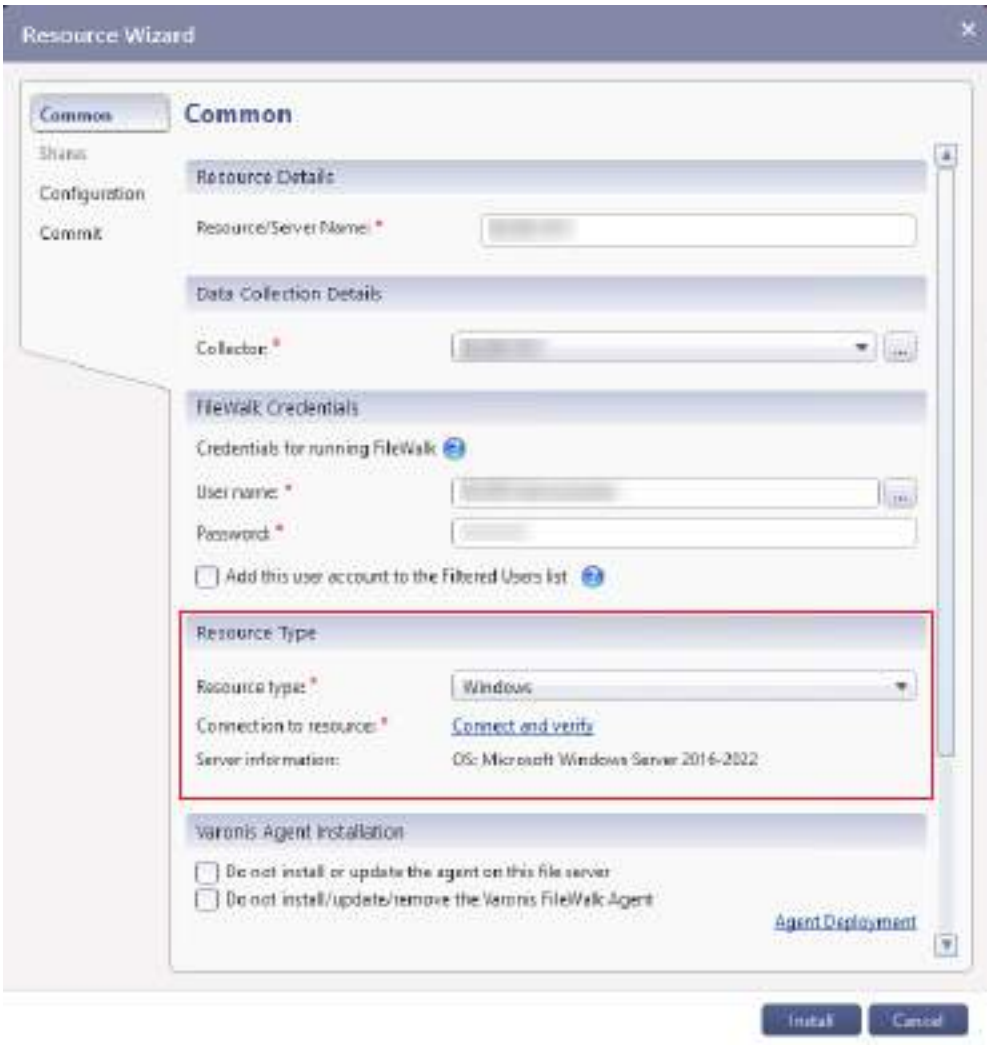
Now that you've fulfilled the requirements, you can deploy a Windows data source.

Note: Each Windows data source represents a monitored Windows Server. In some cases, the Varonis UI displays the term File Server or Resource instead of

Data Source. To monitor multiple Windows Servers, add a Windows data source per Windows Server.

1. Set common data source parameters

1. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.
   The Resource Wizard is opened to the Common pane, where you can specify the data source and set the relevant parameters.



2. In the Common pane, set the following parameters:
   a. Resource Details - Specify the data source name.
   b. Data Collection Details - Select the relevant Collector from the dropdown list.

c. FileWalk Credentials - Enter the credentials for running directory structure monitoring. File System operations include directory structure monitoring, event auditing (if set) and account enumeration on local accounts (if set).
   - This account must have Backup Operator and Power User roles (Windows or NAS devices) on the data source during installation.
   - These credentials are cached, so that they are automatically entered if another data source is added during the same session.
   - User name - Type the name of the user account to be used for directory structure monitoring, event auditing, and local account enumeration.
   - Password - Type the account's password.
   - Add this user account to the Filtered Users list - The defined user for FileWalk Credentials will be added to the filtered users list. If you clear this checkbox, a large number of events may be generated by the user defined for directory structure monitoring. It is recommended to keep this checkbox enabled.

   Important: You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.

d. Resource Type - Select the data source type from the dropdown list.
   - Connect and verify - Click this link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

     Note:
     - The Connect and verify link is displayed only when all relevant data is entered.
     - A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

e. Varonis Agent Installation

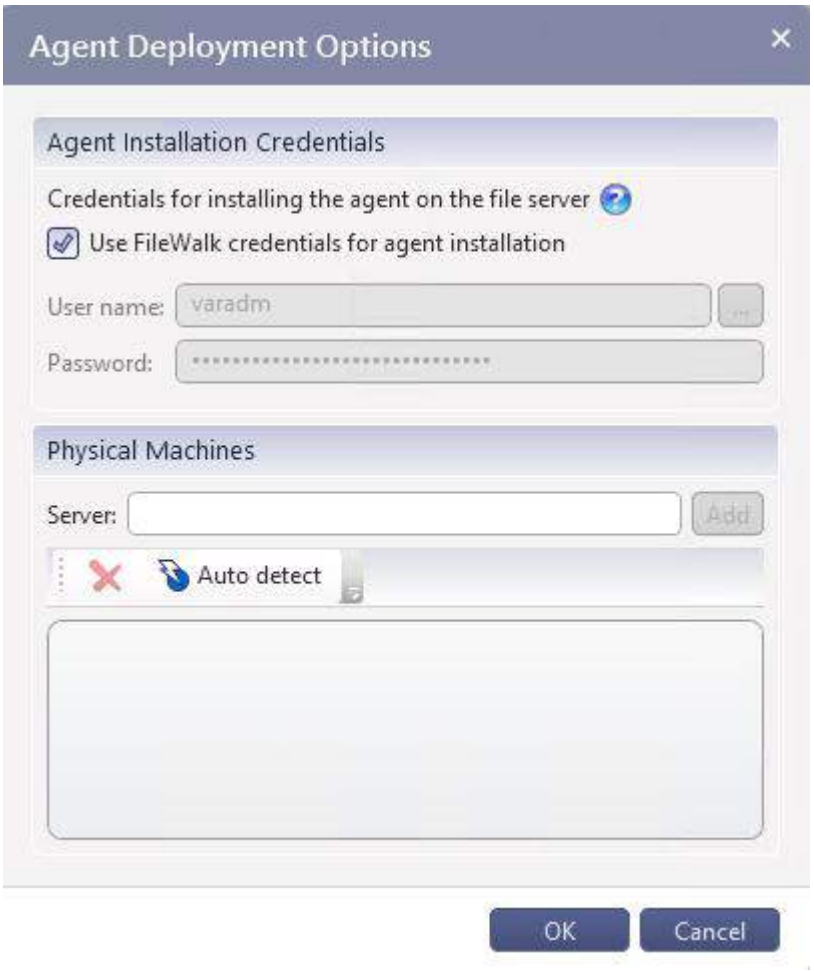
   Note:
   - For Windows 2008/2008 R2, you need to manually install the agent. Download the Windows agent from My Downloads on varonis.com (located under EventsCollection > Varonis.Agent.Setup.2008.x64) and install it on your Windows data source.

- If you're using the FileWalk method, then you'll need to also deploy the FileWalk agent manually.

- Do not install or update the filter agent on this server - Select this checkbox if you do not want the Varonis filter agent automatically installed or updated on the data source.
- Do not install/update/remove the Varonis FileWalk agent - Select this checkbox if you do not want the Varonis FileWalk agent automatically installed, updated, or removed from this data source.
- Agent Deployment - Click this link to define the credentials used to install the agent on the data source.

  Note: For existing data sources already deployed in Varonis SaaS, if a new agent version is released, you need to update the agent manually on the Windows Server. The agent doesn't automatically update to new versions.

The Agent Deployment Options window is displayed.



- Agent Installation Credentials
  - Use FileWalk credentials for agent installation - Select this checkbox to install the agent using the same credentials as the FileWalk Credentials.

    Note: If you select this option, ensure that the specified account has the required permissions for installing the agent on the file system.
  - User name - Type the agent installation account's user name.
  - Password - Type the agent installation account's password.

f. Monitored Shares - Select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source installed and share detection is completed.

- Automatically monitor detected shares - Select this option to automate monitoring for all detected shares. Share monitoring will automatically start after the data source installation is completed. Varonis will monitor all shares that aren't marked as "ignored". When this option is selected, click the Advanced setting link to modify share detection preferences. By default, the option is set to Prefer regular shares over equivalent admin shares. In this case, an admin share that has an equivalent regular share will be marked as "ignored" and the equivalent regular share will be detected for monitoring. Note: Any change in the monitored shares configuration, including the detection method, admin shares configuration, and selected shares, requires rerunning the resource detection.
- Monitor selected shares - This option is selected by default. You can manually select the shares to be monitored only after the data source is installed and share detection is completed. You'll need to open the Edit window for the installed data source and select the shares. For more information, see Post-installation share detection and registration.

Once the above settings are configured, you can proceed to review and adjust configuration settings.

2. Review and adjust configuration settings

1. On the left menu, click Configuration and confirm the information.
   The general configuration settings are displayed.
2. In the Local Accounts area, review the options:
   - Collect information regarding local accounts from this file server - Select this checkbox to collect user accounts from this file system.
3. In the FileWalk Settings area, review the options:
   - Identify actual unique folders and file system inconsistencies - Select this checkbox (if it's not already selected) to detect broken permissions in NTFS file systems.
   - FileWalk Method - Select the method to be used for directory structure monitoring. If you change the method, you will need to rescan the shares.
     - Varonis - A method of running directory structure monitoring through the agent. This method only works if the agent is installed.
       - An error will occur if this option is selected but there is no agent installed.
       - Cluster installation - If the Varonis FileWalk method is selected, the agent must be installed on all nodes.

Note: When monitoring resources within a Windows cluster, enter the cluster role name as the resource within the Management Console rather than the hostnames of the individual cluster nodes.

- CIFS - Uses the Common Internet File System (CIFS) protocol. The Varonis FileWalk agent need not be installed if CIFS is selected, since it uses the UNC path.

4. In the Event Auditing Parameters area, review the options:
   - Port in use - The port through which the Varonis agent on the data source communicates with the Collector.
   - Filter out false "File Opened" events - Open events may be triggered unintentionally for a variety of reasons, resulting in inaccurate analysis of file system access. Select this option to filter such unintentional Open events and gather Open events only if enough file content is actually read. Small files and certain operations may still trigger Read events.
   - Collect Access Denied events - Select this checkbox to audit events in which an attempt was made to access an entity by a user with insufficient credentials.
     - Include denied attempts to open folders - Select if preferred.

       CAUTION: Selecting this option may result in the creation of a large number of false access denied events.

Note:
Servers may have duplicate SIDs. This is common when the machine you are adding has been cloned from another machine and was not system-prepared (via the `Sysprep` command) prior to deployment. It might have been cloned from a machine already being monitored, or perhaps both servers were cloned from an original one and neither of them was system-prepared.

You can add the data source with the duplicated SID. You will be able to audit events and crawl the server for directory structure and permissions. However, you cannot collect local account information on any machines that have matching SIDs in Varonis.
By default, the option to Collect information regarding local accounts from this file server will be cleared if there is already a machine with that SID being monitored; when two machines have duplicate SIDs, there is no way for Varonis to identify the machine from which those local accounts came.

The duplicate machine will have a fake SID entry in the VarVaronisonis Domain database. It is possible to switch which machine has the fake entry and the real

entry by enabling advanced features in the Management Console. Contact Varonis Support for assistance.

3. (Optional) Customize commit credentials

You can use different commit credentials instead of the default FileWalk credentials.

1. On the left menu, select Commit.
   The commit settings are displayed.
2. (Optional) Clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials. (By default, this checkbox is selected to use the FileWalk credentials, and the User name and Password fields are disabled for editing.)

   Note:
   - If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
   - If the Collector is in a lower version than 8, the FileWalk credentials will be used.
3. In the Group OU area, if required, select Uniquely defined to choose a different OU from that defined in the data source's domain. Click the Browse button (...) to select the required OU.

4. Install the data source

After configuration is complete, click Install to install the data source.

A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the File Servers pane. When the installation completes, the status shows "Installed 100%".

5. (Optional) Enable SMB signing

The Data Security Platform supports SMB signing in SMB versions 2 and 3.

SMB signing (also known as security signatures) is a security mechanism in the SMB protocol. SMB signing means that every SMB 3.1.1 message contains a signature that is generated by using the session key and the Advanced Encryption Standard (AES)

algorithm. The client puts a hash of the entire message into the signature field of the SMB header.

If someone changes a message during transmission, the hash will not match, and SMB will know that someone tampered with the data. The signature also confirms the sender's and receiver's identities. This breaks relay attacks.

To enable SMB signing for a Windows data source:

1. Disable SMB1 on the server side (Windows data source):
   - In PowerShell call “Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol ”.
   - For additional methods to disable SMB1, see the following Microsoft article.
2. Enable SMB signing on the server and client sides (Windows data source and Collector or DSP Server in case of a consolidated setup). Set the following Local Security Policies to Enabled:
   - Local Policies > Security Options > Microsoft network client: Digitally sign communications (always)
   - Local Policies > Security Options > Microsoft network server: Digitally sign communications (always)

   For more information on the Local Security Policy for SMB signing, see the following Microsoft article.

6. Post-installation share detection and registration

After the data source installation and share detection are completed, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. The following procedure describes the manual registration and automatic share detection flows.

> Important: If after the data source is installed, share detection fails for any reason, the Share Detection Status column will remain "In Progress" until the issue is fixed, and share detection completes successfully at least once.

After the data source is installed, the Shares pane is enabled, and you can view the share settings.

1. On the left menu, click Shares.
   The share settings are displayed. The pane's heading indicates the option you selected when adding a data source.

2. In the Available Shares area, you can filter the shares based on the reason they are not registered for monitoring and easily identify the shares that can be added. The default filter is Accessible Shares. You can change the filter to see the rest of the shares. Options include:
   - Accessible shares - Can be added for monitoring (this option is selected by default)
   - Ignored shares - Are marked as "ignored"
   - Incompatible and inaccessible shares - Cannot be monitored since the exposed protocol does not match the security style of the volume (relevant to multiprotocol platforms only) or the Varonis service account does not have access to this share
   - Child share of a monitored share - Is monitored via its parent folder
3. Do one of the following:
   - If you chose to monitor selected shares, in the Available Shares area, select the required shares and click the down arrow. The selected shares are moved to the Registered Shares area. (The registered shares list is empty until you make your selections.)
   - If you chose to automatically monitor detected shares, Varonis will monitor all shares that aren't marked as "ignored". The automated share detection runs every few hours. The Registered Shares area is autopopulated with the shares to be monitored.
4. For each share, review and set the following information as required:
   - Ignore Detection - Select the shares to be ignored (and not be the subject of automatic detection and notifications) by the data source monitor.
   - Events - Select this checkbox to audit events for the share.
   - Crawl - To enable or disable monitoring for the share, in the Crawl column, select the relevant option.

     Note: You can also right-click the grid and select the required options for event auditing and crawling.
5. In the Additional Share Settings area, review the options:
   - Remove deleted shares - Select this checkbox to remove deleted shares. Shares that were deleted from the data source will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the data source is unavailable, the shares will not be removed.
   - Enable event auditing - Select this checkbox to audit events from all shares added from this data source.

After share detection and registration are completed, the status and number of registered volumes are respectively displayed in the Share Detection Status and Registered Shares columns in the File Servers pane.

What To Do Next

Now that you've added the Windows data source, go ahead and configure services related to the Varonis agent, namely the Varonis Audit Event Service and Varonis Audit Event Monitor.

Configuring the Windows Data Source Following Deployment

After deployment of the Windows data source, the following configurations related to the Varonis agent can be configured in case some issues arise.

Services can be configured through the Registry Editor (from the `Start` menu, select Run > regedit.

All the relevant registry keys are located at:

`HKEY_LOCAL_MACHINE\SOFTWARE\VARONIS`

Configuring the Varonis Audit Event Service (vrnsCifsQueue)

To configure the Varonis Audit Event Service (vrnsCifsQueue), set the following in the registry key:

- QueueSize - Set the number of Common Internet File System (CIFS) events that can be stored in a queue. If the maximum number is reached, new events are not queued until the buffer is cleared.
- BypassMonitor - When set to 1, VaronisCifsDevice can be started without the monitor.

Configuring the Varonis Audit Event Monitor (vrnsmon)

To configure the Varonis Audit Event Monitor (vrnsmon), set the following in the registry key:

- CpuThreshold - The threshold for CPU deviation (set by the Deviation parameter), in percentages. The default is 10.
- Deviation - The number of continuous loops (set by the Interval parameter) on which the monitored service has passed its CPU threshold. The default is 10.

- Interval - The interval, in milliseconds, between monitored service polls. The default is 1000.
- MailFrom - The email address from which alerts are sent. The default is data source@varonis.com.
- MailTo - The email addresses of alert recipients. Several alert recipients can be defined. Recipient addresses must be comma-delimited. The default is, for example, employee@varonis.com.
- SMTP - The SMTP server.
- MemoryThreshold - The threshold for the monitored service's memory usage. If the monitored service passes this threshold, the monitor terminates the service. The default is 32M.
- MonitoredService - The name of the service to be monitored. The default is VaronisCifsDevice.
- MonitoredServiceExe - The name of the executable file to be monitored. The default is vrnsCifsQueue.exe.
- Path to VaronisMsg.dll in the registry - `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Eventlog\Varonis\VaronisC` and `VaronisMonitor` default path values are located under the `CategoryMessageFile` and `EventMessageFile` keys, with the default path `\SystemRoot\System32\VaronisMsg.Dll`.

What To Do Next

Now let's take a look at the supported events for the monitored Windows data sources.

Supported Events For Windows Data Sources

SMB (CIFS) Events for Windows Data Sources

> Note: SMB v2 and v3 are supported.

Event Auditing Method

Local file system filter

Supported File Operations

- File created

- File deleted
- File modified
- File opened
- File renamed
- Folder created
- Folder deleted
- Folder renamed
- Owner changed
- Permissions added
- Permissions removed
- Protection added
- Protection removed

Access Denied Events

- File deleted
- File opened
- Folder deleted
- Folder opened - only logged if it's triggered by security permissions, not by share permissions
- File/Folder set security

File Opened Events

File opened events may be triggered for a variety of reasons, resulting in inaccurate analysis of file system access.

What Triggers a File Opened Event

- Opening or accessing a file
- Copying a file - The copy creates a File opened event, and the paste creates a File created event.

What Does Not Trigger a File Opened Event

- Copying a file that is empty (0 KB in size) will not create a File opened event. There is no content to read.

What Can Cause a False File Opened Event

- Windows search
- Hovering over the file (to see the preview)
- Right-clicking the file and viewing the properties and metadata
- Single-clicking the file

What Causes a File Open - Access Denied Event

- An account tries to access the file but does not have the permissions to do so.

Unintentional File Opened Events

- To reduce unintentional File opened events, there is an option in the Management Console to filter out false File Opened events.
- File opened events are triggered only if enough file content is actually read. For threshold details, see the table below.

Thresholds

File opened events are triggered only if a sufficiently large portion of the file in question is read. Thresholds are:

File Size	Portion Read
8 KB	100%
16 KB	100%

File Size	Portion Read
32 KB	81%
64 KB	75%
128 KB	87%
1 MB	50%
4 MB	31%
16 MB	15%
256 MB	3%
1 GB	3%
4 GB	3%

4 AMAZON FSX FOR WINDOWS DATA SOURCES

Note: Private Preview. If you'd like to use Amazon FSx for Windows, contact your Sales Engineer.

What This Section Contains

This section describes how to deploy and monitor Amazon FSx for Windows sources; the requirements, deployment and configuration steps, and supported events.

What To Do Next

Before you dive in, click here to learn more about how Varonis monitors Amazon FSx for Windows accounts, directory structure and permissions, and events.

Amazon FSx For Windows Monitoring Overview

Note: Private Preview. If you'd like to use Amazon FSx for Windows, contact your Sales Engineer.

Note: Each Amazon FSx for Windows data source represents a monitored Amazon FSx for Windows Server. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source.

Varonis monitors Amazon FSx for Windows via the following parallel data streams.

File System

- Varonis collects folder structure, permissions, and metadata via a dedicated service for directory structure monitoring (FileWalk) that runs on the assigned Collector. This connection is made over SMB.

Events

- Varonis monitors Amazon FSx for Windows events using a dedicated event auditing service (Forwarder) that runs on the Collector.

What To Do Next

First, make sure you fulfill the Amazon FSx for Windows requirements.

Amazon FSx For Windows Requirements

Note: Private Preview. If you'd like to use Amazon FSx for Windows, contact your Sales Engineer.

Varonis Service Account

Varonis requires a dedicated service account. The service account can be reused for multiple data source installations and configurations.

- Service Account Read Operations:
  - Traverse and enumerate files, folders, and directory structures.
  - Gather data source metadata as part of normal system operations.

Varonis Installation and Requirements

- A Varonis Collector is required.
- For event auditing, deploy the AWS cloud infrastructure with the CloudFormation script automatically or manually. For more information, see Upload an AWS CloudFormation template and deploy a cloud infrastructure and (Optional) Manually Setting up Amazon FSx for Windows/Varonis Environment on AWS.

Requirements for the Varonis Service Account for Read Operations

- Automatic – The user must be a member in the Delegated Administrators group.

What To Do Next

Now that you've fulfilled the requirements, proceed to configure event auditing.

Configuring Event Auditing for Amazon FSx for Windows Data Source

Prior to adding Amazon FSx for Windows data sources, configure event auditing.

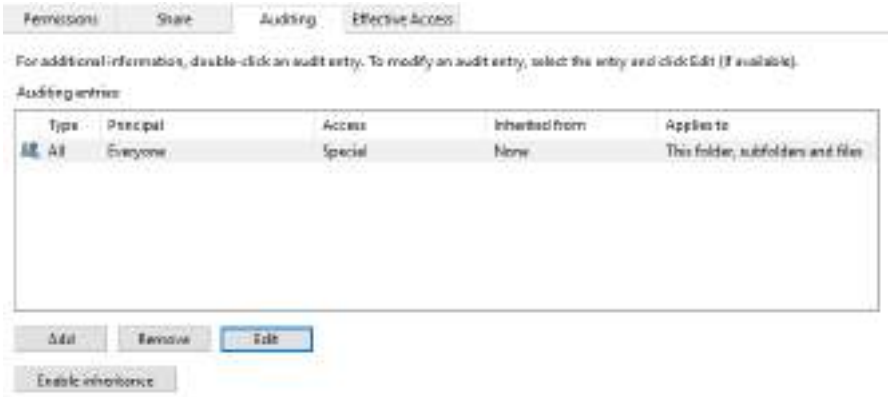
> Note: Private Preview. If you'd like to use Amazon FSx for Windows, contact your Sales Engineer.

1. Set audit controls on files and folders

You need to set audit controls on the files and folders that you want audited for user access attempts. Audit controls are also known as NTFS system access control lists (SACLs).

You configure audit controls using the Windows-native GUI interface or programmatically using Windows PowerShell commands. If inheritance is enabled, you typically need to set audit controls only on the top-level folders for which you want to log accesses.

1. Right-click the share root folder and select the Properties > Security > Advanced > Auditing tab.



2. Click Add, select a principal (like "Everyone"), and select the desired settings.



2. Upload an AWS CloudFormation template and deploy a cloud infrastructure

You can use the Management Console to generate a script or you can manually set up an AWS environment for event auditing.

After you've generated the script, follow the steps below to run the script in your AWS environment to deploy the components required for event auditing.

> Note: If you don't want to use a script, you can manually configure event auditing.

1. Open your AWS Management Console and go to CloudFormation.
2. Click Create stack > With new resources (standard).
3. Click Upload a template file, then click Choose file, and select the CloudFormation template.



4. Click Next.
5. You can choose to Roll back all stack resources which is the default option.
6. Click Next.
7. (Optional.) If your organization requires tags, you may enter them at this point. You can also leave them blank.
8. At the bottom of the page, click I acknowledge that AWS CloudFormation might create IAM resources with custom names. The acknowledgment is required when creating a CloudFormation stack using the AWS console.
9. Click Submit.
10. This will take you to the CloudFormation stack status page, showing the stack creation in progress.
    a. Click the Events tab.
    b. Any errors encountered during the creation of the stack will be listed in this tab.
    c. When the CREATE_COMPLETE status is displayed, then you are finished with this step.
11. Deployment will finish in about a minute.

3. Enable file access auditing (AWS FSx)

After you've deployed the cloud infrastructure (step 2 above), follow the steps below to enable file access auditing.

1. Open the Amazon FSx console.
2. Navigate to File systems and choose the Windows file system for which you want to manage file access auditing.
3. Click the Administration tab.

4. On the File Access Auditing panel, click Manage.
5. In the Manage file access auditing settings dialog box, edit the desired settings, and select the Kinesis Data Firehose that was created earlier as the destination.



6. Click Save.

What To Do Next

Now that you've configured event auditing for Amazon FSx for Windows, it's time to add a monitored Amazon FSx for Windows data source. First familiarize yourself with the deployment steps summary and then dive into the detailed procedure.

(Optional) Manually Setting up Amazon FSx for Windows/Varonis Environment on AWS

If you're deploying an AWS CloudFormation script, you can skip this section. Follow the steps below to manually set up an AWS environment for event auditing. This procedure can be used instead of deploying an AWS CloudFormation script. Perform this step before adding an Amazon FSx for Window data source in the Varonis Management Console.

Note: Private Preview. If you'd like to use Amazon FSx for Windows, contact your Sales Engineer.

1. Create an AWS bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console.
2. In the left navigation pane, choose Buckets.
3. Choose Create bucket.
   The Create Bucket page is displayed.
4. For Bucket name, enter a name for your bucket.
   The bucket name must:
   - Be unique within a partition. A partition is a grouping of regions. AWS currently has three partitions: aws (Standard Regions), aws-cn (China Regions), and aws-us-gov (AWS GovCloud (US) Regions).
   - Be 3-63 characters long.
   - Consist only of lowercase letters, numbers, dots (.), and hyphens (-). For best compatibility, we recommend that you avoid using dots (.) in bucket names, except for buckets that are used only for static website hosting.
   - Begin and end with a letter or number.
5. For Region, choose the AWS region where you want the bucket to reside.
6. Under Object Ownership, choose ACLs disabled.
7. Under Block Public Access settings for this bucket, choose Block all public access.
8. Under Bucket Versioning, choose Disable.
   a. Under Default encryption, choose Amazon S3 managed key (SSE-S3).
   b. Under Bucket Key, choose Enable.
   For more information, see Step 1: Create your first S3 bucket - Amazon Simple Storage Service.

To set life cycle configuration on a bucket:

1. Sign in to the AWS Management Console and open the Amazon S3 console.

2. In the Buckets list, choose the name of the bucket for which you want to create a lifecycle rule.
3. Choose the Management tab, and choose Create lifecycle rule.
4. In Lifecycle rule name, enter a name for your rule.
   The name must be unique within the bucket. For example: ExpirationInDays.
5. To apply this lifecycle rule to all objects in the bucket, choose This rule applies to all objects in the bucket, and choose I acknowledge that this rule applies to all objects in the bucket.
   a. Under Lifecycle rule actions, choose Expire current versions of objects.
   b. Days after object creation: 1.
   c. Click Save.

2. Create a role for an AWS service

1. Sign in to the AWS Management Console and open the IAM console.
2. In the navigation pane, choose Roles, and then choose Create role.
3. Select Custom trust policy.
   a. Select AssumeRole.
   b. Add a principal, select AWS Services “firehose.amazonaws.com”.
   c. Create Rule.
   d. Under Roles, select the role from the last step and click Add permissions – Create inline policy.
   e. Select JSON.
   f. Replace the bucket name with your bucket name, copy and paste to the Policy editor.

```
{

    "Version": "2012-10-17",

    "Statement": [

        {

            "Action": [
```

```
                "s3:GetObject",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::[your bucket name]",
                "arn:aws:s3:::[your bucket name]/*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

4. Click Create Policy.

3. Create a stream via the AWS Management Console

1. Sign in to the AWS Management Console and open the Kinesis Data Firehose console.
2. Choose Create Delivery Stream.
3. On the Destination page, choose the following options:

- Source – Choose Direct PUT.
- Destination – Choose Amazon S3.
- Delivery stream name – Type a name for the delivery stream. The name of the Kinesis Data Firehose delivery stream must begin with the "aws-fsx-" prefix.
- S3 bucket – Choose an existing bucket.
- S3 prefix – Leave this field empty.

4. In the Advanced settings, choose the existing IAM role and select the role that was created in "Create a role for an AWS service" above.
5. Choose Create Delivery Stream.
   For more information, see Step 1: Create your first S3 bucket - Amazon Simple Storage Service.

4. Create OpenID Connect (OIDC) identity providers

Note: This procedure is needed only when using the Managed Identity option in the Management Console.

1. Sign in to the AWS Management Console and open the IAM console.
2. In the navigation pane, choose Identity providers, and then choose Add provider.
3. For Configure provider, choose OpenID Connect.
4. For the Provider URL, type the URL of the IdP: https://sts.windows.net/7d43e2cb-4b86-4bfa-8bc9-2124c4df7608/. This ID is the Varonis Tenant ID from the Management Console.
5. Choose Get thumbprint to verify the server certificate of your IdP.
6. For Audience, type the client ID of the application that you registered with the IdP: https://management.azure.com.
7. Verify the information that you have provided. When you are done choose Add provider.
8. In the navigation pane, choose Roles, and then choose Create role.
9. Select Web identity.
10. Select the identity provider: https://sts.windows.net/7d43e2cb-4b86-4bfa-8bc9-2124c4df7608/. This ID is the Varonis Tenant ID from the Management Console.
11. Audience - https://management.azure.com.
    a. Click Next, then Next.
    b. Specify the Role Name.

c. Create Role.

To embed an inline policy for a role:

1. In the navigation pane, choose Role.
2. In the list, choose the name of the role from the last step to which you want to embed a policy.
3. Choose the Permissions tab.
4. Choose Add permissions and then choose Create inline policy.
5. Select JSON.
6. Replace the bucket name with [your bucket name], copy and paste to the Policy editor.

```
{

    "Version": "2012-10-17",

    "Statement": [

        {

            "Action": [

                "s3:GetObject",

                "s3:GetBucketLocation",

                "s3:ListBucket",

                "s3:ListBucketMultipartUploads"

            ],

            "Resource": [

                "arn:aws:s3:::[your bucket name]",
```

```
                "arn:aws:s3:::[your bucket name]/*"

            ],

            "Effect": "Allow"

        }

    ]

}
```

7. Under Trust relationships, click Edit trust policy and modify it according to the following:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Federated": "arn:aws:iam::[AWS Account I
D]:oidc-provider/sts.windows.net/[Varonis Tenant ID]/"
            },
            "Action": "sts:AssumeRoleWithWebIdentity",
            "Condition": {
                "StringEquals": {
                    "sts.windows.net/[Varonis Tenant ID]/
:aud": https://management.azure.com,
                    "sts.windows.net/[Varonis Tenant ID]/
:sub": "[Varonis Managed Identity ID]"
                }
            }
        }
```

```
        ]
}
```

8. Click Update Policy.

5. Create and view your access key ID and secret access key (existing user)

Note: This procedure is needed only when using the Access Key/ID option in the Management Console.

1. Sign in to the AWS Management Console and open the IAM console.
2. In the navigation pane, choose Users.
3. Choose your IAM user name (not the checkbox).
4. Open the Security credentials tab, and then choose Create access key.
5. To see the new access key, choose Show. Your credentials resemble the following examples:
   - Access key ID - AKIAIOSFODNN7EXAMPLE
   - Secret access key - wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

6. Embed an inline policy for a user (existing user)

Note: This procedure is needed only when using the Access Key/ID option in the Management Console.

1. Sign in to the AWS Management Console and open the IAM console.
2. In the navigation pane, choose Users.
3. In the list, choose the name of the user to which you want to embed a policy.
4. Choose the Permissions tab.
5. Choose Add permissions and then choose Create inline policy.
6. Select JSON.
7. Replace the bucket name with your bucket name, copy and paste to the Policy editor.

```
{

    "Version": "2012-10-17",

    "Statement": [

        {

            "Action": [

                "s3:GetObject",

                "s3:ListBucketMultipartUploads",

                "s3:ListBucket",

                "s3:GetBucketLocation"

            ],

            "Resource": [

                "arn:aws:s3:::[your bucket name]",

                "arn:aws:s3:::[your bucket name]/*"

            ],

            "Effect": "Allow"
        }
    ]
}
```

8. Click Create Policy.

7. Enable file access auditing (AWS FSx)

Follow the steps below to enable file access auditing.

1. Open the Amazon FSx console.
2. Navigate to File systems, and choose the Windows file system for which you want to manage file access auditing.
3. Click the Administration tab.
4. On the File Access Auditing panel, click Manage.
5. In the Manage file access auditing settings dialog box, choose Log successful attempts, Log failed attempts, Log successful attempts, and Log failed attempts.
6. On Kinesis Data Firehose, select your Kinesis Firehose Delivery Stream.



7. Click Save.

What To Do Next

Proceed to add a monitored Amazon FSx for Windows data source.

Adding Amazon FSx for Windows Data Sources - Detailed Procedure

Follow the steps below to deploy an Amazon FSx for Windows data source.

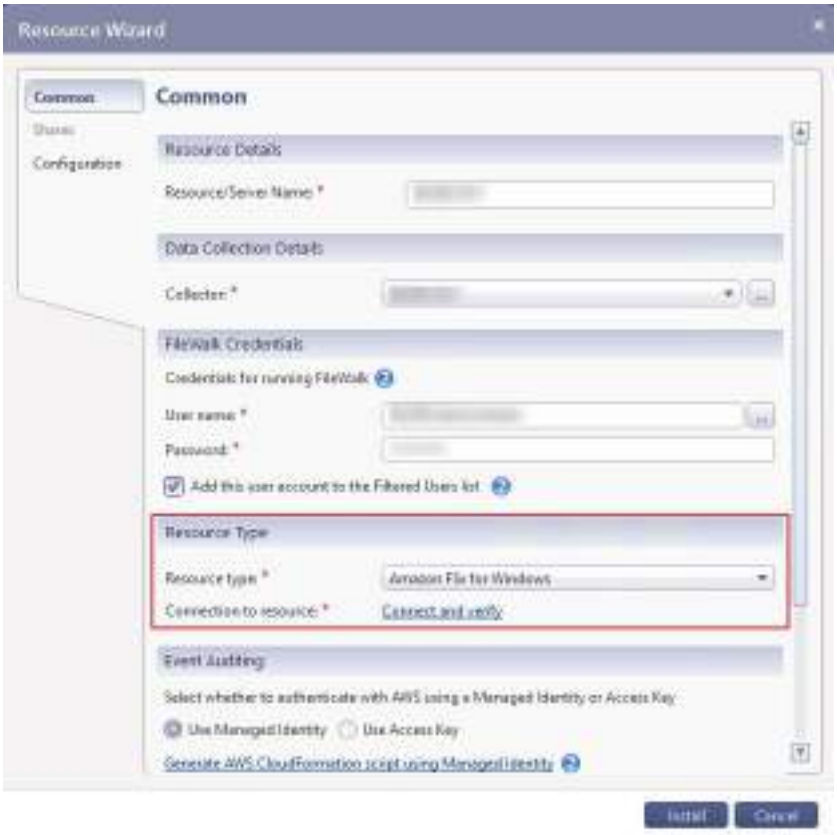
> Note: Private Preview. If you'd like to use Amazon FSx for Windows, contact your Sales Engineer.

> Note: Each Amazon FSx for Windows data source represents a monitored Amazon FSx for Windows Server. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source. To monitor multiple Windows Servers, add an Amazon FSx for Windows data source per Windows Server.

1. Set common data source parameters

1. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.

The Resource Wizard is opened to the Common pane, where you can specify the data source and set the relevant parameters.



2. In the Common pane, set the following parameters:
   a. Resource Details - Specify the data source name.
   b. Data Collection Details - Select the relevant Collector from the dropdown list.
   c. FileWalk Credentials - Enter the credentials for running directory structure monitoring. File System operations include directory structure monitoring.

      Note:

      - Configure the Varonis service account using one of the following methods:
        - Automatic – The user must be a member in the Delegated Administrators group.

      - These credentials are cached, so that they are automatically entered if another data source is added during the same session.
      - User name - Type the name of the user account to be used for directory structure monitoring.
      - Password - Type the account's password.

- Add this user account to the Filtered Users list - The defined user for FileWalk Credentials will be added to the filtered users list. If you clear this checkbox, a large number of events may be generated by the user defined for directory structure monitoring. It is recommended to keep this checkbox enabled.

> Important: You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.

d. Resource Type - Select the data source type from the dropdown list.
   - Connect and verify - Click this link to validate the credentials of the service account used to connect to the data source.

> Note:
> - The Connect and verify link is displayed only when all relevant data is entered.
> - A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

e. Event Auditing - Select whether to authenticate with AWS using a Managed Identity or Access Key.
   - To authenticate with AWS using a Managed Identity, proceed to step f.
   - To authentication with AWS using an Access Key, proceed to step g.
   - To manually set up the AWS environment, see (Optional) Manually Setting up Amazon FSx for Windows/Varonis Environment on AWS.

f. To use a Managed Identity, select Use Managed Identity and do the following steps:
   i. Generate a script. Click the Generate AWS CloudFormation script using Managed Identity link and then the Generate script button.



   Upon opening this dialog box, fields are automatically filled with suggested

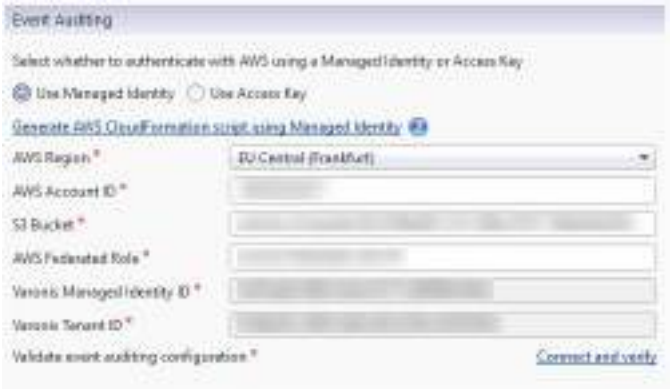
names for the resources that will be created when deploying the script. You can edit the fields as needed.

- S3 Bucket - AWS storage for event auditing.
- AWS Firehose Delivery Role - Grants AWS Firehose the permissions to access the S3 Bucket.
- AWS Delivery Stream - AWS Firehose used to stream audit events to the S3 Bucket.
- S3 Firehose Access Policy - The name of the permissions policy that will be attached to the AWS Firehose Delivery Role.
- AWS Federated Role - The name of the role that Varonis will assume to gain access to the S3 Bucket.
- S3 Federated Access Policy - The name of the permissions policy that will be attached to the AWS Federated Role.

ii. Deploy in AWS CloudFormation. For instructions, see Upload an AWS CloudFormation template and deploy a cloud infrastructure.

iii. Connect Amazon FSx to the AWS Kinesis Firehose and configure auditing settings. For instructions, see Enable file access auditing (AWS FSx).

iv. In the Event Auditing area, set the following parameters:



- AWS Region - Select the AWS region from the dropdown list.
- AWS Account ID - Enter your AWS account ID.
- S3 Bucket - AWS storage for event auditing. Autopopulated after script generation.
- AWS Federated Role - The name of the role that Varonis will assume to gain access to the S3 Bucket. Autopopulated after script generation.
- Varonis Managed Identity ID - Grayed out, autopopulated.
- Varonis Tenant ID - Grayed out, autopopulated.
- Validate event auditing configuration - Validation status.
- Click Connect and verify to verify the connection to the S3 bucket.

g. To use an Access Key, select Use Access Key and set the following parameters:

i. Generate a script. Click the Generate AWS CloudFormation script using Access Key link and then the Generate script button.

> Note: When you generate a script for an Access Key, you need to provide a user name. You may need to create a user beforehand.



Upon opening this dialog box, fields are automatically filled with suggested names for the resources that will be created when deploying the script. You can edit the fields as needed.

- S3 Bucket - AWS storage for event auditing.
- AWS Firehose Delivery Role - Grants AWS Firehose the permissions to access the S3 bucket.
- AWS Delivery Stream - AWS Firehose used to stream audit events to the S3 Bucket.
- S3 Firehose Access Policy - The name of the permissions policy that will be attached to the AWS Firehose Delivery Role.
- UserAccessPolicy - The name of the permissions policy that will be attached to the specified user.
- UserName - The AWS user whose Access key will be used by Varonis to access the S3 Bucket (must be an existing user).

ii. Deploy in AWS CloudFormation. For instructions, see Upload an AWS CloudFormation template and deploy a cloud infrastructure.

iii. Connect Amazon FSx to the AWS Kinesis Firehose and configure auditing settings. For instructions, see Enable file access auditing (AWS FSx).

iv. In the Event Auditing area, set the following parameters:



- AWS Region - Select the AWS region from the dropdown list.
- S3 Bucket - AWS storage for event auditing. Autopopulated after generating the script.
- Access Key ID - Enter your Access Key ID. See To get your access key ID and secret access key (existing user) in (Optional) Manually Setting up Amazon FSx for Windows/Varonis Environment on AWS.
- Secret Access Key - Enter your Secret Access Key. For more information, see To get your access key ID and secret access key (existing user) in (Optional) Manually Setting up Amazon FSx for Windows/Varonis Environment on AWS.
- Validate event auditing configuration - Validation status.
- Click Connect and verify to verify the connection to the S3 bucket.

h. Monitored Shares - Select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source installed and share detection is completed.

- Automatically monitor detected shares - Select this option to automate monitoring for all detected shares. Share monitoring will automatically start after the data source installation is completed. Varonis will monitor all shares that aren't marked as "ignored". When this option is selected, click the Advanced setting link to modify share detection preferences. By default, the option is set to Prefer regular shares over equivalent admin shares. In this case, an admin share that has an equivalent regular share will be marked as "ignored" and the equivalent regular share will be detected for monitoring. Note: Any change in the monitored shares configuration, including the detection method, admin shares configuration, and selected shares, requires rerunning the resource detection.
- Monitor selected shares - This option is selected by default. You can manually select the shares to be monitored only after the data source is installed and share detection is completed. You'll need to open the Edit

window for the installed data source and select the shares. For more information, see Post-installation share detection and registration.

Once the above settings are configured, you can proceed to review and adjust configuration settings.

2. Review and adjust configuration settings

1. On the left menu, click Configuration and confirm the information.
   The general configuration settings are displayed.
2. In the FileWalk Settings area, review the options:
   - Identify actual unique folders and file system inconsistencies - Select this checkbox (if it's not already selected) to detect broken permissions in NTFS file systems.

3. Install the data source

After configuration is complete, click Install to install the data source.

A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the File Servers pane. When the installation completes, the status shows "Installed 100%".

4. Post-installation share detection and registration

After the data source installation and share detection are completed, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. The following procedure describes the manual registration and automatic share detection flows.

> Important: If after the data source is installed, share detection fails for any reason, the Share Detection Status column will remain "In Progress" until the issue is fixed, and share detection completes successfully at least once.

After the data source is installed, the Shares pane is enabled, and you can view the share settings.

1. On the left menu, click Shares.
   The share settings are displayed. The pane's heading indicates the option you selected when adding a data source.

2. In the Available Shares area, you can filter the shares based on the reason they are not registered for monitoring and easily identify the shares that can be added. The default filter is Accessible Shares. You can change the filter to see the rest of the shares. Options include:
   - Accessible shares - Can be added for monitoring (this option is selected by default)
   - Ignored shares - Are marked as "ignored"
   - Incompatible and inaccessible shares - Cannot be monitored since the exposed protocol does not match the security style of the volume (relevant to multiprotocol platforms only) or the Varonis service account does not have access to this share
   - Child share of a monitored share - Is monitored via its parent folder
3. Do one of the following:
   - If you chose to monitor selected shares, in the Available Shares area, select the required shares and click the down arrow. The selected shares are moved to the Registered Shares area. (The registered shares list is empty until you make your selections.)
   - If you chose to automatically monitor detected shares, Varonis will monitor all shares that aren't marked as "ignored". The automated share detection runs every few hours. The Registered Shares area is autopopulated with the shares to be monitored.
4. For each share, review and set the following information as required:
   - Ignore Detection - Select the shares to be ignored (and not be the subject of automatic detection and notifications) by the data source monitor.
   - Events - Select this checkbox to audit events for the share.
   - Crawl - To enable or disable monitoring for the share, in the Crawl column, select the relevant option.

     Note: You can also right-click the grid and select the required options for event auditing and crawling.
5. In the Additional Share Settings area, review the options:
   - Remove deleted shares - Select this checkbox to remove deleted shares. Shares that were deleted from the data source will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the data source is unavailable, the shares will not be removed.
   - Enable event auditing - Select this checkbox to audit events from all shares added from this data source.

After share detection and registration are completed, the status and number of registered volumes are respectively displayed in the Share Detection Status and Registered Shares columns in the File Servers pane.

What To Do Next

Now let's take a look at the supported events for the monitored Amazon FSx for Windows data sources.

Supported Events For Amazon FSx For Windows Data Sources

Note: Private Preview. If you'd like to use Amazon FSx for Windows, contact your Sales Engineer.

SMB (CIFS) Events for Amazon FSx for Windows Data Sources

Note: SMB v2 and v3 are supported.

Event Auditing Method

Amazon S3 API

Supported File Operations

- File deleted
- File modified
- File opened
- Owner changed
- Permissions added
- Permissions removed
- Protection added
- Protection removed

Access Denied Events

- File deleted
- File opened

- Folder deleted
- Folder opened denied
- Owner changed
- Permissions added

Limitations

Varonis uses the Amazon FSx for Windows File Access Log which supports only the event types listed above. Therefore, we have the following limitations:

- Reading the events by Varonis might cause additional costs to Amazon since data is downloaded.
- Due to the missing events, not all threat detection policies are supported:
  - The following threat detection policies are partially supported:
    - Activity on known nefarious files (supported: File opened, File deleted, non-supported: File created, File renamed)
    - Immediate pattern detected: user actions resemble ransomware (supported: File opened, File deleted, File modified, non-supported: File created, File renamed, Folder created)
    - Potential encryption of multiple files (supported: File modified, non-supported: File created, File renamed)
    - Abnormal behavior: unusual amount of system files accessed (File created)
    - Abnormal behavior: unusual amount of script files accessed (File created)
    - Abnormal executive behavior: unusual amount of files with denied access across executive accounts (File created)
    - Abnormal executive behavior: accumulative increase in amount of files with denied access across executive accounts (File created)
    - Abnormal executive behavior: unusual amount of script, configuration and backup files accessed (File created)
    - Abnormal executive behavior: accumulative increase in amount of script, configuration and backup files accessed across executive accounts (File created)
  - The following threat detection policies are not supported:
    - Security tools created or modified
    - Potential ransomware note file was created
    - System administration tools created or modified

  - Penetration testing and hacking tools created or modified
  - Exploitation software created or modified
- Data protection policies are not supported.

5 M365 DATA SOURCES

What This Section Contains

This section describes how to deploy and monitor M365 data sources; the requirements, deployment and configuration steps, and supported events.

What To Do Next

Before you dive in, click here to learn more about the requirements for deploying and monitoring Entra ID domains, SharePoint Online, OneDrive, and Exchange Online data sources.

Requirements For Monitoring M365 Data Sources

This section describes the requirements needed to successfully deploy and monitor Entra ID domains, SharePoint Online, OneDrive, and Exchange Online data sources.

General M365 Requirements

Unified Audit Log

To audit events in Entra ID, SharePoint Online, OneDrive, and Exchange Online, enable auditing in M365 as described in Turn on auditing.

To audit events in Exchange Online, auditing should be enabled for each of the monitored mailboxes. Varonis will automatically turn on event auditing for each mailbox as part of the event auditing process.

Scanning Speed and User Volume

Varonis uses Entra ID applications to scan your data source. These applications are limited to an API quota that is allocated by Microsoft. Microsoft enforces this quota by a throttling mechanism, activated when the Entra ID applications attempt to exceed the allocated quota.

The quota is impacted by the number of licensed Microsoft users on your tenant: The more licensed users you have, the larger the quota, resulting in a faster scanning speed.

For more information, learn about Microsoft Application Throttling.

Adding Trusted Sites

Before adding an Entra ID domain in the Management Console, make sure that the following sites are defined as trusted on the Management Console host:

- https://login.microsoftonline.com
- https://aadcdn.msauth.net
- https:/adfs.{Domain}.com (optional)

Define sites as trusted as follows:

1. On the Management Console host, search for "Internet Options" in the start menu. The Internet Properties dialog box appears.
2. Select the Security tab and click Trusted sites. Then click Sites.



3. Separately enter each trusted site listed above into the Add this website to the zone field and click Add after each entering each one.



4. When you have added all the sites, click Close, then click OK.
   You are now ready to add an Entra ID domain.

Granting Consent to the VaronisAppRegistration Application (Optional)

The VaronisAppRegistration application is managed by Varonis and is intended strictly for the M365 data source deployment process (it is not used outside of the deployment process). Before every use of the application, the Varonis Management Console

displays the Microsoft Sign in page, requiring the user who granted the consent to actively authenticate to Microsoft.

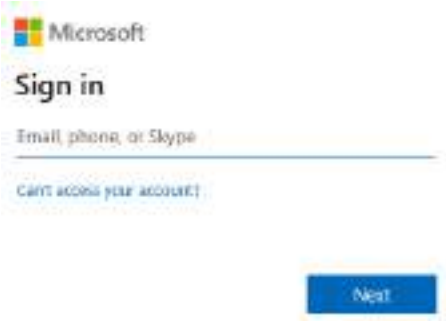
You need to grant consent to VaronisAppRegistration per each M365 monitored tenant to enable the following Varonis capabilities:

Usage	Service	Permission	Requirement
Auto-create the Entra ID application for SharePoint Online and OneDrive monitoring	Microsoft Graph	Application.ReadWrite.All	Mandatory
Auto-create the Entra ID application for SharePoint Online and OneDrive monitoring	Microsoft Graph	Directory.Read.All	Mandatory
Auto-create the Entra ID application for SharePoint Online and OneDrive monitoring	Microsoft Graph	RoleManagement.ReadWrite.Dir	Mandatory
Grant consent to automatically generatedEntra ID applications	Microsoft Graph	AppRoleAssignment.ReadWrite.All	Recommended: Without this permission, you will not be able to automatically grant consent to auto-created Entra ID applications

Usage	Service	Permission	Requirement
Grant consent to automatically generated Entra ID applications	Microsoft Graph	DelegatedPermissionGrant.ReadWrite.All	Recommended: Without this permission, you will not be able to automatically grant consent to auto-created Entra ID applications

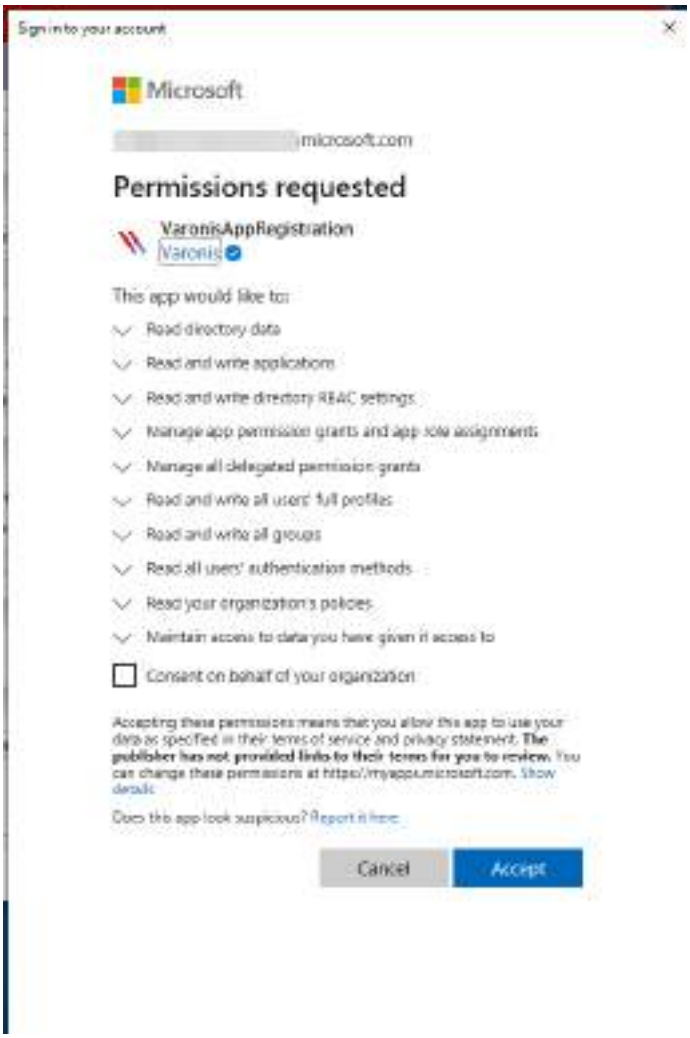
To grant consent to the VaronisAppRegistration application, proceed as follows:

1. When the Microsoft Sign in page is displayed, enter the credentials of a user with Global Administrator permissions.



   Enter the user name, click Next, enter the account password, and click Sign in. The

Permissions requested page is displayed for the VaronisAppRegistration



2. Click Accept. This grants your consent to the VaronisAppRegistration application. You are now ready to add an Entra ID domain.

Entra ID Requirements

Installation Requirements

In addition to the full firewall, proxy, and certificate requirements and Varonis SaaS deployment prerequisites, the following are also required:

Requirement	Notes
A user with permissions to create	The following users meet this requirement :

Requirement	Notes
applications in Entra ID.	• Global Administrator • Application Administrator • Cloud Application Administrator • A user who is temporarily allowed to create applications in Entra ID
A user with the Global Administrator role.	This user is required to grant consent to the permissions added to the Entra ID application.

Operational Requirements

This section describes the requirements for monitoring and remediating your Entra ID data sources.

Varonis monitors Entra ID using an Entra ID application, which you are required to create via the Microsoft Entra admin center or Varonis Management Console. This application is also used to monitor the M365 Unified Audit Log (which logs Entra ID, SharePoint Online and OneDrive events).

Entra ID Application Role Assignment Requirements

Usage	Role	Assignment Type	Requirement
Manage role assignments in Entra ID.	Privileged Role Administrator	Permanent (not eligible)	Recommended: Without this role, you will not be able to remove members from role-assigned groups.

Entra ID Application Permission Requirements

Usage	Service	Permission	Type	Requirement
Read the organization's activity data	Office 365 Management	Activity.Feed.Read	Application	Mandatory
Get all accounts in the tenant	Microsoft Graph	Directory.Read.All	Application	Mandatory
Get the `LastSignInDateTime` property of Entra ID users	Microsoft Graph	AuditLog.Read.All	Application	Mandatory
Get the `LastSignInDateTime` property of Entra ID users and check the availability of Entra ID sign-in logs	Microsoft Graph	Organization.Read.All	Application	Mandatory
Identify Microsoft 365 groups that are connected to Teams	Microsoft Graph	Files.Read.All	Application	Mandatory

Usage	Service	Permission	Type	Requirement
Note: Files.Read.All is the least privileged permission required by Microsoft to invoke API calls to identify the Microsoft 365 groups connected to Teams.				
Run remediation policies	Microsoft Graph	Group.ReadWrite.All	Application	Recommended: Without this permission, you will not be able to remove memberships
Run remediation policies	Microsoft Graph	User.ReadWrite.All	Application	Recommended: Without this permission, you will not be able to disable users
Read organization policies	Microsoft Graph	Policy.Read.All	Application	Recommended: Without this permission, you will not be able to get organization MFA data, leading to more accurate threat detection

Usage	Service	Permission	Type	Requirement
				and mitigation strategies.
Read the authentication methods of all users in your organization	Microsoft Graph	UserAuthenticationMethod.Read.All	Application	Recommended: Without this permission, you will not be able to get your user MFA data, leading to more accurate threat detection and mitigation strategies.
Read Copilot prompts and responses	Microsoft Graph	Mail.Read	Application	Optional: Without this permission, you will not be able to monitor Copilot prompts and responses.

For Varonis to monitor your Entra ID Sign-In Logs, you need a Microsoft subscription that stores these logs: A Microsoft E3 or Entra ID P1 license or above. If you do not have the required license, there will be no data for extended log-in analytics.

Note: A single E3/P1 license is sufficient.

SharePoint Online Requirements

Installation Requirements

In addition to the full firewall, proxy, and certificate requirements and Varonis SaaS deployment prerequisites, the following are also required:

Requirement	Notes
Entra ID domain	A relevant Entra ID domain must already be configured in the Management Console.
A user with permissions to create applications inEntra ID.	The following users meet this requirement : • Global Administrator • Application Administrator • Cloud Application Administrator • A user who is temporarily allowed to create applications in Entra ID
A user with the Global Administrator role.	This user is required to grant consent to the permissions added to the Entra ID application.

Note: Make sure that you have the correct TLS 1.2 ciphers configured. For detailed instructions, see O365 : SPO / OD TLS 1.2 - Crypto Ciphers.

Operational Requirements

Varonis monitors SharePoint Online using four Entra ID applications, which you are required to create via the Management Console or the Microsoft Entra admin center. Each application is dedicated to a specific product flow, for example: Data classification, visibility, remediation, etc.

The following are required for monitoring SharePoint Online:

Requirement	Notes
An Entra ID application with the permissions listed in the table below.	You can create this application in the following ways: • Automatically - via the Management Console, during the Entra ID data source deployment process: The application already includes the required application permissions (listed in the table below), and a Global Administrator is required to grant consent. • Manually - via Entra ID: Make sure the required application permissions (listed in the table below) are included and are granted consent.
A Collector	You are required to configure a Collector.

SharePoint Online Application Permission Requirements

Usage	Service	Permission	Type	Requirement
Read directory data	Microsoft Graph	Directory.Read.All	Application	Mandatory
Read data in all sites	Microsoft Graph	Sites.Read.All	Application	Mandatory
Read, update and	SharePoint	Sites.FullControl.All	Application	Mandatory

Usage	Service	Permission	Type	Requirement
classify resources				

Note: Due to Microsoft's lack of permissions granularity, Sites.FullControl.All is mandatory: It is the only permission that allows invoking API calls to retrieve direct access and sharing links information on sites, folders, and files (that is: Even for read only purposes, without making updates).

Note: To audit SharePoint Online events, the Entra ID application that monitors Entra ID must include the Office 365 Management API: ActivityFeed.Read.

OneDrive Requirements

Installation Requirements

In addition to the full firewall, proxy, and certificate requirements and Varonis SaaS deployment prerequisites, the following are also required:

Requirement	Notes
Entra ID domain	A relevant Entra ID domain must already be configured in the Management Console.
A user with permissions to create applications in Entra ID.	The following users meet this requirement : • Global Administrator • Application Administrator • Cloud Application Administrator • A user who is temporarily allowed to create applications in Entra ID

Requirement	Notes
A user with the Global Administrator role.	This user is required to grant consent to the permissions added to the Entra ID application.

Note: Make sure that you have the correct TLS 1.2 ciphers configured. For detailed instructions, see O365 : SPO / OD TLS 1.2 - Crypto Ciphers.

Operational Requirements

Varonis monitors OneDreive using four Entra ID applications, which you are required to create via the Management Console or the Microsoft Entra admin center. Each application is dedicated to a specific product flow, for example: Data classification, visibility, remediation, etc.

The following are required for monitoring OneDrive:

Requirement	Notes
An Entra ID application with the permissions listed in the table below.	You can create this application in the following ways: • Automatically - via the Management Console, during the Entra ID data source deployment process: The application already includes the required application permissions (listed in the table below), and a Global Administrator is required to grant consent. • Manually - via Entra ID: Make sure the required application permissions (listed in the table below) are included and are granted consent.

Requirement	Notes
A Collector	You are required to configure a Collector.

OneDrive Application Permission Requirements

Usage	Service	Permission	Type	Requirement
Read directory data	Microsoft Graph	Directory.Read.All	Application	Mandatory
Read data in all sites	Microsoft Graph	Sites.Read.All	Application	Mandatory
Read, update and classify resources	SharePoint	Sites.FullControl.All	Application	Mandatory

Note: Due to Microsoft's lack of permissions granularity, Sites.FullControl.All is mandatory: It is the only permission that allows invoking API calls to retrieve direct access and sharing links information on sites, folders, and files (that is: Even for read only purposes, without making updates).

Note: To audit OneDrive events, the Entra ID application that monitors Entra ID must include the Office 365 Management API: ActivityFeed.Read.

Exchange Online Requirements

Installation Prerequisites

In addition to the full firewall, proxy, and certificate requirements and Varonis SaaS deployment prerequisites, the following are also required:

Requirement	Notes
Entra ID domain	A relevant Entra ID domain must already be configured in the Management Console.

Authentication and Authorization Prerequisites

The following permissions are required for the deployment of the Exchange Online data source:

Prerequisite	Notes
A user with permissions to create applications in Entra ID	A user with the Global Administrator, Application Administrator, Application Developer, or Cloud Application Administrator role is required for creating the Entra ID application, or all users have to be temporarily allowed to create applications in Entra ID. This permission is required only if you want to use the "Create New" procedure when adding the Exchange Online data source.
A user with the Global Administrator role	A user with the Global Administrator role is required to grant consent to the permissions added to the Entra ID application.

The following Entra ID application permissions are required to monitor Exchange Online:

Prerequisite	Notes

An Entra ID application with the Exchange Administrator role and the following permissions are required for Exchange Online visibility:
• Microsoft Graph API:
  • Directory.Read.All – Reads directory data.
  • Mail.Read – Retrieves email attachment information.
• Office 365 Exchange Online:
  • Exchange.ManageAsApp - Grants application permissions.
  • full_access_as_app– Grants access to all mailboxes.
	The Exchange Administrator role is part of the required settings of the application and is automatically assigned during the new application registration step of the installation.
	If you decide to use an existing application, you will need to add this role.
	The Exchange Administrator role is required for:
	• Application permissions
	• Running PowerShell commands such as `Get-MailboxPermission` and `Get-MailUser` to enable mailbox auditing, to read the mailbox list, and to read the permissions per each mailbox
	If you chose to automatically create the application via the Management Console during the Exchange Online data source deployment process, an application with those permissions will be automatically created and you will be required only to grant consent for them. If you chose to manually create the application in Entra ID, you will be required to ensure that those permissions are present and have been granted consent.
	The Mail.Read permission is required for message classification and to retrieve attachment information as part of Exchange Online Message Delivered events.

Prerequisite	Notes
	Due to Microsoft's lack of permissions granularity, full_access_as_app is required when using an EWS with application permissions. The full_access_as_app permissions should allow access to all mailboxes. Exchange Online visibility will not be supported if access is limited only to a specific set of mailboxes by using Microsoft's Application Access Policy. For the application object to access Exchange Online resources, it needs the Office 365 Exchange Online API permission: Exchange.ManageAsApp.

Note: To audit Exchange Online events, the Entra ID application that monitors Entra ID must include Office 365 Management API: ActivityFeed.Read.

Entra ID Data Sources

What This Section Contains

This section describes how to deploy and monitor Entra ID data sources; it includes the deployment and configuration steps and supported events.

What To Do Next

First, make sure you fulfill the Entra ID requirements.

After that, proceed to add the Entra ID domain in the Management Console.

Adding an Entra ID Data Source

After the required Collectors are installed, you must add an Entra ID data source; it is required to resolve the Entra ID users and groups who have permissions to the data stored in other monitored data sources.

This section describes how to add an Entra ID domain data source in the Management Console and how to add the Entra ID application to the Entra ID domain.

Before You Begin

Note the following:

- To reduce throttling issues, you are required to create separate applications for monitoring Entra ID, SharePoint Online, OneDrive, and Exchange Online.
- When monitoring an M365 tenant, users from all the domains in the tenant are monitored. There is no option to limit the monitored users to a single domain in the tenant.
- The process uses the tenant ID.
- The procedure for deploying an Entra ID data source includes a step which you select whether to automatically register a new Entra ID application (using the Create new option), or to use an existing Entra ID application (using the Use existing option).
- When you select Create new, the Management Console automatically creates an application in Entra ID for you during the data source deployment.
- If you select Use existing, you must first have manually created an Entra ID application in Entra ID. You then configure the Entra ID application details during the data source deployment.
- To monitor multiple M365 tenants, create an Entra ID data source for each tenant as explained below.

Add an Entra ID Data Source

1. Run the Management Console as an administrator.
2. Select Management > Components > Root > Domains and on the toolbar, click Add.

   Note: Alternatively, you can use the Quick Create menu on the title bar of the Management Console, and select Add New Domain.

The Domain Properties page is displayed, showing the General pane.

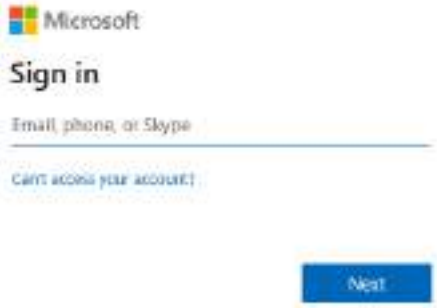


3. Select Entra ID as the Domain Type for your Entra ID and Collector.
4. In the Configuration area, enter the Tenant ID.
5. In the Connection Details area, choose whether to Grant Global Administrator consent for the application permissions (selected by default): Use this option to simplify the creation of a new Entra ID application, by automatically granting consent to the required permissions.

   > Important: It is recommended to select automatic consent, unless you prefer to use an existing application. If you disable automatic consent, you will have to manually grant consent after the application is created. This is done either using the link provided on the screen, or directly via the Entra ID portal.

   To set up the required Entra ID application, choose whether to create a new application (step 6), or use an existing one that you've created in Entra ID (step 7).
6. To create a new Entra ID application:

a. Click the Create New button. The Microsoft Sign in page is displayed.

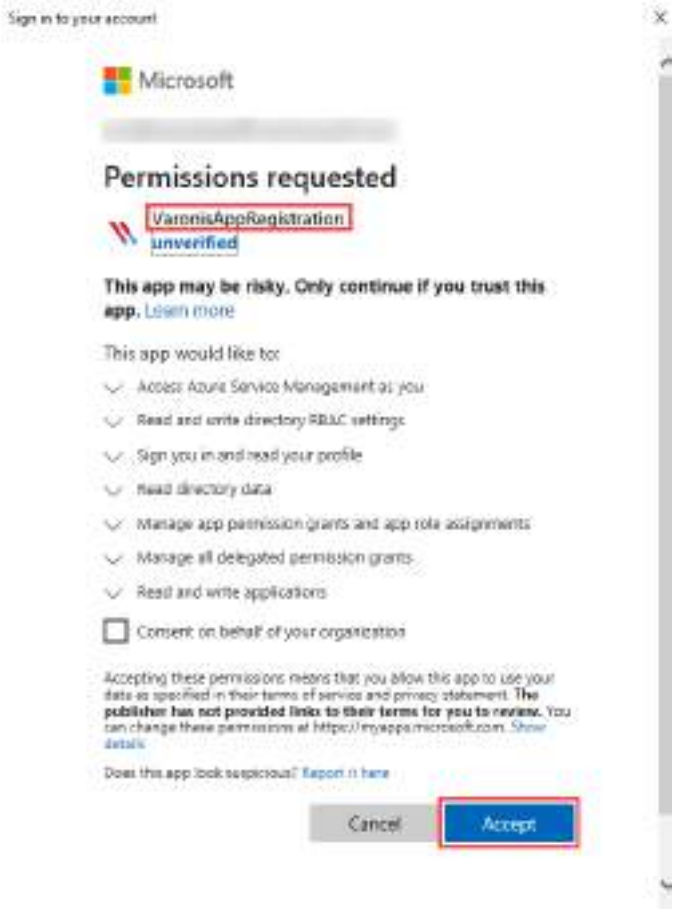


b. Enter the credentials of a user with permissions to create an application in Entra ID. Enter the user name, click Next, enter the account password, and click Sign in.



The Permissions requested page is displayed for the VaronisAppRegistration

application.



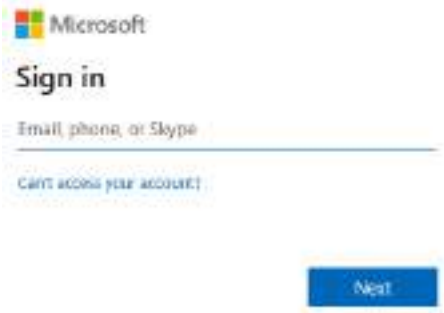
c. Click Accept. This grants your consent to the VaronisAppRegistration application.
A new application is now created in Entra ID. When completed, a confirmation message is displayed indicating that the application was successfully created.



d. Grant Global Administrator consent for the application permissions:

> Note: This step is required only if you cleared the Grant Global Administrator consent for the application permissions option.

i. Click the here link to grant this application permissions. The Microsoft Sign In page is displayed.

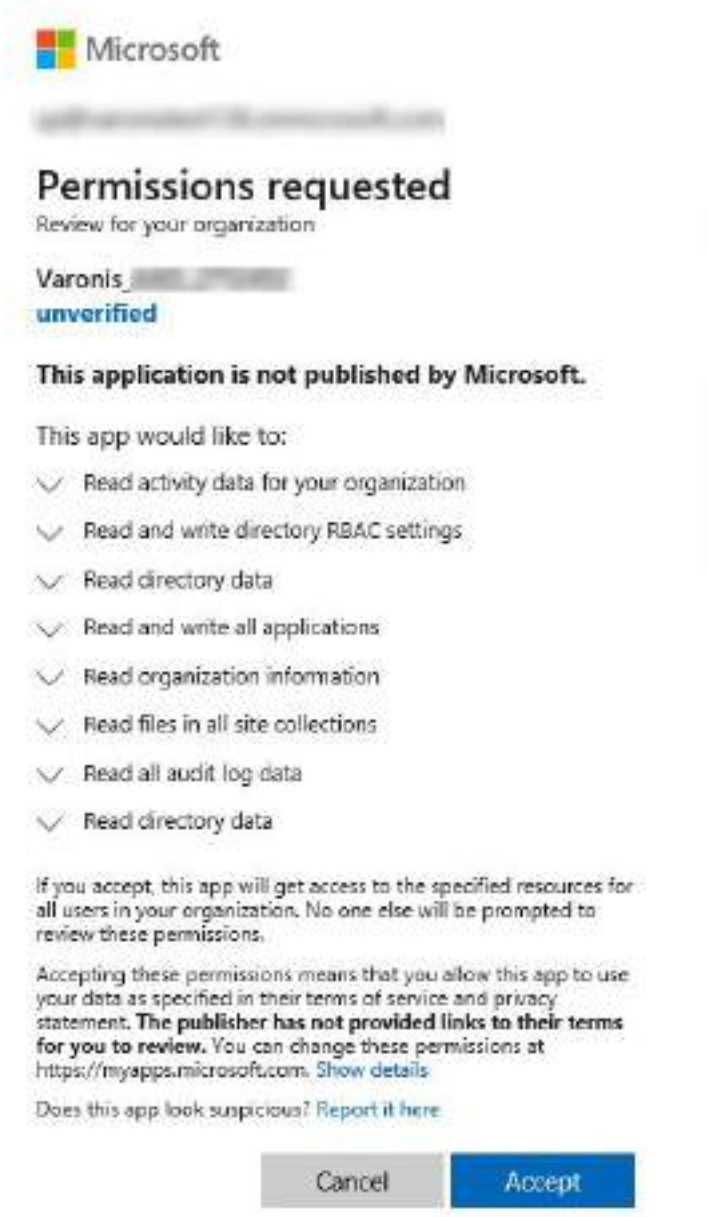


ii. Enter the Global Administrator credentials, user name and password, and click Next. Permissions must be consented by the Global Administrator.



iii. Enter the account password, and click Sign in. The Microsoft Permissions requested page opens, displaying the Entra ID application name (at the top)

and the requested permissions.



iv. Click Accept.

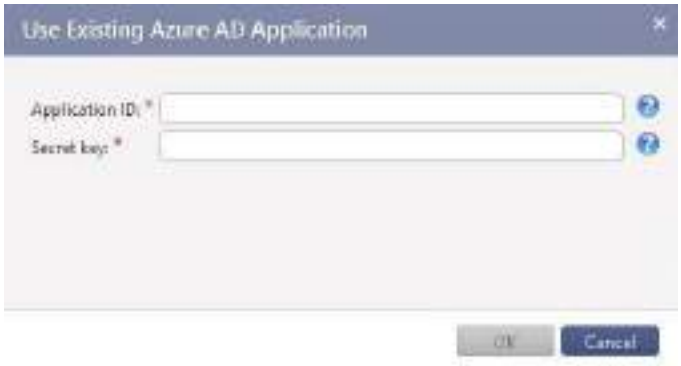
v. In the Management Console Action Required dialog box, click OK to close it.

e. In the Connection Details area, the Entra ID application name is now displayed (it's grayed out).

> Note: During the synchronization of the application in Entra ID, the link Click here to grant Global Admin consent for the permissions may be displayed in

this area. Click it to consent, or wait until Microsoft finishes processing the new application settings and grants permissions

7. To use an existing Entra ID application:
   a. In the Connection Details area, select Use existing.
   b. The Use Existing Entra ID Application dialog box is displayed.



   c. Enter the Application ID.
   d. Enter the Secret key. For more information, see Entra ID Requirements.
   e. Click OK to close the dialog box.
8. In the Data Collection Details area, the Collector is specified by default. If more than one Collector is available, you can choose a different one from the Collectors dropdown list as needed. (This step can be performed at any time before clicking Install.) For more information, see Collector Requirements in Varonis SaaS Deployment Prerequisites.
9. In the Active Directory Sync area, All is selected by default. That is, all domain forests synchronized to Entra ID are selected.
   The mapping between the AD user and the Entra ID user is done according to the default `sourceAnchor` attribute defined by Microsoft in Entra ID Connect:
   - Users are mapped via objectGUID
   - Groups are mapped via objectNAME
10. In the Event Collection Settings area, the Audit events checkbox is selected by default. This indicates Varonis will monitor audit events in Entra ID.
11. Go to the Monitored Accounts tab to select the Entra ID accounts you want to monitor. By default, All acocunts are monitored. To monitor only selected Entra ID accounts, take the following steps:

a. Go to the Monitored Accounts section and select the Accounts by rule option.



b. Set the Accounts by list to one of the following rules:

- Group:
  - Enter the name of the predefined Entra ID group you created with accounts to be monitored:



- Attribute:
  - Select the relevant account attribute from the drop-down list (Administrative unit, Company name, Department, Division, User principal name, or one of the Extension attributes).
  - Select the relevant operator from the drop-down list (Equals or Contains) and enter the attribute value.



Varonis will monitor the accounts by the selected rule: Group (including its nested accounts) or Attribute.

Note: In addition to monitoring accounts by the specified group or attribute, Varonis also monitors the following entities:

- Any other groups of which these accounts (users or nested groups) are members.

- Guest users, applications, devices, service principles, roles, and contacts from the entire domain.

After configuration is complete, click Save to add the Entra ID data source.

A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the File Servers pane. When the installation completes, the status shows "Installed 100%".

What To Do Next

Now let's take a look at the supported Entra ID events.

Supported Events for Entra ID Data Sources

The following events are audited for Entra ID data sources:

- Account disabled
- Account enabled
- Application added
- Application consent approved
- Application consent removed
- Application owner added
- Application owner removed
- Application removed
- Application updated
- Device added
- Device owner added
- Device owner removed
- Device registered user added
- Device registered user removed
- Device removed
- Device updated
- Group added
- Group deleted
- Group license set

- Group member added
- Group member removed
- Group owner added
- Group owner removed
- Group updated
- Interacted with Copilot
- License properties set
- Login
- Role member added
- Role member removed
- Role updated
- Service principal added
- Service principal credentials added
- Service principal credentials removed

  Note: "Service principal credentials added" and "Service principal credentials removed" events are generated only if the credentials are added or removed programmatically (using code, as opposed to UI).

- Service principal owner added
- Service principal owner removed
- Service principal removed
- Service principal updated
- Set force change user password
- User added
- User deleted
- User invited to organization
- User license changed
- User restored
- User updated

Allowing your Entra ID Application to Collect Copilot Prompts

Note: Private Preview. If you'd like to use Conversation Investigation, contact your Sales Engineer.

To collect Copilot prompts and responses, your Entra ID application requires a specific permission: `Mail.Read`.

Note: To activate Copliot prompt collection, you must have a Copilot license, and enable the option to collect logs in the Varonis Web Interface (Configuration > Settings > AI Conversation Auditing > Audit AI Conversations).

Starting from version 11, if you allow Varonis to automatically create your Entra ID application, the new application has permission to collect Copilot prompts and responses.

However, if you already deployed Varonis for M365 before v11, or if you chose to manually create your application, you must manually add the `Mail.Read` permission to your application permissions.

To manually add Mail.Read to your Entra ID application permissions:

1. Find the name of your Entra ID application in the Management Console:
   a. Go to Management Console > Domains and select your Entra ID domain.
   b. Under Connection details find your application name.
2. Add `Mail.Read` to your application permissions in Entra ID:
   a. Go to Microsoft Entra ID > App Registration and search for your Entra ID application.
   b. Select Add permission > Microsoft graph > Application permissions > Mail.Read > App permissions > Grant admin consent > Save and continue > Yes.

SharePoint Online Data Sources

What This Section Contains

This section describes how to deploy and monitor SharePoint Online data sources; it includes the deployment and configuration steps and supported events.

What To Do Next

First, make sure you fulfill the SharePoint Online requirements.

After that, familiarize yourself with the deployment steps summary and then dive into the detailed procedure.

Adding a SharePoint Online Data Source - Summary

This section summarizes the procedure for deploying SharePoint Online data sources in the Management Console.

1. Run the Management Console as an administrator.
2. Select Management > Components > Root > Domains and verify that an Entra ID domain has been added.
3. Add a SharePoint Online data source: Select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.
4. Select the Resource type > SharePoint Online/OneDrive.
5. In the Resource Wizard's Common pane, check the Collector selected by default and change it if needed.
6. In the Connection Details area, go to Entra ID application and select your domain.
7. In the Applications pane, add four applications. Each application is dedicated to a specific product flow, for example: Data classification, visibility, remediation, etc.
8. Grant Global Administration consent for the permissions that Varonis requires.
9. In the Monitor Sites pane, go to Site Collection Details → SharePoint admin center and enter the URL of the SharePoint Admin Center website in the format https://{tenant-name}-admin.sharepoint.com.
10. In the Monitored Sites area, determine how to select the sites to be monitored by Varonis. Choose one of the following options:
    - All Sites - Automatically detect and monitor all sites available on your tenant.
    - Import sites - Monitor only sites specified in an imported list defined in a CSV or TXT file.
    - Sites by Rule - Automatically detect and monitor only sites that meet a specific rule: Primary admin or Owner.

      Note: Choose this option to monitor a single M365 tenant that is shared by multiple organizations (sub-orgs).
11. In the Configuration pane, review the List Item Types and Files to Collect.
12. After configuration is complete, click Install to add the SharePoint Online data source.
13. Grant consent to the Varonis DCE application for SharePoint Online file analysis

What To Do Next

Now that you're familiar with the deployment steps, it's time to dive into the detailed procedure.

Adding a SharePoint Online Data Source - Detailed Procedure

This section describes the full procedure for deploying SharePoint Online data sources in the Management Console.

Before You Begin

Note the following:

- To reduce throttling issues, you are required to create separate applications for monitoring Entra ID, SharePoint Online, OneDrive, and Exchange Online.
- The procedure for deploying a SharePoint Online data source includes a step which you select whether to automatically register a new Entra ID application (using the Create new option), or to use an existing Entra ID application (using the Use existing option).
- When you select Create new, the Management Console automatically creates an application in Entra ID for you during the data source deployment.
- If you select Use existing, you must first have manually created an Entra ID application in Entra ID. You then configure the Entra ID application details during the data source deployment.

1. Check if an Entra ID data source exists

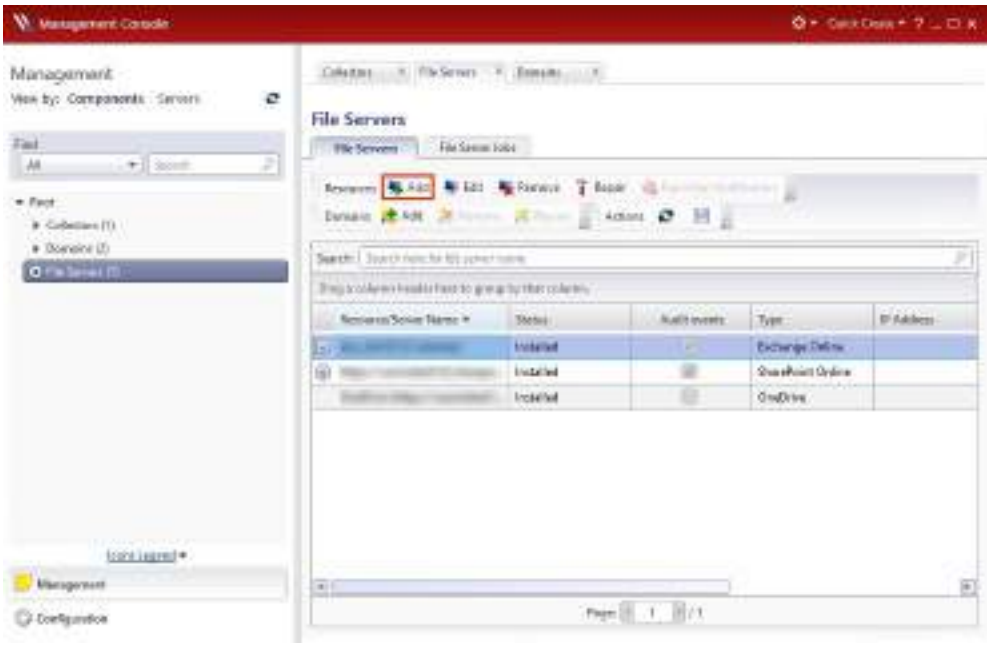
1. Run the Management Console as an administrator.
2. Select Management > Components > Root > Domains and verify that an Entra ID domain has been added.



2. Add a SharePoint Online data source

1. In the Management Console, select Management > Components > Root > File Servers.
2. In the File Servers tab, go to the Resources toolbar and click Add.

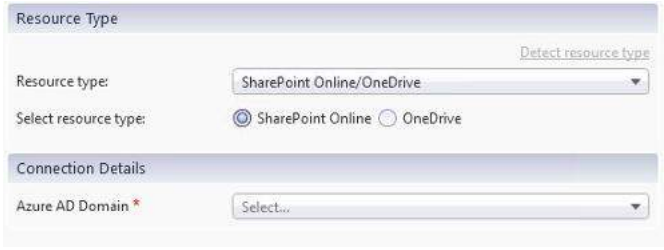
> Note: Alternatively, you can use the Quick Create menu on the title bar of the Management Console, and select Add New File Server.



The Resource Wizard is opened to the Common pane.



3. In the Resource Type area, select SharePoint Online/OneDrive from the dropdown list.
   In Select resource type, SharePoint Online is selected by default, and a new area - Connection Details - is displayed.



4. In the Connection Details area, go to the Entra ID Domain dropdown list and select your domain.
   The Applications and Monitor Sites panes are enabled.

Continue to the Applications pane and configure Entra ID applications.

3. Configure Entra ID applications

Varonis uses Entra ID applications to monitor your data sources. The Applications pane allows you to create four unique Entra ID applications. Each application is dedicated to a specific product flow, for example: Data classification, visibility and remediation, etc.

> Note: If you previously deployed your data source with one or two applications, add the missing applications required to meet the recommendation of four applications per data source.

You can either add existing applications, or automatically create new applications. Only applications that are added here are used for scanning.



> Note: To automatically create applications, Varonis requires specific permissions (as specified in "Granting Consent to the VaronisAppRegistration Application (Optional)" under General M365 Requirements). If you do not grant permissions to create Entra ID applications, you will only be able to add existing applications. If

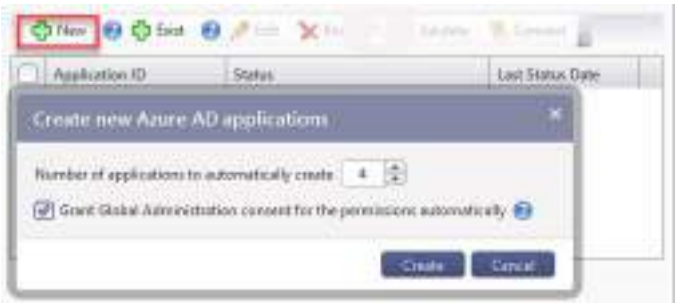
you do not grant permissions for automatic consent, you will need to grant consent manually for each new application you add.

To create and manage your Entra ID applications, take the following steps:

1. In the Applications tab, you can either create a new application, or add an existing application:
   - To create a new application - proceed to step 2
   - To add an existing application - proceed to step 3

   Note: When you create new applications, they are immediately saved, even if you cancel the process before clicking Install. You can remove applications from Entra ID, but not from this pane (the record remains, with an error in the Status column). The option to remove applications will be available in future versions.

2. To create a new Entra ID application:
   a. Click New. The Create new Entra ID applications dialog is displayed.



   b. In Number of applications to automatically create, set the required number (default is 4).
   c. In Grant Global Administration consent for the permissions automatically, select whether to grant consent to the permissions that Varonis requires (specified in SharePoint Online Requirements).

      Note: Granting Global Administration consent is mandatory. If you uncheck this option, you will be obligated to grant consent manually after the application is created.

   d. Click Create. The first time you create applications, the Microsoft Sign in page is displayed and you are required to provide credentials (this is a one-time

operation that will not be required the next time you create applications).

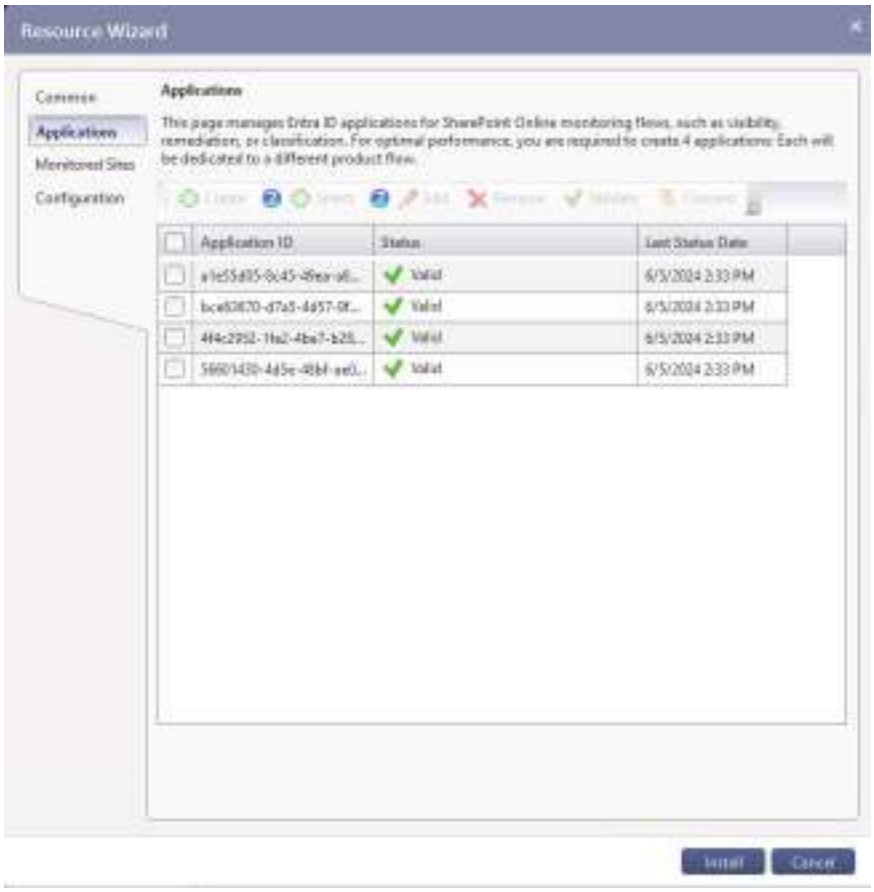


e. Enter the name of an account with permissions to create an Entra ID application and click Next.

f. Enter the account's password and click Sign in.



The specified number of new applications is created: The applications are added to the list, and you can follow its validation progress, indicated by the Status column.



If you did not grant consent for the application, the Status column indicates that consent is missing, and displays a Grant Consent for the application link.

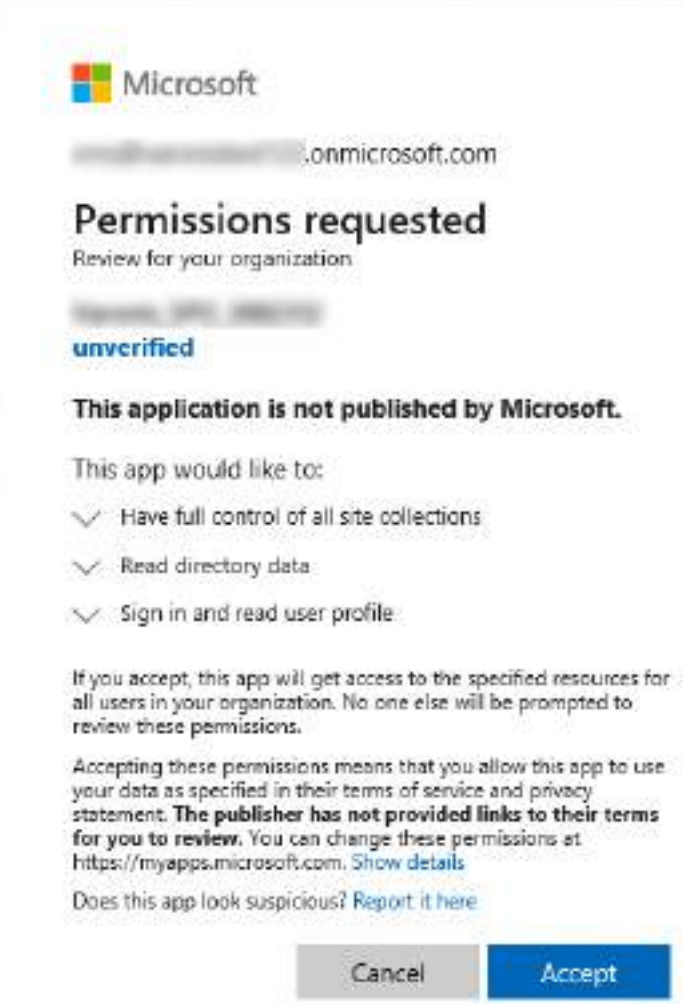


3. To manually grant consent after creating the application:
   a. In the applications list, click the Grant Consent for the application link. The Action Required dialog is displayed.



   b. Click the here link. The Microsoft Sign Inpage is displayed.
   c. Enter the Global Administrator username and password, click Sign In and then click Next. The Microsoft Permissions requested page opens, displaying the

Entra ID application name (at the top) and the permissions to be granted.



> Note: Only the Global Administrator is authorized to accept, grant, and give consent for the application's permissions.

d. Click Accept to grant these permissions and close the page.

e. Back in the Action Required dialog box, click OK to close it.
The application is validated and its status is updated.

> Note: During the synchronization of the application in Entra ID, the Click here to grant Global Admin consent for the permissions link may be displayed in this area. Wait, or grant consent if you haven't yet.

4. To use an existing Entra ID application:

> Important: Before you begin this procedure, make sure you have added a certificate via the Microsoft Entra admin center. Click here and go to step "5. Add a certificate" section for instructions.

When you use an existing application, it must be dedicated to a single data source. Proceed as follows:

a. Click Exist. The Use Existing Entra ID Application dialog box is displayed.



b. Enter the Application ID: To locate the Application ID, go to entra.microsoft.com > Identity > Applications > Enterprise applications, select the application you created, and copy the Application ID.

c. Enter the Certificate file path: Click the Browse (…) button to upload a certificate (public key) with a PFX file type.

d. Enter the Certificate file password. This is the password provided for the encryption of the PFX file.

e. Click OK to close the dialog box.

The existing application is added to the list.

5. Go to Manage applications used for SharePointOnline data classification and repeat the previous steps to add an Entra ID application.

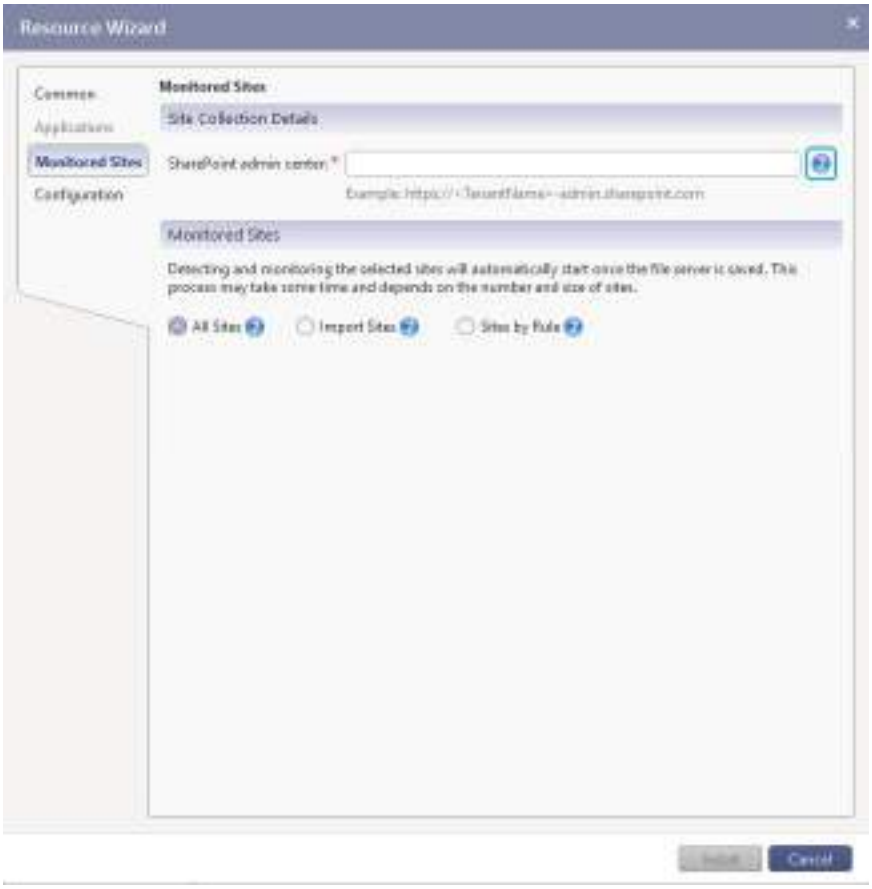
Continue to the Monitor sites pane to set the admin center URL and select the sites to be monitored.

4. Set the admin center URL and sites for monitoring

Configure the admin center URL and define which sites are monitored by Varonis: All sites or specific sites.

1. In the Monitored Sites pane, go to Site Collection Details.

2. In the SharePoint admin center field, enter the URL of the SharePoint admin center website in the format https://{tenant-name}-admin.sharepoint.com. To locate the URL, open the SharePoint admin center in a web browser and copy it.



Note: For an M365 Multi-Geo tenant, configure a separate SharePoint Online file server. For each geolocation, use the associated SharePoint admin center website.

3. In the Monitored Sites area, select the sites to be monitored by Varonis as follows:
   - Select All Sites to automatically detect and monitor all sites available on your tenant.

     Note: You can cancel the All Sites operation at any time and choose another option.

   - Select Import sites to monitor only sites specified in an imported list defined in a CSV or TXT file.
     To import a CSV or TXT file with specific sites:
     - Click Import sites.
       - For a TXT file, format each line as follows: URL, <url> or UPN, <upn>.

For example:

UPN,admin@varonis.com

URL,https://varonis.sharepoint.com

- For each line in a CSV file, fill the first column with the string “URL” or “UPN” and the second column with the actual URL or UPN.

- Select the CSV or TXT file and click Open.

  Note: The list of imported sites overrides the existing list of monitored sites.

- Select Sites by Rule to automatically detect and monitor only sites that meet a specific rule.

  Note: Choose this option to monitor a single M365 tenant that is shared by multiple organizations (sub-orgs).

  Choose one of the following rules:

  - Primary admin - Monitor only sites administered by members of the selected group. A primary admin is a user or a group who is a member of the “Site admins” group. Once you choose this option, you are required to enter the group name.
  - Owner- Monitor only sites owned by members of the selected group. An owner represents user(s) or group(s) who are member(s) of the “Site owners” group. Once you choose this option, you are required to enter the group name.
  - Site name - Monitor only sites whose names match the specified criteria: Select the relevant operator from the drop-down list (Contains, Starts with, or Ends with) and enter free text.

    Note: Keep in mind that the site name may be different from the site URL.

Continue to the Configuration pane to select list item types and the files to be collected.

5. Review and adjust configuration settings

1. On the left menu, click Configuration and confirm the information.

The general configuration settings are displayed.



2. In the List Item Types area, review the options.
3. In the Files to Collect area, review the options:
   - Files with classification hits - Files and list items with classification hits are collected according to the Data Classification Engine license and configuration. This checkbox is always selected and disabled.
   - Files with unique permissions - Collects files and list items that do not inherit permissions. These entities may have explicit permissions or links uniquely assigned to them. This checkbox is selected by default.
   - All files - Collects all files and list items. Selecting this option can result in reduced performance. This checkbox is cleared by default.

After configuration is complete, click Install to add the SharePoint Online data source.

A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the File Servers pane. When the installation completes, the status shows "Installed 100%".

6. (Post-Installation) Grant consent for File Analysis

To analyze data classification results of a file in SharePoint Online data sources, you should have the File Analysis Elevated Permissions role. To add the role to the user, in the Management Console, go to Configuration > Security. Alternatively, you can grant Global Administrator consent to the Varonis DCE application in Microsoft Entra ID. To do so, perform the steps below.

Important:

- The data source must already be installed for the DCE Application for File Analysis area to be visible.
- The application uses the permissions of the logged-in user to access files in SharePoint Online data sources so the user must have read permissions to the file they want to analyze.

1. In the File Servers grid of the Management Console, select the relevant data source for file analysis, and on the Resources toolbar, click Edit.
   The Editing file server window is displayed.
2. On the left menu, click Configuration.
3. In the DCE Application for File Analysis area, click the link in To grant Global Administrator consent for the application, click here.



You will be redirected to the Microsoft portal login page.

4. In the Microsoft Sign in page, enter the Global Administrator user name and click Next.



5. Enter the account password and click Sign in.



The Global Administrator consent status is changed to Granted in the DCE Application for File Analysis area.



6. Click Save to install the updates.
   A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the File Servers pane. When the installation completes, the status shows "Installed 100%".

What To Do Next

Now let's take a look at the supported events for the monitored SharePoint Online data sources.

Supported Events for SharePoint Online Data Sources

The following events are audited for SharePoint Online data sources:

- Detected malware in file
- File access request approved
- File copied
- File deleted
- File downloaded to a synced local folder
- File downloaded
- File invitation accepted
- File invitation canceled
- File invitation created
- File invitation updated
- File modified
- File moved
- File opened
- File referenced by Copilot interaction
- File renamed
- File restored
- File retention label changed
- File sensitivity label applied
- File sensitivity label changed
- File shared link created
- File shared link removed
- File shared link updated
- File shared link used
- File uploaded
- File uploaded from a synced local folder
- Folder access request approved

- Folder copied
- Folder created
- Folder deleted
- Folder invitation accepted
- Folder invitation canceled
- Folder invitation created
- Folder invitation updated
- Folder moved
- Folder renamed
- Folder restored
- Folder shared link created
- Folder shared link removed
- Folder shared link updated
- Folder shared link used
- Group added
- Group deleted
- Group member added
- Group member removed
- Members Can Share setting modified
- Permissions added
- Permission inheritance broken
- Permission inheritance restored
- Permissions removed
- Sensitivity label removed from site
- Sharing policy changed
- Site collection admin added
- Site collection admin removed
- Site deleted
- Site geo move scheduled
- Site geo move completed
- Site geo move canceled
- Site permission level added

- Site permission level modified
- Site permission level removed
- Site sensitivity label applied
- Site sensitivity label changed

OneDrive Data Sources

What This Section Contains

This section describes how to deploy and monitor OneDrive data sources; it includes the deployment and configuration steps and supported events.

What To Do Next

First, make sure you fulfill the OneDrive requirements.

After that, familiarize yourself with the deployment steps summary and then dive into the detailed procedure.

Adding a OneDrive Data Source - Summary

This section summarizes the procedure for deploying OneDrive data sources in the Management Console.

1. Run the Management Console as an administrator.
2. Select Management > Components > Root > Domains and verify that an Entra ID domain has been added.
3. Add a OneDrive data source: Select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.
4. Select the Resource type > SharePoint Online/OneDrive and then select OneDrive.
5. In the Resource Wizard's Common pane, check the Collector selected by default and change it if needed.
6. In the Connection Details area, go to Entra ID application and select your domain.
7. In the Applications pane, add four applications. Each application is dedicated to a specific product flow, for example: Data classification, visibility, remediation, etc.
8. Grant Global Administration consent for the permissions that Varonis requires.
9. In the Monitor Sites pane, go to Site Collection Details → SharePoint admin center and enter the URL of the SharePoint Admin Center website in the format https://{tenant-name}-admin.sharepoint.com.

10. In the Monitored Sites area, determine how to select the sites to be monitored by Varonis. Choose one of the following options:
    - All Sites - Automatically detect and monitor all sites available on your tenant.
    - Import sites - Monitor only sites specified in an imported list defined in a CSV or TXT file.
    - Sites by Rule - Automatically detect and monitor only sites that meet a specific rule: Primary admin or Owner.

      Note: Choose this option to monitor a single M365 tenant that is shared by multiple organizations (sub-orgs).
11. In the Configuration pane, review the List Item Types and Files to Collect.
12. After configuration is complete, click Install to add the OneDrive data source.
13. Grant consent to the Varonis DCE application for OneDrive file analysis.

What To Do Next

Now that you're familiar with the deployment steps, it's time to dive into the detailed procedure.

Adding a OneDrive Data Source - Detailed Procedure

This section describes the full procedure for deploying OneDrive data sources in the Management Console.

Before You Begin

Note the following:

- To reduce throttling issues, you are required to create separate applications for monitoring Entra ID, SharePoint Online, OneDrive, and Exchange Online.
- The procedure for deploying a OneDrive data source includes a step which you select whether to automatically register a new Entra ID application (using the Create new option), or to use an existing Entra ID application (using the Use existing option).
- When you select Create new, the Management Console automatically creates an application in Entra ID for you during the data source deployment.
- If you select Use existing, you must first have manually created an Entra ID application in Entra ID. You then configure the Entra ID application details during the data source deployment.

1. Check if an Entra ID data source exists

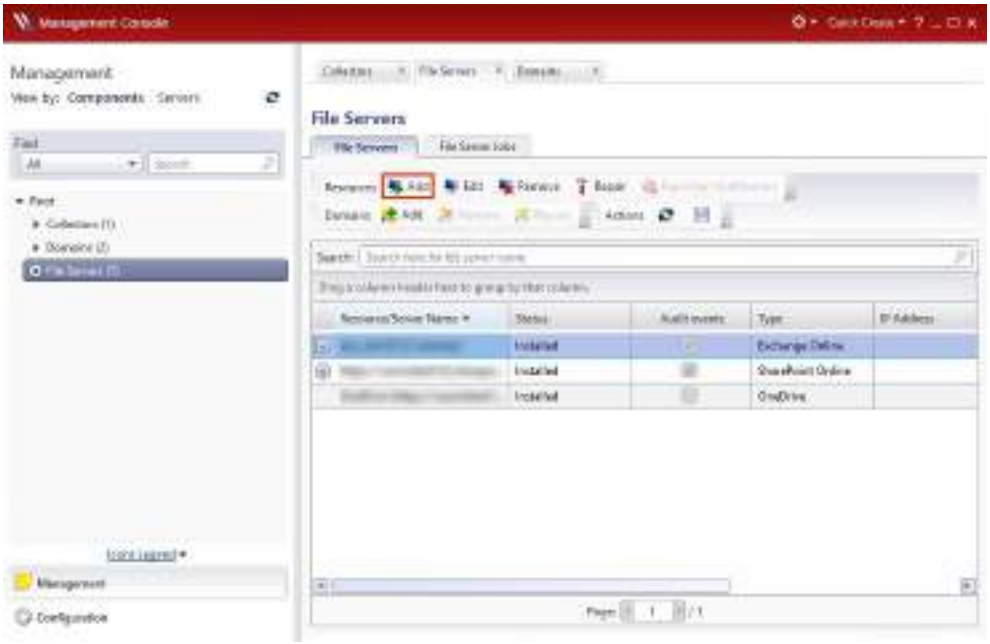
1. Run the Management Console as an administrator.
2. Select Management > Components > Root > Domains and verify that an Entra ID domain has been added.



2. Add a OneDrive data source

1. In the Management Console, select Management > Components > Root > File Servers.
2. In the File Servers tab, go to the Resources toolbar and click Add.

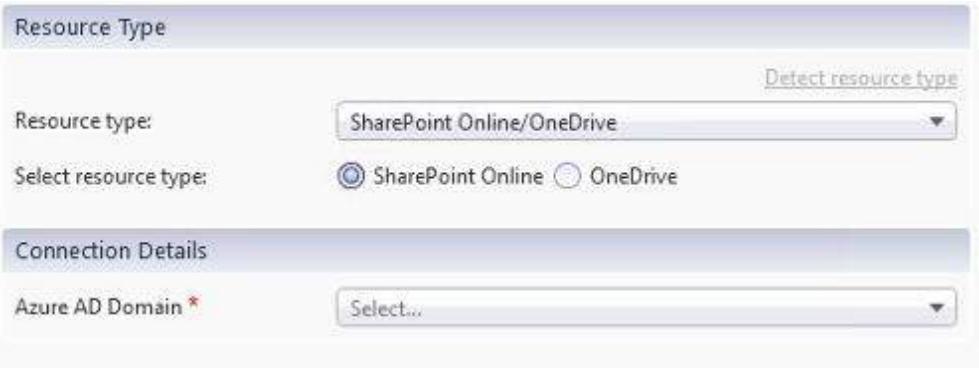
> Note: Alternatively, you can use the Quick Create menu on the title bar of the Management Console, and select Add New File Server.


Management Console
Management
View by: Components Servers
Find
All
Management
Configuration
File Servers
Add
Edit
Remove
Repair
Actions
Search
Status
Type
Installed
Exchange Online
SharePoint Online
OneDrive

The Resource Wizard is opened to the Common pane.



3. In the Resource Type area, select SharePoint Online/OneDrive from the dropdown list.
   In Select resource type, SharePoint Online is selected by default, and a new area - Connection Details - is displayed.



4. Change the selection to OneDrive.
5. In the Connection Details area, go to the Entra ID Domain dropdown list and select your domain.
   The Applications and Monitor Sites panes are enabled.

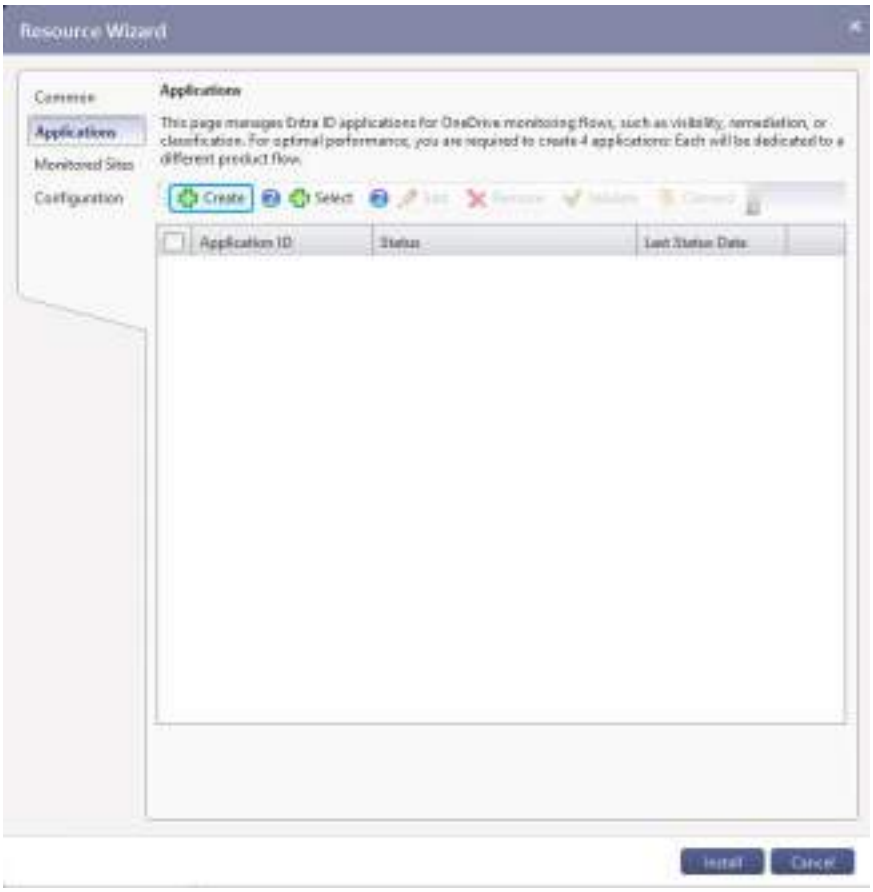
Continue to the Applications pane and configure Entra ID applications.

3. Configure Entra ID applications

Varonis uses Entra ID applications to monitor your data sources.The Applications pane allows you to create four unique Entra ID applications. Each application is dedicated to a specific product flow, for example: Data classification, visibility and remediation, etc.

> Note: If you previously deployed your data source with one or two applications, add the missing applications required to meet the recommendation of four applications per data source.

You can either add existing applications, or automatically create new applications. Only applications that are added here are used for scanning.



> Note: To automatically create applications, Varonis requires specific permissions (as specified in "Granting Consent to the VaronisAppRegistration Application

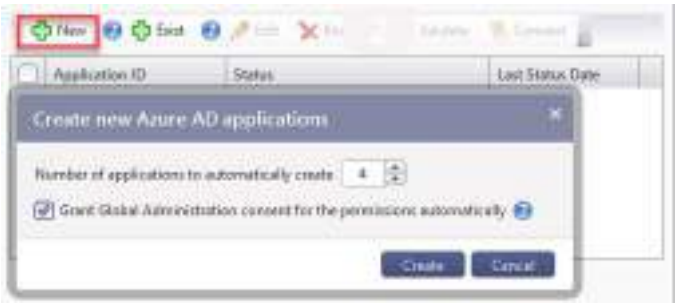
(Optional)" under General M365 Requirements). If you do not grant permissions to create Entra ID applications, you will only be able to add existing applications. If you do not grant permissions for automatic consent, you will need to grant consent manually for each new application you add.

To create and manage your Entra ID applications, take the following steps:

1. In the Applications tab, you can either create a new application, or add an existing application:
   - To create a new application - proceed to step 2
   - To add an existing application - proceed to step 3

   Note: When you create new applications, they are immediately saved, even if you cancel the process before clicking Install. You can remove applications from Entra ID, but not from this pane (the record remains, with an error in the Status column). The option to remove applications will be available in future versions.

2. To create a new Entra ID application:
   a. Click New. The Create new Entra ID applications dialog is displayed.



   b. In Number of applications to automatically create, set the required number (default is 4).
   c. In Grant Global Administration consent for the permissions automatically, select whether to grant consent to the permissions that Varonis requires (specified in OneDrive Requirements).

      Note: Granting Global Administration consent is mandatory. If you uncheck this option, you will be obligated to grant consent manually after the application is created.

   d. Click Create. The first time you create applications, the Microsoft Sign in page is displayed and you are required to provide credentials (this is a one-time

operation that will not be required the next time you create applications).



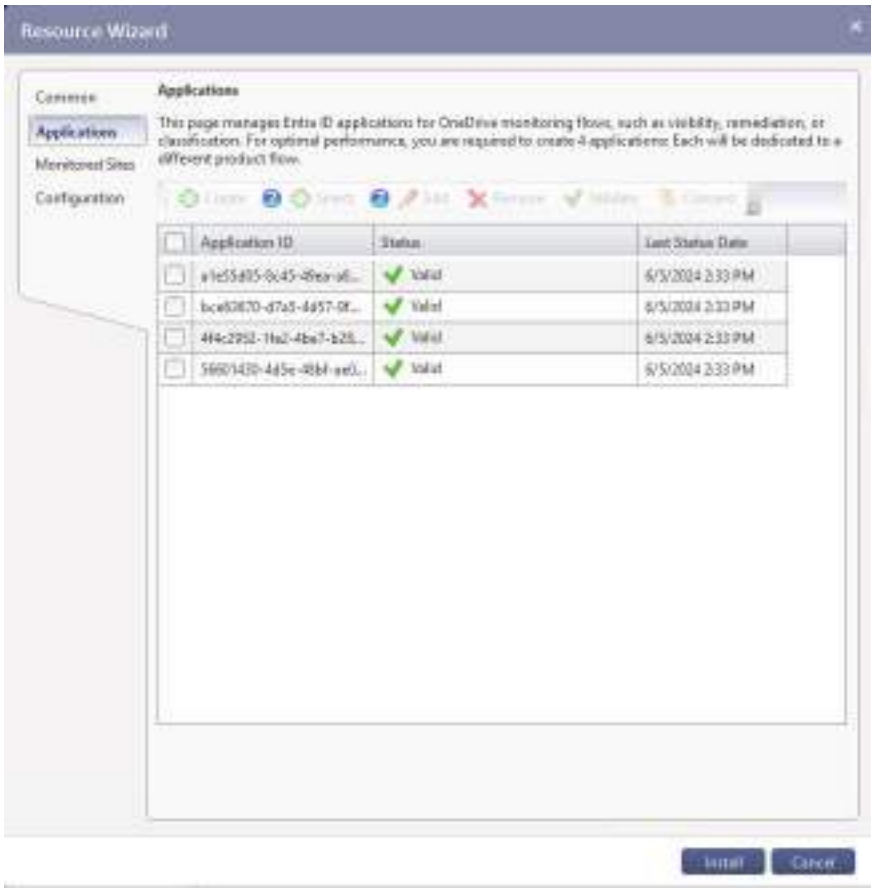
e. Enter the name of an account with permissions to create an Entra ID application and click Next.

f. Enter the account's password and click Sign in.



The specified number of new applications is created: The applications are added to the list, and you can follow its validation progress, indicated by the

Status column.



If you did not grant consent for the application, the Status column indicates that consent is missing, and displays a Grant Consent for the application link.

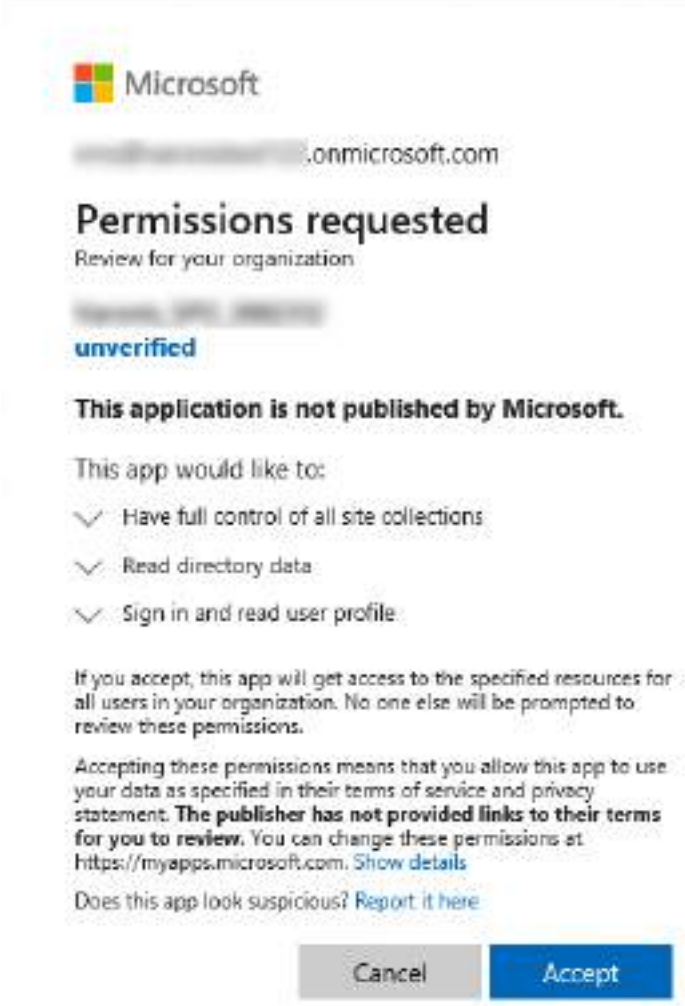


3. To manually grant consent after creating the application:
   a. In the applications list, click the Grant Consent for the application link. The Action Required dialog is displayed.



   b. Click the here link. The Microsoft Sign Inpage is displayed.
   c. Enter the Global Administrator username and password, click Sign In and then click Next. The Microsoft Permissions requested page opens, displaying the

Entra ID application name (at the top) and the permissions to be granted.



> Note: Only the Global Administrator is authorized to accept, grant, and give consent for the application's permissions.

d. Click Accept to grant these permissions and close the page.

e. Back in the Action Required dialog box, click OK to close it.
The application is validated and its status is updated.

> Note: During the synchronization of the application in Entra ID, the Click here to grant Global Admin consent for the permissions link may be displayed in this area. Wait, or grant consent if you haven't yet.

4. To use an existing Entra ID application:

> Important: Before you begin this procedure, make sure you have added a certificate via the Microsoft Entra admin center. Click here and go to step "5. Add a certificate" section for instructions.

When you use an existing application, it must be dedicated to a single data source. Proceed as follows:

a. Click Exist. The Use Existing Entra ID Application dialog box is displayed.



b. Enter the Application ID: To locate the Application ID, go to entra.microsoft.com > Identity > Applications > Enterprise applications, select the application you created, and copy the Application ID.

c. Enter the Certificate file path: Click the Browse (…) button to upload a certificate (public key) with a PFX file type.

d. Enter the Certificate file password. This is the password provided for the encryption of the PFX file.

e. Click OK to close the dialog box.

The existing application is added to the list.

5. Go to Manage applications used for OneDrive data classification and repeat the previous steps to add an Entra ID application.

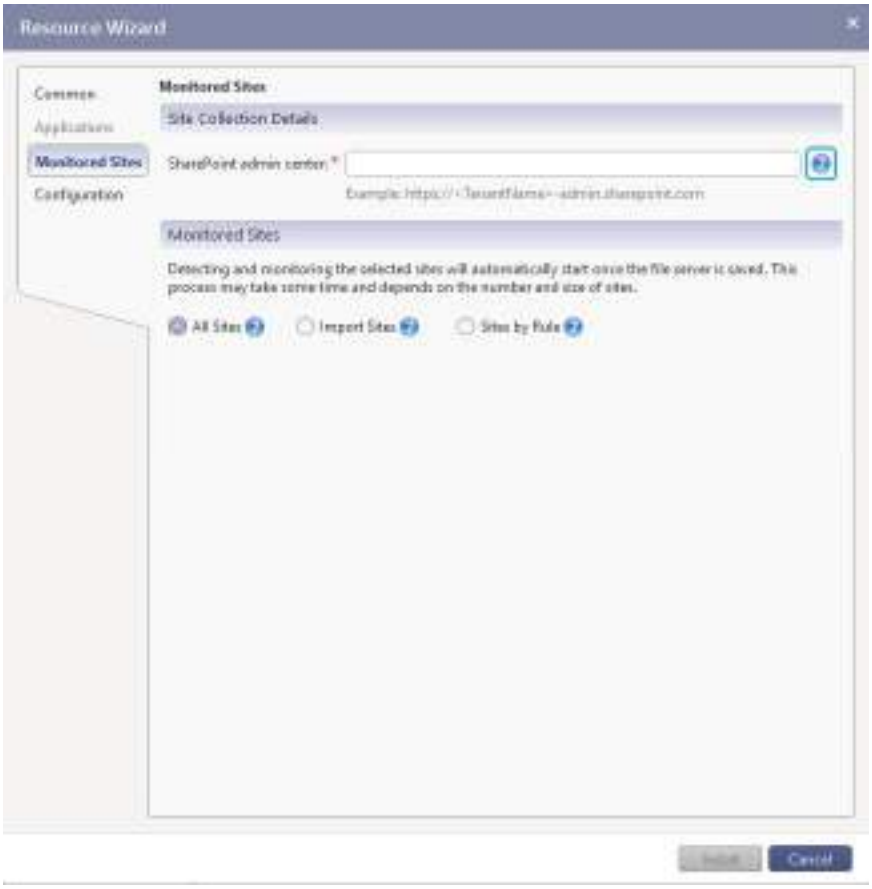
Continue to the Monitor sites pane to set the admin center URL and select the sites to be monitored.

4. Set the admin center URL and sites for monitoring

Configure the admin center URL and define which sites are monitored by Varonis: All sites or specific sites.

1. In the Monitored Sites pane, go to Site Collection Details.

2. In the OneDrive admin center field, enter the URL of the OneDrive admin center website in the format https://{tenant-name}-admin.sharepoint.com. To locate the URL, open the OneDrive admin center in a web browser and copy it.



Note: For an M365 Multi-Geo tenant, configure a separate OneDrive file server. For each geolocation, use the associated OneDrive admin center website.

3. In the Monitored Sites area, select the sites to be monitored by Varonis as follows:
   - Select All Sites to automatically detect and monitor all sites available on your tenant.

     Note: You can cancel the All Sites operation at any time and choose another option.

   - Select Import sites to monitor only sites specified in an imported list defined in a CSV or TXT file.
     To import a CSV or TXT file with specific sites:
     - Click Import sites.
       - For a TXT file, format each line as follows: URL, <url> or UPN, <upn>.

For example:

UPN,admin@varonis.com

URL,https://varonis.onedrive.com

- For each line in a CSV file, fill the first column with the string “URL” or “UPN” and the second column with the actual URL or UPN.

- Select the CSV or TXT file and click Open.

  Note: The list of imported sites overrides the existing list of monitored sites.

- Select Sites by Rule to automatically detect and monitor only sites that meet a specific rule.

  Note: Choose this option to monitor a single M365 tenant that is shared by multiple organizations (sub-orgs).

  Choose one of the following rules:

  - Primary admin - Monitor only sites administered by members of the selected group. A primary admin is a user or a group who is a member of the “Site admins” group. Once you choose this option, you are required to enter the group name.
  - Owner- Monitor only sites owned by members of the selected group. An owner represents user(s) or group(s) who are member(s) of the “Site owners” group. Once you choose this option, you are required to enter the group name.
  - Site name - Monitor only sites whose names match the specified criteria: Select the relevant operator from the drop-down list (Contains, Starts with, or Ends with) and enter free text.

    Note: Keep in mind that the site name may be different from the site URL.

Continue to the Configuration pane to select list item types and the files to be collected.

5. Review and adjust configuration settings

1. On the left menu, click Configuration and confirm the information.

The general configuration settings are displayed.



2. In the List Item Types area, review the options.
3. In the Files to Collect area, review the options:
   - Files with classification hits - Files and list items with classification hits are collected according to the Data Classification Engine license and configuration. This checkbox is always selected and disabled.
   - Files with unique permissions - Collects files and list items that do not inherit permissions. These entities may have explicit permissions or links uniquely assigned to them. This checkbox is selected by default.
   - All files - Collects all files and list items. Selecting this option can result in reduced performance. This checkbox is cleared by default. Selecting this option requires also selecting the files with unique permissions option to ensure that all the relevant files and list items are marked as such that are shared publicly or shared with external users.

After configuration is complete, click Install to add the OneDrive data source.

A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the File Servers pane. When the installation completes, the status shows "Installed 100%".

6. (Post-Installation) Grant consent for File Analysis

To analyze data classification results of a file in OneDrive data sources, you should have the File Analysis Elevated Permissions role. To add the role to the user, in the Management Console, go to Configuration > Security. Alternatively, you can grant Global Administrator consent to the Varonis DCE application in Microsoft Entra ID. To do so, perform the steps below.

Important:

- The data source must already be installed for the DCE Application for File Analysis area to be visible.
- The application uses the permissions of the logged-in user to access files in OneDrive data sources so the user must have read permissions to the file they want to analyze.

1. In the File Servers grid of the Management Console, select the relevant data source for file analysis, and on the Resources toolbar, click Edit.
   The Editing file server window is displayed.
2. On the left menu, click Configuration.
3. In the DCE Application for File Analysis area, click the link in To grant Global Administrator consent for the application, click here.



You will be redirected to the Microsoft portal login page.

4. In the Microsoft Sign in page, enter the Global Administrator user name and click Next.



5. Enter the account password and click Sign in.



The Global Administrator consent status is changed to Granted in the DCE Application for File Analysis area.



6. Click Save to install the updates.
   A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the File Servers pane. When the installation completes, the status shows "Installed 100%".

What To Do Next

Now let's take a look at the supported events for the monitored OneDrive data sources.

Supported Events for OneDrive Data Sources

The following events are audited for OneDrive data sources:

- Detected malware in file
- File access request approved
- File copied
- File deleted
- File downloaded to a synced local folder
- File downloaded
- File invitation accepted
- File invitation canceled
- File invitation created
- File invitation updated
- File modified
- File moved
- File opened
- File referenced by Copilot interaction
- File renamed
- File restored
- File retention label changed
- File sensitivity label applied
- File sensitivity label changed
- File shared link created
- File shared link removed
- File shared link updated
- File shared link used
- File uploaded
- File uploaded from a synced local folder
- Folder access request approved

- Folder copied
- Folder created
- Folder deleted
- Folder invitation accepted
- Folder invitation canceled
- Folder invitation created
- Folder invitation updated
- Folder moved
- Folder renamed
- Folder restored
- Folder shared link created
- Folder shared link removed
- Folder shared link updated
- Folder shared link used
- Group added
- Group deleted
- Group member added
- Group member removed
- Members Can Share setting modified
- Permissions added
- Permission inheritance broken
- Permission inheritance restored
- Permissions removed
- Sensitivity label removed from site
- Sharing policy changed
- Site collection admin added
- Site collection admin removed
- Site deleted
- Site geo move scheduled
- Site geo move completed
- Site geo move canceled
- Site permission level added

- Site permission level modified
- Site permission level removed
- Site sensitivity label applied
- Site sensitivity label changed

Exchange Online Data Sources

What This Section Contains

This section describes how to deploy and monitor Exchange Online data sources; it includes the deployment and configuration steps and supported events.

What To Do Next

First, make sure you fulfill the Exchange Online requirements.

After that, proceed to add an Exchange Online data source.

Adding an Exchange Online Data Source

This section describes the full procedure for deploying Exchange Online data sources in the Management Console.

Before You Begin

Note the following:

- To reduce throttling issues, you are required to create separate applications for monitoring Entra ID, SharePoint Online, OneDrive, and Exchange Online.
- The procedure for deploying an Exchange Online data source includes a step which you select whether to automatically register a new Entra ID application (using the Create new option), or to use an existing Entra ID application (using the Use existing option).
- When you select Create new, the Management Console automatically creates an application in Entra ID for you during the data source deployment.
- If you select Use existing, you must first have manually created an Entra ID application in Entra ID. You then configure the Entra ID application details during the data source deployment.

1. Check if an Entra ID domain exists

1. Run the Management Console as an administrator.
2. In the Management pane, go to Root > Domains and verify that an Entra ID domain has been added.

2. Add an Exchange Online data source

1. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.

   > Note: Alternatively, you can use the Quick Create menu on the title bar of the Management Console, and select Add New File Server.

   The Resource Wizard is opened to the Common pane.
2. In the Resource Details area, specify the data source name.
3. In the Resource Type area, select Exchange Online from the Resource type dropdown list.

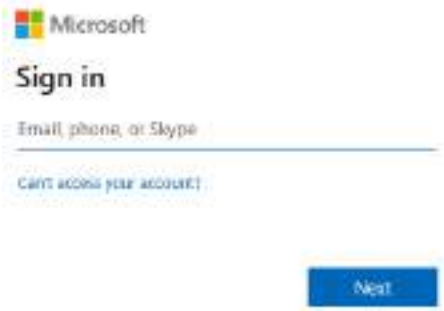


4. In the Connection Details area, select your Entra ID domain from the Entra ID Domain dropdown list.
   After the Entra ID domain is selected, additional options are displayed in the Connection Details area to automatically create a new Entra ID application or use an existing one.
5. In the Connection Details area, the Create New option is selected by default. You can decide to create a new Entra ID application (step 5a) or use an existing one that you've created in Entra ID (step 5b). Follow either of the procedures below to set up the required Entra ID application.



   a. To create a new Entra ID application:

i. Click the Browse (…) button next to the Entra ID application field. The Microsoft Sign in page opens.



Enter the credentials of a user with permissions to create an application in Entra ID. Enter the user name, click Next, enter the account password, and click Sign in.



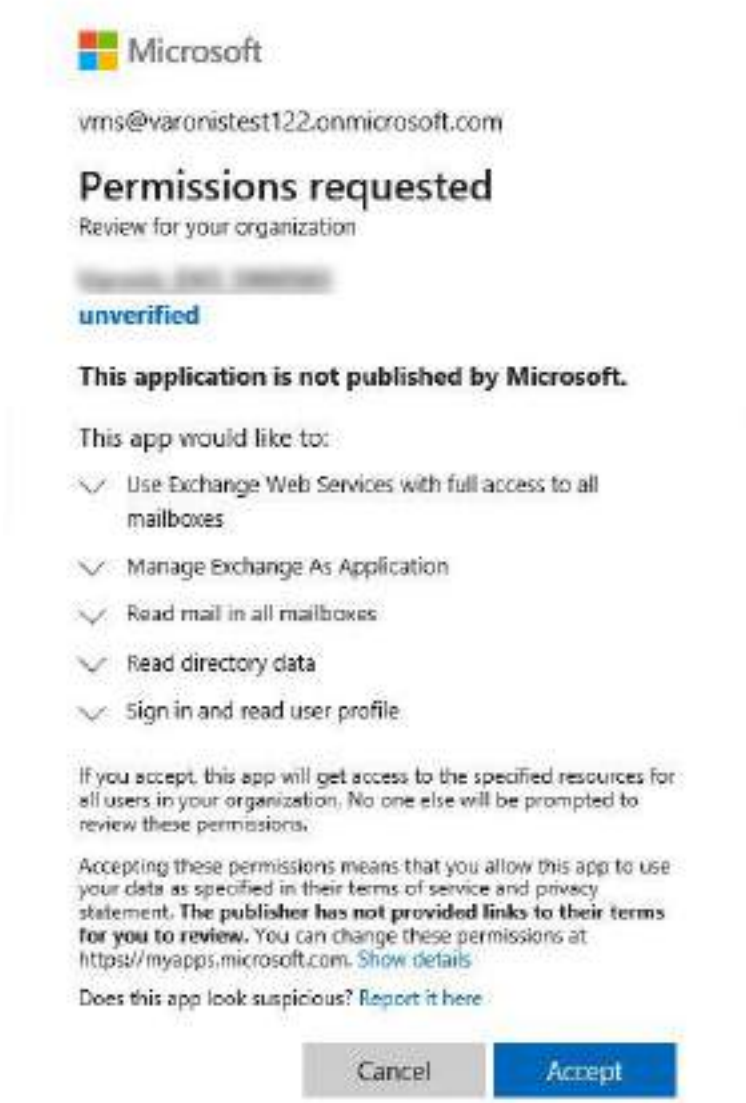
A new application is now created in Entra ID. When completed, a confirmation message is displayed indicating that the application was successfully created.



ii. Click the here link to grant this application permissions.

iii. Enter the Global Administrator credentials, user name and password, click Sign In and click Next. The Microsoft Sign In page is displayed. The Microsoft Permissions requested page opens, displaying the Entra ID application name

(at the top) and the permissions that should be granted.



iv. Only the Global Admin has the right to accept, grant, and consent these permissions. The Global Administrator must give consent for the application's permissions. Click Accept.

v. In the Management Console Action Required dialog box, click OK to close it.

vi. In the Connection Details area, the Entra ID application name is now displayed (it's grayed out).



> Note: During the synchronization of the application in Entra ID, the link Click here to grant Global Admin consent for the permissions may be displayed in this area. Wait, or consent if you haven't yet.

b. To use an existing Entra ID application:

> Important: Before you begin this procedure, make sure you have added a certificate via the Microsoft Entra admin center. Click here and go to step "5. Add a certificate" section for instructions.

When you use an existing application, it must be dedicated to a single data source. Proceed as follows:

i. In the Connection Details area, select Use existing.



ii. Click the Browse (…) button next to the Entra ID application field. The Use Existing Entra ID Application dialog box is displayed.



iii. Enter the Application ID. To locate the Application ID, go to entra.microsoft.com > Identity > Applications > Enterprise applications, select the application you created, and copy the Application ID.

iv. Enter the Certificate file path. Click the Browse (…) button to upload a certificate (public key) with a PFX file type.

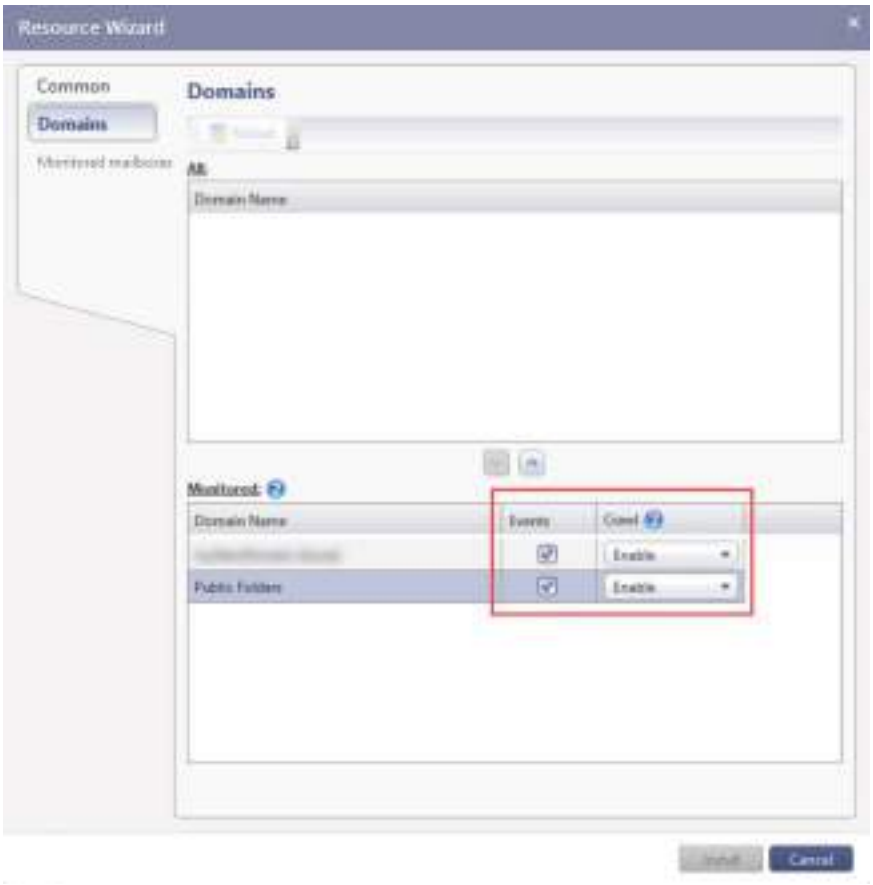
v. Enter the Certificate file path password. This the password provided for encryption of the PFX file.

vi. Click OK to close the dialog box.

6. To define monitored domains, on the left menu, click Domains.
7. In the All area, use the SHIFT key on your keyboard to select the Entra Exchange domain and Public Folders (if used). Click the arrow to add them to the Monitored area.



8. In the Monitored area, select the Events checkbox to activate event auditing for each domain.
9. In the Crawl column, enable or disable monitoring for each domain.



10. To define monitored mailboxes, on the left menu, click Monitored Mailboxes.



- Select All Mailboxes to automatically detect and monitor all mailboxes.

  Note: You can cancel the All Mailboxes operation at any time and then use the Import Mailboxes option instead.

- Select Import sites to monitor specific mailboxes from an imported list defined in a CSV or TXT file.

To import a CSV or TXT file with specific mailboxes:

a. Click Import Mailboxes.
   i. Create a CSV or TXT file.
   ii. For a TXT file, format each line as follows: UPN, <upn>. For example: UPN,admin@varonis.com
   iii. For each line in a CSV file, fill the first column with the string “UPN” and the second column with the actual UPN.

b. Select the CSV or TXT file and click Open.

   Note: The list of imported mailboxes overrides the existing list of monitored mailboxes.

After configuration is complete, click Install to add the Exchange Online data source.

A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the File Servers pane. When the installation completes, the status shows "Installed 100%".

What To Do Next

Now let's take a look at the supported events for the monitored Exchange Online data sources.

Supported Events for Exchange Online Data Sources

The following events are audited for Exchange Online data sources:

- Exchange folder created
- Exchange folder deleted
- Exchange folder moved - Supported for folders in mailboxes
- Exchange folder opened - Supported for public folders only
- Exchange folder permissions added
- Exchange folder permissions changed - Supported for mailbox and public folders. Also supported when performed using the Exchange admin center (EAC) or the Exchange Control Panel (ECP).
- Exchange folder permissions removed
- Exchange folder renamed - Supported for public folders only
- Forward rule created
- Forward rule updated
- Mailbox logon
- Mailbox permission added (includes Sent as, Sent on behalf of X and Full Access) - Also supported when performed using the Exchange admin center (EAC) or the Exchange Control Panel (ECP).
- Mailbox permission removed (includesSent as, Sent on behalf of X and Full Access) - Also supported when performed using the Exchange admin center (EAC) or the Exchange Control Panel (ECP).
- Message created
- Message deleted
- Message edited
- Message moved

- Message sent as
- Message sent on behalf
- Message sent
- Message received
- Public folder administrative permission added - Supported for public folders only
- Transport rule created
- Transport rule disabled
- Transport rule enabled
- Transport rule removed
- Transport rule updated
- Remove DLP policy
- Set mailbox audit bypass association
- Remove malware filter rule
- Remove malware filter policy
- Disable malware filter rule
- Disable safe attachment rule
- Disable safe links rule
- Remove antiphish policy
- Remove antiphish rule
- Disable antiphish rule
- Set DKIM signing config
- Role group member added
- Role group member removed
- Role group role assignment added
- Role group role assignment removed
- Role group added
- Role group deleted
- Deleted quarantined message
- Exported quarantined message
- Previewed quarantined message
- Released quarantined message
- Requested to release quarantined message

- Viewed quarantined message header

Note: For the Mailbox permission added or removed (sent on behalf of X) event types, the following two events are created:

- Remove all Sent on behalf of X permission events
- Add the Sent on behalf of X permission event, to include all users to which the permission was granted

Note: Message copied events are no longer supported. Message copied events could previously be audited only by using the cmdlets `Search-Mailbox` and `New-MailboxSearch`, which were retired in July 2020, and are no longer supported by Microsoft.

What To Do Next

Next, take a look at the supported mailboxes for the monitored Exchange Online data sources.

Supported Mailboxes for Exchange Online

The following mailboxes are supported for Exchange Online data sources:

- User mailboxes
- Shared mailboxes

What To Do Next

Read on to find out how to improve FileWalk performance for large Exchange Online environments.

Improving Directory Structure Crawling for Large Exchange Online Environments

For environments with more than 50,000 mailboxes, Exchange Remote PowerShell throttling policies must be updated to align with the tenant size. The PowerShell throttling policy determines the number of cmdlets that can be run every five seconds without being throttled.

This operation improves directory structure monitoring performance and reduces scanning time. To increase the PowerShell throttling policies, see the Microsoft documentation, or perform the following procedure:

1. Make sure that you have purchased a full subscription that allows you to view and operate throttling diagnostics on tenants.
2. Make sure that the organization is hydrated and that you can run the Enable-OrganizationCustomization command in the Exchange Online PowerShell.
3. In the Microsoft 365 Admin Center, click the help icon and type “Exchange PowerShell Throttling” in the search box.
4. Select Update throttling policies to align with your tenant size and click Run Test.

6 NETAPP DATA SOURCES

What This Section Contains

This section describes how to deploy and monitor NetApp data sources; the requirements, deployment and configuration steps, and supported events.

What To Do Next

Before you dive in, click here to learn more about how Varonis monitors NetApp accounts, file system, and events.

NetApp Monitoring Overview

Note: Each NetApp data source represents a monitored NetApp server. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source.

Varonis monitors NetApp via the following parallel data streams.

Accounts

- Varonis enumerates local account information remotely from the Collector with a dedicated service account.

File System

- Varonis collects folder structure, permissions, and metadata via a dedicated service for directory structure monitoring (FileWalk) that runs on the assigned Collector. This connection is made over SMB.

Data Classification and Labeling

- Varonis supports data classification and labeling on files that reside in the monitored data sources.

Events

- An FPolicy is configured on the NetApp data source to send event data relevant for the monitored file system to the assigned Collector.

What To Do Next

First, make sure you fulfill the NetApp requirements.

NetApp Requirements

Varonis Service Account

Varonis requires a dedicated service account. The service account can be reused for multiple data source installations and configurations.

- Service Account Read Operations:
  - Traverse and enumerate files, folders, directory structures, users, and groups.
  - Gather data source, user, and group metadata as part of normal system operations.
- Service Account Write Operations:
  - Used for executing Varonis Policies, if policies are defined.

Varonis Installation and Requirements

- Creation of a new FPolicy is required (requires root credentials).
- The NetApp proxy requires only a Windows data source on which the Varonis Windows agent is installed.

Requirements for the Varonis Service Account for Read Operations (Relevant for Cluster Mode Only)

- IMPORTANT: To preserve the access data on files, the Varonis service account must be a member of the Backup Operators group. Otherwise, the access data will be changed.
- To add a member to the Backup Operators and Power User groups, run the following commands (enter the relevant parameters for `VSERVER` and `DOMAIN\USER`):

```
vserver cifs users-and-groups local-group add-members -gr
oup-name "BUILTIN\Backup Operators" -vserver VSERVER -mem
ber-names DOMAIN\USER
```

```
vserver cifs users-and-groups local-group add-members -gr
oup-name "BUILTIN\Power Users" -vserver VSERVER -member-n
ames DOMAIN\USER
```

- To add Varonis service account read permissions, run the following command (enter the relevant parameters for SHARE, VSERVER, and DOMAIN\USER):

```
vserver cifs share access-control create -share SHARE -us
er-or-group DOMAIN\USER -user-group-type windows -permiss
ion Read -vserver VSERVER
```

  For more information about the ONTAP CLI commands, see the NetApp ONTAP documentation

- To configure the Varonis service account for Unix, NFS-based, set the following:
  - UID defined with read permissions on exported volumes
  - UID=0 must be honored from the Collector server.
- To verify that the commands worked, run the following commands (enter the relevant parameter for VSERVER):

```
vserver cifs users-and-groups local-group show-members -v
server VSERVER -group-name "BUILTIN\Backup Operators"
```

```
vserver cifs users-and-groups local-group show-members -v
server VSERVER -group-name "BUILTIN\Power Users"
```

- To connect from the Collector to the proxy and retrieve events, use the same account for account enumeration/Varonis service account. Make sure the user has these permissions:
  - A member of the VaronisEventsRetrieval group with permissions to read status, interrogate, query status, pause/continue, start/stop services on the Windows Server where the AD proxy is installed; the VaronisEventsRetrieval group should be configured as a Domain local (group scope) Security group (group type)
  - A member in any of these groups:
    - Administrators
    - Power Users
    - Backup Operators
- Amazon FSx for NetApp ONTAP has an issue with adding REST API permissions. Use the vsadmin role as a workaround.

Requirements for the Varonis Service Account for Write Operations (Relevant for Cluster Mode Only)

In addition to the requirements for the read operations, the Varonis service account for write operations requires SMB (CIFS) SeTcbPrivilege privileges.

REST API Requirements (Relevant for Cluster Mode Only)

- Varonis supports REST API in NetApp cluster mode.
- Important to note that the transition from ONTAPI/ZAPI to REST API is not significantly urgent since ONTAPI/ZAPI will still be supported for the next few versions. Reference the below:
  - NetApp versions released in June 2023 (9.13.1) will still support ZAPI.
  - NetApp versions released in December 2023 (9.14.1) and June 2024 (9.15.1) will automatically detect if ZAPI is used and enable it automatically. You can also enable it manually.
  - NetApp versions released in December 2024 (9.16.1) and June 2025 (9.17.1) will not automatically support ZAPI and can be enabled upon request to NetApp if needed.
  - Starting December 2025 (9.18.1), ZAPI will not be supported.
- To use REST API calls, a new role called rest-role will need to be created. The rest-role is a set of permissions for executing REST API calls. Due to Netapp limitations, the Varonis custom rest-role can be created for versions 9.13.1 and up. Follow the steps below to create the rest-role, attach it to the user, and verify it:
  - To create the rest-role vrns_rest_role and add the correct permissions, run following commands:

```
security login rest-role create -role vrns_rest_role -a
pi /api/network/ip/interfaces  -access readonly -vserve
r  DATA_LIF_VSERVER

security login rest-role create -role vrns_rest_role -a
pi /api/protocols/cifs/local-groups  -access all -vserv
er  DATA_LIF_VSERVER

security login rest-role create -role vrns_rest_role -a
pi /api/protocols/cifs/local-users  -access readonly -v
```

```
server  DATA_LIF_VSERVER

security login rest-role create -role vrns_rest_role -a
pi /api/protocols/cifs/shares  -access all -vserver  DA
TA_LIF_VSERVER

security login rest-role create -role vrns_rest_role -a
pi /api/protocols/fpolicy  -access all -vserver  DATA_L
IF_VSERVER

security login rest-role create -role vrns_rest_role -a
pi /api/storage/qtrees -access readonly -vserver  DATA_
LIF_VSERVER

security login rest-role create -role vrns_rest_role -a
pi /api/storage/volumes  -access readonly -vserver  DAT
A_LIF_VSERVER

security login rest-role create -role vrns_rest_role -a
pi /api/svm/svms  -access readonly -vserver  DATA_LIF_V
SERVER

security login rest-role create -role vrns_rest_role -a
pi /api/cluster -access readonly -vserver  DATA_LIF_VSE
RVER
```

- Attach the vrns_rest_role to the domain Admin user or Varonis service account with this command:

```
security login create -user-or-group-name DOMAIN\USER -
application http -authentication-method domain -role vr
ns_rest_role -vserver  DATA_LIF_VSERVER
```

- Verify by running these commands:

```
security login show -vserver DATA_LIF_VSERVER
```

```
security login rest-role show -vserver DATA_LIF_VSERVER
 -role vrns_rest_role
```

The above commands should show 10 entries in the rest-role.

Notes

- Varonis supports NetApp local accounts.
- The Lenovo ThinkSystem DM Series runs the ONTAP data management software. Varonis detects the Lenovo ThinkSystem DM data sources as NetApp.
- SMBv3 is supported for NetApp clusters.
- FPolicy API - v7.1.x is not supported.
- To work with NetApp in cluster mode, you need to create a login method. You can either use the predefined vsadmin role or create a new role with the required permissions listed in Creating a Login Method for Varonis SaaS.
- Varonis service account is supported as a local account and not only as a domain user. Domain membership is recommended, but not mandatory.
- ONTAP versions released before April 2023 do not use RPC Sealing, so when NetApp attempts to authenticate our service account to the DC, it will fail. To resolve this, create the following registry key on the DCs as a workaround and set the registry key to 1 (compatibility mode):

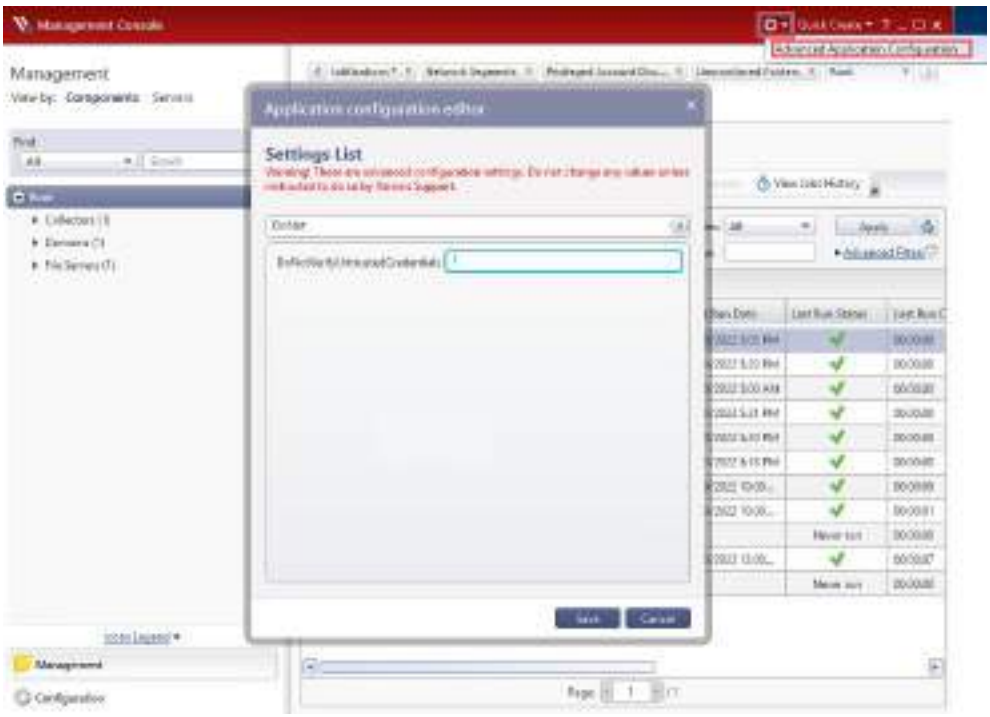
Registry key	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters
Value	RequireSeal
Data type	REG_DWORD
Data	1 - Compatibility mode. Windows domain controllers will require that Netlogon clients use RPC Seal if they are running Windows, or if they are acting as either domain controllers or Trust accounts. 2 - Enforcement mode. All clients are required to use RPC Seal. For

	more information, see this Microsoft article.
Restart required?	No

For more information, see this KB article.

To use FileWalk as a local user, perform the following steps:

1. Navigate to the FileWalk directory: Program Files (x86)\Varonis\DatAdvantage\GridCollector\FilewalkNA.
2. Open the config file Varonis.Core.FileWalkWorker.exe.varonis.config, and under the section <ntap_cm>, set DisableWinImpersonation to 1.
3. Open the Management Console, go to Tools > Advanced Application Configuration, and set DoNotVerifyUntrustedCredentials to 1.



4. Restart the Management Console.

What To Do Next

Next, take a look at Amazon FSx for NetApp ONTAP.

Mixed Security Style In NetApp Data Sources

Security style refers to the style of file permissions and the type of authorization needed to access the directories and files within a volume or qtree.
On NetApp data sources, the qtree security style indicates the type of security that is in effect. The following options are available:

- qtree with Unix security style - Indicates that the qtree's file security style is Unix-based
- qtree with NTFS security style - Indicates that the qtree's file security style is Windows-based
- qtree with Mixed security style - Indicates that either the Unix or the NTFS file security style can be the effective security style for each file or folder within the qtree.

With mixed volumes or qtrees, each file or folder has only one security style. It can be either NTFS or Unix, but not both.

A file's security style depends on whether the permission was last set from CIFS or NFS. For example, if a file currently uses the Unix security style and a CIFS user sends a set-ACL request to the file, the file's security style is changed to NTFS. If a file currently uses the NTFS style and an NFS user sends a set-permission request to the file, the file's security style is changed to Unix.

- Data in all three security styles can be accessed from both Windows and Unix hosts, if the appropriate user mapping is in place and if the share, export, and file access permissions allow it.
- For the Unix security style, authorization to access directories and files is based on access allowed to the user's Unix UID and GIDs, with access rules following the Unix style of file permissions (rwxrwxrwx).
- For the Windows security style, authorization to access folders and files is based on access allowed to the user's Windows SID and Windows group SIDs, with access rules based on NTFS Windows security descriptors.

Monitoring NetApp with Mixed Security Style

- If the security style is NTFS or mixed security, Varonis will automatically use CIFS for monitoring the data source. If the security style is Unix, Varonis will use NFS to monitor the data source.
- The Protocol column shows either CIFS or NFS. If your server's exposed protocol is not compatible with the security style, the share row in the Available Shares grid

will be grayed out and you will not be able to register the share. A tooltip in the Access Details column will indicate the protocol mismatch.

- All NFS and CIFS events are audited regardless of the protocol used for monitoring.
- NFS v3 should be enabled.
- The Collector IP should be listed in the export policy of the share with read permissions.
- The NFS exports should be mountable.

Amazon FSx for NetApp ONTAP

Amazon FSx for NetApp ONTAP is a fully managed shared storage in the AWS Cloud built on NetApp ONTAP file system.

Varonis SaaS detects and handles the Amazon FSx for NetApp ONTAP data sources as NetApp. All the information and steps described in this guide are relevant for Amazon FSx for NetApp ONTAP.

Version Support

FSx for NetApp ONTAP is a fully managed service; tenants are constantly updated with the latest ONTAP GA version.

Each ONTAP GA version is followed by an FSx ONTAP release which is automatically deployed to all tenants in the next maintenance window. That means that there are a maximum of two versions deployed across all tenants simultaneously, and Varonis will proactively certify and support those versions.

What To Do Next

Now learn about the performance recommendations for monitored NetApp data sources.

NetApp Performance Recommendations

- For ONTAP versions 9.8 and higher, the recommended send buffer size may be different than the default value (256KB). See the official NetApp guide for instructions how to calculate and set up the correct send buffer size.
  - To check the existing buffer size, run the following command on the NetApp data source:

```
vserver fpolicy policy external-engine show -vserver <v
server_name> -engine-name <external-engine_name>   iphw
 send-buffer-size
```

The value will be shown in bytes.

- It is recommended to shorten the time interval in which the node waits for a response from the FPolicy server; this enables releasing pending items sooner. This could be very useful with long latency between the Collector and the FPolicy server, environments with event rate spikes, and other such cases. The default value is 40s; the recommended value is 5s. Use the following command to set the value:

  ```
  fpolicy policy external-engine modify [-reqs-abort-timeou
  t <[<integer>h][<integer>m][<integer>s]>]
  ```

  See the official NetApp FPolicy configuration guide for more details.

What To Do Next

Now it's time to configure FPolicies for NetApp data sources operating in cluster mode.

Configuring FPolicies for NetApp Data Sources Operating in Cluster Mode

To enable Varonis SaaS to connect to a NetApp data source operating in cluster mode, you must configure an FPolicy for it.

FPolicy Overview

The FPolicy structure is defined as follows:

- Events Policy - Defines which operations and protocol types the FPolicy will audit.
- External Engine - Defines the end point (the Varonis Collector) to which the FPolicy sends notification information.
- Policy - The aggregation of events policy, external engine, and scope.
- Scope - Defines the volumes, shares, export policies, and file extensions to which the FPolicy policy will apply. You can also include and exclude all relevant filters.

  Note: The shares must reside on the volume monitored for CIFS events.

Limitation

- Not all ONTAP versions accept certificates signed by an intermediate Certificate Authority (CA) for FPolicy connections for SSL/TLS server authentication. For more information and to verify if your version supports this functionality, see the following NetApp KB article.

What To Do Next

Follow the instructions in the next topic to create an FPolicy event using the TCP protocol.

Creating an FPolicy Event Using the TCP Protocol

To create an FPolicy event, you must be a user with the vsadmin role and have a user name that is associated with the ontapi application. The order in which you create an FPolicy event is important.

> Note: The vsadmin role is only required for this procedure when creating the FPolicy.

To create an FPolicy event using TCP:

1. Connect to NetApp Data ONTAP management.
2. To create and verify an FPolicy event object:
   a. For NetApp ONTAP versions 9 and higher, run the following command:
   For SMB (CIFS) events:
   - _ setattr-with-owner-change _ - Filter the client setattr requests for changing the owner of a file or directory.
   - _ setattr-with-sacl-change _ - Filter the client setattr requests for changing sacl on a file or directory.
   - _ setattr-with-dacl-change _ - Filter the client setattr requests for changing dacl on a file or directory.

```
fpolicy policy event create -vserver VSERVER -event-nam
e fp_event_varonis_cifs   pi stivations create, create_
dir, delete, delete_dir, open, read, write, rename, ren
ame_dir, setattr -protocol cifs   pxivw  vwx viad,  vwx
```

```
 0vmxi$ open-with-delete-intent, setattr-with-owner-cha
nge, setattr-with-sacl-change, setattr-with-dacl-change
```

For NFS events:

- _ setattr-with-owner-change _ - Filter the client setattr requests for changing the owner of a file or directory.
- _ setattr-with-group-change _ - Filter the client setattr requests for changing the group of a file or directory.
- _ setattr-with-mode-change _ - Filter the client setattr requests for changing the mode bits on a file or directory.

```
fpolicy policy event create -vserver <Vserver Name> -ev
ent-name fp_event_varonis_nfsv3   pi stivations create,
 create_dir, delete, delete_dir, read, write, rename, r
ename_dir, setattr -protocol nfsv3   pxivw  vwx viad,
vwx 0vmxi$ setattr-with-owner-change, setattr-with-grou
p-change, setattr-with-mode-change
```

Starting from NetApp ONTAP version 8.3.1, run the following command:

For SMB (CIFS) events:

```
fpolicy policy event create -vserver VSERVER -event-nam
e fp_event_varonis_cifs   pi stivations create, create_
dir, delete, delete_dir, open, read, write, rename, ren
ame_dir, setattr -protocol cifs   pxivw  vwx viad,  vwx
 0vmxi$ open-with-delete-intent
```

For NFS events:

```
fpolicy policy event create -vserver <Vserver Name> -ev
ent-name fp_event_varonis_nfsv3   pi stivations create,
 create_dir, delete, delete_dir, read, write, rename, r
ename_dir, setattr -protocol nfsv3   pxivw  vwx viad,
vwx 0vmxi
```

For lower ONTAP versions, run the following command (enter the relevant parameter for VSERVER):

```
fpolicy policy event create -vserver VSERVER -event-nam
e fp_event_varonis_cifs   pi stivations create, create_
dir, delete, delete_dir, read , write, rename, rename_d
ir, setattr -protocol cifs   pxivw  vwx viad,  vwx 0vmx
i
```

Where:

- `-vserver` - The name of the Vserver on which you want to create an FPolicy event.
- `-event-name` - The name of the FPolicy event that you want to create.
- `pi stivations` - The file operations for the FPolicy event. For example: `create, create_dir, delete, delete_dir, read, write, rename, rename_dir, setattr`.
- `-protocol` - The name of the protocol for which the event is created. Possible values are:
  - `cifs`
- `pxivw` - Specifies the filters used with a given file operation for the protocol specified in the `-protocol` parameter. For example: `vwx viah$ vwx 0vmxi`.

  Note: While use of the `vwx viad` filter can result in dramatic improvement in NetApp performance, it may not be used concurrently with the Filter False-Open Events feature.

b. To view the event object, run the following command:

```
fpolicy policy event show fp_event_varonis_<protocol> –
instance
```

3. To create and verify an FPolicy external engine:
   a. Run the following command (enter the relevant parameter for VSERVER and COLLECTOR_IP):

```
fpolicy policy external-engine create -vserver VSERVER
-engine-name fp_ex_eng -primary-servers COLLECTOR_IP -p
ort 2002 -extern-engine-type asynchronous -ssl-option n
o-auth
```

Where:

- `-vserver` - The name of the Vserver on which you want to create an FPolicy external engine
- `-engine-name` - The name of the external engine that you want to create
- `-primary-servers` - The IP addresses for the primary FPolicy servers
- `-port` - The port number for the FPolicy service
- Note: By default, the port number for the TCP protocol is 2002. This can be changed by configuring another port in the `VrnsForwarderSvc.exe.vavsrmw#gsr k` file.
- `-extern-engine-type` - The type of external engine. Only asynchronous is supported.

b. To view the external engine you created, run the following command:
`FPolicy policy external-engine show`

4. To create and verify an FPolicy object:
   - For NetApp ONTAP versions 9.14.1 and higher:
     - Create an empty volume on the SVM that can be provisioned for the persistent store:

```
volume create -vserver <SVM Name> -volume <volume> -s
tate <online> -policy <default> -unix-permissions <77
7> -size <value> -aggregate <aggregate name> -snapsho
t-policy <none>
```

       - An aggregate is a collection of disks (or partitions) arranged into one or more RAID groups. For more information, see the NetApp article What is an aggregate? - NetApp Knowledge Base.
       - Recommended volume size for the persistent store is 32GB. For a calculation with greater precision, see the NetApp article Create persistent stores.
     - Create the persistent store:

```
vserver fpolicy persistent store create -vserver <SVM
> -persistent-store <PS_name> -volume <volume>
```

       - persistent-store: The persistent store name
       - volume: The persistent store volume

- Run the following command:
  - For existing fpolicies, run this command:

```
vserver fpolicy policy modify -vserver VSERVER -po
licy-name fp_event_varonis_cifs -persistent-store
<PS_name>
```

  - For new fpolicies, run this command:

```
fpolicy policy create -vserver VSERVER -policy-nam
e Varonis -events fp_event_varonis_cifs -engine fp
_ex_eng -is-mandatory false -persistent-store <PS_
name>
```

  - To view the policy you created, run `fpolicy policy show`.
- For lower ONTAP versions:
  - Run the following command (enter the relevant parameter for VSERVER):
    `fpolicy policy create -vserver VSERVER -policy-name Var onis -events fp_event_varonis_cifs -engine fp_ex_eng -i s-mandatory false`
    Where:
    - `-vserver` - The name of the Vserver on which you want to create an FPolicy policy.
    - `-policy-name` - The name of the FPolicy policy that you want to create. The default policy name, as registered in the Management Console, is `Varonis`.
    - `-events` - A list of events to monitor for the FPolicy policy.
    - `-engine` - The name of the external engine for this FPolicy policy.
    - `-is-mandatory` - Determines whether the FPolicy object is mandatory.
  - To view the policy you created, run `fpolicy policy show`.

5. To create and verify an FPolicy scope object:
   a. Run the following command (enter the relevant parameter for VSERVER):

```
fpolicy policy scope create -vserver VSERVER -policy-na
me Varonis -volumes-to-include "*" -export-policies-to-
include "*"
```

Where:

- `-vserver` - The name of the Vserver on which you want to create the FPolicy scope for an FPolicy policy.
- `-policy-name` - The name of the FPolicy policy for which the FPolicy scope will be created. The default policy name, as registered in the Management Console, is `Varonis`.
- `-volumes-to-include` - A comma-separated list of volumes to be monitored. Varonis recommends monitoring all volumes. Wildcards are supported.
- `-export-policies-to-include` - A comma-separated list of export policies for monitoring file access. Wildcards are supported.

> Note: The shares must reside on the volume monitored for CIFS events.

b. To view the FPolicy scope you created, run the following command (enter the relevant parameter for VSERVER):

```
fpolicy policy scope show -vserver VSERVER -policy-name
 Varonis
```

6. To enable the new FPolicy policy, run the following command (enter the relevant parameter for VSERVER):

```
fpolicy enable -vserver VSERVER -policy-name Varonis –seq
uence-number <seq no>
```

What To Do Next

Create a login method to enable working with NetApp in cluster mode.

Creating a Login Method for Varonis SaaS

You must create a login method to enable working with NetApp in cluster mode.

> Important:
>
> - Both the domain and the user name are case-sensitive and must be identical to those defined in the Management Console.
> - Ensure that the name of the Varonis service account is limited to 15 characters.

Assigning the vsadmin Role

To assign the vsadmin role:

1. Connect to NetApp ONTAP data management.
2. Run the following command (enter the relevant parameters for `DOMAIN\USER` and `VSERVER`):

   ```
   security login create -username DOMAIN\USER -application
   ontapi -authmethod domain -role vsadmin -vserver VSERVER
   ```

   Where:

   - `-username` - The user name of the login method.
   - `-application` - The application of the login method.
   - `-authmethod` - The Active Directory authentication method of the login method.
   - `-role` - The access-control role name for the login method.
   - `-vserver` - The Vserver name of the login method.
3. After the command is executed, issue the `security login show` command to view information about the user login methods on the data source.

Creating a Custom Varonis Role

Certain permissions are required to perform the following activities:

- Start the FPolicy engine after the Collector starts
- Get the volume information
- Get the `gpswi sr qshm gation` settings
- Get user information

Ordinarily, the predefined vsadmin role is sufficient. If it is not possible to use this role, use the following permissions:

Note: Some roles have the `-access` parameter set to `all` and not `readonly` so that the FPolicy can be enabled or disabled as needed.

Run the following commands (enter the relevant parameter for `VSERVER`):

- `security login role create -role vrnsrole -cmddirname "vserver fpolicy" -vserver <SVM_name> -access all`
- `security login role create -role vrnsrole -cmddirname "volume" -vserver VSERVER -access readonly`
- `security login role create -role vrnsrole -cmddirname "vserver" -vserver VSERVER -access readonly`
- `security login role create -role vrnsrole -cmddirname "version" -vserver VSERVER -access readonly`

What To Do Next

Take a look at how to create FPolicy events using the Creating FPolicy Events Using the SSL Protocol.

Creating FPolicy Events Using the SSL Protocol

You can create an FPolicy event using the SSL protocol.

Prerequisites

To create an FPolicy event using the SSL protocol, you must follow several prerequisites:

- Create and install a public certificate of certificate authority (CA) in NetApp Data ONTAP 8.2. This should be performed by a NetApp engineer.
- Have the FPolicy server certificate and client or public key certificate.
- Be a user with the vsadmin role and have a user name that is associated with the ontapi application. You can issue the `security login show` command to view your defined rights.

1. Install a public certificate of Certificate Authority (NetApp cluster mode)

You can install a public certificate of certificate authority (CA) that is used to sign the FPolicy server certificate.

> Note: This is relevant only for NetApp cluster mode.

To install a public certificate of CA:

1. Connect to NetApp ONTAP data management via PuTTY.

2. To install a public certificate and a private key:

   Note: Installing a public certificate and a private key for an FPolicy server certificate is required for mutual authentication.

   a. Run the following command (enter the relevant parameter for VSERVER):

      ```
      security givxm gexi install -type server -vserver VSERV
      ER
      ```

      Where:

      - `-type` - The certificate type
      - `-vserver` - The name of the Vserver that contains the certificate

   b. When prompted, perform the following steps in the clustered ONTAP CLI window:
      i. Enter the certificate by copying the content of the certificate file.
      ii. Enter the private key by copying the content of the key file.

      Note: From a Windows machine on which the certificate and key were created, you can run the `cat` command on the certificate and key files, copy the command to the clipboard, and paste the content in the clustered ONTAP CLI window.

3. To install the public certificate of CA:

   a. Run the following command (enter the relevant parameter for VSERVER):

      ```
      security givxm gexi install -type client-ca -vserver VS
      ERVER
      ```

      Where:

      - `-type` - The public key certificate
      - `-vserver` - The name of the Vserver that contains the certificate

      Note:

      - The FPolicy server certificate and the public certificate are signed by the same CA.
      - Installing a public certificate of CA is required for FPolicy server authentication.

b. To view the public certificate of CA , run the `security givxm gexi show` command.

> Note: When the certificates have been installed, you can use this command to view the serial, common name, and the certificate's CA name.

2. Create an FPolicy event using the SSL protocol

You can create an FPolicy event using the SSL protocol.

> Note: The order in which you create an FPolicy event is important.

To create an FPolicy event using the SSL protocol:

1. Copy the FPolicy server certificate files to the Varonis Collector and configure the valid path in the `ZvrwHsv0evhivVzg#i1i#zevsrmw#gsr k` file.
2. Connect to NetApp Data ONTAP management via PuTTY.
3. For NetApp ONTAP versions 9 and higher, run the following command:
   For SMB (CIFS) events:
   - _ setattr-with-owner-change _ - Filter the client setattr requests for changing the owner of a file or directory.
   - _ setattr-with-sacl-change _ - Filter the client setattr requests for changing sacl on a file or directory.
   - _ setattr-with-dacl-change _ - Filter the client setattr requests for changing dacl on a file or directory.

```
fpolicy policy event create -vserver VSERVER -event-nam
e fp_event_varonis_cifs   pi stivexmsrw create, create_di
r, delete, delete_dir, open, read, write, rename, rename_
dir, setattr -protocol cifs   pxivw  vwx vieh$  vwx 0vmxi
$ open-with-delete-intent, setattr-with-owner-change, set
attr-with-sacl-change, setattr-with-dacl-change
```

   For NFS events:
   - _ setattr-with-owner-change _ - Filter the client setattr requests for changing the owner of a file or directory.
   - _ setattr-with-group-change _ - Filter the client setattr requests for changing the group of a file or directory.

- _ setattr-with-mode-change _ - Filter the client setattr requests for changing the mode bits on a file or directory.

```
fpolicy policy event create -vserver <Vserver Name> -even
t-name fp_event_varonis_nfsv3   pi stivexmsrw create, cre
ate_dir, delete, delete_dir, read, write, rename, rename_
dir, setattr -protocol nfsv3   pxivw  vwx vieh$  vwx 0vmx
i$ setattr-with-owner-change, setattr-with-group-change,
setattr-with-mode-change
```

Starting from NetApp ONTAP version 8.3.1, run the following command:

For SMB (CIFS) events:

```
fpolicy policy event create -vserver VSERVER -event-nam
e fp_event_varonis_cifs   pi stivexmsrw create, create_di
r, delete, delete_dir, open, read, write, rename, rename_
dir, setattr -protocol cifs   pxivw  vwx vieh$  vwx 0vmxi
$ open-with-delete-intent
```

For NFS events:

```
fpolicy policy event create -vserver <Vserver Name> -even
t-name fp_event_varonis_nfsv3   pi stivexmsrw create, cre
ate_dir, delete, delete_dir, read, write, rename, rename_
dir, setattr -protocol nfsv3   pxivw  vwx vieh$  vwx 0vmx
i
```

4. To create and verify an FPolicy external-engine object:
   Run either one of the following commands:

```
fpolicy policy external-engine create -vserver <Vserver N
ame> -engine-name fp_ex_eng -primary-servers <Varonis Col
lector IP> -port 2003 -extern-engine-type asynchronous -s
sl-option mutual-auth
```

```
fpolicy policy external-engine create -vserver <Vserver N
ame> -engine-name fp_ex_eng -primary-servers <Varonis Col
```

```
lector IP> -port 2003 -extern-engine-type asynchronous -s
sl-option server-auth
```

5. In the <ntap_cm> section of the ZvrwHsv0evhivVzg#i1i#zevsrmw#gsr k file, add the parameters that were modified.
6. To create and verify an FPolicy object:
   - For NetApp ONTAP versions 9.14.1 and higher:
     - Create an empty volume on the SVM that can be provisioned for the persistent store:

       ```
       volume create -vserver <SVM Name> -volume <volume> -s
       tate <online> -junction-path <path> -policy <default
       > -unix-permissions <777> -size <value> -aggregate <a
       ggregate name> -snapshot-policy <none>
       ```

       - Recommended volume size for the persistent store is 32GB. For a calculation with greater precision, see the NetApp article Create persistent stores.
     - Create the persistent store:

       ```
       vserver fpolicy persistent store create -vserver <SVM
       > -persistent-store <PS_name> -volume <volume>
       ```

       - persistent-store: The persistent store name
       - volume: The persistent store volume
     - Run the following command:
       - For existing fpolicies, run this command:

         ```
         vserver fpolicy policy modify -vserver VSERVER -po
         licy-name fp_event_varonis_cifs -persistent-store
         <PS_name>
         ```

       - For new fpolicies, run this command:

         ```
         fpolicy policy create -vserver VSERVER -policy-nam
         e Varonis -events fp_event_varonis_cifs -engine fp
         _ex_eng -is-mandatory false -persistent-store <PS_
         name>
         ```

- To view the policy you created, run `fpolicy policy show`.

- For lower ONTAP versions:
  - Run the following command (enter the relevant parameter for VSERVER):
    `fpolicy policy create -vserver VSERVER -policy-name Varonis -events fp_event_varonis_cifs -engine fp_ex_eng -is-mandatory false`
    Where:
    - `-vserver` - The name of the Vserver on which you want to create an FPolicy policy.
    - `-policy-name` - The name of the FPolicy policy that you want to create. The default policy name, as registered in the Management Console, is `Varonis`.
    - `-events` - A list of events to monitor for the FPolicy policy.
    - `-engine` - The name of the external engine for this FPolicy policy.
    - `-is-mandatory` - Determines whether the FPolicy object is mandatory.
  - To view the policy you created, run `fpolicy policy show`.

7. To create an FPolicy scope object:
   a. Run the following command (enter the relevant parameter for VSERVER):

```
fpolicy policy scope create -vserver VSERVER -policy-name Varonis -volumes-to-include "*" -export-policies-to-include "*"
```

   Note: The shares must reside on the volume monitored for CIFS events.

   b. To view the FPolicy scope:
   Run the following command (enter the relevant parameter for VSERVER):

```
fpolicy policy scope show -vserver VSERVER -policy-name Varonis
```

8. To enable the new FPolicy policy:
   Run the following command (enter the relevant parameter for VSERVER):

```
fpolicy enable -vserver VSERVER -policy-name Varonis
```

3. View NetApp FPolicy arguments

- `-engine-name` - The name of the FPolicy external engine that you want to create
- `-engine` - The name of the external engine for this FPolicy policy.
- `-event-name` - The name of the FPolicy event that you want to create
- `-events` - A list of events to monitor for the FPolicy policy.
- `-export-policies-to-include` - A comma-separated list of export policies for monitoring file access .
- `-extern-engine-type` - The external engine type.
- `pi stivexmsrw` - The file operations for the FPolicy event, which can include one or more of the following operations: create, create_dir, delete, delete_dir, read, write, rename, rename_dir, setattr.
- `pxivw` - Specifies the filters used with a given file operation for the protocol specified in the `-protocol` parameter. For example: `vwx vieh$ vwx 0vmxi`.

  Note: While use of the `vwx vieh` filter can result in dramatic improvement in NetApp performance, it may not be used concurrently with the Filter False-Open Events feature.

- `fp_varonis` - The name of the FPolicy policy for which the FPolicy scope was created
- `-is-mandatory` - Sets whether the FPolicy is mandatory. This must be set to `false`.
- `-policy-name` - The name of the FPolicy policy that you want to create or for which the scope will be created. The default policy name, as registered in the Management Console, is `Varonis`.
- `-port` - The port number for the FPolicy service.

  Note: By default, the port number for the SSL protocol is 2003. This can be changed by configuring another port in the `ZvrwHsv0evhivVzg#i1i#zevsrmw#gsr k` file.

- `-primary-servers` - The IP addresses for the primary FPolicy servers
- `-protocol` - The name of the protocol for which the event will be created. Possible values are:

  - cifs
- `-ssl-option` - The SSL option for external communication with the FPolicy server. Possible values include the following:
  - `mutual-auth` - Provides both Collector and NetApp authentication. When set to `mutual-auth`, the SSL`MutualAuth` parameter should be changed to "1" in the `ZvrwHsv0evhivVzg#i1i#zevsrmw#gsr k` file.
  - `server-auth` - Provides Collector authentication
- `-volumes-to-include` - A comma-separated list of volumes to be monitored.
- `vserver` - The name of the Vserver on which you want to create an FPolicy event, an FPolicy external engine, FPolicy policy, or FPolicy scope.

What To Do Next

Configure NetApp firewalls to allow connectivity to the Varonis Collector.
Configuring Firewalls/Service Policies

The NetApp firewall may block communication from the Varonis Collector. To allow connectivity, you can modify the NetApp policy.

For the Latest NetApp ONTAP Cluster Mode Versions

1. Run the following command to create an explicit rule to create the service policy; the allowed IP addresses are the IPs of the Varonis Collector (enter the relevant parameters for VSERVER and COLLECTOR_IP):

   ```
   network interface service-policy add-service -vserver VSE
   RVER -policy default-data  piw -service management-https
   -allowed-addresses COLLECTOR_IP/32
   ```

   For example, using sample IP addresses:

   ```
   network interface service-policy add-service -vserver VSE
   RVER -policy default-data  piw -service management-https
   -allowed-addresses 10.32.12.91/32, 10.32.12.95/32
   ```

2. For a custom policy, it is required to add the service management HTTPS to this policy as well. Run the following command to view the available policies (enter the relevant parameter for VSERVER):

```
net interface service-policy show -vserver VSERVER
```

3. Run the following commands to add the service (enter the relevant parameters for VSERVER and CUSTOM_POLICY):

```
set advanced
```

> Note: `set advanced` is required. The command `network interface service-policy add-service` is available to cluster administrators at the advanced privilege level. See network interface service-policy add-service (netapp.com).

```
network interface service-policy add-service -vserver VSE
RVER  -policy CUSTOM_POLICY -service management-https
```

4. For NetApp Cluster Mode versions 9.8 and higher: Make sure that `data-fpolicy-client` is only set on the network interfaces (Logical Interfaces) that communicate with the Varonis Collector.

> Note: For Amazon FSx for NetApp ONTAP, see step 5 below.

To add `data-fpolicy-client` to the LIFs to be used with Varonis, run the following command:

```
net int service-policy add-service -vserver [vserver name
] -policy [policy name] -service data-fpolicy-client
```

To remove `data-fpolicy-client` from other LIFs not intended to be used with Varonis, run the following command:

```
net int service-policy remove-service -vserver [vserver n
ame] -policy [policy name] -service data-fpolicy-client
```

If you need to keep the FPolicy Client on other network interfaces, make sure these interfaces can communicate with the Varonis Collector. Set the firewall rule to allow

port 2002 communication from all nodes/data LIFs that have the `data-fpolicy-client` service to the Varonis Collector.

5. For Amazon FSx for NetApp ONTAP: Allow traffic using port 2002 between the Varonis Collector and both iSCSI IP addresses, iscsi_1 and iscsi_2 logical interfaces (LIFs).

For Older NetApp ONTAP Cluster Mode Versions

For NetApp ONTAP versions 9.0-9.5, perform the following steps:

1. Run the following commands to create an explicit rule (enter the relevant parameters for VSERVER, COLLECTOR_IP, and LIF):

```
system services  vi0all policy create -policy fp_varonis
-service https -action allow -ip-list COLLECTOR_IP/32
```

```
network interface modify -vserver VSERVER -lif LIF   vi0a
ll-policy fp_varonis
```

Note: For NetApp version 9.0 and below, use HTTP in the command instead of HTTPS.

2. The first command above creates a new firewall policy. However, since it is possible to define only one policy per data logical interface (LIF), it is recommended to first retrieve the relevant policy, check which services are allowed or denied, and define the same in the `fp_varonis` policy. To do so, run the following (enter the relevant parameters for VSERVER and LIF):

```
network interface show -vserver VSERVER -lif LIF
```

3. To retrieve the firewall policy configured on the network interface, run the following:

```
system services  vi0all policy show -policy data
```

4. Create a new policy, using the same services as above but allowing an HTTP connection with the Varonis Collector IP. To do so:
   a. Clone the above policy (enter the relevant parameter for VSERVER):

```
system services  vi0all policy clone -vserver VSERVER -
policy data -destination-vserver VSERVER -destination-p
olicy fp_varonis
```

b. Update the policy (enter the relevant parameters for VSERVER and IP_ADDRESSES):

```
system services  vi0all policy modify -policy fp_varoni
s -vserver VSERVER -service https -allow-list IP_ADDRES
SES
```

What To Do Next

Now that you've configured the FPolicies and firewalls, proceed to configure the Varonis Collector to connect to NetApp.

Adding a NetApp Data Source Operating in Cluster Mode - Summary

Now that you've configured the Varonis Collector to connect to NetApp, you can deploy a NetApp data source operating in Cluster Mode to be monitored by the Varonis Collector. This section summarizes the procedure for deploying NetApp data sources operating in Cluster Mode in the Management Console.

Important: You must create a login method before configuring Varonis for a NetApp data source operating in Cluster Mode. You will need the login method to enter your FileWalk Credentials.

1. Run the Management Console as an administrator.
2. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.
3. In the Resource Wizard's Common pane, specify the data source name or IP address of the data logical interface (LIF) you want to monitor, check the Collector selected by default and change it if needed, and enter the credentials for running directory structure monitoring (FileWalk).

   Important:

   - This account must have Backup Operator and Power User roles on the data source during installation.

- You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.

4. In the Resource Type area, select the data source type from the dropdown list. Then, click the Connect and verify link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

Note:

- The Connect and verify link is displayed only when all relevant data is entered.
- A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

- UUID - The Vserver/SVM Universal Unique Identifier (UUID) is required to retrieve events from the Vserver. The UUID can be displayed by running the `vserver show-instance` command in the ONTAP console.

Note: The Vserver/SVM UUID is unique from the Cluster UUID; using the Cluster UUID will cause failures in monitoring.

5. In the Monitored Shares area, select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source is installed and share detection is completed.
6. In the Configuration pane, review the Local Accounts, FileWalk Settings, and Event Auditing Parameters settings.
7. In the Proxy configuration area, define a proxy server. The proxy can be installed on any Windows machine in the same LAN as the NetApp data source being monitored. A single proxy can be used to monitor more than one data source.
8. (Optional) In the Commit pane, clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials.

Note:

- If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.

- If the Collector is in a lower version than 8, the FileWalk credentials will be used.

In the Group OU area, if required, select Uniquely defined to choose a different OU from that defined in the data source's domain.

9. After configuration is complete, click Install to add the data source.
10. (Optional) Enable SMB signing. Follow the steps described in Adding a NetApp Data Source Operating in Cluster Mode - Detailed Procedure.
11. (Optional) Enable Delete events in NetApp cluster mode. Follow the steps described in Adding a NetApp Data Source Operating in Cluster Mode - Detailed Procedure.
12. After the data source installation and share detection are completed, in the Shares pane, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. If you chose to monitor selected shares, you can select and register the required shares.

Note: If the security style is changed on the data source, then Varonis will automatically identify it and change the protocol that's used (from CIFS to NFS, for example).

What To Do Next

Now that you're familiar with the deployment steps, it's time to dive into the detailed procedure.

Adding a NetApp Data Source Operating in Cluster Mode - Detailed Procedure

Now that you've configured the Varonis Collector to connect to NetApp, you can deploy a NetApp data source operating in Cluster Mode to be monitored by the Varonis Collector.

Note: Varonis monitors CIFS shares on this data source.

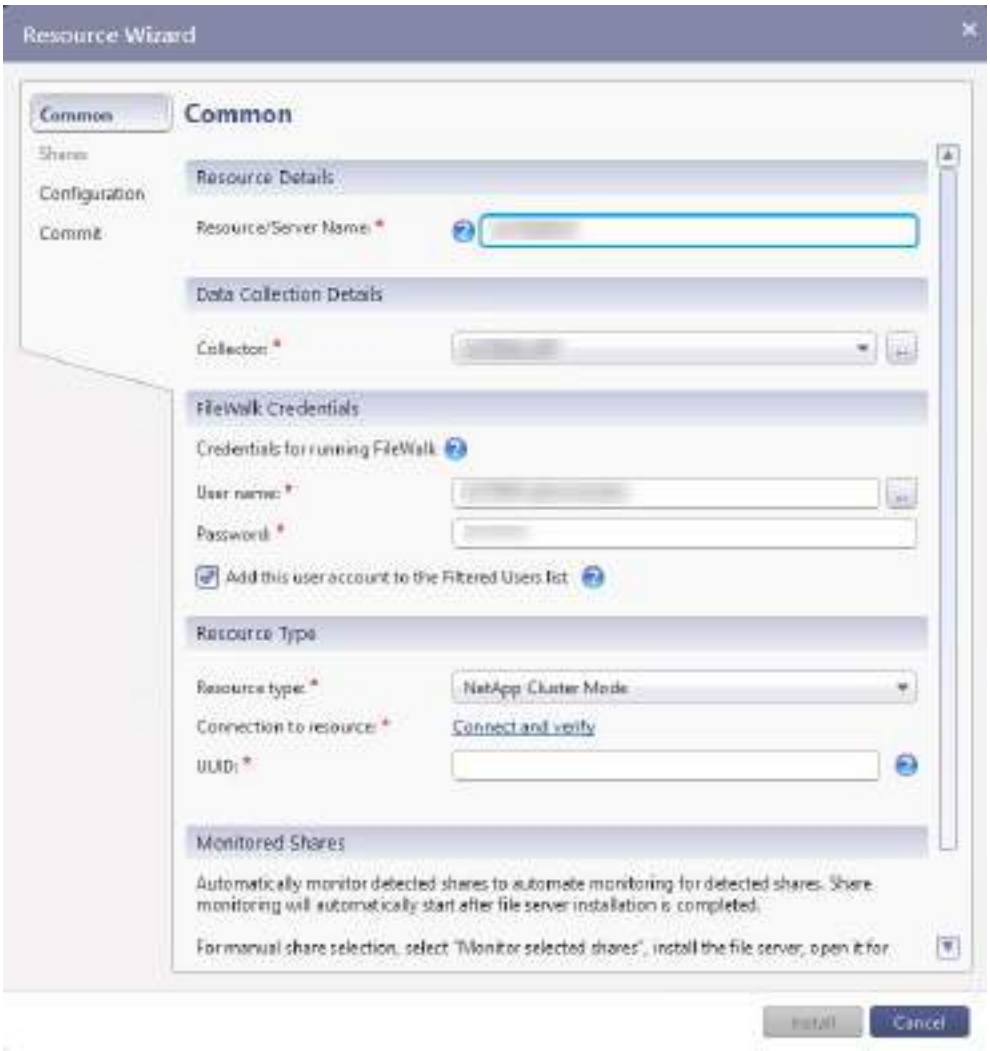
Note: Each NetApp data source represents a monitored NetApp Server. In some cases, the Varonis UI displays the term File Server or Resource instead of Data

Source. To monitor multiple NetApp servers, add a NetApp data source per NetApp server.

1. Set common data source parameters

Important: You must create a login method before configuring Varonis for a NetApp data source operating in Cluster Mode. You will need the login method to enter your FileWalk Credentials.

1. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.
   The Resource Wizard is opened to the Common pane, where you can specify the data source and set the relevant parameters.



2. In the Common pane, set the following parameters:
   a. Resource Details - Enter the name or IP address of the data logical interface (LIF) you want to monitor.
   b. Data Collection Details - Select the relevant Collector from the dropdown list.
   c. FileWalk Credentials - Enter the credentials for running directory structure monitoring. File System operations include directory structure monitoring, event auditing (if set) and account enumeration on local accounts (if set).

      Note:
      - This account must have Backup Operator and Power User roles on the data source during installation.
      - These credentials are cached, so that they are automatically entered if another data source is added during the same session.

      - User name - Type the name of the user account to be used for directory structure monitoring, event auditing, and local account enumeration.
      - Password - Type the account's password.
      - Add this user account to the Filtered Users list - The defined user for FileWalk Credentials will be added to the filtered users list. If you clear this checkbox, a large number of events may be generated by the user defined for directory structure monitoring. It is recommended to keep this checkbox enabled.

      Important: You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.

   d. Resource Type - Select the data source type from the dropdown list.
      - Connect and verify - Click this link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

        Note:
        - The Connect and verify link is displayed only when all relevant data is entered.
        - A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

- UUID - The Vserver/SVM Universal Unique Identifier (UUID) is required to retrieve events from the Vserver. The UUID can be displayed by running the `vserver show-instance` command in the ONTAP console.

  Note: The Vserver/SVM UUID is unique from the Cluster UUID; using the Cluster UUID will cause failures in monitoring.

e. Monitored Shares - Select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source installed and share detection is completed.

- Automatically monitor detected shares - Select this option to automate monitoring for all detected shares. Share monitoring will automatically start after the data source installation is completed. Varonis will monitor all shares that aren't marked as "ignored". When this option is selected, click the Advanced setting link to modify share detection preferences. By default, the option is set to Prefer regular shares over equivalent admin shares. In this case, an admin share that has an equivalent regular share will be marked as "ignored" and the equivalent regular share will be detected for monitoring. Note: Any change in the monitored shares configuration, including the detection method, admin shares configuration, and selected shares, requires rerunning the resource detection.
- Monitor selected shares - This option is selected by default. You can manually select the shares to be monitored only after the data source is installed and share detection is completed. You'll need to open the Edit window for the installed data source and select the shares. For more information, see Post-installation share detection and registration.

Once the above settings are configured, you can proceed to review and adjust configuration settings.

2. Review and adjust configuration settings

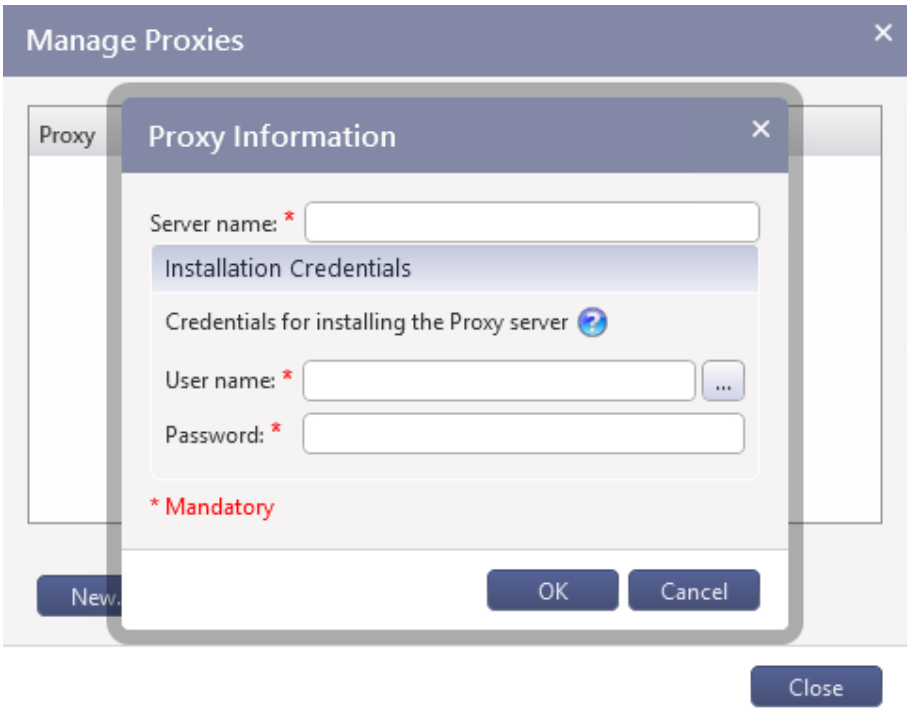
1. On the left menu, click Configuration and confirm the information.
   The general configuration settings are displayed.
2. In the Local Accounts area, review the options:
   - Collect information regarding local accounts from this file server - Select this checkbox to collect user accounts from this file system.
3. In the FileWalk Settings area, review the options:

- Identify actual unique folders and file system inconsistencies - Select this checkbox (if it not already selected) to detect broken permissions in NTFS file systems.

4. In the Event Auditing Parameters area, review the options:
   - FPolicy name - Type the name of the FPolicy.

     Important: The name of the FPolicy is case sensitive.

   - Filter out false "File Opened" events - Open events may be triggered unintentionally for a variety of reasons, resulting in inaccurate analysis of file system access. Select this option to filter such unintentional Open events and gather Open events only if enough file content is actually read. Small files and certain operations may still trigger Read events.
   - In the Proxy configuration area, define a proxy server. For performance reasons, it is possible to define a proxy that is located near the NetApp data source. The proxy can be installed on any Windows machine in the same LAN as the NetApp data source being monitored. A single proxy can be used to monitor more than one data source.
     - Proxy server - From the dropdown list, select the proxy to be used to monitor the data source.
     - Manage - Click this link to add, edit, or remove proxy servers. The Manage Proxies dialog box is displayed, where you can click New to add a new proxy. Set the relevant parameters in the Proxy Information dialog box.



For the required permissions for installing the proxy, see Varonis Service Account Requirements in NetApp Requirements.

3. (Optional) Customize commit credentials

You can use different commit credentials instead of the default FileWalk credentials.

1. On the left menu, select Commit.
   The commit settings are displayed.
2. (Optional) Clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials. (By default, this checkbox is selected to use the FileWalk credentials, and the User name and Password fields are disabled for editing.)

   Note:
   - If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
   - If the Collector is in a lower version than 8, the FileWalk credentials will be used.
3. In the Group OU area, if required, select Uniquely defined to choose a different OU from that defined in the data source's domain. Click the Browse button (...) to select the required OU.

4. Install the data source

After configuration is complete, click Install to install the data source.

A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the File Servers pane. When the installation completes, the status shows "Installed 100%".

5. (Optional) Enable SMB signing

The Data Security Platform supports SMB signing in SMB versions 2 and 3.

SMB signing (also known as security signatures) is a security mechanism in the SMB protocol. SMB signing means that every SMB 3.1.1 message contains a signature that is generated by using the session key and the Advanced Encryption Standard (AES) algorithm. The client puts a hash of the entire message into the signature field of the SMB header.

If someone changes a message during transmission, the hash will not match, and SMB will know that someone tampered with the data. The signature also confirms the sender's and receiver's identities. This breaks relay attacks.

To enable SMB signing for a NetApp data source:

1. Disable SMB1 on the server side (NetApp data source). For more information, see the following Microsoft article.
2. Enable SMB signing on the server and client sides (NetApp data source and Collector or DSP Server in case of a consolidated setup). For more information, see the following Microsoft article.

6. (Optional) Enable Delete events in NetApp cluster mode

1. Navigate to the GridCollector folder on the Collector and edit the `ZvrwHsv0evhivVzg#i1i#zevsrmw#gsr k` file.
   a. Go to the section that begins with:

```
 <!-- Netapp Cluster Mode wtigm g gsr kyvexmsrw
      <ntap_cm  pi ?ZvrwHsv0evhivVzg#i1i#ywiv#gsr k?  <
!-- Netapp Cluster Mode wtigm g gsr kyvexmsrw
      <ntap_cm  pi ?ZvrwHsv0evhivVzg#i1i#ywiv#gsr k?
```

   b. Change the `SMB3Enabled` value from "0" to "1":

```
<!-- Enable SMB3 Delete support
        <add key="SMB3Enabled" zepyi ?5?
```

2. Restart the Varonis Forwarder Service (NetApp cluster mode) service.

7. Post-installation share detection and registration

After the data source installation and share detection are completed, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. The following procedure describes the manual registration and automatic share detection flows.

Important: If after the data source is installed, share detection fails for any reason, the Share Detection Status column will remain "In Progress" until the issue is fixed, and share detection completes successfully at least once.

Important:

- If the security style is NTFS or mixed security, Varonis will automatically use CIFS for monitoring the data source. If the security style is Unix, Varonis will use NFS to monitor the data source.
- The Protocol column shows either CIFS or NFS. If your server's exposed protocol is not compatible with the security style, the share row in the Available Shares grid will be grayed out and you will not be able to register the share. A tooltip in the Access Details column will indicate the protocol mismatch.
- All NFS and CIFS events are audited regardless of the protocol used for monitoring.

After the data source is installed, the Shares pane is enabled, and you can view the share settings.

1. On the left menu, click Shares.
   The share settings are displayed. The pane's heading indicates the option you selected when adding a data source.
2. In the Available Shares area, you can filter the shares based on the reason they are not registered for monitoring and easily identify the shares that can be added. The default filter is Accessible Shares. You can change the filter to see the rest of the shares. Options include:
   - Accessible shares - Can be added for monitoring (this option is selected by default)
   - Ignored shares - Are marked as "ignored"
   - Incompatible and inaccessible shares - Cannot be monitored since the exposed protocol does not match the security style of the volume (relevant to multiprotocol platforms only) or the Varonis service account does not have access to this share
   - Child share of a monitored share - Is monitored via its parent folder
3. Do one of the following:
   - If you chose to monitor selected shares, in the Available Shares area, select the required shares and click the down arrow. The selected shares are moved to

the Registered Shares area. (The registered shares list is empty until you make your selections.)

- If you chose to automatically monitor detected shares, Varonis will monitor all shares that aren't marked as "ignored". The automated share detection runs every few hours. The Registered Shares area is autopopulated with the shares to be monitored.

4. For each share, review and set the following information as required:
   - Ignore Detection - Select the shares to be ignored (and not be the subject of automatic detection and notifications) by the data source monitor.
   - Events - Select this checkbox to audit events for the share.
   - Crawl - To enable or disable monitoring for the share, in the Crawl column, select the relevant option.

     Note: You can also right-click the grid and select the required options for event auditing and crawling.

5. In the Additional Share Settings area, review the options:
   - Remove deleted shares - Select this checkbox to remove deleted shares. Shares that were deleted from the data source will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the data source is unavailable, the shares will not be removed.
   - Enable event auditing - Select this checkbox to audit events from all shares added from this data source.

   After share detection and registration are completed, the status and number of registered volumes are respectively displayed in the Share Detection Status and Registered Shares columns in the File Servers pane.

Note: If the security style is changed on the data source, then Varonis will automatically identify it and change the protocol that's used (from CIFS to NFS, for example).

What To Do Next

Now let's take a look at the supported events for the monitored NetApp data sources.

Supported Events For NetApp Data Sources

The monitored data sources and NAS devices support various SMB (CIFS) and NFS events.

Note: SMB v2 and v3 are supported.

Event Auditing Method

NetApp FPolicy API

SMB (CIFS) Events for NetApp Data Sources

Supported File Operations

For more details about the "numbered" operations below, see the corresponding numbers in the "Limitations and Known Issues" list following this table.

- File created
- File deleted
- File opened
- File modified[1]
- Folder created
- Folder deleted
- Folder renamed
- Folder permissions changed

Note: Permissions changed events do not include the details of the permissions that were changed.

Limitations and Known Issues

1. The ability to distinguish File modified from File opened events is configured through the UI (default=off) due to network issues that might affect client latency.
2. For SMB (CIFS), it is important to enable setting security: `fpolicy options <PolicyName> cifs_setattr on`.

NFS Events for NetApp Data Sources

Supported File Operations

- File created
- File deleted
- File renamed
- File modified
- File permissions changed
- Folder created
- Folder deleted
- Folder renamed
- Folder permissions changed

Note:

- NFS File opened events are inconsistent because the NFS client caches the results of the requests; requests similar to previous requests will not reach the NAS device and, therefore, won't be logged.
- Permissions changed events do not include the details of the permissions that were changed.

7 DELL POWERSCALE ONEFS (ISILON) DATA SOURCES

What This Section Contains

This section describes how to deploy and monitor Dell PowerScale OneFS (Isilon) data sources; the requirements, deployment and configuration steps, and supported events.

Note: This section provides recommendations for configuring software from third-party vendors. Varonis is not responsible for ensuring the information contained herein is up to date. For more information, see the individual vendors' documentation. You should comply with any standard software and/or hardware licenses and related terms and conditions embedded in or furnished in connection with the third-party software, all of which are provided to you under the terms of those licenses and are not included as part of the Varonis end-user license agreement. Varonis shall have no responsibility for any products or services provided by third-party vendors.

What To Do Next

Before you dive in, click here to learn more about how Varonis monitors Dell PowerScale OneFS (Isilon) data sources.

Dell PowerScale OneFS (Isilon) Monitoring Overview

To monitor Dell PowerScale OneFS (Isilon) data sources, you need to configure Varonis to work with the Dell Common Event Publishing Agent (CEPA) event collection method. This requires installing the Common Event Enabler (CEE) package and configuring the CEE framework.

The Dell CEE framework is used to provide a working environment for various facilities. These include:

- Dell Common AntiVirus Agent (CAVA) - A Dell-provided agent that runs on a Windows Server and communicates with a standard antivirus engine to scan CIFS files stored on Dell Attached Storage.
- Dell CEPA - A Dell-provided agent that runs on a Windows Server and provides external applications with notification and optional control of changes made by CIFS clients in file systems on the Dell Network Server in real time. CEPA delivers both event notification and associated context to the application in one message. Context may comprise the file metadata or directory metadata needed to decide business policy.

While the CEE framework includes both CAVA and CEPA, they can run independently of each other or run together.

The Dell CEPA service and the Collector can be installed on the same server or on separate servers. For optimal performance, Varonis recommends installing them on separate servers.

Multiple Access Zones

- Varonis supports monitoring multiple access zones that reside in the same Dell PowerScale OneFS (Isilon) cluster.
- For each access zone, you'll need to configure a separate Dell PowerScale OneFS (Isilon) data source in the Varonis Management Console.

Data Classification and Labeling

- Varonis supports data classification and labeling on files that reside in the monitored data sources.

What To Do Next

First, make sure you fulfill the Dell PowerScale OneFS (Isilon) requirements.

Dell PowerScale OneFS (Isilon) Requirements

Varonis Service Account

Varonis requires a dedicated service account. The service account can be reused for multiple data source installations and configurations.

- Service Account Read Operations:
  - Traverse and enumerate files, folders, directory structures, users, and groups.
  - Gather data source, user, and group metadata as part of normal system operations.
- Service Account Write Operations:
  - Used for executing Varonis Policies, if policies are defined.

Varonis Installation and Requirements

- Event auditing:
  - CEPA is required.
  - Optional – CEPA service on a dedicated server.
- A Windows Server capable of running the CEE framework package

Requirements for the Varonis Service Account for Read Operations

- Membership in the monitored access zone local Administrator group, which can be configured within the Dell PowerScale OneFS (Isilon) management
- Membership in the System access zone Backup Admin role, which can be configured within the Dell PowerScale OneFS (Isilon) management
- Read rights on an appropriate top-level SMB share for which all data to be indexed is a child object
- Permissions for the REST API and for data source deployment. For more information, see Configuring the Varonis Service Account and REST API User for Dell PowerScale OneFS (Isilon).

Requirements for the Varonis Service Account for Write Operations

In addition to the requirements for the read operations, the Varonis service account for write operations requires run as root privileges on the SMB (CIFS) share.

What To Do Next

Now that you've fulfilled the requirements, proceed to Install and Configure the Dell CEE Framework.

Monitoring Dell PowerScale OneFS (Isilon) With Mixed Security Style

- If the security style is NTFS or mixed security, Varonis will automatically use CIFS for monitoring the data source. If the security style is Unix, Varonis will use NFS to monitor the data source.
- The Protocol column shows either CIFS or NFS. If your server's exposed protocol is not compatible with the security style, the share row in the Available Shares grid will be grayed out and you will not be able to register the share. A tooltip in the Access Details column will indicate the protocol mismatch.
- All NFS and CIFS events are audited regardless of the protocol used for monitoring.
- NFS v3 should be enabled.
- The Collector IP should be listed in the export policy of the share with read permissions.
- The NFS exports should be mountable.

Installing and Configuring the Dell CEE Framework

The CEPA service is configured by installing the Dell Common Event Enabler (CEE) framework package on a supported Windows Server.
For complete requirements and instructions on configuring CEE, see Dell's documentation.

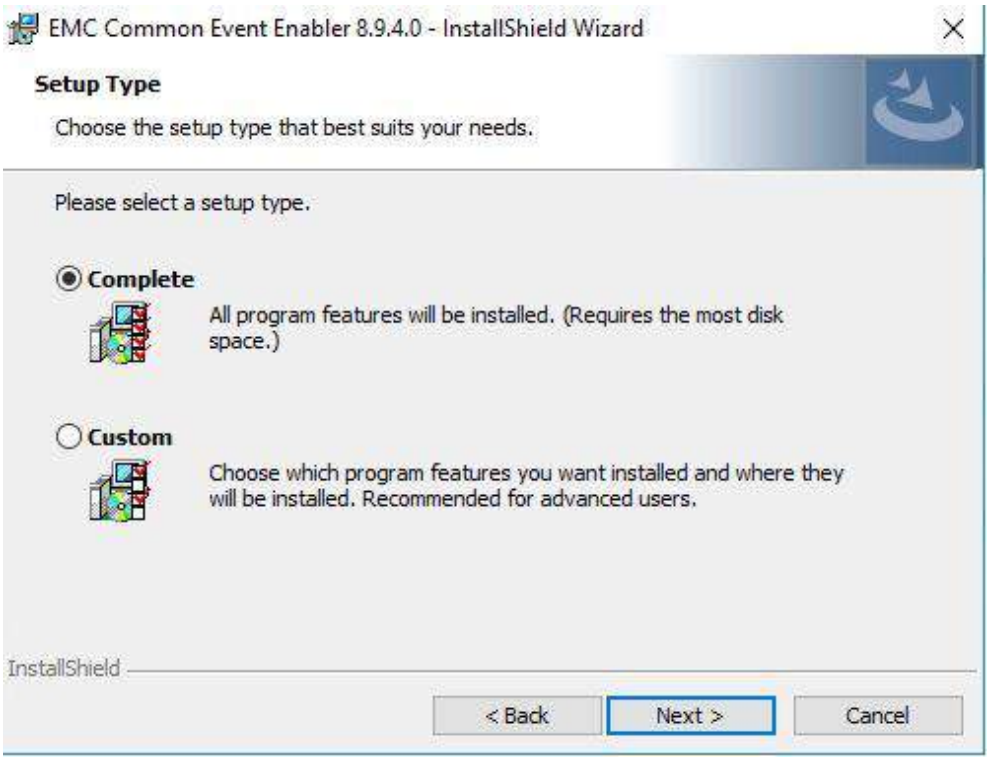
> Note: For performance reasons, it is not recommended to install the CEPA service on the same server as the Collector.

For all the CEE server connections (to/from Dell PowerScale OneFS (Isilon) and the Collector), see Varonis SaaS Firewall Rules.

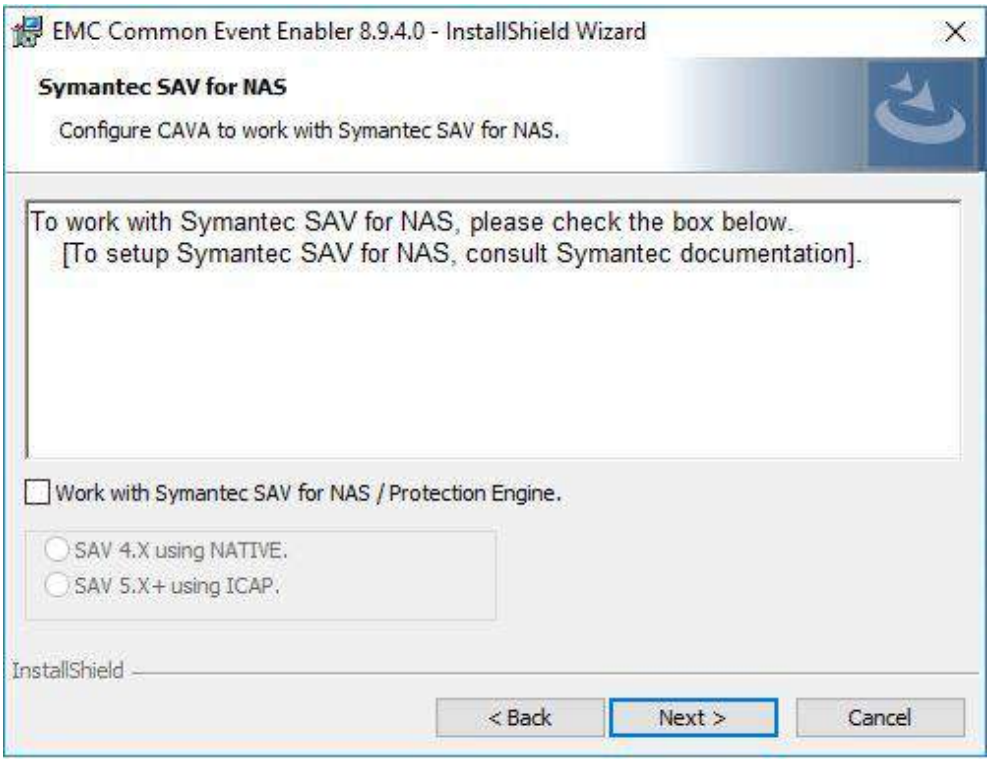
Installing the Dell CEE Framework

Run the CEE installer package to install the Dell CEE framework.

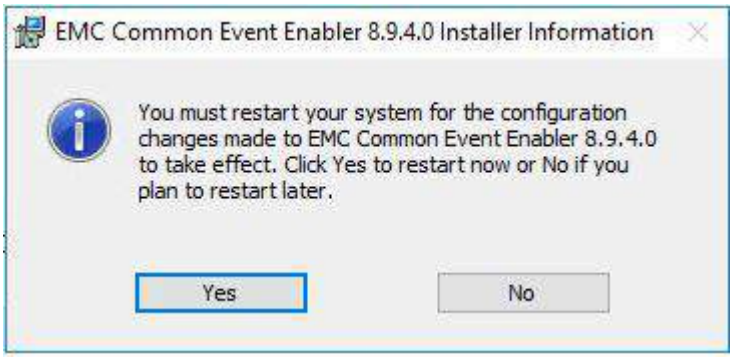
1. If any versions of Dell CEE Framework software earlier than v8.6 (including stand-alone CAVA or CEPA) are already installed on the CEE server, uninstall them before continuing.
2. Make sure to use the latest Dell CEE Framework version. Contact Dell technical support or your Peer Software technical to obtain the latest version.
3. Download and stage the 64-bit Dell CEE Framework installer on the CEE server. Proceed with the following steps to install the Dell CEE Framework software.
4. Run the Dell CEE Framework installer as an administrator.
   The Welcome page of the CEE Installation wizard is displayed.
5. Click Next.
   The License Agreement page is displayed.
6. Accept the terms of the license agreement, and click Next.
   The Customer Information page is displayed.
7. Enter your user name and organization, select Anyone who uses this computer (all users), and click Next.
   The Setup Type page is displayed.



8. Select Complete or Custom. If you select Custom, you must select at least these two: CEPA and CEE Monitor. Then, click Next.
   The Symantec SAV for NAS page is displayed.



9. Ensure that the Work with Symantec SAV for NAS/Protection Engine checkbox is not selected, and click Next.
   The Ready to Install the Program page is displayed.
10. Click Install.
    When the installation is complete, the InstallShield Wizard Completed page is displayed.
11. Click Finish.
    A message is displayed, prompting you to restart the system.



12. Click No. You will restart the system later.

Post-Installation Configuration for the Dell CEE Framework

This section describes the procedures required for Dell CEE Framework post-installation configuration.

Editing the Registry for the CEE

You need to make some changes to the registry for the CEE.

CEE Versions 6.0-8.7

Make the following changes to the registry:

> Note: If the Dell CEE Framework is upgraded or reinstalled, these registry changes must be re-entered. If the Varonis endpoint value is not set after upgrading the CEE, events are not collected.

1. Open the registry: Select Start > Run > regedit.
2. Locate the following key:
   - Up to CEE 6.0 (exclusive): `HKLM\Software\EMC\Celerra Event Grefpiv;EGSS;Cyhmx;Esr kyvexmsr`.
   - CEE 6.0.x: `KNOP;Vsjx0evi;GPE;EGG;EGSS;Cyhmx;Esr kyvexmsr`.
3. Edit the Endpoint string value as follows:
   - If the Varonis Collector is installed on the same server as the CEE, set the value to `Varonis`.
   - If the Varonis Collector is installed on a different server than the CEE, set the value to `Varonis@<CollectorIP>`, where `<CollectorIP>` is the IP address of the Varonis Collector.
   - When monitoring multiple Dell PowerScale OneFS Isilon zones, if the data sources are using different Collectors, all the Collectors should be configured on the CEE server, separated by semi-colons. For example, `Varonis@<CollectorIP1>;Varonis@<CollectorIP2>`.

     > Note: When using multiple Collectors as endpoints, ensure that all data sources connected to the same CEE server are configured to be monitored by the same set of Collectors. Otherwise, separate CEE servers can be used to monitor different data sources.

CEE Version 8.8 and Higher

Make the following changes to the registry:

> Note: If the Dell CEE Framework is upgraded or reinstalled, these registry changes must be re-entered. If the Varonis endpoint value is not set after upgrading the CEE, events are not collected.

1. Open the registry: Select Start > Run > regedit.
2. Locate the following key:
   `KNOP;Vsjx0evi;GPE;EGG;EGSS;Cyhmx;Esr kyvexmsr`
3. Edit the Endpoint string value as follows:
   - If the Varonis Collector is installed on the same server, set the value to `Varonis`.
   - If the Varonis Collector is installed on another server, set the value to `Varonis@<CollectorIP>`, where `<CollectorIP>` is the IP address of the Varonis Collector.
   - When monitoring multiple Dell PowerScale OneFS Isilon zones, if the data sources are using different Collectors, all the Collectors should be configured on the CEE server, separated by semi-colons. For example, `Varonis@<CollectorIP1>;Varonis@<CollectorIP2>`.

     > Note: When using multiple Collectors as endpoints, ensure that all data sources connected to the same CEE server are configured to be monitored by the same set of Collectors. Otherwise, separate CEE servers can be used to monitor different data sources.
4. Locate the following key:
   `HKLM\Software\EMC\CEE\CEPP\Audit\Enabled`
5. Change the Enabled DWORD value to 1.

Setting Service Credentials

You need to set credentials for the Dell CAVA service.

Make the following changes to the Dell CAVA service:

1. Open the Dell CAVA service (select Start > Run > services.msc).
2. Right-click the Dell CAVA service and select Properties.

3. Close the Services dialog box. The Dell CAVA service is set.

Completing the Dell CEE Framework Installation

After editing the registry and setting the required credentials, restart the Dell CAVA service to complete the installation.

What To Do Next

Now you're ready to configure the Dell storage device.

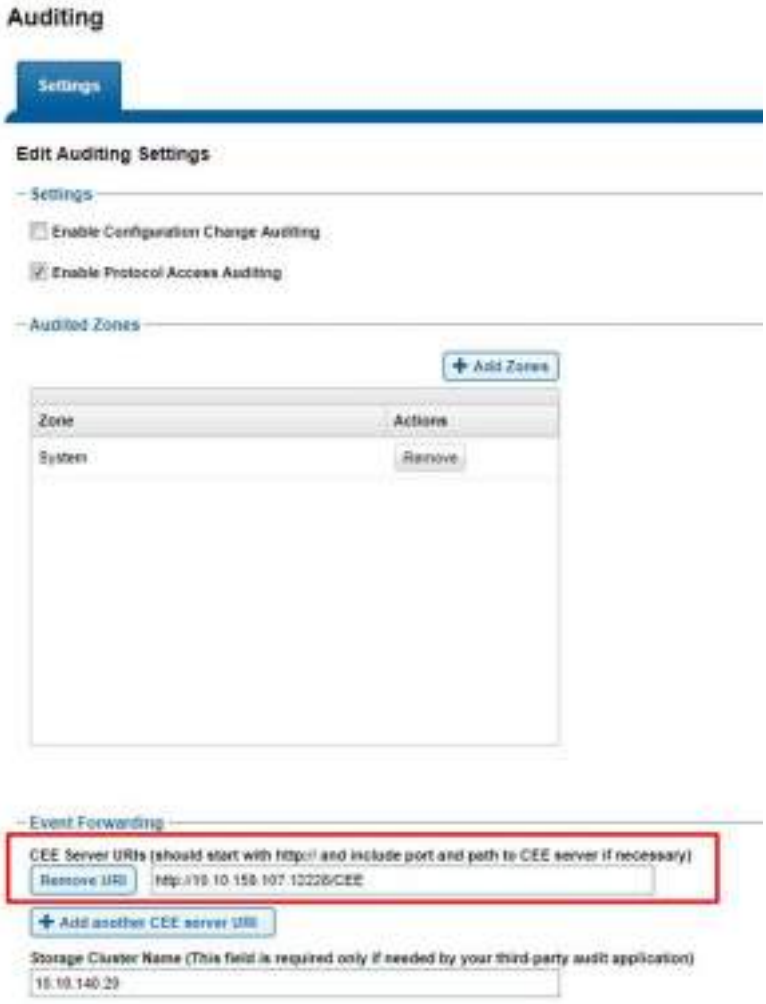
Configuring Dell PowerScale OneFS (Isilon)

There are several best practice recommendations for configuring Dell PowerScale OneFS (Isilon) storage.
For instructions on configuring Dell PowerScale OneFS (Isilon) storage to work with Varonis, see the Dell documentation.

Recommendations

- Dell PowerScale OneFS (Isilon) logs events even if it is not connected to the designated CEPA servers, which can result in a very large backlog of audit events. To minimize the effects of this issue:
  - After completing configuration in other areas, select the Enable Protocol Access auditing option.
  - OneFS 8.x - Set isi audit settings global modify --cee-log-time. This option enables users to set a starting point for CEE event forwarding, ignore backlogs and start event delivery at a specified day and time.
- The Audited Zones section enables adding the access zones that pass their audit logs to the CEPA server. This area is crucial to the overall performance of the Dell PowerScale OneFS (Isilon) auditing feature.
  - BEST PRACTICE - Create access zones that segregate service accounts from live user data and only include the access zones with user data in this field.
- Add Dell PowerScale OneFS (Isilon) to Varonis with an access zone that is not included in the audited zones section under Cluster Management > Auditing in the OneFS web UI. This limits event auditing overhead by not auditing events that Varonis directory structure monitoring would create through its normal daily functions.
- Clear "Run as Root" in the Dell PowerScale OneFS UI if events show as "Abstract\Root". Ensure directory permissions are audited and set for proper user and group access.

- In the OneFS Web UI, under Auditing > Settings > Event Forwarding, add a CEE Server URI: http://<IP_ADDRESS_OF_CEE_MACHINE>:12228/CEE



Examples of OneFS Access Control Commands

Examples of OneFS access control commands that may help for configuring the Varonis service account for Dell PowerScale OneFS (Isilon).

- To add a user to a role:

```
 isi auth roles modify <role name case sensitive> --add-u
ser=<user name in user@domain.com or domain\user>
```

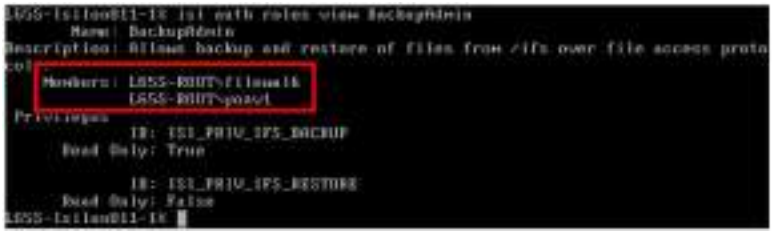
For example:



- To get configurations of roles:

```
isi auth roles view <role name case sensitive>
```

For example:



- To get configuration of local groups:

```
isi auth groups members list <group name case sensitive>
```

For example:



- To add user share permissions:

```
isi smb shares permission create <share name> --user=<use
r in various ways> --permission-type=allow -permission=re
ad --zone=System
```

For example:



- To get a list of share permissions:

```
isi smb shares permission list <share name>
```

For example:



Known Issues with Dell PowerScale OneFS (Isilon)

- If the Dell PowerScale OneFS (Isilon) service is down, the server is detected as Windows 2008 R2.
- Local users and groups are not resolved in account enumeration.
- Local users and local operations do not produce events.

What To Do Next

Now proceed to configure the Varonis service account and REST API Access user for Dell PowerScale OneFS (Isilon).

Configuring the Varonis Service Account and REST API User for Dell PowerScale OneFS (Isilon)

Before you add Dell PowerScale OneFS (Isilon) data sources, you need to configure the Varonis service account and Rest API access user.

Required Configurations

- Rest API user creation - The Rest API user forDell PowerScale OneFS (Isilon) and CloudPool and SmartPool roles should be created in the system zone. All required roles are mandatory, especially on the system zone, even if the system zone is not monitored.
- Dell management access REST API settings - The IP address of the system zone should be entered in the Dell Management Access Settings area in the Varonis Management Console.
- Role/user creation - The user should be created in the system zone with CloudPool and SmartPool roles for cluster information access, and Auth and Platform API roles for RestAPI access.
- User format in the Varonis Management Console - A Domain user is required, and the format should be: `<domain_name>\<user_name>`.

Creating a Role for the User

1. Log in to the Dell PowerScale OneFS Storage Administration UI.

2. Create a role for the user. Go to Access > Membership and roles, choose the system zone , and in the Roles tab, click Create a role, enter a name for the role, and click Next.
3. Assign the role to the user that's used to install the Dell PowerScale OneFS (Isilon) data source in the Varonis Management Console:
   a. Click Add Member and search for Users.
   b. In the User field, enter the user (for example, administrator)
   c. Select the Provider and AD domain to which the user belongs.
   d. Click Search. The relevant user that's used to install the Dell PowerScale OneFS (Isilon) data source is displayed in the search results.
   e. Click Select User.
   f. Click Next.
4. Add the privileges for the role (define what the user can do). Click Edit to edit the role details.

   Note: For Dell PowerScale OneFS (Isilon) versions lower than 9.3, set the following:
   - Auth - Read
   - CloudPool - Read
   - SmartPools - Read
   - Platform API - Read - required for each one of the monitored access zones

   For Dell PowerScale OneFS (Isilon) version 9.3 and higher, set the following:
   - Auth - Read
   - Auth Groups - No permission
   - Auth Providers - No permission
   - Auth Rules - No permission
   - Auth ACL Policy settings - Read

     Attention: Make sure Auth ACL Policy settings is set to Read.
   - Auth global authentication - No permission
   - Auth Users - No permission
   - Auth access zones - No permission
   - CloudPool - Read
   - SmartPools - Read
   - Platform API - Read - required for each one of the monitored access zones
5. Click Next.

The role summary is displayed.

6. Click Submit.
   A message is displayed, indicating that the role is created successfully.

What To Do Next

Now that you've configured the Varonis service account and Rest API access user, it's time to add a monitored Dell PowerScale OneFS (Isilon) data source. First familiarize yourself with the deployment steps summary and then dive into the detailed procedure.

Adding a Dell PowerScale OneFS (Isilon) Data Source - Summary

Now that you've installed the Dell CEE Framework and configured Dell to work with Varonis, you can deploy a Dell PowerScale OneFS (Isilon) data source to be monitored by the Varonis Collector. This section summarizes the procedure for deploying Dell PowerScale OneFS (Isilon) data sources in the Management Console.

> Note: If you do not want to open a large range of Dell ports for RPC, you can choose to open only specific ports. For more information, see the following Microsoft article.

1. Run the Management Console as an administrator.
2. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.
3. In the Resource Wizard's Common pane, specify the data source name, check the Collector selected by default and change it if needed, and enter the credentials for running directory structure monitoring (FileWalk).

   > Important:
   > - If you want to monitor a zone with a unique dedicated IP, you need to enter the name or IP for this specific zone in the Resource Details area.
   > - This account must have Backup Operator and Power User roles on the data source during installation.
   > - You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.

4. In the Resource Type area, select the data source type from the dropdown list. Then, click the Connect and verify link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

Note:

- The Connect and verify link is displayed only when all relevant data is entered.
- A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

5. In the Dell Management Access Settings area, to retrieve cluster information and the security style for shares, enter the credentials required for system zone IP access. Then, click Connect and verify to verify that the user is able to retrieve cluster information and the security style for shares. The connection status to the Dell Management API is displayed, indicating whether the user has access to the REST API.
6. In the Cluster Details area, after you click Connect and verify above, the cluster and zone information are auto-populated here.
   - Audit events from all access zones - This option is displayed only for system zones.

     Note: When selected, Varonis will audit events from all access zones and will associate them with the system zone data source. If a non-system access zone is installed as a data source, the events will be duplicated and associated with both the system and non-system data sources.
7. In the Monitored Shares area, select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source is installed and share detection is completed.
8. In the Configuration pane, review the Local Accounts, FileWalk Settings, and Event Auditing Parameters settings.
9. (Optional) In the Commit pane, clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials.

   Note:

   - If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
   - If the Collector is in a lower version than 8, the FileWalk credentials will be used.

In the Group OU area, if required, select Uniquely defined to choose a different OU from that defined in the data source's domain.

10. After configuration is complete, click Install to add the data source.
11. After the data source installation and share detection are completed, in the Shares pane, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. If you chose to monitor selected shares, you can select and register the required shares.

Note: If the security style is changed on the data source, then Varonis will automatically identify it and change the protocol that's used (from CIFS to NFS, for example).

What To Do Next

Now that you're familiar with the deployment steps, it's time to dive into the detailed procedure.

Adding a Dell PowerScale OneFS (Isilon) Data Source - Detailed Procedure

Now that you've installed the Dell CEE Framework and configured Dell to work with Varonis, you can deploy a Dell PowerScale OneFS (Isilon) data source to be monitored by the Varonis Collector.

Note: Varonis monitors CIFS shares on this data source.

Note: Each Dell PowerScale OneFS (Isilon) data source represents a monitored Dell PowerScale OneFS (Isilon) server. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source.

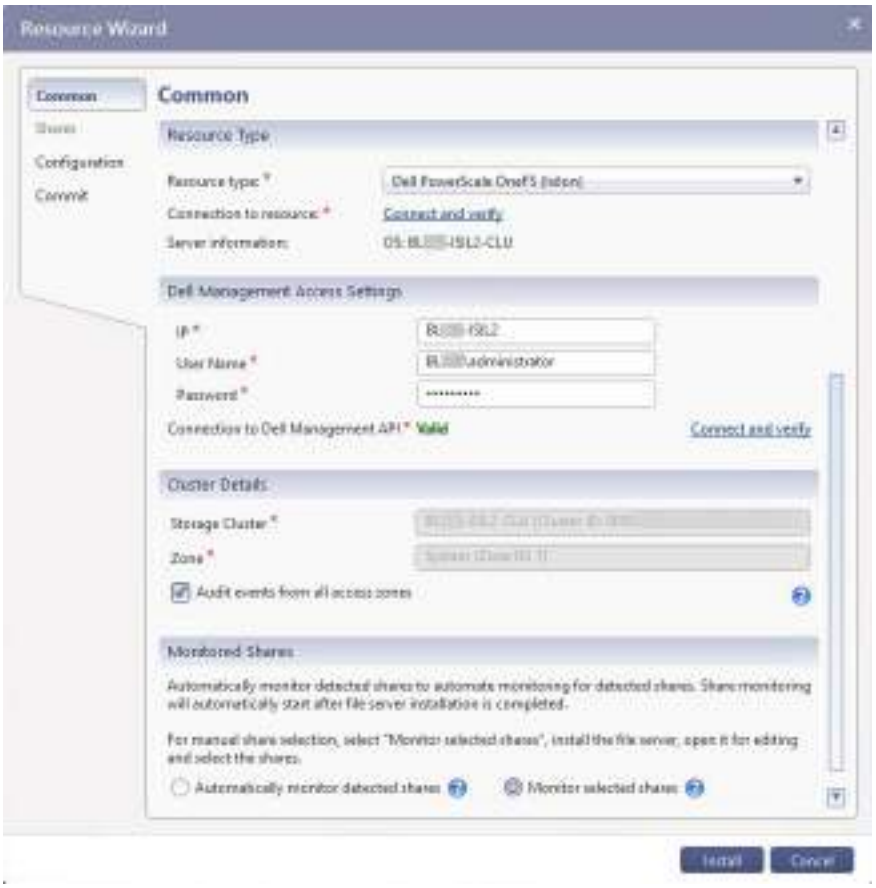
Note: If you do not want to open a large range of Dell ports for RPC, you can choose to open only specific ports. For more information, see the following Microsoft article.

Note: After Collector upgrade, if you need to edit your Dell PowerScale OneFS (Isilon) data source settings or your wish to monitor additional zones from the

same cluster, you'll need to fill in the system zone IP and credentials for automatic detection of cluster and zone information.

1. Set common data source parameters

1. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.
   The Resource Wizard is opened to the Common pane, where you can specify the data source and set the relevant parameters.



2. In the Common pane, set the following parameters:
   a. Resource Details - Specify the data source name. If you want to monitor a zone with a unique dedicated IP, you need to enter the name or IP for this specific zone.
   b. Data Collection Details - Select the relevant Collector from the dropdown list.
   c. FileWalk Credentials - Enter the credentials for running directory structure monitoring. File System operations include directory structure monitoring, event auditing (if set) and account enumeration on local accounts (if set).

- This account must have backup operator and power user roles on the data source during installation.
- These credentials are cached, so that they are automatically entered if another data source is added during the same session.
- User name - Type the name of the user account to be used for directory structure monitoring, event auditing, and local account enumeration.
- Password - Type the account's password.
- Add this user account to the Filtered Users list - The defined user for FileWalk Credentials will be added to the filtered users list. If you clear this checkbox, a large number of events may be generated by the user defined for directory structure monitoring. It is recommended to keep this checkbox enabled.

Important: You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.

d. Resource Type - Select the data source type from the dropdown list.
   - Connect and verify - Click this link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

     Note:
     - The Connect and verify link is displayed only when all relevant data is entered.
     - A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

e. Dell Management Access (REST API) Settings - Retrieving cluster information and the security style for shares require Dell Management REST API. Set the following:
   - IP - Type the system zone IP.
   - User name - Type the name of a user with permissions to access the system zone IP. Enter "Domain\user" if using a non-local account.
   - Password - Type the password for the relevant user.
   - Connect and verify access to Dell Management REST API - Click the Connect and verify link to verify that the user is able to retrieve cluster information and the security style for shares. The connection status to the

Dell Management API is displayed, indicating whether the user has access to the REST API.

f. Cluster Details - After you click Connect and verify above, the cluster and zone information are auto-populated in this area.

- Audit events from all access zones - This option is displayed only for system zones.

> Note: When selected, Varonis will audit events from all access zones and will associate them with the system zone data source. If a non-system access zone is installed as a data source, the events will be duplicated and associated with both the system and non-system data sources.

g. Monitored Shares - Select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source installed and share detection is completed.

- Automatically monitor detected shares - Select this option to automate monitoring for all detected shares. Share monitoring will automatically start after the data source installation is completed. Varonis will monitor all shares that aren't marked as "ignored". When this option is selected, click the Advanced setting link to modify share detection preferences. By default, the option is set to Prefer regular shares over equivalent admin shares. In this case, an admin share that has an equivalent regular share will be marked as "ignored" and the equivalent regular share will be detected for monitoring. Note: Any change in the monitored shares configuration, including the detection method, admin shares configuration, and selected shares, requires rerunning the resource detection.
- Monitor selected shares - This option is selected by default. You can manually select the shares to be monitored only after the data source is installed and share detection is completed. You'll need to open the Edit window for the installed data source and select the shares. For more information, see Post-installation share detection and registration.

Once the above settings are configured, you can proceed to review and adjust configuration settings.

2. Review and adjust configuration settings

1. On the left menu, click Configuration and confirm the information.
   The general configuration settings are displayed.
2. In the Local Accounts area, review the options:

- Collect information regarding local accounts from this file server - Select this checkbox to collect user accounts from this file system.

3. In the FileWalk Settings area, review the options:
   - Identify actual unique folders and file system inconsistencies - Select this checkbox (if it not already selected) to detect broken permissions in NTFS file systems.
4. In the Event Auditing Parameters area, review the options:
   - Filter out false "File Opened" events - Open events may be triggered unintentionally for a variety of reasons, resulting in inaccurate analysis of file system access. Select this option to filter such unintentional Open events and gather Open events only if enough file content is actually read. Small files and certain operations may still trigger Read events.
   - Collect Access Denied events - Select as necessary.

3. (Optional) Customize commit credentials

You can use different commit credentials instead of the default FileWalk credentials.

1. On the left menu, select Commit.
   The commit settings are displayed.
2. (Optional) Clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials. (By default, this checkbox is selected to use the FileWalk credentials, and the User name and Password fields are disabled for editing.)

   Note:
   - If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
   - If the Collector is in a lower version than 8, the FileWalk credentials will be used.
3. In the Group OU area, if required, select Uniquely defined to choose a different OU from that defined in the data source's domain. Click the Browse button (...) to select the required OU.

4. Install the data source

After configuration is complete, click Install to install the data source.

A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the File Servers pane. When the installation completes, the status shows "Installed 100%".

5. Post-installation share detection and registration

After the data source installation and share detection are completed, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. The following procedure describes the manual registration and automatic share detection flows.

Important: If after the data source is installed, share detection fails for any reason, the Share Detection Status column will remain "In Progress" until the issue is fixed, and share detection completes successfully at least once.

Important:

- If the security style is NTFS or mixed security, Varonis will automatically use CIFS for monitoring the data source. If the security style is Unix, Varonis will use NFS to monitor the data source.
- The Protocol column shows either CIFS or NFS. If your server's exposed protocol is not compatible with the security style, the share row in the Available Shares grid will be grayed out and you will not be able to register the share. A tooltip in the Access Details column will indicate the protocol mismatch.
- All NFS and CIFS events are audited regardless of the protocol used for monitoring.

After the data source is installed, the Shares pane is enabled, and you can view the share settings.

1. On the left menu, click Shares.
   The share settings are displayed. The pane's heading indicates the option you selected when adding a data source.
2. In the Available Shares area, you can filter the shares based on the reason they are not registered for monitoring and easily identify the shares that can be added. The default filter is Accessible Shares. You can change the filter to see the rest of the shares. Options include:
   - Accessible shares - Can be added for monitoring (this option is selected by default)
   - Ignored shares - Are marked as "ignored"

- Incompatible and inaccessible shares - Cannot be monitored since the exposed protocol does not match the security style of the volume (relevant to multiprotocol platforms only) or the Varonis service account does not have access to this share
- Child share of a monitored share - Is monitored via its parent folder

3. Do one of the following:
   - If you chose to monitor selected shares, in the Available Shares area, select the required shares and click the down arrow. The selected shares are moved to the Registered Shares area. (The registered shares list is empty until you make your selections.)
   - If you chose to automatically monitor detected shares, Varonis will monitor all shares that aren't marked as "ignored". The automated share detection runs every few hours. The Registered Shares area is autopopulated with the shares to be monitored.
4. For each share, review and set the following information as required:
   - Ignore Detection - Select the shares to be ignored (and not be the subject of automatic detection and notifications) by the data source monitor.
   - Events - Select this checkbox to audit events for the share.
   - Crawl - To enable or disable monitoring for the share, in the Crawl column, select the relevant option.

     Note: You can also right-click the grid and select the required options for event auditing and crawling.
5. In the Additional Share Settings area, review the options:
   - Remove deleted shares - Select this checkbox to remove deleted shares. Shares that were deleted from the data source will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the data source is unavailable, the shares will not be removed.
   - Enable event auditing - Select this checkbox to audit events from all shares added from this data source.

   After share detection and registration are completed, the status and number of registered volumes are respectively displayed in the Share Detection Status and Registered Shares columns in the File Servers pane.

Note: If the security style is changed on the data source, then Varonis will automatically identify it and change the protocol that's used (from CIFS to NFS, for example).

What To Do Next

Now let's take a look at the supported events for the monitored Dell PowerScale OneFS (Isilon) data sources.

Supported Events For Dell PowerScale OneFS (Isilon) Data Sources

The monitored data sources and NAS devices support various SMB (CIFS) and NFS events.

> Note: SMB v2 and v3 are supported.

Event Auditing Method

Dell auditing mechanism/CEPA

SMB (CIFS) Events for Dell PowerScale OneFS (Isilon) Data Sources

Supported File Operations

For more details about the "numbered" operations below, see the corresponding numbers in the "Limitations and Known Issues" following this list.

- File created
- File deleted[1]
- File modified[2]
- File opened
- File renamed
- File permissions changed [2]
- Folder created
- Folder deleted[1]
- Folder renamed
- Folder permissions changed [2]

> Note:

- File renamed and Folder renamed operations are supported only by CEPA.
- Permissions changed events do not include the details of the permissions that were changed.

Access Denied Events

Access denied events for Dell systems are supported according to the data received from the data source. These may vary among different versions of Dell, CEPA, and end-user clients.

- File deleted
- File opened

Limitations and Known Issues

1. Some DELETE_DIR is received for files. The Collector fixes it if finds "FILE" addressing in its cache or the name includes a file extension.
2. Dummy operations are sometimes executed.

NFS Events for Dell PowerScale OneFS (Isilon) Data Sources

Supported File Operations

- File created
- File deleted
- File renamed
- File modified
- File permissions changed
- Folder created
- Folder deleted
- Folder renamed
- Folder permissions changed

Note:

- NFS File opened events are inconsistent because the NFS client caches the results of the requests; requests similar to previous requests will not reach the NAS device and, therefore, won't be logged.
- Permissions changed events do not include the details of the permissions that were changed.

8 DELL UNITY DATA SOURCES

What This Section Contains

This section describes how to deploy and monitor Dell Unity data sources; the requirements, deployment and configuration steps, and supported events.

> Note: This section provides recommendations for configuring software from third-party vendors. Varonis is not responsible for ensuring the information contained herein is up to date. For more information, see the individual vendors' documentation. You should comply with any standard software and/or hardware licenses and related terms and conditions embedded in or furnished in connection with the third-party software, all of which are provided to you under the terms of those licenses and are not included as part of the Varonis end-user license agreement. Varonis shall have no responsibility for any products or services provided by third-party vendors.

What To Do Next

Before you dive in, click here to learn more about how Varonis monitors Dell Unity data sources.

Dell Unity Monitoring Overview

To monitor Dell Unity data sources, you need to configure Varonis to work with the Dell Common Event Publishing Agent (CEPA) event audting method. This requires installing the Common Event Enabler (CEE) package and configuring the CEE framework.

The Dell CEE framework is used to provide a working environment for various facilities. These include:

- Dell Common AntiVirus Agent (CAVA) - A Dell-provided agent that runs on a Windows Server and communicates with a standard antivirus engine to scan CIFS files stored on Dell Attached Storage.
- Dell CEPA - A Dell-provided agent that runs on a Windows Server and provides external applications with notification and optional control of changes made by CIFS clients in file systems on the Dell Network Server in real time. CEPA delivers both event notification and associated context to the application in one message. Context may comprise the file metadata or directory metadata needed to decide business policy.

While the CEE framework includes both CAVA and CEPA, they can run independently of each other or run together.

The Dell CEPA service and the Collector can be installed on the same server or on separate servers. For optimal performance, Varonis recommends installing them on separate servers.

Data Discovery and Classification

- Varonis supports data classification on files that reside in the monitored data sources.

What To Do Next

First, make sure you fulfill the Dell Unity requirements.

Dell Unity Requirements

Varonis Service Account

Varonis requires a dedicated service account. The service account can be reused for multiple data source installations and configurations.

- Service Account Read Operations:
  - Traverse and enumerate files, folders, directory structures, users, and groups.
  - Gather data source, user, and group metadata as part of normal system operations.
- Service Account Write Operations:
  - Used for executing Varonis Policies, if policies are defined.

Varonis Installation and Requirements

Important: Varonis does not support Dell Unity local accounts, only group information is collected instead of user information.

- Event auditing:
  - CEPA is required.
  - Optional – CEPA service on a dedicated server.
- A Windows Server capable of running the CEE framework package

Requirements for the Varonis Service Account for Read Operations

- Crawling:
  - NTFS - User with permissions to view all file system directories and their permissions (Administrator or Backup Operator and Power User).
- A Varonis service account (domain user) with local administrator credentials on the server running the CEE framework.

What To Do Next

Now that you've fulfilled the requirements, proceed to Install and Configure the Dell CEE Framework.

Requirements for the Varonis Service Account for Write Operations

Same as the Varonis service account for read operations.

Monitoring Dell Unity With Mixed Security Style

- If the security style is NTFS or mixed security, Varonis will automatically use CIFS for monitoring the data source. If the security style is Unix, Varonis will use NFS to monitor the data source.
- The Protocol column shows either CIFS or NFS. If your server's exposed protocol is not compatible with the security style, the share row in the Available Shares grid will be grayed out and you will not be able to register the share. A tooltip in the Access Details column will indicate the protocol mismatch.
- All NFS and CIFS events are audited regardless of the protocol used for monitoring.
- NFS v3 should be enabled.
- The Collector IP should be listed in the export policy of the share with read permissions.
- The NFS exports should be mountable.

Installing and Configuring the Dell CEE Framework

The CEPA service is configured by installing the Dell Common Event Enabler (CEE) framework package on a supported Windows Server.
For complete requirements and instructions on configuring CEE, see Dell's documentation.

> Note: For performance reasons, it is not recommended to install the CEPA service on the same server as the Collector.

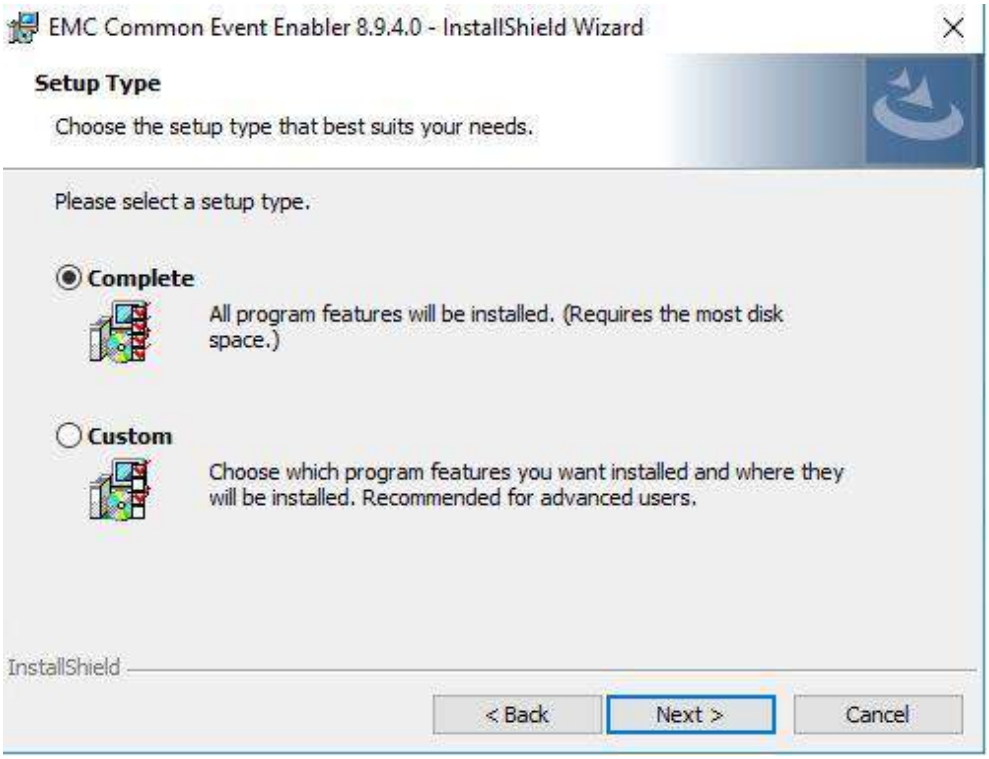
For all the CEE server connections (to/from Dell PowerScale OneFS (Isilon) and the Collector), see Varonis SaaS Firewall Rules.

Installing the Dell CEE Framework

Run the CEE installer package to install the Dell CEE framework.

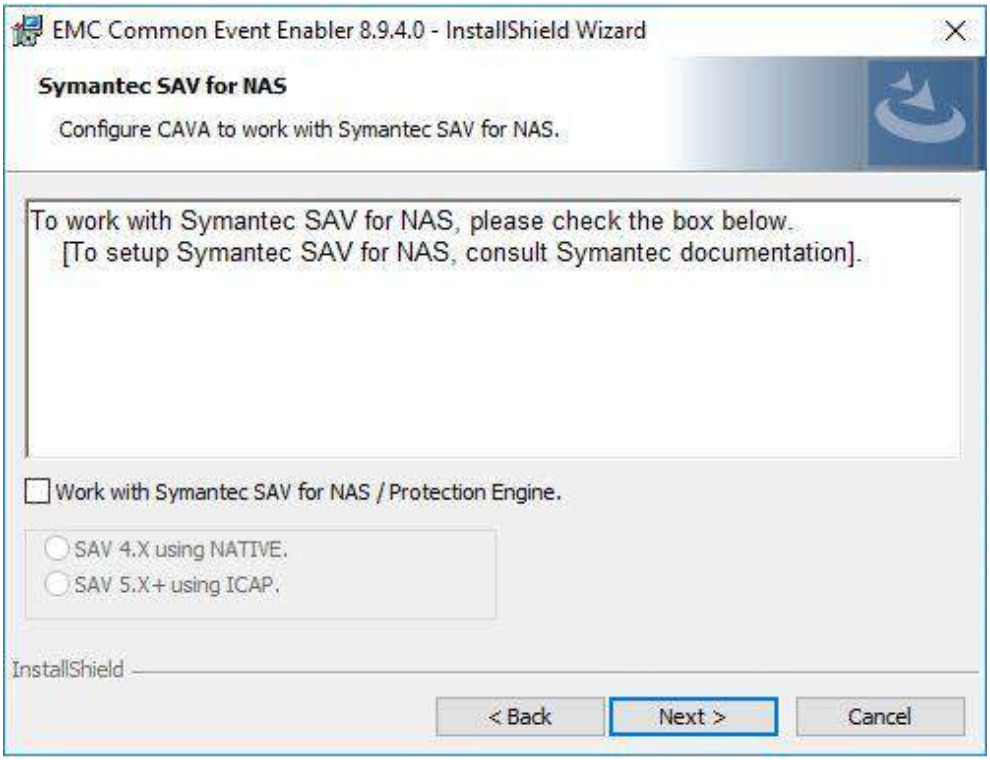
1. If any versions of Dell CEE Framework software earlier than v8.6 (including stand-alone CAVA or CEPA) are already installed on the CEE server, uninstall them before continuing.
2. Make sure to use the latest Dell CEE Framework version. Contact Dell technical support or your Peer Software technical to obtain the latest version.
3. Download and stage the 64-bit Dell CEE Framework installer on the CEE server. Proceed with the following steps to install the Dell CEE Framework software.
4. Run the Dell CEE Framework installer as an administrator.
   The Welcome page of the CEE Installation wizard is displayed.

5. Click Next.
   The License Agreement page is displayed.
6. Accept the terms of the license agreement, and click Next.
   The Customer Information page is displayed.
7. Enter your user name and organization, select Anyone who uses this computer (all users), and click Next.
   The Setup Type page is displayed.

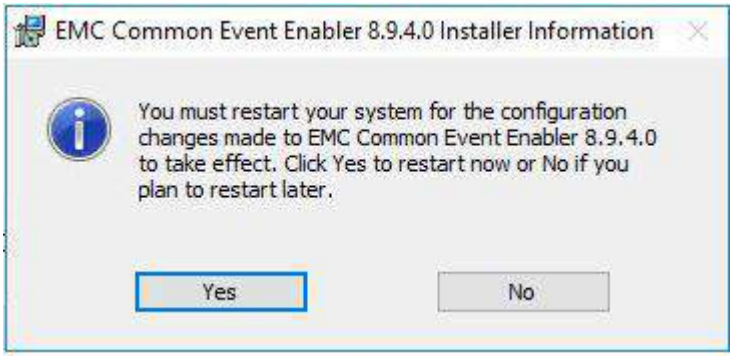


8. Select Complete or Custom. If you select Custom, you must select at least these two: CEPA and CEE Monitor. Then, click Next.

The Symantec SAV for NAS page is displayed.



9. Ensure that the Work with Symantec SAV for NAS/Protection Engine checkbox is not selected, and click Next.
   The Ready to Install the Program page is displayed.
10. Click Install.
    When the installation is complete, the InstallShield Wizard Completed page is displayed.
11. Click Finish.
    A message is displayed, prompting you to restart the system.



12. Click No. You will restart the system later.

Post-Installation Configuration for the Dell CEE Framework

This section describes the procedures required for Dell CEE Framework post-installation configuration.

Editing the Registry for the CEE

You need to make some changes to the registry for the CEE.

CEE Versions 6.0-8.7

Make the following changes to the registry:

> Note: If the Dell CEE Framework is upgraded or reinstalled, these registry changes must be re-entered. If the Varonis endpoint value is not set after upgrading the CEE, events are not collected.

1. Open the registry: Select Start > Run > regedit.
2. Locate the following key:
   - Up to CEE 6.0 (exclusive): `HKLM\Software\EMC\Celerra Event Grefpiv;EGSS;Cyhmx;Esr kyvexmsr`.
   - CEE 6.0.x: `KNOP;Vsjx0evi;GPE;EGG;EGSS;Cyhmx;Esr kyvexmsr`.
3. Edit the Endpoint string value as follows:
   - If the Varonis Collector is installed on the same machine, set the value to `Varonis`.
   - If the Varonis Collector is installed on another machine, set the value to `Varonis@<CollectorIP>`, where `<CollectorIP>` is the IP address of the Varonis Collector.

CEE Version 8.8 and Higher

Make the following changes to the registry:

> Note: If the Dell CEE Framework is upgraded or reinstalled, these registry changes must be re-entered. If the Varonis endpoint value is not set after upgrading the CEE, events are not collected.

1. Open the registry: Select Start > Run > regedit.

2. Locate the following key:
   `KNOP;Vsjx0evi;GPE;EGG;EGSS;Cyhmx;Esr kyvexmsr`
3. Edit the Endpoint string value as follows:
   - If the Varonis Collector is installed on the same machine, set the value to `Varonis`.
   - If the Varonis Collector is installed on another machine, set the value to `Varonis@<CollectorIP>`, where `<CollectorIP>` is the IP address of the Varonis Collector.
4. Locate the following key:
   `KNOP;Vsjx0evi;GPE;EGG;EGSS;Cyhmx;Esr kyvexmsr;Grefpih`
5. Change the Enabled DWORD value to 1.

Setting Service Credentials

You need to set credentials for the Dell CAVA service.

Make the following changes to the Dell CAVA service:

1. Open the Dell CAVA service (select Start > Run > services.msc).
2. Right-click the Dell CAVA service and select Properties.
3. Close the Services dialog box. The Dell CAVA service is set.

Completing the Dell CEE Framework Installation

After editing the registry and setting the required credentials, restart the Dell CAVA service to complete the installation.

What To Do Next

Now you're ready to configure the Dell storage device.

Configuring Dell Unity

Prior to configuring Dell Unity, ensure all required networks, file systems, and NAS servers are configured through the Dell Unisphere UI.

1. Access the Dell Unisphere UI.
2. For each NAS server on which you want to enable event publishing:
   a. Select the NAS server and edit its properties.

b. Select the Protection and Events tab.
c. Select the Events Publishing option from the left menu.
d. Create a CEPA pool for this NAS Server.
e. Configure the required post and post-error events.
f. Click Configure.

3. For each file system to be part of event publishing:
   a. Select the file system from the left menu.
   b. Select the Advanced tab.
   c. Select the Enable SMB Events publishing option.
   d. Click Apply.
4. Ensure that events are now moved from Unity to CEE/CEPA and published to the Varonis Collector.

What To Do Next

Now proceed to configure the Dell Unity REST API user.

Configuring the Dell Unity REST API Access User

Before you add Dell data sources, you need to configure the REST API access user.

The REST API credentials are used for continual polling of file system storage, ID, access policies, and supported protocols.

1. Access the Dell Unisphere UI.
2. Click the Settings icon, then select Users and Groups > User Management and click Add (+ sign).
   The Create User or Group page is displayed.
3. Select Local User. Then, click Next.
4. Enter the Username and Password. Then, click Next.
5. Select Operator for the role. Then, click Next.
6. Review your selections in the Summary page and click Finish.

What To Do Next

Now that you've configured Dell to work with Varonis SaaS, it's time to add a monitored Dell Unity data source. First familiarize yourself with the deployment steps summary and then dive into the detailed procedure.

Adding a Dell Unity Data Source - Summary

Now that you've installed the Dell CEE Framework and configured Dell to work with Varonis, you can deploy a Dell Unity data source to be monitored by the Varonis Collector. This section summarizes the procedure for deploying Dell Unity data sources in the Management Console.

Note: If you do not want to open a large range of Dell ports for RPC, you can choose to open only specific ports. For more information, see the following Microsoft article.

1. Run the Management Console as an administrator.
2. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.
3. In the Resource Wizard's Common pane, specify the data source name, check the Collector selected by default and change it if needed, and enter the credentials for running directory structure monitoring (FileWalk).

   Important:
   - This account must have Backup Operator and Power User roles on the data source during installation.
   - You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.
4. In the Resource Type area, select the data source type from the dropdown list. Then, click the Connect and verify link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

   Note:
   - The Connect and verify link is displayed only when all relevant data is entered.
   - A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.
5. In the Dell Management Access Settings area, to verify that the user is able to retrieve the security style for shares, connect and verify access to the Dell

Management REST API. Enter the IP of the Unity Management and the required credentials.

6. In the Monitored Shares area, select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source is installed and share detection is completed.
7. In the Configuration pane, review the Local Accounts, FileWalk Settings, and Event Auditing Parameters settings.
8. (Optional) In the Commit pane, clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials.

   Note:

   - If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
   - If the Collector is in a lower version than 8, the FileWalk credentials will be used.

   In the Group OU area, if required, select Uniquely defined to choose a different OU from that defined in the data source's domain.
9. After configuration is complete, click Install to add the data source.
10. After the data source installation and share detection are completed, in the Shares pane, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. If you chose to monitor selected shares, you can select and register the required shares.

Note: If the security style is changed on the data source, then Varonis will automatically identify it and change the protocol that's used (from CIFS to NFS, for example).

What To Do Next

Now that you're familiar with the deployment steps, it's time to dive into the detailed procedure.

Adding a Dell Unity Data Source - Detailed Procedure

Now that you've installed the Dell CEE Framework and configured Dell to work with Varonis, you can deploy a Dell Unity data source to be monitored by the Varonis Collector.

Note: Varonis monitors CIFS shares on this data source.

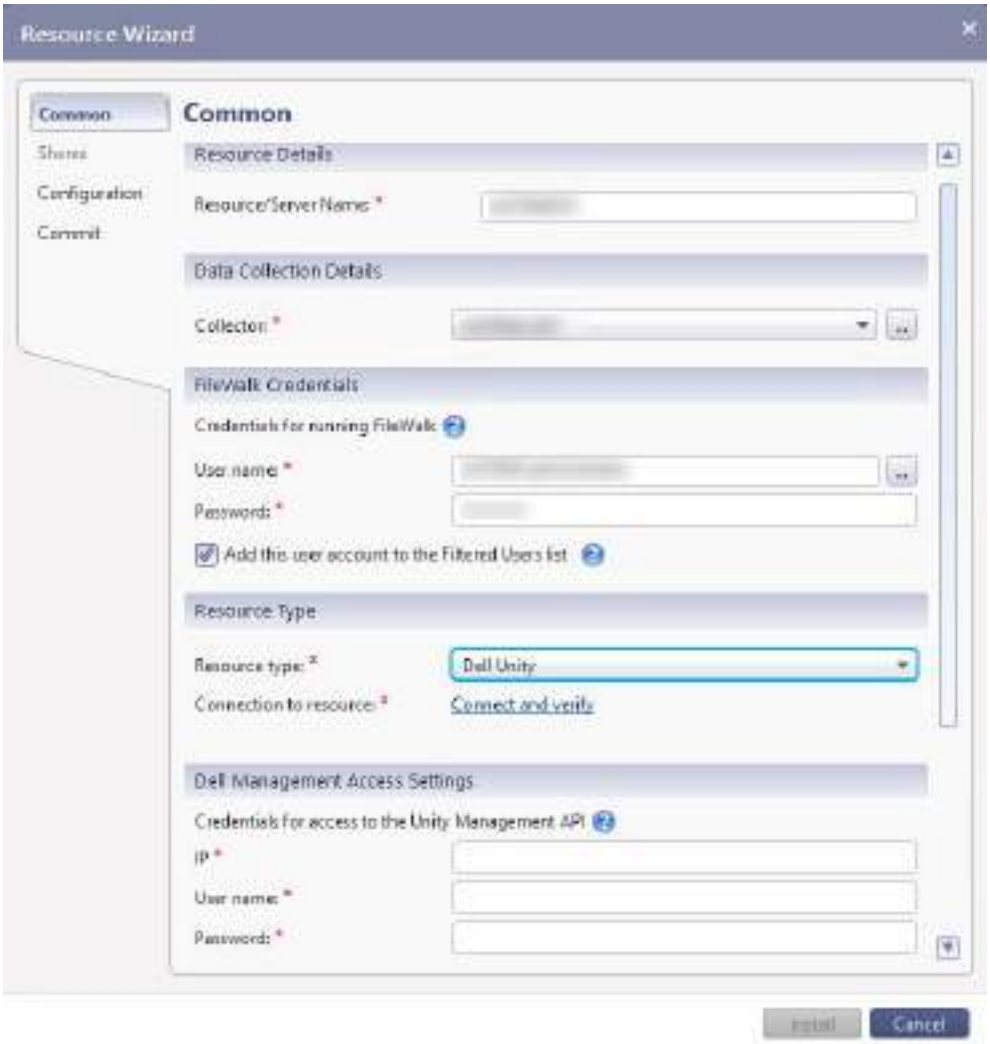
Note: Each Dell Unity data source represents a monitored Dell Unity server. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source.

Note: If you do not want to open a large range of Dell ports for RPC, you can choose to open only specific ports. For more information, see the following Microsoft article.

1. Set common data source parameters

1. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.

The Resource Wizard is opened to the Common pane, where you can specify the data source and set the relevant parameters.



2. In the Common pane, set the following parameters:
   a. Resource Details - Specify the data source name.
   b. Data Collection Details - Select the relevant Collector from the dropdown list.
   c. FileWalk Credentials - Enter the credentials for running directory structure monitoring. File System operations include directory structure monitoring, event auditing (if set) and account enumeration on local accounts (if set).
      - This account must have backup operator and power user roles on the data source during installation.
      - These credentials are cached, so that they are automatically entered if another data source is added during the same session.
      - User name - Type the name of the user account to be used for directory structure monitoring, event auditing, and local account enumeration.

- Password - Type the account's password.
- Add this user account to the Filtered Users list - The defined user for FileWalk Credentials will be added to the filtered users list. If you clear this checkbox, a large number of events may be generated by the user defined for directory structure monitoring. It is recommended to keep this checkbox enabled.

> Important: You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.

d. Resource Type - Select the data source type from the dropdown list.
   - Connect and verify - Click this link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

     > Note:
     > - The Connect and verify link is displayed only when all relevant data is entered.
     > - A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

e. Dell Management Access Settings - Retrieving the security style for shares requires Dell Management REST API. Enter the following credentials:
   - IP - Enter the IP of the Unity Management.
   - User name - Create a new local user with the Operator role. Insert a REST API user name.
   - Password - Insert a REST API password.
   - Connect and verify - Click this link to verify that the user is able to retrieve the security style for shares. The connection status to the Dell Management API is displayed, indicating whether the user has access to the REST API.

f. Monitored Shares - Select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source installed and share detection is completed.
   - Automatically monitor detected shares - Select this option to automate monitoring for all detected shares. Share monitoring will automatically start after the data source installation is completed. Varonis will monitor all shares that aren't marked as "ignored". When this option is selected, click the Advanced setting link to modify share detection preferences. By default, the

option is set to Prefer regular shares over equivalent admin shares. In this case, an admin share that has an equivalent regular share will be marked as "ignored" and the equivalent regular share will be detected for monitoring. Note: Any change in the monitored shares configuration, including the detection method, admin shares configuration, and selected shares, requires rerunning the resource detection.

- Monitor selected shares - This option is selected by default. You can manually select the shares to be monitored only after the data source is installed and share detection is completed. You'll need to open the Edit window for the installed data source and select the shares. For more information, see Post-installation share detection and registration.

Once the above settings are configured, you can proceed to review and adjust configuration settings.

2. Review and adjust configuration settings

1. On the left menu, click Configuration and confirm the information.
   The general configuration settings are displayed.
2. In the Local Accounts area, review the options:
   - Collect information regarding local accounts from this file server - Select this checkbox to collect user accounts from this file system.
3. In the FileWalk Settings area, review the options:
   - Identify actual unique folders and file system inconsistencies - Select this checkbox (if it not already selected) to detect broken permissions in NTFS file systems.
4. In the Event Auditing Parameters area, review the options:
   - Filter out false "File Opened" events - Open events may be triggered unintentionally for a variety of reasons, resulting in inaccurate analysis of file system access. Select this option to filter such unintentional Open events and gather Open events only if enough file content is actually read. Small files and certain operations may still trigger Read events.
   - Collect Access Denied events - Select as necessary.

3. (Optional) Customize commit credentials

You can use different commit credentials instead of the default FileWalk credentials.

1. On the left menu, select Commit.

The commit settings are displayed.

2. (Optional) Clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials. (By default, this checkbox is selected to use the FileWalk credentials, and the User name and Password fields are disabled for editing.)

   Note:

   - If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
   - If the Collector is in a lower version than 8, the FileWalk credentials will be used.

3. In the Group OU area, if required, select Uniquely defined to choose a different OU from that defined in the data source's domain. Click the Browse button (...) to select the required OU.

4. Install the data source

After configuration is complete, click Install to install the data source.

A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the File Servers pane. When the installation completes, the status shows "Installed 100%".

5. Post-installation share detection and registration

After the data source installation and share detection are completed, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. The following procedure describes the manual registration and automatic share detection flows.

Important: If after the data source is installed, share detection fails for any reason, the Share Detection Status column will remain "In Progress" until the issue is fixed, and share detection completes successfully at least once.

Important:

- If the security style is NTFS or mixed security, Varonis will automatically use CIFS for monitoring the data source. If the security style is Unix, Varonis will use NFS to monitor the data source.

- The Protocol column shows either CIFS or NFS. If your server's exposed protocol is not compatible with the security style, the share row in the Available Shares grid will be grayed out and you will not be able to register the share. A tooltip in the Access Details column will indicate the protocol mismatch.
- All NFS and CIFS events are audited regardless of the protocol used for monitoring.

After the data source is installed, the Shares pane is enabled, and you can view the share settings.

1. On the left menu, click Shares.
   The share settings are displayed. The pane's heading indicates the option you selected when adding a data source.
2. In the Available Shares area, you can filter the shares based on the reason they are not registered for monitoring and easily identify the shares that can be added. The default filter is Accessible Shares. You can change the filter to see the rest of the shares. Options include:
   - Accessible shares - Can be added for monitoring (this option is selected by default)
   - Ignored shares - Are marked as "ignored"
   - Incompatible and inaccessible shares - Cannot be monitored since the exposed protocol does not match the security style of the volume (relevant to multiprotocol platforms only) or the Varonis service account does not have access to this share
   - Child share of a monitored share - Is monitored via its parent folder
3. Do one of the following:
   - If you chose to monitor selected shares, in the Available Shares area, select the required shares and click the down arrow. The selected shares are moved to the Registered Shares area. (The registered shares list is empty until you make your selections.)
   - If you chose to automatically monitor detected shares, Varonis will monitor all shares that aren't marked as "ignored". The automated share detection runs every few hours. The Registered Shares area is autopopulated with the shares to be monitored.
4. For each share, review and set the following information as required:
   - Ignore Detection - Select the shares to be ignored (and not be the subject of automatic detection and notifications) by the data source monitor.

- Events - Select this checkbox to audit events for the share.
- Crawl - To enable or disable monitoring for the share, in the Crawl column, select the relevant option.

  Note: You can also right-click the grid and select the required options for event auditing and crawling.

5. In the Additional Share Settings area, review the options:
   - Remove deleted shares - Select this checkbox to remove deleted shares. Shares that were deleted from the data source will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the data source is unavailable, the shares will not be removed.
   - Enable event auditing - Select this checkbox to audit events from all shares added from this data source.

   After share detection and registration are completed, the status and number of registered volumes are respectively displayed in the Share Detection Status and Registered Shares columns in the File Servers pane.

Note: If the security style is changed on the data source, then Varonis will automatically identify it and change the protocol that's used (from CIFS to NFS, for example).

What To Do Next

Now let's take a look at the supported events for the monitored Dell Unity data sources.

Supported Events For Dell Unity Data Sources

The monitored data sources and NAS devices support various SMB (CIFS) and NFS events.

Note: SMB v2 and v3 are supported.

Event Auditing Method

Dell auditing mechanism/CEPA

SMB (CIFS) Events for Dell Unity Data Sources

Relevant for Dell Unity data sources, starting from version 4.1.

Supported File Operations

For more details about the "numbered" operations below, see the corresponding numbers in the "Limitations and Known Issues" following this list.

- File modified[2]
- File opened
- File created
- File deleted[1, 2]
- File renamed[2]
- File permissions changed[2]
- Folder created
- Folder deleted[1, 2]
- Folder renamed[2]
- Folder permissions changed[2]

Note:

- File renamed and Folder renamed operations are supported only by CEPA.
- Permissions changed events do not include the details of the permissions that were changed.

Access Denied Events

Access denied events for Dell systems are supported according to the data received from the data source. These may vary among different versions of Dell, CEPA, and end-user clients.

- File modified
- File created
- File opened
- File permissions changed
- Folder created

- Folder opened
- Folder permissions changed

Limitations and Known Issues

1. Some DELETE_DIR is received for files. The Collector fixes it if finds "FILE" addressing in its cache or the name includes a file extension.
2. Dummy operations are sometimes executed.

NFS Events for Dell Unity Data Sources

Supported File Operations

- File created
- File deleted
- File renamed
- File modified
- File permissions changed
- Folder created
- Folder deleted
- Folder renamed
- Folder permissions changed

Note:

- NFS File opened events are inconsistent because the NFS client caches the results of the requests; requests similar to previous requests will not reach the NAS device and, therefore, won't be logged.
- Permissions changed events do not include the details of the permissions that were changed.

Access Denied Events

Access denied events for Dell systems are supported according to the data received from the data source. These may vary among different versions of Dell, CEPA, and end-user clients.

- File deleted
- File permissions changed
- Folder deleted
- Folder permissions changed

Note: File opened NFS access denied events are not supported for Dell Unity.

9 AZURE FILES DATA SOURCES

What This Section Contains

This section describes how to deploy and monitor Azure Files data sources; the requirements, deployment and configuration steps, and supported events.

What To Do Next

Before you dive in, click here to learn more about how Varonis monitors Azure Files accounts, file system, and events.

Azure Files Monitoring Overview

Note: Each data source represents a monitored Azure Files storage account. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source. To monitor multiple storage accounts, you will need to add a data source per storage account.

About Azure Files

- The Azure Files data is stored in Azure (Microsoft's public cloud). Some customers also deploy on-premises cache servers called Azure Files Sync servers, which are Windows servers running Azure Files Sync components.
- Each Azure subscription can contain one or more Azure Files storage accounts. Each storage account contains one or more shares.
- Users and apps can access the Azure Files data either via direct access to Azure, or via the Azure Files Sync servers, depending on the customer's preferred topology and configuration.
- Each Azure Files Sync server is always synced to a single storage account. Each Azure Files Sync server is limited to 30 shares (Microsoft's limitation).
- Users can configure the Azure Files Sync servers to store only the recently accessed data (that is, cloud tiering enabled) or all data (that is, cloud tiering disabled). Storing all data on the Azure Files Sync servers can be costly and is therefore avoided by most customers. The directory structure and permissions are always stored on the Azure Files Sync servers.
- The ACEs (permissions) of AD, Entra ID, and local accounts on the Azure Files resources (share/folder/file) are all stored in Azure Files on Azure.
- When users and apps access Azure Files directly (not via the Azure Files Sync servers), events are triggered and logged in the Azure Storage Log, but only if Azure's File Diagnostic Settings are enabled. To enable the File Diagnostic Settings, you must configure a destination to which the logs will be shipped from the Azure Storage Log.
- When users and apps access Azure Files via the Azure Files Sync servers, events are triggered locally on the Azure Files Sync servers, identically to plain Windows servers.
- Each Azure Files resource (share/folder/file) has a unique path in Azure's storage account. When using Azure Files Sync servers, the synced files also get a local path. Varonis always displays the Azure's storage account's path.

How Varonis Monitors Azure Files

- Collectors:
  - You are required to configure a primary Collector. To optimize for low latency and reduced costs, the Collector should reside in Azure, as close as possible to the monitored Azure Files data.
  - If you're using Azure Files Sync servers, additional Collectors should be configured as close as possible, ideally within LAN proximity, to each Azure Files Sync server (same as for monitored Windows Servers). Each Azure Files Sync server can be monitored by a different Collector.
- Accounts:
  - Entra ID accounts are directly enumerated from the Varonis tenant in Azure.
  - AD accounts are enumerated from the local Collector.
  - Local Windows accounts are enumerated from the associated local Collector monitoring each Azure Files Sync server.
- Events:
  - During the Azure Files deployment, Varonis enables Azure's File Diagnostic Settings and configures it to ship the events from the Azure Storage Log to the Azure Event Hub (an events queue). The primary Collector (via the Forwarder process) monitors the events from the event hub.
  - To audit events from each Azure Files Sync server, an agent (identical to the Windows agent) must be installed on each Azure Files Sync server. The agent can be automatically installed during the deployment process or manually later during a change control window (same as for monitored Windows Servers).
- Directory structure and permissions, and data classification:
  - Directory structure monitoring and Data Classification processes run from the primary Collector, connect directly to Azure Files via SMB (CIFS), and monitor the directory structure and permissions, and file contents.
  - The Incremental FileWalk (directory structure monitoring) process runs on the primary Collector and on each Collector monitoring one or more Azure Files Sync servers:
    - Incremental FileWalk, which runs on the primary Collector, is triggered by events audited from Azure Event Hub, and by Data Classification, if it detects sensitive files.
    - Incremental FileWalk, which runs on each Collector monitoring Azure Files Sync servers, is triggered by events audited from the Azure Files Sync servers, and by Data Classification, if it detects sensitive files.

Limitations

- When users/applications access Azure Files directly to perform permission changes, respective events are not logged in the Azure Storage Log (Microsoft limitation). Therefore, Varonis does not monitor permission change events if the permissions were performed via direct access.

What To Do Next

First, make sure you fulfill the Azure Files requirements.

Azure Files Requirements

Varonis Service Account

Varonis requires a dedicated service account. The service account can be reused for multiple data source installations and configurations.

- Service Account Read Operations:
  - Traverse and enumerate files, folders, directory structures, users, and groups.
  - Gather data source, user, and group metadata as part of normal system operations.
- Service Account Write Operations:
  - Used for executing Varonis Policies, if policies are defined.

General Operational Requirements

- For optimal performance, ensure that a Varonis Collector resides in Azure, next to the monitored Azure Files data.
- The following should be deployed:
  - A separate Azure Files data source per each Azure Files storage account that you wish to monitor.
  - Entra ID domains with accounts that have access to the Azure Files data.
  - AD domains with accounts that have access to the cache servers.

Requirements for the Varonis Service Account for Read Operations

- Must be a domain user that has direct SMB (CIFS) access to the Azure file shares.
- Requires the Storage File Data SMB Share Contributor role for API calls on files and folders such as GetFileAttributes (metadata). The Storage File Data SMB Share Reader role is not sufficient.
- Requires AD Domain Services (AD DS) authentication over SMB to access the shares. For this, AD is required as the storage account's primary identity-based access provider. Go to the Microsoft Azure portal to verify that AD is enabled. If it's not enabled, click here for instructions.
- Operations such as reading folder metadata or accessing certain share-level resources require elevated roles. These operations not provided with the SMB Reader and require the SMB Contributor role instead.
- The account should have NTFS permissions for all the folders and files under the share, in addition to the share permissions.

Requirements for the Varonis Service Account for Write Operations

In addition to the requirements for the read operations, the Varonis service account for write operations requires the Storage File Data SMB (CIFS) Share Contributor role.

Azure Files Sync Server Requirements

- Deploy one or more Collectors for the monitored Azure Files Sync servers (for monitoring local accounts and events from the Azure Files Sync servers). Each Collector should ideally monitor only the nearby Azure Files Sync servers. This step is optional and required only if you're using Azure Files Sync servers.
- To monitor Azure Files Sync servers, the Storage Sync Services must be under the same Resource Group as the Azure file shares.

Requirements for Deploying Azure Files Data Sources

- Must be a domain user that has direct SMB (CIFS) access to the Azure file shares.
- Requires the User Access Administrator role assigned in the subscription. The User Access Administrator (RBAC) role is required to grant and revoke permissions on Azure resources. This role is essential for Varonis to assign the Reader role to the application that monitors Azure Files. This enables Varonis to

view the Sync Servers topology when the data source is deployed in the Management Console. This role can be removed upon completion of the installation process. For more information, see this article.

- Requires the Storage File Data SMB Share Contributor role for API calls on files and folders such as GetFileAttributes (metadata). The Storage File Data SMB Share Reader role is not sufficient.
- Requires AD Domain Services (AD DS) authentication over SMB to access the shares. For this, AD is required as the storage account's primary identity-based access provider. Go to the Microsoft Azure portal to verify that AD is enabled. If it's not enabled, click here for instructions.

What To Do Next

Now that you've fulfilled the requirements, proceed to configure the User Access Administrator.

Configuring a User Access Administrator for Creating a New Entra ID Application

Before you add Azure Files data sources, you need to configure an Azure user with the User Access Administrator role assigned in the subscription. This is required for the Varonis automatic Entra ID application creation process.

This is required for the Varonis automatic Entra ID application creation process

1. Go to the Microsoft Azure portal.
2. Log in using an account with permissions to create applications in Entra ID.
3. Click Subscriptions and click on your subscription.
4. Click Access control (IAM) (on the left).
5. Click the Role Assignments tab.
6. Click Add and select Add role assignment.
   The Add role assignment page is opened to the Role tab.
7. Click the Privileged administrator roles tab.
8. Select User Access Administrator. Then, click Next.
9. In the Members tab, click Select members, and in the pane on the right, select the name of the user you want to use to create the new Entra ID application when installing the Azure File data source. Click Select.
10. Click Review + assign.

What To Do Next

Now that you've configured the Azure user with the User Access Administrator role, proceed to configure permissions for direct access SMB.

Configuring Permissions for Direct Access SMB

Before you add Azure Files data sources, you need to configure permissions for direct access SMB.

1. In the Microsoft Azure portal home page, select the storage account in which the shares reside.
2. Under Data storage (on the left), select File Shares.
3. Do one of the following:
   - To configure access for all the shares in the storage account for all synced AD users in the organization, set Active Directory wide role settings:
     - Under File share settings (on the upper right), click the Identify-based access: Configured link . The Active Directory page is opened.
     - For Default share-level permissions, select Enable permissions for all authenticated users and groups.
     - From the Select appropriate role dropdown list, choose Storage File Data SMB Share Contributor. This is required for directory structure monitoring and data classification.
     - Click Save. This can take a while to complete (up to 3 hours). This sets access to all shares to all synced AD users.
   - To configure access to specific shares in the storage account, set share-wide role settings:
     - Under File share settings, click the relevant share.
     - Click Access Control (IAM) (on the left).
     - Click the Role Assignments tab.
     - Click Add and select Add role assignment. The Add role assignment page is opened to the Role tab.
     - In the Job function roles tab, select Storage File Data SMB Share Contributor. Then, click Next.
     - In the Members tab, click Select members, and in the pane on the right, select the name of the AD user that is synced to Azure. This is the user used for direct access SMB in the Varonis Management Console (the Varonis service account). Click Select.

- Click Review + assign. This can take a while to complete (up to 3 hours). This sets access to the specified shares for the synced AD user.

4. To verify that the Varonis service account has access to a share, open the Collector server in a Windows Explorer tab in the following path: `\\<storage account reqi # pi#gsvi#0mrhs0w#rix\<share name>`. If you have access with the Varonis service account connected to the Collector, you can proceed to install the Azure Files data source.

> Note: If you add a new share on the share level and not on the storage account level, you will need to configure the service account user permissions manually.

What To Do Next

Now that you've configured permissions for direct access SMB, proceed to add a monitored Azure Files data source. First familiarize yourself with the deployment steps summary and then dive into the detailed procedure.

Adding an Azure Files Data Source - Summary

This section summarizes the procedure for deploying Azure Files data sources in the Management Console.

1. Run the Management Console as an administrator.
2. Select Management > Components > Root > Domains and verify that an Entra ID domain has been added.
3. Add an Azure Files data source: Select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.
4. Select the Resource type > Azure Files.
5. In the Resource Wizard's Common pane, check the Collector selected by default and change it if needed (make sure that it has direct access to SMB).
6. In the Connection Details area, select the Entra ID domain, the subscription, and add one dedicated application (existing or new).

> Note: To autodiscover the subscription list and to monitor events from the Azure Event Hub after the deployment, you need to provide an Entra ID application. The Entra ID application can be automatically created through the Management Console, or manually through the Microsoft Entra admin center. If you choose to create the application automatically, it will be created using the credentials of the Entra ID application that was defined in the Entra ID domain

7. In the Monitored Storage Account area, select the resource group and Azure storage account.
8. In the Event Auditing area, leave the Audit direct access events for Azure Files Shares option as selected and configure a file diagnostic setting (create a new one or use an existing one) for event auditing.
9. In the Monitoring Directory Structure and Permissions area, enter the credentials for monitoring directory structure and permissions in the format domain\username.
10. In the Monitored Shares area, select whether to automatically monitor all detected shares or to monitor selected shares. Share selection is only available after the data source is installed and share detection is completed.
11. In the AFS Sync Servers pane, register the Azure Files Sync servers to be monitored for event auditing and local account enumeration. Configure the automatic or manual installation of an agent on each monitored Azure Files Sync server.
12. In the Configuration pane, review the Local Accounts and Event Auditing Parameters settings.
13. (Optional) In the Commit pane, clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials.

    Note:

    - If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
    - If the Collector is in a lower version than 8, the FileWalk credentials will be used.

14. After configuration is complete, click Install to add the Azure Files data source.
15. After the data source installation and share detection are completed, in the Shares pane, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. If you chose to monitor selected share, you can select and register the required shares.

What To Do Next

Now that you're familiar with the deployment steps, it's time to dive into the detailed procedure.

Adding an Azure Files Data Source - Detailed Procedure

Now that you've configured the Azure user with the User Access Administrator role, you can deploy an Azure Files data source.

Note: Each data source represents a monitored Azure Files storage account. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source. To monitor multiple storage accounts, you will need to add a data source per storage account.

1. Check if an Entra ID data source exists

1. Run the Management Console as an administrator.
2. Select Management > Components > Root > Domains and verify that an Entra ID domain has been added.

2. Add an Azure Files data source

Important:

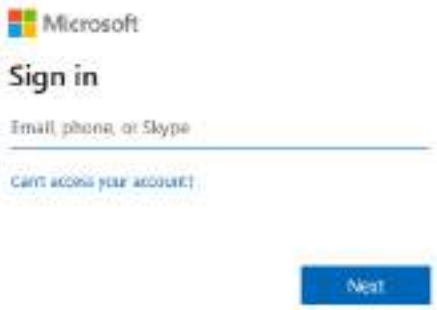
- You cannot install more than one Azure Files server from the same storage account.
- A single Entra ID application can be used to monitor multiple Azure Files storage accounts.
- You can monitor multiple Azure Files storage accounts that use the same Windows Servers as Sync servers. This requires upgrading the Varonis Windows Agent on the Azure Files Sync servers to agent version 11 or higher.
- You can monitor a Sync Server as a Windows Data source in parallel to being monitored as a Sync server, if the Azure Files server is using cloud tiering enabled, data classification on the Windows server may hydrate the cache.

1. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.
   The Resource Wizard is opened to the Common pane, where you can specify the data source and set the relevant parameters.
2. In the Resource Type area, select Azure Files from the dropdown list.
   The Connection Details area is displayed.

3. Select the Entra ID Domain from the dropdown list. This step is required if you have more than one Entra ID domain installed; otherwise, this field is autopopulated.



4. Click Load Subscriptions List to get the subscription list for the specified Entra ID domain.
   The Microsoft Sign in page is displayed.



5. Enter the credentials of a user with permissions to create an application in Entra ID. Enter the username, click Next, enter the account password, and click Sign in.



6. Then, select the subscription from the Subscription dropdown list. This step is required if you have more than one subscription in your tenant; otherwise, this field is autopopulated.
   After the Entra ID domain and subscription are selected, additional options are displayed in the Connection Details area to automatically create a new Entra ID application or use an existing one.
7. In the Connection Details area, the Create New option is selected by default. You can decide to create a new Entra ID application (step 6a) or use an existing one that you've created in Entra ID (step 6b). Follow either of the procedures below to set up the required Entra ID application.



   a. To create a new Entra ID application:

      Important: Before you begin this procedure, make sure you have configured the Azure user with the User Access Administrator role assigned in the subscription. Click here for instructions.

      i. Click the Browse (…) button next to the Entra ID application field.

      ii. Enter the credentials of a user with permissions to create an application in Entra ID. Enter the username, click Next, enter the account password, and click Sign in.
      A new application is now created in Entra ID. When completed, a confirmation message is displayed indicating that the application was successfully created. The name of the Entra ID application is now displayed in the field in the Management Console (it's grayed out).

b. To use an existing Entra ID application:

Important:

- Before you begin this procedure, make sure you have added a certificate via the Microsoft Entra admin center and that the Entra ID application has user_impersonation delegated permission assigned. Click here for instructions.
- To audit events, the application used for monitoring Azure File Shares needs to be assigned the Contributor and Azure Event Hubs Data Receiver roles under the subscription. This is necessary when an event hub is created automatically. However, if the event hub namespace and name are manually entered, user_impersonation delegated permission is required to enable Varonis to validate the connection between the event hub and Azure Files.

i. In the Connection Details area, select Use existing.



ii. Click the Browse (…) button next to the Entra ID application field. The Use Existing Entra ID Application dialog box is displayed.



iii. Enter the Application ID. To locate the Application ID, go to entra.microsoft.com > Identity > Applications > Enterprise applications, select the application you created, and copy the Application ID.

iv. Enter the Certificate file path. Click the Browse (…) button to upload a certificate (public key) with a PFX file type.

v. Enter the Certificate file path password. This the password provided for encryption of the PFX file.

vi. Click OK to close the dialog box.

After the application settings have been completed, the Monitored Storage Account area is displayed. Proceed to set the parameters.

8. In the Monitored Storage Account area, set the following parameters:
   - Resource Group - Select the Azure resource group from the dropdown list.
   - Storage Account - Select the Azure storage account from the dropdown list.

     Note: Only storage accounts with Azure File Shares will be displayed in the list.

9. In the Event Auditing area, set the following parameters:
   - Audit direct access events for Azure Files Shares - Selected by default. It's not recommended to clear this option; otherwise, event loss may occur.
   - File Diagnostic Settings - The Create New option is selected by default. You can decide to create a new file diagnostic setting (step 9a) for event auditing or use an existing one that you've created in the Microsoft Entra admin center (step 9b).

   a. To create a new file diagnostic setting:
      i. Click Create new.
      ii. Click the Browse (…) button next to the Event hub namespace field, enter the credentials of a user with permissions to create an application in Entra ID. Enter the username, click Next, enter the account password, and click Sign in. The Permissions requested page is displayed. Click Accept. The name of the Event hub namespace is now displayed in the field in the Management Console (it's grayed out).

   b. To use an existing file diagnostic setting:

      Important: Before you begin this procedure, make sure you have configured an event hub and file diagnostic setting. Click here for instructions.

      i. Click Use existing.
      ii. Click the Browse (…) button next to the Event hub namespace field. The Use Existing Event Hub dialog box is displayed.



      iii. Enter the Event hub namespace and Event hub name. To locate these, go to entra.microsoft.com > Storage accounts, select your storage account, go to

Monitoring > Diagnostic settings, click file, click Edit setting next to the file diagnostic setting you want to use and copy the Event hub namespace and Event hub name.

iv. Click OK. The Microsoft Sign in page is displayed.

v. Enter the credentials of a user with permissions to create an application in Entra ID. Enter the username, click Next, enter the account password, and click Sign in. The Permissions requested page is displayed. Click Accept. The name of the Event hub namespace is now displayed in the field in the Management Console (it's grayed out).

10. In the Data Collection Details area, select the relevant Collector (that has direct access to SMB) from the dropdown list.
11. In the Monitoring Directory Structure and Permissions area, enter the credentials for monitoring directory structure and permissions in the format domain\username:
    - User name - Type the name of the user account to be used for directory structure monitoring and event auditing.
    - Password - Type the account's password.
    - Add this user account to the Filtered Users list - The defined user for Azure Files Sync server credentials will be added to the filtered users list. If you clear this checkbox, a large number of events may be generated by the user defined for directory structure monitoring. It is recommended to keep this checkbox enabled.
12. In Monitored Shares - Select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source installed and share detection is completed.
    - Automatically monitor detected shares - Select this option to automate monitoring for all detected shares. Share monitoring will automatically start after the data source installation is completed. Varonis will monitor all shares that aren't marked as "ignored". When this option is selected, click the Advanced setting link to modify share detection preferences. By default, the option is set to Prefer regular shares over equivalent admin shares. In this case, an admin share that has an equivalent regular share will be marked as "ignored" and the equivalent regular share will be detected for monitoring. Note: Any change in the monitored shares configuration, including the detection method, admin shares configuration, and selected shares, requires rerunning the resource detection.
    - Monitor selected shares - This option is selected by default. You can manually select the shares to be monitored only after the data source is installed and share detection is completed. You'll need to open the Edit window for the

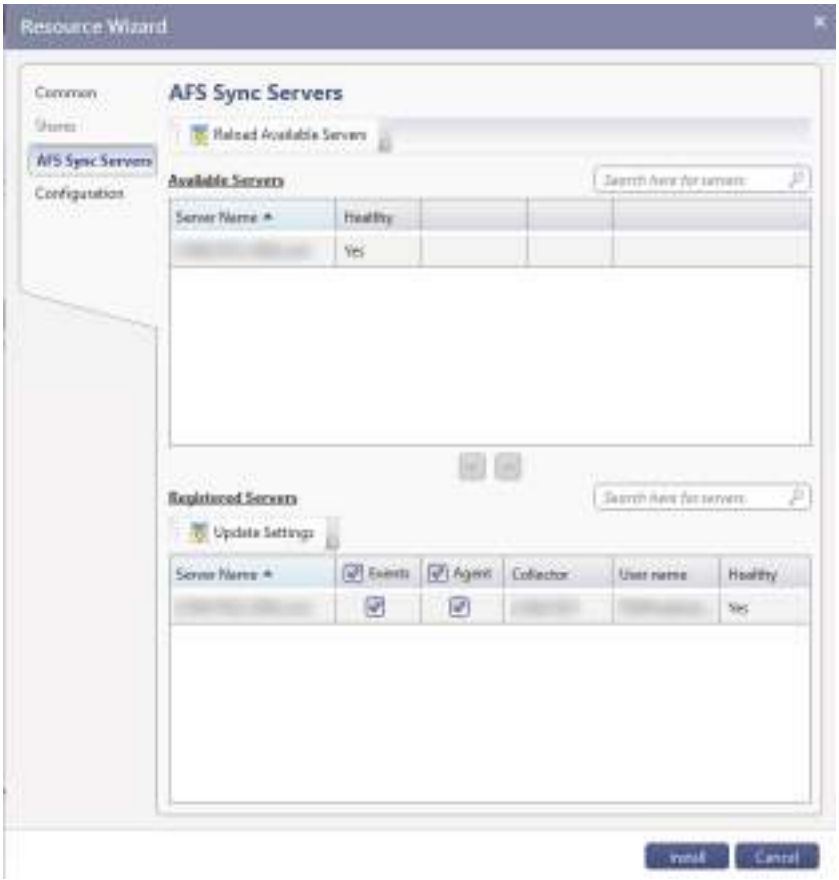
installed data source and select the shares. For more information, see Post-installation share detection and registration.

Proceed to register the Azure Files Sync servers to be monitored.

2. Register the Azure File Sync servers

Register the Azure Files Sync servers to be monitored for event auditing and localaccount enumeration.

1. On the left menu, click AFS Sync Servers.
   The AFS Sync server settings are displayed.



2. In the Available Servers area, select the required servers and click the down arrow.

The AFS Sync Servers dialog box is displayed.



Specify the Collector and credentials for the AFS Sync server. You can select the same Collector or a different one than that which you selected previously when configuring the AFS sync server in the Common pane.

Click OK when done.

The selected server is moved to the Registered Servers area. (The registered servers list is empty until you make your selection.)

You can add additional AFS Sync servers. When you add each server, you'll be prompted to specify the Collector and credentials for accessing the AFS Sync server. You can use the same Collector for all AFS Sync servers or different Collectors for each server.

3. For each server, review and set the following information as required:
   - Events - Select this checkbox to audit events for the server.

     Note: You can also right-click the grid and select the required options for event auditing.

   - Agent - Select the checkbox so the agent for the local events in the Azure Files Sync server will be installed by Varonis during the data source deployment process. If you clear this checkbox, you will need to manually install the agent.
4. (Optional) Click Update Settings if you want to change the Collector or credentials for auditing the events or local accounts.
5. You can repeat the above steps to add additional AFS Sync servers.
   Once the above settings are configured, you can proceed to review and adjust configuration settings.

3. Review and adjust configuration settings

1. On the left menu, click Configuration and confirm the information.
   The general configuration settings are displayed.

2. In the Local Accounts area, review the options:
   - Collect information regarding local accounts from this file server - Select this checkbox (if it not already selected) to collect user accounts from this file system.
3. In the Event Auditing Parameters area, review the options:
   - Filter out false "File Opened" events - Select this checkbox to filter out false File Open events and collect File Open events only if enough file content is read. Small files and certain operations may still trigger Read events.
   - Collect Access Denied events - Select this checkbox to collect events in which an attempt was made to access an entity by a user with insufficient credentials.

4. (Optional) Customize commit credentials

You can use different commit credentials instead of the default FileWalk credentials.

1. On the left menu, select Commit.
   The commit settings are displayed.
2. (Optional) Clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials. (By default, this checkbox is selected to use the FileWalk credentials, and the User name and Password fields are disabled for editing.)

   Note:
   - If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
   - If the Collector is in a lower version than 8, the FileWalk credentials will be used.

5. Install the data source

After configuration is complete, click Install to install the data source.

Note: When you install the data source, the Varonis agent is installed on the Azure File Sync server if the Agent checkbox in the Registered Servers area was selected in the AFS Sync Servers pane.

A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the File Servers pane. When the installation completes, the status shows "Installed 100%".

6. Post-installation share detection and registration

After the data source installation and share detection are completed, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. The following procedure describes the manual registration and automatic share detection flows.

> Important: If after the data source is installed, share detection fails for any reason, the Share Detection Status column will remain "In Progress" until the issue is fixed, and share detection completes successfully at least once.

After the data source is installed, the Shares pane is enabled, and you can view the share settings.

1. On the left menu, click Shares.
   The share settings are displayed. The pane's heading indicates the option you selected when adding a data source.
2. In the Available Shares area, you can filter the shares based on the reason they are not registered for monitoring and easily identify the shares that can be added. The default filter is Accessible Shares. You can change the filter to see the rest of the shares. Options include:
   - Accessible shares - Can be added for monitoring (this option is selected by default)
   - Ignored shares - Are marked as "ignored"
   - Incompatible and inaccessible shares - Cannot be monitored since the exposed protocol does not match the security style of the volume (relevant to multiprotocol platforms only) or the Varonis service account does not have access to this share
   - Child share of a monitored share - Is monitored via its parent folder
3. Do one of the following:
   - If you chose to monitor selected shares, in the Available Shares area, select the required shares and click the down arrow. The selected shares are moved to the Registered Shares area. (The registered shares list is empty until you make your selections.)
   - If you chose to automatically monitor detected shares, Varonis will monitor all shares that aren't marked as "ignored". The automated share detection runs every few hours. The Registered Shares area is autopopulated with the shares to be monitored.
4. For each share, review and set the following information as required:

- Ignore Detection - Select the shares to be ignored (and not be the subject of automatic detection and notifications) by the data source monitor.
- Events - Select this checkbox to audit events for the share.
- Crawl - To enable or disable monitoring for the share, in the Crawl column, select the relevant option.

  Note: You can also right-click the grid and select the required options for event auditing and crawling.

5. In the Additional Share Settings area, review the options:
   - Remove deleted shares - Select this checkbox to remove deleted shares. Shares that were deleted from the data source will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the data source is unavailable, the shares will not be removed.
   - Enable event auditing - Select this checkbox to audit events from all shares added from this data source.

   After share detection and registration are completed, the status and number of registered volumes are respectively displayed in the Share Detection Status and Registered Shares columns in the File Servers pane.

What To Do Next

Now let's take a look at the supported events for the monitored Azure Files data sources.

Manual Installation Using an Existing Azure Application

You can use existing an Entra ID application for monitoring Azure Files. You'll need to add a certificate and assign the “user_impersonation” delegated permission to the Entra ID domain application.

1. Add a certificate

1. Click Certificates & secrets to add a certificate.
   You can use a purchased certificate signed by a certificate authority (recommended) or create a self-signed certificate.
   For certificate authentication, Entra ID requires the following:
   - Certificates in X.509 V3 format for client and server authentication.
   - A key length of 2048 bits.
   - Key usage digital signature and key encipherment.

- The RSA cryptographic algorithm.
- Certificates signed with the SHA256 hash algorithm.
- The CN (subject), issuer, and validity period fields should be set.

> Note: Certificates exported without a private key in the CER or PEM file should be uploaded to the App registrations screen in Entra ID. Certificates with a password-encrypted private key in PFX format should be uploaded to the Collector when adding a file server (including the password of the PFX file).

To purchase a certificate signed by a certificate authority, see this example.
To create a self-signed certificate, follow these steps:

> Note: The following PowerShell commands are compatible with PowerShell 5.1 and Windows Server 2016. For older Windows Server versions, see Microsoft documentation.

a. Open Windows PowerShell Integrated Scripting Environment (ISE) as an administrator.

b. Run the following commands:

> Important: When copying the following PowerShell commands from this document, line breaks may be mistakenly added. Make sure to remove the line breaks, so that each command line resides on a single line. Otherwise, the commands may fail.

```
$notAfter = (Get-Date).AddMonths(24) # Valid for 24 mon
ths
```

```
$cer = \Qi0 VipjVmkrihEivxm gate -Subject "CN=MyService
" -Provider "Microsoft Enhanced RSA and AES Cryptograph
ic Provider" -CertStoreLocation "cert:\LocalMachine\My"
 -KeyExportPolicy Exportable -NotAfter $notAfter -KeyLe
ngth 2048 -HashAlgorithm SHA256)
```

```
G1tsvx Eivxm gate -Type CERT -FilePath c:\cert5.cer -Ce
rt $cer
```

```
$mypwd = ConvertTo-SecureString -String "1234" -Force -
AsPlainText
```

```
G1tsvx Sj1Eivxm gate -FilePath c:\cert5.pfx -Password $
mypwd -Cert $cer
```

c. Configure the script as follows:
   - In the first command line, set the expiration time of the certificate.
   - In the second command line, the certificate is created.
   - In the third command line, set the path to which to export the certificate CER file. This file will be uploaded later to Entra ID as part of the Entra ID application creation.
   - In the fourth command line, set the password for encrypting the certificate PFX file.
   - In the fifth command line, set the path to which to export the certificate PFX file. This file will be uploaded later to the Management Console.

2. When you have an available certificate, select the Certificates tab and click Upload certificate.
3. Select the certificate CER file, click Open and then click Add.
   The certificate is displayed in the Certificates tab.

2. Add user_impersonation permissions

For manual installation using an existing Azure application, make sure that the Entra ID domain application has the “user_impersonation” delegated permission assigned.

1. Go to the Microsoft Entra admin center.
2. Log in using an account with permissions to create applications in Entra ID.
3. Go to entra.microsoft.com > Identity > Applications > App registrations and select the relevant application.
   Follow these steps to create a new application:
   a. Select New registration. The Register an application page is displayed.
   b. Configure the application as follows:
      - In the Name field, set a name for this application.
      - In the Supported account types section, select Accounts in this organizational directory only (… Single tenant).
   c. Click Register. The application is created, and the application configuration page is displayed.
   d. Copy and save the Application (client) ID (the application ID) value for later use.

> Note: The application ID is required when adding the Entra ID application to the data source in the Management Console.

4. Click API permissions to set up permissions for the application.
   The API permissions page is displayed.
5. Click Add a permission.
   The Request API permissions page is displayed.
6. Select Azure Service Management.
7. Select user_impersonation.
8. Click Add.
9. Assign the application a Reader role under the subscription you want to monitor.
10. If you want Varonis to configure the File Diagnostic settings automatically, you need to assign the application a Contributor role under the subscription you want to monitor. For the role assignment steps, click here.

    > Note: If you would like to configure everything manually by yourself, you should assign a Reader role instead of Contributor. The same steps apply.

11. If you wish to monitor direct access events and monitor them using the application, you need to assign the Azure Event Hubs Data Receiver role to the application under the subscription. For the role assignment steps, click here.

What To Do Next

> Remember: Now that you've added a certificate and assigned the "user_impersonation" delegated permission to the Entra ID application, you can proceed to add an Azure Files data source with the Use Existing Entra ID Application option in the Management Console.
> Have the following values ready from this procedure:
>
> - Application (client) ID
> - Certificate

Manually Configuring an Event Hub and File Diagnostic Setting for Event Auditing

You can use an existing event hub and file diagnostic settings for auditing events for Azure Files. Follow the instructions below to create a new event hub and file diagnostic settings if they are not already in place.

Note: When creating an event hub manually, it is required to have 4 partitions.

1. Create an event hub

An Event Hub namespace provides a unique scoping container, in which you create one or more event hubs.

During the installation, you select a subscription and resource group, then need to create the event hub under the selected resource group.

To create a namespace in your resource group using the Microsoft Azure portal:

1. Go to the Microsoft Azure portal.
2. Log in using an account with permissions to create applications in Entra ID.
3. Select Create a resource.
4. Select All services in the left menu, and under Analytics, select the star (*) next to Event Hubs. Confirm that Event Hubs is added to FAVORITES in the left menu.
5. Select Event Hubs under FAVORITES in the left menu and click Create.
6. In the Create namespace page, do the following:
   a. Select the Subscription in which you want to create the namespace.
   b. Select the Resource Group under which you will create the event hub.
   c. Enter a name for the Namespace. The system immediately checks to see if the name is available.
   d. Select a Location for the namespace.
   e. Choose Standard for the Pricing tier. To learn about differences between tiers, see the Quotas and limits, Event Hubs Premium, and Event Hubs Dedicated articles.
   f. Leave the Throughput Units (for standard tier) or processing units (for premium tier) settings as it is. To learn about throughput units or processing units, see Event Hubs scalability.
   g. Click Review + create at the bottom of the page.
   h. On the Review + Create page, review the settings, and select Create. Wait for the deployment to complete.
7. On the Deployment page, select Go to resource to navigate to the page for your namespace.

2. Create a file diagnostic setting

1. In the Microsoft Azure portal home page, select Storage Accounts, and select the storage account you want to monitor.
2. In your storage account page, under Monitoring, select Diagnostic settings in the left menu.
3. In the Diagnostics settings page, click file. The file diagnostic settings are displayed.
4. Click Add diagnostic setting.
5. Specify the Categories needed for file diagnostic settings:
   - StorageRead
   - StorageWrite
   - StorageDelete
6. Under Destination details, select the Stream to an event hub checkbox.
   Once the event hub namespace is created, an event hub is created automatically. The Event hub namespace and Event hub name are displayed for your storage account.

What To Do Next

Remember: To add an Azure Files data source with the Use existing file diagnostic setting option in the Management Console, have the following values ready from this procedure:

- Event hub namespace
- Event hub name

Supported Events For Azure Files Data Sources

SMB (CIFS) Events for Azure Files Data Sources

The monitored data sources and NAS devices support various SMB (CIFS) events.

Event Auditing Method

N/A

Supported File Operations

- File created
- File deleted
- File modified
- File opened
- File renamed
- Folder created
- Folder deleted
- Folder renamed
- File permissions changed
- Folder permissions changed
- Owner changed

Access Denied Events:

- File access denied
- Folder access denied

> Note: All CIFS access denied events will arrive as File open denied events.

Limitations

- When users or apps access Azure Files directly to perform permission changes, respective events are not logged in the Azure Storage Log (Microsoft limitation). Therefore, Varonis does not monitor permission change events if the permissions were performed via direct access.

10 HITACHI NAS DATA SOURCES

What This Section Contains

This section describes how to deploy and monitor Hitachi NAS data sources; the requirements, deployment and configuration steps, and supported events.

Before You Begin

Make sure you've added a certificate for the Collector used for monitoring this data source. For instructions, click here.

What To Do Next

Before you dive in, click here to learn more about how Varonis monitors Hitachi NAS accounts, file system, and events.

Hitachi NAS Monitoring Overview

Note: Each Hitachi NAS data source represents a monitored Hitachi NAS server. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source.

About Hitachi NAS

- Hitachi NAS is a network attached storage (NAS) device with outstanding read/write speeds. It uses a virtualization technique to support multiple data sources, with multiple operating systems on the same physical device.
- Each physical Hitachi NAS machine houses multiple Enterprise Virtual Servers (EVS), which are host to multiple (virtual) data sources. The data sources can be CIFS-based.
- Each (virtual) data source has its own IP address, through which it is contacted directly. This means the data sources can be treated as single, independent units, so each IP will be listed as if it resided on a separate machine.
- Each (virtual) data source has its own shares, with data distributed among them. There are no "drives" or "administrative" ($) shares.

Varonis monitors Hitachi NAS via the following parallel data streams.

File System

- Varonis collects folder structure, permissions, and metadata via a dedicated service for directory structure monitoring (FileWalk) that runs on the assigned Collector. This connection is made over SMB.

Data Classification and Labeling

- Varonis supports data classification and labeling on files that reside in the monitored data sources.

Events

- Varonis monitors Hitachi NAS events using a dedicated event auditing service (Forwarder) that runs on the Collector.

What To Do Next

First, make sure you fulfill the Hitachi NAS requirements.

Hitachi NAS Requirements

Varonis Service Account

Varonis requires a dedicated service account. The service account can be reused for multiple data source installations and configurations.

- Service Account Read Operations:
  - Traverse and enumerate files, folders, directory structures, users, and groups.
  - Gather data source, user, and group metadata as part of normal system operations.
- Service Account Write Operations:
  - Used for executing Varonis Policies, if policies are defined.

Note:

- Local accounts are not supported on Hitachi NAS.
- IP Resolving is not supported.

Varonis Installation and Requirements

- Auditing must be enabled on the Hitachi NAS server (this can be done through the HDS server console).

Requirements for the Varonis Service Account for Read Operations

- A regular domain user is required with sufficient permissions to view the file system log.
- For the Varonis service account - either a member of the administrators local group and/or a user with Backup Operator privileges is required, both of those local groups on the Hitachi NAS server.

Requirements for the Varonis Service Account for Write Operations

In addition to the requirements for the read operations, the Varonis service account for write operations requires the Backup Operator role.

What To Do Next

Now that you've fulfilled the requirements, proceed to configure event auditing.

Configuring Event Auditing for Hitachi NAS

Prior to adding Hitachi NAS data sources, configure event auditing.

1. Open a browser and enter the Hitachi NAS Manager's IP address in the address bar.
   The NAS Manager window is displayed.
2. Authenticate with the credentials to log in. You need to have an administrator role on the device.
3. Click File Services.
4. On the File Services screen, click Enable File Services in the File Service Protocols section.
5. On the Enable File Services screen, verify the CIFS/Windows service is selected.
6. On the File Services screen, click File System Security in the File Service Protocols section.
   The File System Security screen is displayed.
7. Select the relevant EVS Security Context.
8. Verify the default file system security mode is Mixed (Windows and Unix) for all monitored virtual file systems (EVS). If it's not, click Switch Mode link and set to Mixed (Windows and Unix) for all monitored virtual file systems (EVS).
9. Enable auditing on the EVS:
   a. On the File Services page, click File System Audit Policies in the CIFS & NFS section.
      The File System Audit Policies screen is displayed.
   b. Select the relevant EVS/file system.
   c. In the Audit Log Consolidated Cache section, check whether cache is enabled. If it's not, click Modify and enable it.
   d. Click Add.
      The Add File System Audit Policy window is displayed.

e. In the Access via Unsupported Protocols section, select Allow Access (without auditing).

f. In the Audit Log section, set the maximum log file size to a value of at least 8MB (it is recommended to set it to 16MB).

g. In the Log roll over policy section, select the preferred option, either New or Wrap. Wrap is recommended.

10. Click OK to close.
A confirmation message indicates that the new audit policy is successfully saved.

What To Do Next

Now proceed to configure Hitachi NAS shares for Windows.

Configuring Hitachi NAS Shares for Windows

Hitachi NAS file shares can be configured for Windows.

1. On the Windows computer, select Start > Computer.
2. Right-click Computer and select Manage.
The Computer Management window is displayed.
3. In the right panel, select More Actions > Connect to another computer.
4. In the Select Computer dialog box, enter the IP address of the Hitachi NAS machine and then enter the required credentials.
5. In the Computer Management window, expand the tree: Computer Management > System Tools > Shared Folders > Shares.
The Hitachi NAS virtual file systems are listed.
6. Right-click the relevant share (that is, the virtual file system) and select Properties.
The Properties dialog box is displayed.
7. On the Security tab, click Advanced.
The Advanced Security Settings dialog box is displayed.
8. Select the Auditing tab.
9. Click Add or Edit to select the users and groups to be audited. It is recommended to select the Everyone group.

> Note: This guide assumes all users and groups are audited for all events. To avoid unnecessary overhead, it is possible to limit specific users, groups, and file system objects, and restrict the set of events which cause an audit event to be logged. The warning message The current Audit Policy for this computer does not have auditing turned on is expected.

10. Select the Full control option for Successful (i.e., permissions allowed).
11. Click OK to close.

What To Do Next

Now that you've configured the Hitachi NAS shares for Windows, it's time to add a monitored Hitachi NAS data source. First familiarize yourself with the deployment steps summary and then dive into the detailed procedure.

Adding a Hitachi NAS Data Source - Summary

Now that you've configured the Hitachi NAS event auditing and shares for Windows, you can deploy a Hitachi NAS data source. This section summarizes the procedure for deploying Hitachi NAS data sources.

1. Run the Management Console as an administrator.
2. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.
3. In the Resource Wizard's Common pane, specify the data source name, check the Collector selected by default and change it if needed, and enter the credentials for running directory structure monitoring (FileWalk).

   Important: You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.

4. In the Resource Type area, select the data source type from the dropdown list. Then, click the Connect and verify link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

   Note:

   - The Connect and verify link is displayed only when all relevant data is entered.
   - A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

5. In the Monitored Shares area, select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data

source installation is completed, and share selection is only available after the data source is installed and share detection is completed.

6. In the Configuration pane, review the FileWalk Settings and Event Auditing Parameters setting.
7. (Optional) In the Commit pane, clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials.

   Note:
   - If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
   - If the Collector is in a lower version than 8, the FileWalk credentials will be used.

   In the Group OU area, if required, select Uniquely defined to choose a different OU from that defined in the data source's domain.
8. After configuration is complete, click Install to add the data source.
9. After the data source installation and share detection are completed, in the Shares pane, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. If you chose to monitor selected shares, you can select and register the required shares.

What To Do Next

Now that you're familiar with the deployment steps, it's time to dive into the detailed procedure.

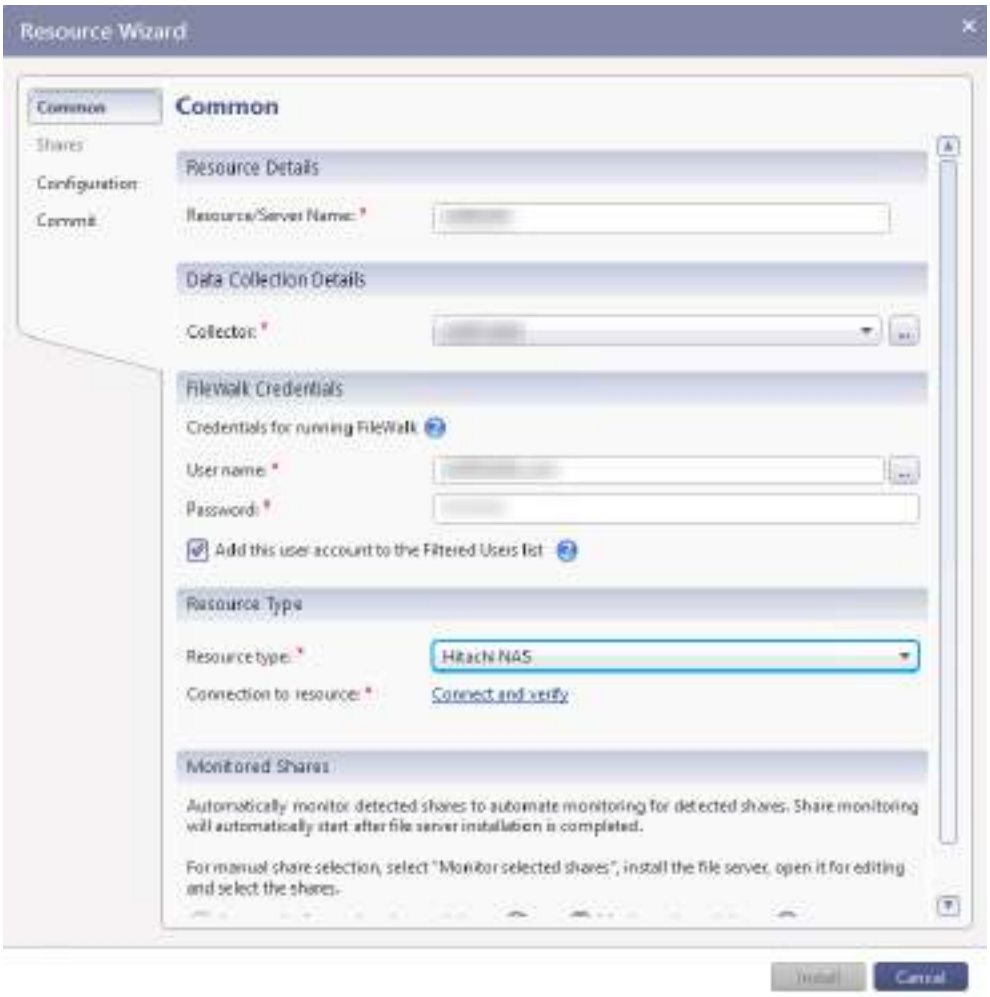
Adding a Hitachi NAS Data Source - Detailed Procedure

Now that you've configured the Hitachi NAS event auditing and shares for Windows, you can deploy a Hitachi NAS data source.

Note: Each Hitachi NAS data source represents a monitored Hitachi NAS Server. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source. To monitor multiple Hitachi NAS servers, add a Hitachi NAS data source per Hitachi NAS server.

1. Set common data source parameters

1. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.
   The Resource Wizard is opened to the Common pane, where you can specify the data source and set the relevant parameters.



2. In the Common pane, set the following parameters:
   a. Resource Details - Specify the data source name.
   b. Data Collection Details - Select the relevant Collector (assigned with a certificate) from the dropdown list. For instructions on adding a certificate for a Collector, click here.
   c. FileWalk Credentials - Enter the credentials for running directory structure monitoring. File System operations include directory structure monitoring, event auditing (if set).

   > Note: These credentials are cached, so that they are automatically entered if another data source is added during the same session.

- User name - Type the name of the user account to be used for directory structure monitoring, event auditing, and local account enumeration.
- Password - Type the account's password.
- Add this user account to the Filtered Users list - The defined user for FileWalk Credentials will be added to the filtered users list. If you clear this checkbox, a large number of events may be generated by the user defined for directory structure monitoring. It is recommended to keep this checkbox enabled.

Important: You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.

d. Resource Type - Select the data source type from the dropdown list.
   - Connect and verify - Click this link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

     Note:
     - The Connect and verify link is displayed only when all relevant data is entered.
     - A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

e. Monitored Shares - Select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source installed and share detection is completed.
   - Automatically monitor detected shares - Select this option to automate monitoring for all detected shares. Share monitoring will automatically start after the data source installation is completed. Varonis will monitor all shares that aren't marked as "ignored". When this option is selected, click the Advanced setting link to modify share detection preferences. By default, the option is set to Prefer regular shares over equivalent admin shares. In this case, an admin share that has an equivalent regular share will be marked as "ignored" and the equivalent regular share will be detected for monitoring. Note: Any change in the monitored shares configuration, including the detection method, admin shares configuration, and selected shares, requires rerunning the resource detection.

- Monitor selected shares - This option is selected by default. You can manually select the shares to be monitored only after the data source is installed and share detection is completed. You'll need to open the Edit window for the installed data source and select the shares. For more information, see Post-installation share detection and registration.

Once the above settings are configured, you can proceed to review and adjust configuration settings.

2. Review and adjust configuration settings

1. On the left menu, click Configuration and confirm the information.
   The general configuration settings are displayed.
2. In the FileWalk Settings area, review the options:
   - Identify actual unique folders and file system inconsistencies - Select this checkbox (if it not already selected) to detect broken permissions in NTFS file systems.
3. In the Event Auditing Parameters area, review the options:
   - Collect Access Denied event - Select this checkbox to collect events in which an attempt was made to access an entity by a user with insufficient credentials. Access Denied events must be enabled on the Hitachi NAS auditing system

3. (Optional) Customize commit credentials

You can use different commit credentials instead of the default FileWalk credentials.

1. On the left menu, select Commit.
   The commit settings are displayed.
2. (Optional) Clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials. (By default, this checkbox is selected to use the FileWalk credentials, and the User name and Password fields are disabled for editing.)

   Note:
   - If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
   - If the Collector is in a lower version than 8, the FileWalk credentials will be used.

3. In the Group OU area, if required, select Uniquely defined to choose a different OU from that defined in the data source's domain. Click the Browse button (...) to select the required OU.

4. Install the data source

After configuration is complete, click Install to install the data source.

A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the File Servers pane. When the installation completes, the status shows "Installed 100%".

5. Post-installation share detection and registration

After the data source installation and share detection are completed, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. The following procedure describes the manual registration and automatic share detection flows.

> Important: If after the data source is installed, share detection fails for any reason, the Share Detection Status column will remain "In Progress" until the issue is fixed, and share detection completes successfully at least once.

After the data source is installed, the Shares pane is enabled, and you can view the share settings.

1. On the left menu, click Shares.
   The share settings are displayed. The pane's heading indicates the option you selected when adding a data source.
2. In the Available Shares area, you can filter the shares based on the reason they are not registered for monitoring and easily identify the shares that can be added. The default filter is Accessible Shares. You can change the filter to see the rest of the shares. Options include:
   - Accessible shares - Can be added for monitoring (this option is selected by default)
   - Ignored shares - Are marked as "ignored"
   - Incompatible and inaccessible shares - Cannot be monitored since the exposed protocol does not match the security style of the volume (relevant to multiprotocol platforms only) or the Varonis service account does not have access to this share
   - Child share of a monitored share - Is monitored via its parent folder

3. Do one of the following:
   - If you chose to monitor selected shares, in the Available Shares area, select the required shares and click the down arrow. The selected shares are moved to the Registered Shares area. (The registered shares list is empty until you make your selections.)
   - If you chose to automatically monitor detected shares, Varonis will monitor all shares that aren't marked as "ignored". The automated share detection runs every few hours. The Registered Shares area is autopopulated with the shares to be monitored.
4. For each share, review and set the following information as required:
   - Ignore Detection - Select the shares to be ignored (and not be the subject of automatic detection and notifications) by the data source monitor.
   - Events - Select this checkbox to audit events for the share.
   - Crawl - To enable or disable monitoring for the share, in the Crawl column, select the relevant option.

     Note: You can also right-click the grid and select the required options for event auditing and crawling.
5. In the Additional Share Settings area, review the options:
   - Remove deleted shares - Select this checkbox to remove deleted shares. Shares that were deleted from the data source will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the data source is unavailable, the shares will not be removed.
   - Enable event auditing - Select this checkbox to audit events from all shares added from this data source.

   After share detection and registration are completed, the status and number of registered volumes are respectively displayed in the Share Detection Status and Registered Shares columns in the File Servers pane.

What To Do Next

Now let's take a look at the supported events for the monitored Hitachi NAS data sources.

Supported Events For Hitachi NAS Data Sources

SMB (CIFS) Events for Hitachi NAS Data Sources

The monitored data sources and NAS devices support various SMB (CIFS) events.

Note: SMB v2 and v3 are supported.

Event Auditing Method

File System (FS) Audit Log

Supported File Operations

- File created
- File deleted
- File modified
- File opened
- File renamed
- Folder created
- Folder deleted
- Folder renamed
- File permissions changed
- Folder permissions changed
- Owner changed

Access Denied Events:

- File created
- File deleted
- File modified
- File opened
- File permissions changed
- Folder access denied (Hitachi NAS only)
- Folder created
- Folder permissions changed

Note: Access Denied events are not supported for Hitachi NAS version 14.x.

11 NASUNI DATA SOURCES

What This Section Contains

This section describes how to deploy and monitor Nasuni data sources; the requirements, deployment and configuration steps, and supported events.

Before You Begin

Make sure you've added a certificate for the Collector used for monitoring this data source. For instructions, click here.

What To Do Next

Before you dive in, click here to learn more about how Varonis monitors Nasuni accounts, file system, and events.

Nasuni Monitoring Overview

Note: Each Nasuni data source represents a monitored Nasuni server. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source.

Varonis monitors Nasuni via the following parallel data streams.

Accounts

- Varonis enumerates local account information remotely from the Collector with a dedicated service account.

File System

- Varonis collects folder structure, permissions, and metadata via a dedicated service for directory structure monitoring (FileWalk) that runs on the assigned Collector. This connection is made over SMB.

Data Classification and Labeling

- Varonis supports data classification and labeling on files that reside in the monitored data sources.

Events

- Varonis monitors Nasuni events using a dedicated event auditing service (Forwarder) that runs on the Collector.

What To Do Next

First, make sure you fulfill the Nasuni requirements.

Nasuni Requirements

Varonis and Nasuni Best Practices

See Varonis and Nasuni best practices to ensure maximum performance.

Varonis Service Account

Varonis requires a dedicated service account. The service account can be reused for multiple data source installations and configurations.

- Service Account Read Operations:
  - Traverse and enumerate files, folders, directory structures, users, and groups.
  - Gather data source, user, and group metadata as part of normal system operations.
- Service Account Write Operations:
  - Used for executing Varonis Policies, if policies are defined.

Varonis Installation and Requirements

- If the Nasuni Edge Appliance is deployed on-premises, the Collector should be deployed on-premises. If the Nasuni Edge Appliance is deployed in the cloud, the Collector should be deployed in the cloud.
- It is recommended to use a dedicated Nasuni Edge Appliance pair per each different cloud region and not use a production appliance to ensure better performance, address GDPR concerns, and minimize egress fees by avoiding cross region traffic, which will be charged by the public cloud provider.
- In a multi-region environment that does not involve data sovereignty concerns and where cost takes precedence over scan duration, it is more cost-effective to use a single pair of Nasuni Edge Appliances and the Varonis Collector to scan multiple regions. Consider how much data will be scanned by Varonis, and thus how much data will traverse the cloud service provider's network. DatAdvantage involves the scanning of metadata; therefore, egress fees will almost always be less than the cost of deploying multiple VMs in each region. However, when Varonis Data Classification is used, significantly more data will be involved in each scan. The major cloud service providers offer cost calculators than can be used to determine the break-even point for data being scanned across regions versus the cost of deploying additional VMs.
- Event Auditing:
  - When sharing an existing volume with a new Nasuni file server, event auditing from this file server will start only after running the resource monitor. If you wish to expedite the process and not wait for the resource monitor, you need to edit and save the Nasuni file server through the Management Console. For more information, see Adding a Nasuni Data Source - Detailed Procedure.

  - When event auditing for shares is enabled in the Varonis Management Console, the events will not be logged in the Nasuni Management Console (NMC). Nasuni will audit events in the NMC for shares that are not monitored by Varonis.
- Snapshots are enabled by default on all Nasuni volumes and Edge Appliances so that the Data Security Platform can provide visibility and monitor the most updated file system structure. If disabled, the following may occur:
  - When snapshots are disabled on a particular Nasuni Edge Appliance for a particular volume, changes made to that volume via that Edge Appliance will not be detected by the other Nasuni Edge Appliances connected to the volume, and therefore cannot be crawled or monitored by the Data Security Platform.
  - When snapshots are disabled, new data written to that volume on that Edge Appliance will not be protected (by Nasuni).

  For more information about the snapshot process, see the Nasuni documentation, Nasuni Snapshot Processing.

Data Classification

- Data Classification configuration should be modified to run 30 I/O threads.
- Make sure that there is no outbound/inbound rate limit on the Nasuni Edge Appliances.
- To prevent directory structure monitoring performance issues while the Data Classification scan is running, the metadata for each volume will be pinned into the cache on environments with Varonis dedicated Edge appliances.

Network Architecture

Take the following into consideration when planning network architecture to assure connectivity between the relevant components:

- File system audit event traffic - Events are sent from the Nasuni Edge file servers (whether on-premises or on the cloud) to the Collector on the cloud through RabbitMQ.
- Scan traffic - Directory structure monitoring and Data Classification processes run from the Varonis Collector through the dedicated Nasuni Edge Appliance.
- Varonis traffic - The Collector requires connectivity to Varonis for sending data for analysis and processing.

- All events, folder and file metadata are transferred from the Collector to Varonis. Take into consideration any network, compliance, and regulation implications.
- The Nasuni Edge Appliance requires connectivity to Active Directory Domain Controllers, and the Collector requires access to Varonis. If these infrastructure resources are deployed solely on-premises, then a trusted network path must be created between the public cloud and your data centers. Alternatively, infrastructure resources that already exist in the public cloud can be used by the Nasuni Edge Appliance and the Collector.

Notes

- Directory structure monitoring and Data Classification scan performance are slower than on-premises due to cloud bandwidth and latency.
- Account Enumeration:
  - Nasuni Storage Groups are considered as Local Groups. Only Nasuni Native users which are members of Nasuni Storage groups are considered and collected as Local Users.
  - Membership of Native users is not brought into the Storage Groups.
- Only SMB (CIFS) shares are supported.
- Secure Hash Standard (SHS) is not supported.
- Nasuni is supported only for file servers that are joined to an Active Directory Domain. There is no support for LDAP.

What To Do Next

Now that you've fulfilled the requirements, proceed to configure the Varonis service account for Nasuni.

Configuring the Varonis Service Account for Nasuni

Before you add Nasuni data sources, you need to configure the Varonis service account.

Requirements for the Varonis Service Account for Read Operations

Note:

- The Varonis service account must be a domain user from the primary domain.

- The Varonis service account must be a Nasuni administrative user.

1. To configure the Varonis service account to be a Nasuni administrative user, do the following for each Edge appliance:
   a. In the Nasuni Edge Appliance user interface, click Configuration, and select General Settings from the list.
      The General CIFS Settings page is displayed.
   b. In the Administrative Users text box, add the Varonis service account. Insert a comma or semicolon to separate it from other users listed, as relevant.

      Note:
      - Use the Varonis service account name. Specifying a group is not supported.
      - Do not use the domain name.
      - For more information, see the official Nasuni Edge Appliance Administration Guide.
2. Open the Nasuni Management Console.
   The Nasuni Management Console main window is displayed.
3. Select Volumes.
   The Volumes window is displayed.
4. On the left, select Access Points > Shares.
   The Shares window is displayed.
5. For the volume that is shared with the Varonis dedicated Nasuni Edge, in the Actions column, click the Edit button.
   The Edit Share dialog box is displayed.
6. Scroll down to Advanced Settings, and note the following:
   The options available for each share vary according to the Authentication/Visibility choices.
   - In Authentication, if you select Authenticate Only Specified Groups and Users, to prevent Varonis service account operations from failing on that share, you must add the Varonis service account (or group that contains the Varonis service account) with Read-Only or Read-Write access and verify that the Varonis service account does not have direct or indirect access denied permissions.
   - If you select the Hide Unreadable Files checkbox, only folders and files with Read permissions will be scanned/crawled for theVaronis service account. All

other files and folders are skipped without any warnings/errors on the event viewer, and there will not be any entries for these folders/files in the database nor in Varonis.

- If you do not select the Hide Unreadable Files checkbox, you will receive errors/warnings on folders without Read permissions for the Varonis service account, and Varonis service account operations will not continue scanning inside these folders.

  Note: There will be corresponding entries in the database for the objects that were not accessed.

7. Configure the relevant settings and click Update Share.

Requirements for the Varonis Service Account for Write Operations

Same as the Varonis service account for read operations.

What To Do Next

Now that you've configured the Varonis service account for Nasuni, proceed to configure the NMC user.

Configuring the NMC User

Before you add Nasuni data sources, you need to configure the Nasuni Management Console (NMC) user and associate it with a local group with particular access permissions.

1. Create a local Nasuni group with the necessary permissions. The Nasuni local group should have “User Interface Access" and the appropriate permissions to enable automatic file server configuration.
2. To create the group, do the following:
   a. Go to the Nasuni Management Console > Console Settings > USERS & SECURITY > Users/Groups.
   b. Click Manage Groups.
   c. Click Add Group.
   d. In Group Name, enter a group name.
   e. From Access Type, select User Interface Access.
   f. Set the following permissions:
      i. In the NMC API Permissions area, select Enable NMC API Access.

ii. In the Filer Permissions area, select both Manage Multi Site Settings/ Connections and Manage Volume Settings (Can't add/delete).

iii. In the Filer Access area, select the dedicated Varonis appliance and the checkboxes of each one of the Nasuni monitored Edge Filers, or alternatively, select Manage All Filers (super user) to select all of the Nasuni filers.

iv. Click Add Group.

3. Associate the NMC selected user with the group created in step 1 above. The NMC user should be a native Nasuni user or a domain user which is a member of the above Nasuni local group. Do one of the following:
   - Create or use an existing domain/native Nasuni user and add it to the group created in step 1 above.
   - Associate the group created in step 1 above with a domain group. Use a domain user that is a direct or indirect member of this domain group.

What To Do Next

Now that you've configured the NMC user, it's time to add a monitored Nasuni data source. First familiarize yourself with the deployment steps summary and then dive into the detailed procedure.

Adding a Nasuni Data Source - Summary

Now that you've configured the NMC user, you can deploy a Nasuni data source. This section summarizes the procedure for deploying Nasuni data sources.

1. Run the Management Console as an administrator.
2. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.
3. In the Resource Wizard's Common pane, specify the data source name, check the Collector selected by default and change it if needed, and enter the credentials for running directory structure monitoring (FileWalk).

   Important:
   - The "Filer Description" in the Nasuni Management Console must match the filer Hostname.
   - Make sure a Collector that's assigned with a certificate is selected. For instructions on adding a certificate for a Collector, click here.

- You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.

4. In the Resource Type area, select the data source type from the dropdown list. Then, click the Connect and verify link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

   Note:
   - The Connect and verify link is displayed only when all relevant data is entered.
   - A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

5. In the Nasuni Management Console API Access Settings area, enter the NMC Host and user credentials required to access the Nasuni Management Console (NMC) API, retrieve information about the file system, and audit events. Then, click the Connect and verify link to validate the NMC credentials, retrieve the dedicated data source version, and enable adding the data source to the Management Console.

   Note: For additional requirements, see Configuring the NMC User.

6. In the Monitored Shares area, select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source is installed and share detection is completed.
7. In the Configuration pane, review the Local Accounts settings and FileWalk Settings.
8. (Optional) In the Commit pane, clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials.

   Note:
   - If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
   - If the Collector is in a lower version than 8, the FileWalk credentials will be used.

In the Group OU area, if required, select Uniquely defined to choose a different OU from that defined in the data source's domain.

9. After configuration is complete, click Install to add the data source.
10. After the data source installation and share detection are completed, in the Shares pane, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. If you chose to monitor selected shares, you can select and register the required shares.

What To Do Next

Now that you're familiar with the deployment steps, it's time to dive into the detailed procedure.

Adding a Nasuni Data Source - Detailed Procedure

Now that you've configured the NMC user, you can deploy a Nasuni data source.

> Note: Each Nasuni data source represents a monitored Nasuni Server. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source. To monitor multiple Nasuni servers, add a Nasuni data source per Nasuni server.

1. Set common data source parameters

1. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.

The Resource Wizard is opened to the Common pane, where you can specify the data source and set the relevant parameters.



2. In the Common pane, set the following parameters:
   a. Resource Details - Specify the data source name. The "Filer Description" in the Nasuni Management Console must match the filer Hostname.
   b. Data Collection Details - Select the relevant Collector (assigned with a certificate) from the dropdown list. For instructions on adding a certificate for a Collector, click here.
   c. FileWalk Credentials - Enter the credentials for running directory structure monitoring. File System operations include directory structure monitoring, event auditing (if set) and account enumeration on local accounts (if set).

      Note: These credentials are cached, so that they are automatically entered if another data source is added during the same session.

- User name - Type the name of the user account to be used for directory structure monitoring, event auditing, and local account enumeration.
- Password - Type the account's password.
- Add this user account to the Filtered Users list - The defined user for FileWalk Credentials will be added to the filtered users list. If you clear this checkbox, a large number of events may be generated by the user defined for directory structure monitoring. It is recommended to keep this checkbox enabled.

Important: You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.

d. Resource Type - Select the data source type from the dropdown list.
   - Connect and verify - Click this link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

     Note:
     - The Connect and verify link is displayed only when all relevant data is entered.
     - A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

e. Nasuni Management Console API Access Settings - Enter the following credentials required to access the Nasuni Management Console (NMC) API, retrieve information about the file system and audit events:
   - NMC host name
   - NMC user name
   - NMC password
   - Connect and verify – Click this link to validate the NMC credentials, retrieve the dedicated data source version, and enable adding the data source to the Management Console.

     Note: For additional requirements, see Configuring the NMC User.

f. Monitored Shares - Select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source installed and share detection is completed.

- Automatically monitor detected shares - Select this option to automate monitoring for all detected shares. Share monitoring will automatically start after the data source installation is completed. Varonis will monitor all shares that aren't marked as "ignored". When this option is selected, click the Advanced setting link to modify share detection preferences. By default, the option is set to Prefer regular shares over equivalent admin shares. In this case, an admin share that has an equivalent regular share will be marked as "ignored" and the equivalent regular share will be detected for monitoring. Note: Any change in the monitored shares configuration, including the detection method, admin shares configuration, and selected shares, requires rerunning the resource detection.
- Monitor selected shares - This option is selected by default. You can manually select the shares to be monitored only after the data source is installed and share detection is completed. You'll need to open the Edit window for the installed data source and select the shares. For more information, see Post-installation share detection and registration.

Once the above settings are configured, you can proceed to review and adjust configuration settings.

2. Review and adjust configuration settings

1. On the left menu, click Configuration and confirm the information.
   The general configuration settings are displayed.
2. In the Local Accounts area, review the options:
   - Collect information regarding local accounts from this file server - Select this checkbox to collect user accounts from this file system.
3. In the FileWalk Settings area, review the options:
   - Identify actual unique folders and file system inconsistencies - Select this checkbox (if it not already selected) to detect broken permissions in NTFS file systems.

3. (Optional) Customize commit credentials

You can use different commit credentials instead of the default FileWalk credentials.

1. On the left menu, select Commit.
   The commit settings are displayed.

2. (Optional) Clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials. (By default, this checkbox is selected to use the FileWalk credentials, and the User name and Password fields are disabled for editing.)

   Note:
   - If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
   - If the Collector is in a lower version than 8, the FileWalk credentials will be used.

3. In the Group OU area, if required, select Uniquely defined to choose a different OU from that defined in the data source's domain. Click the Browse button (...) to select the required OU.

4. Install the data source

After configuration is complete, click Install to install the data source.

A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the File Servers pane. When the installation completes, the status shows "Installed 100%".

5. Post-installation share detection and registration

After the data source installation and share detection are completed, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. The following procedure describes the manual registration and automatic share detection flows.

Important: If after the data source is installed, share detection fails for any reason, the Share Detection Status column will remain "In Progress" until the issue is fixed, and share detection completes successfully at least once.

After the data source is installed, the Shares pane is enabled, and you can view the share settings.

1. On the left menu, click Shares.
   The share settings are displayed. The pane's heading indicates the option you selected when adding a data source.

2. In the Available Shares area, you can filter the shares based on the reason they are not registered for monitoring and easily identify the shares that can be added. The default filter is Accessible Shares. You can change the filter to see the rest of the shares. Options include:
   - Accessible shares - Can be added for monitoring (this option is selected by default)
   - Ignored shares - Are marked as "ignored"
   - Incompatible and inaccessible shares - Cannot be monitored since the exposed protocol does not match the security style of the volume (relevant to multiprotocol platforms only) or the Varonis service account does not have access to this share
   - Child share of a monitored share - Is monitored via its parent folder
3. Do one of the following:
   - If you chose to monitor selected shares, in the Available Shares area, select the required shares and click the down arrow. The selected shares are moved to the Registered Shares area. (The registered shares list is empty until you make your selections.)
   - If you chose to automatically monitor detected shares, Varonis will monitor all shares that aren't marked as "ignored". The automated share detection runs every few hours. The Registered Shares area is autopopulated with the shares to be monitored.
4. For each share, review and set the following information as required:
   - Ignore Detection - Select the shares to be ignored (and not be the subject of automatic detection and notifications) by the data source monitor.
   - Events - Select this checkbox to audit events for the share.
   - Crawl - To enable or disable monitoring for the share, in the Crawl column, select the relevant option.

     Note: You can also right-click the grid and select the required options for event auditing and crawling.
5. In the Additional Share Settings area, review the options:
   - Remove deleted shares - Select this checkbox to remove deleted shares. Shares that were deleted from the data source will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the data source is unavailable, the shares will not be removed.
   - Enable event auditing - Select this checkbox to audit events from all shares added from this data source.

After share detection and registration are completed, the status and number of registered volumes are respectively displayed in the Share Detection Status and Registered Shares columns in the File Servers pane.

What To Do Next

Now let's take a look at the supported events for the monitored Nasuni data sources.

Supported Events For Nasuni Data Sources

SMB (CIFS) Events for Nasuni Data Sources

The monitored data sources and NAS devices support various SMB (CIFS) events.

> Note: SMB v2 and v3 are supported.

Event Auditing Method

Varonis API

Supported File Operations

- File created
- File deleted
- File modified
- File opened
- File renamed
- Folder created
- Folder deleted
- Folder renamed
- File permissions changed
- Folder permissions changed
- Owner changed

> Note: There are no Owner changed events when the new or old owner is "Everyone Group", or when the logged-on user changes the ownership to or from themselves.

12 PANZURA DATA SOURCES

What This Section Contains

This section describes how to deploy and monitor Panzura data sources; the requirements, deployment and configuration steps, and supported events.

Before You Begin

Make sure you've added a certificate for the Collector used for monitoring this data source. For instructions, click here.

What To Do Next

Before you dive in, click here to learn more about how Varonis monitors Panzura accounts, file system, and events.

Panzura Monitoring Overview

Note: Each Panzura data source represents a monitored Panzura server. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source.

Varonis monitors Panzura via the following parallel data streams.

Accounts

- Varonis enumerates local account information remotely from the Collector with a dedicated service account.

File System

- Varonis collects folder structure, permissions, and metadata via a dedicated service for directory structure monitoring (FileWalk) that runs on the assigned Collector. This connection is made over SMB.

Data Classification and Labeling

- Varonis supports data classification and labeling on files that reside in the monitored data sources.

Events

- Varonis monitors Panzura events using a dedicated event auditing service (Forwarder) that runs on the Collector.

What To Do Next

First, make sure you fulfill the Panzura requirements.

Panzura Requirements

Varonis Service Account

Varonis requires a dedicated service account. The service account can be reused for multiple data source installations and configurations.

- Service Account Read Operations:
  - Traverse and enumerate files, folders, directory structures, users, and groups.
  - Gather data source, user, and group metadata as part of normal system operations.
- Service Account Write Operations:
  - Used for executing Varonis Policies, if policies are defined.

Varonis Installation and Requirements

- A dedicated Panzura file server (that is, a Panzura Edge file server, Master or subordinate, that is dedicated only for Varonis) and a Varonis Collector should be deployed closest to the storage pool. If the storage pool is in the cloud, then both the dedicated file server and the Collector should be deployed in the cloud.
- The Varonis dedicated Panzura file server is the only Panzura Edge appliance that should be added to the Varonis Management Console.
- The monitored Panzura file servers (including the dedicated file server) should contain one Master file server and the others should be its subordinates for event collection purposes.
- The Varonis dedicated Panzura file server is used to crawl the global file system for metadata, and for Data Classification Engine also the data. Having a dedicated file server located closest to the storage pool effects the following:
  - Provides a single source of truth. The file system is scanned only using the dedicated file server. If each one of the Panzura user Edge appliances would be scanned separately, then the same items could potentially be scanned multiple times.
  - Avoids impact on the Panzura Edge appliance cache. The Data Classification Engine scan can trigger file rehydration only on the dedicated file server.
  - By deploying the Collector and dedicated file server in the cloud, the need for transferring the entire data set across a wide area network (WAN) to the Edge appliance is eliminated. This reduces the duration of scans and minimizes any egress fees charged by the cloud provider.

- The Master file server and the dedicated file server should be able to connect with the Collector server (Management Console) through port 443.
- For more information about Panzura licensing requirements, see the article Panzura Best Practices: Varonis.
- Panzura REST API credentials are required to add Panzura file servers to the Management Console. The REST API credentials are the same as the Panzura Web UI credentials.

Notes

- Only SMB (CIFS) shares are supported.
- The File Size parameter, by default, reflects the physical file size of the files scanned on Panzura file servers, and may not be accurate. This field can be changed to display the logical file size, which is always accurate. Contact Varonis Support for assistance.
- Panzura file servers do not support local users with storage access, but they do have some local groups that can have domain users as members.

What To Do Next

Now that you've fulfilled the requirements, proceed to configure the Varonis service account for Panzura.

Configuring the Varonis Service Account for Panzura

Before you add Panzura data sources, you need to configure the Varonis service account.

Requirements for the Varonis Service Account for Read Operations

Note:

- The Varonis service account must be a domain user.
- The Varonis service account must be a member of the local Panzura backup operator and power user groups.

1. Open the Computer Management Console (or the Microsoft Management Console). In the Windows search box on the taskbar, type "computer management" and click the appropriate search result.
   The Computer Management Console is displayed.
2. From the Action menu, select Connect to another computer.
   The Select Computer dialog box is displayed.
3. In the Another computer field, enter the Panzura file server name or IP address, and click OK.
4. After connecting to the Panzura data source, from the left pane of the Computer Management Console, go to System Tools > Local Users and Groups > Groups. Backup Operators and Power Users groups are listed among others.
5. To select the Varonis service account for the backup operator and power user groups, do the following:
   a. Right-click the relevant group, Backup Operators or Power Users, and select Properties.
      The group Properties dialog box is displayed.
   b. In the General tab, click the Add button.
      The Select Users, Computers, Service Accounts, or Groups dialog box is displayed.
   c. Select the Varonis service account, and click OK.
      The group Properties dialog box is displayed.
   d. Click Apply, then click OK.
   e. Repeat the above steps for the other group.

Requirements for the Varonis Service Account for Write Operations

Same as the Varonis service account for read operations.

What To Do Next

Now that you've configured the Varonis service account for Panzura, proceed to configure event auditing.

Configuring Event Auditing for Panzura

You need to install and activate the AS-Audit and AS-Varonis license modules on each Panzura Edge appliance (including the Master, subordinates, and the Varonis dedicated data source), so that they will be able to connect to the Collector and send events to RabbitMQ on the Collector. You'll also need to enable the Generate PDS Audit Log setting for all user actions so that the Panzura node will receive events.

1. Go to the Panzura Web UI of each monitored Panzura data source.
2. In the Panzura main window, click Configuration, and from the navigation pane, select License Manager.
   The License Manager window is displayed.
3. Click Installed License Modules at the top of the window.
4. Make sure that the AS-Audit and AS-Varonis licenses are activated. If they are inactive, select their checkboxes and click the Activate button.
5. Select the AS-Audit checkbox and click the Edit button.
   The Edit License window is displayed.
6. Select all events on all files and folders. Configure the Audit license with the following:
   - sysloghost: "-"
   - include files: "*"
   - exclude files: "-"
   - access: “create, open, mkdir, read, write, remove, rmdir, rename, close, setxattr, delxattr”
7. To allow the Panzura node to receive events, from the navigation pane, select Monitoring, toggle on Generate PDS Audit Log, and set User Actions to All. This can be configured per node in Panzura, or at the global level for all nodes.
8. Click the Done button to complete the configuration.

What To Do Next

Now that you've configured event auditing for Panzura, it's time to add a monitored Panzura data source. First familiarize yourself with the deployment steps summary and then dive into the detailed procedure.

Adding a Panzura Data Source - Summary

Now that you've configured the REST API Access user, you can deploy a Panzura data source. This section summarizes the procedure for deploying Panzura data sources.

1. Run the Management Console as an administrator.
2. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.

3. In the Resource Wizard's Common pane, specify the data source name, check the Collector selected by default and change it if needed, and enter the credentials for running directory structure monitoring (FileWalk).

   Important:

   - The Panzura dedicated file server can be either a Master file server or a subordinate.
   - Make sure a Collector that's assigned with a certificate is selected. For instructions on adding a certificate for a Collector, click here.
   - You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.

4. In the Resource Type area, select the data source type from the dropdown list. Then, click the Connect and verify link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

   Note:

   - The Connect and verify link is displayed only when all relevant data is entered.
   - A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

5. In the Panzura REST API Credentials area, enter the REST API credentials required to retrieve information about the file system and audit events. Then, click the Connect and verify link to validate the Panzura credentials, retrieve the dedicated data source version, and enable adding the data source to the Management Console.

   Note: The REST API credentials are the same as the Panzura Web UI credentials.

6. In the Monitored Shares area, select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source is installed and share detection is completed.
7. In the Configuration pane, review the FileWalk Settings and Event Auditing Parameters settings.

8. (Optional) In the Commit pane, clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials.

   Note:

   - If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
   - If the Collector is in a lower version than 8, the FileWalk credentials will be used.

   In the Group OU area, if required, select Uniquely defined to choose a different OU from that defined in the data source's domain.
9. After configuration is complete, click Install to add the data source.
10. After the data source installation and share detection are completed, in the Shares pane, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. If you chose to monitor selected shares, you can select and register the required shares.

What To Do Next

Now that you're familiar with the deployment steps, it's time to dive into the detailed procedure.

Adding a Panzura Data Source - Detailed Procedure

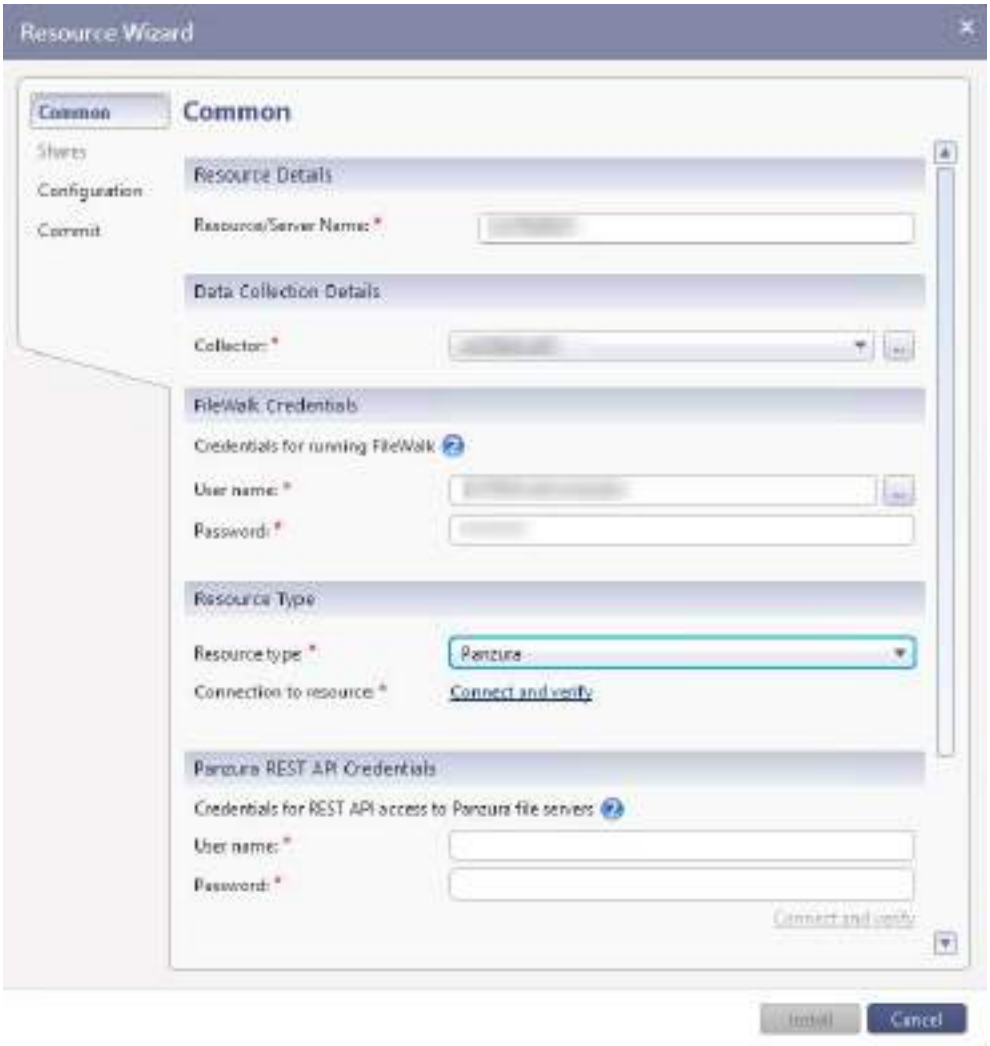
Now that you've configured the REST API Access user, you can deploy a Panzura data source.

Note: Each Panzura data source represents a monitored Panzura Server. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source. To monitor multiple Panzura servers, add a Panzura data source per Panzura server.

1. Set common data source parameters

1. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.

The Resource Wizard is opened to the Common pane, where you can specify the data source and set the relevant parameters.



2. In the Common pane, set the following parameters:
   a. Resource Details - Specify the data source name.

      Note: The Panzura dedicated file server can be either a Master file server or a subordinate.

   b. Data Collection Details - Select the relevant Collector (assigned with a certificate) from the dropdown list. For instructions on adding a certificate for a Collector, click here.

   c. FileWalk Credentials - Enter the credentials for running directory structure monitoring. File System operations include directory structure monitoring, event auditing (if set) and account enumeration on local accounts (if set).

      Note:

- These credentials are cached, so that they are automatically entered if another data source is added during the same session.

- User name - Type the name of the user account to be used for directory structure monitoring, event auditing, and local account enumeration.
- Password - Type the account's password.

Important: You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.

d. Resource Type - Select the data source type from the dropdown list.
   - Connect and verify - Click this link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

     Note:
     - The Connect and verify link is displayed only when all relevant data is entered.
     - A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

e. Panzura REST API Credentials - Enter the following credentials required to retrieve information about the file system and audit events:

   Note: The REST API credentials are the same as the Panzura Web UI credentials.

   - User name - Insert a REST API user name.
   - Password - Insert a REST API password.
   - Connect and verify – Click this link to validate the Panzura credentials, retrieve the dedicated data source version, and enable adding the data source to the Management Console.

f. Monitored Shares - Select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source installed and share detection is completed.
   - Automatically monitor detected shares - Select this option to automate monitoring for all detected shares. Share monitoring will automatically start

after the data source installation is completed. Varonis will monitor all shares that aren't marked as "ignored". When this option is selected, click the Advanced setting link to modify share detection preferences. By default, the option is set to Prefer regular shares over equivalent admin shares. In this case, an admin share that has an equivalent regular share will be marked as "ignored" and the equivalent regular share will be detected for monitoring. Note: Any change in the monitored shares configuration, including the detection method, admin shares configuration, and selected shares, requires rerunning the resource detection.

- Monitor selected shares - This option is selected by default. You can manually select the shares to be monitored only after the data source is installed and share detection is completed. You'll need to open the Edit window for the installed data source and select the shares. For more information, see Post-installation share detection and registration.

Once the above settings are configured, you can proceed to review and adjust configuration settings.

2. Review and adjust configuration settings

1. On the left menu, click Configuration and confirm the information.
   The general configuration settings are displayed.
2. In the FileWalk Settings area, review the options:
   - Identify actual unique folders and file system inconsistencies - Select this checkbox (if it not already selected) to detect broken permissions in NTFS file systems.
3. In the Event Auditing Parameters area, review the options:
   - Filter out false "File Opened" events - Select this checkbox to filter out false File Open events and collect File Open events only if enough file content is actually read. Small files and certain operations may still trigger Read events.

3. (Optional) Customize commit credentials

You can use different commit credentials instead of the default FileWalk credentials.

1. On the left menu, select Commit.
   The commit settings are displayed.
2. (Optional) Clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials. (By default, this checkbox is selected to use the

FileWalk credentials, and the User name and Password fields are disabled for editing.)

Note:

- If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
- If the Collector is in a lower version than 8, the FileWalk credentials will be used.

3. In the Group OU area, if required, select Uniquely defined to choose a different OU from that defined in the data source's domain. Click the Browse button (...) to select the required OU.

4. Install the data source

After configuration is complete, click Install to install the data source.

A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the File Servers pane. When the installation completes, the status shows "Installed 100%".

5. Post-installation share detection and registration

After the data source installation and share detection are completed, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. The following procedure describes the manual registration and automatic share detection flows.

Important: If after the data source is installed, share detection fails for any reason, the Share Detection Status column will remain "In Progress" until the issue is fixed, and share detection completes successfully at least once.

After the data source is installed, the Shares pane is enabled, and you can view the share settings.

1. On the left menu, click Shares.
   The share settings are displayed. The pane's heading indicates the option you selected when adding a data source.
2. In the Available Shares area, you can filter the shares based on the reason they are not registered for monitoring and easily identify the shares that can be added. The default filter is Accessible Shares. You can change the filter to see the rest of the shares. Options include:

- Accessible shares - Can be added for monitoring (this option is selected by default)
- Ignored shares - Are marked as "ignored"
- Incompatible and inaccessible shares - Cannot be monitored since the exposed protocol does not match the security style of the volume (relevant to multiprotocol platforms only) or the Varonis service account does not have access to this share
- Child share of a monitored share - Is monitored via its parent folder

3. Do one of the following:
   - If you chose to monitor selected shares, in the Available Shares area, select the required shares and click the down arrow. The selected shares are moved to the Registered Shares area. (The registered shares list is empty until you make your selections.)
   - If you chose to automatically monitor detected shares, Varonis will monitor all shares that aren't marked as "ignored". The automated share detection runs every few hours. The Registered Shares area is autopopulated with the shares to be monitored.
4. For each share, review and set the following information as required:
   - Ignore Detection - Select the shares to be ignored (and not be the subject of automatic detection and notifications) by the data source monitor.
   - Events - Select this checkbox to audit events for the share.
   - Crawl - To enable or disable monitoring for the share, in the Crawl column, select the relevant option.

     Note: You can also right-click the grid and select the required options for event auditing and crawling.
5. In the Additional Share Settings area, review the options:
   - Remove deleted shares - Select this checkbox to remove deleted shares. Shares that were deleted from the data source will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the data source is unavailable, the shares will not be removed.
   - Enable event auditing - Select this checkbox to audit events from all shares added from this data source.

   After share detection and registration are completed, the status and number of registered volumes are respectively displayed in the Share Detection Status and Registered Shares columns in the File Servers pane.

What To Do Next

Now let's take a look at the supported events for the monitored Panzura data sources.

Supported Events For Panzura Data Sources

SMB (CIFS) Events for Panzura Data Sources

The monitored data sources and NAS devices support various SMB (CIFS) events.

> Note: SMB v2 and v3 are supported.

Event Auditing Method

Panzura API

Supported File Operations

- File created
- File deleted
- File modified
- File opened
- File renamed
- File permissions changed
- File protection added
- File protection removed
- Folder created
- Folder deleted
- Folder renamed
- Folder permissions changed
- Folder protection added
- Folder protection removed
- Owner changed

> Note: Access Denied events are not supported.

13 NUTANIX DATA SOURCES

What This Section Contains

This section describes how to deploy and monitor Nutanix data sources; the requirements, deployment and configuration steps, and supported events.

Before You Begin

Make sure you've added a certificate for the Collector used for monitoring this data source. For instructions, click here.

What To Do Next

Before you dive in, click here to learn more about how Varonis monitors Nutanix accounts, file system, and events.

Nutanix Monitoring Overview

Note: Each Nutanix data source represents a monitored Nutanix server. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source.

Varonis monitors Nutanix via the following parallel data streams.

Accounts

- Varonis enumerates local account information remotely from the Collector with a dedicated service account.

File System

- Varonis collects folder structure, permissions, and metadata via a dedicated service for directory structure monitoring (FileWalk) that runs on the assigned Collector. This connection is made over SMB.

Data Classification and Labeling

- Varonis supports data classification and labeling on files that reside in the monitored data sources.

Events

- Varonis monitors Nutanix events using a dedicated event auditing service (Forwarder) that runs on the Collector.

What To Do Next

First, make sure you fulfill the Nutanix requirements.

Nutanix Requirements

Varonis Service Account

Varonis requires a dedicated service account. The service account can be reused for multiple data source installations and configurations.

- Service Account Read Operations:
  - Traverse and enumerate files, folders, directory structures, users, and groups.
  - Gather data source, user, and group metadata as part of normal system operations.
- Service Account Write Operations:
  - Used for executing Varonis Policies, if policies are defined.

Varonis Installation and Requirements

- The Varonis service account requires the role "Backup Admin: Backup access only" to read files and/or "File Server Admin: Full Access" to execute Varonis Policies.
- Nutanix REST API credentials are required to add Nutanix data sources to the Management Console.

Notes

- Varonis supports only Nutanix Acropolis File Services (AFS).
- Varonis does not support local Nutanix users and groups.
- Make sure you've added a certificate for the Collector used for monitoring this data source. For instructions, click here.

What To Do Next

Now that you've fulfilled the requirements, proceed to configure the Varonis service account for Nutanix.

Configuring the Varonis Service Account for Nutanix

Before you add Nutanix data sources, you need to configure the Varonis service account.

Requirements for the Varonis Service Account for Read Operations

Note:

- The Varonis service account must be a domain user from the primary domain.
- The Varonis service account should use the backup admin role for operations, and server admin role for applications that require the ability to perform changes.

You need to configure the Varonis service account with the Nutanix backup admin role or server admin role.

1. In the Nutanix Prism (UI management), from the main menu, select File Server, click the file server name, and click Manage Roles.
   The Manage Roles page is displayed.
2. In the Add admins area, click the New User button.
3. In the User field, enter the Varonis service account name.

   Note:
   - Use the Varonis service account name. Specifying a group is not supported.
   - Use the user's full name, including the domain name.
4. In the Role field, select Backup Admin: Backup access only or File Server Admin: Full access.

Requirements for the Varonis Service Account for Write Operations

Same as the Varonis service account for read operations.

What To Do Next

Now proceed to configure the Nutanix REST API user.

Configuring the Nutanix REST API Access User

Before you add Nutanix data sources, you need to configure the Nutanix Rest API access user.

1. In the Nutanix Prism (UI management), from the main menu, select File Server, click the file server name, and click Manage Roles.
   The Manage Roles page is displayed.
2. In the REST API access users area, click the New User button, and add the new user. Use only lowercase letters. (Uppercase and special characters including underscores (_) are NOT supported.)

   Note: This is not a domain user.

What To Do Next

Now that you've configured the Nutanix REST API access user, it's time to add a monitored Nutanix data source. First familiarize yourself with the deployment steps summary and then dive into the detailed procedure.

Adding a Nutanix Data Source - Summary

Now that you've configured the REST API Access user, you can deploy a Nutanix data source. This section summarizes the procedure for deploying Nutanix data sources.

1. Run the Management Console as an administrator.
2. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.
3. In the Resource Wizard's Common pane, specify the data source name, check the Collector selected by default and change it if needed, and enter the credentials for running directory structure monitoring (FileWalk).

   Important:

   - Make sure a Collector that's assigned with a certificate is selected. For instructions on adding a certificate for a Collector, click here.
   - You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.
4. In the Resource Type area, select the data source type from the dropdown list. Then, click the Connect and verify link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

   Note:

- The Connect and verify link is displayed only when all relevant data is entered.
- A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

5. In the Nutanix REST API Credentials area, - enter the REST API credentials required to retrieve information about the file system and audit events. Then, click the Connect and verify link to verify the credentials that were entered.

   Important: Make sure that the user name you entered in Nutanix Prism is only lowercase letters. Uppercase and special characters including underscores (_) are NOT supported.

6. In the Monitored Shares area, select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source is installed and share detection is completed.
7. In the Configuration pane, review the FileWalk Settings and Event Auditing Parameters.
8. (Optional) In the Commit pane, clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials.

   Note:

   - If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
   - If the Collector is in a lower version than 8, the FileWalk credentials will be used.

   In the Group OU area, if required, select Uniquely defined to choose a different OU from that defined in the data source's domain.
9. After configuration is complete, click Install to add the data source.
10. After the data source installation and share detection are completed, in the Shares pane, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. If you chose to monitor selected shares, you can select and register the required shares.

What To Do Next

Now that you're familiar with the deployment steps, it's time to dive into the detailed procedure.

Adding a Nutanix Data Source - Detailed Procedure

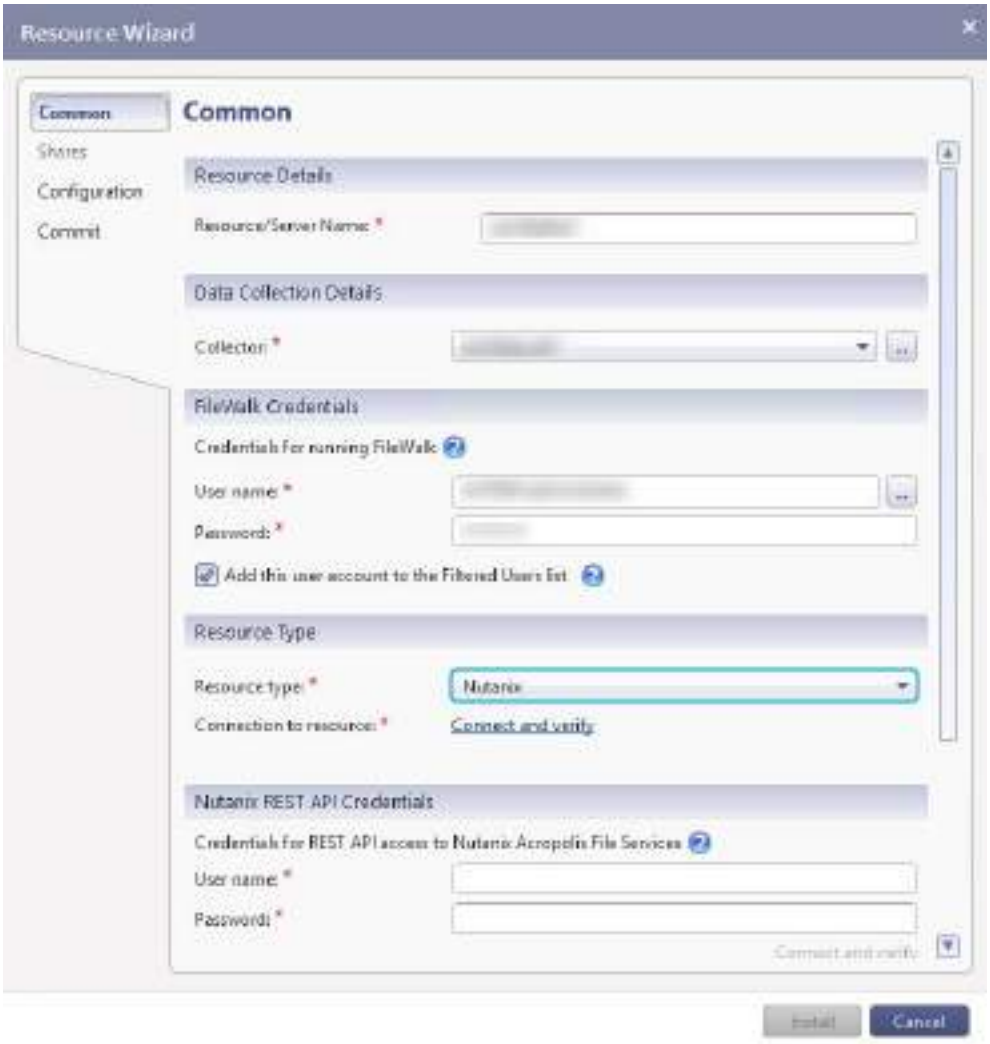
Now that you've configured the REST API Access user, you can deploy a Nutanix data source.

> Note: Each Nutanix data source represents a monitored Nutanix Server. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source. To monitor multiple Nutanix servers, add a Nutanix data source per Nutanix server.

1. Set common data source parameters

1. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.

The Resource Wizard is opened to the Common pane, where you can specify the data source and set the relevant parameters.



2. In the Common pane, set the following parameters:
   a. Resource Details - Specify the data source name.
   b. Data Collection Details - Select the relevant Collector (assigned with a certificate) from the dropdown list. For instructions on adding a certificate for a Collector, click here.
   c. FileWalk Credentials - Enter the credentials for running directory structure monitoring. File System operations include directory structure monitoring, event auditing (if set) and account enumeration on local accounts (if set).

   Note:
   - These credentials are cached, so that they are automatically entered if another data source is added during the same session.

- User name - Type the name of the user account to be used for directory structure monitoring, event auditing, and local account enumeration.
- Password - Type the account's password.
- Add this user account to the Filtered Users list - The defined user for FileWalk Credentials will be added to the filtered users list. If you clear this checkbox, a large number of events may be generated by the user defined for directory structure monitoring. It is recommended to keep this checkbox enabled.

> Important: You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.

d. Resource Type - Select the data source type from the dropdown list.
   - Connect and verify - Click this link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

     > Note:
     > - The Connect and verify link is displayed only when all relevant data is entered.
     > - A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

e. Nutanix REST API Credentials - Enter the following credentials required to retrieve information about the file system and audit events:
   - User name - Insert a REST API user name.

     > Important: Make sure that the user name you entered in Nutanix Prism is only lowercase letters. Uppercase and special characters including underscores (_) are NOT supported.

   - Password - Insert a REST API password.
   - Connect and verify - Click this link to verify the credentials that were entered.

f. Monitored Shares - Select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source installed and share detection is completed.
   - Automatically monitor detected shares - Select this option to automate monitoring for all detected shares. Share monitoring will automatically start

after the data source installation is completed. Varonis will monitor all shares that aren't marked as "ignored". When this option is selected, click the Advanced setting link to modify share detection preferences. By default, the option is set to Prefer regular shares over equivalent admin shares. In this case, an admin share that has an equivalent regular share will be marked as "ignored" and the equivalent regular share will be detected for monitoring. Note: Any change in the monitored shares configuration, including the detection method, admin shares configuration, and selected shares, requires rerunning the resource detection.

- Monitor selected shares - This option is selected by default. You can manually select the shares to be monitored only after the data source is installed and share detection is completed. You'll need to open the Edit window for the installed data source and select the shares. For more information, see Post-installation share detection and registration.

Once the above settings are configured, you can proceed to review and adjust configuration settings.

2. Review and adjust configuration settings

1. On the left menu, click Configuration and confirm the information.
   The general configuration settings are displayed.
2. In the FileWalk Settings area, review the options:
   - Identify actual unique folders and file system inconsistencies - Select this checkbox (if it not already selected) to detect broken permissions in NTFS file systems.
3. In the Event Auditing Parameters area, review the options:
   - Filter out false "File Opened" events - Select this checkbox to filter out false File Open events and collect File Open events only if enough file content is actually read. Small files and certain operations may still trigger Read events.

3. (Optional) Customize commit credentials

You can use different commit credentials instead of the default FileWalk credentials.

1. On the left menu, select Commit.
   The commit settings are displayed.
2. (Optional) Clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials. (By default, this checkbox is selected to use the

FileWalk credentials, and the User name and Password fields are disabled for editing.)

Note:

- If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
- If the Collector is in a lower version than 8, the FileWalk credentials will be used.

3. In the Group OU area, if required, select Uniquely defined to choose a different OU from that defined in the data source's domain. Click the Browse button (...) to select the required OU.

4. Install the data source

After configuration is complete, click Install to install the data source.

A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the File Servers pane. When the installation completes, the status shows "Installed 100%".

5. Post-installation share detection and registration

After the data source installation and share detection are completed, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. The following procedure describes the manual registration and automatic share detection flows.

Important: If after the data source is installed, share detection fails for any reason, the Share Detection Status column will remain "In Progress" until the issue is fixed, and share detection completes successfully at least once.

After the data source is installed, the Shares pane is enabled, and you can view the share settings.

1. On the left menu, click Shares.
   The share settings are displayed. The pane's heading indicates the option you selected when adding a data source.
2. In the Available Shares area, you can filter the shares based on the reason they are not registered for monitoring and easily identify the shares that can be added. The default filter is Accessible Shares. You can change the filter to see the rest of the shares. Options include:

- Accessible shares - Can be added for monitoring (this option is selected by default)
- Ignored shares - Are marked as "ignored"
- Incompatible and inaccessible shares - Cannot be monitored since the exposed protocol does not match the security style of the volume (relevant to multiprotocol platforms only) or the Varonis service account does not have access to this share
- Child share of a monitored share - Is monitored via its parent folder

3. Do one of the following:
   - If you chose to monitor selected shares, in the Available Shares area, select the required shares and click the down arrow. The selected shares are moved to the Registered Shares area. (The registered shares list is empty until you make your selections.)
   - If you chose to automatically monitor detected shares, Varonis will monitor all shares that aren't marked as "ignored". The automated share detection runs every few hours. The Registered Shares area is autopopulated with the shares to be monitored.
4. For each share, review and set the following information as required:
   - Ignore Detection - Select the shares to be ignored (and not be the subject of automatic detection and notifications) by the data source monitor.
   - Events - Select this checkbox to audit events for the share.
   - Crawl - To enable or disable monitoring for the share, in the Crawl column, select the relevant option.

     Note: You can also right-click the grid and select the required options for event auditing and crawling.
5. In the Additional Share Settings area, review the options:
   - Remove deleted shares - Select this checkbox to remove deleted shares. Shares that were deleted from the data source will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the data source is unavailable, the shares will not be removed.
   - Enable event auditing - Select this checkbox to audit events from all shares added from this data source.

   After share detection and registration are completed, the status and number of registered volumes are respectively displayed in the Share Detection Status and Registered Shares columns in the File Servers pane.

What To Do Next

Now let's take a look at the supported events for the monitored Nutanix data sources.

Supported Events For Nutanix Data Sources

SMB (CIFS) Events for Nutanix Data Sources

The monitored data sources and NAS devices support various SMB (CIFS) events.

Event Auditing Method

Nutanix API

Supported File Operations

- File created
- File deleted
- File modified
- File opened
- File renamed
- Folder created
- Folder deleted
- Folder renamed
- File permissions changed
- Folder permissions changed
- Owner changed

Access Denied Events:

- File access denied
- Folder access denied

Note: All CIFS access denied events will arrive as File open denied events.

14 COHESITY DATA SOURCES

What This Section Contains

This section describes how to deploy and monitor Cohesity data sources; the requirements, deployment and configuration steps, and supported events.

Before You Begin

Make sure you've added a certificate for the Collector used for monitoring this data source. For instructions, click here.

What To Do Next

Before you dive in, click here to learn more about how Varonis monitors Cohesity accounts, file system, and events.

Cohesity Monitoring Overview

Note: Each Cohesity data source represents a monitored Cohesity server. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source.

Varonis monitors Cohesity via the following parallel data streams.

Accounts

- Varonis enumerates local account information remotely from the Collector with a dedicated service account.

File System

- Varonis collects folder structure, permissions, and metadata via a dedicated service for directory structure monitoring (FileWalk) that runs on the assigned Collector. This connection is made over SMB.

Data Classification and Labeling

- Varonis supports data classification and labeling on files that reside in the monitored data sources.

Events

- Varonis monitors Cohesity events using a dedicated event auditing service (Forwarder) that runs on the Collector.

What To Do Next

First, make sure you fulfill the Cohesity requirements.

Cohesity Requirements

Varonis Service Account

Varonis requires a dedicated service account. The service account can be reused for multiple data source installations and configurations.

- Service Account Read Operations:
  - Traverse and enumerate files, folders, directory structures, users, and groups.
  - Gather data source, user, and group metadata as part of normal system operations.
- Service Account Write Operations:
  - Used for executing Varonis Policies, if policies are defined.

Varonis Installation and Requirements

- Cohesity REST API credentials are required to add Cohesity file servers to the Management Console.
- For event auditing, the Cohesity Connector for the Varonis app from the Cohesity Marketplace should be installed on the monitored Cohesity file server. For more information, see Adding a Cohesity Data Source - Detailed Procedure.

Known Limitation

- Varonis can detect, crawl, and monitor only Browsable Shares. Shares for which the Browsable Shares configuration is disabled in the Cohesity UI (via View Settings > SMB Options > Browsable Shares) are not supported by Varonis.
- Varonis cannot be used to monitor a Cohesity ROBO node (single node cluster).
- The "Collect information regarding local accounts from this file server" collects only local users that are members of the primary group.
  To enable scanning local users and groups via account enumeration, make sure at least one user that is a member of at least one group is specified and enable the Set primary group to enable file access option:
  - Navigate to the Cohesity Admin site > Settings > Summary > Configure.
  - Enable the option Enable Local Groups.
  - Edit the local user under Groups and choose the relevant group.
  - Enable Set primary group to enable file access, select the primary group, and save the changes.

- User membership in local built-in groups is not supported.
- For local account enumeration, additional groups are displayed in the Varonis Web Interface that are not displayed in the Cohesity UI; this is by design according to Cohesity.

What To Do Next

Now that you've fulfilled the requirements, proceed to configure the Varonis service account for Cohesity.

Configuring the Varonis Service Account for Cohesity

Before you add Cohesity data sources, you need to configure the Varonis service account.

Requirements for the Varonis Service Account for Read Operations

Note:
Before you begin, note the following requirements for Varonis service account:

- Must be a domain user from the primary domain
- Should have "List folder contents" permissions to be able to scan the volume size.
- Should have "Read" permissions for data discovery and classification file scanning.

1. To configure a new role for the Varonis service account: In the Cohesity UI management page, from the main menu, select Settings > Cluster > Access Management > Roles, click Add Custom Role, and set the following:
   - Access Management > View Users
   - Cluster Management > View Cluster Details
   - Cluster Management > Manage Cluster
   - Storage Management > Read Cohesity Views
   - Storage Management > Manage Cohesity Views
   - Storage Management > Manage Cohesity Storage Domains
   - SMB Security > SMB Backup
   - SMB Security > SMB Restore

- SMB Security > Manage system access control list on SMB files

2. To add the domain Varonis service account: In the Cohesity UI management page, from the main menu, select Settings > Cluster > Access Management > Add AD Users and Groups, and do the following:
   a. Select Active Directory Users and Groups.
   b. Add the AD principal - Varonis service account.

      Note: Use the Varonis service account name. Specifying a group is not supported.

   c. Under Roles, select the dedicated Varonis service account role created in step 1 above.

Requirements for the Varonis Service Account for Write Operations

Same as the Varonis service account for read operations.

What To Do Next

Now proceed to configure the Cohesity REST API user.

Configuring the Cohesity REST API Access User

Before you add Cohesity data sources, you need to configure the REST API access user.

The REST API credentials are used to enable auditing on the data sources' shares.

You need to configure a user with the Cohesity REST API role and assign the user to the “Users” primary group.

1. To configure the REST API role: In the Cohesity UI management page, from the main menu, select Settings > Access Management > Roles, click Add Custom Role, and set the following:
   - Cluster Management > View Cluster Details
   - Cluster Management > Manage Cluster
   - Storage Management > Read Cohesity Views
   - Storage Management > Manage Cohesity Views
   - SMB Security > SMB Backup
   - SMB Security > SMB Restore

2. To add the local user: In the Cohesity UI management page, from the main menu, select Settings > Access Management > Add AD Users and Groups from the upper right corner, and do the following:
   a. Select Local User and enter the Username, Email, and Password.
   b. Under Roles, select the RestAPI role configured in step 1.

What To Do Next

Now proceed to install the Cohesity connector for the Varonis app, required for event auditing.

Installing the Cohesity Connector for Varonis App on the Cohesity Cluster

Before you add Cohesity data sources, you need to get the Cohesity Connector for the Varonis app from Cohesity Helios and install it on the Cohesity Cluster. This is required for event auditing.

Installing the App on Connected Sites

1. Log in to Cohesity Helios with valid credentials.
2. Navigate to Marketplace > All Apps.
   The Cohesity Marketplace page is displayed.
3. Click the Cohesity Connector for Varonis app.
   The app details page is displayed.
4. Click Get App. (This may take few minutes.)
5. Select the cluster(s) on which you want to install the app.
6. Click Install to install the app immediately. Click Install Later if you want to install the app at a later point in time.
7. After you've installed the app, in the App settings > Connectivity area, enable Allow external connectivity from apps.

Installing the App on Disconnected Sites

1. Log in to the cluster on which the app must be installed.
2. Navigate to Marketplace > All Apps.
   The Cohesity Marketplace page is displayed.
3. Click the Cohesity Connector for Varonis app.
   The app details page is displayed.

4. Click Get App.
5. Skip the step Select Clusters to Install Cohesity Connector for Varonis.
6. Navigate to the Download tab, select the appropriate cluster version, and click Get App Versions.
7. Click on the latest version of the app displayed, to initiate downloading of the app package.
8. Navigate to Marketplace > My Apps.

   Note: If the All Instances tab is displayed, click the My Apps tab.

9. In the App settings > Connectivity area, enable Allow external connectivity from apps.
10. Click Upload App.
11. Browse and select the downloaded app package, and click Upload and Install.
    It may take about ten minutes for the app to be displayed in the interface. The Run App button is displayed only after the installation is complete.
12. Navigate to the All Instances tab and click Open App to launch the app in a new tab.
13. Sign in with valid credentials.
    Initially, you must log in with admin credentials. Subsequent logins depend on the roles assigned by the admin.
    For more information about Cohesity Marketplace and the procedure to manage apps, see MarketPlace Apps.

What To Do Next

Now that you've installed the Cohesity Connector required for event auditing, it's time to add a monitored Cohesity data source. First familiarize yourself with the deployment steps summary and then dive into the detailed procedure.

Adding a Cohesity Data Source - Summary

Now that you've installed the Cohesity Connector, you can deploy a Cohesity data source. This section summarizes the procedure for deploying Cohesity data sources.

1. Run the Management Console as an administrator.
2. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.
3. In the Resource Wizard's Common pane, specify the data source name, check the Collector selected by default and change it if needed, and enter the credentials for running directory structure monitoring (FileWalk).

Important:

- In the Resource Details area, type the Cohesity cluster NetBIOS name.
- Make sure a Collector that's assigned with a certificate is selected. For instructions on adding a certificate for a Collector, click here.
- You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.

4. In the Resource Type area, select the data source type from the dropdown list. Then, click the Connect and verify link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

   Note:

   - The Connect and verify link is displayed only when all relevant data is entered.
   - A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

5. In the Cohesity REST API Credentials area, enter the REST API credentials required to retrieve information about the file system and audit events. Then, click the Connect and verify link to verify the credentials that were entered.
6. In the Monitored Shares area, select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source is installed and share detection is completed.
7. In the Configuration pane, review the Local Accounts, FileWalk Settings, and Event Auditing Parameters settings.

   Note: When the Collect information regarding local accounts from this file server checkbox is selected:

   - Only Cohesity local users that are members of the primary group are collected.
   - User membership in Cohesity local built-in groups is not supported.

8. (Optional) In the Commit pane, clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials.

Note:

- If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
- If the Collector is in a lower version than 8, the FileWalk credentials will be used.

In the Group OU area, if required, select Uniquely defined to choose a different OU from that defined in the data source's domain.

9. After configuration is complete, click Install to add the data source.
10. After the data source installation and share detection are completed, in the Shares pane, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. If you chose to monitor selected shares, you can select and register the required shares.

What To Do Next

Now that you're familiar with the deployment steps, it's time to dive into the detailed procedure.

Adding a Cohesity Data Source - Detailed Procedure

Now that you've installed the Cohesity Connector, you can deploy a Cohesity data source.

Note: Each Cohesity data source represents a monitored Cohesity Server. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source. To monitor multiple Cohesity servers, add a Cohesity data source per Cohesity server.

1. Set common data source parameters

1. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.

The Resource Wizard is opened to the Common pane, where you can specify the data source and set the relevant parameters.



2. In the Common pane, set the following parameters:
   a. Resource Details - Type the Cohesity cluster NetBIOS name.
   b. Data Collection Details - Select the relevant Collector (assigned with a certificate) from the dropdown list. For instructions on adding a certificate for a Collector, click here.
   c. FileWalk Credentials - Enter the credentials for running directory structure monitoring. File System operations include directory structure monitoring, event auditing (if set) and account enumeration on local accounts (if set).

   Note:
   - These credentials are cached, so that they are automatically entered if another data source is added during the same session.

- User name - Type the name of the user account to be used for directory structure monitoring, event auditing, and local account enumeration.
- Password - Type the account's password.
- Add this user account to the Filtered Users list - The defined user for FileWalk Credentials will be added to the filtered users list. If you clear this checkbox, a large number of events may be generated by the user defined for directory structure monitoring. It is recommended to keep this checkbox enabled.

Important: You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.

d. Resource Type - Select the data source type from the dropdown list.
   - Connect and verify - Click this link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

     Note:
     - The Connect and verify link is displayed only when all relevant data is entered.
     - A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

e. Cohesity REST API Credentials - Enter the following credentials required to retrieve information about the file system and audit events:
   - User name - Insert a REST API user name.
   - Password - Insert a REST API password.
   - Connect and verify - Click this link to verify the credentials that were entered.

f. Monitored Shares - Select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source installed and share detection is completed.
   - Automatically monitor detected shares - Select this option to automate monitoring for all detected shares. Share monitoring will automatically start after the data source installation is completed. Varonis will monitor all shares that aren't marked as "ignored". When this option is selected, click the Advanced setting link to modify share detection preferences. By default, the option is set to Prefer regular shares over equivalent admin shares. In this

case, an admin share that has an equivalent regular share will be marked as "ignored" and the equivalent regular share will be detected for monitoring. Note: Any change in the monitored shares configuration, including the detection method, admin shares configuration, and selected shares, requires rerunning the resource detection.

- Monitor selected shares - This option is selected by default. You can manually select the shares to be monitored only after the data source is installed and share detection is completed. You'll need to open the Edit window for the installed data source and select the shares. For more information, see Post-installation share detection and registration.

Once the above settings are configured, you can proceed to review and adjust configuration settings.

2. Review and adjust configuration settings

1. On the left menu, click Configuration and confirm the information.
   The general configuration settings are displayed.
2. In the Local Accounts area, review the options:
   - Collect information regarding local accounts from this file server - Select this checkbox to collect user accounts from this file system.

     Note:
     - Only Cohesity local users that are members of the primary group are collected.
     - User membership in Cohesity local built-in groups is not supported.
3. In the FileWalk Settings area, review the options:
   - Identify actual unique folders and file system inconsistencies - Select this checkbox (if it not already selected) to detect broken permissions in NTFS file systems.
4. In the Event Auditing Parameters area, review the options:
   - Filter out false "File Opened" events - Select this checkbox to filter out false File Open events and collect File Open events only if enough file content is actually read. Small files and certain operations may still trigger Read events.

3. (Optional) Customize commit credentials

You can use different commit credentials instead of the default FileWalk credentials.

1. On the left menu, select Commit.
   The commit settings are displayed.
2. (Optional) Clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials. (By default, this checkbox is selected to use the FileWalk credentials, and the User name and Password fields are disabled for editing.)

   Note:
   - If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
   - If the Collector is in a lower version than 8, the FileWalk credentials will be used.
3. In the Group OU area, if required, select Uniquely defined to choose a different OU from that defined in the data source's domain. Click the Browse button (...) to select the required OU.

4. Install the data source

After configuration is complete, click Install to install the data source.

A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the File Servers pane. When the installation completes, the status shows "Installed 100%".

5. Post-installation share detection and registration

After the data source installation and share detection are completed, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. The following procedure describes the manual registration and automatic share detection flows.

Important: If after the data source is installed, share detection fails for any reason, the Share Detection Status column will remain "In Progress" until the issue is fixed, and share detection completes successfully at least once.

After the data source is installed, the Shares pane is enabled, and you can view the share settings.

1. On the left menu, click Shares.

The share settings are displayed. The pane's heading indicates the option you selected when adding a data source.

2. In the Available Shares area, you can filter the shares based on the reason they are not registered for monitoring and easily identify the shares that can be added. The default filter is Accessible Shares. You can change the filter to see the rest of the shares. Options include:
   - Accessible shares - Can be added for monitoring (this option is selected by default)
   - Ignored shares - Are marked as "ignored"
   - Incompatible and inaccessible shares - Cannot be monitored since the exposed protocol does not match the security style of the volume (relevant to multiprotocol platforms only) or the Varonis service account does not have access to this share
   - Child share of a monitored share - Is monitored via its parent folder
3. Do one of the following:
   - If you chose to monitor selected shares, in the Available Shares area, select the required shares and click the down arrow. The selected shares are moved to the Registered Shares area. (The registered shares list is empty until you make your selections.)
   - If you chose to automatically monitor detected shares, Varonis will monitor all shares that aren't marked as "ignored". The automated share detection runs every few hours. The Registered Shares area is autopopulated with the shares to be monitored.
4. For each share, review and set the following information as required:
   - Ignore Detection - Select the shares to be ignored (and not be the subject of automatic detection and notifications) by the data source monitor.
   - Events - Select this checkbox to audit events for the share.
   - Crawl - To enable or disable monitoring for the share, in the Crawl column, select the relevant option.

     Note: You can also right-click the grid and select the required options for event auditing and crawling.
5. In the Additional Share Settings area, review the options:
   - Remove deleted shares - Select this checkbox to remove deleted shares. Shares that were deleted from the data source will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the data source is unavailable, the shares will not be removed.

- Enable event auditing - Select this checkbox to audit events from all shares added from this data source.

After share detection and registration are completed, the status and number of registered volumes are respectively displayed in the Share Detection Status and Registered Shares columns in the File Servers pane.

What To Do Next

Now let's take a look at the supported events for the monitored Cohesity data sources.

Supported Events For Cohesity Data Sources

SMB (CIFS) Events for Cohesity Data Sources

The monitored data sources and NAS devices support various SMB (CIFS) events.

> Note: SMB v2 and v3 are supported.

Event Auditing Method

RabbitMQ

Supported File Operations

- File created
- File deleted
- File modified
- File opened
- File renamed
- Folder created
- Folder deleted
- Folder renamed
- Owner changed
- Permission added
- Permission removed
- Protection added
- Protection removed

15 CTERA DATA SOURCES

What This Section Contains

This section describes how to deploy and monitor CTERA data sources; the requirements, deployment and configuration steps, and supported events.

Before You Begin

Make sure you've added a certificate for the Collector used for monitoring this data source. For instructions, click here.

What To Do Next

Before you dive in, click here to learn more about how Varonis monitors CTERA accounts, file system, and events.

CTERA Monitoring Overview

Note: Each CTERA data source represents a monitored CTERA server. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source.

Varonis monitors CTERA via the following parallel data streams.

Accounts

- Varonis enumerates local account information remotely from the Collector with a dedicated service account.

File System

- Varonis collects folder structure, permissions, and metadata via a dedicated service for directory structure monitoring (FileWalk) that runs on the assigned Collector. This connection is made over SMB.

Data Classification and Labeling

- Varonis supports data classification and labeling on files that reside in the monitored data sources.

Events

- Varonis monitors CTERA events using a dedicated event auditing service (Forwarder) that runs on the Collector.

What To Do Next

First, make sure you fulfill the CTERA requirements.

CTERA Requirements

Varonis Service Account

Varonis requires a dedicated service account. The service account can be reused for multiple data source installations and configurations.

- Service Account Read Operations:
  - Traverse and enumerate files, folders, directory structures, users, and groups.
  - Gather data source, user, and group metadata as part of normal system operations.
- Service Account Write Operations:
  - Used for executing Varonis Policies, if policies are defined.

Varonis Installation and Requirements

- Deploy a dedicated CTERA Edge Filer for Varonis along with a Varonis Collector on the Cloud local to the region where the CTERA Global File System resides. This eliminates the need to transfer the entire data set across a wide area network. It enables data scans, metadata scans, and event collection without latency, reduces scan duration, and avoids file content transfer from the cloud to on-premises. In addition, the users' daily work is not compromised.
- Crawling:
  - The dedicated CTERA Edge Filer is scanned by directory structure monitoring and Data Classification from the Varonis Collector.
- Event auditing:
  - Varonis supports SMB event collection from the CTERA Edge Filers as follows:
    - The log shipper on the CTERA Branch Edge Filers sends audit logs to the CTERA log forwarder.
    - The CTERA log forwarder parses the logs, adjusts them to Varonis event formatting, and sends the events to the Varonis Collector via RabbitMQ.
- Configure connectivity between the CTERA Virtual DNS Portal and Varonis - do one of the following:
  - Go to `C:\Windows\System32\drivers\etc` and in the `hosts` file, enter the IP of the CTERA portal. You need to add the DNS portal name and IP of the CTERA gateway.
  - Add a DNS host record to the DNS server, enter the IP of the CTERA portal and the DNS portal name.

Security Requirements

- CTERA REST API credentials and the Virtual Portal DNS Name are required to add CTERA file servers to the Management Console.

Notes

- Varonis does not support local CTERA users and groups.
- On CTERA file servers, the File Accessed Date attribute is continuously updated on daily basis.
- To enable Data Classification scanning of CTERA file servers that may contain stub files, the default configuration needs to be changed. Contact Varonis Support for assistance. The updated default configuration will affect all file servers that Data Classification scans and not only CTERA.
- A license from CTERA is required to use the Varonis service. For more information, see Integrating CTERA with Varonis Data Security Platform.

What To Do Next

Now that you've fulfilled the requirements, proceed to configure the Varonis service account for CTERA.

Configuring the Varonis Service Account for CTERA

Before you add CTERA data sources, you need to configure the Varonis service account.

Requirements for the Varonis Service Account for Read Operations

Note:

- The Varonis service account must be a domain user from the primary domain.
- The Varonis service account must be a member of both the local CTERA backup operator group and read-only administrators group.
- The configurations should be done in the CTERA Gateway, not in the CTERA Portal.

First configure the Varonis service account for the local CTERA backup operator group:

1. In the CTERA Gateway web interface, from the main menu, select Users > Groups. The Groups page is displayed.
2. Select the Backup Operators group.
3. Click Next.
4. Select Domain Users and enter the Varonis service account name.

   Note: Use the Varonis service account name. Specifying a group is not supported.
5. Click Next.
6. Click Finish.
7. Repeat the steps above to add the Varonis service account to the read-only administrators group.

Requirements for the Varonis Service Account for Write Operations

Same as the Varonis service account for read operations.

What To Do Next

Now that you've configured the Varonis service account for CTERA, it's time to configure the CTERA REST API access user.

Configuring the CTERA REST API Access User

Before you add CTERA data sources, you need to configure the CTERA REST API access user.

The REST API credentials are used to enable auditing on the data sources' shares.

You need to configure a user with the CTERA REST API role and assign the user to the “Users” primary group.

Note: The configurations should be done in the CTERA Portal, not in the CTERA Gateway.

1. In the CTERA Portal, go to Administration > Services > Varonis.
2. To configure the Varonis service, select Settings > Configure Service (on upper right).

The Varonis Connector Settings dialog box is displayed.

3. For initial configuration, enter the API user name, and click Generate Password to generate the API password automatically.

   Note: Store the password in a handy location for later use, if needed.

4. Click Save. The service will be active after synchronization completes.

What To Do Next

Now proceed to configure CTERA for event auditing.

Configuring Event Auditing for CTERA

Prior to adding CTERA data sources, configure event auditing.

Note: The configurations should be done in the CTERA Portal, not in the CTERA Gateway.

1. In the CTERA Portal, go to Administration > Services > Messaging and verify that the messaging service is active.
2. Go to Gateway > Logs > Audit Logs, and do the following:
   - Verify that Enable CIFS/SMB Audit Logs is selected.
   - Verify that Save log files to is set to your shares path in your browser.
3. Click Save.
4. Verify that all the Events to Log checkboxes are selected.

What To Do Next

Now that you've configured event auditing for CTERA, it's time to add a monitored Cohesity data source. First familiarize yourself with the deployment steps summary and then dive into the detailed procedure.

Adding a CTERA Data Source - Summary

Now that you've configured event auditing, you can deploy a CTERA data source. This section summarizes the procedure for deploying CTERA data sources.

1. Run the Management Console as an administrator.
2. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.

3. In the Resource Wizard's Common pane, specify the data source name, check the Collector selected by default and change it if needed, and enter the credentials for running directory structure monitoring (FileWalk).

   Important:

   - Make sure a Collector that's assigned with a certificate is selected. For instructions on adding a certificate for a Collector, click here.

4. In the Resource Type area, select the data source type from the dropdown list.
5. In the CTERA REST API Credentials area, enter the REST API credentials required to retrieve information about the file system and audit events. Then, click the Connect and verify link to verify the credentials that were entered.

   Important:

   - The user should have credentials for REST API access to CTERA data sources. (This is not a domain user.)
   - For the Virtual Portal DNS Name, insert the portal name in DNS format (`portal.<DNS wyj 1 from the global setting>`). This attribute should not be updated after the file server was installed.

6. In the Monitored Shares area, select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source is installed and share detection is completed.
7. In the Configuration pane, review the FileWalk Settings and Event Auditing Parameters settings.
8. (Optional) In the Commit pane, clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials.

   Note:

   - If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
   - If the Collector is in a lower version than 8, the FileWalk credentials will be used.

   In the Group OU area, if required, select Uniquely defined to choose a different OU from that defined in the data source's domain.

9. After configuration is complete, click Install to add the data source.

10. After the data source installation and share detection are completed, in the Shares pane, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. If you chose to monitor selected shares, you can select and register the required shares.

What To Do Next

Now that you're familiar with the deployment steps, it's time to dive into the detailed procedure.

Adding a CTERA Data Source - Detailed Procedure

Now that you've configured event auditing, you can deploy a CTERA data source.

> Note: Each CTERA data source represents a monitored CTERA Server. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source. To monitor multiple CTERA servers, add a CTERA data source per CTERA server.

1. Set common data source parameters

1. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.

The Resource Wizard is opened to the Common pane, where you can specify the data source and set the relevant parameters.



2. In the Common pane, set the following parameters:
   a. Resource Details - Specify the data source name.
   b. Data Collection Details - Select the relevant Collector (assigned with a certificate) from the dropdown list. For instructions on adding a certificate for a Collector, click here.
   c. FileWalk Credentials - Enter the credentials for running directory structure monitoring. File System operations include directory structure monitoring, event auditing (if set) and account enumeration on local accounts (if set).

   Note:
   - These credentials are cached, so that they are automatically entered if another data source is added during the same session.

- User name - Type the name of the user account to be used for directory structure monitoring, event auditing, and local account enumeration.
- Password - Type the account's password.

d. Resource Type - Select the data source type from the dropdown list.

e. CTERA REST API Credentials - Enter the following credentials required to retrieve information about the file system and audit events:

> Note: The user should have credentials for REST API access to CTERA data sources. (This is not a domain user.)

- Virtual Portal DNS Name - Insert the portal name in DNS format (`portal.<DNS wyj 1 from the global setting>`). This attribute should not be updated after the data source was installed.

  > Note: You can deploy multiple CTERA data sources that are using the same Virtual Portal DNS Name.

- User name - Insert a REST API user name.
- Password - Insert a REST API password.
- Connect and verify - Click this link to verify the credentials that were entered.

f. Monitored Shares - Select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source installed and share detection is completed.

- Automatically monitor detected shares - Select this option to automate monitoring for all detected shares. Share monitoring will automatically start after the data source installation is completed. Varonis will monitor all shares that aren't marked as "ignored". When this option is selected, click the Advanced setting link to modify share detection preferences. By default, the option is set to Prefer regular shares over equivalent admin shares. In this case, an admin share that has an equivalent regular share will be marked as "ignored" and the equivalent regular share will be detected for monitoring. Note: Any change in the monitored shares configuration, including the detection method, admin shares configuration, and selected shares, requires rerunning the resource detection.
- Monitor selected shares - This option is selected by default. You can manually select the shares to be monitored only after the data source is installed and share detection is completed. You'll need to open the Edit window for the installed data source and select the shares. For more information, see Post-installation share detection and registration.

Once the above settings are configured, you can proceed to review and adjust configuration settings.

2. Review and adjust configuration settings

1. On the left menu, click Configuration and confirm the information.
   The general configuration settings are displayed.
2. In the FileWalk Settings area, review the options:
   - Identify actual unique folders and file system inconsistencies - Select this checkbox (if it not already selected) to detect broken permissions in NTFS file systems.
3. In the Event Auditing Parameters area, review the options:
   - Filter out false "File Opened" events - Select this checkbox to filter out false File Open events and collect File Open events only if enough file content is actually read. Small files and certain operations may still trigger Read events.

3. (Optional) Customize commit credentials

You can use different commit credentials instead of the default FileWalk credentials.

1. On the left menu, select Commit.
   The commit settings are displayed.
2. (Optional) Clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials. (By default, this checkbox is selected to use the FileWalk credentials, and the User name and Password fields are disabled for editing.)

   Note:
   - If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
   - If the Collector is in a lower version than 8, the FileWalk credentials will be used.
3. In the Group OU area, if required, select Uniquely defined to choose a different OU from that defined in the data source's domain. Click the Browse button (...) to select the required OU.

4. Install the data source

After configuration is complete, click Install to install the data source.

A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the File Servers pane. When the installation completes, the status shows "Installed 100%".

5. Post-installation share detection and registration

After the data source installation and share detection are completed, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. The following procedure describes the manual registration and automatic share detection flows.

> Important: If after the data source is installed, share detection fails for any reason, the Share Detection Status column will remain "In Progress" until the issue is fixed, and share detection completes successfully at least once.

After the data source is installed, the Shares pane is enabled, and you can view the share settings.

1. On the left menu, click Shares.
   The share settings are displayed. The pane's heading indicates the option you selected when adding a data source.
2. In the Available Shares area, you can filter the shares based on the reason they are not registered for monitoring and easily identify the shares that can be added. The default filter is Accessible Shares. You can change the filter to see the rest of the shares. Options include:
   - Accessible shares - Can be added for monitoring (this option is selected by default)
   - Ignored shares - Are marked as "ignored"
   - Incompatible and inaccessible shares - Cannot be monitored since the exposed protocol does not match the security style of the volume (relevant to multiprotocol platforms only) or the Varonis service account does not have access to this share
   - Child share of a monitored share - Is monitored via its parent folder
3. Do one of the following:
   - If you chose to monitor selected shares, in the Available Shares area, select the required shares and click the down arrow. The selected shares are moved to

the Registered Shares area. (The registered shares list is empty until you make your selections.)

- If you chose to automatically monitor detected shares, Varonis will monitor all shares that aren't marked as "ignored". The automated share detection runs every few hours. The Registered Shares area is autopopulated with the shares to be monitored.

4. For each share, review and set the following information as required:
   - Ignore Detection - Select the shares to be ignored (and not be the subject of automatic detection and notifications) by the data source monitor.
   - Events - Select this checkbox to audit events for the share.
   - Crawl - To enable or disable monitoring for the share, in the Crawl column, select the relevant option.

     Note: You can also right-click the grid and select the required options for event auditing and crawling.

5. In the Additional Share Settings area, review the options:
   - Remove deleted shares - Select this checkbox to remove deleted shares. Shares that were deleted from the data source will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the data source is unavailable, the shares will not be removed.
   - Enable event auditing - Select this checkbox to audit events from all shares added from this data source.

   After share detection and registration are completed, the status and number of registered volumes are respectively displayed in the Share Detection Status and Registered Shares columns in the File Servers pane.

What To Do Next

Now let's take a look at the supported events for the monitored CTERA data sources.

Supported Events For CTERA Data Sources

SMB (CIFS) Events for CTERA Data Sources

The monitored data sources and NAS devices support various SMB (CIFS) events.

Note: SMB v2 and v3 are supported.

Event Auditing Method

Events are sent to the Collector via RabbitMQ by the CTERA Log Forwarder.

Supported File Operations

- File created
- File deleted
- File modified
- File opened
- File renamed
- Folder created
- Folder deleted
- Folder renamed
- File permissions changed
- Folder permissions changed
- Owner changed

> Note:
> When performing CIFS Folder created and File created events on a CTERA file server, additional events are generated:
>
> - Owner changed
> - Folder permissions changed

Access Denied Events:

- File deleted
- File permission added
- Folder deleted
- Folder opened
- Folder permission added

16 QUMULO DATA SOURCES

What This Section Contains

This section describes how to deploy and monitor Qumulo data sources; the requirements, deployment and configuration steps, and supported events.

Before You Begin

Make sure you've added a certificate for the Collector used for monitoring this data source. For instructions, click here.

What To Do Next

Before you dive in, click here to learn more about how Varonis monitors Qumulo accounts, file system, and events.

Qumulo Monitoring Overview

Note: Each Qumulo data source represents a monitored Qumulo cluster. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source.

About Qumulo

Qumulo is a software-defined storage platform that can be deployed on diverse hardware types and in private and public clouds.

A Qumulo cluster is comprised of multiple identical nodes, with a single namespace. If the customer has multiple clusters with different namespaces, Varonis requires deploying a separate Qumulo data source per namespace.

How Varonis Monitors Qumulo

The events logged by Qumulo are first shipped to a dedicated event proxy server (which needs to be deployed along with Qumulo) which, in turn, forwards the events to the Varonis events queue (RabbitMQ) on the Collector.

Varonis monitors Qumulo:

- Local accounts
- Directory structure and permissions
- Data - and classifies it
- Events

Data Classification and Labeling

- Varonis supports data classification and labeling on files that reside in the monitored data sources.

What To Do Next

First, make sure you fulfill the Qumulo requirements.

Qumulo Requirements

Varonis Service Account

Varonis requires a dedicated service account. The service account can be reused for multiple data source installations and configurations.

- Service Account Read Operations:
  - Traverse and enumerate files, folders, directory structures, users, and groups.
  - Gather data source, user, and group metadata as part of normal system operations.
- Service Account Write Operations:
  - Used for executing Varonis Policies, if policies are defined.

Deployment Requirements

- The Qumulo Broker (middleware) server must be deployed for integration with Varonis. For more information, click here.

  Note: The Qumulo Broker must be configured as UTC time zone.

- The Varonis service account requires the backup admin role within the Qumulo Admin Console. For more information, see Configuring the Varonis Service Account for Qumulo.
- Qumulo REST API credentials are required to add Qumulo data sources to the Management Console.
- Deploy a Collector that resides within LAN proximity to the monitored Qumulo cluster. It is recommended that the Qumulo event proxy resides in the same LAN too.
- Provide the DNS name that represents the IP pool of the cluster nodes (recommended for better resilience) or the IP address or hostname of a specific node.

What To Do Next

Now that you've fulfilled the requirements, proceed to configure the Varonis service account for Qumulo.

Configuring the Varonis Service Account for Qumulo

Before you add Qumulo data sources, you need to configure the Varonis service account.

Requirements for the Varonis Service Account for Read Operations

Note:

- The Varonis service account must be a domain user from the primary domain.
- The Varonis service account requires the backup admin role within the Qumulo Admin Console.
- The user must be assigned to the File Server Admin: Administrators or Data-Administrators role for the REST API access to function correctly.

You need to configure the Varonis service account with the Qumulo Data-Administrators role with an additional role which has the File_FULL_ACCESS privilege.

1. In the Qumulo Admin Console, from the main menu, select Cluster > Local Users and Groups. Take note of the service account user you wish to use.
2. From the main menu, select Cluster > Role Management. Both the Varonis service account and access credentials should be a data administrator or higher.
3. Assign the roles to an existing AD account or new user. To add a new user, click the New Member button.
4. In the Trustee field, enter the Varonis service account name.

   Note:

   - Use the Varonis service accountname.
   - Use the Varonis service account's full name, including the domain name.

Requirements for the Varonis Service Account for Write Operations

In addition to the requirements for the read operations, the Varonis service account for write operations requires the Data-Administrators, File_Full_Access, and Observers roles.

You need to configure the Varonis service account with the Qumulo Data-Administrators role with an additional role which has the File_FULL_ACCESS privilege.

1. From the main menu, select Cluster > Role Management and click the Create Role button.
2. Assign the roles to an existing AD account or new user. To add a new user, click the New Member button.
3. In the Trustee field, enter the Varonis service account name.

   Note:
   - Use the Varonis service accountname.
   - Use the Varonis service account's full name, including the domain name.

What To Do Next

Now proceed to configure the Qumulo REST API user.

Configuring the Qumulo REST API Access User

Before you add Qumulo data sources, you need to configure the Qumulo Rest API access user.

1. Log in to the Qumulo Core cluster with the relevant admin credentials (username and password). Ensure that the Qumulo version is 6.0.1.
2. In the Qumulo Admin Console, from the main menu, select API & Tools.
3. Log in to the API using the relevant admin credentials. Then, click Apply credentials. A message is displayed indicating whether the authentication succeeded.
4. Search for Audit Log and expand the PUT section. To configure the cluster to send events to the middleware server, enter the following parameters:
   - `server_address` - Enter the IP address of the middleware server
   - `server_port` - `514`
   - `format` - `json`

   Then, click Try it out.

   Note: Try it out must be selected prior to entering the information.

5. Click Execute. Confirm that all's configured as expected. Status code 200 indicates a success.
6. From the main menu, select Cluster > Audit.
   The configured settings are displayed in the Remote Syslog Address and Port Number areas. The status shows Connected (in green).

What To Do Next

Now that you've configured the Qumulo REST API access user, it's time to add a monitored Qumulo data source. First familiarize yourself with the deployment steps summary and then dive into the detailed procedure.

Adding a Qumulo Data Source - Summary

Now that you've configured the REST API Access user, you can deploy a Qumulo data source. This section summarizes the procedure for deploying Qumulo data sources.

1. Run the Management Console as an administrator.
2. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.
3. In the Resource Wizard's Common pane, in the Resource Details area, enter the FQDN or IP address of the Qumulo node. Then, check the Collector selected by default and change it if needed, and enter the Qumulo admin credentials for running directory structure monitoring (FileWalk).

   Important:
   - Make sure a Collector that's assigned with a certificate is selected. For instructions on adding a certificate for a Collector, click here.
   - You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.

4. In the Resource Type area, select the data source type from the dropdown list. Then, click the Connect and verify link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

   Note:
   - The Connect and verify link is displayed only when all relevant data is entered.

- A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

Important: Before continuing, verify the configuration in the Qumulo admin console. Follow the steps described in Configuring the Varonis Service Account for Qumulo and Configuring the Qumulo REST API Access User.

5. In the Qumulo REST API AMQP Credentials area, enter the REST API credentials required to retrieve information about the file system and audit events. Then, click the Connect and verify link to verify the credentials that were entered.

   Note: For the Event Auditing Middleware IP, enter the IP of the middleware server, required for event auditing.

6. In the Monitored Shares area, select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source is installed and share detection is completed.
7. In the Configuration pane, review the FileWalk Settings and Event Auditing Parameters settings.
8. (Optional) In the Commit pane, clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials.

   Note:

   - If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
   - If the Collector is in a lower version than 8, the FileWalk credentials will be used.

   In the Group OU area, if required, select Uniquely defined to choose a different OU from that defined in the data source's domain.
9. After configuration is complete, click Install to add the data source.
10. After the data source installation and share detection are completed, in the Shares pane, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. If you chose to monitor selected shares, you can select and register the required shares.

What To Do Next

Now that you're familiar with the deployment steps, it's time to dive into the detailed procedure.

Adding a Qumulo Data Source - Detailed Procedure

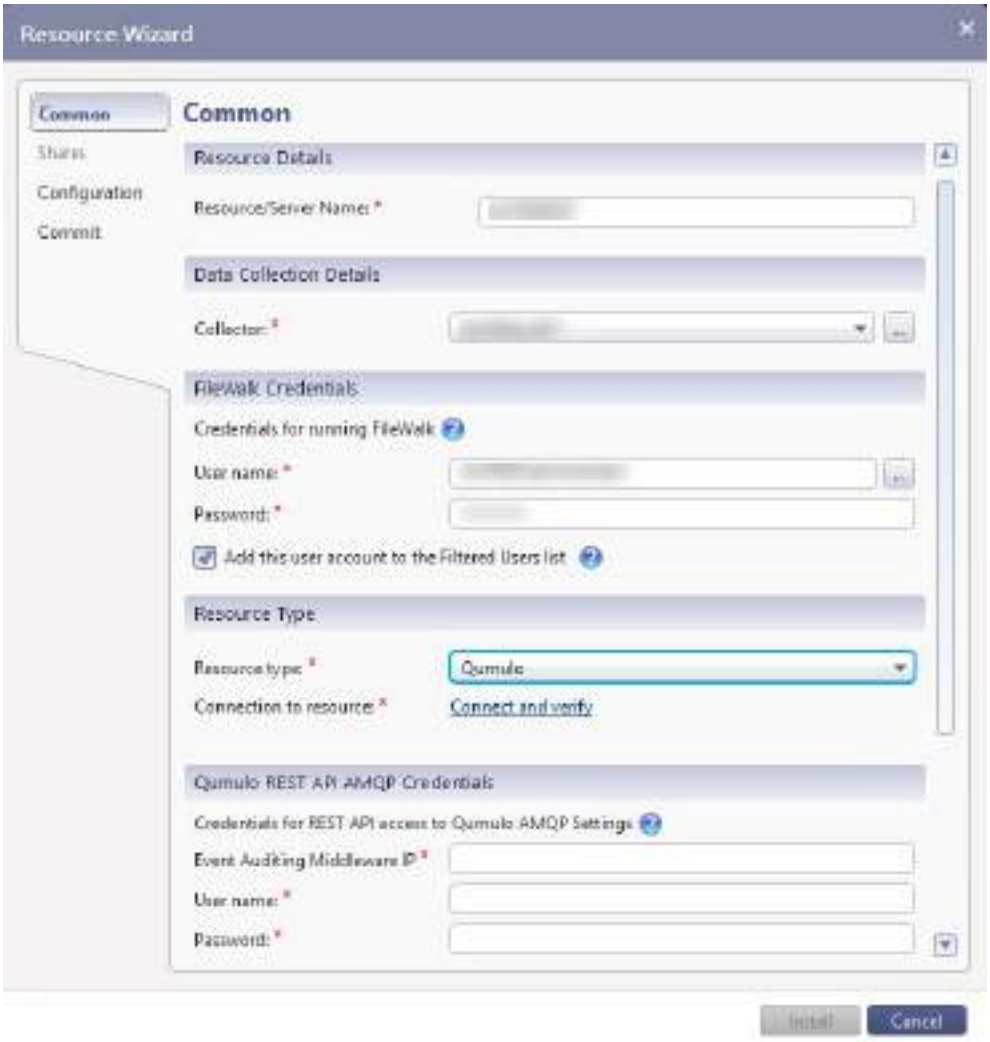
Now that you've configured the REST API Access user, you can deploy a Qumulo data source.

> Note: Each Qumulo data source represents a monitored Qumulo cluster. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source.

1. Set common data source parameters

1. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.

The Resource Wizard is opened to the Common pane, where you can specify the data source and set the relevant parameters.



2. In the Common pane, set the following parameters:
   a. Resource Details - Specify the data source name. Enter the FQDN or IP address of the Qumulo node.
   b. Data Collection Details - Select the relevant Collector (assigned with a certificate) from the dropdown list. For instructions on adding a certificate for a Collector, click here.
   c. FileWalk Credentials - Enter the Qumulo admin credentials for running directory structure monitoring. File System operations include directory structure monitoring, event auditing (if set) and account enumeration on local accounts (if set).

   Note:

- These credentials are cached, so that they are automatically entered if another data source is added during the same session.

- User name - Type the name of the user account to be used for directory structure monitoring, event auditing, and local account enumeration.
- Password - Type the account's password.
- Add this user account to the Filtered Users list - The defined user for FileWalk Credentials will be added to the filtered users list. If you clear this checkbox, a large number of events may be generated by the user defined for directory structure monitoring. It is recommended to keep this checkbox enabled.

Important: You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.

d. Resource Type - Select the data source type from the dropdown list.
   - Connect and verify - Click this link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

     Note:
     - The Connect and verify link is displayed only when all relevant data is entered.
     - A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

e. Qumulo REST API AMQP Credentials - Enter the following credentials required to retrieve information about the file system and audit events:

   Note: Before continuing, verify the configuration in the Qumulo admin console. Follow the steps described in Configuring the Varonis Service Account for Qumulo and Configuring the Qumulo REST API Access User.

   - Event Auditing Middleware IP - Enter the IP of the middleware server, required for event auditing.
   - User name - Insert a REST API user name.
   - Password - Insert a REST API password.
   - Connect and verify - Click this link to verify the credentials that were entered.

f. Monitored Shares - Select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source installed and share detection is completed.

- Automatically monitor detected shares - Select this option to automate monitoring for all detected shares. Share monitoring will automatically start after the data source installation is completed. Varonis will monitor all shares that aren't marked as "ignored". When this option is selected, click the Advanced setting link to modify share detection preferences. By default, the option is set to Prefer regular shares over equivalent admin shares. In this case, an admin share that has an equivalent regular share will be marked as "ignored" and the equivalent regular share will be detected for monitoring. Note: Any change in the monitored shares configuration, including the detection method, admin shares configuration, and selected shares, requires rerunning the resource detection.
- Monitor selected shares - This option is selected by default. You can manually select the shares to be monitored only after the data source is installed and share detection is completed. You'll need to open the Edit window for the installed data source and select the shares. For more information, see Post-installation share detection and registration.

Once the above settings are configured, you can proceed to review and adjust configuration settings.

2. Review and adjust configuration settings

1. On the left menu, click Configuration and confirm the information.
   The general configuration settings are displayed.
2. In the FileWalk Settings area, review the options:
   - Identify actual unique folders and file system inconsistencies - Select this checkbox (if it not already selected) to detect broken permissions in NTFS file systems.
3. In the Event Auditing Parameters area, review the options:
   - Filter out false "File Opened" events - Select this checkbox to filter out false File Open events and collect File Open events only if enough file content is actually read. Small files and certain operations may still trigger Read events.

3. (Optional) Customize commit credentials

You can use different commit credentials instead of the default FileWalk credentials.

1. On the left menu, select Commit.
   The commit settings are displayed.
2. (Optional) Clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials. (By default, this checkbox is selected to use the FileWalk credentials, and the User name and Password fields are disabled for editing.)

   Note:
   - If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
   - If the Collector is in a lower version than 8, the FileWalk credentials will be used.
3. In the Group OU area, if required, select Uniquely defined to choose a different OU from that defined in the data source's domain. Click the Browse button (...) to select the required OU.

4. Install the data source

After configuration is complete, click Install to install the data source.

A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the File Servers pane. When the installation completes, the status shows "Installed 100%".

5. Post-installation share detection and registration

After the data source installation and share detection are completed, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. The following procedure describes the manual registration and automatic share detection flows.

Important: If after the data source is installed, share detection fails for any reason, the Share Detection Status column will remain "In Progress" until the issue is fixed, and share detection completes successfully at least once.

After the data source is installed, the Shares pane is enabled, and you can view the share settings.

1. On the left menu, click Shares.

The share settings are displayed. The pane's heading indicates the option you selected when adding a data source.

2. In the Available Shares area, you can filter the shares based on the reason they are not registered for monitoring and easily identify the shares that can be added. The default filter is Accessible Shares. You can change the filter to see the rest of the shares. Options include:
   - Accessible shares - Can be added for monitoring (this option is selected by default)
   - Ignored shares - Are marked as "ignored"
   - Incompatible and inaccessible shares - Cannot be monitored since the exposed protocol does not match the security style of the volume (relevant to multiprotocol platforms only) or the Varonis service account does not have access to this share
   - Child share of a monitored share - Is monitored via its parent folder
3. Do one of the following:
   - If you chose to monitor selected shares, in the Available Shares area, select the required shares and click the down arrow. The selected shares are moved to the Registered Shares area. (The registered shares list is empty until you make your selections.)
   - If you chose to automatically monitor detected shares, Varonis will monitor all shares that aren't marked as "ignored". The automated share detection runs every few hours. The Registered Shares area is autopopulated with the shares to be monitored.
4. For each share, review and set the following information as required:
   - Ignore Detection - Select the shares to be ignored (and not be the subject of automatic detection and notifications) by the data source monitor.
   - Events - Select this checkbox to audit events for the share.
   - Crawl - To enable or disable monitoring for the share, in the Crawl column, select the relevant option.

     Note: You can also right-click the grid and select the required options for event auditing and crawling.
5. In the Additional Share Settings area, review the options:
   - Remove deleted shares - Select this checkbox to remove deleted shares. Shares that were deleted from the data source will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the data source is unavailable, the shares will not be removed.

- Enable event auditing - Select this checkbox to audit events from all shares added from this data source.

After share detection and registration are completed, the status and number of registered volumes are respectively displayed in the Share Detection Status and Registered Shares columns in the File Servers pane.

What To Do Next

Now let's take a look at the supported events for the monitored Qumulo data sources.

Supported Events For Qumulo Data Sources

SMB (CIFS) Events for Qumulo Data Sources

The monitored data sources and NAS devices support various SMB (CIFS) events.

Event Auditing Method

Qumulo API

Supported File Operations

- File created
- File deleted
- File modified
- File opened
- File renamed
- Folder created
- Folder deleted
- Folder renamed
- File permissions changed
- Folder permissions changed
- Owner changed

Access Denied Events:

- File access denied
- Folder access denied

Note: All CIFS access denied events will arrive as File open denied events.

17 PURE STORAGE FLASHBLADE DATA SOURCES

Note: Private Preview. If you'd like to deploy and monitor Pure Storage FlashBlade data sources, contact your Sales Engineer.

What This Section Contains

This section describes how to deploy and monitor Pure Storage FlashBlade data sources; the requirements, deployment and configuration steps, and supported events.

What To Do Next

Before you dive in, click here to learn more about how Varonis monitors Pure Storage FlashBlade directory structure and permissions, data, and events.

Pure Storage FlashBlade Monitoring Overview

Note: Private Preview. If you'd like to deploy and monitor Pure Storage FlashBlade data sources, contact your Sales Engineer.

Note: Each Pure Storage FlashBlade data source represents a monitored Pure Storage FlashBlade cluster. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source.

About Pure Storage FlashBlade

Pure Storage FlashBlade is an all-flash storage solution designed to handle unstructured data workloads at high speed. It provides a unified platform for file and object storage, enabling organizations to manage and scale data-intensive applications with low latency and high performance. Built by Pure Storage, FlashBlade supports modern data architectures that demand rapid access to large volumes of data, such as analytics, artificial intelligence (AI), machine learning (ML), and large-scale file processing.

How Varonis Monitors Pure Storage Data Sources

Using Syslog, events are sent to the Varonis Collector. There, the events are parsed and handled, and then sent to the Varonis Web Interface.

Varonis monitors Pure Storage FlashBlade:

- Directory structure and permissions
- Data - and classifies it
- Events

Data Classification and Labeling

- Varonis supports data classification and labeling on files that reside in the monitored data sources.

What To Do Next

First, make sure you fulfill the Pure Storage FlashBlade requirements.

Pure Storage FlashBlade Requirements

Note: Private Preview. If you'd like to deploy and monitor Pure Storage FlashBlade data sources, contact your Sales Engineer.

Varonis Service Account

Varonis requires a dedicated service account. The service account can be reused for multiple data source installations and configurations.

- Service Account Read Operations:
  - Traverse and enumerate files, folders, directory structures, users, and groups.
  - Gather data source, user, and group metadata as part of normal system operations.
- Service Account Write Operations:
  - Used for executing Varonis Policies, if policies are defined.

Deployment Requirements

- Pure Storage token credentials are required to add Pure Storage data sources to the Management Console.
- Deploy a Collector that resides within LAN proximity to the monitored Pure Storage cluster.
- Provide the DNS name that represents the IP pool of the cluster nodes (recommended for better resilience) or the IP address or hostname of a specific node.
- Member of AD groups that allow event auditing.

What To Do Next

Now that you've fulfilled the requirements, proceed to configure the Varonis service account for Pure Storage FlashBlade.

Configuring the Varonis Service Account for Pure Storage FlashBlade

Before you add Pure Storage FlashBlade data sources, you need to configure the Varonis service account.

Note: Private Preview. If you'd like to deploy and monitor Pure Storage FlashBlade data sources, contact your Sales Engineer.

Requirements for the Varonis Service Account for Read Operations

Note:

- The Varonis service account must be a domain user from the primary domain.
- The Varonis service account must be a part of the backup operators group.

Requirements for the Varonis Service Account for Write Operations

In addition to the requirements for the read operations, the Varonis service account for write operations requires the Audit Operator and Backup Operator roles.

What To Do Next

Now that you've configured the Varonis service account for Pure Storage FlashBlade, it's time to add a monitored Pure Storage FlashBlade data source. First familiarize yourself with the deployment steps summary and then dive into the detailed procedure.

Adding a Pure Storage FlashBlade Data Source - Summary

Now that you've configured the Varonis service account, you can deploy a Pure Storage FlashBlade data source. This section summarizes the procedure for deploying Pure Storage FlashBlade data sources.

Note: Private Preview. If you'd like to deploy and monitor Pure Storage FlashBlade data sources, contact your Sales Engineer.

1. Run the Management Console as an administrator.
2. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.
3. In the Resource Wizard's Common pane, in the Resource Details area, enter the FQDN or IP address of the Pure Storage FlashBlade node, the validity of which can be verified by trying to access it via SMB (CIFS). Then, check the Collector

selected by default and change it if needed, and enter the Pure Storage FlashBlade admin credentials for running directory structure monitoring (FileWalk).

> Important: You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.

4. In the Resource Type area, select the data source type from the dropdown list. Then, click the Connect and verify link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

> Note:
>
> - The Connect and verify link is displayed only when all relevant data is entered.
> - A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

> Important: Before continuing, verify the configuration in the Pure Storage FlashBlade admin console. Follow the steps described in Configuring the Varonis Service Account for Pure Storage FlashBlade.

5. In the Affiliated Domain area, select the domain associated with the Pure Storage data source from the dropdown list.
6. In the Pure Storage FlashBlade REST API Credentials area, enter the REST API credentials required to retrieve information about the file system and audit events. Then, click the Connect and verify link to verify the credentials that were entered.

> Note: Insert a REST API token retrieved from the data source using the CLI command.

7. In the Monitored Shares area, select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source is installed and share detection is completed.
8. In the Configuration pane, review the FileWalk Settings and Event Auditing Parameters settings.
9. (Optional) In the Commit pane, clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials.

Note:

- If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
- If the Collector is in a lower version than 8, the FileWalk credentials will be used.

In the Group OU area, if required, select Uniquely defined to choose a different OU from that defined in the data source's domain.

10. After configuration is complete, click Install to add the data source.
11. After the data source installation and share detection are completed, in the Shares pane, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. If you chose to monitor selected shares, you can select and register the required shares.

What To Do Next

Now that you're familiar with the deployment steps, it's time to dive into the detailed procedure.

Adding a Pure Storage FlashBlade Data Source - Detailed Procedure

Now that you've configured the REST API Access user, you can deploy a Pure Storage FlashBlade data source.

Note: Private Preview. If you'd like to deploy and monitor Pure Storage FlashBlade data sources, contact your Sales Engineer.

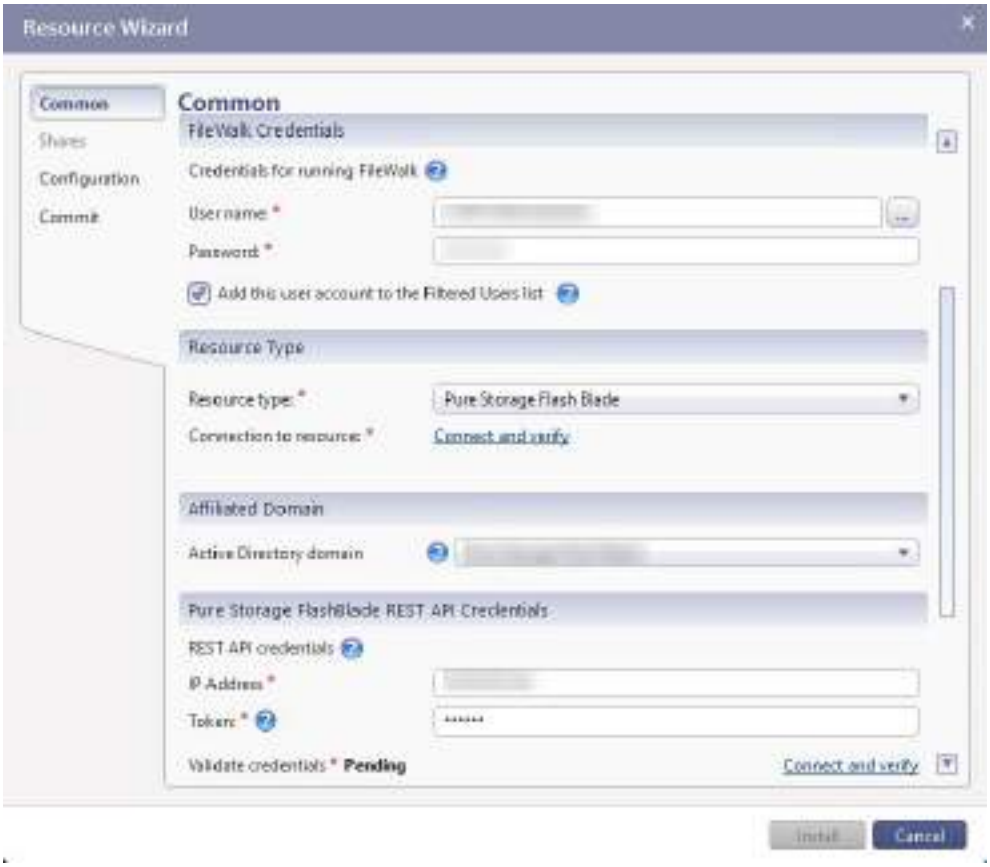
Note: Each Pure Storage FlashBlade data source represents a monitored Pure Storage FlashBlade cluster. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source.

Note: Before you install Pure Storage data source, you must first add a domain affiliated with the data source.

1. Set common data source parameters

1. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.

The Resource Wizard is opened to the Common pane, where you can specify the data source and set the relevant parameters.



2. In the Common pane, set the following parameters:
   a. Resource Details - Specify the data source name. Enter the FQDN or IP address of the Pure Storage FlashBlade node, the validity of which can be verified by trying to access it via SMB (CIFS).
   b. Data Collection Details - Select the relevant Collector from the dropdown list.
   c. FileWalk Credentials - Enter the Pure Storage FlashBlade admin credentials for running directory structure monitoring. File System operations include directory structure monitoring, event auditing (if set) and account enumeration on local accounts (if set).

      Note:
      - These credentials are cached, so that they are automatically entered if another data source is added during the same session.

      - User name - Type the name of the user account to be used for directory structure monitoring, event auditing, and local account enumeration.
      - Password - Type the account's password.

- Add this user account to the Filtered Users list - The defined user for FileWalk Credentials will be added to the filtered users list. If you clear this checkbox, a large number of events may be generated by the user defined for directory structure monitoring. It is recommended to keep this checkbox enabled.

> Important: You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.

d. Resource Type - Select the data source type from the dropdown list.
   - Connect and verify - Click this link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

     > Note:
     > - The Connect and verify link is displayed only when all relevant data is entered.
     > - A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

e. Affiliated Domain - Select the domain associated with the Pure Storage data source from the dropdown list.
f. Pure Storage FlashBlade REST API Credentials - Enter the following credentials required to retrieve information about the file system and audit events:

   > Note: Before continuing, verify the configuration in the Pure Storage FlashBlade admin console. Follow the steps described in Configuring the Varonis Service Account for Pure Storage FlashBlade.

   - IP Address - Enter the IP of the server required for event auditing.
   - Token - Insert a REST API token retrieved from the data source using the CLI command.
   - Connect and verify - Click this link to verify the credentials that were entered.

g. Monitored Shares - Select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source installed and share detection is completed.
   - Automatically monitor detected shares - Select this option to automate monitoring for all detected shares. Share monitoring will automatically start

after the data source installation is completed. Varonis will monitor all shares that aren't marked as "ignored". When this option is selected, click the Advanced setting link to modify share detection preferences. By default, the option is set to Prefer regular shares over equivalent admin shares. In this case, an admin share that has an equivalent regular share will be marked as "ignored" and the equivalent regular share will be detected for monitoring. Note: Any change in the monitored shares configuration, including the detection method, admin shares configuration, and selected shares, requires rerunning the resource detection.

- Monitor selected shares - This option is selected by default. You can manually select the shares to be monitored only after the data source is installed and share detection is completed. You'll need to open the Edit window for the installed data source and select the shares. For more information, see Post-installation share detection and registration.

Once the above settings are configured, you can proceed to review and adjust configuration settings.

2. Review and adjust configuration settings

1. On the left menu, click Configuration and confirm the information.
   The general configuration settings are displayed.
2. In the FileWalk Settings area, review the options:
   - Identify actual unique folders and file system inconsistencies - Select this checkbox (if it not already selected) to detect broken permissions in NTFS file systems.
3. In the Event Auditing Parameters area, review the options:
   - Filter out false "File Opened" events - Select this checkbox to filter out false File Open events and collect File Open events only if enough file content is actually read. Small files and certain operations may still trigger Read events.

3. (Optional) Customize commit credentials

You can use different commit credentials instead of the default FileWalk credentials.

1. On the left menu, select Commit.
   The commit settings are displayed.
2. (Optional) Clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials. (By default, this checkbox is selected to use the

FileWalk credentials, and the User name and Password fields are disabled for editing.)

Note:

- If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
- If the Collector is in a lower version than 8, the FileWalk credentials will be used.

3. In the Group OU area, if required, select Uniquely defined to choose a different OU from that defined in the data source's domain. Click the Browse button (...) to select the required OU.

4. Install the data source

After configuration is complete, click Install to install the data source.

A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the File Servers pane. When the installation completes, the status shows "Installed 100%".

5. Post-installation share detection and registration

After the data source installation and share detection are completed, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. The following procedure describes the manual registration and automatic share detection flows.

Important: If after the data source is installed, share detection fails for any reason, the Share Detection Status column will remain "In Progress" until the issue is fixed, and share detection completes successfully at least once.

After the data source is installed, the Shares pane is enabled, and you can view the share settings.

1. On the left menu, click Shares.
   The share settings are displayed. The pane's heading indicates the option you selected when adding a data source.
2. In the Available Shares area, you can filter the shares based on the reason they are not registered for monitoring and easily identify the shares that can be added. The default filter is Accessible Shares. You can change the filter to see the rest of the shares. Options include:

- Accessible shares - Can be added for monitoring (this option is selected by default)
- Ignored shares - Are marked as "ignored"
- Incompatible and inaccessible shares - Cannot be monitored since the exposed protocol does not match the security style of the volume (relevant to multiprotocol platforms only) or the Varonis service account does not have access to this share
- Child share of a monitored share - Is monitored via its parent folder

3. Do one of the following:
   - If you chose to monitor selected shares, in the Available Shares area, select the required shares and click the down arrow. The selected shares are moved to the Registered Shares area. (The registered shares list is empty until you make your selections.)
   - If you chose to automatically monitor detected shares, Varonis will monitor all shares that aren't marked as "ignored". The automated share detection runs every few hours. The Registered Shares area is autopopulated with the shares to be monitored.
4. For each share, review and set the following information as required:
   - Ignore Detection - Select the shares to be ignored (and not be the subject of automatic detection and notifications) by the data source monitor.
   - Events - Select this checkbox to audit events for the share.
   - Crawl - To enable or disable monitoring for the share, in the Crawl column, select the relevant option.

     Note: You can also right-click the grid and select the required options for event auditing and crawling.
5. In the Additional Share Settings area, review the options:
   - Remove deleted shares - Select this checkbox to remove deleted shares. Shares that were deleted from the data source will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the data source is unavailable, the shares will not be removed.
   - Enable event auditing - Select this checkbox to audit events from all shares added from this data source.

   After share detection and registration are completed, the status and number of registered volumes are respectively displayed in the Share Detection Status and Registered Shares columns in the File Servers pane.

What To Do Next

Now let's take a look at the supported events for the monitored Pure Storage FlashBlade data sources.

Supported Events For Pure Storage FlashBlade Data Sources

Note: Private Preview. If you'd like to deploy and monitor Pure Storage FlashBlade data sources, contact your Sales Engineer.

SMB (CIFS) Events for Pure Storage FlashBlade Data Sources

The monitored data sources and NAS devices support various SMB (CIFS) events.

Event Auditing Method

Syslog

Supported File Operations

- File created
- File deleted
- File modified
- File opened
- File renamed
- Folder created
- Folder deleted
- Folder renamed
- File permissions changed
- Folder permissions changed

18 PURE STORAGE FLASHARRAY DATA SOURCES

Note: Private Preview. If you'd like to deploy and monitor Pure Storage FlashArray data sources, contact your Sales Engineer.

What This Section Contains

This section describes how to deploy and monitor Pure Storage FlashArray data sources; the requirements, deployment and configuration steps, and supported events.

What To Do Next

Before you dive in, click here to learn more about how Varonis monitors Pure Storage FlashArray directory structure and permissions, data, and events.

Pure Storage FlashArray Monitoring Overview

Note: Private Preview. If you'd like to deploy and monitor Pure Storage FlashArray data sources, contact your Sales Engineer.

Note: Each Pure Storage FlashArray data source represents a monitored Pure Storage FlashArray cluster. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source.

About Pure Storage FlashArray

Pure Storage FlashArray is a high-performance, all-flash storage solution designed to accelerate mission-critical applications with power and efficiency. It provides a unified platform for both block and file storage, simplifying data management and increasing flexibility. With enterprise-level performance, reliability, and availability, it is ideal for critical business services. FlashArray features non-disruptive upgrades through Pure Storage's Evergreen architecture, ensuring continuous operation. It includes advanced data protection features like always-on encryption and SafeMode for ransomware protection. Additionally, it offers significant performance boosts, increased memory speeds, high data reduction rates, and energy efficiency, making it a powerful and efficient choice for modern data centers and enterprise environments.

How Varonis Monitors Pure Storage Data Sources

Using Syslog, events are sent to the Varonis Collector. There, the events are parsed and handled, and then sent to the Varonis Web Interface.

Varonis monitors Pure Storage FlashArray:

- Directory structure and permissions
- Data - and classifies it
- Events

Data Classification and Labeling

- Varonis supports data classification and labeling on files that reside in the monitored data sources.

What To Do Next

First, make sure you fulfill the Pure Storage FlashArray requirements.

Pure Storage FlashArray Requirements

> Note: Private Preview. If you'd like to deploy and monitor Pure Storage FlashArray data sources, contact your Sales Engineer.

Varonis Service Account

Varonis requires a dedicated service account. The service account can be reused for multiple data source installations and configurations.

- Service Account Read Operations:
  - Traverse and enumerate files, folders, directory structures, users, and groups.
  - Gather data source, user, and group metadata as part of normal system operations.
- Service Account Write Operations:
  - Used for executing Varonis Policies, if policies are defined.

Deployment Requirements

- The Varonis service account requires the Backup Operator role within the Pure Storage FlashArray Console. For more information, see Configuring the Varonis Service Account for Pure Storage FlashArray.
- Pure Storage token credentials are required to add Pure Storage data sources to the Management Console.
- Deploy a Collector that resides within LAN proximity to the monitored Pure Storage cluster.
- Provide the DNS name that represents the IP pool of the cluster nodes (recommended for better resilience) or the IP address or hostname of a specific node.

What To Do Next

Now that you've fulfilled the requirements, proceed to configure the Varonis service account for Pure Storage FlashArray.

Configuring the Varonis Service Account for Pure Storage FlashArray

Before you add Pure Storage FlashArray data sources, you need to configure the Varonis service account.

> Note: Private Preview. If you'd like to deploy and monitor Pure Storage FlashArray data sources, contact your Sales Engineer.

Requirements for the Varonis Service Account for Read Operations

> Note:
>
> - The Varonis service account must be a domain user from the primary domain.
> - The Varonis service account must be a part of the Backup Operators group.

1. In the Pure Storage FlashArray Console. go to Settings > Access > File Services > Backup Operators > Add External Members. Take note of the service account user you wish to use.
2. (Optional) Add the user to the Audit Operators group to change ACLs. If no user is added, Varonis will monitor only the default event types.

Requirements for the Varonis Service Account for Write Operations

In addition to the requirements for the read operations, the Varonis service account for write operations requires the Audit Operator and Backup Operator roles.

What To Do Next

Now that you've configured the Varonis service account for Pure Storage FlashArray, it's time to add a monitored Pure Storage FlashArray data source. First familiarize yourself with the deployment steps summary and then dive into the detailed procedure.

Adding a Pure Storage FlashArray Data Source - Summary

Now that you've configured the Varonis service account, you can deploy a Pure Storage FlashArray data source. This section summarizes the procedure for deploying Pure Storage FlashArray data sources.

Note: Private Preview. If you'd like to deploy and monitor Pure Storage FlashArray data sources, contact your Sales Engineer.

1. Run the Management Console as an administrator.
2. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.
3. In the Resource Wizard's Common pane, in the Resource Details area, enter the FQDN or IP address of the Pure Storage FlashArray node, the validity of which can be verified by trying to access it via SMB (CIFS). Then, check the Collector selected by default and change it if needed, and enter the Pure Storage FlashArray admin credentials for running directory structure monitoring (FileWalk).

   Important: You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.

4. In the Resource Type area, select the data source type from the dropdown list. Then, click the Connect and verify link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

   Note:

   - The Connect and verify link is displayed only when all relevant data is entered.
   - A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

   Important: Before continuing, verify the configuration in the Pure Storage FlashArray admin console. Follow the steps described in Configuring the Varonis Service Account for Pure Storage FlashArray.

5. In the Affiliated Domain area, select the domain associated with the Pure Storage data source from the dropdown list.

6. In the Pure Storage FlashArray REST API Credentials area, enter the REST API credentials required to retrieve information about the file system and audit events. Then, click the Connect and verify link to verify the credentials that were entered.

   Note: Insert a REST API token retrieved from the data source using the CLI command.

7. In the Monitored Shares area, select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source is installed and share detection is completed.
8. In the Configuration pane, review the FileWalk Settings and Event Auditing Parameters settings.
9. (Optional) In the Commit pane, clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials.

   Note:

   - If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
   - If the Collector is in a lower version than 8, the FileWalk credentials will be used.

   In the Group OU area, if required, select Uniquely defined to choose a different OU from that defined in the data source's domain.
10. After configuration is complete, click Install to add the data source.
11. After the data source installation and share detection are completed, in the Shares pane, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. If you chose to monitor selected shares, you can select and register the required shares.

What To Do Next

Now that you're familiar with the deployment steps, it's time to dive into the detailed procedure.

Adding a Pure Storage FlashArray Data Source - Detailed Procedure

Now that you've configured the REST API Access user, you can deploy a Pure Storage FlashArray data source.

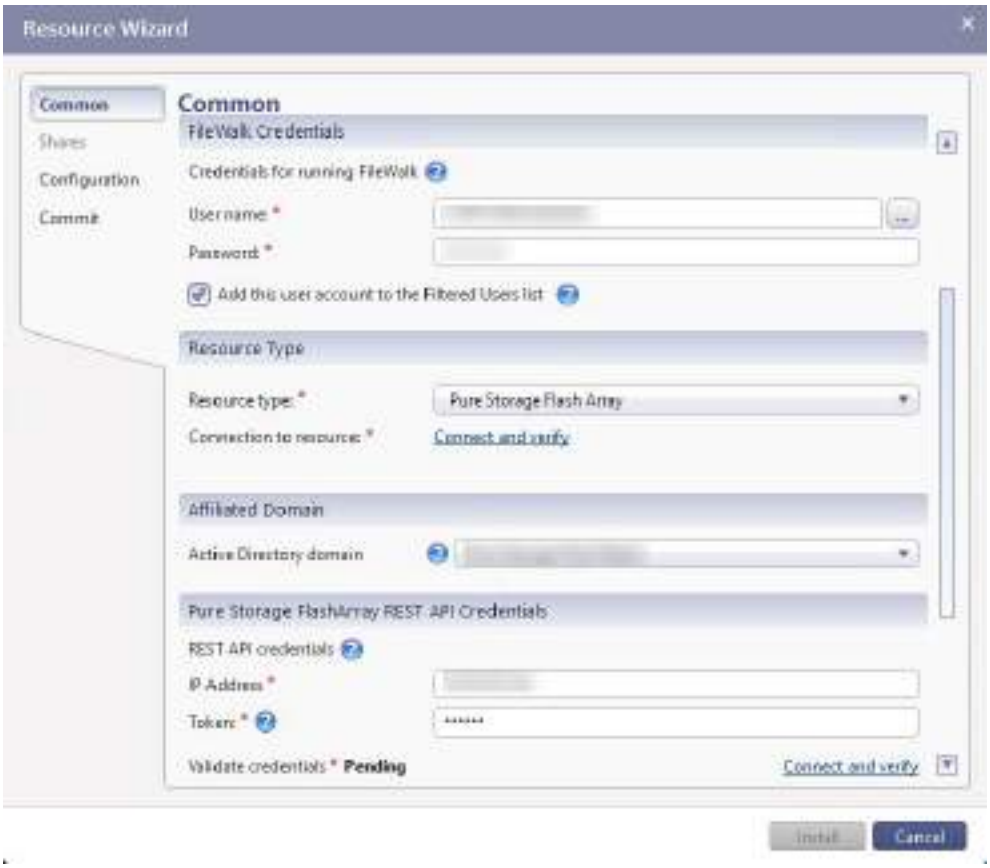
Note: Private Preview. If you'd like to deploy and monitor Pure Storage FlashArray data sources, contact your Sales Engineer.

Note: Each Pure Storage FlashArray data source represents a monitored Pure Storage FlashArray cluster. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source.

Note: Before you install Pure Storage data source, you must first add a domain affiliated with the data source.

1. Set common data source parameters

1. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.
   The Resource Wizard is opened to the Common pane, where you can specify the data source and set the relevant parameters.



2. In the Common pane, set the following parameters:
   a. Resource Details - Specify the data source name. Enter the FQDN or IP address of the Pure Storage FlashArray node, the validity of which can be verified by trying to access it via SMB (CIFS).
   b. Data Collection Details - Select the relevant Collector from the dropdown list.
   c. FileWalk Credentials - Enter the Pure Storage FlashArray admin credentials for running directory structure monitoring. File System operations include directory structure monitoring, event auditing (if set) and account enumeration on local accounts (if set).

      Note:
      - These credentials are cached, so that they are automatically entered if another data source is added during the same session.

      - User name - Type the name of the user account to be used for directory structure monitoring, event auditing, and local account enumeration.
      - Password - Type the account's password.
      - Add this user account to the Filtered Users list - The defined user for FileWalk Credentials will be added to the filtered users list. If you clear this checkbox, a large number of events may be generated by the user defined for directory structure monitoring. It is recommended to keep this checkbox enabled.

      Important: You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.

   d. Resource Type - Select the data source type from the dropdown list.
      - Connect and verify - Click this link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

        Note:
        - The Connect and verify link is displayed only when all relevant data is entered.
        - A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

   e. Affiliated Domain - Select the domain associated with the Pure Storage data source from the dropdown list.

f. Pure Storage FlashArray REST API Credentials - Enter the following credentials required to retrieve information about the file system and audit events:

> Note: Before continuing, verify the configuration in the Pure Storage FlashArray admin console. Follow the steps described in Configuring the Varonis Service Account for Pure Storage FlashArray.

- IP Address - Enter the IP of the server, required for event auditing.
- Token - Insert a REST API token. Retrieve the token from the data source using a CLI command.
- Connect and verify - Click this link to verify the credentials that were entered.

g. Monitored Shares - Select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source installed and share detection is completed.

- Automatically monitor detected shares - Select this option to automate monitoring for all detected shares. Share monitoring will automatically start after the data source installation is completed. Varonis will monitor all shares that aren't marked as "ignored". When this option is selected, click the Advanced setting link to modify share detection preferences. By default, the option is set to Prefer regular shares over equivalent admin shares. In this case, an admin share that has an equivalent regular share will be marked as "ignored" and the equivalent regular share will be detected for monitoring. Note: Any change in the monitored shares configuration, including the detection method, admin shares configuration, and selected shares, requires rerunning the resource detection.
- Monitor selected shares - This option is selected by default. You can manually select the shares to be monitored only after the data source is installed and share detection is completed. You'll need to open the Edit window for the installed data source and select the shares. For more information, see Post-installation share detection and registration.

Once the above settings are configured, you can proceed to review and adjust configuration settings.

2. Review and adjust configuration settings

1. On the left menu, click Configuration and confirm the information.
   The general configuration settings are displayed.
2. In the FileWalk Settings area, review the options:

- Identify actual unique folders and file system inconsistencies - Select this checkbox (if it not already selected) to detect broken permissions in NTFS file systems.

3. In the Event Auditing Parameters area, review the options:
   - Filter out false "File Opened" events - Select this checkbox to filter out false File Open events and collect File Open events only if enough file content is actually read. Small files and certain operations may still trigger Read events.

3. (Optional) Customize commit credentials

You can use different commit credentials instead of the default FileWalk credentials.

1. On the left menu, select Commit.
   The commit settings are displayed.
2. (Optional) Clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials. (By default, this checkbox is selected to use the FileWalk credentials, and the User name and Password fields are disabled for editing.)

   Note:
   - If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
   - If the Collector is in a lower version than 8, the FileWalk credentials will be used.

3. In the Group OU area, if required, select Uniquely defined to choose a different OU from that defined in the data source's domain. Click the Browse button (...) to select the required OU.

4. Install the data source

After configuration is complete, click Install to install the data source.

A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the File Servers pane. When the installation completes, the status shows "Installed 100%".

5. Post-installation share detection and registration

After the data source installation and share detection are completed, you can select the shares to be monitored. If, when adding the data source, you chose to automate

monitoring for detected shares, all shares will be monitored. The following procedure describes the manual registration and automatic share detection flows.

> Important: If after the data source is installed, share detection fails for any reason, the Share Detection Status column will remain "In Progress" until the issue is fixed, and share detection completes successfully at least once.

After the data source is installed, the Shares pane is enabled, and you can view the share settings.

1. On the left menu, click Shares.
   The share settings are displayed. The pane's heading indicates the option you selected when adding a data source.
2. In the Available Shares area, you can filter the shares based on the reason they are not registered for monitoring and easily identify the shares that can be added. The default filter is Accessible Shares. You can change the filter to see the rest of the shares. Options include:
   - Accessible shares - Can be added for monitoring (this option is selected by default)
   - Ignored shares - Are marked as "ignored"
   - Incompatible and inaccessible shares - Cannot be monitored since the exposed protocol does not match the security style of the volume (relevant to multiprotocol platforms only) or the Varonis service account does not have access to this share
   - Child share of a monitored share - Is monitored via its parent folder
3. Do one of the following:
   - If you chose to monitor selected shares, in the Available Shares area, select the required shares and click the down arrow. The selected shares are moved to the Registered Shares area. (The registered shares list is empty until you make your selections.)
   - If you chose to automatically monitor detected shares, Varonis will monitor all shares that aren't marked as "ignored". The automated share detection runs every few hours. The Registered Shares area is autopopulated with the shares to be monitored.
4. For each share, review and set the following information as required:
   - Ignore Detection - Select the shares to be ignored (and not be the subject of automatic detection and notifications) by the data source monitor.
   - Events - Select this checkbox to audit events for the share.

- Crawl - To enable or disable monitoring for the share, in the Crawl column, select the relevant option.

  Note: You can also right-click the grid and select the required options for event auditing and crawling.

5. In the Additional Share Settings area, review the options:
   - Remove deleted shares - Select this checkbox to remove deleted shares. Shares that were deleted from the data source will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the data source is unavailable, the shares will not be removed.
   - Enable event auditing - Select this checkbox to audit events from all shares added from this data source.

   After share detection and registration are completed, the status and number of registered volumes are respectively displayed in the Share Detection Status and Registered Shares columns in the File Servers pane.

What To Do Next

Now let's take a look at the supported events for the monitored Pure Storage FlashArray data sources.

Supported Events For Pure Storage FlashArray Data Sources

Note: Private Preview. If you'd like to deploy and monitor Pure Storage FlashArray data sources, contact your Sales Engineer.

SMB (CIFS) Events for Pure Storage FlashArray Data Sources

The monitored data sources and NAS devices support various SMB (CIFS) events.

Event Auditing Method

Syslog

Supported File Operations

- File created
- File deleted
- File modified

- File opened
- File renamed
- Folder created
- Folder deleted
- Folder renamed
- File permissions changed
- Folder permissions changed

19 VAST DATA SOURCES

Note: Private Preview. If you'd like to deploy and monitor VAST data sources, contact your Sales Engineer.

What This Section Contains

This section describes how to deploy and monitor VAST data sources; the requirements, deployment and configuration steps, and supported events.

What To Do Next

Before you dive in, click here to learn more about how Varonis monitors VAST directory structure and permissions, data, and events.

VAST Monitoring Overview

Note: Private Preview. If you'd like to deploy and monitor VAST data sources, contact your Sales Engineer.

Note: Each VAST data source represents a monitored VAST cluster. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source.

About VAST

VAST Management System is a comprehensive data platform designed to handle the complexities of modern data management by integrating databases, data warehouses, and data lakes into a single system. It offers scalability from edge to cloud with a global high-performance namespace and utilizes an affordable all-flash storage tier to eliminate the need for data tiering. Additionally, its DataEngine feature transforms unstructured data into structured, searchable information, making it particularly beneficial for organizations that manage large volumes of unstructured data, especially in AI and big data analytics contexts.

How Varonis Monitors Data Sources

VAST provides dedicated REST API to retrieve event data.

To authenticate as part of the installation, Varonis needs to obtain:

- Management host (can be either an IP address or a hostname)
- VMS Manager username and password

Varonis monitors VAST:

- Directory structure and permissions
- Data - and classifies it
- Events

Data Classification and Labeling

- Varonis supports data classification and labeling on files that reside in the monitored data sources.

What To Do Next

First, make sure you fulfill the VAST requirements.

VAST Requirements

Note: Private Preview. If you'd like to deploy and monitor VAST data sources, contact your Sales Engineer.

Varonis Service Account

Varonis requires a dedicated service account. The service account can be reused for multiple data source installations and configurations.

- Service Account Read Operations:
  - Traverse and enumerate files, folders, directory structures, users, and groups.
  - Gather data source, user, and group metadata as part of normal system operations.
- Service Account Write Operations:
  - Used for executing Varonis Policies, if policies are defined.

Deployment Requirements

- By default, in VAST, all domain users have access to all views. However, you can add individual limitations for each view. To avoid this and allow a user to scan all views, VAST allows us to define a Backup Operator user.
- The Varonis service account requires the Backup Operator role within the VAST Console. For more information, see Configuring the Varonis Service Account for VAST.
- VMS credentials are required to add data sources to the Management Console.
- Deploy a Collector that resides within LAN proximity to the monitored cluster.

Notes

- VAST supports case-sensitive shares; Varonis does not.

What To Do Next

Now that you've fulfilled the requirements, proceed to configure the Varonis service account for VAST.

Configuring the Varonis Service Account for VAST

Before you add VAST data sources, you need to configure the Varonis service account.

Note: Private Preview. If you'd like to deploy and monitor VAST data sources, contact your Sales Engineer.

Requirements for the Varonis Service Account for Read Operations

Note:

- The Varonis service account must be a domain user from the primary domain.
- The Varonis service account must be a part of the Backup Operators group.

You need to create a new group on the domain controller and assign it in the VAST portal as a Backup Operator.

1. In the VAST Console, go to Element Store > Tenant.
2. Edit the relevant tenant.
3. Enable the Enable privileged domain group backup access option.
4. Enter the SID of the group.

Requirements for the Varonis Service Account for Write Operations

The Varonis service account requires REST API user permissions.

What To Do Next

Now proceed to configure the VAST REST API user.

Configuring the VAST REST API Access User

Before you add VAST data sources, you need to configure the VAST Rest API access user. Select one of the following options.

Option 1: VAST Manager User

1. In the VAST Web UI, go to Administrator > Roles.
2. Create a new role with Realm: Logical + Create + View permissions.
3. Assign this role to an administrator user (Administrator > Users).

Option 2: Active Directory User

1. Create a new group on the Domain Controller (DC) and assign the relevant user to this group.
2. In the VAST Web UI, go to Administrator > Roles.
3. Create a new role with Realm: Logical + Create + View permissions.
4. Assign this role to the new AD group.
5. Go to User Management > Active Directory.
6. Select the relevant AD and click Edit.
7. Go to Advanced and enable VMS Auth provider.

What To Do Next

Now that you've configured the VAST REST API access user, it's time to add a monitored VAST data source. First familiarize yourself with the deployment steps summary and then dive into the detailed procedure.

Adding a VAST Data Source - Summary

Now that you've configured the Varonis service account, you can deploy a VAST data source. This section summarizes the procedure for deploying VAST data sources.

> Note: Private Preview. If you'd like to deploy and monitor VAST data sources, contact your Sales Engineer.

1. Run the Management Console as an administrator.

2. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.
3. In the Resource Wizard's Common pane, in the Resource Details area, enter the FQDN or IP address of the VAST node. Then, check the Collector selected by default and change it if needed, and enter the VAST admin credentials for running directory structure monitoring (FileWalk).

   Important: You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.

4. In the Resource Type area, select the data source type from the dropdown list. Then, click the Connect and verify link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

   Note:

   - The Connect and verify link is displayed only when all relevant data is entered.
   - A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

   Important: Before continuing, verify the configuration in the VAST admin console. Follow the steps described in Configuring the Varonis Service Account for VAST.

5. In the Event Auditing area, enter the VMS manager host and user credentials required to access the VMS API, retrieve information about the file system, and audit events. Then, click the Verify event auditing connection link to validate the VMS credentials, retrieve the dedicated data source version, and enable adding the data source to the Management Console.
6. In the Monitored Shares area, select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source is installed and share detection is completed.
7. In the Configuration pane, review the FileWalk Settings and Event Auditing Parameters settings.
8. (Optional) In the Commit pane, clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials.

Note:

- If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
- If the Collector is in a lower version than 8, the FileWalk credentials will be used.

In the Group OU area, if required, select Uniquely defined to choose a different OU from that defined in the data source's domain.

9. After configuration is complete, click Install to add the data source.
10. After the data source installation and share detection are completed, in the Shares pane, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. If you chose to monitor selected shares, you can select and register the required shares.

What To Do Next

Now that you're familiar with the deployment steps, it's time to dive into the detailed procedure.

Adding a VAST Data Source - Detailed Procedure

Now that you've configured the REST API Access user, you can deploy a VAST data source.

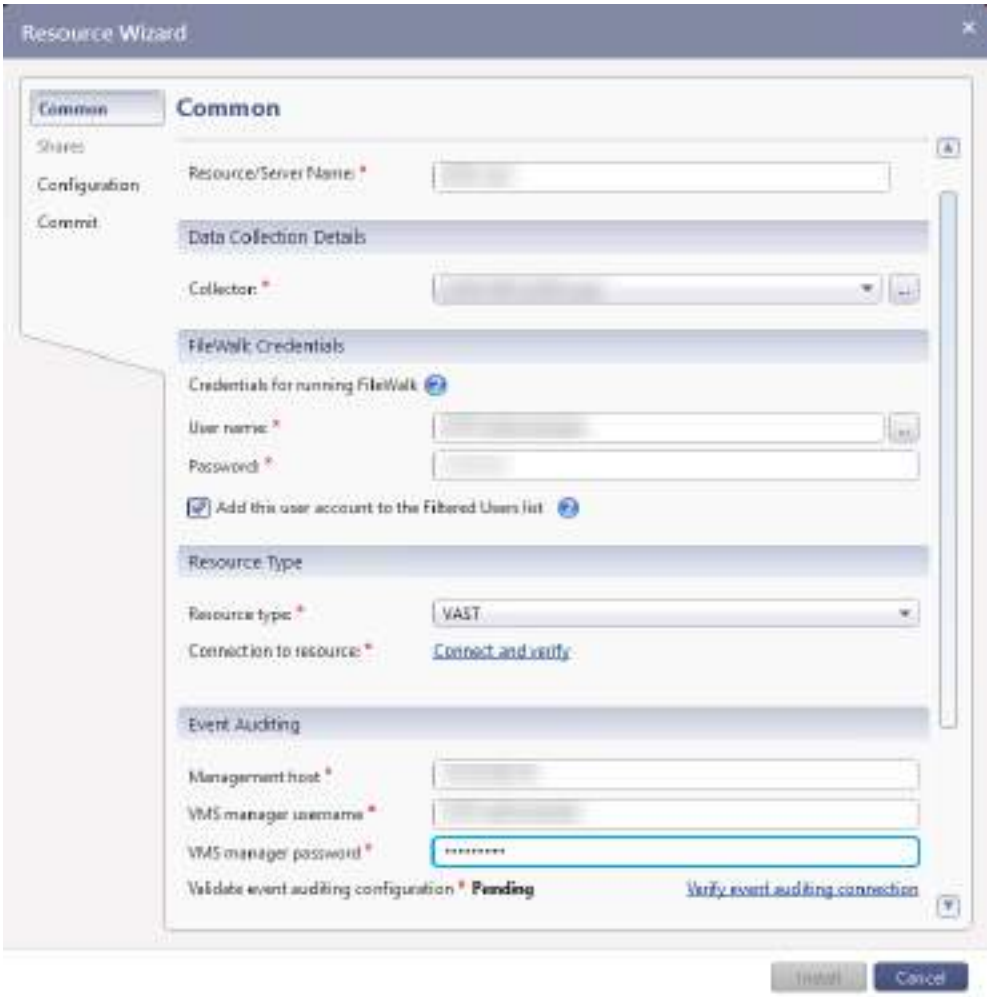
Note: Private Preview. If you'd like to deploy and monitor VAST data sources, contact your Sales Engineer.

Note: Each VAST data source represents a monitored VAST cluster. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source.

1. Set common data source parameters

1. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.

The Resource Wizard is opened to the Common pane, where you can specify the data source and set the relevant parameters.



2. In the Common pane, set the following parameters:
   a. Resource Details - Specify the data source name. Enter the FQDN or IP address of the VAST node.
   b. Data Collection Details - Select the relevant Collector from the dropdown list.
   c. FileWalk Credentials - Enter the VAST admin credentials for running directory structure monitoring. File System operations include directory structure monitoring, event auditing (if set) and account enumeration on local accounts (if set).

   Note:
   - These credentials are cached, so that they are automatically entered if another data source is added during the same session.

- User name - Type the name of the user account to be used for directory structure monitoring, event auditing, and local account enumeration.
- Password - Type the account's password.
- Add this user account to the Filtered Users list - The defined user for FileWalk Credentials will be added to the filtered users list. If you clear this checkbox, a large number of events may be generated by the user defined for directory structure monitoring. It is recommended to keep this checkbox enabled.

Important: You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.

d. Resource Type - Select the data source type from the dropdown list.
   - Connect and verify - Click this link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

     Note:
     - The Connect and verify link is displayed only when all relevant data is entered.
     - A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

e. Event Auditing - Enter the following credentials required to access the VMS API, retrieve information about the file system, and audit events:
   - Management Host
   - VMS manager username
   - VMS manager password
   - Verify event auditing connection - Click this link to validate the VMS credentials, retrieve the dedicated data source version, and enable adding the data source to the Management Console.

f. Monitored Shares - Select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source installed and share detection is completed.
   - Automatically monitor detected shares - Select this option to automate monitoring for all detected shares. Share monitoring will automatically start after the data source installation is completed. Varonis will monitor all shares

that aren't marked as "ignored". When this option is selected, click the Advanced setting link to modify share detection preferences. By default, the option is set to Prefer regular shares over equivalent admin shares. In this case, an admin share that has an equivalent regular share will be marked as "ignored" and the equivalent regular share will be detected for monitoring. Note: Any change in the monitored shares configuration, including the detection method, admin shares configuration, and selected shares, requires rerunning the resource detection.

- Monitor selected shares - This option is selected by default. You can manually select the shares to be monitored only after the data source is installed and share detection is completed. You'll need to open the Edit window for the installed data source and select the shares. For more information, see Post-installation share detection and registration.

Once the above settings are configured, you can proceed to review and adjust configuration settings.

2. Review and adjust configuration settings

1. On the left menu, click Configuration and confirm the information.
   The general configuration settings are displayed.
2. In the FileWalk Settings area, review the options:
   - Identify actual unique folders and file system inconsistencies - Select this checkbox (if it not already selected) to detect broken permissions in NTFS file systems.
3. In the Event Auditing Parameters area, review the options:
   - Filter out false "File Opened" events - Select this checkbox to filter out false File Open events and collect File Open events only if enough file content is actually read. Small files and certain operations may still trigger Read events.

3. (Optional) Customize commit credentials

You can use different commit credentials instead of the default FileWalk credentials.

1. On the left menu, select Commit.
   The commit settings are displayed.
2. (Optional) Clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials. (By default, this checkbox is selected to use the

FileWalk credentials, and the User name and Password fields are disabled for editing.)

Note:

- If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
- If the Collector is in a lower version than 8, the FileWalk credentials will be used.

3. In the Group OU area, if required, select Uniquely defined to choose a different OU from that defined in the data source's domain. Click the Browse button (...) to select the required OU.

4. Install the data source

After configuration is complete, click Install to install the data source.

A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the File Servers pane. When the installation completes, the status shows "Installed 100%".

5. Post-installation share detection and registration

After the data source installation and share detection are completed, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. The following procedure describes the manual registration and automatic share detection flows.

Important: If after the data source is installed, share detection fails for any reason, the Share Detection Status column will remain "In Progress" until the issue is fixed, and share detection completes successfully at least once.

After the data source is installed, the Shares pane is enabled, and you can view the share settings.

1. On the left menu, click Shares.
   The share settings are displayed. The pane's heading indicates the option you selected when adding a data source.
2. In the Available Shares area, you can filter the shares based on the reason they are not registered for monitoring and easily identify the shares that can be added. The default filter is Accessible Shares. You can change the filter to see the rest of the shares. Options include:

- Accessible shares - Can be added for monitoring (this option is selected by default)
- Ignored shares - Are marked as "ignored"
- Incompatible and inaccessible shares - Cannot be monitored since the exposed protocol does not match the security style of the volume (relevant to multiprotocol platforms only) or the Varonis service account does not have access to this share
- Child share of a monitored share - Is monitored via its parent folder

3. Do one of the following:
   - If you chose to monitor selected shares, in the Available Shares area, select the required shares and click the down arrow. The selected shares are moved to the Registered Shares area. (The registered shares list is empty until you make your selections.)
   - If you chose to automatically monitor detected shares, Varonis will monitor all shares that aren't marked as "ignored". The automated share detection runs every few hours. The Registered Shares area is autopopulated with the shares to be monitored.
4. For each share, review and set the following information as required:
   - Ignore Detection - Select the shares to be ignored (and not be the subject of automatic detection and notifications) by the data source monitor.
   - Events - Select this checkbox to audit events for the share.
   - Crawl - To enable or disable monitoring for the share, in the Crawl column, select the relevant option.

     Note: You can also right-click the grid and select the required options for event auditing and crawling.
5. In the Additional Share Settings area, review the options:
   - Remove deleted shares - Select this checkbox to remove deleted shares. Shares that were deleted from the data source will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the data source is unavailable, the shares will not be removed.
   - Enable event auditing - Select this checkbox to audit events from all shares added from this data source.

   After share detection and registration are completed, the status and number of registered volumes are respectively displayed in the Share Detection Status and Registered Shares columns in the File Servers pane.

What To Do Next

Now let's take a look at the supported events for the monitored VAST data sources.

Supported Events For VAST Data Sources

Note: Private Preview. If you'd like to deploy and monitor VAST data sources, contact your Sales Engineer.

SMB (CIFS) Events for VAST Data Sources

The monitored data sources and NAS devices support various SMB (CIFS) events.

Event Auditing Method

VAST API

Supported File Operations

- File created
- File deleted
- File modified
- File opened
- File renamed
- Folder created
- Folder deleted
- Folder renamed
- Owner changed
- File permissions changed
- Folder permissions changed
- Protection added
- Protection removed

Note:

- From VAST's perspective, there is no distinction between different permission change events; Varonis categorizes them all as "File/Folder permissions changed".
- Access Denied events are not supported.

20 LINUX DATA SOURCES

What This Section Contains

This section describes how to deploy and monitor Linux data sources; the requirements, deployment and configuration steps, and supported events.

What To Do Next

Before you dive in, click here to learn more about how Varonis monitors Linux accounts, file system, and events.

Linux Monitoring Overview

Note: Each Linux data source represents a monitored Linux server. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source.

A Red Hat Linux file server can be deployed through the Management Console, its local accounts and directory structure and permissions monitored, its sensitive data classified, its events audited, and respective alerts raised.

Limitations:

- Remediation policies are not supported.
- Data Classification Labels are not supported.
- Monitoring Linux RedHat events requires a compatible Varonis agent. For the list of supported versions, see Supported Linux Versions and Requirements.

Data Discovery and Classification

- Varonis supports data classification on files that reside in the monitored data sources.

What To Do Next

First, take a look at the supported versions and make sure you fulfill the Linux requirements.

Supported Linux Versions And Requirements

Important: If the required Linux kernel is not in the installation package, refer to your Varonis representative for assistance in manually installing it from the Varonis Unix repository (auto-detection is not possible).

Supported Linux Versions

The following table lists the supported Linux OSs. Varonis provides an Agent that supports the Linux OS within 6 months from the request date, for up to a period of 5 years, or less if the vendor deprecates the Linux OS sooner.

Distribution	Agent Version	OS Version	Kernel Version
Debian	6.5.2834	9	4.9.0
Debian	6.6.678	12	6.1.0-13
Debian	6.6.682	9	4.9.0-6
Debian	6.6.688	12	6.1.0-21-amd64
AltLinux	6.6.625	9.1	5.4.51
Astra	6.6.3029	2.12	4.15.3-1
Astra	6.6.3029	2	4.15.3-2-generic
Oracle	1.3.0095	SunOS-5.8-sparc	
Oracle	6.3.139	SunOS-5.9-sparc	
Oracle	6.4.000	SunOS-5.10-sparc	
Oracle	6.3.139	SunOS-5.10-x86	
Oracle	6.3.139	SunOS-5.11-sparc	
Oracle	6.4.000	SunOS-5.11-x86	
Oracle Linux	6.6.651	7.9	4.1.12-124
Oracle Linux	6.6.656	8.6	5.4.17-2136

Distribution	Agent Version	OS Version	Kernel Version
RHEL	6.4.002	4	2.6.9
RHEL	6.4.002	5	2.6.18
RHEL	6.4.002	5	2.6.18pae
RHEL	6.4.002	5	2.6.18xen
RHEL	6.4.002	6	2.6.32-71
RHEL	6.4.002	6.2	2.6.32-220
RHEL	6.4.002	6.3	2.6.32-279
RHEL	6.4.002	6.4	2.6.32-358
RHEL	6.4.002	6.5	2.6.32-431
RHEL	6.4.002	6.6	2.6.32-504
RHEL	6.4.002	6.7	2.6.32-573
RHEL	6.4.002	6.8	2.6.32-642
RHEL	6.4.002	6.9	2.6.32-696
RHEL	6.4.002	6.10	2.6.32-754
RHEL	6.4.002	7.0 GA	3.10.0-123
RHEL	6.4.002	7.1	3.10.0-229

Distribution	Agent Version	OS Version	Kernel Version
RHEL	6.4.002	7.2	3.10.0-327
RHEL	6.4.002	7.3	3.10.0-514
RHEL	6.4.002	7.4	3.10.0-693
RHEL	6.4.002	7.5	3.10.0-862
RHEL	6.4.002	7.6	3.10.0-957
RHEL	6.5.286	7.7	3.10.0-1062
RHEL	6.6.2997	7.8	3.10.0-1127
RHEL	6.6.648	7.9	3.10.0-1160
RHEL	6.6.3059	8	4.18.0-80
RHEL	6.6.2998	8.1	4.18.0-147
RHEL	6.6.3017	8.2	4.18.0-193
RHEL	6.6.3078	8.3	4.18.0-240
RHEL	6.6.590	8.4	4.18.0-305
RHEL	6.6.648	8.5	4.18.0-348
RHEL	6.6.652	8.6	4.18.0-372.9.1
RHEL	6.6.652	8.7	4.18.0-425.3.1

Distribution	Agent Version	OS Version	Kernel Version
RHEL	6.6.651	9.0	5.14.0-70.13.1
RHEL	6.6.656	9.0	5.14.0-162
RHEL	6.6.656	8	4.18.0-477-x86-64
RHEL	6.6.678	9.2	5.14.0-284.11.1
RHEL	6.6.682	8	4.18.0-513
RHEL	6.6.685	9	5.14.0-362
RHEL	6.6.691	8	4.18.0-553
RHEL	6.6.693	9	5.14.0-427
SUSE	6.4.002	SLES10	2.6.16xenpae
SUSE	6.4.002	SLES10	2.6.16
SUSE	6.4.002	SLES11	3.0.76-0
SUSE	6.4.002	SLES11	3.0.101-0
SUSE	6.4.002	SLES11	3.0.101-108
SUSE	6.4.002	SLES11	3.0.101-63
SUSE	6.4.002	SLES11	3.0.101-68
SUSE	6.4.002	SLES11	3.0.101-80

Distribution	Agent Version	OS Version	Kernel Version
SUSE	6.4.002	SLES11	3.0.101-94
SUSE	6.4.002	SLES12	3.12.28-4
SUSE	6.4.002	SLES12 SP1	3.12.49-11
SUSE	6.4.002	SLES12 SP1	3.12.69-60
SUSE	6.4.002	SLES12 SP2	4.4.103-92
SUSE	6.4.002	SLES12 SP3	4.4.131-94
SUSE	6.4.002	SLES12 SP3	4.4.156-94
SUSE	6.5.2860	SLES12 SP4	4.12.14-95
SUSE	6.6.2999	SLES12 SP5	4.12.14-122
SUSE	6.6.3053	SLES15 SP1	4.12.14-197
SUSE	6.6.3054	SLES15 SP1	4.12.14-lp151
SUSE	6.6.3053	SLES15 SP2	5.3.18-22
SUSE	6.6.3053	SLES15 SP2	5.3.18-24
SUSE	6.6.631	SLES15 SP3	5.3.18-59
SUSE	6.6.654	SLES15 SP4	5.14.21-150400.22.1

Distribution	Agent Version	OS Version	Kernel Version
SUSE	6.6.654	SLES15 SP5	5.14.21-50500.55.22
SUSE	6.6.656	SLES15 SP3	5.3.18-150300
Ubuntu	5.8.0138	8.04	2.6.24-x64
Ubuntu	6.4.002	8.04	2.6.24-x32
Ubuntu	6.4.002	10.04	2.6.32-33
Ubuntu	6.4.002	10.04	2.6.32-33pae
Ubuntu	6.4.002	10.04	2.6.32-38
Ubuntu	6.4.002	10.04	2.6.32-42
Ubuntu	6.4.002	10.04	2.6.32-52pae
Ubuntu	6.4.002	12.04	3.2.0-29
Ubuntu	6.4.002	12.04	3.2.0-83
Ubuntu	6.4.002	14.04	3.13.0-24
Ubuntu	6.4.002	14.04	3.13.0-74
Ubuntu	6.6.3003	18.04	4.15.0-76
Ubuntu	6.6.3082	18.04	4.15.0-132
Ubuntu	6.6.656	18.04	5.3.0-62

Distribution	Agent Version	OS Version	Kernel Version
Ubuntu	6.6.656	20	5.15.0-71-generic
Ubuntu	6.6.664	22	5.15.0-71-generic
Ubuntu	6.6.672	18	4.15.0-212-generic
Ubuntu	6.6.668	20	5.4.0-148-generic
Ubuntu	6.6.668	20	5.4.0-149-generic
Ubuntu	6.6.668	20	5.4.0-150-generic
Ubuntu	6.6.668	20	5.4.0-152-generic
Ubuntu	6.6.668	20	5.4.0-153-generic
Ubuntu	6.6.668	20	5.4.0-155-generic
Ubuntu	6.6.672	22	5.15.0-76-generic

Security Requirements

- Directory structure monitoring - You will have the option to perform directory structure monitoring via either an NFS integration or through the Varonis agent:
  - NFS method - A UID that is defined with read permissions on exported volumes. UID=0 must be honored from the Collector server.
  - Varonis agent method - A local user with SSH access. This local user is used for daily operations such as retrieving mounts from the data source.
  - The Varonis service account must be added to the "Varonis" group. The "Varonis" group is a group that's created in the installation process, only users under this group can do specific operations.

- Event auditing:
  - The Varonis agent should be installed. The Varonis agent is required only when using the Varonis method.

Requirements for Varonis Group Permissions and Linux File Structures

- Permissions for Varonis Group and Linux Permission Structure:
  - Varonis group is used to run Varonis binaries on the Unix server as the root user.
  - The “sticky bit” is utilized for this purpose.
  - This group is exclusively for Varonis binaries and does not affect any other applications on the machine.
- Agent Scanning for Permissions and File Structure:
  - Varonis binary scans the file system.
  - It runs Unix commands to retrieve permissions and structure.
- Agent Auditing Events:
  - Events are audited by installing a kernel driver.

What To Do Next

Now that you've fulfilled the requirements, proceed to add a monitored Linux data source. First familiarize yourself with the deployment steps summary and then dive into the detailed procedure.

Adding a Linux Data Source - Summary

Now that you've fulfilled the requirements, you can deploy a Linux data source. This section summarizes the procedure for deploying Linux data sources in the Management Console.

1. Run the Management Console as an administrator.
2. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.
3. In the Resource Wizard's Common pane, specify the data source name, check the Collector selected by default and change it if needed, and enter the credentials for running directory structure monitoring (FileWalk). Select the authentication method: Unix or SSH-keys.

Important:

- You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.

4. In the Resource Type area, select the data source type from the dropdown list. Then, click the Connect and verify link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

Note:

- The Connect and verify link is displayed only when all relevant data is entered.
- A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

5. Select the relevant Varonis Agent Installation options, and click the Agent Deployment link to define the credentials used to install the agent on the data source.
6. In the Monitored Shares area, select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source is installed and share detection is completed.
7. In the Configuration pane, review the Unix Domain, Local Accounts, FileWalk Settings, and POSIX Access Control settings.
   - Make sure to define the Unix domains prior to defining the data source. By default, the domain is set to local.
   - If you change the FileWalk method, you will need to rescan the shares.
   - The Varonis method runs the directory structure monitoring through the agent. This method only works if the agent is installed. An error will occur if this option is selected but there is no agent installed.
   - The NFS method uses the Network File System (NFS) protocol.
8. After configuration is complete, click Install to add the data source.
9. After the data source installation and share/mount detection are completed, in the Shares/Mounts pane, you can select the shares/mounts to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares/mounts, all shares/mounts will be monitored. If you chose to monitor selected shares/mounts, you can select and register the required shares/mounts.

What To Do Next

Now that you're familiar with the deployment steps, it's time to dive into the detailed procedure.

Adding a Linux Data Source - Detailed Procedure

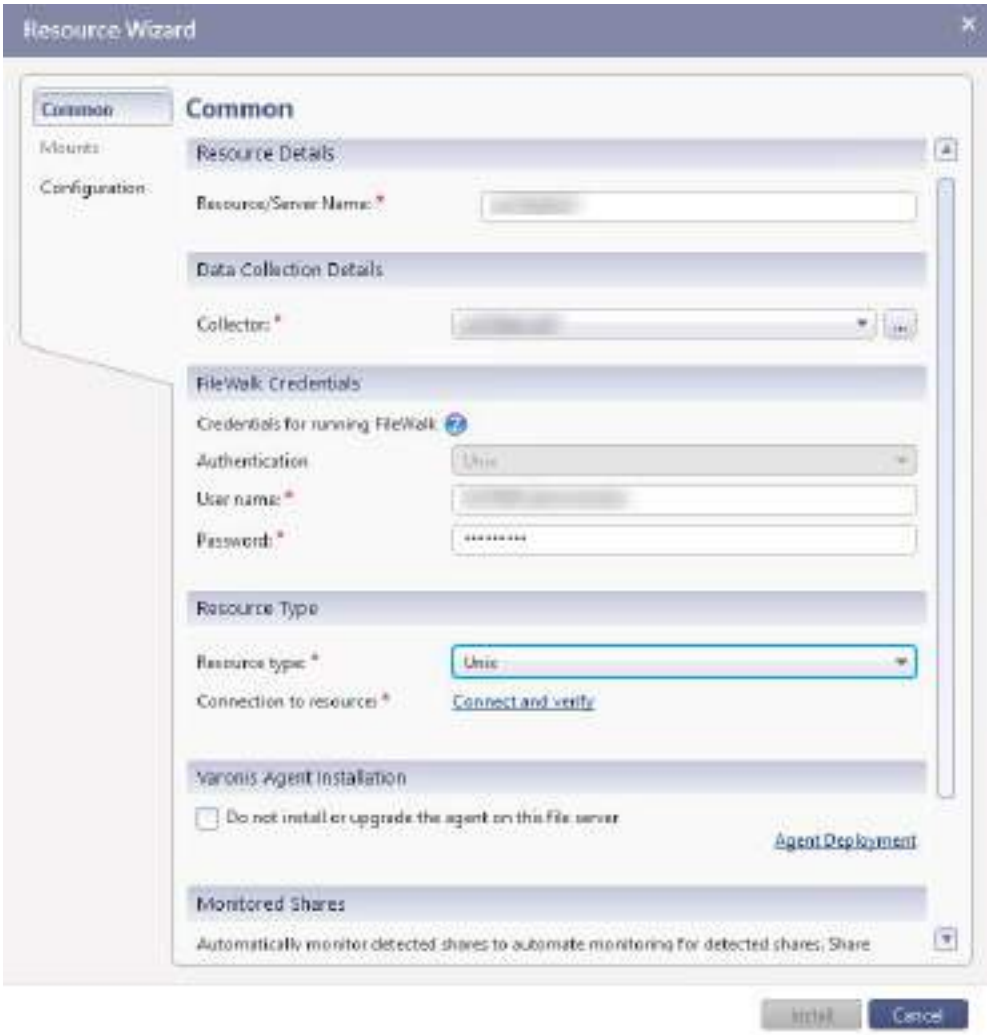
Now that you've fulfilled the requirements, you can deploy a Linux data source.

> Note: Each Linux data source represents a monitored Linux Server. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source. To monitor multiple Linux servers, add a Linux data source per Linux server.

1. Set common data source parameters

1. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.

The Resource Wizard is opened to the Common pane, where you can specify the data source and set the relevant parameters.



2. In the Common pane, set the following parameters:
   a. Resource Details - Specify the data source name.
   b. Data Collection Details - Select the relevant Collector (assigned with a certificate) from the dropdown list.
   c. FileWalk Credentials - Enter the credentials for running directory structure monitoring. File System operations include directory structure monitoring, event auditing (if set) and account enumeration on local accounts (if set).

   Note:
   - These credentials are cached, so that they are automatically entered if another data source is added during the same session.

- Authentication - From the dropdown list, select the authentication method: Unix or SSH-keys.

  Note: These credentials must be valid Unix-style credentials.

- User name - Type the name of the user account to be used for directory structure monitoring, event auditing, and local account enumeration.
- Password - Type the account's password.

  Note: This field is only displayed when Unix authentication is selected.

- Load SSH key from file - Browse to the SSH key file that contains the account's client keys. Different key files (for different file servers) must have different names.

  Note: This field is only displayed when SSH-keys authentication is selected.

- SSH file/user password - Type the password for the SSH key file.

  Note: This field is only displayed when SSH-keys authentication is selected.



Important: You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.

d. Resource Type - Select the data source type from the dropdown list.

- Connect and verify - Click this link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

  Note:

- The Connect and verify link is displayed only when all relevant data is entered.
- A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

e. Varonis Agent Installation - Set the following parameters. (For installation instructions, see Installing the Varonis Unix Agent.)

- Do not install or upgrade the agent on this file server - Select this checkbox if you do not want the Varonis agent automatically installed or upgraded on the data source.
- Agent Deployment - Click this link to define the credentials used to install the agent on the data source.
  The Agent Deployment Options window is displayed.



  - Agent Installation Credentials
    - Use FileWalk credentials for agent installation - Select this checkbox to install the agent using the same credentials as the FileWalk Credentials.

      Note: If you select this option, ensure that the specified account has the required permissions for installing the agent on the file system.

    - User name - Type the agent installation account's user name.
    - Password - Type the agent installation account's password.

f. Monitored Shares - Select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source installed and share detection is completed.

- Automatically monitor detected shares - Select this option to automate monitoring for all detected shares. Share monitoring will automatically start

after the data source installation is completed. Varonis will monitor all shares that aren't marked as "ignored".

- Monitor selected shares - This option is selected by default. You can manually select the shares to be monitored only after the data source is installed and share detection is completed. You'll need to open the Edit window for the installed data source and select the shares. For more information, see Post-installation mount detection and registration.

Once the above settings are configured, you can proceed to review and adjust configuration settings.

2. Review and adjust configuration settings

1. On the left menu, click Configuration and confirm the information.
   The general configuration settings are displayed.
2. In the Unix Domain area, review the options:
   - Select the affiliated Unix user repository for this file server or Samba domain - From the dropdown list, select a predefined Unix domain.

     Note: Be sure to define these domains prior to defining the file server. By default, the domain is set to local.
3. In the Local Accounts area, review the options:
   - Collect information regarding local accounts from this file server - Select this option to collect user accounts from this file system using data source credentials.
4. In the FileWalk Settings area, review the options:
   - Identify actual unique folders and file system inconsistencies - Select this checkbox (if it not already selected) to detect broken permissions in NTFS file systems.
   - FileWalk Method - Select the method to be used for directory structure monitoring. If you change the method, you will need to rescan the shares.
     - Varonis - A method of running the directory structure monitoring through the agent. This method only works if the agent is installed.
       - An error will occur if this option is selected but there is no agent installed.
     - NFS - Uses the Network File System (NFS) protocol (without event auditing).
5. In the POSIX Access Control List area, review the options:
   - Enable collection and management of POSIX ACLs - Select this option as relevant for Unix flavors that support POSIX ACLs.

3. Install the data source

After configuration is complete, click Install to install the data source.

A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the File Servers pane. When the installation completes, the status shows "Installed 100%".

4. Post-installation mount detection and registration

After the data source installation and mount detection are completed, you can select the mounts to be monitored. If, when adding the data source, you chose to automate monitoring for detected mounts, all mounts will be monitored. The following procedure describes the manual registration and automatic mount detection flows.

> Important: If after the data source is installed, share detection fails for any reason, the Share Detection Status column will remain "In Progress" until the issue is fixed and share detection completes successfully at least once.

After the data source is installed, the Mounts pane is enabled, and you can view the mount settings.

1. On the left menu, click Mounts
   The mount settings are displayed. The pane's heading indicates the option you selected when adding a data source.
2. In the Available Mounts area, you can filter the shares based on the reason they are not registered for monitoring and easily identify the shares that can be added. The default filter is Accessible Shares. You can change the filter to see the rest of the shares. Options include:
   - Accessible shares - Can be added for monitoring (this option is selected by default)
   - Ignored shares - Are marked as "ignored"
   - Incompatible and inaccessible shares - Cannot be monitored since the exposed protocol does not match the security style of the volume (relevant to multiprotocol platforms only) or the Varonis service account does not have access to this share
   - Child share of a monitored share - Is monitored via its parent folder
3. Do one of the following:
   - If you chose to monitor selected mounts, in the Available Mounts area, select the required mounts and click the down arrow . The selected mounts are

moved to the Registered Mounts area. (The registered shares list is empty until you make your selections.)

- If you chose to automatically monitor detected mounts, Varonis will monitor all mounts that aren't marked as "ignored". The automated share detection runs every few hours. The Registered Mounts area is auto-populated with the mounts to be monitored.

4. For each mount, review and set the following information as required:
   - Ignore Detection - Select the mounts to be ignored (and not be the subject of automatic detection and notifications) by the data source monitor.
   - Events - Select this checkbox to audit events for the mount.
   - Crawl - To enable or disable monitoring for the mount, in the Crawl column, select the relevant option.

     Note: You can also right-click the grid and select the required options for event auditing and crawling.

5. In the Additional Share Settings area, review the options:
   - Remove deleted shares - Select this checkbox to remove deleted mounts. mounts that were deleted from the data source will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the data source is unavailable, the mounts will not be removed.
   - Enable event auditing - Select this checkbox to audit events from all mounts added from this data source.

   After share detection and registration are completed, the status and number of registered volumes are respectively displayed in the Share Detection Status and Registered Shares columns in the File Servers pane.

What To Do Next

Learn how to deploy the Varonis Agent using a non-root or Centrify user.

Installing the Varonis Unix Agent

Follow the instructions below to verify the Secure Hash Algorithm-512 (SHA-512) signature and deploy the Varonis Agent, either manually or using a non-root or Centrify user.

(Optional) SHA-512 Signature Verification

Note: (Optional, Relevant only for new Varonis Unix agents added after September 2023) The agents are published now with SHA-512 signatures for the agent file. Refer to the Unix Agent Repository to get the SHA for the specific agent.

1. Download the Unix Agent Repository package from https://help.varonis.com/s/my-downloads and copy it to your current Unix data source.
2. In the Unix Agent Packages folder, go to the sha512 folder, and copy the TAR file and relevant SHA file (if it exists) for the data source.
3. Run the following command to get the SHA-512 number:

```
sha512sum <Name of tar  pi    #.( pirame]
```

   The Unix data source will create a new file with the filename you provided.
4. To display the content, run the command `cat ( pirame]`.
5. Compare the generated number displayed in the filename with the SHA-512 file (TAR) you downloaded from the Varonis repository. The numbers should be identical.

Manually Deploying the Varonis Unix Agent

1. Download the Unix Agent Repository package from https://help.varonis.com/s/my-downloads and copy it to your current Unix data source.
2. Extract the TAR file.
3. Run the `vrns_install.sh` script.
4. Go to the directory `opt/varonis` and run `./vrns_mon.sh start`.
5. From the Collector, restart the Varonis Forwarder of the Unix service.

Running the Varonis Unix Agent Installation with a Non-Root User

The workflow for installing and configuring the Varonis Agent using a non-root or Centrify user includes several steps.

1. Add a Unix data source without using a root account.
2. Run a Unix data source with Centrify using DZDO instead of SUDO.
3. Configure a user for Data Security Platform installation when working with Centrify.

Adding Unix Data Sources without Using a Root Account

To add a Unix data source without using a Root account:

1. Add a user. Run the following command:

```
# passwd sa2
```

2. Add the user to the Varonis group. Run the following command:

```
# usermod -a -G varonis sa2
```

3. Provide SUDO privileges
   Method 1: Modify the sudoers file
   a. Edit the sudoers file via the `visudo` command.
   b. Duplicate the line  and replace the word “root” with the name of the user account.

   Method 2: Add the user to the SUDO-users group
   a. In every Linux distribution, there is a group that has permissions for all actions. You can find this group by looking in the sudoers file for “ALL=(ALL) ALL”. For example, in CENTOS distribution, the name of the group is “wheel” and the line in sudoers look like this:
   
   b. Add the user to the group as follows:

```
# usermod -a -G wheel sa2
```

   where:

   - `wheel` - The name of the group
   - `sa2` - The name of the user

4. Add the data source with the user via the Management Console.
5. Run FileWalk, and if a Collector is used, run Collector FileWalk Data Delivery.

Until resolved, the following error message will be displayed.

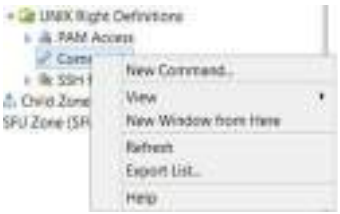


6. Complete the agent installation process with the non-root user account.

Running Unix Data Sources with Centrify Using DZDO Instead of SUDO

Running Unix data sources with Centrify requires defining and assigning DZDO as a user role.
To run a Unix data source with Centrify using DZDO instead of SUDO:

1. Open Centrify Access Manager.
2. Expand theAuthorization and Unix Right Definitions nodes, right-click Commands and select New Command.



The DZDO Properties window is displayed.

3. In the General tab, configure the following settings for Name, Description, Command, and Match path:



4. In the Restricted Shell tab, select the Can be used in a restricted role checkbox and select the User running the command option:



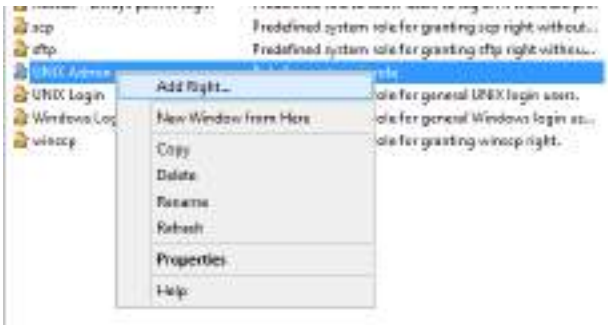
5. In the Run as tab, select the Can be used by dzdo checkbox and in the User area, specify root.



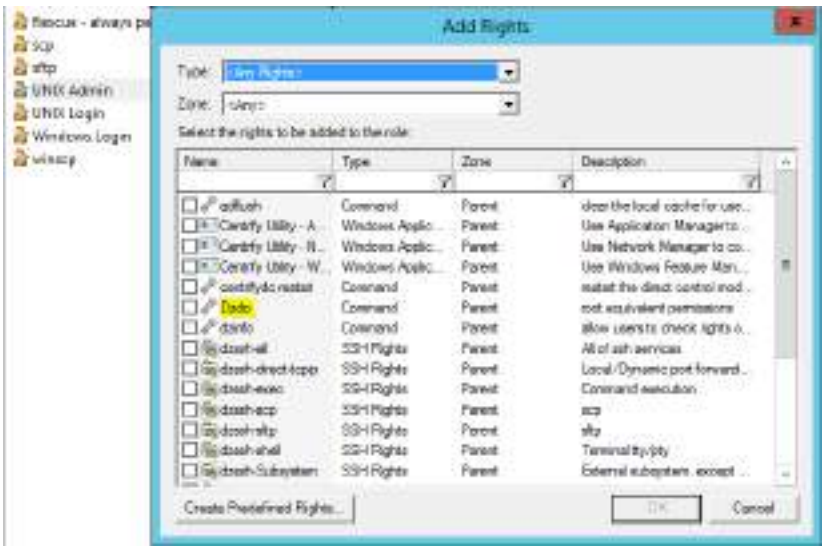
6. In the Environment tab, keep the default settings.
7. In the Attributes tab, specify whether re-authentication is required.



8. Click Apply to apply the changes.
9. To assign the command to the Unix Admin role:
   a. Expand the Authorization node and right-click Role Definitions.
   b. Click Add Role and type `Unix Admin` for the role name.
   c. Right-click the Unix Admin role and select Add Right.

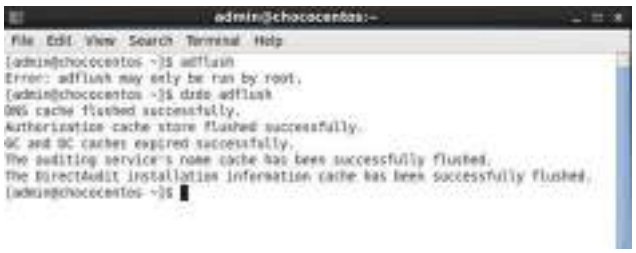


The Add Rights window is displayed.



d. Select Dzdo and click OK.

10. Now you are ready to test your command. Confirm that it is set up correctly by running a root privilege command such as `ah ywl` using `dzdo`.



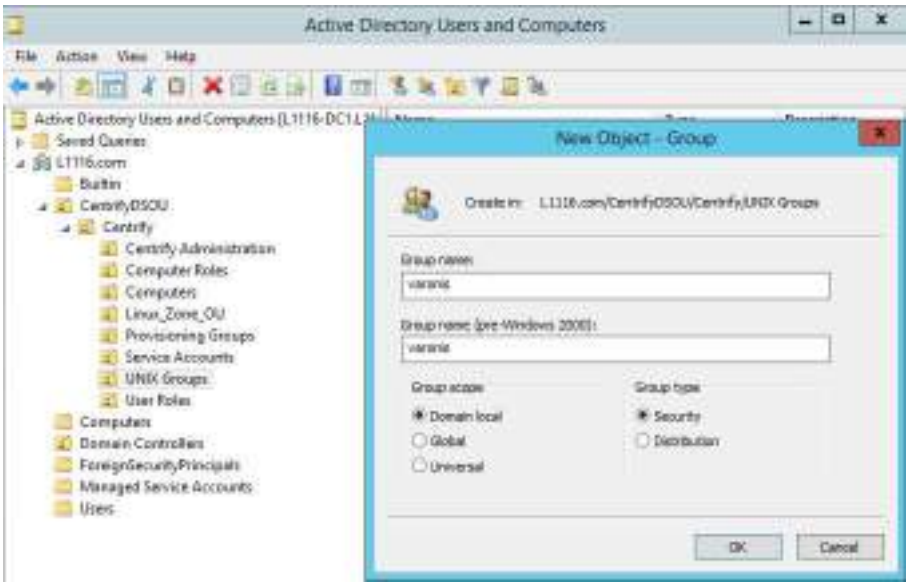
Configuring Users for Data Security Platform Installation when Working with Centrify

To configure a user for Data Security Platform when working with Centrify:

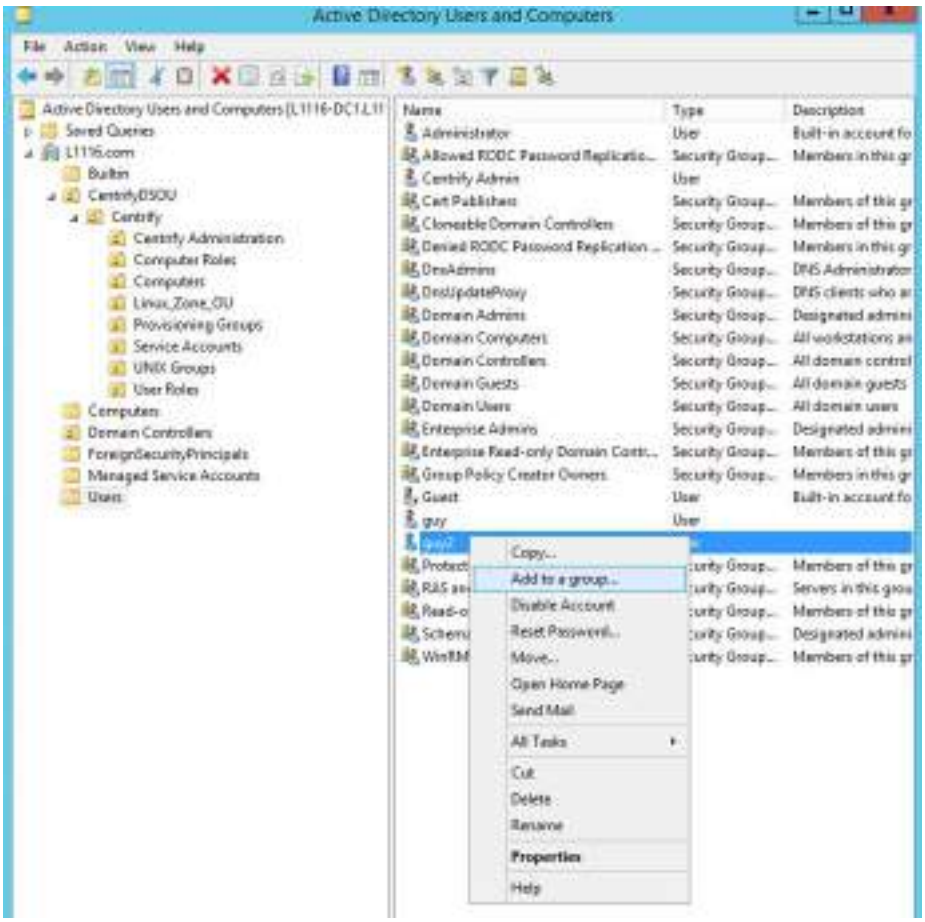
1. Create a user in Active Directory (in the Domain Controller).



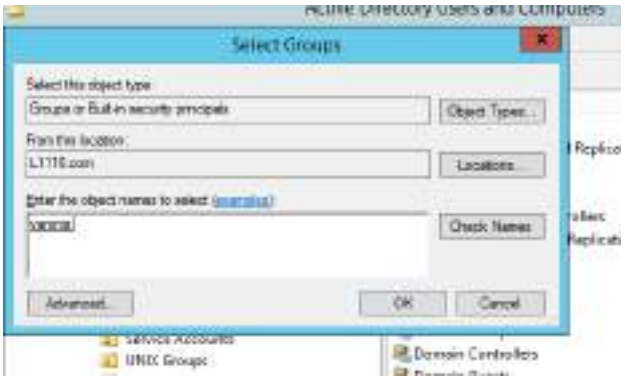
2. Add a “varonis” local Unix group in Active Directory.



3. Add the user to the group. Right-click the user and select Add to a group.



The Select Groups dialog box is displayed, showing "varonis".



4. Disable auditing on the user so that the Data Security Platform installation will be able to detect the operating system using this user. To disable auditing, on the Linux machine run the following commands:

```
# cd /etc/centrifyda
# vi centrifyda.conf
```

5. Look for the following line:

```
# nss.user.override.userlist:
```

If it does not exist, add it.

6. Add the user to the end of the last line shown below and add `:no audit` after the user name. The following example shows a user name sa3 and the corresponding line in the `centrifyda.conf` file:



7. Restart the configuration. On the Linux machine, type the following:

```
# systemctl restart centrifyda.service
```

8. Synchronize with Linux. On the Linux machine, execute `ah ywl`.

What To Do Next

Learn how to configure configure Unix data source services.

Configuring Unix Data Source Services

Configuring Unix data sources includes configuring local accounts and manually installing the Varonis Driver.

Local Accounts

To automatically configure local accounts in Root mode (using the Root password):

1. After installation is complete, make the Unix data source unmonitored in order to suppress the Probe's errors (for example, the driver is not installed).
2. Proceed with the manual installation as described below.

To automatically configure local accounts in User mode (using a non-Root password):

1. After installation is complete, make the Unix data source unmonitored in order to suppress the Probe's errors (for example, the driver is not installed).
2. Log in to the data source as root, and execute the following commands under `/tmp/VaronisInstall.<user>/`:

```
tar -xvf Varonis-<OS>-<PROCESSOR>.pkg.tar
./varonis_install.sh
```

Manual Installation of the Varonis Driver for Unix Systems

1. Navigate to the `%temp%\VaronisInstall` directory.
2. Execute the following command:

```
ssh\pscp.exe -pw <your_password> Filer\Unix\Varonis-<OS>-
<PROCESSOR>.pkg.tar 2syv ywiv 2syv  piv%.xqt
```

3. Log in to the data source as root and execute the following command under `/tmp/VaronisInstall/<user>/`:

```
 tar -xvf Varonis-<OS>-<PROCESSOR>.pkg.tar
./varonis_install.sh
```

Manual Uninstallation

- Log in to the data source as root and execute the following command under `/opt/varonis`:

```
./vrns_uninstall.sh
```

What To Do Next

Now let's take a look at the supported events for the monitored Linux data sources.

Supported NFS Events For Linux Data Sources

The Linux monitored file servers support various NFS events.

> Note: NFS v2 and v3 are supported.

Monitored File Servers

RedHat Enterprise Linux:

- 4.8 (kernel 2.6.9)
- 4.8 (kernel 2.6.9)

CPU Architecture

RedHat Enterprise Linux:

- x86
- x64

Event Auditing Method

For RedHat Enterprise Linux:

- Agent

Supported File Operations

For RedHat Enterprise Linux:

- File created
- File deleted
- File modified
- File opened
- File renamed
- Folder created
- Folder deleted
- Folder renamed
- File permissions changed
- Folder permissions changed

21 UNIX DATA SOURCES

What This Section Contains

This section describes how to deploy and monitor Unix data sources; the requirements, deployment and configuration steps, and supported events.

What To Do Next

Before you dive in, click here to learn more about how Varonis monitors Unix accounts, file system, and events.

Unix Monitoring Overview

Note: Each Unix data source represents a monitored Unix server. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source.

An IBM AIX Unix file server can be deployed through the Management Console, its local accounts and directory structure and permissions monitored, its sensitive data classified, its events audited, and respective alerts raised.

Limitations:

- Remediation policies are not supported.
- Data Classification Labels are not supported.

Data Discovery and Classification

- Varonis supports data classification on files that reside in the monitored data sources.

What To Do Next

First, take a look at the supported versions and make sure you fulfill the Unix requirements.

Unix Requirements

Varonis Service Account

Varonis requires a dedicated service account. The service account can be reused for multiple data source installations and configurations.

- Service Account Read Operations:
  - Traverse and enumerate files, folders, directory structures, users, and groups.
  - Gather data source, user, and group metadata as part of normal system operations.
- Service Account Write Operations:
  - Used for executing Varonis Policies, if policies are defined.

Security Requirements

- SSH-based - User with list credentials on all directories to be enumerated (for example, root, or a user that is a member of all groups)

Deployment Requirements

- Verify that NFS is installed and RPC are installed and running are part of Unix installation
- SSH must be enabled on the default port.
- For AIX servers that have Dell PowerPath version 5.7, installing the Data Security Platform agent can be problematic as the server is rebooted. The solution is to upgrade Dell PowerPath from 5.7 to 6.1.
- NFS mount points must exist and be accessible by Varonis for directory structure monitoring (FileWalk) via NFS.
- The user ID of the user to walk NFS mounts must be known (for example, 0). A negative UID number forces the directory structure monitoring (FileWalk) to run over SSH.
- User repository information for NIS or LDAP domains must exist, if required.
- The user ID to gather audit events must be known, and have rights to connect via SSH.
- Agent package installation requires root privileges (one-time procedure).
- Add the user to the Varonis group. Run the following command:

```
usermod -g varonis <user name>
```

What To Do Next

Now that you've fulfilled the requirements, proceed to add a monitored Unix data source. First familiarize yourself with the deployment steps summary and then dive into the detailed procedure.

Adding a Unix Data Source - Summary

Now that you've fulfilled the requirements, you can deploy a Unix data source. This section summarizes the procedure for deploying Unix data sources in the Management Console.

1. Run the Management Console as an administrator.
2. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.
3. In the Resource Wizard's Common pane, specify the data source name, check the Collector selected by default and change it if needed, and enter the credentials for running directory structure monitoring (FileWalk). Select the authentication method: Unix or SSH-keys.

   Important:

   - You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.

4. In the Resource Type area, select the data source type from the dropdown list. Then, click the Connect and verify link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

   Note:

   - The Connect and verify link is displayed only when all relevant data is entered.
   - A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

5. Select the relevant Varonis Agent Installation options, and click the Agent Deployment link to define the credentials used to install the agent on the data source.
6. In the Monitored Shares area, select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source is installed and share detection is completed.
7. In the Configuration pane, review the Unix Domain, Local Accounts, FileWalk Settings, and POSIX Access Control settings.
   - Make sure to define the Unix domains prior to defining the data source. By default, the domain is set to local.
   - If you change the FileWalk method, you will need to rescan the shares.

- The Varonis method runs the directory structure monitoring through the agent. This method only works if the agent is installed. An error will occur if this option is selected but there is no agent installed.
- The NFS method uses the Network File System (NFS) protocol.

8. After configuration is complete, click Install to add the data source.
9. After the data source installation and share/mount detection are completed, in the Shares/Mounts pane, you can select the shares/mounts to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares/mounts, all shares/mounts will be monitored. If you chose to monitor selected shares/mounts, you can select and register the required shares/mounts.

What To Do Next

Now that you're familiar with the deployment steps, it's time to dive into the detailed procedure.

Adding a Unix Data Source - Detailed Procedure

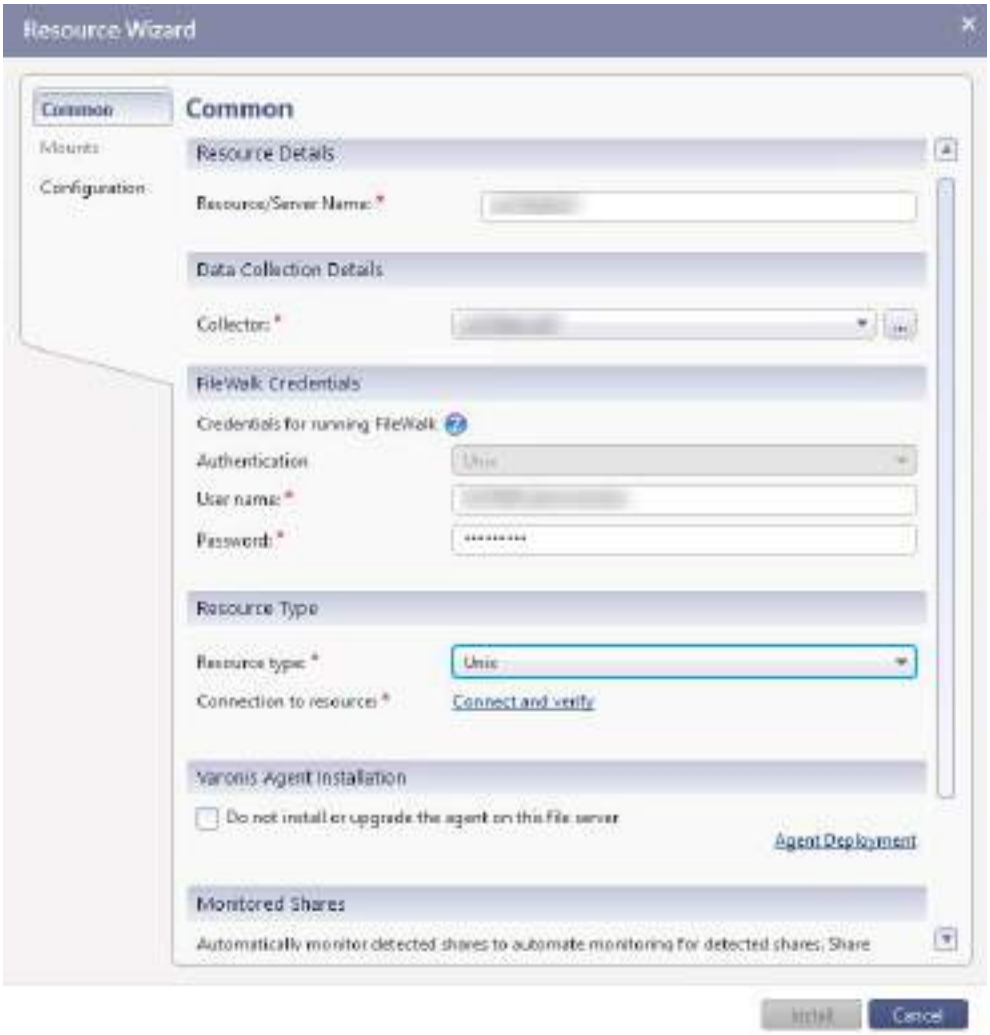
Now that you've fulfilled the requirements, you can deploy a Unix data source.

> Note: Each Unix data source represents a monitored Unix Server. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source. To monitor multiple Unix servers, add a Unix data source per Unix server.

1. Set common data source parameters

1. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.

The Resource Wizard is opened to the Common pane, where you can specify the data source and set the relevant parameters.



2. In the Common pane, set the following parameters:
   a. Resource Details - Specify the data source name.
   b. Data Collection Details - Select the relevant Collector (assigned with a certificate) from the dropdown list.
   c. FileWalk Credentials - Enter the credentials for running directory structure monitoring. File System operations include directory structure monitoring, event auditing (if set) and account enumeration on local accounts (if set).

   Note:
   - These credentials are cached, so that they are automatically entered if another data source is added during the same session.

- Authentication - From the dropdown list, select the authentication method: Unix or SSH-keys.

  Note: These credentials must be valid Unix-style credentials.

- User name - Type the name of the user account to be used for directory structure monitoring, event auditing, and local account enumeration. Make sure to use a user that's a member of the Varonis group. For more information, see Unix Requirements.
- Password - Type the account's password.

  Note: This field is only displayed when Unix authentication is selected.

- Load SSH key from file - Browse to the SSH key file that contains the account's client keys. Different key files (for different file servers) must have different names.

  Note: This field is only displayed when SSH-keys authentication is selected.

- SSH file/user password - Type the password for the SSH key file.

  Note: This field is only displayed when SSH-keys authentication is selected.



Important: You must enter the FileWalk Credentials before you can validate the Varonis connection to the data source.

d. Resource Type - Select the data source type from the dropdown list.

- Connect and verify - Click this link to validate the credentials of the service account used to connect to the data source and retrieve the dedicated data source version.

Note:

- The Connect and verify link is displayed only when all relevant data is entered.
- A warning message is displayed when the data source type and version aren't verified. It's best to correct these before proceeding with the deployment but it will not block you from configuring and installing the data source.

e. Varonis Agent Installation - Set the following parameters. (For installation instructions, see Installing the Varonis Unix Agent.)

- Do not install or upgrade the agent on this file server - Select this checkbox if you do not want the Varonis agent automatically installed or upgraded on the data source. If you choose this option, you need to manually install the Varonis Agent. Download the Unix agent from My Downloads on varonis.com and copy it to your current Unix data source.
- Agent Deployment - Click this link to define the credentials used to install the agent on the data source.
  The Agent Deployment Options window is displayed.



  - Agent Installation Credentials
    - Use FileWalk credentials for agent installation - Select this checkbox to install the agent using the same credentials as the FileWalk Credentials.

      Note: If you select this option, ensure that the specified account has the required permissions for installing the agent on the file system.

    - User name - Type the agent installation account's user name.
    - Password - Type the agent installation account's password.

f. Monitored Shares - Select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data

source installation is completed, and share selection is only available after the data source installed and share detection is completed.

- Automatically monitor detected shares - Select this option to automate monitoring for all detected shares. Share monitoring will automatically start after the data source installation is completed. Varonis will monitor all shares that aren't marked as "ignored".
- Monitor selected shares - This option is selected by default. You can manually select the shares to be monitored only after the data source is installed and share detection is completed. You'll need to open the Edit window for the installed data source and select the shares. For more information, see Post-installation mount detection and registration.

Once the above settings are configured, you can proceed to review and adjust configuration settings.

2. Review and adjust configuration settings

1. On the left menu, click Configuration and confirm the information.
   The general configuration settings are displayed.
2. In the Unix Domain area, review the options:
   - Select the affiliated Unix user repository for this file server or Samba domain - From the dropdown list, select a predefined Unix domain.

     Note: Be sure to define these domains prior to defining the file server. By default, the domain is set to local.
3. In the Local Accounts area, review the options:
   - Collect information regarding local accounts from this file server - Select this option to collect user accounts from this file system using data source credentials.
4. In the FileWalk Settings area, review the options:
   - Identify actual unique folders and file system inconsistencies - Select this checkbox (if it not already selected) to detect broken permissions in NTFS file systems.
   - FileWalk Method - Select the method to be used for directory structure monitoring. If you change the method, you will need to rescan the shares.
     - Varonis - A method of running the directory structure monitoring through the agent. This method only works if the agent is installed.
       - An error will occur if this option is selected but there is no agent installed.

- NFS - Uses the Network File System (NFS) protocol (without event auditing).

5. In the POSIX Access Control List area, review the options:
   - Enable collection and management of POSIX ACLs - Select this option as relevant for Unix flavors that support POSIX ACLs.

3. Install the data source

After configuration is complete, click Install to install the data source.

A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the File Servers pane. When the installation completes, the status shows "Installed 100%".

4. Post-installation mount detection and registration

After the data source installation and mount detection are completed, you can select the mounts to be monitored. If, when adding the data source, you chose to automate monitoring for detected mounts, all mounts will be monitored. The following procedure describes the manual registration and automatic mount detection flows.

> Important: If after the data source is installed, share detection fails for any reason, the Share Detection Status column will remain "In Progress" until the issue is fixed and share detection completes successfully at least once.

After the data source is installed, the Mounts pane is enabled, and you can view the mount settings.

1. On the left menu, click Mounts
   The mount settings are displayed. The pane's heading indicates the option you selected when adding a data source.
2. In the Available Mounts area, you can filter the shares based on the reason they are not registered for monitoring and easily identify the shares that can be added. The default filter is Accessible Shares. You can change the filter to see the rest of the shares. Options include:
   - Accessible shares - Can be added for monitoring (this option is selected by default)
   - Ignored shares - Are marked as "ignored"
   - Incompatible and inaccessible shares - Cannot be monitored since the exposed protocol does not match the security style of the volume (relevant to multiprotocol platforms only) or the Varonis service account does not have access to this share

- Child share of a monitored share - Is monitored via its parent folder

3. Do one of the following:
   - If you chose to monitor selected mounts, in the Available Mounts area, select the required mounts and click the down arrow . The selected mounts are moved to the Registered Mounts area. (The registered shares list is empty until you make your selections.)
   - If you chose to automatically monitor detected mounts, Varonis will monitor all mounts that aren't marked as "ignored". The automated share detection runs every few hours. The Registered Mounts area is auto-populated with the mounts to be monitored.
4. For each mount, review and set the following information as required:
   - Ignore Detection - Select the mounts to be ignored (and not be the subject of automatic detection and notifications) by the data source monitor.
   - Events - Select this checkbox to audit events for the mount.
   - Crawl - To enable or disable monitoring for the mount, in the Crawl column, select the relevant option.

     Note: You can also right-click the grid and select the required options for event auditing and crawling.
5. In the Additional Share Settings area, review the options:
   - Remove deleted shares - Select this checkbox to remove deleted mounts. mounts that were deleted from the data source will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the data source is unavailable, the mounts will not be removed.
   - Enable event auditing - Select this checkbox to audit events from all mounts added from this data source.

   After share detection and registration are completed, the status and number of registered volumes are respectively displayed in the Share Detection Status and Registered Shares columns in the File Servers pane.

What To Do Next

Now let's take a look at the supported events for the monitored Unix data sources.

Supported NFS Events For Unix Data Sources

The Unix monitored file servers support various NFS events.

Note: NFS v2 and v3 are supported.

CPU Architecture

- x64

Event Auditing Method

- Agent

Supported File Operations

- File created
- File deleted
- File modified
- File opened
- File renamed
- Folder created
- Folder deleted
- Folder renamed
- File permissions changed[1]
- Folder permissions changed[1]

Note

1. Events generated by editing specific ACL sets are not supported.

22 UNIX DIRECTORY SERVICES

What This Section Contains

This section describes how to configure Unix Directory Services domains; the requirements, deployment and configuration steps.

What To Do Next

Before you dive in, click here to learn more about how Varonis monitors Unix Directory Services.

Unix Directory Services Monitoring Overview

Lightweight Directory Access Protocol (LDAP) Directory Services

LDAP is a protocol that allows locating data about organizations, users, groups, and other resources, such as files and devices in a network. Multiple directory service solutions (other than Microsoft's Windows Active Directory) support LDAP, such as OpenLDAP and ApacheDS. Such solutions are deployed for Varonis users who use them to manage their accounts.

With this feature, Varonis users who manage their accounts using an LDAP solution can now monitor them in account and membership analytics. If permissions to data source resources are granted to the LDAP accounts, Varonis will resolve them in permission analytics and access intelligence. If events on data source resources are performed by LDAP accounts, Varonis will resolve them in event analytics.

Note: Only users, groups, and group memberships are monitored.

Samba Active Directory (AD) Directory Services

Samba is an open-source application suite that implements the Server Message Block (SMB) protocol. It allows, among other things, for Windows clients to access Linux/Unix servers over the network transparently, for example, sharing a Linux drive with Windows servers or sharing a Linux printer with Windows servers.

Samba servers can also be configured as Active Directory (AD) Domain Controllers (DCs), facilitating a centralized place for managing accounts and for authenticating users and apps from both Unix/Linux and/or Windows clients.

With this feature, if permissions to data source resources are granted to Samba AD accounts, Varonis will resolve them to the respective AD account in permission analytics and access intelligence. If events on data resource resources are performed by Samba AD accounts, Varonis will resolve them to the respective AD account in event analytics.

Note:
Users, groups, and memberships are not visible in account and membership analytics.

Limitations

- Events are not monitored.

- DatAlert Suite is not supported.

What To Do Next

Learn how to configure the Unix Directory Services domains, see:

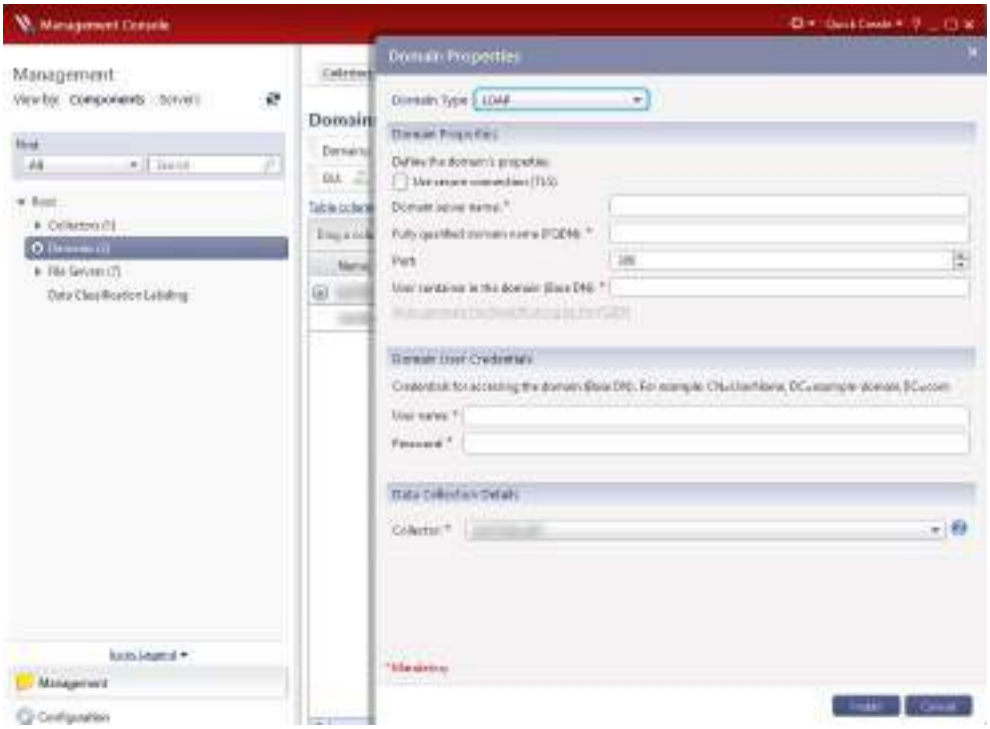
- Adding an LDAP Domain
- Adding a Samba AD Domain

Adding An LDAP Domain

You can install an LDAP domain and configure related settings, including the domain properties and user credentials.

1. Set domain properties

1. In the Management Console, select Management > Components > Root > Domains, and on the toolbar, click Add.
   The Domain Properties page is displayed, showing the General pane.
2. From the Domain Type dropdown list located at the top of the page, select LDAP.



3. Set the following parameters:
   - Domain Properties
     - Use secure connection (TLS) - Select this checkbox to define a connection using Transport Layer Security.
     - Domain Server Name - Type the name of the server on which the domain is located.
     - Fully qualified domain name (FQDN) - Type the fully qualified domain name.
     - Port - Type the port to be used for the domain.
     - User container in the domain (Base DN) - Type the base container for the user and group accounts. This is the full LDAP path to the container.
     - Auto-generate the BaseDN string by the FQDN - Click this link as necessary.
   - Domain User Credentials
     - User Name (full LDAP name) - Type the name of the user used to access this domain. This is the full Distinguished Name of the object, including the container and domain (for example, uid=username,cn=commonName1,cn=commonName2,ou=organizationalUnitName,dc=domainComp

- Password - Type the user's password.

4. In the Data Collection Details area, select the relevant Collector from the dropdown list.

2. Install the domain

After configuration is complete, click Install to install the domain.

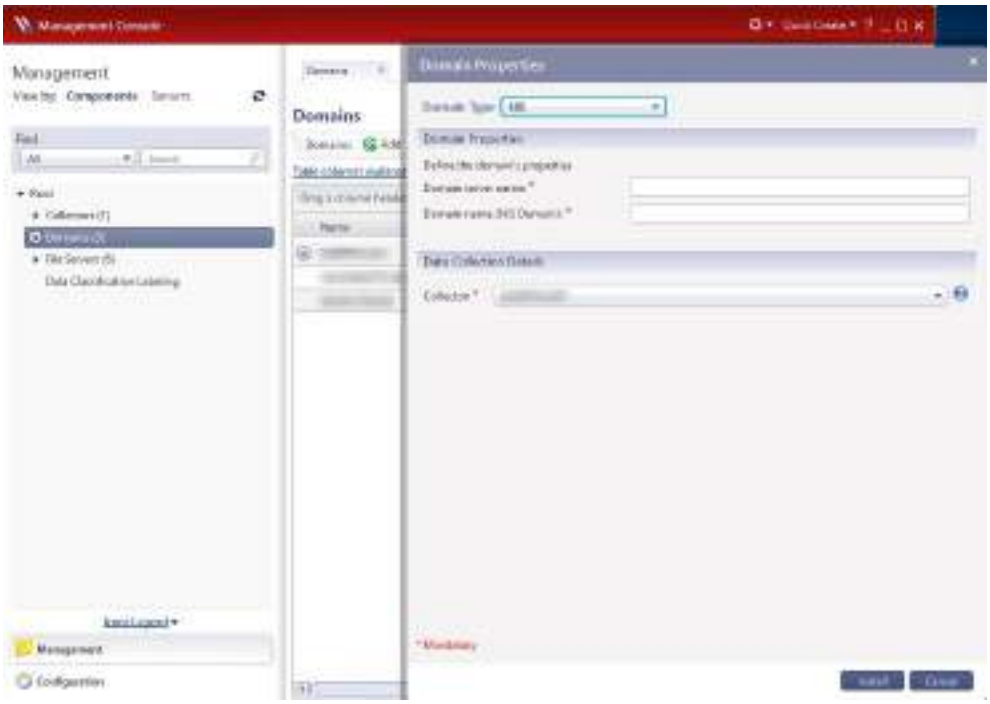
A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the Domains pane. When the installation completes, the status shows "Installed 100%".

Adding A NIS Domain

You can install a NIS domain and configure related settings, including the domain properties and the server on which the domain is located.

1. Set domain properties

1. In the Management Console, select Management > Components > Root > Domains, and on the toolbar, click Add.
   The Domain Properties page is displayed, showing the General pane.
2. From the Domain Type drop-down list located at the top of the page, select NIS.



3. Set the following parameters:
   - Domain server name - Type the name of the server on which the domain is located.
   - Domain name (NIS Domain) - Type the name of the NIS domain.
4. In the Data Collection Details area, select the relevant Collector from the dropdown list.

2. Install the domain

After configuration is complete, click Install to install the domain.

A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the Domains pane. When the installation completes, the status shows "Installed 100%".

Adding A Samba AD Domain

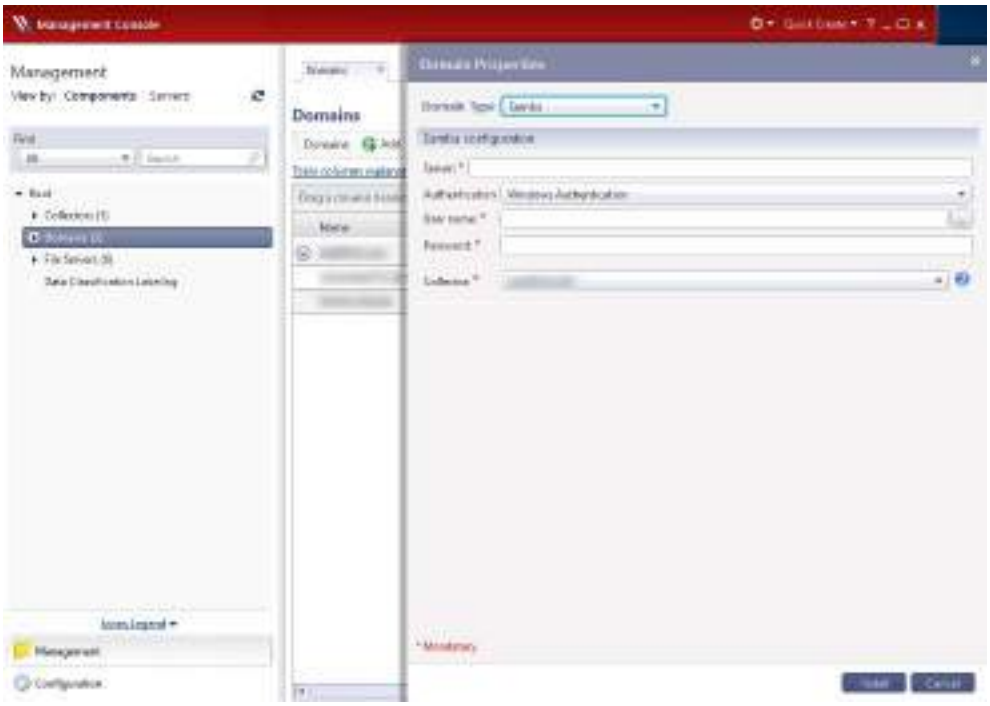
You can install a Samba AD domain and configure related settings, including the domain properties and the server on which the domain is located.

Samba Domain Requirement

- Enable Winbind authentication on the Samba domain to authenticate AD users.

1. Set domain properties

1. In the Management Console, select Management > Components > Root > Domains, and on the toolbar, click Add.
   The Domain Properties page is displayed, showing the General pane.
2. From the Domain Type dropdown list located at the top of the page, select Samba.



3. Set the following parameters:
   - Server - Click the Browse button to select the server on which the domain is located.

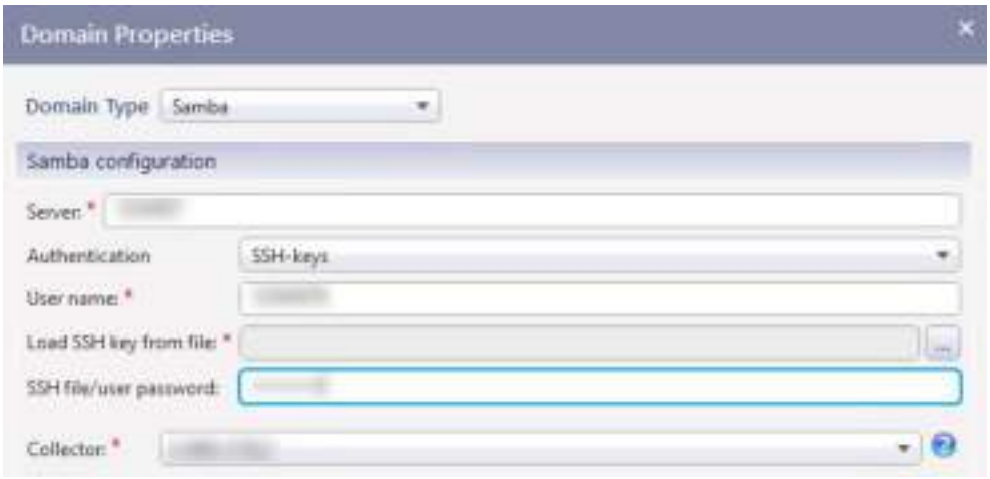
- Authentication - From the dropdown list, select the authentication method: Windows Authentication or SSH-keys.
- User name - Set the name of the user that can access this domain.

  Note: The name is case sensitive. Ensure the name you enter matches the one in AD.
- Password - Type the user's password.

  Note: This field is only displayed when Windows Authentication is selected.
- Load SSH key from file - Browse to the SSH key file that contains the account's client keys. Different key files (for different file servers) must have different names.

  Note: This field is only displayed when SSH-keys authentication is selected.
- SSH file/user password - Type the password for the SSH key file.

  Note: This field is only displayed when SSH-keys authentication is selected.



4. Select the relevant Collector from the dropdown list.

2. Install the domain

After configuration is complete, click Install to install the domain.

A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the Domains pane. When the installation completes, the status shows "Installed 100%".

23 NETWORK DEVICE (VARONIS EDGE) DATA SOURCES

What This Section Contains

This section describes how to deploy network devices to monitor perimeter activity of organizations by auditing events from VPN gateways, Web Proxies, and DNS servers. It describes the requirements, deployment and configuration steps, and supported events.

What To Do Next

Before you dive in, click here to learn about the workflow for deploying network devices to work with Varonis to audit events from VPN, Web Proxy, and DNS sources.

Network Device (Varonis Edge) Deployment Overview

About Deploying Network Devices

You can deploy network devices to work with Varonis to monitor the perimeter activity of organizations by auditing activity events from VPN Gateways, Web Proxies, and DNS servers.

Varonis can monitor events directly from the source devices using Syslog, or log shippers such as Filebeat and NXLog. If the data is already collected in Splunk, you can configure Varonis to get the events from Splunk.

Workflow for Deploying Network Devices

1. Configure a Collector to support network devices.
2. Before configuring a network device data source, make sure to first install Java Development Kit 1.8/JRE (Java 8) 64-bit on each Collector server that supports network devices and define JAVA_HOME as a system environment variable. For more information, see the Network Devices (Varonis Edge) Requirements and the Java documentation.
3. Configure the data source in the Management Console.
4. Configure the network device data source to use Splunk, Syslog, or Filebeat to collect data.
5. For each source, regardless of collection method, a network device is defined and assigned to a Collector which will do the event auditing/activity monitoring.
6. Ensure that the interface configuration is properly configured to receive the events.
7. Configure the VPN, Web Proxy, or DNS sources to send events to Varonis. For more information, see the relevant sections in this guide.

What To Do Next

Now that you've learned about the deployment workflow for network devices, let's take a look at the supported source products and versions.

Supported Source Products And Versions

Network devices (Varonis Edge) support receiving events from various products and product versions.
The following lists the various products and their respective versions from where network devices receive events.

Note: The network device configuration instructions provided to customers may vary between third-party versions.

VPN

- Check Point version R77.x, 80.x, and 81.x
- Cisco ASA version 9.x (AnyConnect)
- Cisco Firepower Threat Defense (FTD) version 6.x or 7.x
- Citrix ADC (Netscaler) version 12.x, 13.x, 14.x, or 15.x
- F5 BIG-IP APM v12.x, 13.x, 14.x, 15.x, or 16.x
- Fortinet FortiGate (with or without FortiAnalyzer) running FortiOS version 5.x, 6.x, or 7.x
- Palo Alto firewalls running PAN-OS 8.x, 9.x, 10.x, or 11.x
- Pulse Secure version 8.xR.x or 9.x
- SonicWall SonicOS version 6.x or 7.x
- Sophos XG VPN version 18.x or 20.x

Web Proxy

- Apache HTTP Server version 2.x
- Barracuda Web Security Gateway version 14.x or 15.x
- Cisco Firepower Threat Defense (FTD) version 6.x or 7.x
- Cisco (IronPort) Web Security Appliances AsyncOS 10.x-14.x
- Cisco Umbrella
- Forcepoint (WebSense) Web Security 8.x
- Fortinet FortiGate (with or without FortiAnalyzer) running FortiOS version 6.x or 7.x
- McAfee Web Gateway 7.x or 10.x; Skyhigh Secure Web Gateway (On Prem) version 10.x (previously McAfee Web Gateway)
- Palo Alto firewalls running PAN-OS 7.x, 8.x, 9.x, 10.x, or 11.x
- Sophos XG Proxy version 18.x or 20.x
- Squid versions 3.x, 4.x, and 5.x
- Symantec (Bluecoat) ProxySG 6.x

- Zscaler Proxy versions 5.x and 6.x

DNS

- BlueCat versions 9.3.0 and 9.4.0
- Cisco Umbrella
- Infoblox version 8.x
- Microsoft Windows Server 2012 R2, 2016, 2019, and 2022

Firewall

Note: Private Preview. If you'd like to monitor firewall activity, contact your Sales Engineer.

- Check Point version R81.x
- Cisco ASA 9.15 Secure Firewall Threat Defense 7.2.0
- Palo Alto firewalls running PAN-OS 8.x, 9.x, 10.x, or 11.x

What To Do Next

First, make sure you fulfill the Network Devices (Varonis Edge) Requirements.

Network Devices (Varonis Edge) Requirements

Network devices have various requirements for software and installation.

Installation

- For automatic Filebeat deployment:
  - When using automatic Filebeat during deployment, if you want to monitor domain controllers from different domains, you need to create a trust relationship between the domains. The trust can be removed after deployment is done and the system is working properly.

Note:

- Other versions from a supported vendor may work as long as they send the same events in the same format.
- Network devices (Edge) require a dedicated Collector according to the sizing guidelines.
- When using network device data sources with Splunk, make sure that there are ports available in the range 34550-34600 on the localhost IP address 127.0.0.1.

.NET Framework

- 4.7.2

Software

- Java Development Kit 1.8/JRE (Java 8) 64-bit must be installed on each Collector that supports network devices.

  Note:
  - Only Amazon Corretto 8 OpenJDK and Oracle JDK 8 are supported. If Oracle JDK 8 is already installed, replacing it with Amazon Corretto 8 requires a manual process. Contact Varonis Support for assistance.
  - The minimum required Java version is jdk-8u102-windows-x64.

What To Do Next

Now that you've fulfilled the requirements, proceed to configure a network device data source. Make sure to first configure a Collector to support network devices.

Configuring A Network Device (Edge) Data Source

What This Section Contains

This section describes how to configure a network device data source. It provides instructions for configuring a Collector to support network devices, adding and editing network device data sources, and setting the date and time format.

What To Do Next

To get started, configure a Collector to support network devices.

Configuring a Collector to Support Network Devices (Edge)

Before you can deploy a network device, you must first configure a Collector to support it.

Note:

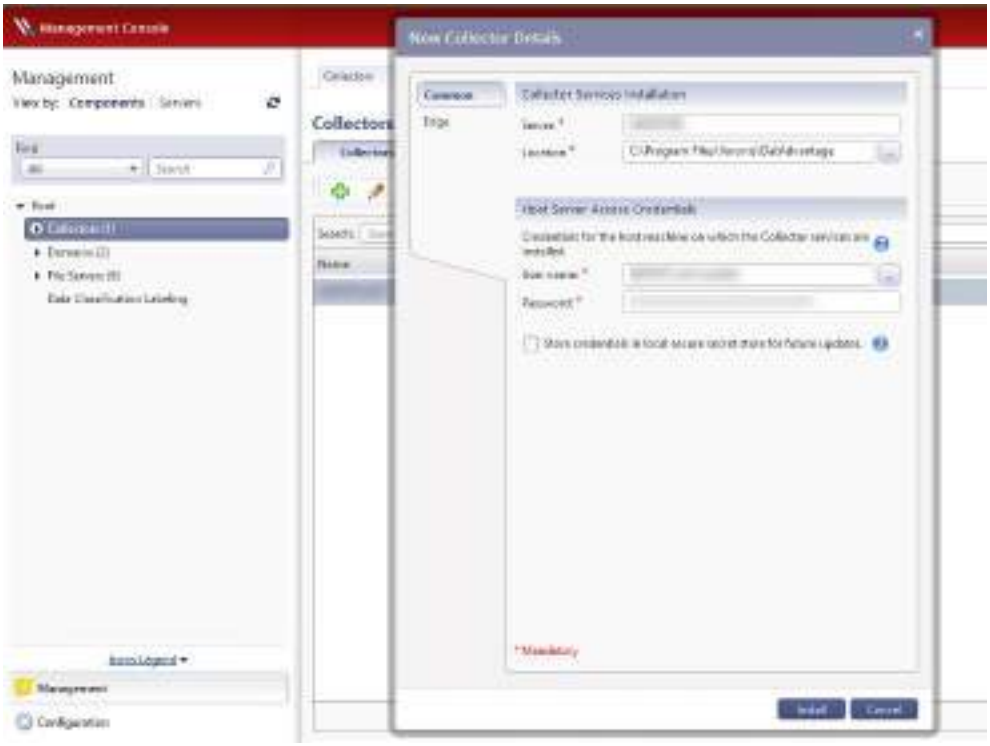
- Before configuring a network device data source, make sure to first install Java Development Kit 1.8/JRE (Java 8) 64-bit on each Collector that supports network devices, and define JAVA_HOME as a system environment variable. For more information, see the Network Devices (Varonis Edge) Requirements and the Java documentation.
- For clean installations, Collectors are now deployed and activated in the Varonis Web Interface. For instructions for using the Varonis Web Interface to configure a Collector to support network devices, click here. After you've configured the Collector, you'll need to use the Management Console to configure the network device data sources.

If you are working with a Deployment Hub, you'll need to use the Management Console to configure a Collector to support network devices.

To configure a Collector to support network devices using the Management Console:

1. In the Management Console, from the menu in the left pane, select Management > Components > Root > Collectors.
   The Collectors pane is displayed on the right.
2. On the toolbar, click Add to define a new Collector. Alternatively, you can edit an existing Collector.

The New Collector Details window is displayed.



3. On the left menu, click Common and then set the following parameters:

> Note: Network devices (Edge) require a dedicated Collector according to the sizing guidelines.

- Collector Services Installation - Select the server and location on which Collector services are installed:
  - Server - Enter the name of the server on which the Collector services are installed. If the relevant server is not listed, click the Browse button to locate it. Use the FQDN/hostname as the Collector address; the IP address cannot be used.
  - Location - Type or browse to the folder on which the Collector services are installed. (The location is changeable.)
- Host Servers Access Credentials - The installation account of the Collector services.

> Note: If you are installing the Collector on a cluster, these fields are automatically completed with the credentials used to access the data source group.

- User name - The installation account's user name.
- Password - The installation account's password.

- Store credentials in local secure secret store for future updates - Select this checkbox to store the credentials you entered.

4. On the left menu, click Edge, and do the following:
   a. In the Support Edge Data Sources area, select the Install Edge data source event collection components checkbox.
   b. In the Installation path, specify the installation location for Logstash.

> Note: Logstash is a software library used by network devices at the Collector which requires approximately 300MB. For example, you can move the installation to an alternative disk that has more space.



5. Click Install.

What To Do Next

Now that you've configured a Collector to support network devices, it's time to add a network device data source.

Adding a New Network Device (Edge) Data Source

You can add a new network device data source for a specific device.

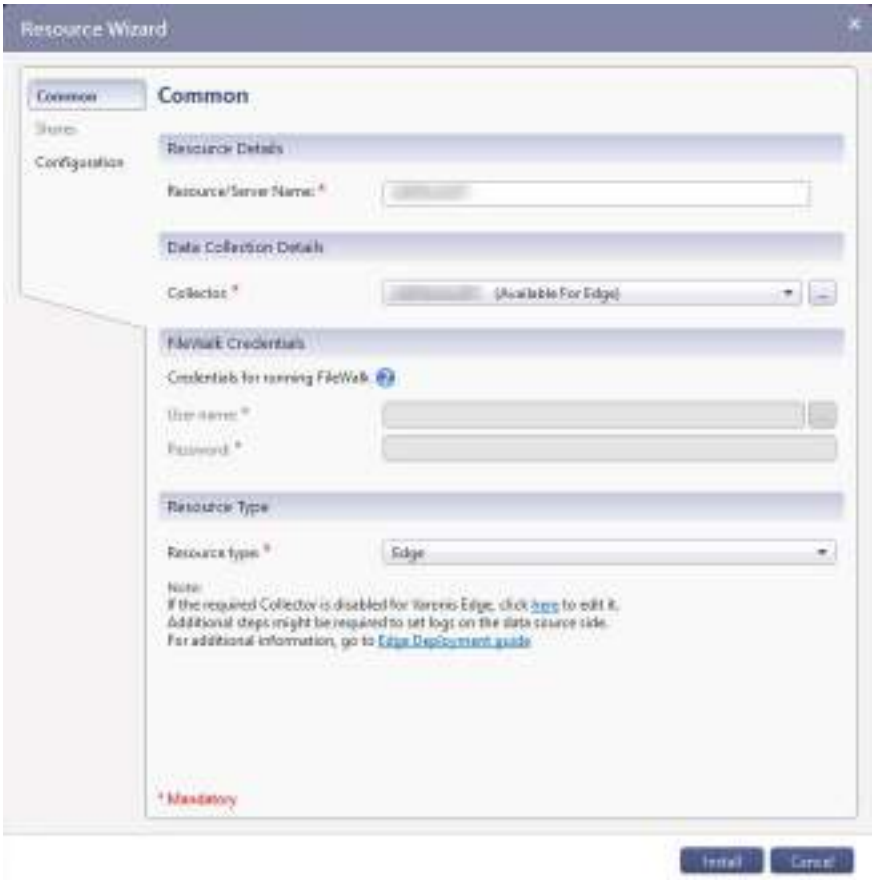
A separate network device data source can be used for multiple sources from the same vendor and product located in the same time zone. For example, all Pulse VPN gateways located in the US Eastern Standard Time Zone can share a single network device data source.

> Note: In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source, even if it's not actually a file server.

1. Set common data source parameters

1. In the Management Console, from the menu in the left pane, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.

The Resource Wizard is opened to the Common pane, where you can specify the data source and set the relevant parameters.

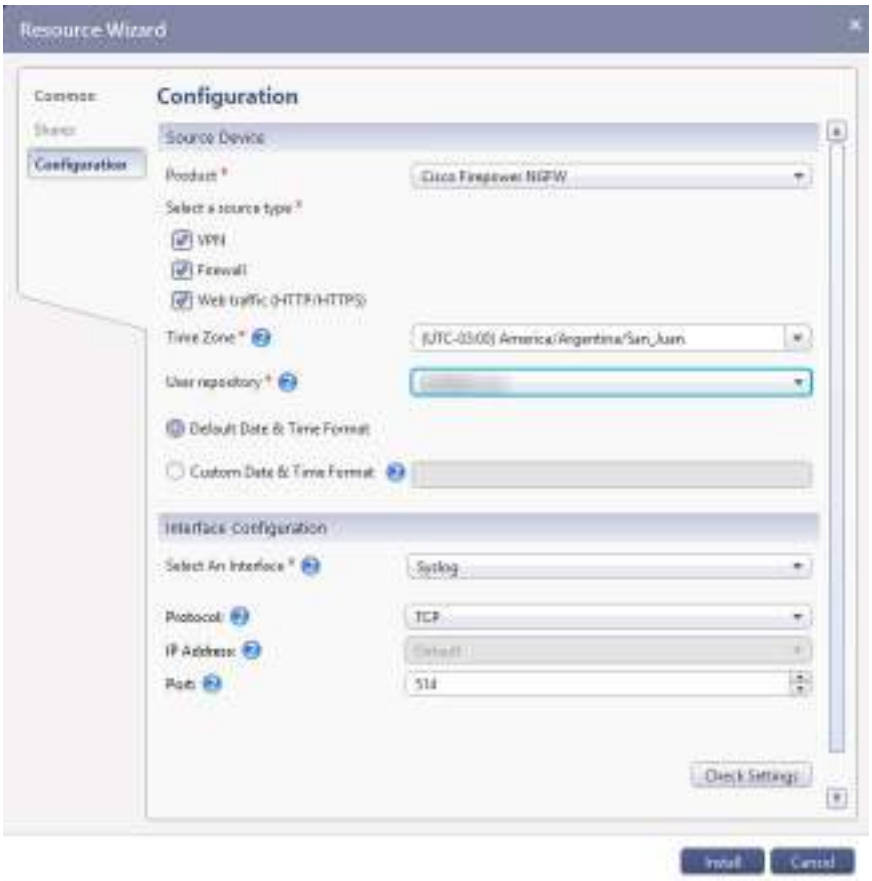


2. In the Common pane, set the following parameters:
   a. Resource Details - Specify the data source name. For example, North America Office VPN.
   b. Data Collection Details - Select a Collector that is configured to support network devices.
   c. Resource Type - Select Edge from the dropdown list. (The FileWalk Credentials will be disabled.)

2. Review and adjust configuration settings

1. On the left menu, click Configuration.

The source device and interface configuration settings are displayed.



2. In the Source Device area, set the following parameters:
   - Product - Select the relevant vendor product from the dropdown list. The options vary according to the data source type specified in the Common pane. For some products, additional checkboxes will be available for selecting supported source types. For example, if you select Cisco Firepower NFGW, you will see the VPN, Firewall, and Web traffic (HTTP/HTTPS) checkboxes.

     Note: Private Preview. If you'd like to monitor firewall activity, contact your Sales Engineer.

   - Time Zone - Select the time zone of the device, used to adjust for the time zone for devices for which events do not include a time zone designator.

     Note: When configuring a new network device data source to use Filebeat or NXLog, it is not necessary to configure the time zone.

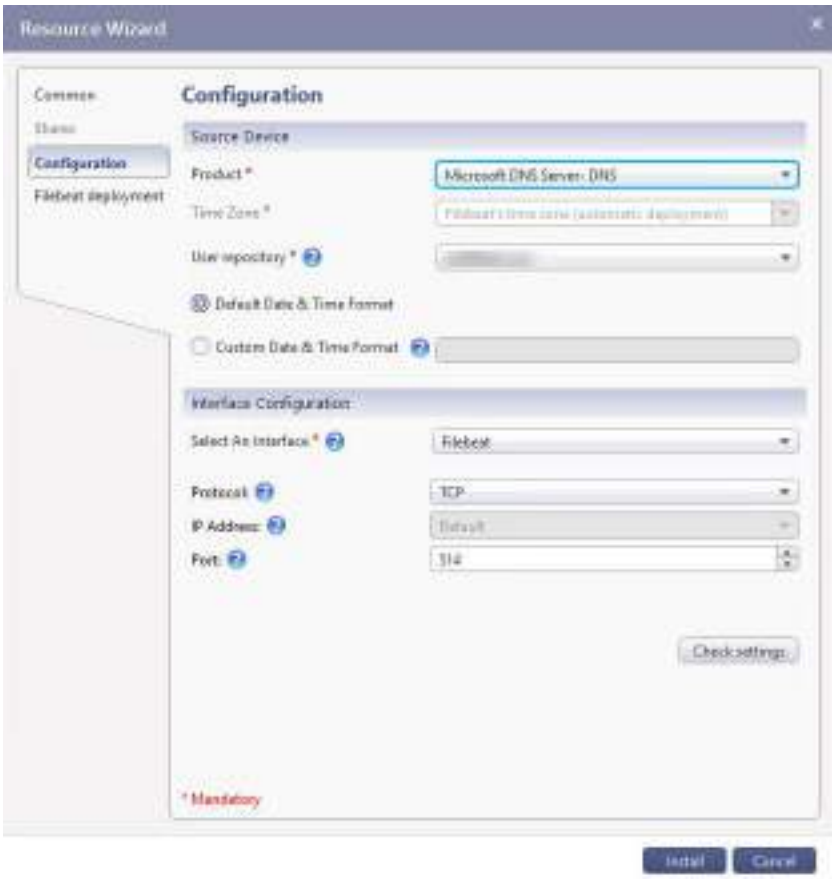
   - User repository - (Relevant only for VPN and Web Proxy sources) Select the user repository/domain with which to match user names in the events (leave the default if your installation contains only a single domain). For example, Active Directory.

- Default Date & Time Format - Select to auto-detect the date and time format used in the logs of the monitored sources (VPN, Proxy, or DNS). If the auto-detection fails, a notification is sent.

  Note: When network device proxy parsers based on splits is enabled (feature toggle EdgeSplitFilters=ON), auto-detection of the date and time format will not work. Only predefined default or custom dates can be used in this case.

- Custom Date & Time Format - Define the vendor's date and time format to avoid possible date format problems with Varonis servers. For information about the date and time format, see Date and Time Format Notation.

3. In the Interface Configuration area, the recommended interface will be automatically selected per the selected product. The network device will use the specified interface to audit events from the source device. The additional parameters to configure vary according to the selected option.
   For example, for Microsoft DNS Server, Filebeat is automatically selected. The other available options for Microsoft DNS Server are: Syslog and Splunk.



For Cisco Umbrella, AWS_S3 is automatically selected. The other available option for Cisco Umbrella is: Splunk.



What To Do Next

Next, configure the interface that the network device will use to audit events:

- To use Splunk to audit events, click here.
- To use Syslog to audit events directly from the source device, click here.
- To use Filebeat to audit events from the source device, click here.
- To use AWS to audit events from a Cisco Umbrella source device, click here.

After that, proceed to configure the VPN, Web Proxy, and DNS source devices to send events to Varonis.

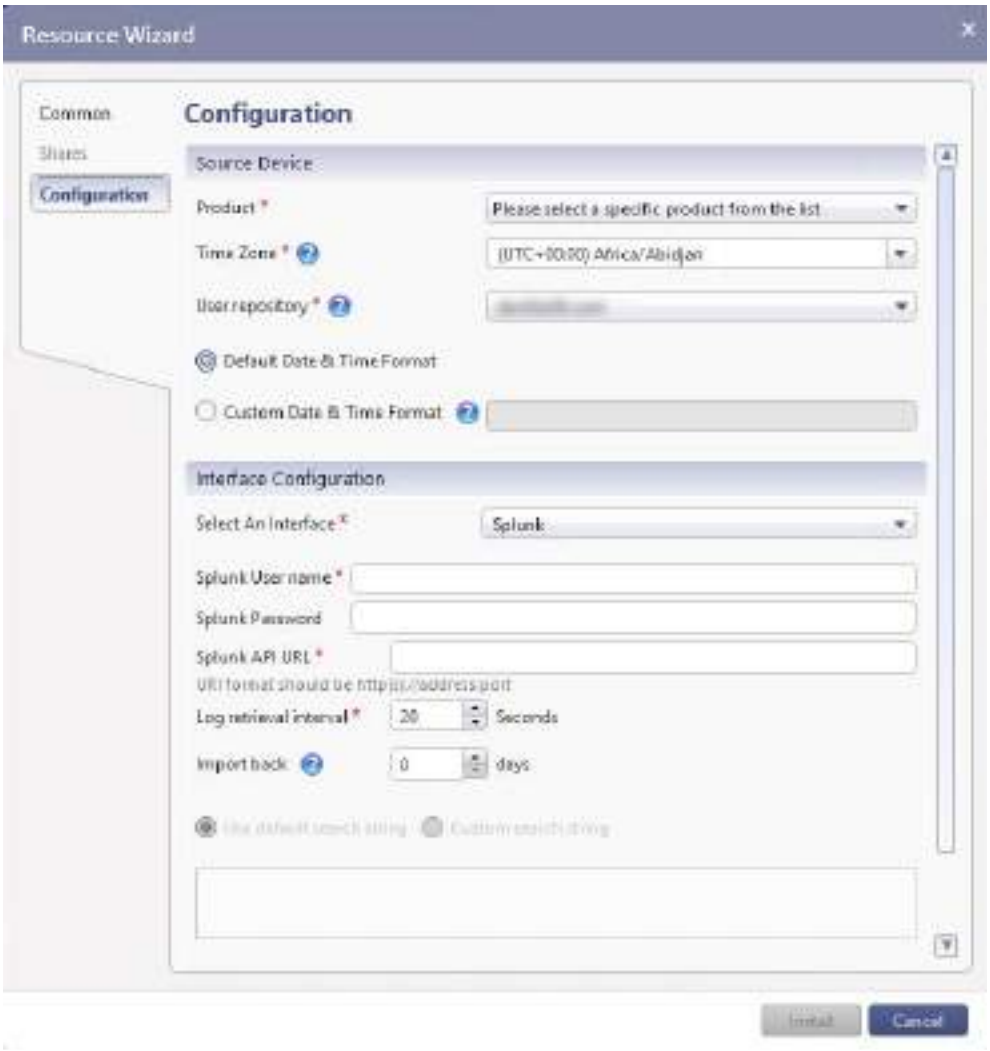
Configuring a New Network Device Data Source to Use Splunk

After adding a new network device data source, you can configure it to use Splunk to collect data.

Note:

- It is not recommended to deploy Splunk on the same machine as network device Collector. If there is no way to avoid this, then you need to change the Splunk port.
- When using network device data sources with Splunk, make sure that there are ports available in the range 34550-34600 on the localhost IP address 127.0.0.1.

1. Ensure that you have followed the procedure in Adding a New Network Device (Edge) Data Source. Make sure to do the following:
   a. In the Common pane in the Resource Wizard, specify the relevant Collector and data source details. From the Resource Type dropdown list, select Edge.
   b. In the Configuration pane in the Resource Wizard in the Source Device area, select the relevant product from the dropdown list and specify the relevant settings.



2. In the Interface Configuration area of the Configuration pane, do the following:
   a. Select an Interface - Select Splunk.
   b. Splunk User Name - Enter the Splunk API user name.
   c. Splunk Password - Enter the Splunk API password.
   d. Splunk API URL - The format is http://<host>:<port> or https://<host>:<port> where <host> is the IP address or host name of the Splunk server and <port> is the port configured in Splunk for the API. The default Splunk port is 8089 and must be specified.
   e. Log retrieval interval - Specify the interval for retrieving Splunk event logs. The default is 20 seconds. The maximum allowed is 60 seconds.
   f. Import back__days - Imports past events from Splunk for network device sources which support importing real-time events. It is possible to select up to 30 days back.

g. Use default search string - Enables you to keep the provided default string (displayed at the bottom). The default search string is useful if using the standard Splunk App provided by the device to audit events.

h. Custom search string - Enables you to modify the default search string. Ensure the _raw field is returned in the search results. Test the custom search string on your Splunk Enterprise console.

3. To test whether the connection is working, click the Test Connection button (scroll down to the bottom of the Interface Configuration area to see it). If it is not working, a warning notification is displayed.



4. Click Install.
The network device data source is installed, and configured to use Splunk to collect data.

Configuring a New Network Device (Edge) Data Source to Use Syslog

After adding a new network device data source, you can configure it to use Syslog to collect data.

> Note: Even though some third-party systems allow using RFC 6587 transmission of Syslog messages over TCP, this RFC is not supported by Varonis, and should not be selected.

1. Ensure that you have followed the procedure in Adding a New Network Device (Edge) Data Source. Make sure to do the following:
   a. In the Common pane in the Resource Wizard, specify the relevant Collector and data source details. From the Resource Type dropdown list, select Edge.

b. In the Configuration pane in the Resource Wizard in the Source Device area, select the relevant product from the dropdown list and specify the relevant settings.



2. In the Interface Configuration area of the Configuration pane, do the following:
   a. Select an Interface - The recommended interface is automatically selected per the selected product. Select Syslog from the dropdown list (if it's not already selected).
   b. Protocol - TCP. The recommended protocol is automatically selected per the selected product. By default, if both TCP and UDP are supported by the source product, TCP is displayed.
   c. IP Address - The Collector IP address that will be used to receive Syslog messages. Use Default for the Collector primary IP address.
   d. Port - Select the port that will be used to receive Syslog messages.
3. Click Check Settings.
   A message confirms whether the interface settings were successfully checked or if the selected port is already taken.
4. Click Install.

The network device data source is installed, and configured to use Syslog to collect data.

Configuring a New Network Device (Edge) Data Source to Use Filebeat

After adding a new network device data source, you can configure it to either automatically or manually use Filebeat to collect data. This option is currently supported only for Microsoft DNS sources.

When configuring Microsoft DNS Servers to generate log files, you need to configure the DNS servers to create debug log files, and then add NXLog or Filebeat to read the log files and send the data to Varonis.

Follow the instructions below to configure the network device data source to automatically use Filebeat to collect data or to manually add Filebeat to read the log files and send the data to Varonis.

Automatic Filebeat Deployment

To configure an network device data source to automatically use Filebeat to collect data:

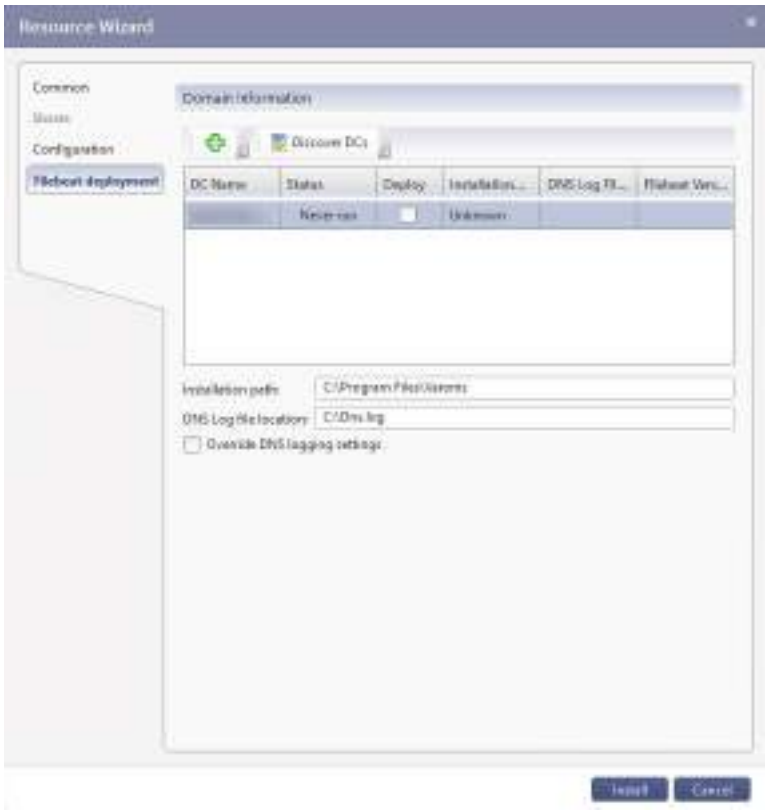
1. Ensure that you have followed the procedure in Adding a New Network Device (Edge) Data Source. Make sure to do the following:
   a. In the Common pane in the Resource Wizard, select Edge from the Resource Type dropdown list.
   b. In the Configuration pane in the Resource Wizard in the Source Device area, select Microsoft DNS Server from the Product dropdown list, and specify the relevant settings.



2. In the Interface Configuration area in the Configuration pane, set the following parameters:
   - Select an Interface - Select Filebeat.
   - Protocol - Select TCP.
   - IP Address - Select the IP address from the dropdown list.
   - Port - Enter the port number.
3. To automatically deploy Filebeat on a Domain Controller server:
   a. Ensure that you have fulfilled the prerequisites for automatic Filebeat deployment described in Network Devices (Varonis Edge) Requirements.
   b. In the Filebeat Deployment pane in the Resource Wizard, view a list of Domain Controller servers in the grid. Only the Domain Controllers that are also DNS servers are displayed.

   Note:
   - If the Filebeat Deployment tab is not displayed, go to the Management Console > Tools > Advanced Application Configuration, and set IsRemoteDcAndFilebeatConfigurationEnabled to 1 to enable the display of this tab.

- You can automatically redeploy Filebeat on selected DNS servers to add heartbeats between Filebeat and the network device service.



c. Do one of the following:

- Click Discover DCs to auto-discover the domain controllers in the domain.
- Click Add to add a new Domain Controller server for Filebeat deployment. In the Servers Picker, browse to select the DC server that you want to add. Use the CTRL key to multi-select and add multiple servers at once.



The selected DC servers are displayed in the grid in the main Filebeat Deployment pane.

d. In the Installation path text box (below the grid), specify the installation directory location for Filebeat deployment, or leave the default path, C:\ProgramFiles\Varonis.

> Note: Filebeat cannot be deployed on a network drive and the installation path cannot contain special characters, such as '$'.

e. By default, the Override DNS logging settings checkbox is cleared to prevent overriding the debug logging settings in the customer's Domain Controller server. To override the existing Microsoft DNS settings when automatically deploying Filebeat, select the Override DNS logging settings checkbox. For more information about configuring DNS servers to create debug log files, see Configuring Microsoft DNS Servers to Generate Log Files.

f. To deploy Filebeat on a Domain Controller server, from the grid, select the relevant DC server with Status "Never run" (use the CTRL key to multi-select multiple servers), click Deploy, and in the Domain User Credentials dialog box, enter the Domain Admin credentials for the PowerShell scripts.
When deployment is successful, the Status column displays Succeeded.

4. Click Install.
The network device data source is installed, and configured to use Filebeat to collect data.

Manual Filebeat Deployment

To manually deploy Filebeat to forward log files to Varonis:

1. In the Management Console, ensure that you configured the DNS data source to use Filebeat.
2. Download the deployment package. Access the Varonis portal through https://help.varonis.com/s/my-downloads and select Edge tools. This will download the Edge tools ZIP.
3. Unzip Edge tools, open the `Edge tools\ManualFilebeatDeploymentPack` folder.
4. Edit the `FilebeatManualDeploy.bat` file; change the following values:
   - `<collector IP address>` - The IP address of Varonis Collector. Use the same value as configured for the network device data source in the Varonis Management Console.

- `<destination Port>` - The port configured for the network device data source in the Varonis Management Console.
- For remote installation, specify the DC host or IP address. `"localhost"` is for local installation.

5. On each DC, copy the folder and execute the `FilebeatManualDeploy.bat` file.
6. For remote installation, you'll need to enter the username and password for the DC host.

Configuring Advanced Filter IP Ranges for Proxy Data Sources

You can configure filtering functionality in the Varonis Forwarder for Proxy data sources.

Filtering by IP Ranges

You can reduce noise (alerts and events) created by specific ranges of IP addresses using the following settings:

To apply a filter range to a specific Proxy data source:

1. Set an additional option to the application configuration file for each data source. The default location of the configuration file is:

```
"Installation Folder\Varonis\DatAdvantage\Streams\Varonis
.Agents.Collector.Streaqw#i1i#gsr k?
```

2. Set the option according to the following format:

```
<add key="FilteringByIPAddressRanges_Proxy_{FilerId}" val
ue="x.x.x.x-x.x.x.x,x.x.x.x-x.x.x.x"
```

   Where FilerId is an ID of the data source installed on the Collector. It can be found in the `input.conf` file of Logstash. For example:

```
C:\Logstawl;Esr kyvations\input.conf
```

Where x.x.x.x is any IPv4 address.



For example:

```
<add key="FilteringByIPAddressRanges_Proxy_1" value="10.0
.0.1-11.0.0.1,192.168.1.1-193.0.1.1 "
```

Multiple ranges can be set. Each data source can be configured with only one set of ranges.

Filtering Process Details

Filtering is applied for each event in several steps:

1. Check the stream type of the event.
2. Get all filters accepted to the selected stream type.
3. Apply the chain of filters for the event.
4. An event will be excluded from processing after the first filter isn't passed.

Date and Time Format Notation

When adding a new data source in the Management Console, you can set the date and time format, as needed.
The syntax used for parsing date and time text uses letters to indicate the type of time value (month, minute, and so on), and a repetition of letters to indicate the form of that value (2-digit month, full month name, and so on).

Other characters, such as separators, are specified as is.

For example, the following are some dates, times, and the matching date format specifiers:

- 23/12/2018 15:32:21 - dd/MM/yyyy HH:mm:ss
- 12-23-2018 03:32:21 pm - MM-dd-yyyy hh:mm:ss

The following is what you can use to parse the dates and times:

- Year:
  - yyyy - Full year number. Example: 2015.
  - yy - Two-digit year. Example: 15 for the year 2015.
- The month and the year:
  - M - Minimal-digit month. Example: 1 for January and 12 for December.
  - MM - Two-digit month. Zero-padded if needed. Example: 01 for January and 12 for December.
  - MMM - Abbreviated month text. Example: Jan for January. Note: The language used depends on your locale. See the locale setting for how to change the language.
  - MMMM - Full month text, Example: January. Note: The language used depends on your locale.
- Day of the month:
  - d - Minimal-digit day. Example: 1 for the 1st of the month.
  - dd - Two-digit day, zero-padded if needed. Example: 01 for the 1st of the month.
- Hour of the day:
  - H - 24-hour clock minimal-digit hour. Example: 0 for midnight.
  - HH - 24-hour clock two-digit hour, zero-padded if needed. Example: 00 for midnight.
  - h - 12-hour clock minimal-digit hour. Example: 0 for midnight.
  - hh - 12-hour clock two-digit hour, zero-padded if needed. Example: 00 for midnight.
  - a - Specifies either am or pm
- Minutes of the hour (60 minutes per hour):
  - m - Minimal-digit minutes. Example: 0.
  - mm - Two-digit minutes, zero-padded if needed. Example: 00.
- Seconds of the minute (60 seconds per minute):

- s - Minimal-digit seconds. Example: 0.
- ss - Two-digit seconds, zero-padded if needed. Example: 00.

For less common formatting options, click here.

Configuring VPN Sources To Send Events To Varonis

This section describes how to configure VPN Sources to send events to Varonis.

F5 Big-IP Access Policy Manager (APM)

Varonis supports receiving VPN events from the F5 Big-IP Access Policy Manager (APM) via Syslog.
F5 Big-IP Access Policy Manager (APM) provides information on how to send events via Syslog to Varonis in the article Configuring the BIG-IP System to Log to a Remote Syslog Server. This article outlines the specific procedure for sending events to Varonis.

Prerequisites for F5 Big-IP Access Policy Manager

Before you begin configuring F5 Big-IP Access Policy Manager to send VPN events to Varonis, you must follow several prerequisites.

- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.

Configure F5 BIG-IP Logging Using a Command Line Interface

Varonis supports receiving VPN events from F5 BIG-IP via both UDP and TCP.

Configure Remote Logging via UDP Using a Command Line interface (CLI)

1. Connect to the F5 appliance via SSH with your credentials (username and password).
2. Log into `tmsh` by entering the following command:

   ```
   # tmsh
   ```

   Some systems are configured to use `tmsh` as a default option so then you don't need this step.
3. Check the current logging configuration:

```
# list /sys syslog remote-servers
sys syslog {
remote-servers none
}
```

4. Configure the Syslog server with IP 10.11.12.13 and UDP port 789:

```
# modify /sys syslog remote-servers add { remotesyslog {h
ost 10.11.12.13 remote-port 789}}
```

If you already have remotesyslog in your configuration - you can use `remotesyslog2` instead:

```
# modify /sys syslog remote-servers add { remotesyslog2 {
host 10.11.12.13 remote-port 789}}
```

5. Check the configuration after modification:

```
# list /sys syslog remote-servers
sys syslog {
remote-servers {
remotesyslog {
host 10.11.12.13
remote-port 789
}
}
}
```

6. Save the configuration after modification:

```
# save /sys gsr k
```

Configure Remote Logging via TCP Using a Command Line interface (CLI)

1. Connect to F5 appliance via SSH with your credentials (username and password).
2. Log into `tmsh` by entering the following command:

```
# tmsh
```

Some systems are configured to use `tmsh` as a default option so then you don't need this step.

3. Configure the Syslog server with IP 10.21.77.14 and TCP port 514:

```
# modify /sys syslog include "destination remote_server {
tcp(10.21.77.14 port \958""=|= pxiv f_alllogs {level (deb
ug...emerg);};log /wsyvgi\w w2wpsk tmti"= pxiv\j epppskw"
=hiwxmrexmsr\viqsxi wivziv"=|=?
```

4. Check the configuration after modification:

```
# list /sys syslog include
sys syslog {
include "destination remote_server {tcp(10.21.77.14 port
\958""=|= pxiv f_alllogs {level (debug...emerg);};log /ws
yvgi\w w2wpsk tmti"= pxiv\j epppskw"=hiwxmrexmsr\viqsxi w
ivziv"=|=?
}
```

5. Save the configuration after modification:

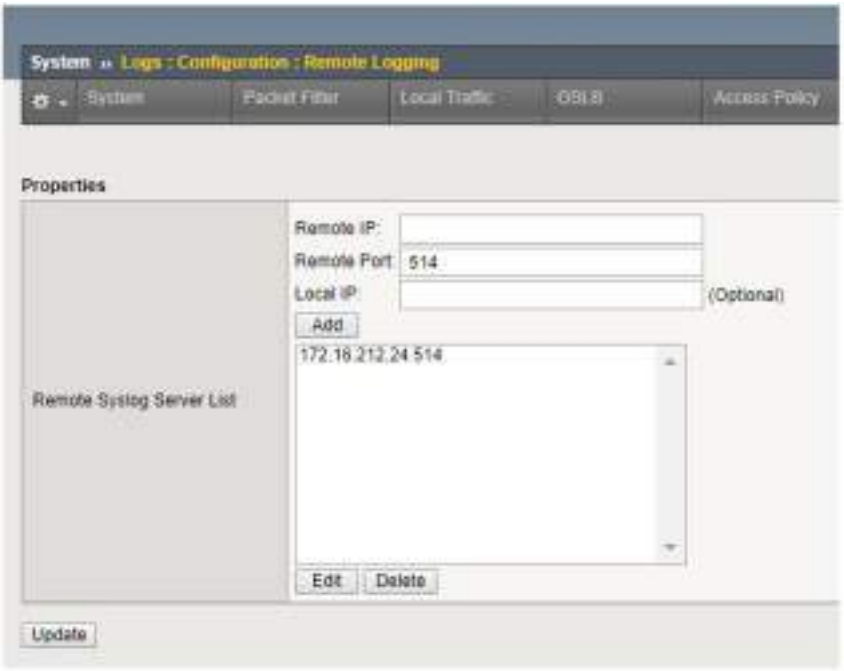
```
# save /sys gsr k
```

Configuring the Syslog Server Using UDP

You can use UDP to configure a Syslog server for logging events.

1. In the F5 configuration utility, from the Main navigation pane on the left, select System > Logs > Configuration > Remote Logging.

The Remote Logging window is displayed.



2. For the following, enter the same value as configured for the network device data source in the Varonis Management Console:
   - Remote IP
   - Remote Port

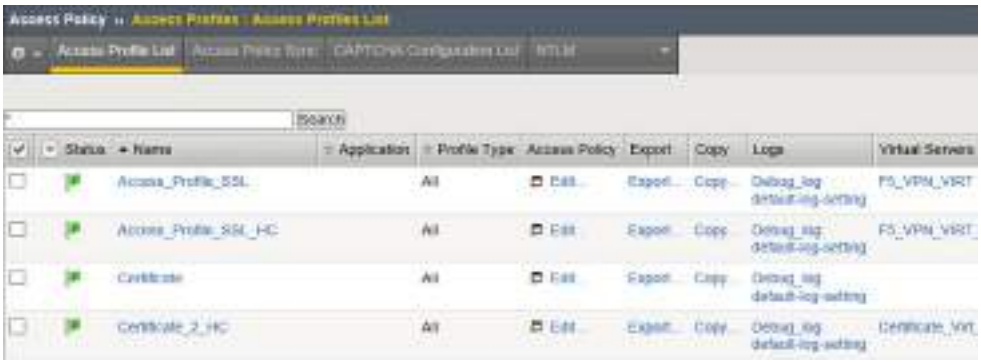
   For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.
3. Click Add, and then click Update.
   The Syslog server is configured.

Adding a Machine Info Step to Access Policies (Optional)

After configuring the Syslog server, it is recommended (though not mandatory) to add a machine info step to log client information such as the MAC address.

1. To view a list of your access profiles, from the main navigation pane on the left, select Access Policy > Access Profiles > Access Profiles List.

The Access Profiles List window is displayed.



2. For each profile of the LTM-APM or All types, add a “Machine Info” item to the access policy to ensure that the events include the remote device MAC address.
   a. Click Edit.
   b. Click the first “+” sign in the access policy.



   c. Select the Endpoint Security (Client-Side) tab.
   d. Select Machine Info.

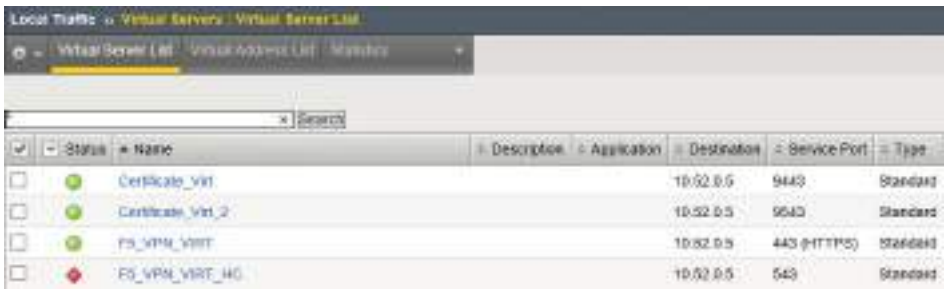


   e. Click Add Item.
   f. Click Save.

Verifying Attached Virtual Servers

After configuring the Syslog server, you must attach a virtual server to each active profile of the LTM-APM or All types.

1. From the main navigation pane on the left, select Local Traffic > Virtual Servers > Virtual Servers List.
   The Virtual Servers List window is displayed.



2. If no virtual servers are attached to the active profiles, attach them by editing the virtual server properties.
3. Save all work when done.

Palo Alto GlobalProtect

Varonis supports receiving VPN events from a Palo Alto Firewall.
Palo Alto provides information on how to send events to a third-party system such as Varonis in the article Configure Syslog Monitoring.

> Note: It is possible to configure log settings from Palo Alto Networks Panorama as well. The configuration steps are similar to those described in the following sections.

PAN-OS 8.x

This section describes the procedures required for PAN-OS version 8.x.

Prerequisites for Palo Alto GlobalProtect

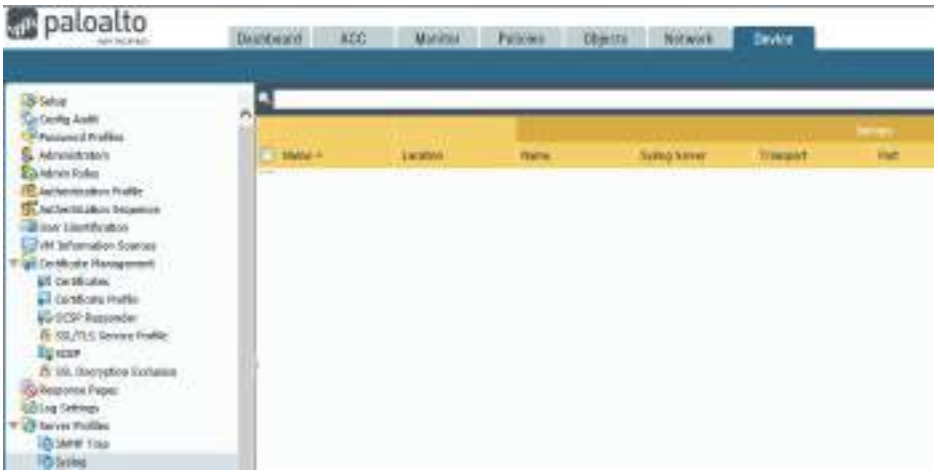
Before you begin configuring Palo Alto GlobalProtect to send VPN events to Varonis, you must follow several prerequisites.

- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.

Creating a Syslog Server Profile

The Palo Alto GlobalProtect configuration process requires creating a Syslog server profile.

1. From the Palo Alto main window, select the Device tab.
   The Device window is displayed.
2. From the navigation pane on the left, select Server Profiles > Syslog.
   The Syslog window is displayed.



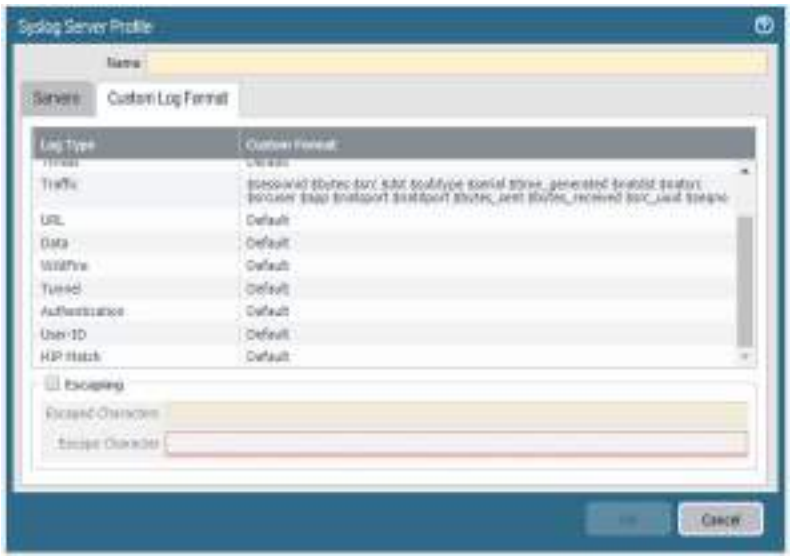
3. From the bottom, click Add.
   The Syslog Server Profile dialog box is displayed.
4. Click Add to add a new server. Enter the following:
   - Name - Enter any name such as Varonis or the name of the specific network device Collector used, for example Varonis NYC Collector.
   - Syslog Server - The IP address or FQDN. Use the same value as configured for the network device data source in the Varonis Management Console.
   - Transport - Select TCP, UDP, or SSL as the protocol for communicating with the Syslog server.
   - Port - The port configured for the network device data source in the Varonis Management Console.
   - Format - Select BSD.
   - Facility - Select any value.



5. Select the Custom Log Format tab.
6. Click the traffic log type format, and in the Custom Format column, modify the format to:

   Note: When copying this string, ensure it is copied as a single line and there is a space between the parts appearing here on separate lines.

```
$sessionid $bytes $src $dst $subtype $serial $time_genera
ted $natdst $natsrc $srcuser $app $natsport $natdport $by
tes_sent $bytes_received $src_uuid $seqno
```



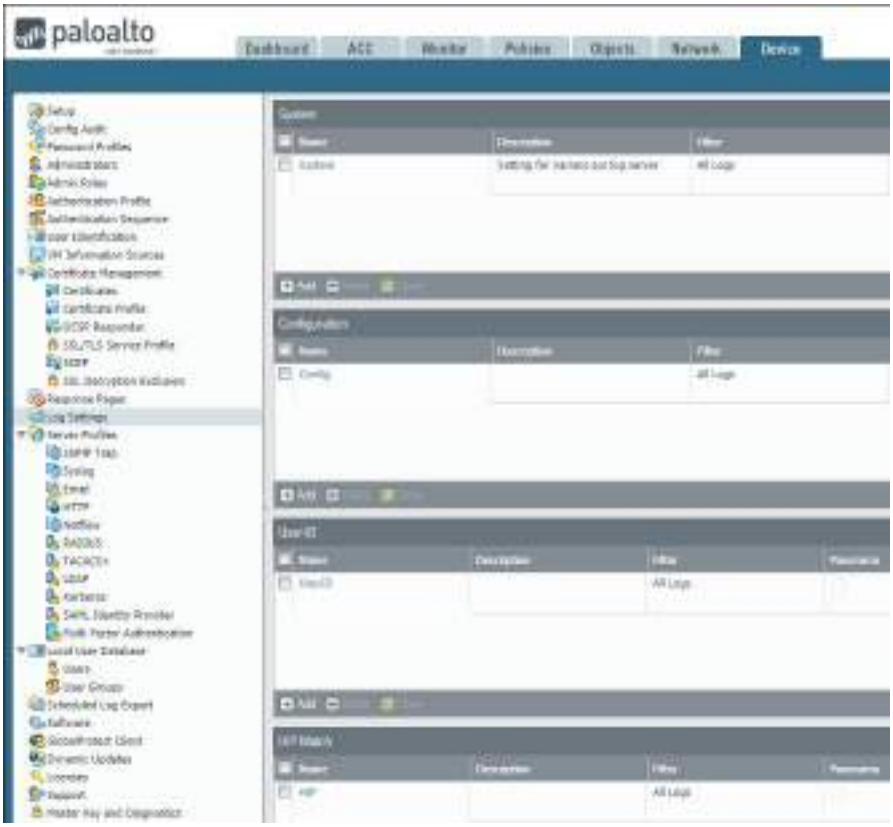
7. Ensure that the tunnel and authentication log type formats are set to Default.
8. Click OK.
   A new Syslog server profile is created.

Configuring Log Settings

You can configure the log settings for Palo Alto GlobalProtect.

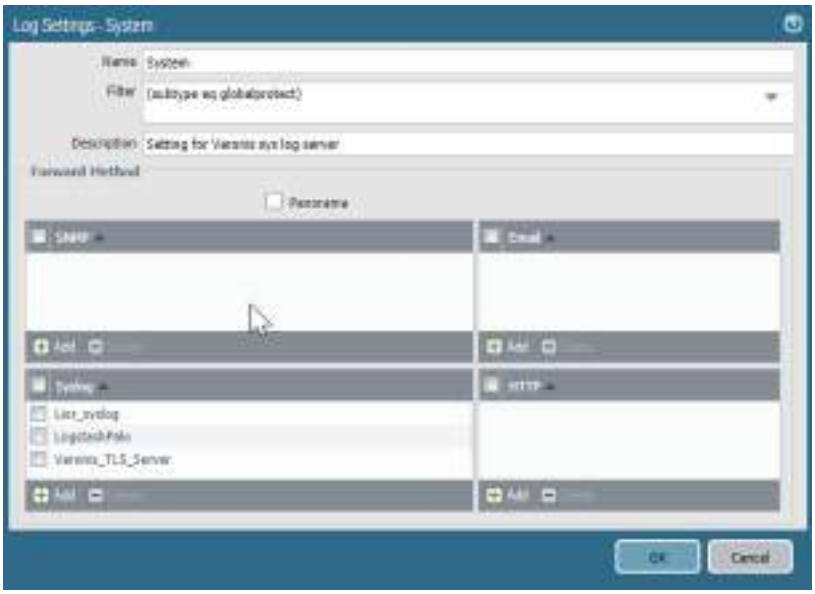
To configure the log settings:

1. From the Palo Alto main window, select the Device tab.
2. From the navigation pane on the left, select Log Settings.



3. For the System section, do the following:
   a. Click Add.
   b. In the Name field, specify a name, such as varonis-system-log-setting, and so on.
   c. In Filter, enter (subtype eq globalprotect).
   (subtype eq globalprotect)
   d. Add the Syslog server profile created above to the Syslog section.

e. Click OK.



4. In the Device tab, click OK.

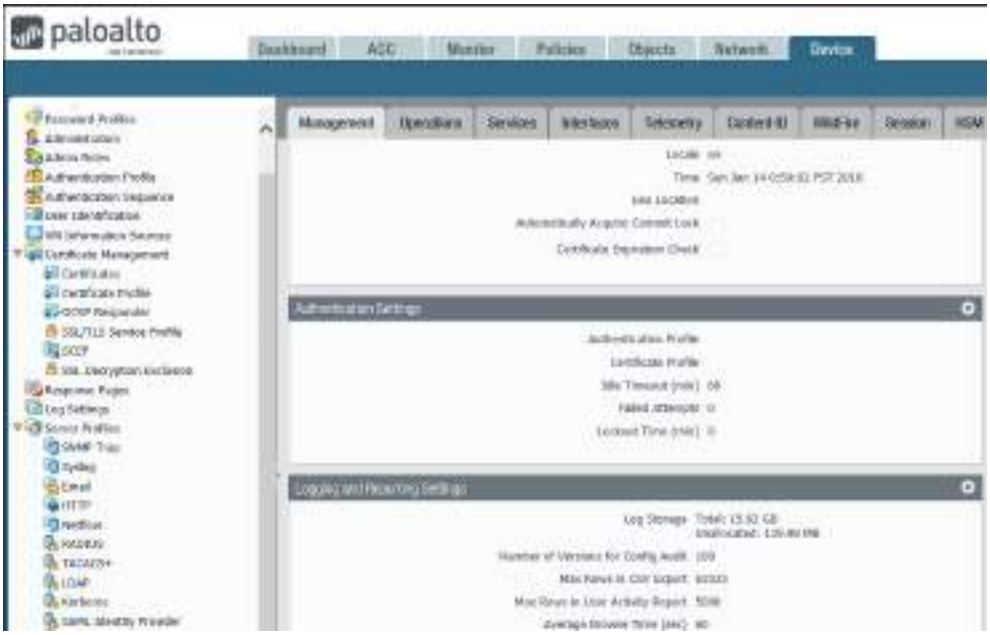
Configuring the Header Format of Syslog Messages

After you have configured the log settings it is important to configure the header format of Syslog messages.

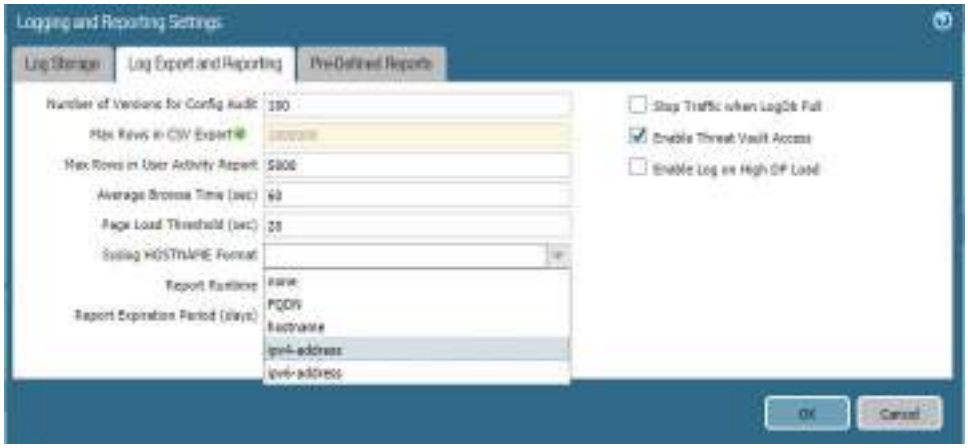
To configure the header format of Syslog messages:

1. Select the Device tab.
   The Device window is displayed.
2. From the navigation pane on the left, select Setup.

3. Select the Management tab.



4. In the Logging and Reporting Settings area, click the edit wheel on the upper right. The area is displayed in edit mode.
5. Select the Log Export and Reporting Settings tab.
6. In the Syslog HOSTNAME Format field, select ipv4-address or FQDN.



7. Click OK.

The Logging and Reporting Settings area is updated.



Committing the Changes

After configuring Palo Alto GlobalProtect and performing all the previous relevant procedures, it is necessary to commit all changes.

To commit the changes:

From of the top of the Palo Alto window, click Commit.
All changes are committed.

PAN-OS 9.x

This section describes the procedures required for PAN-OS version 9.x.

Prerequisites for Palo Alto GlobalProtect

Before you begin configuring Palo Alto GlobalProtect to send VPN events to Varonis, you must follow several prerequisites.

- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.

Creating a Syslog Server Profile

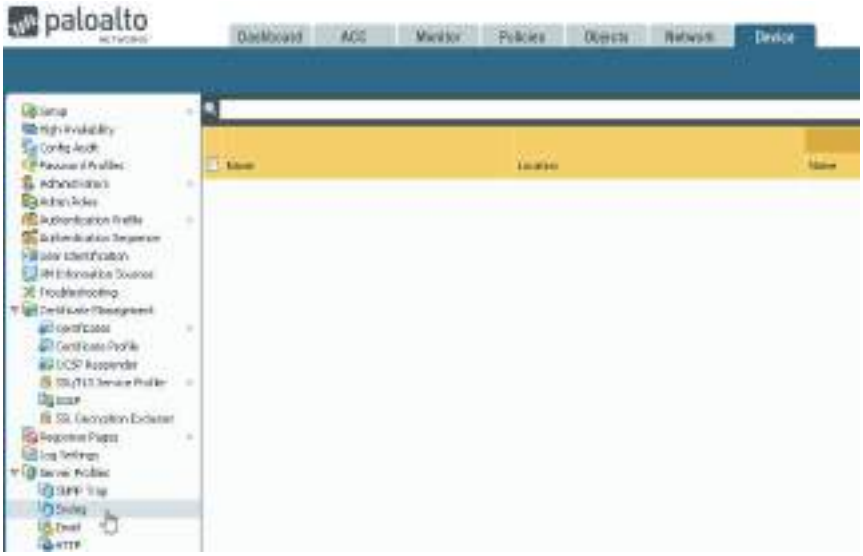
The Palo Alto GlobalProtect configuration process requires creating a Syslog server profile.

1. From the Palo Alto main window, select the Device tab.

The Device window is displayed.



2. From the navigation pane on the left, select Server Profiles > Syslog.
   The Syslog window is displayed.



3. From the bottom, click Add.
   The Syslog Server Profile dialog box is displayed.



4. Click Add to add a new server. Enter the following:
   - Name - Select any name such as Varonis or the name of the specific network device Collector used, for example Varonis NYC Collector.
   - Syslog Server - The IP address or FQDN.
   - Transport - Select TCP or UDP as the protocol for communicating with the Syslog server. Enter the same value as configured for the network device data source in the Varonis Management Console.
   - Port - Enter the same value as configured for the network device data source in the Varonis Management Console
   - Format - Select BSD.

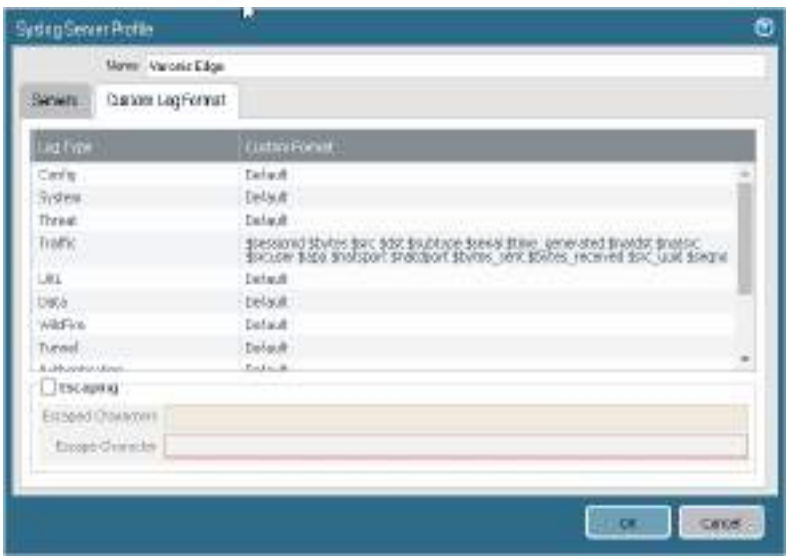
- Facility - Select any value.



5. Select the Custom Log Format tab.
6. Click the traffic log type format, and in the Custom Format column, modify the format to:

> Note: When copying this string, ensure it is copied as a single line and there is a space between the parts appearing here on separate lines.

```
$sessionid $bytes $src $dst $subtype $serial $time_genera
ted $natdst $natsrc $srcuser $app $natsport $natdport $by
tes_sent $bytes_received $src_uuid $seqno
```



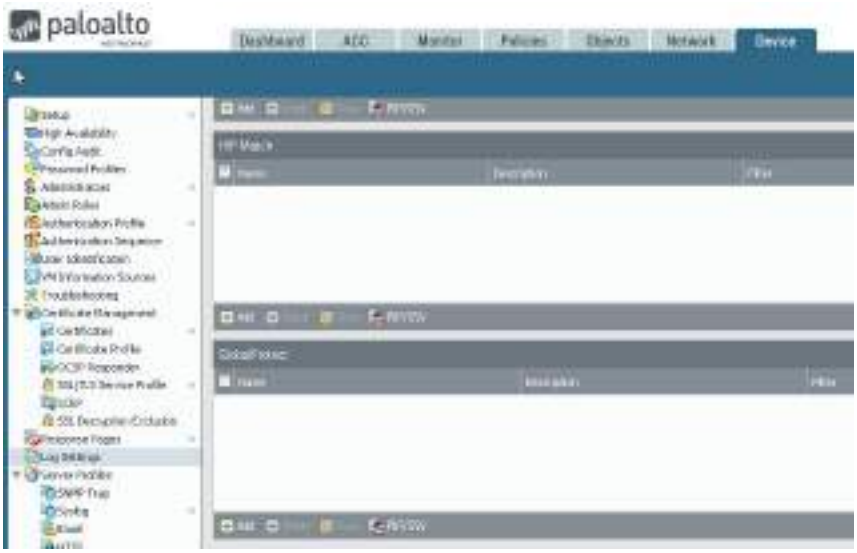
7. Ensure that the tunnel and authentication log type formats are set to Default.
8. Click OK.
   A new Syslog server profile is created.

Configuring Log Settings

You can configure the log settings for Palo Alto GlobalProtect.

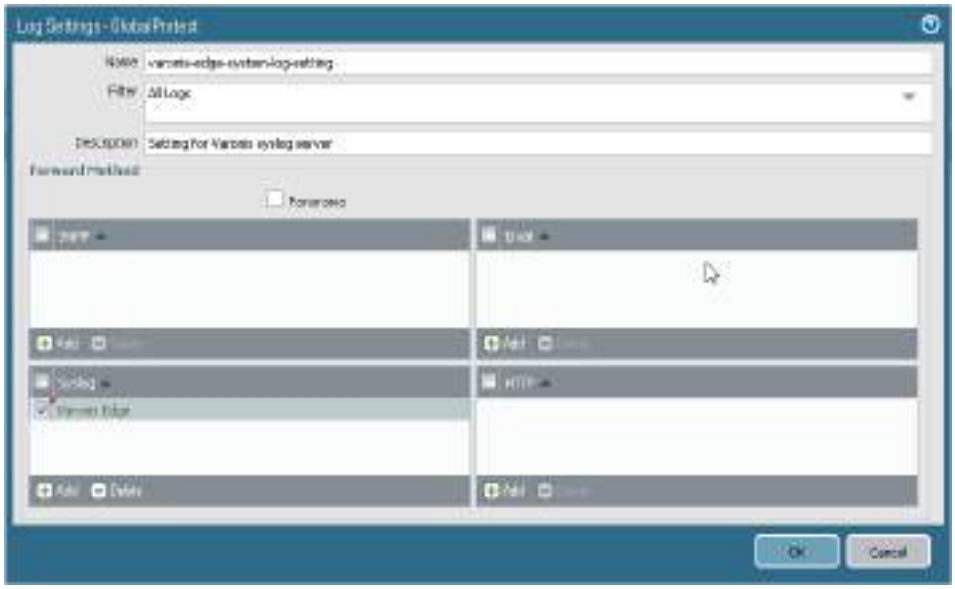
To configure the log settings:

1. From the Palo Alto main window, select the Device tab.
2. From the navigation pane on the left, select Log Settings.



3. For the GlobalProtect section, do the following:
   a. Click Add.
   b. In the Name field, specify a name, such as varonis-system-log-setting, and so on.
   c. Add the Syslog server profile created above to the Syslog section.

d. Click OK.



4. In the Device tab, click OK.

Configuring the Header Format of Syslog Messages

After you have configured the log settings, it is important to configure the header format of Syslog messages.

To configure the header format of Syslog messages:

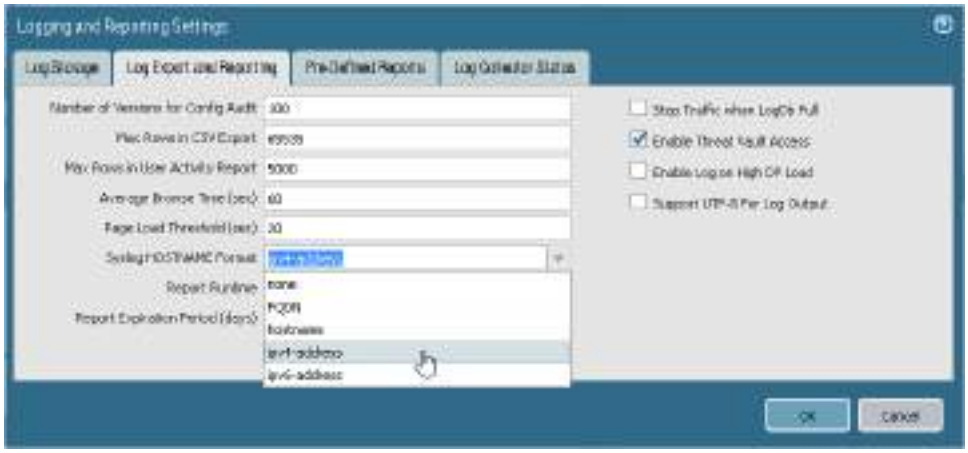
1. Select the Device tab.
   The Device window is displayed.
2. From the navigation pane on the left, select Setup.
3. Select the Management tab.



4. In the Logging and Reporting Settings area, click the edit wheel on the upper right.

The area is displayed in edit mode.

5. Select the Log Export and Reporting Settings tab.
6. In the Syslog HOSTNAME Format field, select ipv4-address or FQDN.



7. Click OK.
   The Logging and Reporting Settings area is updated.



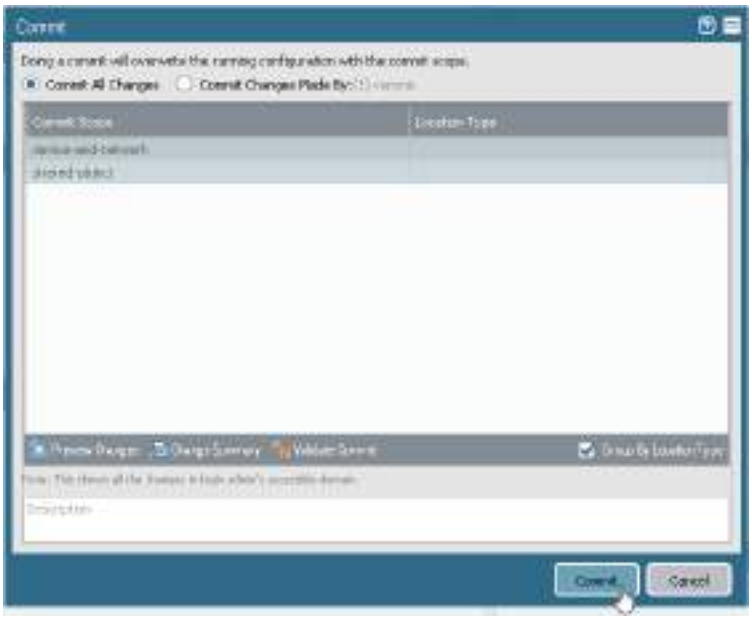
Committing the Changes

After configuring Palo Alto GlobalProtect and performing all the previous relevant procedures, it is necessary to commit all changes.

To commit the changes:

From of the top of the Palo Alto window, click Commit.





All changes are committed.

PAN-OS 10.x and 11.x

This section describes the procedures required for PAN-OS versions 10.x and 11.x.

Prerequisites for Palo Alto GlobalProtect

Before you begin configuring Palo Alto GlobalProtect to send VPN events to Varonis, you must follow several prerequisites.

- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.

Creating a Syslog Server Profile

The Palo Alto GlobalProtect configuration process requires creating a Syslog server profile.

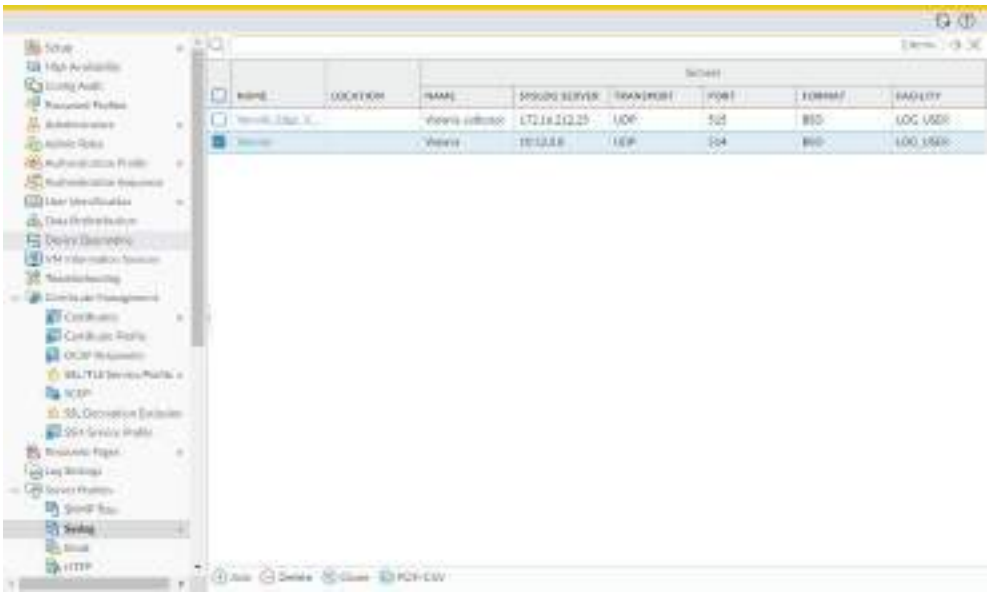
To create a Syslog server profile:

1. From the Palo Alto main window, select the Device tab.
   The Device window is displayed.



2. From the navigation pane on the left, select Server Profiles > Syslog.

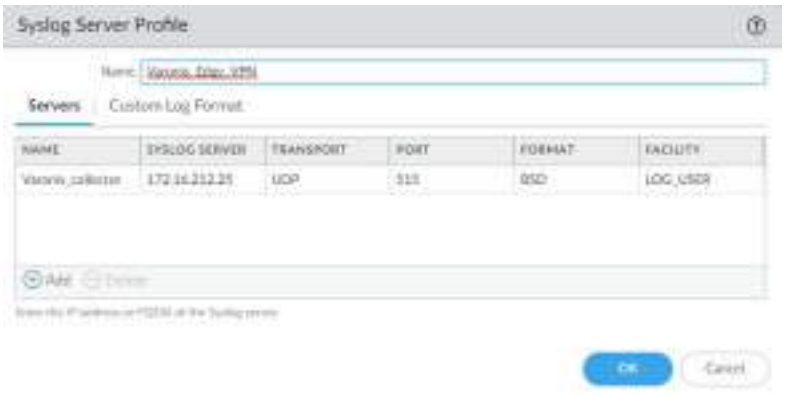
The Syslog window is displayed.



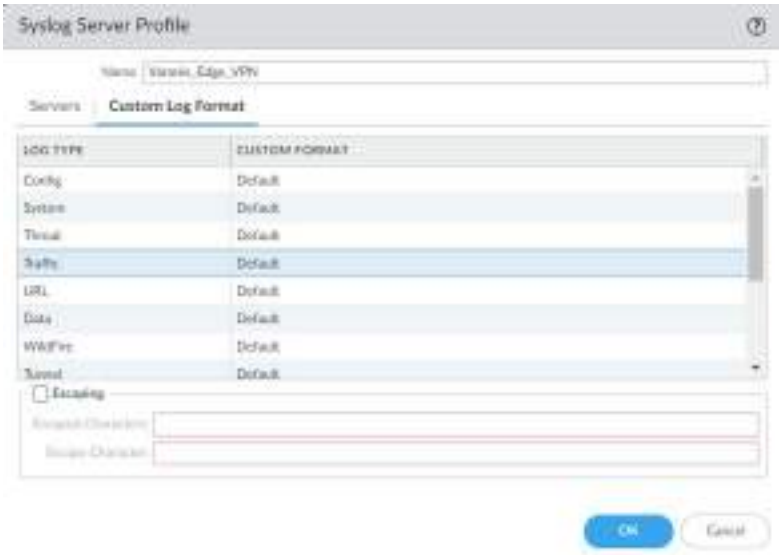
3. From the bottom, click Add.
   The Syslog Server Profile dialog box is displayed.



4. Click Add to add a new server. Enter the following:
   - Name - Enter any name such as Varonis or the name of the specific network device Collector used, for example Varonis NYC Collector.
   - Syslog Server - The IP address or FQDN configured for the network device data source in the Varonis Management Console.
   - Transport - Select TCP or UDP as the protocol for communicating with the Syslog server.
   - Port - The port configured for the network device data source in the Varonis Management Console.
   - Format - Select BSD.
   - Facility - Select any value.



5. Select the Custom Log Format tab.

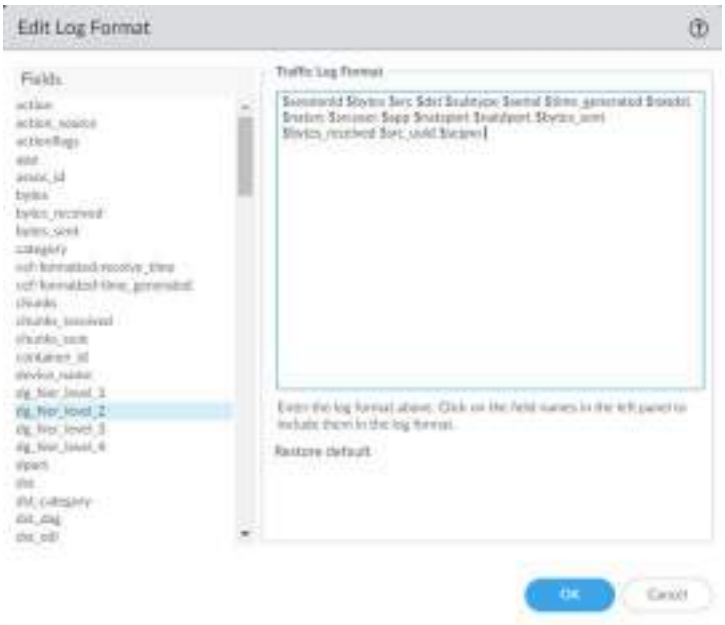


6. Click the traffic log type format, and in the Custom Format column, modify the format to:

> Note: When copying this string, ensure it is copied as a single line and there is a space between the parts appearing here on separate lines.

```
$sessionid $bytes $src $dst $subtype $serial $time_genera
ted $natdst $natsrc $srcuser $app $natsport $natdport $by
tes_sent $bytes_received $src_uuid $seqno
```

7. Ensure that the tunnel and authentication log type formats are set to Default.



8. Click OK.
   A new Syslog server profile is created.

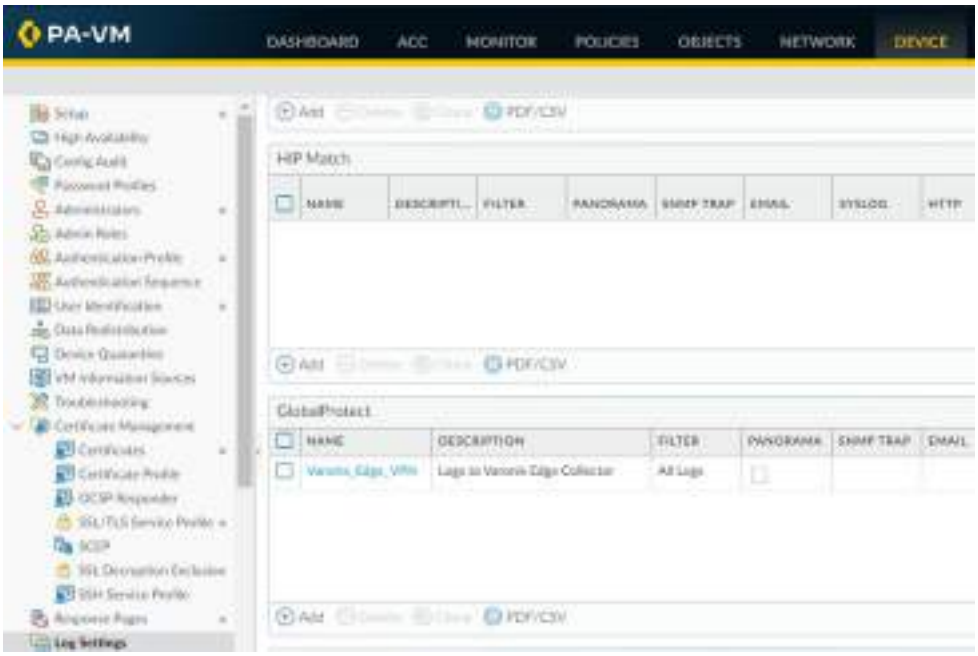
Configuring Log Settings

You can configure the log settings for Palo Alto GlobalProtect.

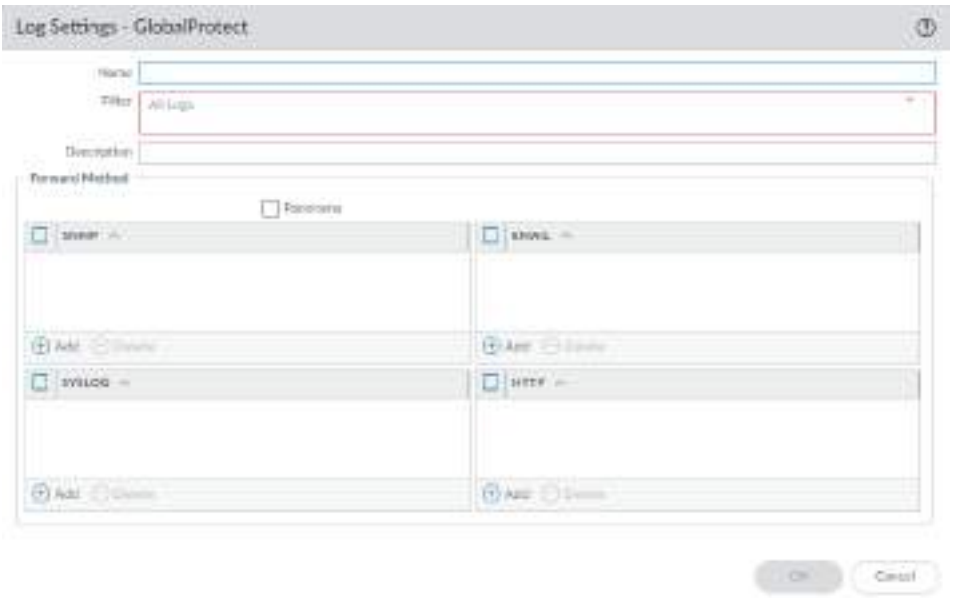
To configure the log settings:

1. From the Palo Alto main window, select the Device tab.

2. From the navigation pane on the left, select Log Settings.

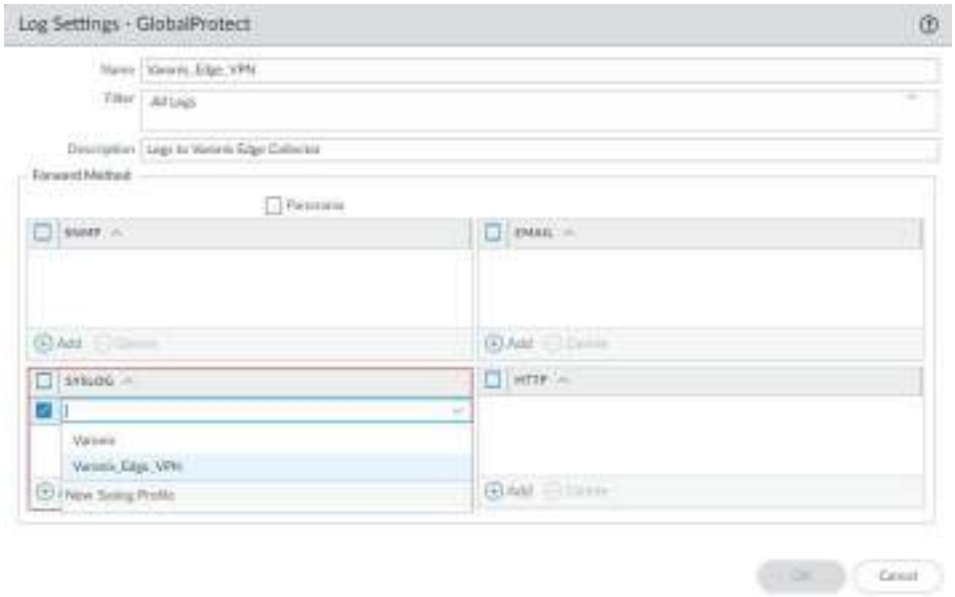


3. In the GlobalProtect area, do the following:
   a. Click Add.



   b. In the Name field, specify a name, such as varonis_vpn, and so on.
   c. Add the Syslog server profile created above to the Syslog section.

d. Click OK.



4. In the Device tab, click OK.

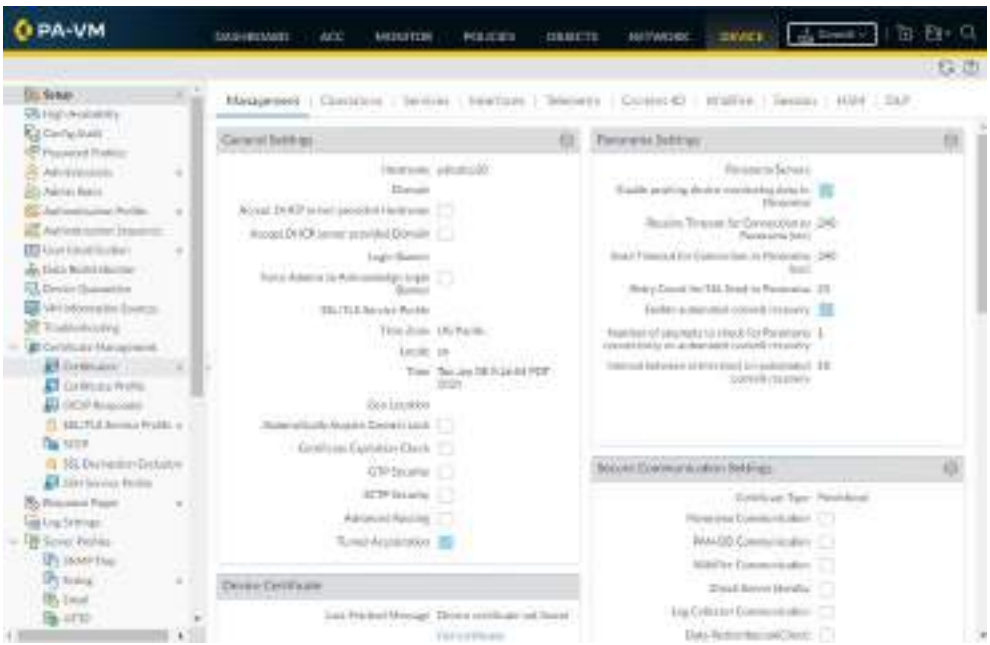
Configuring the Header Format of Syslog Messages

After you have configured the log settings, it is important to configure the header format of Syslog messages.

To configure the header format of Syslog messages:

1. Select the Device tab.

The Device window is displayed.



2. From the navigation pane on the left, select Setup.
3. Select the Management tab.



4. In the Logging and Reporting Settings area, click the edit wheel on the upper right. The area is displayed in edit mode.
5. Select the Log Export and Reporting Settings tab.

6. In the Syslog HOSTNAME Format field, select ipv4-address or FQDN.



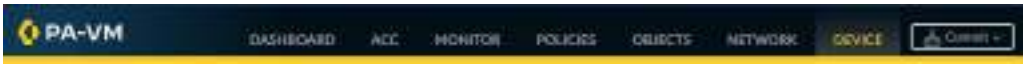
7. Click OK.
   The Logging and Reporting Settings area is updated.

Committing the Changes

After configuring Palo Alto GlobalProtect and performing all the previous relevant procedures, it is necessary to commit all changes.

To commit the changes:

From of the top of the Palo Alto window, click Commit.





All changes are committed.

Check Point VPN

Varonis supports receiving VPN events from Check Point's VPN feature (part of the Check Point Firewall).
Check Point provides information on how to send events to a third-party system such as Varonis.

Prerequisites for Check Point VPN

Before you begin configuring Check Point VPN to send VPN events to Varonis, you must follow several prerequisites.

- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.
- If using Syslog, ensure that the Log Exporter is installed for versions R80.10 and R77.30. For more information, see this article.

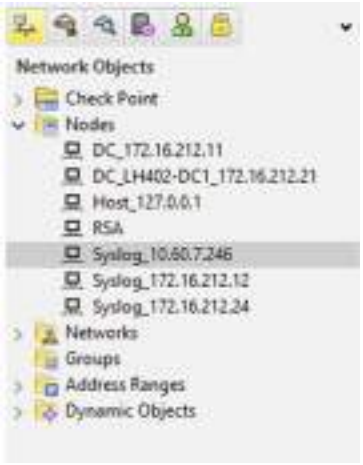
Defining the Network Device Collector as a Node

There are several steps involved in defining the network device Collector as a node.

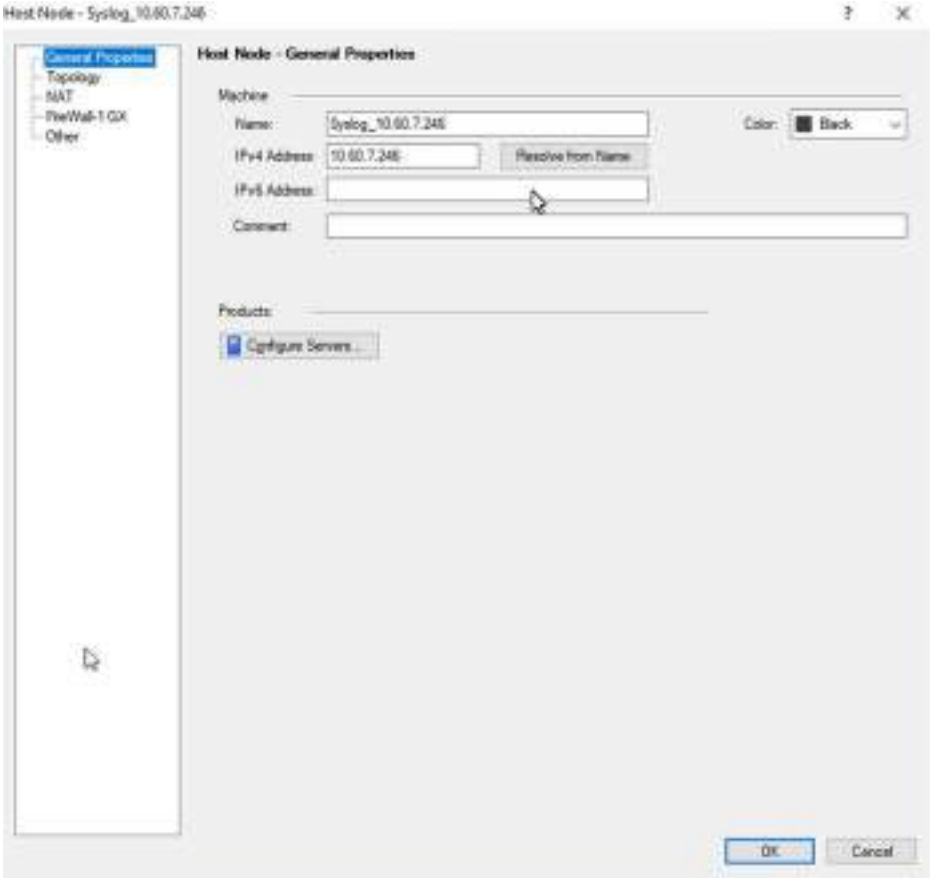
To define the network device Collector as a node:

1. Open the Check Point SmartDashboard.
2. In the lower left navigation pane, click the Network Object button.

The Network Objects tree is displayed.



3. Right-click Nodes and select Host.
   The Host Node dialog box is displayed.



4. In the Name field, enter a descriptive name.
5. In the IPv4 Address field, enter the IP address configured for the network device data source in the Varonis Management Console.
6. (Optional) In the Comment field, enter a free text comment.

7. (Optional) From the Color dropdown list, select the node color.
8. Click OK.

Check Point R77.x

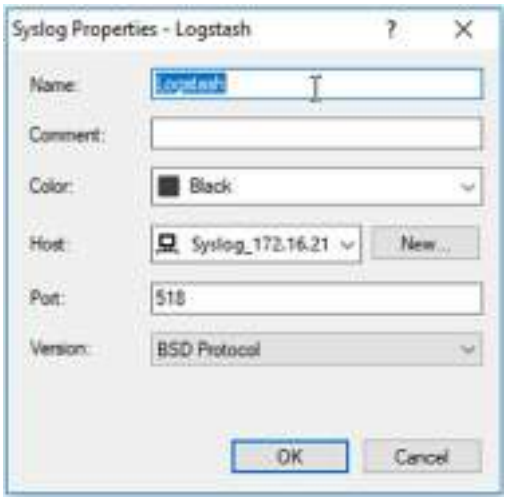
This section describes the procedures required for Check Point R77.x.

Configuring the Syslog Server

After defining the Varonis Collector as a node, you must configure the Syslog server.

To configure the Syslog server:

1. In the lower left pane, click the Servers and OPSec button.
   The Servers and OPSec navigation pane is displayed.
2. Right-click Servers > New > Syslog.
   The Syslog Properties Logstash dialog box is displayed.
3. Do the following:
   - Name - Enter a descriptive name.
   - Comment - (optional) Enter any useful free text comments.
   - Color - (optional) - Set the node color.
   - Host - Select the node defined in Defining the Network Device Collector as a Node.
   - Port - Specify the port configured for the network device data source in the Varonis Management Console.
   - Version - Select BSD Protocol.



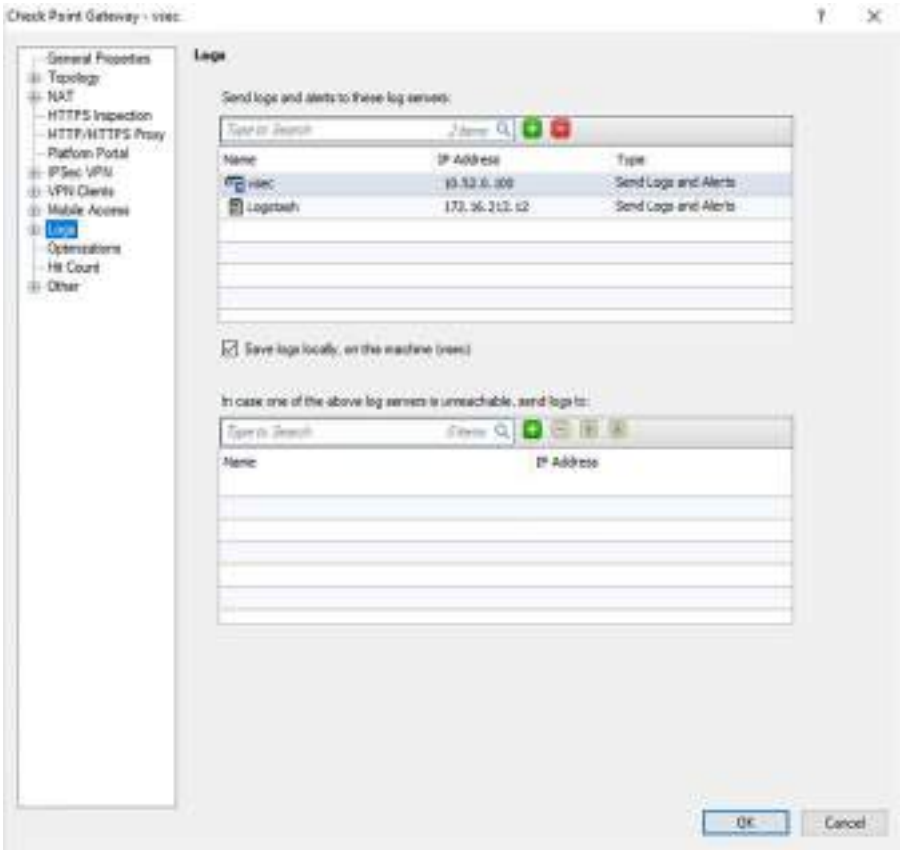
4. Click OK.

Configuring a Gateway to Send Logs to Syslog Servers

After you have configured Syslog servers, you can configure the gateway to send logs to them. To do so, ensure that the Syslog servers are the same type: BSD Protocol or Syslog Protocol.

To configure a gateway to send logs to Syslog servers:

1. In the lower left pane, click the Network Objects button.
   The Network Objects tree is displayed.
2. Under CheckPoint, double-click the CheckPoint gateway.
   The Gateway Properties dialog box is displayed.
3. From the navigation pane on the left, select Logs.
4. In the Send Logs and Alerts to These Log Servers table, click the green Add button and add the Syslog server defined in Configuring the Syslog Server.



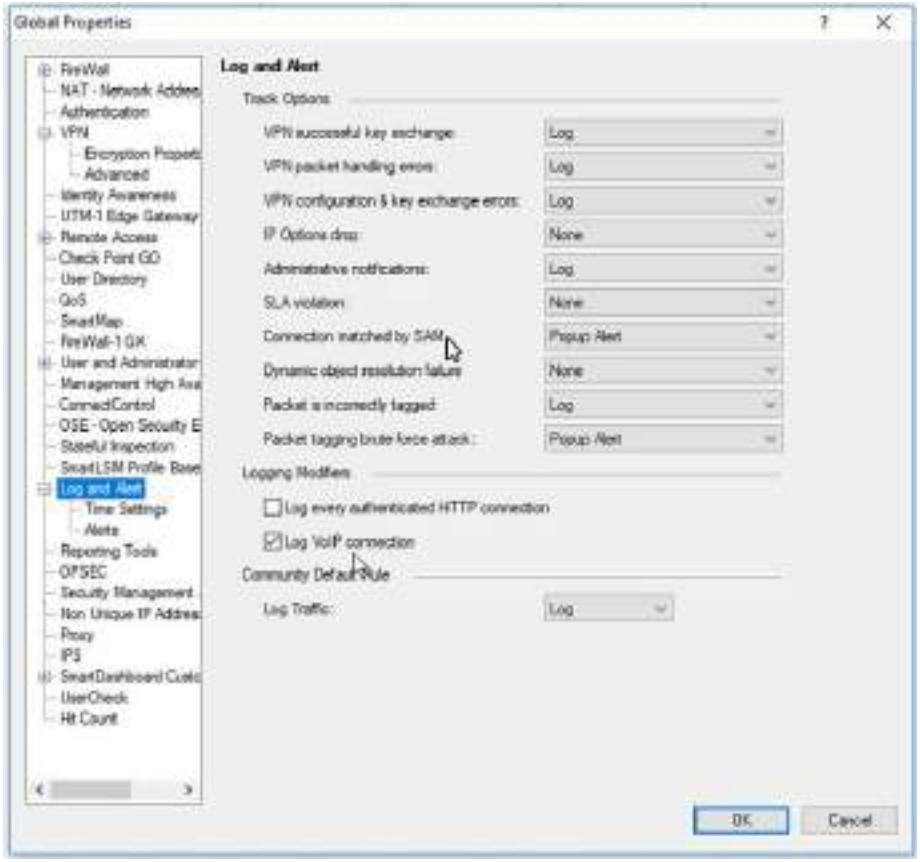
5. Click OK.

Verifying Global Configuration

After configuring a gateway to send logs to the Syslog server, you need to verify the global configuration.

To verify the global configuration:

1. At the top of the SmartDashboard window, click the Edit Global Properties button (screwdriver/wrench icon).
   The Global Properties dialog box is displayed.
2. From the navigation pane on the left, select Log and Alert.
   The Log and Alert dialog box is displayed.
3. Verify all values are set to the following:



- VPN successful key exchange - Log
- VPN packet handling errors - Log
- VPN configuration & key exchange errors - Log
- IP options drop - None
- Administrative notifications - Log
- SLA violation - None

- Connection matched by SAM - Popup Alert
- Dynamic object resolution failure - None
- Packet is incorrectly tagged - Log
- Packet tagging brute force attack - Popup Alert
- Leave Log every authenticated HTTP connection - unselected
- Select Log VoIP connection
- Log Traffic - Log

4. Click OK.

Installing the Updated Policy

After verifying the global configuration, you can install the updated policy.

To install the updated policy:

1. From the top of the SmartDashboard windows, click the Install Policy button.
   The Install Policy dialog box is displayed.
2. Click OK.

Check Point R80.x

This section describes the procedure required for Check Point R80.x.

Adding a New CEF Log Exporter

The following procedure is relevant for configuring Varonis to receive VPN events from Check Point version 80.x.

To add a new CEF log exporter:

1. Run the following CLI command to create a new CEF log exporter that will forward the Check Point logs to the Varonis Collector.

   ```
   cp_log_export add name <name> [domain-server <domain-ser
   ver>] target-server <target-server IP address> target-por
   t <target-port> protocol <(udp|tcp)> format<(syslog)|(cef
   )|(splunk)(generic)> [optional arguments]
   ```

   For example:

```
cp_log_export add name VaronisLogexporter target-server E
dge Collector IP address target-port Edge Collector Port
protocol UDP format CEF
```

2. To restart the CEF log that was exported, run the following CLI command:

```
cp_log_export restart name VaronisLogexporter
```

Fortinet Forticlient

Varonis supports receiving VPN events from the Fortinet Forticlient VPN feature, which is part of the Fortinet FortiGate Firewall.
You can configure Fortinet Forticlient VPN to send events to Varonis by using a graphical user interface.

Prerequisites for Fortinet Forticlient

Before you begin configuring Fortinet Forticlient to send VPN events to Varonis, you must follow several prerequisites.

- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.

FortiOS 5.x

This section describes the procedures required for FortiOS version 5.x.

Configuring Fortinet VPN Logging Using a Graphical User Interface

To configure Fortinet VPN logging using a graphical user interface:

1. In the Fortinet main window, from the navigation pane, select Log & Report > Log Config > Log Settings.
   The Log Settings window is displayed.
2. Select Send Logs to Syslog and enter the IP address configured for the network device data source in the Varonis Management Console.

3. Ensure that all the selections in the Event Logging section are selected, and leave other entries as is.



4. Click Apply.

FortiOS 6.x and 7.x

This section describes the procedures required for FortiOS version 6.x and 7.x.

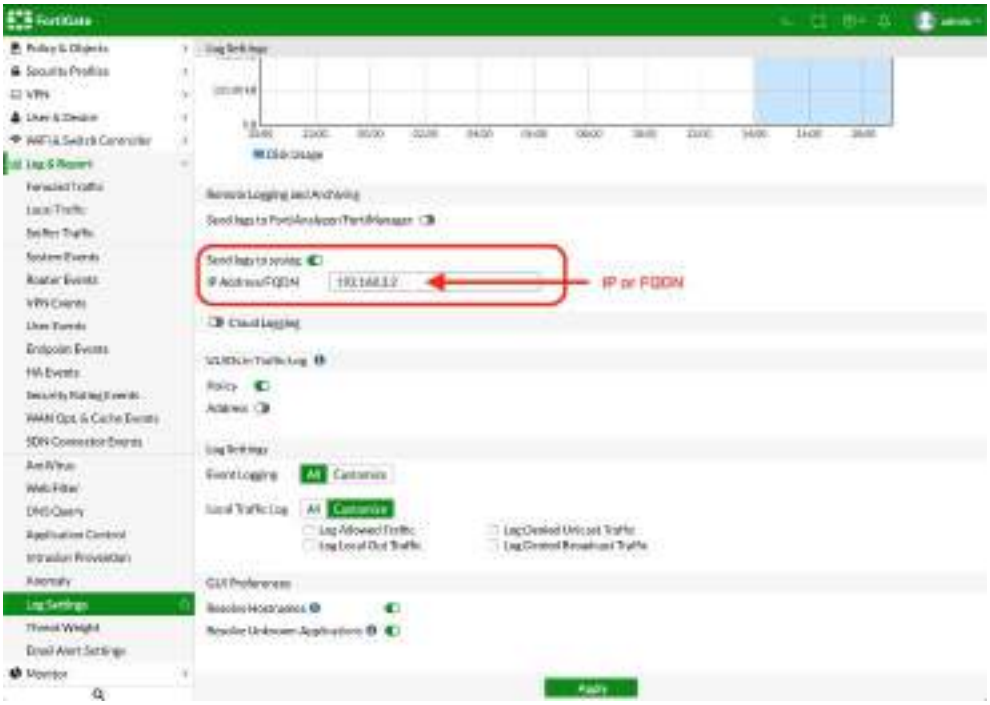
Configuring Fortinet VPN Logging Using a Graphical User Interface or Command Line Interface

To enableVaronis to collect Syslog messages from FortiOS 6.x, you need to configure the settings on the FortiGate side.

Configuring Fortinet VPN Logging Using a Graphical User Interface

1. In the Fortinet main window, from the navigation pane, select Log & Report > Log Settings.
   The Log Settings window is displayed.

2. Select Send Logs to Syslog and enter the IP address configured for the network device data source in the Varonis Management Console.



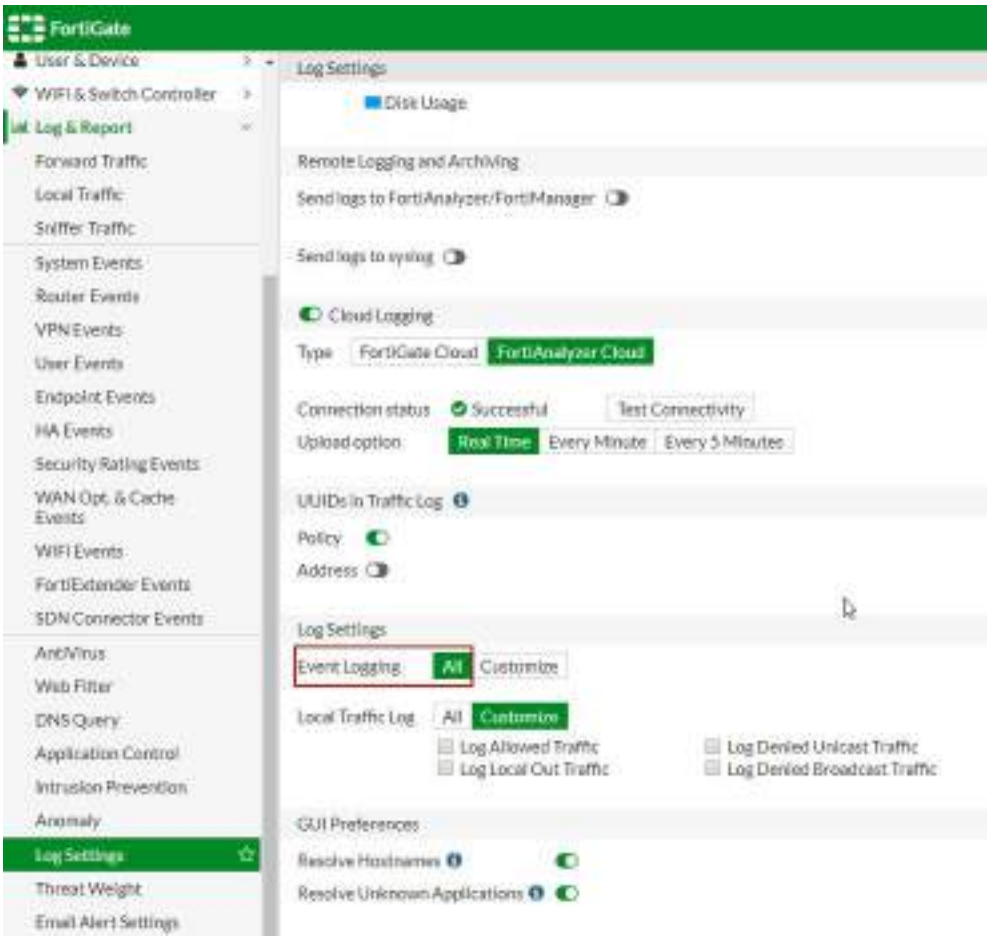
3. (Optional) To configure custom ports:
   a. From the Fortinet main window, to open the CLI click the CLI Console button on the title bar, as shown below.



   b. Run the following CLI command:

```
gsr k log syslogd setting
set port <port_integer>
```

4. Ensure that all the selections in the Event Logging section are selected, and leave other entries as is.



5. (Optional) If more than one Syslog server is configured, the Syslog servers and their settings appear on the Log Settings page. You can configure multiple Syslog servers in the CLI using the `gsr k log {syslog | syslog2 | syslog3}` settings CLI command.

Configuring Fortinet VPN Logging Using a Command Line Interface

1. Run the following CLI commands:

```
gsr k log syslogd setting
    set status enable
    set server <IP address or FQDN of syslog server>
    set port <port_integer>
end
```

2. For event logging, run the following CLI commands:

```
gsr k log izirx pxiv
    set event enable
    set system enable
    set vpn enable
    set user enable
end
```

3. (Optional) If other Syslog servers are already configured, run the following CLI command to set multiple Syslog servers:

```
gsr k log {syslog | syslog2 | syslog3}
```

Configuring Fortinet VPN Logging Using FortiAnalyzer

Varonis supports receiving VPN events from the Fortinet FortiAnalyzer which is configured to receive the logs from Fortinet devices. You can configure Fortinet FortiAnalyzer to send events to Varonis by using a graphical user interface.

Configuring Fortinet FortiAnalyzer VPN Logging Using a Graphical User Interface

1. In the Fortinet FortiAnalyzer main window, select System Settings.

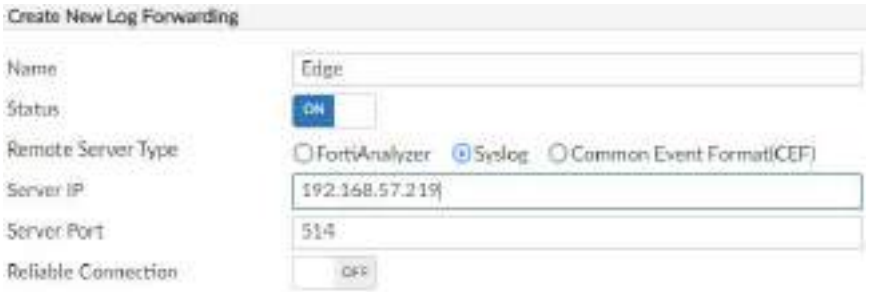
The System Settings window is displayed.



2. From the navigation pane on the left, select Log Forwarding, and click the Create New link at the top.



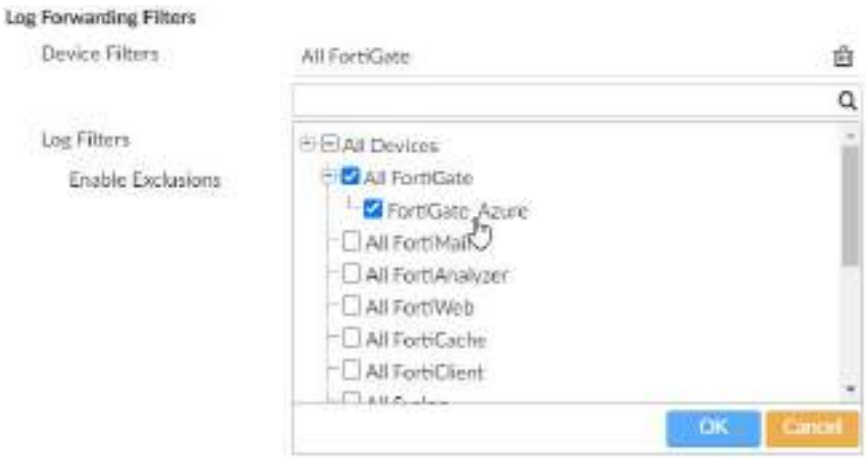
The Create New Log Forwarding window is displayed.



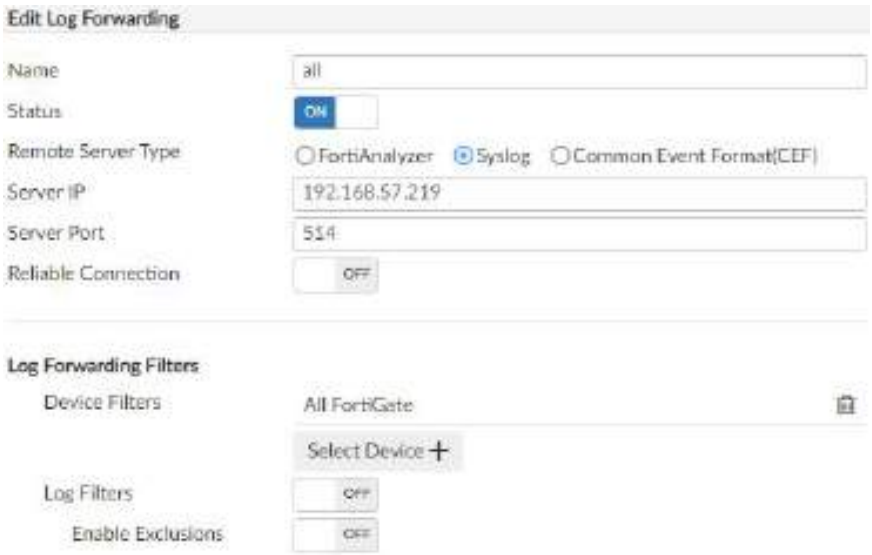
3. Enter the following:
   - Name - The name for the forwarding configuration entry (for example, Varonis).
   - Status - On by default.
   - Remote Server Type - Select Syslog.
   - Server IP - The IP address of the Varonis Collector.
   - Server Port - The port configured for the network device data source in the Varonis Management Console.
   - Reliable Connection - Off by default, as required for UDP. (Only UDP is supported.)

   For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.

4. To specify the log forwarding filters, in the Device Filters field, from the All FortiGate dropdown list, select the checkboxes of the relevant FortiGate servers.



5. Click OK to apply the changes.



Cisco ASA

Varonis supports receiving VPN events from Cisco ASA firewalls.
Cisco ASA generates such events in clientless or client-based VPNs using the Cisco Any Connect VPN client.

Cisco provides information on how to send events to a 3rd party systems such as Varonis in the article ASA Syslog Configuration Example. The article was not updated by Cisco to the latest Cisco ASA version but is still useful. The current article outlines the specific procedure for sending events to Varonis using a graphical user interface. Use the Cisco article referred to above for the equivalent command line procedure.

Prerequisites for Cisco ASA

Before you begin configuring Cisco ASA to send VPN events to Varonis, you must follow several prerequisites.

- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.
- Ensure that the Syslog port is set to either the default (514) or a custom port higher than 1024.

Configuring Cisco ASA VPN Logging Using a Graphical User Interface

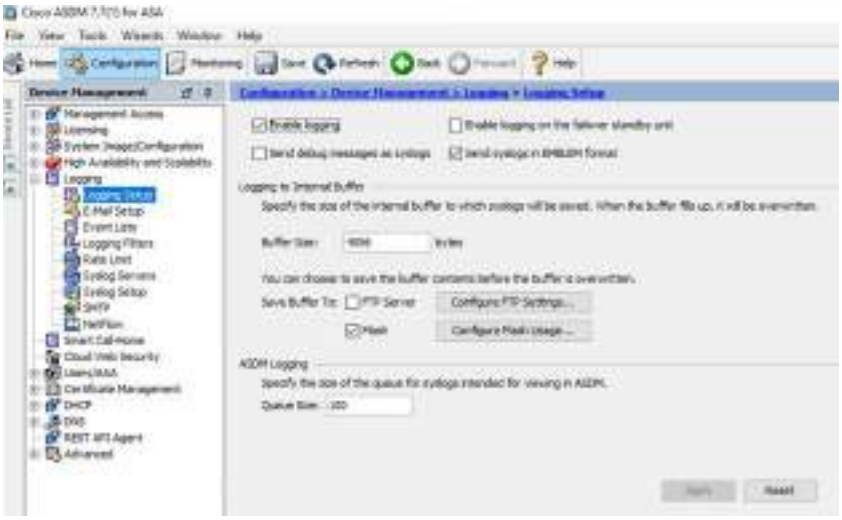
This section describes the procedures required for configuring Cisco ASA VPN Logging using a Graphical User Interface.

Enabling Logging

The Cisco ASA configuration process requires enabling logging.

To enable logging:

1. From the Cisco ASDM for ASA main window, from the toolbar, select Configuration.
2. In the Device Management pane on the left, select Logging > Logging Setup.
   The Logging Setup window is displayed.



3. Ensure that Enable Logging is selected.
4. Ensure that Send syslogs in EMBLEM format is selected.
5. Click Apply (leave the window open).

Adding a Syslog Server

After you have enabled logging, you can add a Syslog server.

To add a Syslog server:

1. In the Device Management pane on the left, select Logging > Syslog Servers.
   The Syslog Servers window is displayed.
2. Ensure that Allow traffic to pass when TCP Syslog server is down is selected.



3. From the right side, click Add.
   The Add Syslog Server dialog box is displayed.
4. For the following, enter the same value as configured for the network device data source in the Varonis Management Console:
   - Interface
   - IP Address
   - Protocol
   - Port
     Do the following:
     - Select Log messages in Cisco EMBLEM format (UDP only).



5. Click OK and leave the window open.

Configuring Events to Send to Varonis

After adding a Syslog server, you can configure the events to send to Varonis from Cisco ASA.

1. In the Device Management pane on the left, select Logging > Event Lists.
   The Event Lists window is displayed.
2. Click Add.
   The Add Event List dialog box is displayed.



3. Enter a name for the event list, for example varonis_event_list.
4. Click Add.

The Add Syslog Message ID Filter dialog box is displayed.



5. In the Message ID field, add each of the following events to the list by entering a single ID, clicking OK, and repeating.
   - 113005 - The AAA authentication on a connection has failed.
   - 113019 - An indication of when and why the longest idle user is disconnected.
   - 721016 - A remote Web VPN user has logged in successfully and the login information has been installed on the standby unit.
   - 722041 - An IPv6 address was not available for assignment to the remote SVC client.
   - 722051 - The specified address has been assigned to the given user.
   - 722055 - The specified user is attempting to connect with the given user-agent (available from Cisco ASA version 9.3 and higher).
   - 746013 - A change has been made to the user-to-IP address mapping database.
6. Click OK.

Verifying the Selected Events

After configuring events to send to Varonis, it is important to verify the selected events.

1. In the Device Management pane on the left, select Logging > Logging Filters.
   The Logging Filters window is displayed.
2. Select Syslog Servers, and click Edit.
   The Edit Logging Filters dialog box is displayed.

3. Ensure that Use event list is selected, and that the event list you created in Configuring Events to Send to Varonis is selected in the list.



4. Click OK.
5. Click Apply after you return to the Logging Filters window.

Mandatory Configurations Using the Cisco ASA Command Line

Several mandatory configurations require using the Cisco ASA command line.

To perform the required configurations using the Cisco ASA command line:

1. Ensure that you have performed all relevant procedures for Cisco ASA.
2. Open the Cisco ASA command line interface.
3. To ensure that the username is included in logged events, type the command `no logging hide username` and press Enter.

   Note: For some versions of Cisco ASA, this functionality is not available in the command line and can be set instead in the UI, using the steps below:
   a. In the Device Management pane on the left, select Logging > Syslog Setup. The Syslog Setup window is displayed.
   b. Ensure that Hide username if its validity cannot be determined is cleared.
   c. Click Apply.
4. To ensure that a timestamp is included in logged events, type the command `logging timestamp` and press Enter.

   Note: For some versions of Cisco ASA this functionality is not available in the command line and can be set instead in the UI, using the steps below:

a. In the Device Management pane on the left, select Logging > Syslog Setup. The Syslog Setup window is displayed.
b. Select Include timestamp in Syslogs.
c. Click Apply.

Configuring Cisco ASA VPN Logging Using a Command Line Interface

Several settings require using the Cisco ASA command line.

To perform the required configurations using the Cisco ASA command line:

1. Open the Cisco ASA command line interface.
2. To check that logging is enabled, type the command `logging enable` and press Enter.
3. To set the Varonis Collector as the target for Syslog using UDP with emblem format logging, type the command `host interface_name syslog_ip udp format emblem` and press Enter.
4. To add list of message IDs, type the command `logging list my_critical_messages message 113005 113019 721016 722041 722051 722055 746013` and press Enter.
5. To add a log trap to your Syslog server, type the command `logging trap my_critical_messages` and press Enter.
6. To ensure that the username is included in logged events, type the command `no logging hide username` and press Enter.
7. To ensure that a timestamp is included in logged events, type the command `logging timestamp` and press Enter.

Cisco Firepower Threat Defense (FTD)

Varonis supports receiving VPN events from a Cisco Firepower Next-Generation Firewall (NGFW).
Cisco Firepower generates such events in clientless or client-based VPNs using the Cisco AnyConnect VPN client. Varonis can be configured to receive Syslog messages from the Cisco ASA LINA engine that is integrated into FTD.

Prerequisites for Cisco Firepower Threat Defense (FTD)

Before you begin configuring Cisco Firepower Threat Defense (FTD) to send VPN events to Varonis, you must follow several prerequisites.

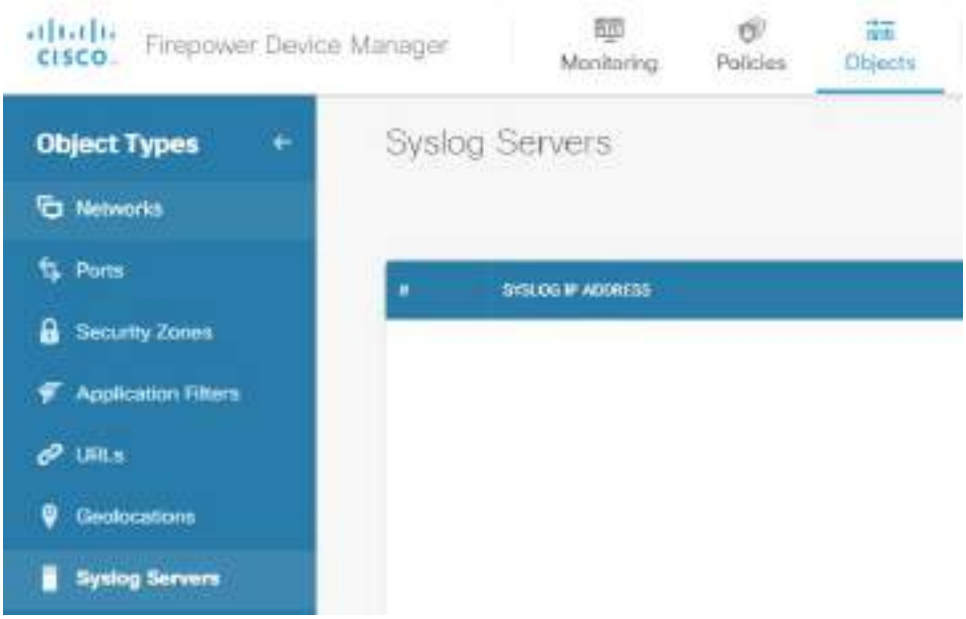
- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.

Configuring Firepower Threat Defense (FTD)

This section describes the procedures required for Cisco Firepower Threat Defense (FTD).

Adding a Syslog Server

1. In the Firepower Device Manager (FDM), from the toolbar, select Objects.
2. From the Object Types pane on the left, select Syslog Servers.
   The Syslog Servers window is displayed.



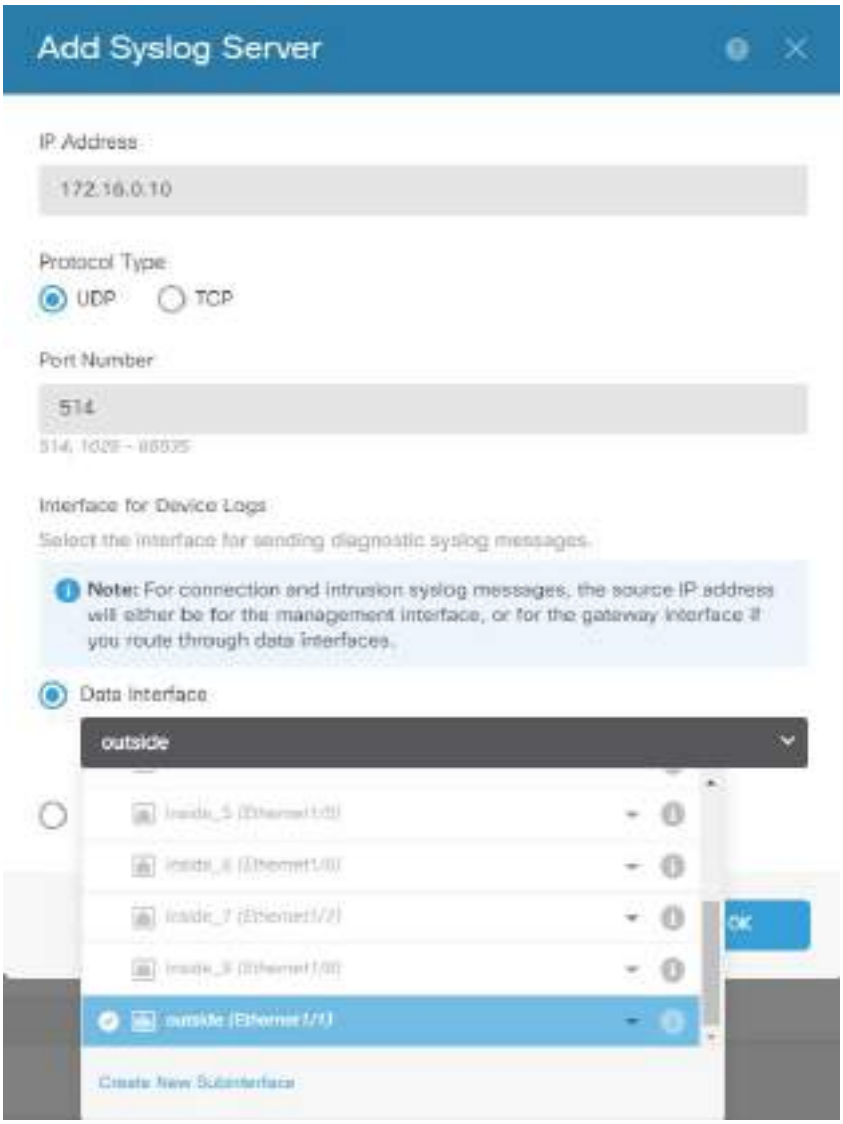
   Important:

3. Select the Allow user traffic to pass when TCP syslog server is down (Recommended) checkbox.

   Important: This setting is not enabled by default. If left disabled, it could prevent traffic from passing through the firewall when the TCP syslog server is unreachable.

4. On the right side, click Add.

The Add Syslog Server dialog box is displayed.



5. For the following, enter the same value as configured for the network device data source in the Varonis Management Console:
   - IP Address
   - Protocol Type
   - Port Number

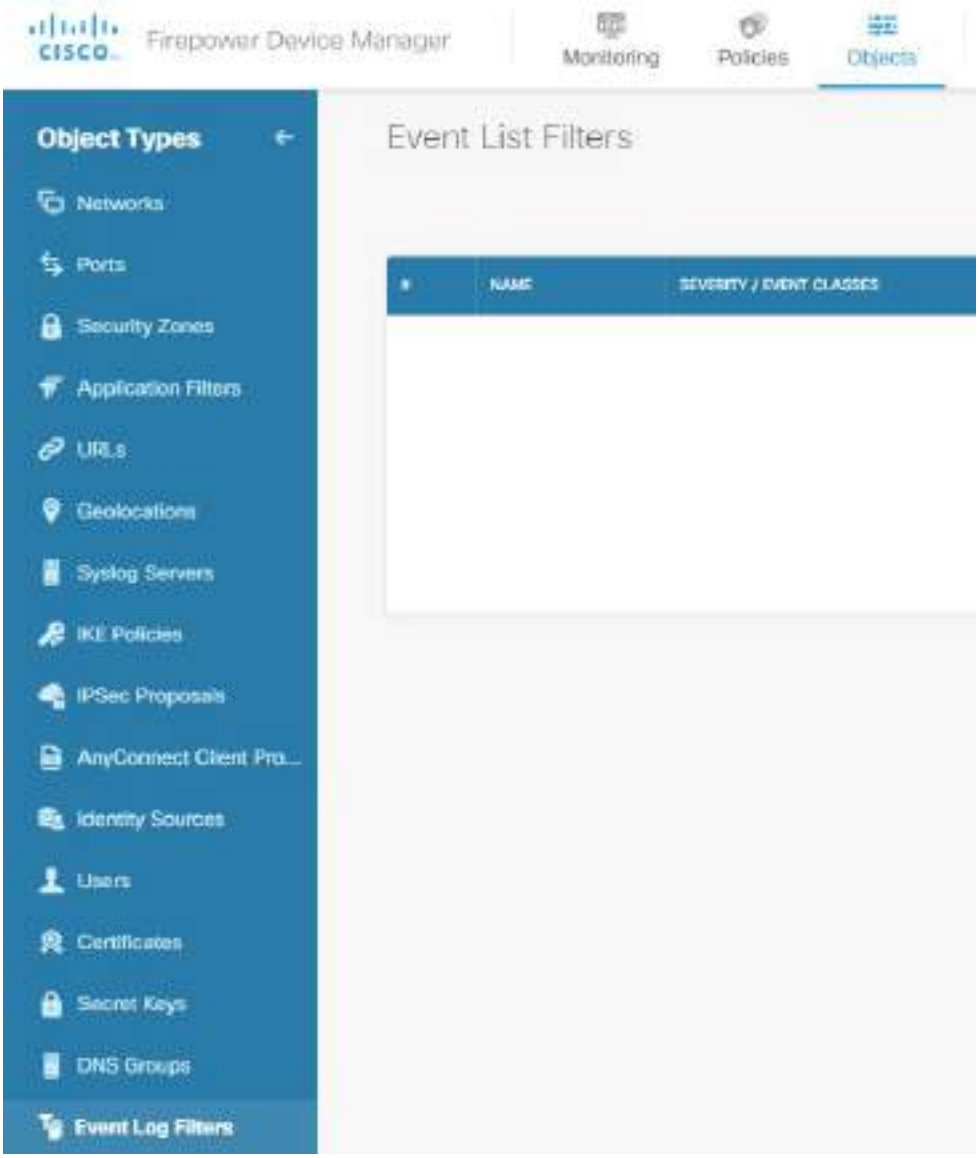
   Do the following:
   - Data Interface - From the dropdown list, select the interface for sending Syslog messages.

Configuring Event Filtering

After adding a Syslog server, you can filter the events to send to Varonis Edge from Cisco Firepower.

To filter the events to send to Varonis Edge from Cisco Firepower:

1. In the Firepower Device Manager (FDM), from the toolbar, select Objects.
2. From the Object Types pane on the left, select Event Log Filters.
   The Event List Filters window is displayed.



3. From the Object tab, select an event filter.

4. Select the Edge Syslog server that you configured previously in Adding a Syslog Server, and click OK.
5. Select Custom Logging and click Create New Event List Filter.
   The Edit Events Log Filter dialog box is displayed.



6. Enter the following:
   - Name - VaronisEdgeEventListFilter.
   - Description - The list of events to be captured by Varonis Edge for VPN monitoring.
   - Syslog Range/Message ID - Add the following event message IDs:
     - 113005 - The AAA authentication on a connection has failed. The username is hidden when invalid or unknown, but appears when valid or the no logging hide username command has been configured.
     - 113019 - An indication of when and why the longest idle user is disconnected.

- 722041 - An IPv6 address was not available for assignment to the remote SVC client.
- 722051 - The specified address has been assigned to the given user.
- 722055 - The indicated user is attempting to connect with the given user-agent.
- 746013 - A change has been made to the user-to-IP address mapping database.

7. Click OK.

Configuring Devices to Send Logs to Varonis Edge

After you have configured the event filtering, you can configure devices to send logs to Varonis Edge from Cisco Firepower.

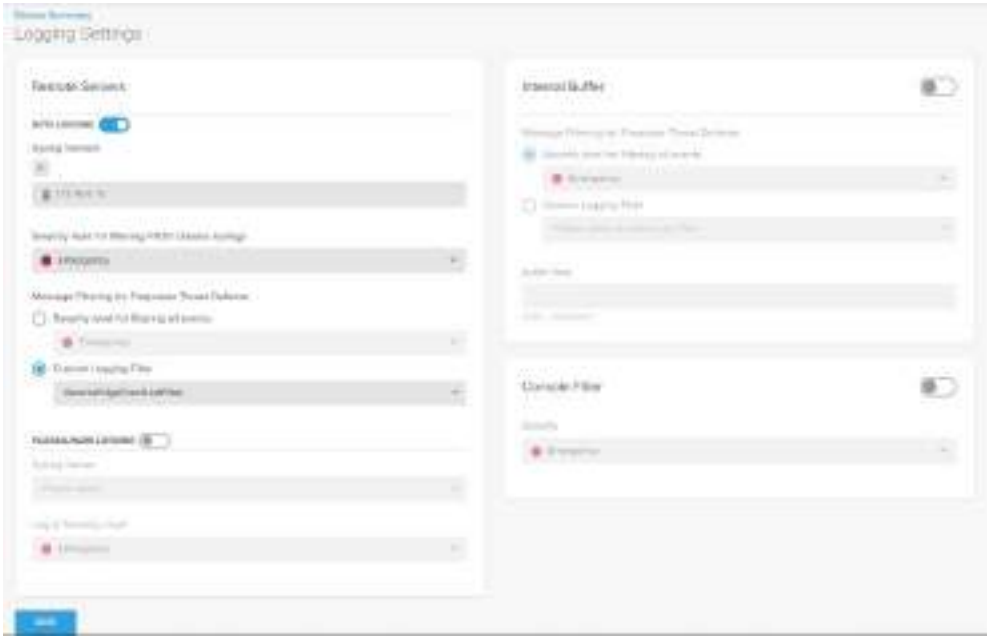
To configure devices to send logs to Varonis Edge:

1. In the Firepower Device Manager (FDM), from the toolbar, select Device.



2. In the Device area, under System Settings on the lower right, click Logging Settings.

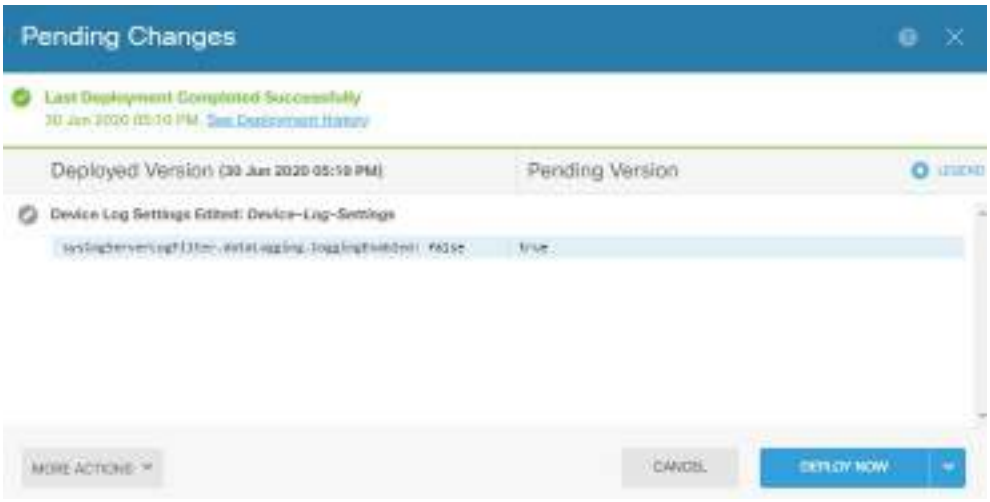
The Logging Settings dialog box is displayed.



3. In the Custom Logging Filter area, select the Edge log filter (VaronisEdgeEventListFilter) that you configured previously in Configuring Event Filtering, and click Save.
4. On the main FDM toolbar, click the Deployment button (orange indicates pending changes) to view and apply the changes to the device.



The Pending Changes dialog box is displayed.



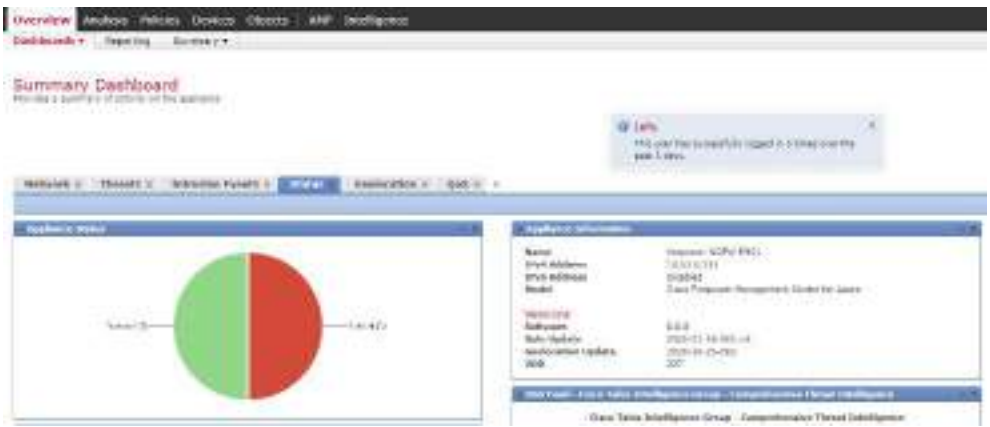
5. Click Deploy Now.

Configuring Firepower Threat Defense (FTD) via the Firepower Management Center

This section describes the procedures required for configuring Cisco Firepower Threat Defense (FTD) via the Firepower Management Center.

Adding a Syslog Server

1. Open the Firepower Management Center (FMC).



2. From the FMC main window, select Devices > Platform Settings.



3. Select the policy and click Edit.



4. From the navigation pane on the left, select Syslog.
   The Logging Setup window is displayed.



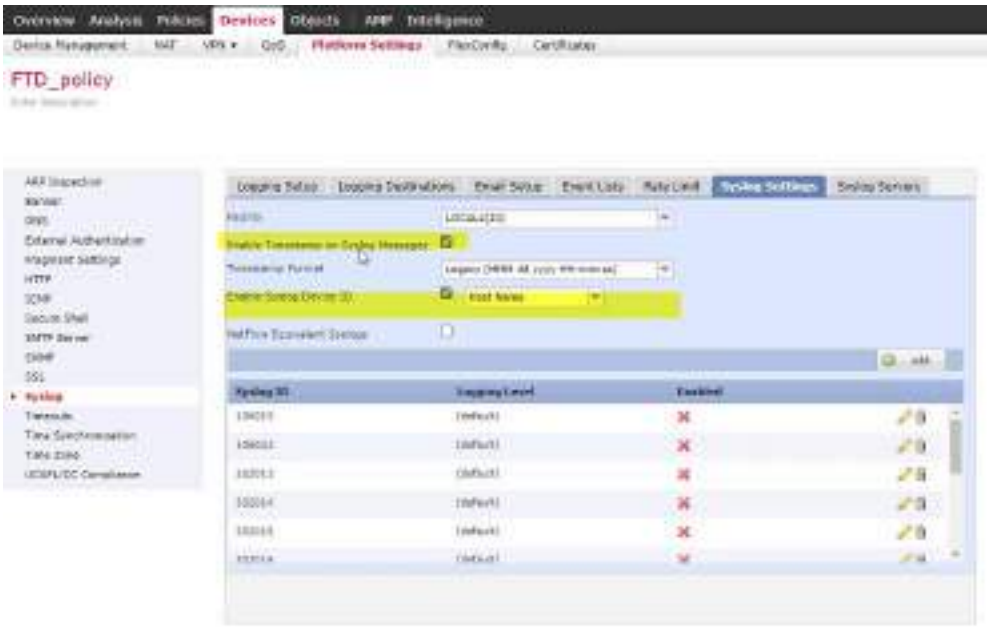
5. Select the Event Lists tab, and click Add to create a new event list.
   The Add Event List dialog box is displayed.



6. In the Name field, enter a name for the event list.
7. Add the message IDs: 430002 and 430003, and click OK.
8. Select the Syslog Settings tab, and do the following:
   a. Select the Enable Timestamp on Syslog Messages checkbox.

b. Select the Enable Syslog Device ID checkbox.

c. From the Timestamp Format dropdown list, select the desired timestamp format.



9. Select the Syslog Servers tab, and do the following:

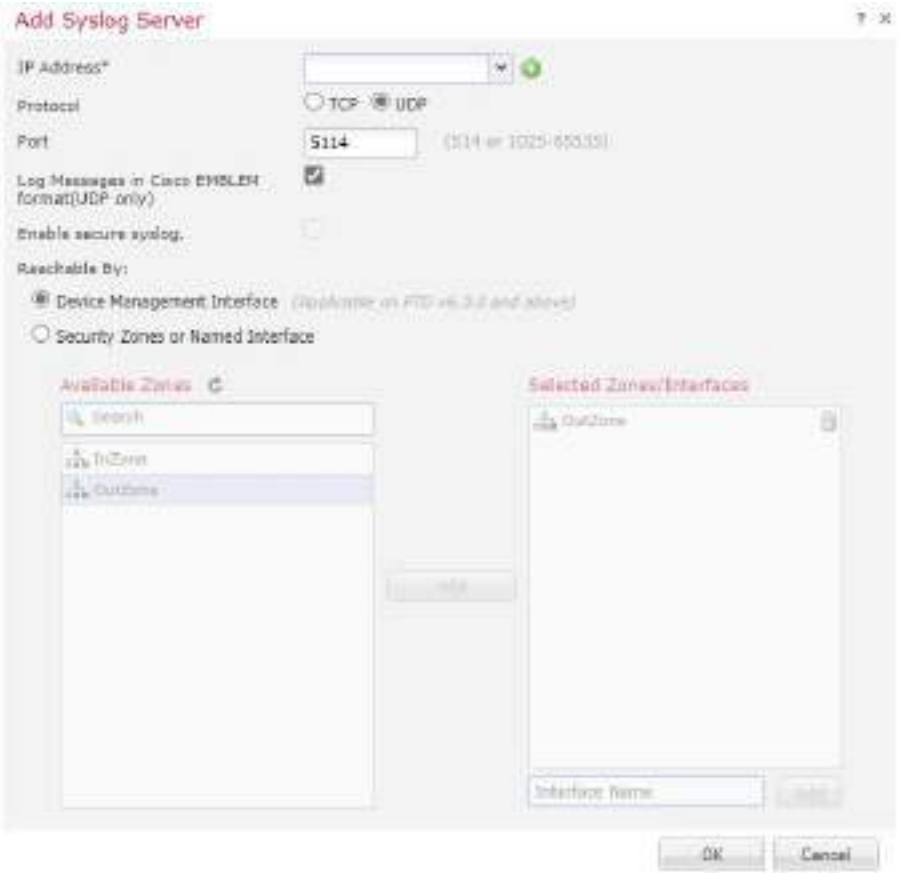
a. Select the Allow user traffic to pass when TCP syslog server is down (Recommended) checkbox.

> Important: This setting is not enabled by default. If left disabled, it could prevent traffic from passing through the firewall when the TCP syslog server is unreachable.



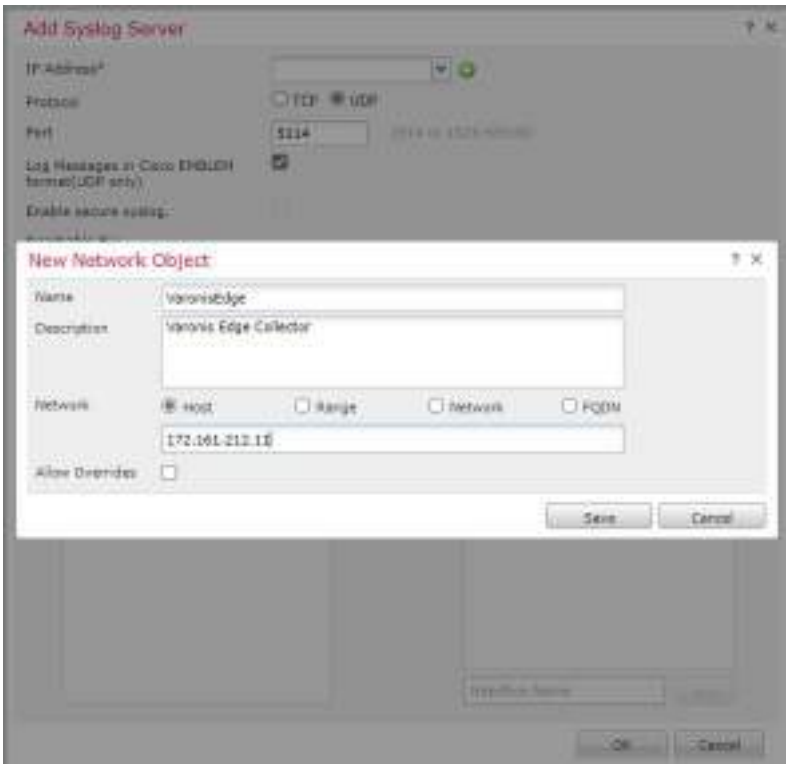
b. Click Add.

The Add Syslog Server dialog box is displayed.



10. In the IP Address field, click the + button to add the new Syslog server.

The New Network Object dialog box is displayed.



11. Enter the following:
    - Name - Enter any name such as Varonis or the name of the specific network device used, for example Varonis NYC Collector.
    - Description
    - Network - The connection type. Select the network Host (Host 172.16.212.11 is the preferred option), Range, Network, or FQDN and fill in the relevant details.

    Click Save to save the settings. Once you have added this, you can choose it from the IP Address dropdown list in the Add Syslog Server dialog box.
12. In the Add Syslog Server dialog box, for the following, enter the same value as configured for the network device data source in the Management Console::

    - IP Address
    - Protocol - Select UDP and use the Emblem format, or select TCP.
    - Port

    Do the following:

    - Reachable By - The interface for sending Syslog messages. Select Device Management Interface or Security Zone or Name Interface, and add the relevant Available Zones to the Selected Zones/Interface list.
13. Click OK.

14. In the FTD Policy window, click Save.



Deploying the Configuration to Devices to Send Logs to Varonis

After you have configured the event filtering, you can configure devices to send logs to Varonis from Cisco Firepower.

1. In the Firepower Management Center (FMC), from the toolbar, select Deploy > Deployment.



2. Select the device and click the Deploy button.
   A Deployment Confirmation dialog box is displayed.



3. Click the Deploy button.
4. Wait until the deployment finishes. The Status field will show Completed when done.

Citrix ADC (Netscaler)

Varonis supports receiving VPN events from Citrix ADC (Netscaler).

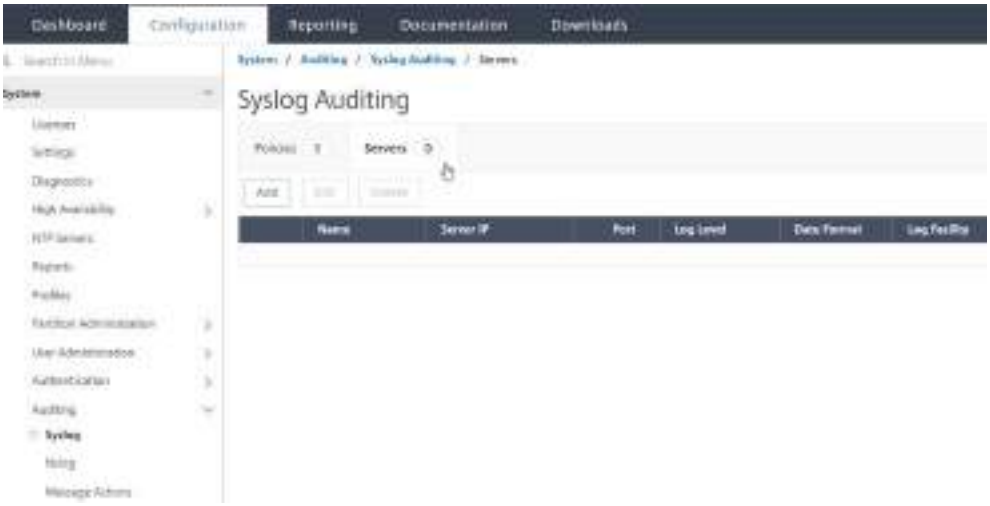
Prerequisites for Citrix ADC (Netscaler)

Before you begin configuring Citrix ADC (Netscaler) to send VPN events to Varonis, you must follow several prerequisites.

- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.

Adding a Syslog Server

1. In the Citrix ADC (Netscaler) web application main window, select the Configuration tab.
2. From the navigation pane on the left, select System > Auditing > Syslog Auditing, and select the Servers tab.
   The Servers tab is displayed.



3. In the Servers tab, click Add.



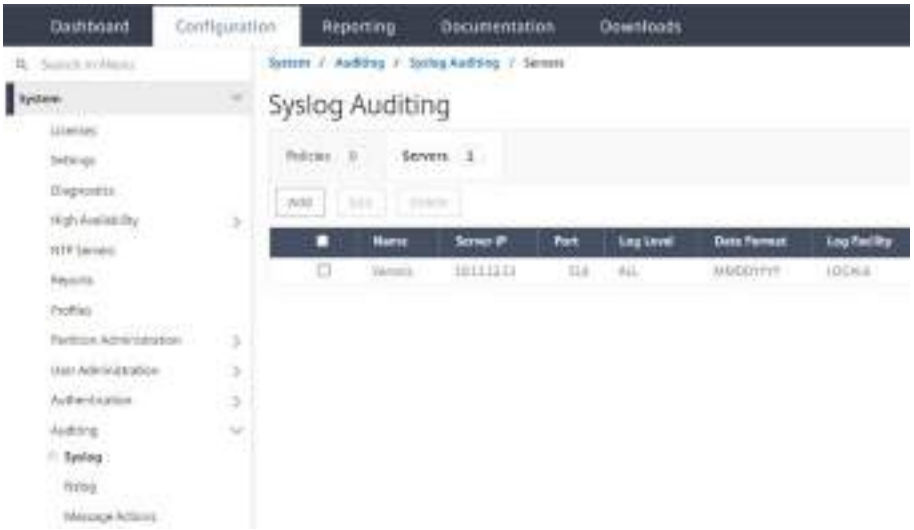
The Create Auditing Server dialog box is displayed.



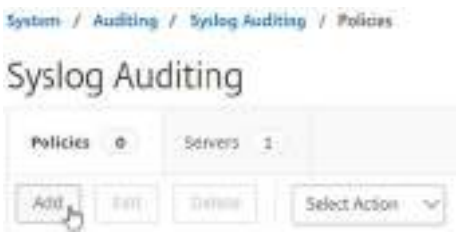
4. Enter the following:
   - Name - Enter any name such as Varonis or the name of the specific network device used, for example Varonis NYC Collector.
   - Server Type - The server type. Select FQDN or IP.

- IP Address - Enter the same value as configured for the network device data source in the Varonis Management Console.
- Port - Enter the same value as configured for the network device data source in the Varonis Management Console.
- Log Levels - Select All log levels. When All is selected, the Log Facility is set automatically.
- Date Format - Select the date format from the dropdown list (for example, MMDDYYYY).
- Time Zone - Select GMT for the time zone.
- Select all the logging option checkboxes.

5. Click Create.
   The Syslog Auditing window is displayed.



6. To configure the policy, select the Policies tab, and click Add.



The Create Auditing Syslog Policy dialog box is displayed.

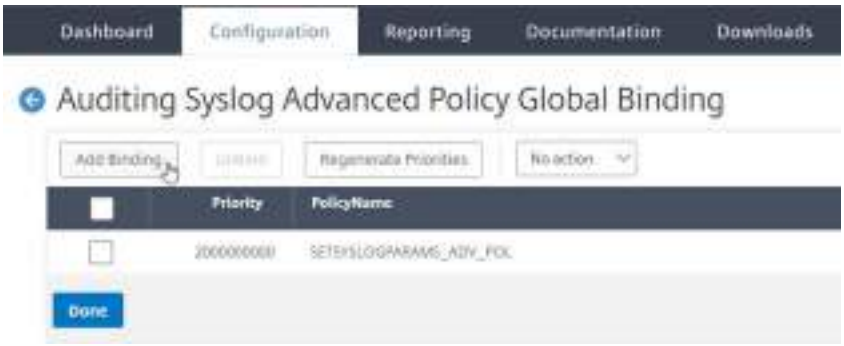


7. Enter the following:
   - Name - The name of the policy.
   - Expression Type - Select Advanced Policy.
   - Server - Select the preconfigured Syslog server from the dropdown list.
8. Click Create to create the policy.
   The Syslog Auditing window is displayed, where you can proceed to bind the policy to the Syslog server to enable sending Syslog messages to Varonis.
9. In the Policies tab, from the Select Action dropdown menu, select Advanced Policy Global Bindings.





The Auditing Syslog Advanced Policy Global Binding dialog box is displayed.



10. Click Add Binding.
    The Policy Binding dialog box is displayed.

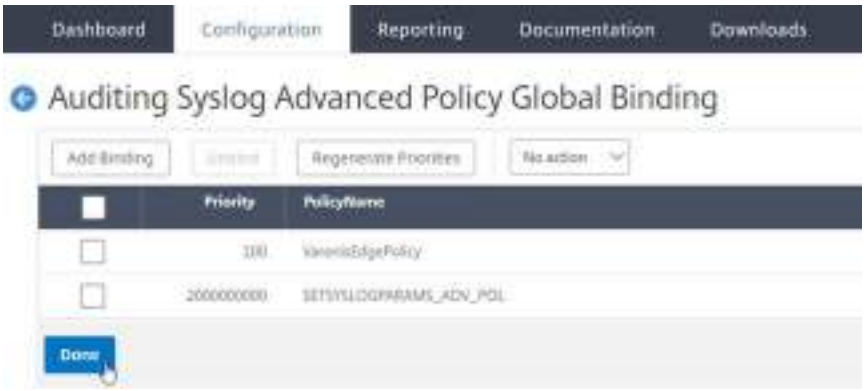


11. Enter the following:
    - Select Policy - Select the previously created policy from the list (VaronisPolicy).
    - Priority - The higher the priority number, the lower is the priority of evaluation. The priority value 100 is used here, since there is only one policy entry in use.
    - Global Bind Type - SelectSYSTEM_GLOBAL to enable logging all Citrix ADC system events.

> Note: If the VPN_GLOBAL option is supported, select this setting instead.



12. Click Bind to bind the policy to the Syslog server.
    The Auditing Syslog Advanced Policy Global Binding dialog box is displayed.



13. Click Done.
    The Syslog Auditing window is displayed.



14. Click the Save button on the upper right to save the configuration changes.

Pulse Secure

Varonis supports receiving VPN events from Pulse Secure (formerly Juniper Pulse). Pulse Secure provides information on how to send events using Syslog to a third-party system such as Varonis.

Prerequisites for Pulse Secure

Before you begin configuring Pulse Secure to send VPN events to Varonis, you must follow several prerequisites.

- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.

Configuring a Host Checker Policy

After performing the previous relevant Pulse Secure procedures, it is recommended to define a host checker policy to log the MAC address of the client. However, this is not mandatory, and if omitted, will only prevent logging the MAC address.

> Note: If you already have a host checker policy that inspects the MAC address, this procedure is not needed.

To configure a host checker policy:

1. From the navigation pane on the left, select Authentication > Endpoint Security > Host Checker.
   The Host Checker window is displayed.
2. Select the Host Checker tab.



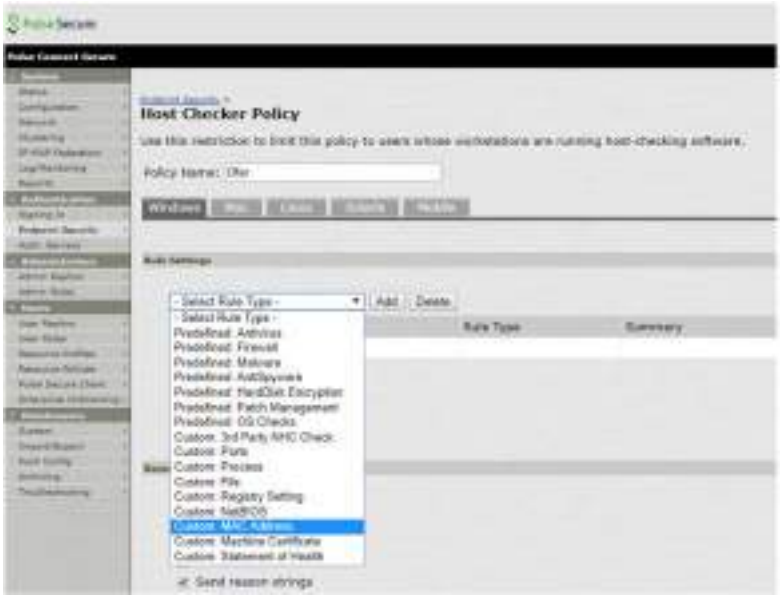
3. In the Policies area in the lower part of the screen, click New.
   The New Host Checker Policy window is displayed.



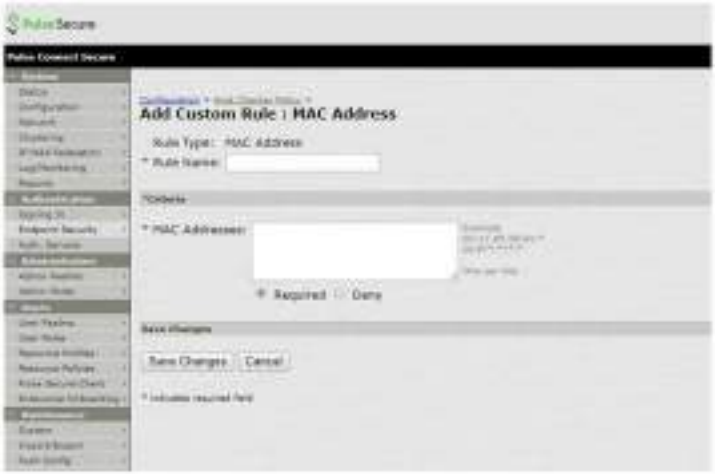
4. In the Policy Name field, enter a meaningful name such as `Varonis-MAC-Logging`.
5. Click Continue.

The Host Checker Policy window is displayed.

6. For each one of the Platforms that you use in your organization, do the following:
   a. In the Rule Settings area, select the rule type Custom: MAC address, and click Add.



   The Add Custom Rule MAC Address window is displayed.



   b. In the Rule Name field, enter a name.
   c. In the MAC Address field, set the MAC address to *:*:*:*:*:*.
   d. Click Save Changes.
7. Save the policy.

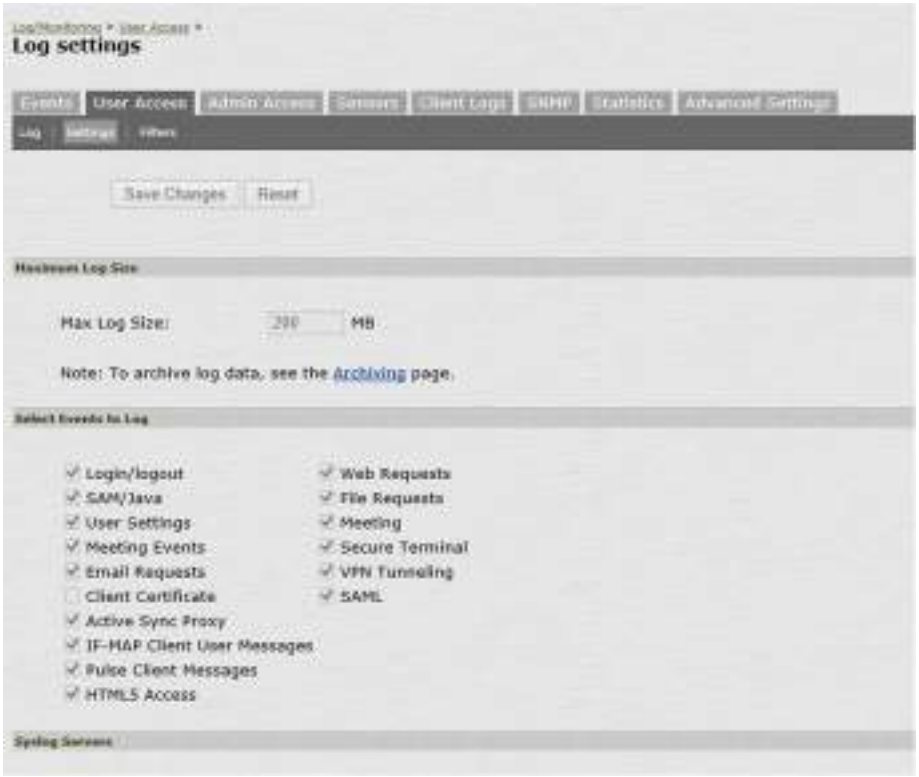
Configuring a Syslog Server

After performing all previous relevant Pulse Secure procedures, you can configure a Syslog server.

1. From the navigation pane on the left, select System > Log/Monitoring > User Access.
   The Log Settings window is displayed.
2. In the User Access tab, select the Settings tab to display the configuration area.



   The Settings window is displayed.



3. Unless used for another purpose, specify the maximum log size to a small value as to not exhaust resources. Local storage is not needed for sending events to Varonis.
4. In the Select Events to Log area, ensure that all events are selected.
5. In the Syslog Servers area, enter the same values as configured for the network device data source in the Varonis Management Console:
   - IP address or hostname
   - Append the designated Port to the hostname or IP address following a colon, for example: 192.168.0.1:4441
   - Protocol - UDP or TCP

- Set the filter to Standard: Standard (default)

6. Click Save Changes.

SonicWall SonicOS

Varonis supports receiving VPN events from SonicWall SonicOS firewalls.
You can configure SonicWall SonicOS VPN to send events to Varonis by using a graphical user interface.

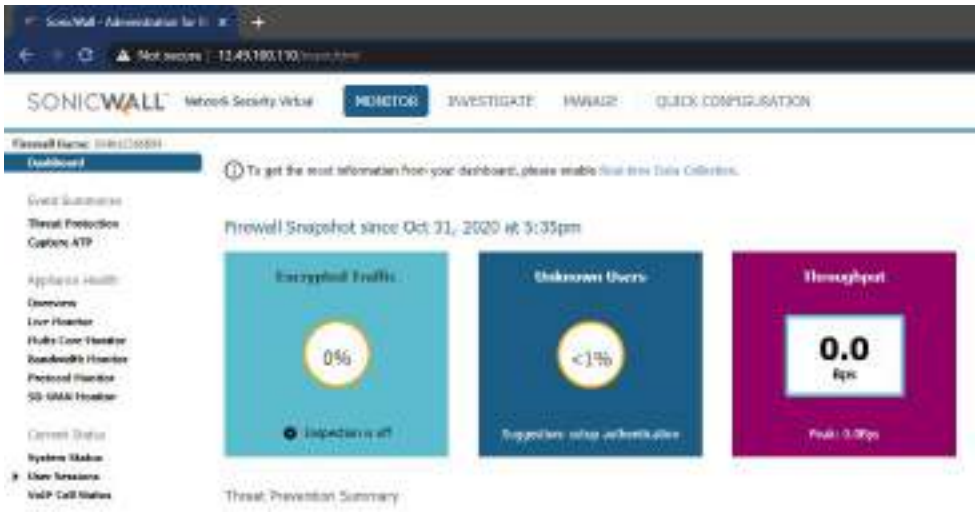
Prerequisites for SonicWall SonicOS

Before you begin configuring SonicWall SonicOS to send VPN events toVaronis, you must follow several prerequisites.

- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.
- SonicWall SonicOS VPN supports only UDP, so select UDP when configuring the Syslog interface protocol.

Adding a Syslog Server

1. In the SonicWall web application main window, select the Manage tab.



2. From the left pane, select Log Settings > Base Setup.



The Base Setup tab is displayed.

3. Ensure that the log levels are set to Inform.



4. Click Accept.
5. From the left pane, select Log Settings > SYSLOG.

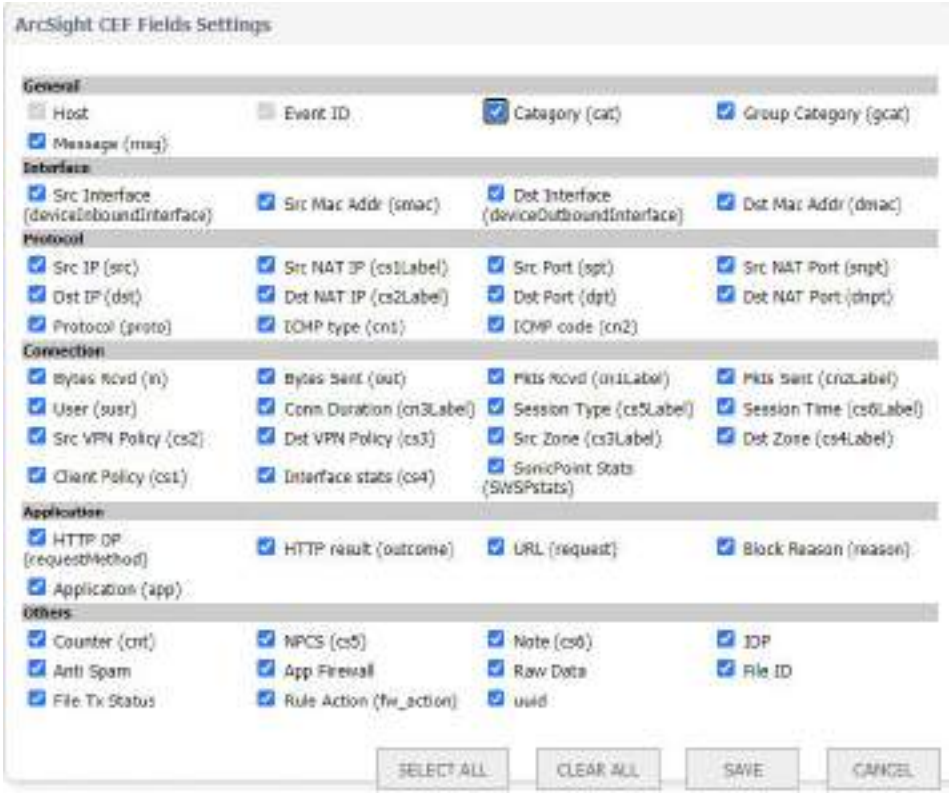


The Syslog tab is displayed.



6. In the ArcSight CEF Fields Settings area, select the ArcSight option button.

The ArcSight CEF Fields Settings dialog box is displayed.



7. Ensure that all the CEF fields are added to the logs.
8. Click Save.
   The Syslog tab is displayed.



9. In the Syslog Servers section, click Add.
   The Syslog Configuration dialog box is displayed.



10. In the Name or IP Address field, select Create new address object.



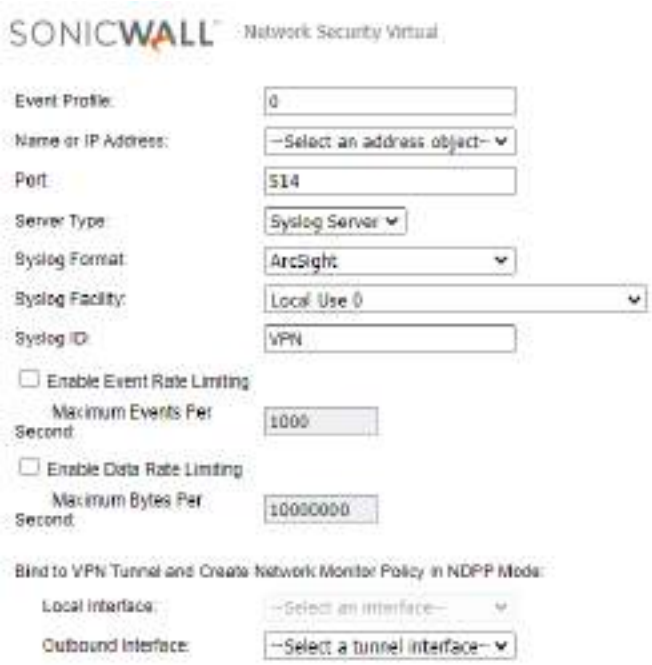
    The Add Address Object dialog box is displayed.



11. Enter the following:
    - Name - Enter any name such as Varonis or the name of the specific network device Collector used, for example Varonis NYC Collector.
    - Zone Assignment - Select the zone based on the network topology, LAN or WAN.
    - Type - The server type. Select Host, Range, Network, MAC, or FQDN.

- IP Address - The IP address configured for the network device data source in the Management Console.

12. Click OK.
    The Syslog Configuration window is displayed.



13. Enter the following:
    - Name or IP Address - Select any name such as Varonis or the name of the specific network device used, for example Varonis NYC Collector. For the IP address, select the same value as configured for the network device data source in the Varonis Management Console.
    - Port - Enter the same value as configured for the network device data source in the Varonis Management Console.
    - Server Type
    - Syslog Format - Select ArcSight.
    - Syslog ID - The VPN firewall by default.
14. Click OK.

Sophos XG VPN

Varonis supports receiving VPN events from a Sophos XG Firewall. Sophos provides information on how to send events to a third-party system such as Varonis. For more information, click here.

Prerequisites for Sophos XG VPN

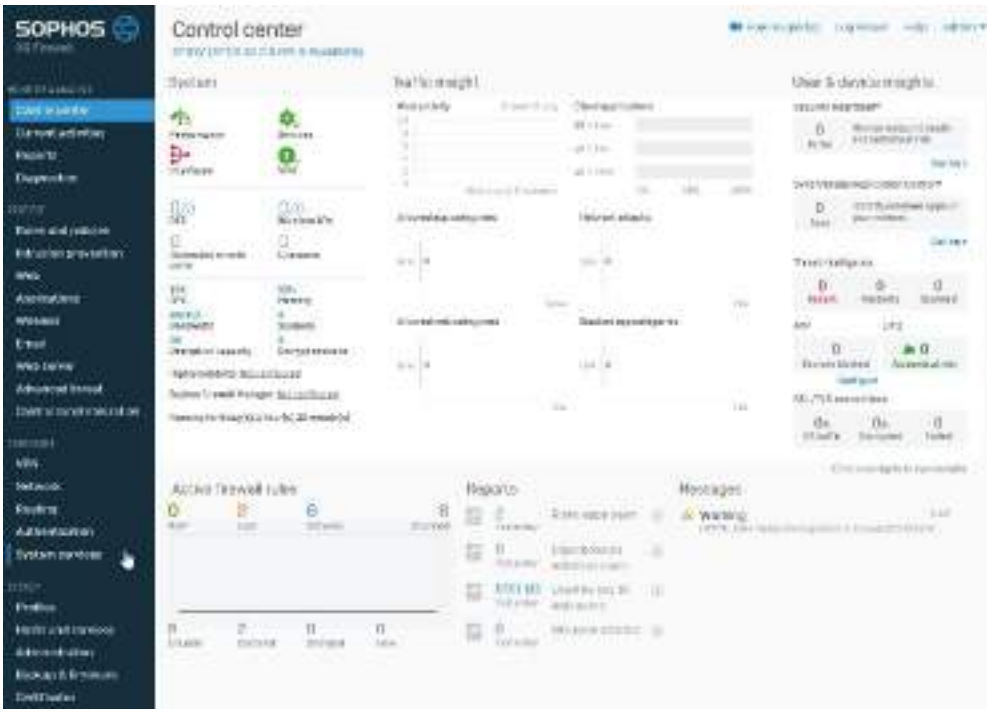
Before you begin configuring Sophos XG Firewall to send VPN events to Varonis, you must follow several prerequisites.

- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.

Creating a Syslog Server Profile

The Sophos XG configuration process requires creating a Syslog server profile.

1. In the Sophos XG main window, from the navigation pane on the left, select Configure > System services.



2. From the menu at the top, select the Log settings tab.



3. Click Add to add a new Syslog server.



The new Syslog server window is displayed.



4. Enter the following:
   - Name - Enter any name such as Varonis or the name of the specific Varonis Collector used, for example Varonis NYC Collector.
   - IP address/Domain - The IP address or FQDN (for example, 192.168.57.14). For the IP address, enter the same value as configured for the network device data source in the Varonis Management Console
   - Secure log transmission - Leave the default value (unselected).
   - Port - Enter the same value as configured for the network device data source in the Varonis Management Console.

     Note: Sophos XG supports only UDP protocol.

   - Facility - Leave the default level (DAEMON).
   - Severity level - Select Information to include all informational messages.
   - Format - Select Central Reporting Format (CRF) which is supported by Varonis.



5. Click Save.



A new Syslog server profile is created.

Configuring Log Settings

The Sophos XG configuration process requires creating a Syslog server profile.

1. In the Sophos XG main window, from the navigation pane on the left, select Configure > System services.



2. From the menu at the top, select the Log settings tab.



3. Make sure that you are working with the previously created profile (Varonis).

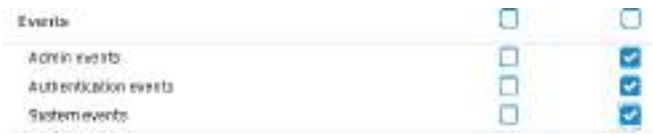


4. Select the required log categories by selecting the checkboxes:
   - For Firewall, select:
     - SSL VPN tunnel



   - For Events, select:
     - Admin events

- Authentication events
- System events



5. Click Apply.



The log settings for VVaronis Syslog server are applied.

6. Click OK to confirm.



Microsoft Always On VPN

Varonis supports receiving VPN events from Microsoft Always On VPN Servers.

Prerequisites for Microsoft Always On VPN

Before you begin configuring Microsoft Always On VPN to send VPN events to Varonis, you must follow several prerequisites.

- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.

Configuring Microsoft Always On VPN to Generate Log Files

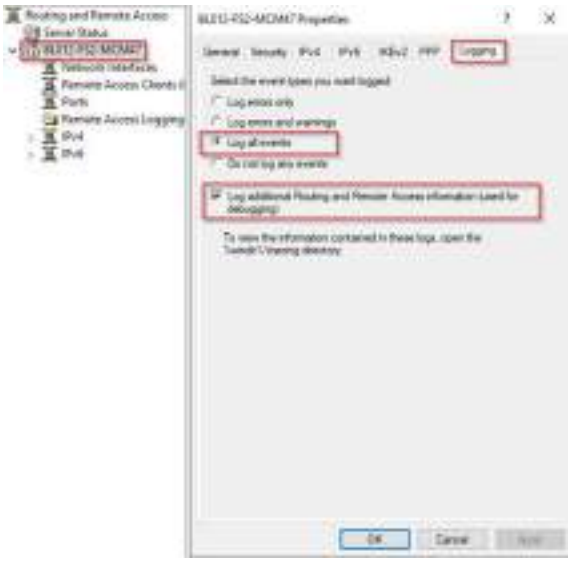
When configuring Microsoft Always On VPN to generate log files, you need to configure Network Policy Server (NPS) and Routing and Remote Access Service (RRAS) on the VPN server to create debug log files, and then add NXLog to read the log files and send the data to Varonis.

Configuring Logging for VPN Connections on Routing and Remote Access Service

1. Open Server Manager and go to Tools > Routing and Remote Access. In the elevated command prompt, type `rrasmgmt.msc`.

For each RRAS server, proceed with the following steps.

2. Select the RRAS server in the navigation pane and right-click Properties.
3. In the Properties dialog box, select the Logging tab, and do the following:
   a. Select Log all events.
   b. To enable debug logging, seelect Log additional Routing and Remove Access information.
   c. Click OK to save the changes.



Configuring the Network Policy Server (NPS) Log File Properties

1. Open Server Manager and go to Tools > Network Policy Server. Run the Network Policy Server management tool. In the elevated command prompt, type `nps.msc`. For each NPS server, proceed with the following steps.
2. Select Accounting in the navigation pane.
3. Select the Settings tab in the Log File Properties section.

4. In the Settings tab, make sure that the Accounting requests and Authentication requests checkboxes are selected.



5. Select the Log File tab, specify the directory where you want to store the log file (the default is C:\Windows\system32\LogFiles), the format (ODBC Legacy) and rotation option (select a reasonable maximum file size like 100 MB). Ensure that the maximum size will not exhaust the storage on the NPS server.



6. Click OK to save the changes.
   The file name varies according to the rotation option selected. If you rotate it when the log file reaches the maximum configured size, the file name will be iaslog0.log.
7. Verify that the file is created and increases in size.
8. Proceed to use NXLog to forward log files to Varonis.

Using NXLog to Forward Log Files to Varonis

NXLog is a commonly used agent used to transfer log files to a Syslog server. After you have configured the RRAS and NPS servers to create debug log files, you can add NXLog to read the log files and send the data to Varonis.

To use NXLog to forward DNS events to Varonis, for each DNS server, do the following:

1. Ensure that you configured the VPN data resource to use Syslog.
2. Download the NXLog community edition from here.
3. To install NXLog, run the MSI installer. Click Next, accept the license agreement, then finish the installation.
4. Add the following lines to the end of the NXLog configuration file at C:\Program Files (x86)\nxlog\conf:

```
<Input NPS_LOGS>
Module mq  pi
File "<full path of NPS log  pi ?
SavePos TRUE
 Lrtyx
<Output out_syslog_server>
Module <output module>
Host <collector ip address>
Port <destination port>
 Ryxtyx
<Route 1>
Path NPS_LOGS => out_syslog_server
 Usyxi
```

5. Change the following:

> Note: When changing, remove the "<" and ">" brackets (do not leave them in).

- <full path of NPS log file> - The full path and file name of the NPS log file (as set above), for example, " C:\Windows\system32\LogFiles\iaslog0.log ".
- <output module> - Whether to select `om_tcp` to use TCP (recommended) or `om_udp` to use UDP.
- <collector ip address> - The IP address of the Varonis Collector. Use the same value as configured for the network device data source in the Varonis Management Console.
- <destination port> - The port configured for the network device data source in the Varonis Management Console.

See the following example:

```
<Input NPS_LOGS>
Module mq  pi
File "C:\Windows\system32\LogFiles\iaslog0.log"
SavePos TRUE
 Lrtyx
<Output out_syslog_server>
Module om_tcp
Host 10.1.2.3
Port 514
 Ryxtyx
<Route 1>
Path NPS_LOGS => out_syslog_server
 Usyxi
```

6. To allow more than one output on NXLog, you should define more than one input (one input per output).
   See the following example:

```
<Input in_a>
Module mq  pi
File "C:\Windows\system32\LogFiles\iaslog0.log"
 Lrtyx

<Input in_b>
Module mq  pi
File "C:\Windows\system32\LogFiles\iaslog1.log "
 Lrtyx
<Output out_a>
Module om_tcp
Host 10.230.78.160
Port 520
 Ryxtyx
<Output out_b>
Module om_tcp
Host 10.230.76.44
Port 520
```

```
 Ryxtyx
<Route 1>
Path in_a => out_a
 Usyxi
<Route 2>
Path in_b => out_b
 Usyxi
```

7. Save the configuration file and restart the NXLog service.

Configuring Web Proxy Sources To Send Events To Varonis

This section describes how to configure Web Proxy Sources to send events to Varonis.

Symantec (Bluecoat) ProxySG

Varonis supports receiving web proxy events from Symantec (Bluecoat) ProxySG. Symantec provides information on how to send events to a third-party system such as Varonis in the SGOS Administration Guide, starting in the chapter Configuring Access Logging and continuing to the chapter Access Log Formats. This document outlines the specific procedure for sending events to Varonis.

Prerequisites for Symantec (Bluecoat) ProxySG

Before you begin configuring Symantec (Bluecoat) ProxySG to send web proxy events to Varonis, you must follow several prerequisites.

- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.

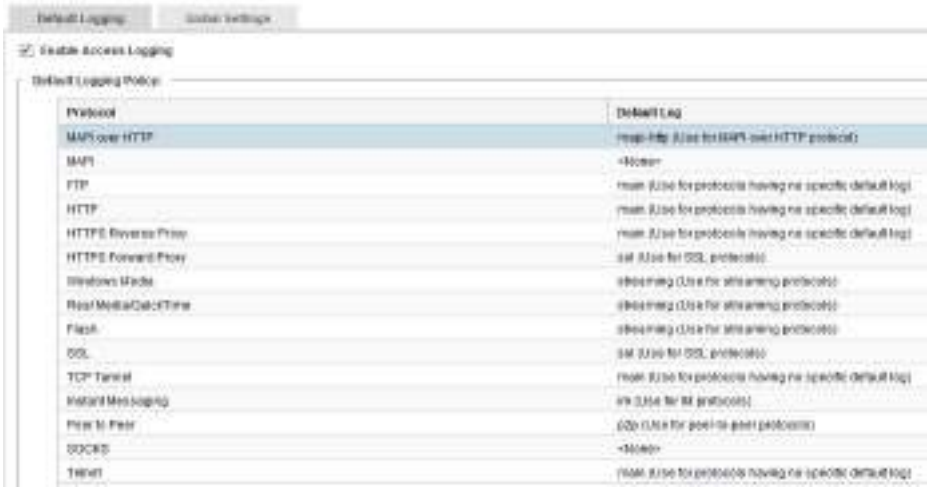
Enabling Logging

The Symantec web proxy configuration process requires enabling logging.

To enable logging:

1. In the ProxySG (Blue Coat) Management Console, select the Configuration tab.
2. From the navigation pane on the left, select Access Logging > General.
3. In the main window, select the Default Logging tab.

The Default Logging window is displayed.



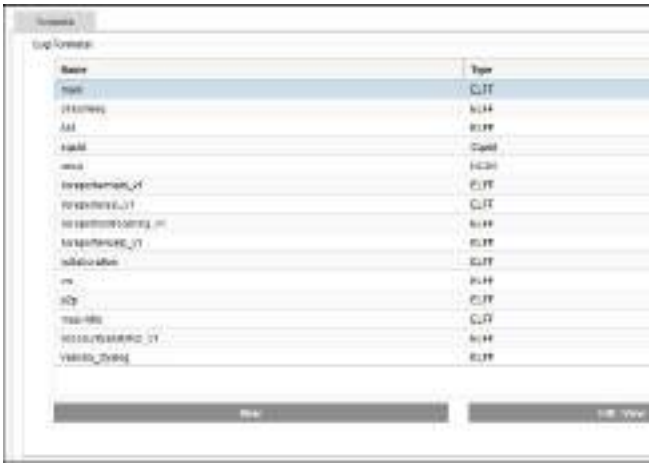
4. Ensure that Enable access logging is selected.
5. Click Apply.

Defining the Log Format

When defining the log format, ensure that you copy the strings correctly.

To define the log format:

1. In the ProxySG (Blue Coat) Management Console, select the Configuration tab.
2. From the navigation pane on the left, select Access Logging > Formats.
   The Log Formats window is displayed.



3. Click New.
   The Create Format dialog box is displayed.
4. In the Format Name filed, enter a name (for example Varonis_Syslog_Format).
5. Select W3C Extended Log Format (ELFF) string.

6. Copy the following string to the text box:

> Note: When copying this string, make sure it is copied as a single line and there is a space between the parts appearing here on separate lines.

```
date time time-taken c-ip sc-status s-action sc-bytes cs
-bytes cs-method cs-uri-scheme cs-host cs-uri-stem cs-us
ername s-supplier-name rs(Content-Type) cs(User-Agent) wg
  pxiv viwypx wg  pxiv gexiksv2 x-virus-id s-ip s-sitenam
e
```

7. From the Multiple-valued header policy dropdown list, select Log last header.



8. Click OK, and then click Apply.

Creating a Log Facility

After defining a log format, you must create a log facility.

To create a log facility:

1. In the ProxySG (Blue Coat) Management Console, select the Configuration tab.
2. From the navigation pane on the left, select Access Logging > Logs.
3. In the main window, select the Logs tab.

The Logs window is displayed.



4. Click New.
   The Create Log dialog box is displayed.



5. In the Log Name field, enter a name such as Varonis_Syslog.
6. From the Log Format dropdown list, select the log format you defined in Defining the Log Format.
7. Leave all other values at their default settings.
8. Click OK, and then click Apply.

Configuring an Upload Client

After creating a log facility, you can configure an upload client.

1. In the ProxySG (Blue Coat) Management Console, select the Configuration tab.
2. From the navigation pane on the left, select Access Logging > Logs.
3. In the main window, select the Upload Client tab.

The Upload Client window is displayed.



4. From the Log dropdown list, select the log facility you defined in Creating a Log Facility as the log to update.
5. From the Client Type dropdown list, select Custom Client.
6. Click Settings.
   The Custom Client settings: Log main dialog box is displayed.



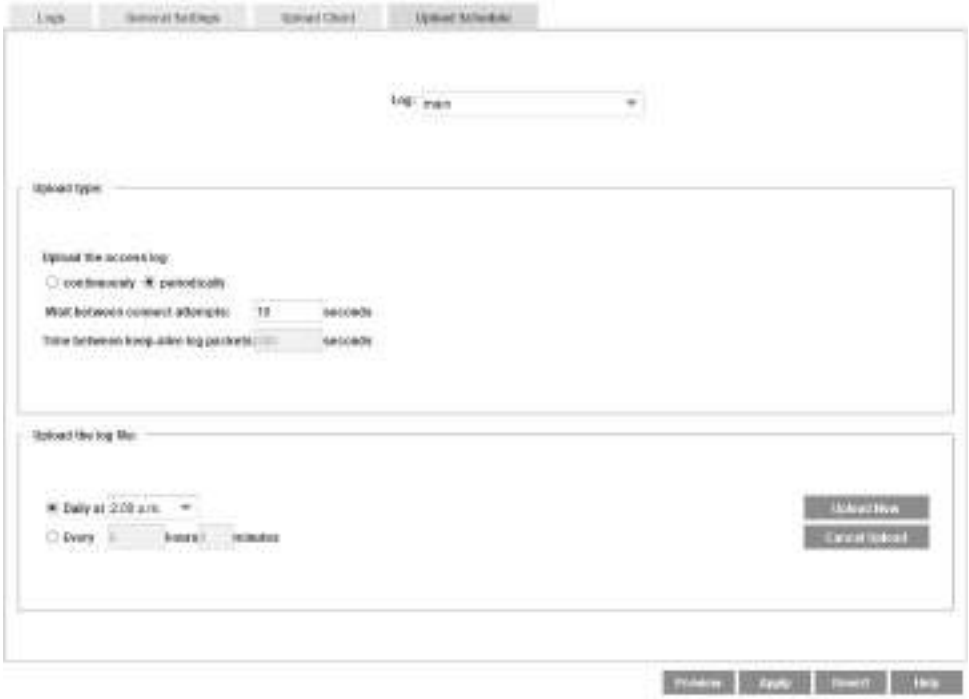
7. In the Host IP field, set the IP to the IP address or hostname of the computer hosting the network deviceCollector configured for the network device data source in the Management Console.
   For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.
8. In the Port field, enter the port configured for the network device data source in the Varonis Management Console.
9. To use a secure connection, select Use secure connections (SSL).
10. Click OK, and then click Apply.

Defining an Upload Schedule

After configuring an upload client, you should define an upload schedule before you continue.

To define an upload schedule:

1. In the ProxySG (Blue Coat) Management Console, select the Configuration tab.
2. From the navigation pane on the left, select Access Logging > Logs.
3. In the main window, select the Upload Schedule tab.
   The Upload Schedule window is displayed.
4. Go to Configuration > Access Logging > Logs > Upload Schedule.



5. From the Log, select the log facility you defined in Creating a Log Facility
6. In Upload Type, select continuously, and leave all other values at their default.
7. Click OK, and then click Apply.

Modifying Access Logging

To modify access logging:

1. Open the Visual Policy Manager.
2. Select the Web Access Layer tab, and set the Action to Modify Access Logging.
3. In the Set Action Object dialog box, click the New button.
4. In the Add Access Logging Object dialog box, set Enable logging to your new access log, and click OK.
5. To ensure that the log is written, go to Statistics > Access Logging > Select "MyLog" > Start Tail.

Skyhigh Secure Web Gateway (Previously McAfee Web Gateway)

Skyhigh Secure Web Gateway is replacing the former McAfee Web Gateway. Varonis supports receiving web proxy events from Skyhigh Secure Web Gateway.
Skyhigh Security provides information on how to send events to a third-party system such as Varonis in the Skyhigh Secure Web Gateway (On Prem) Product Guide in the section Best Practices > Logging and Monitoring > Configure Syslog for your SIEM and in the section Monitoring > Send Access Log Data to a Syslog Server. This article outlines the specific procedure for sending events to Varonis.

Prerequisites for Skyhigh Secure Web Gateway

Before you begin configuring Skyhigh Secure Web Gateway to send web proxy events to Varonis, you must follow several prerequisites.

- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog. Skyhigh Secure Web Gateway supports sending the logs via TCP or UDP protocols.

Configuring CEF Format for Logging Syslog Events

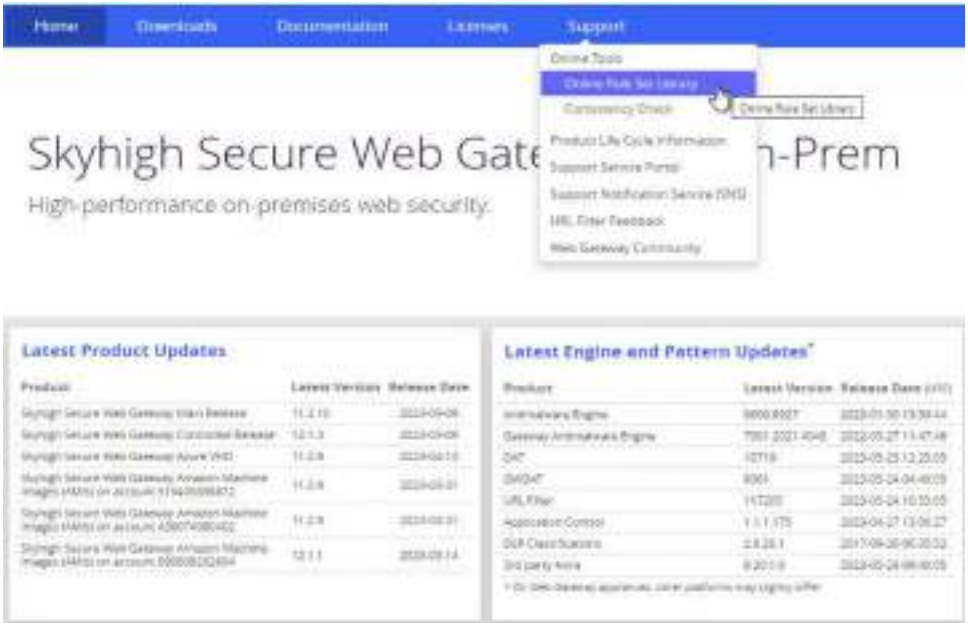
You need to configure the Common Event Format (CEF) for logging Syslog events.

To configure the CEF format:

1. Log in to the Skyhigh Security Content & Cloud Security Portal with your username and password.

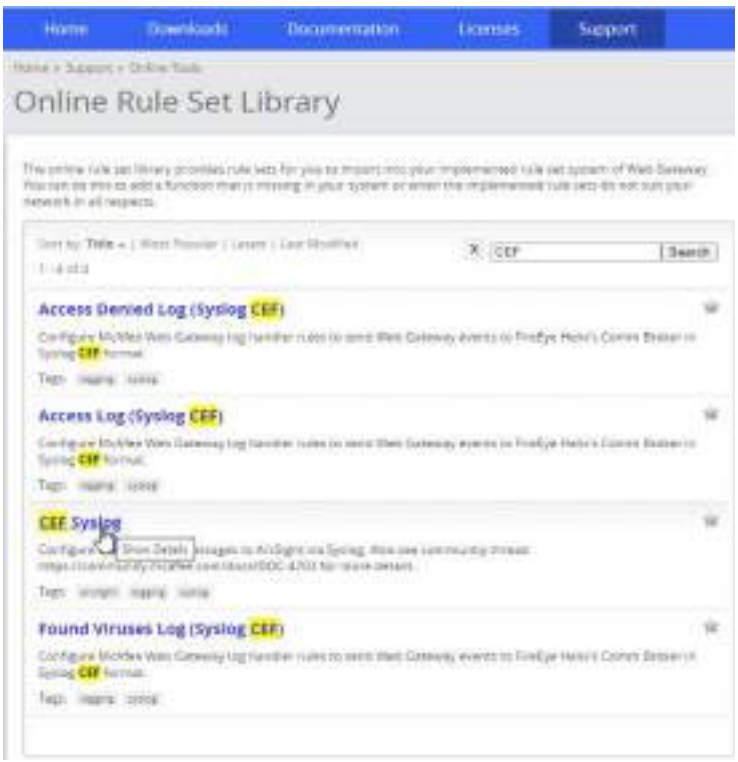


2. Select Support > Online Rule Set Library.



The Online Rule Set Library page is displayed.

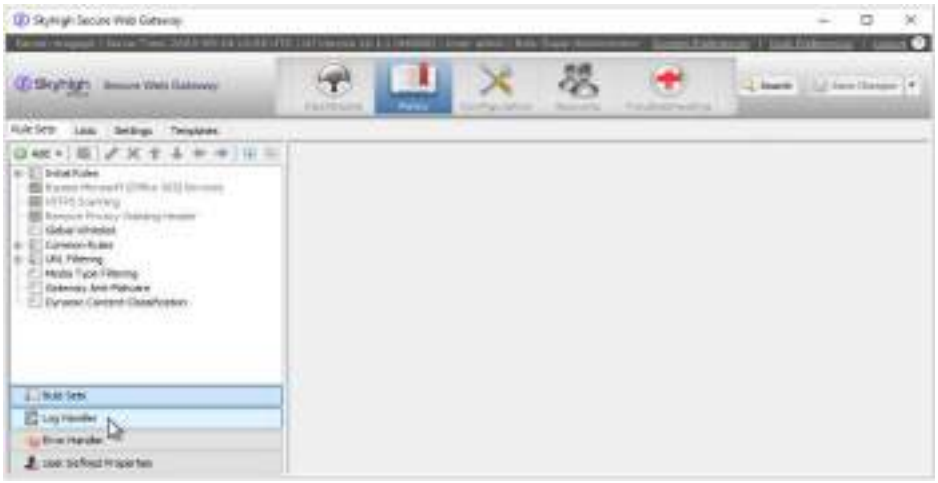
3. Search for CEF and select CEF Syslog.



4. Download the CEF Syslog Rule Set and extract the `ruleset.xml` file from the archive:



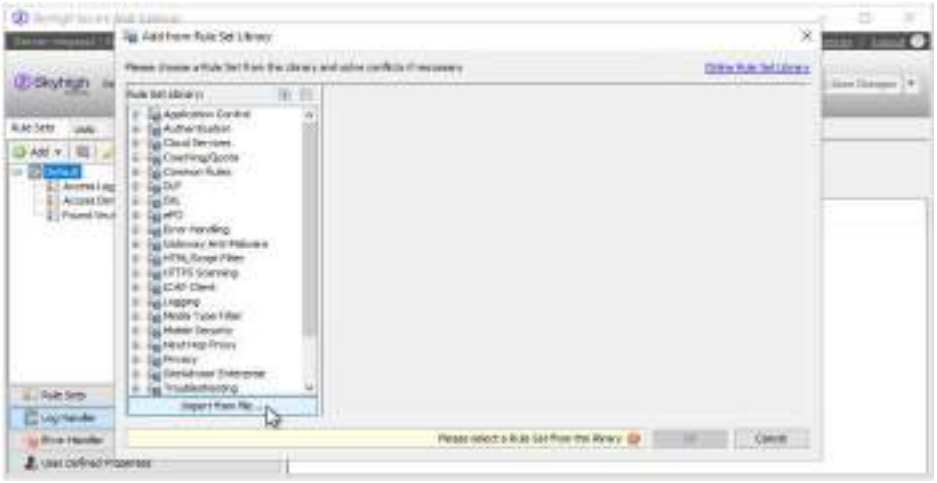
5. Open the Skyhigh Secure Web GatewayPolicy > Log Handler page



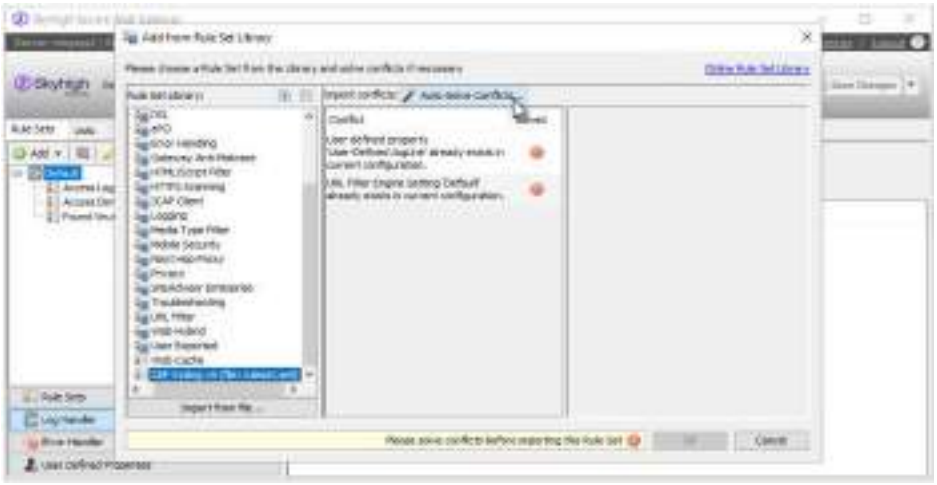
6. Right-click Default and select Add > Rule Set from Library.



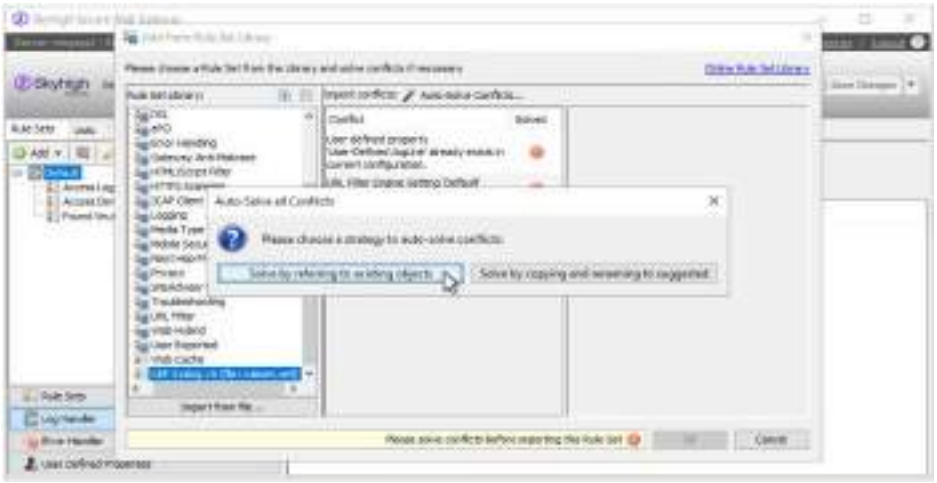
7. Import the rule set from `ruleset.xml`.



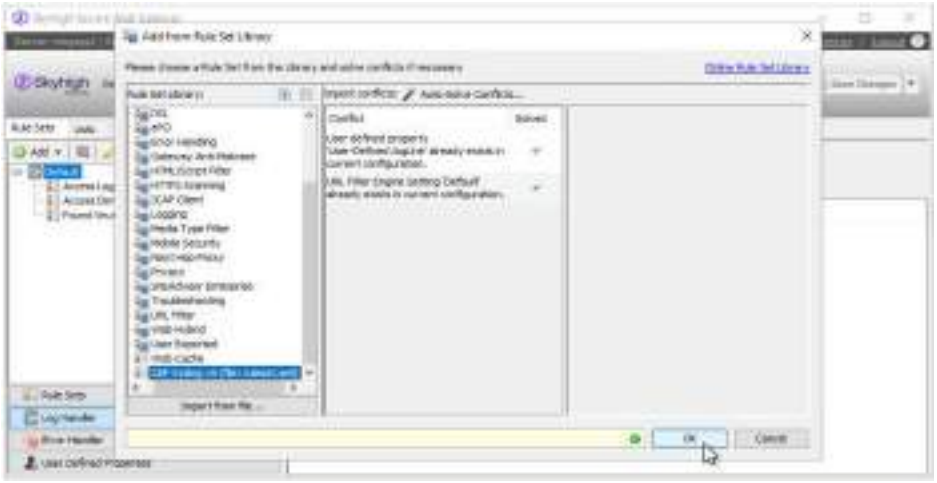
8. Auto-Solve the conflict.



9. Choose Solve by referring to existing objects.



10. Click OK to confirm the changes.



11. Select the Send to syslog checkbox.



12. Click Save Changes.



Editing the Rsyslog Configuration File

After configuring a log handler policy, you can edit the `rsyslog.conf` file and configure the Syslog server parameters.

To edit the `rsyslog.conf` file:

1. Select the Configuration tab, and then select the File Editor tab.
   The Editor window is displayed.



2. In the Files pane, select rsyslog.conf.

The `rsyslog.conf` parameters are displayed in the Editor pane.



3. Find this line: `*.info;mail.none;authpriv.none;cron.none /var/log/messages`.
4. Modify the line to this: `*.info;daemon.none;authpriv.none;cron.none -/var/log/messages`.
5. Add one of these lines at the end, depending on whether you use UDP or TCP:

   Note: When adding one of these lines, remove the "<" and ">" brackets (do not leave them in).

   - For UDP: `daemon.info @<IP_Address>:<Port_number>`
   - For TCP: `daemon.info @@<IP_Address>:<Port_number>`

   Where:

   - `<IP_Address>` is the IP address of the network device Collector.
   - `<Port_number>` is the port number.

   Note: When configuring the above, remove the "<" and ">" brackets (do not leave them in).

6. Click Save Changes.



Forcepoint (Websense) Web Security

Varonis supports receiving web proxy events from Forcepoint (Websense) Web Security.
Forcepoint provides information on how to send events to a third-party system such as a SIEM or Varonis in the article Forcepoint Security Information Event Management (SIEM) Solutions, in the section Integrating with third-party SIEM products. This article outlines the specific procedure for sending events to Varonis.

Prerequisites for Forcepoint (Websense) Web Security

Before you begin configuring Forcepoint (Websense) Web Security to send web proxy events to Varonis, you must follow several prerequisites.

- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.

Configuring Forcepoint Web Protection to Send Events to Varonis

Forcepoint Web Protection must be configured to send events to Varonis.

1. Ensure that you install an instance of a Multiplexer on each Forcepoint Policy Server as outlined in the Forcepoint guide references.
2. From the Forcepoint TRITON Manager main window, click Web at the top to open the web module.
   For each Policy Server instance in your deployment, do the following steps.
3. From the navigation pane on the left, select Settings > General > SIEM Integration.

The SIEM Integration window is displayed.



4. Select the Enable SIEM integration for this Policy Server checkbox.
5. Enter the following:
   - IP address or hostname - For the IP address, enter the same value as configured for the network device data source in the Varonis Management Console.
   - Port - Enter the same value as configured for the network devicedata source in the Varonis Management Console
   - Transport - Specify TCP or UDP as the protocol.

   For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.
6. In the SIEM format field, select Syslog/CEF (ArcSight).
7. Save the changes.
   After the changes have been saved, the Multiplexer distributes the log data it receives from the filtering service to both the log server and the selected SIEM integration.

Fortinet FortiGate

Varonis supports receiving web proxy events from the Fortinet FortiGate Firewall. You can configure Fortinet FortiGate to send web proxy events to Varonis by using a graphical user interface or command line interface.

FortiOS 6.x and 7.x

This section describes the procedures required for FortiOS version 6.x and 7.x.

Prerequisites for Fortinet FortiGate

Before you begin configuring Fortinet FortiGate to send web proxy events to Varonis, you must follow several prerequisites.

- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.

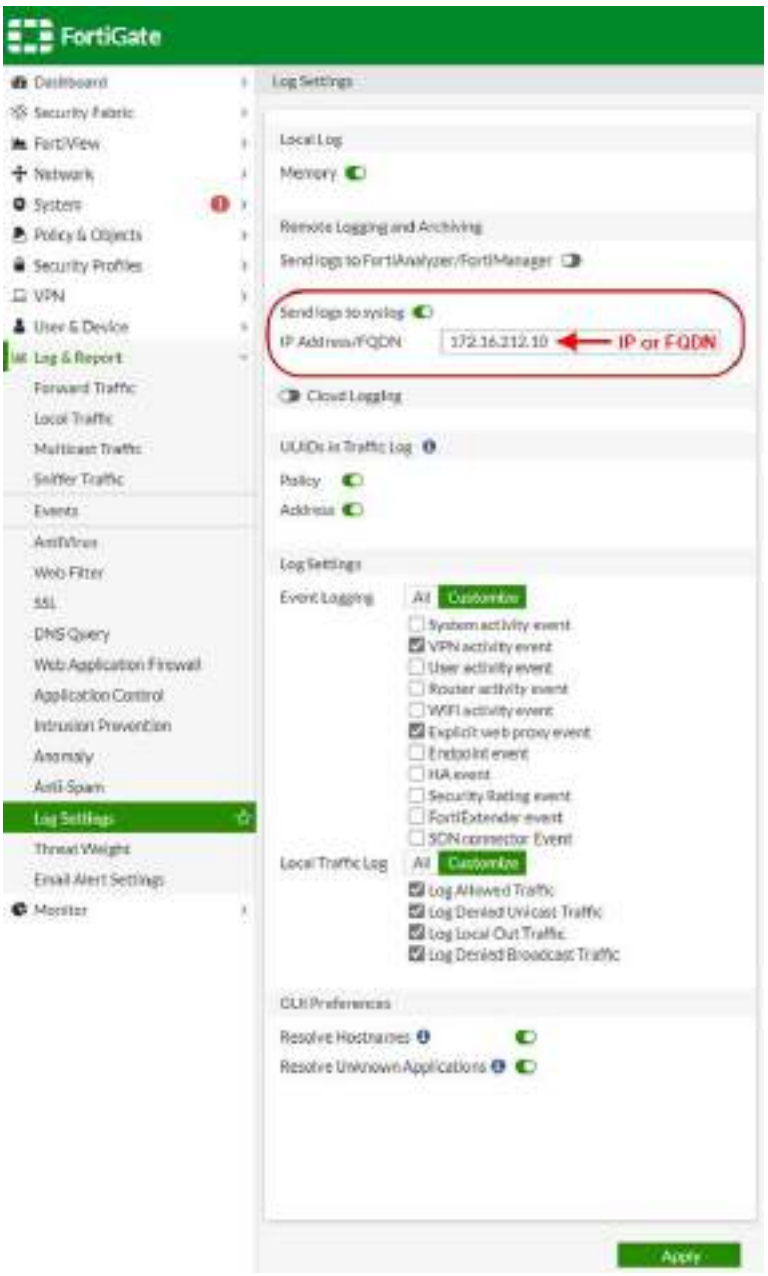
Configuring Fortinet Explicit Web Proxy Logging Using a Graphical User Interface or Command Line Interface

To enable Varonis to collect Syslog messages from FortiOS 6.x, you need to configure the settings on the FortiGate side.

Configuring Fortinet Explicit Web Proxy Logging Using a Graphical User Interface

1. In the Fortinet main window, from the navigation pane, select Log & Report > Log Settings.
   The Log Settings window is displayed.
2. Select Send Logs to Syslog and enter the IP address configured for the network device data source in the Varonis Management Console. This is the FQDN or IP

address of the Varonis Collector server.



3. Ensure that the Policy and Address options in the UUIDs in Traffic Log section are selected.
4. (Optional) To configure custom ports:
   a. From the Fortinet main window, to open the CLI click the CLI Console button on the title bar, as shown below.



   b. Run the following CLI command:

```
set port <port_integer>
```

5. In the Event Logging section, click Customize and select the Explicit web proxy event checkbox. If VPN is also being monitored by Varonis, select also the VPN activity event checkbox. Click Apply to apply the changes.
6. (Optional) If more than one Syslog server is configured, the Syslog servers and their settings appear on the Log Settings page. You can configure multiple Syslog servers in the CLI using the `gsr k log {syslog | syslog2 | syslog3}` settings CLI command.

Configuring Fortinet Explicit Web Proxy Logging Using a Command Line Interface

1. Run the following CLI commands:

```
gsr k log syslogd setting
    set status enable
    set server <IP address or FQDN of syslog server>
    set port <port_integer>
end
```

2. For event logging, run the following CLI commands:

```
gsr k log izirx pxiv
    set event enable
    set system enable
    set vpn enable
    set user enable
end
```

3. (Optional) If other Syslog servers are already configured, run the following CLI command to set multiple Syslog servers:

```
gsr k log {syslog | syslog2 | syslog3}
```

Configuring Fortinet FortiAnalyzer Web Proxy Logging Using a Graphical User Interface

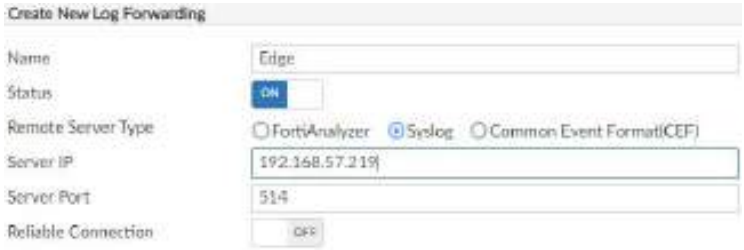
1. In the Fortinet FortiAnalyzer main window, select System Settings.
   The System Settings window is displayed.



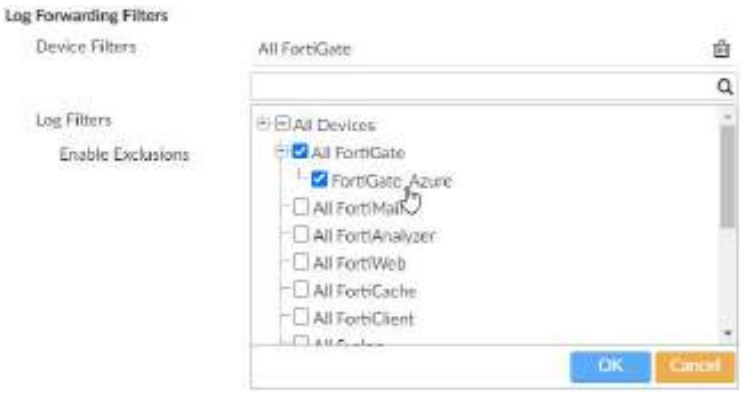
2. From the navigation pane on the left, select Log Forwarding, and click the Create New link at the top.



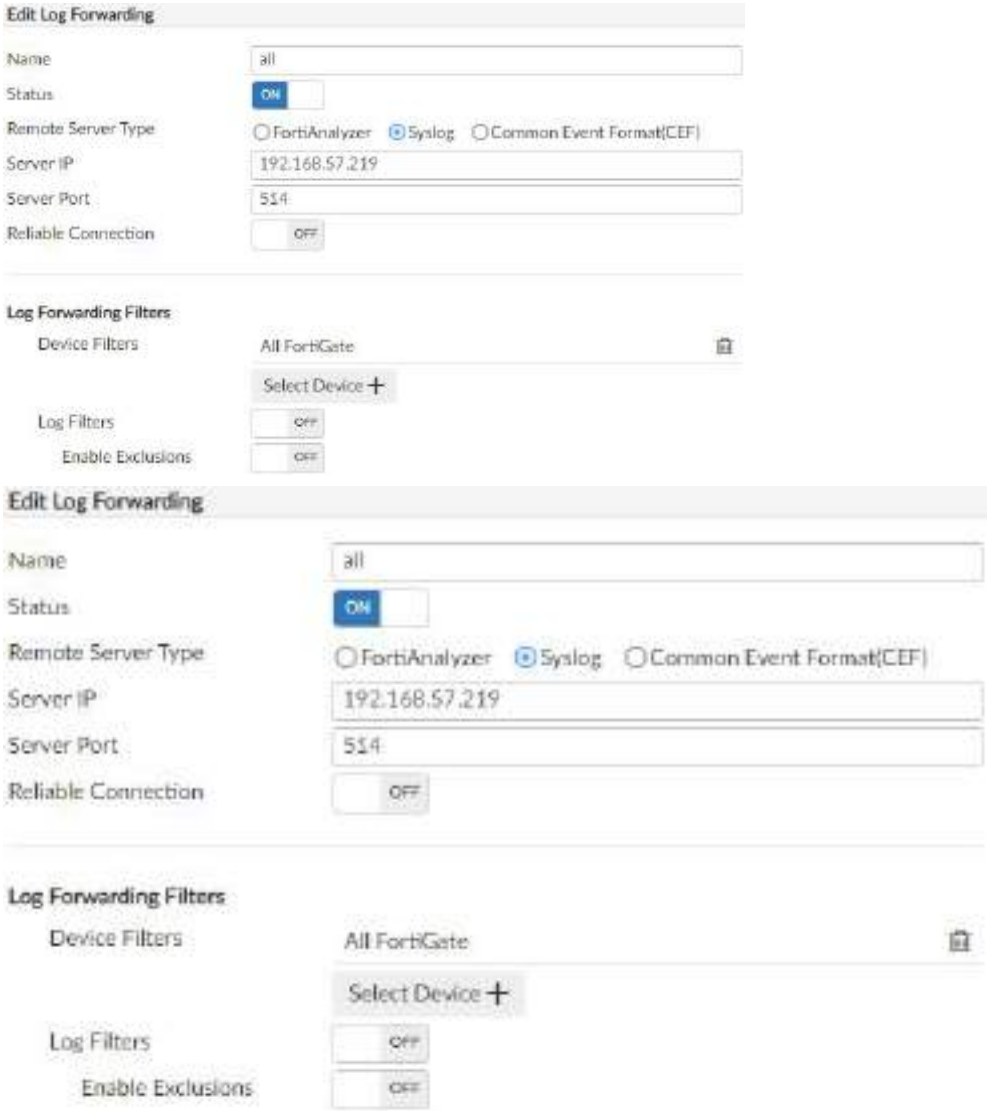
   The Create New Log Forwarding window is displayed.



3. Enter the following:
   - Name - The name for the forwarding configuration entry (for example, Varonis).
   - Status - On by default.
   - Remote Server Type - Select Syslog.
   - Server IP - The IP address of the Varonis Collector, as configured for the Varonis data source in the Varonis Management Console.
   - Server Port - Enter the same value as configured for the Varonis data source in the Varonis Management Console
   - Reliable Connection - Off by default, as required for UDP. If you are using TCP, enable this to On.
4. To specify the log forwarding filters, in the Device Filters field, from the All FortiGate dropdown list, select the checkboxes of the relevant FortiGate servers, or select All Devices to include all of them.



5. Click OK to apply the changes.



6. Ensure that the relevant settings are selected in the Event Logging section, as described in step 4 in "Configuring Fortinet VPN Logging Using a Graphical User Interface or Command Line Interface".

Palo Alto Web Filtering

Varonis supports receiving web proxy events from the Palo Alto Firewalls Web Filtering feature, which is part of the Palo Alto firewall.
Palo Alto provides information on how to send events to a third-party system such as Varonis in the article Configure Syslog Monitoring. This article outlines the specific procedure for sending events to Varonis.

When configuring Palo Alto to send events to Varonis, it is recommended to configure the firewall to monitor SSL traffic and map sessions to user names, as outlined in the Prerequisites for Palo Alto Web Filtering.

> Note: It is possible to configure log settings from Palo Alto Networks Panorama as well. The configuration steps are similar to those described in the following sections.

PAN-OS 7.x and 8.x

This section describes the procedures required for PAN-OS version 7.x and 8.x.

Prerequisites for Palo Alto Web Filtering

Before you begin configuring Palo Alto Web Filtering to send web proxy events to Varonis, you must follow several prerequisites.

- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.
- Setting up the Palo Alto firewall for the following will both help the firewall provide better security and help Varonis derive the maximal value from collecting the events. See these articles on the Palo Alto Networks website:
  - To configure the firewall to decrypt SSL traffic, follow the procedure in How to Implement and Test SSL Decryption.
  - To configure the firewall to map sessions to user names, follow the procedure in Configure User Mapping Using the PAN-OS Integrated User-ID Agent.

Creating a Syslog Server Profile

The Palo Alto Web Filtering configuration process requires creating a Syslog server profile.

1. From the Palo Alto main window, select the Device tab.
   The Device window is displayed.
2. From the navigation pane on the left, select Server Profiles > Syslog.
   The Syslog window is displayed.



3. Click Add (at the bottom).
   The Syslog Server Profile dialog box is displayed.
4. Click Add to add a new server. Enter the following:
   - Name - Enter any name such as Varonis or the name of the specific network device used, for example Varonis NYC Collector.
   - Syslog Server - The IP address or FQDN. For the IP address, enter the same value as configured for the network device data source in the Varonis Management Console.
   - Transport - Select TCP or UDP as the protocol for communicating with the Syslog server. Enter the same value as configured for the network device data source in the Varonis Management Console.
   - Port - Enter the same value as configured for the network device data source in the Varonis Management Console.
   - Format - Select BSD.

- Facility - Keep the default, LOG_USER.



5. Click OK.
   A new Syslog server profile is created.

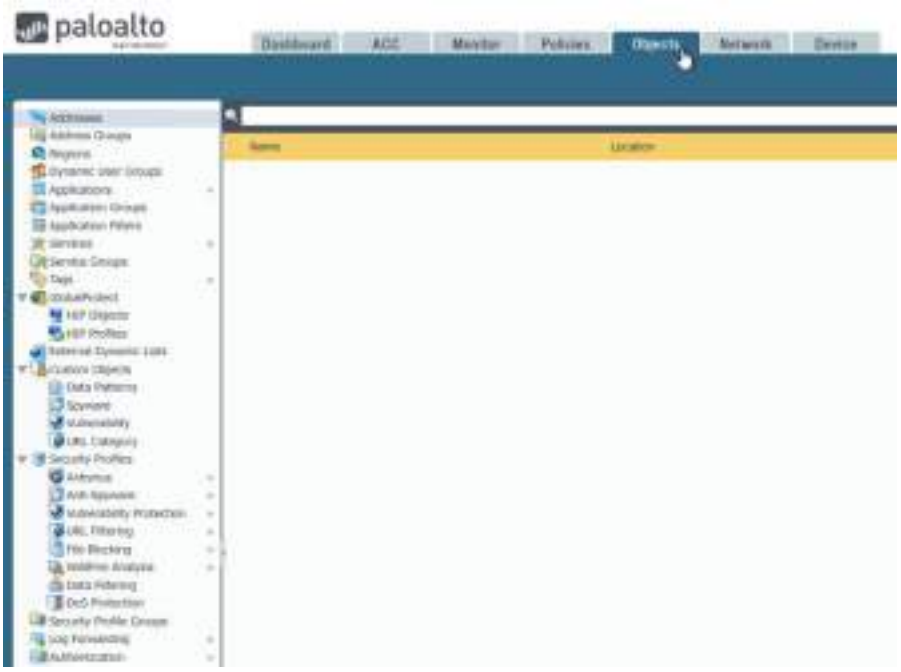
Configuring the Log Forwarding Profile

After creating a Syslog server profile, configure a log forwarding profile, as required by the Palo Alto Web Filtering configuration process.

> Note: If you have already configured a log-forwarding profile, and need to configure an additional profile, for more information, see Adding a Syslog Server to an Existing Log Forwarding Profile.

1. From the Palo Alto main window, select the Objects tab.

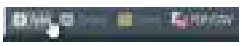
The Objects window is displayed.



2. From the navigation pane on the left, select Log Forwarding.



3. Click Add (at the bottom).

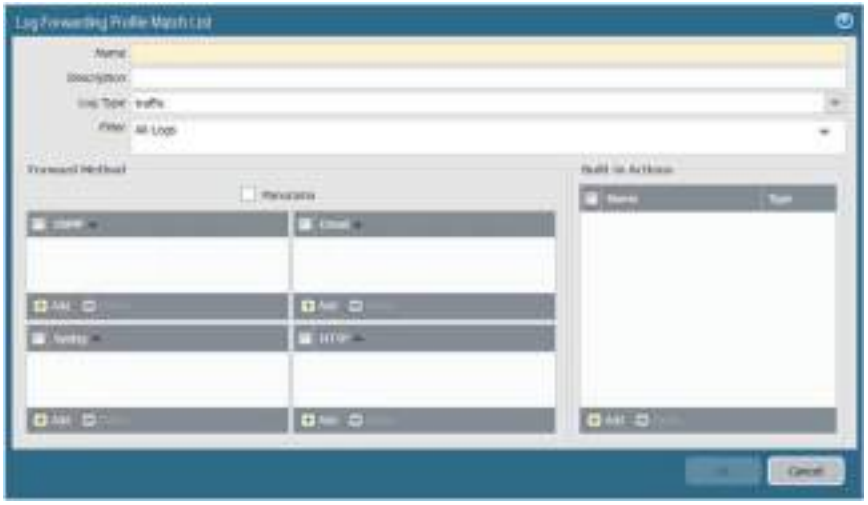


The Log Forwarding Profile dialog box is displayed.

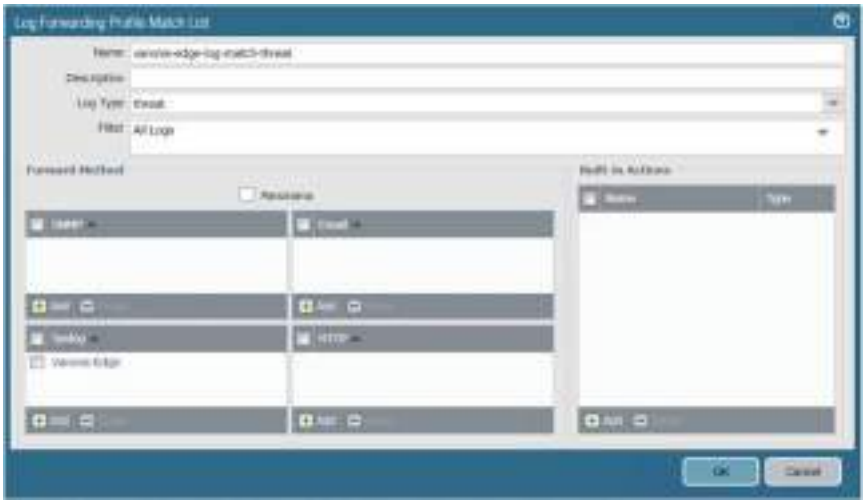


4. Click Add.

The Log Forwarding Profile Match List dialog box is displayed.

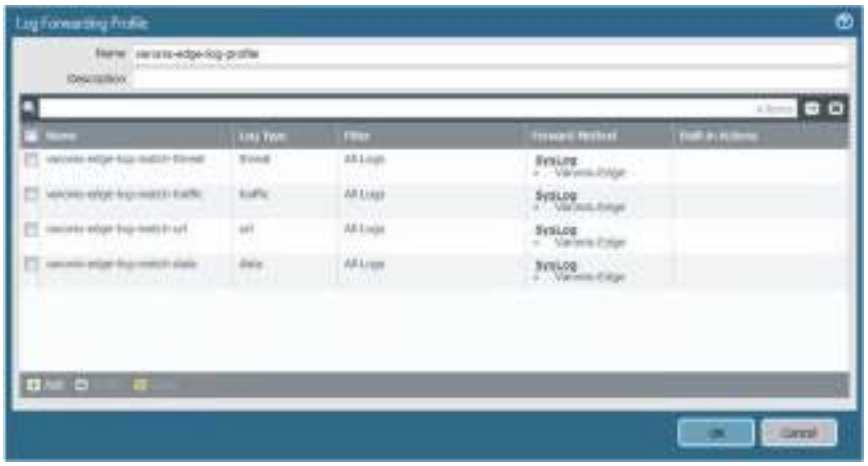


5. In the Name field, enter a name, for example varonis-log-profile.
6. Add a match list profile for each of the following log types: threat, traffic, URL, and data. For each match list profile, do the following:
   a. Click Add.
   b. In the Name field, specify a name, such as varonis-log-match-threat.
   c. In the Log Type field, select the log type.
   d. Add the Syslog server profile created above to the Syslog section.
   e. Click OK.



7. Click OK.

The profiles are displayed in the Log Forwarding Profile dialog box.



8. Click OK.

Adding a Syslog Server to an Existing Log Forwarding Profile

After configuring a log forwarding profile and performing all previous relevant procedures, it is possible to add an additional Syslog server under the existing profile.

To add a Syslog Server to an existing log forwarding profile:

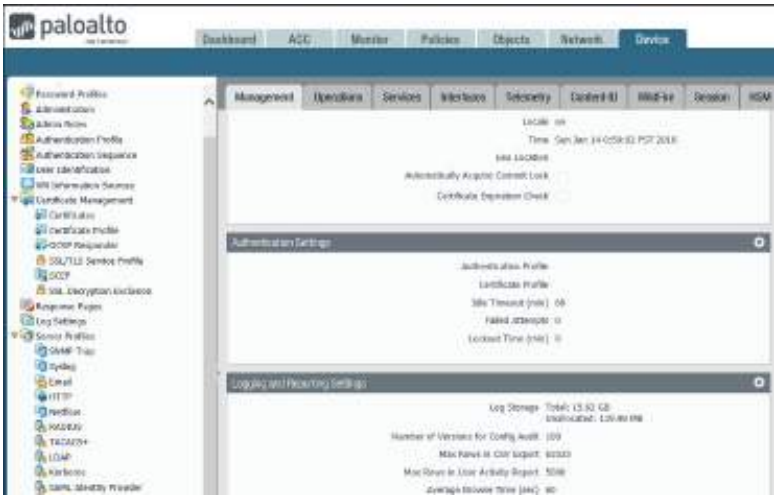
1. From the Palo Alto main window, select the Objects tab.
   The Objects window is displayed.
2. From the navigation pane on the left, select Log Forwarding.
   The Log Forwarding window is displayed.
3. From the Name column, click the existing log forwarding profile.
   The Log Forwarding Profile dialog box is displayed.
4. In the Name column, click the object's name.
   The Log Forwarding Profile Match List dialog box is displayed.
5. In the Syslog area, click Add, and select the new Syslog profile.
6. Click OK, and repeat for all the objects in the Name column in the Log Forwarding Profile dialog box.
7. Click OK when done.
   The new profile is displayed in the Forward Method column in the Log Forwarding Profile dialog box.
8. Click OK, and from the top right of the window, click Commit.
   The new profile is displayed in the Objects tab.

Configuring the Header Format of Syslog Messages

After configuring the log forwarding profile, it is important to configure the header format of Syslog messages.

To configure the header format of Syslog messages:

1. Select the Device tab.
   The Device window is displayed.
2. From the navigation pane on the left, select Setup.
3. Select the Management tab.



4. In the Logging and Reporting Settings area, click the edit wheel .
   The area is displayed in edit mode.
5. Select the Log Export and Reporting Settings tab.
6. In the Syslog HOSTNAME Format field, select ipv4-address or FQDN.



7. Click OK.

The Logging and Reporting Settings area is updated.

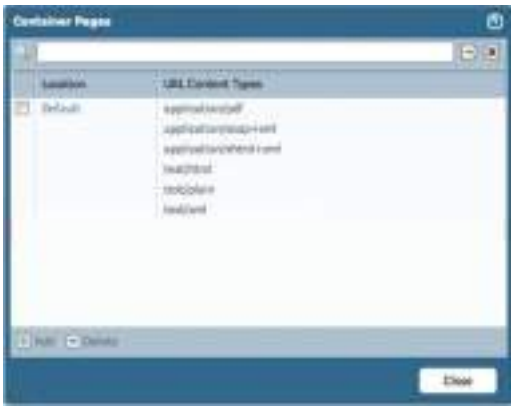


Adding Content Types to the Log

After configuring the header format of Syslog messages, it is necessary add the content types to the log.

1. From the Palo Alto main window, select the Device tab.
   The Device window is displayed.
2. From the navigation pane on the left, select Setup.
3. In the Device window, select the Content-ID tab.
4. In the Content-ID Features area, click Container Pages.
   The Container Pages dialog box is displayed.
5. Click Add (at the bottom).
   The Custom URL Content Type dialog box is displayed.
6. Make sure all content types from the default location exist in the container.
7. Click Add and add the following URL content types:
   - application/

- application/octet-stream



8. Click OK, and then click Close.

Configuring URL Filtering Profiles

After adding content types to the log, it is necessary to configure the URL filtering profiles.

1. From the Palo Alto main window, select the Objects tab.
   The Objects window is displayed.
2. From the navigation pane on the left, select Security Profiles > URL Filtering.
   The URL Filtering window is displayed.
3. Click Add.
   The URL Filtering Profile dialog box is displayed.
4. Do the following for each URL filtering profile used in your security policy:
   a. Select the URL Filtering Settings tab.
   b. In HTTP Header Logging area, select all available HTTP headers.

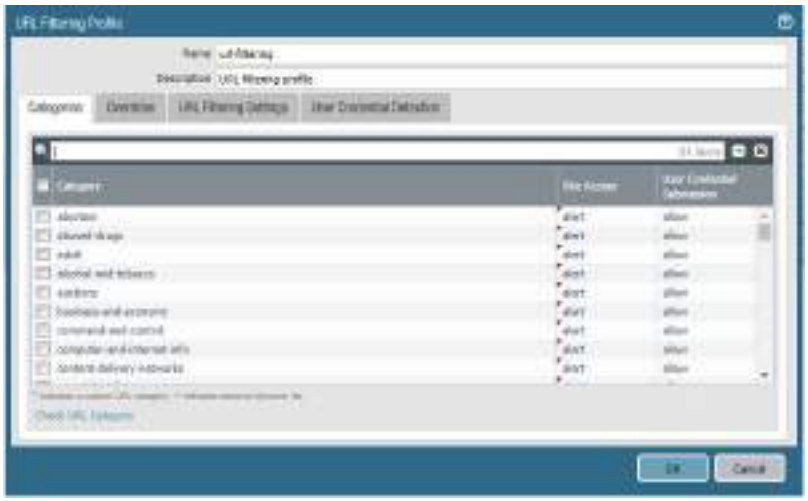


> Note: If SSL decryption is not configured, HTTP headers will not be logged for SSL requests.

   c. Ensure that Log Container page only is selected.

d. Select the Categories tab.

e. Ensure that the associated URL filtering profile has all categories set to an action other than “none”.



5. Click OK.

Configuring Security Policy Rules

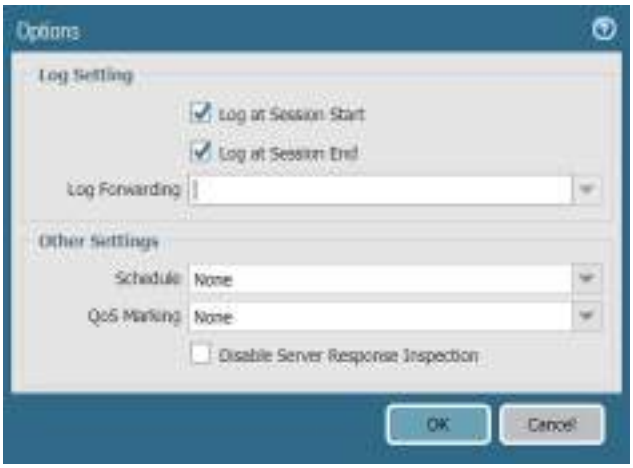
It is important to configure rules to determine your security policy.

1. From the Palo Alto main window, select the Policies tab.
2. From the navigation pane on the left, click Security.



3. For each proxy-related security policy rule, click its cell inside the Options column.

The Options dialog box is displayed.



4. Select the Log at Session Start and Log at Session End checkboxes.
5. From the Log Forwarding dropdown list, select the log forwarding profile you defined previously.
6. Click OK.

Committing the Changes

After configuring Palo Alto Web Filtering and performing all the previous relevant procedures, it is necessary to commit all changes.

From of the top of the Palo Alto window, click Commit.
All changes are committed.

PAN-OS 9.x

This section describes the procedures required for PAN-OS version 9.x.

Prerequisites for Palo Alto Web Filtering

Before you begin configuring Palo Alto Web Filtering to send web proxy events to Varonis, you must follow several prerequisites.

- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.
- Setting up the Palo Alto firewall for the following will both help the firewall provide better security and help Varonis derive the maximal value from collecting the events. See these articles on the Palo Alto Networks website:
  - To configure the firewall to decrypt SSL traffic, follow the procedure in How to Implement and Test SSL Decryption.

- To configure the firewall to map sessions to user names, follow the procedure in Configure User Mapping Using the PAN-OS Integrated User-ID Agent.

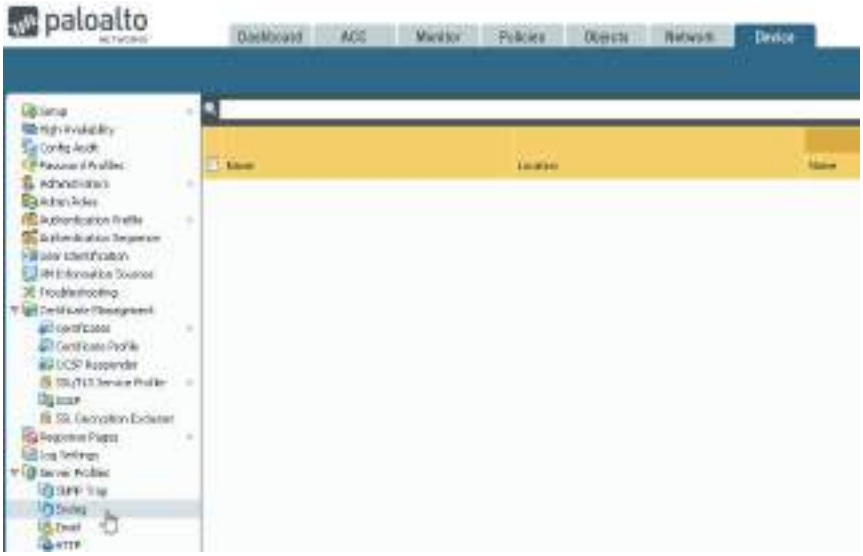
Creating a Syslog Server Profile

The Palo Alto Web Filtering configuration process requires creating a Syslog server profile.

1. From the Palo Alto main window, select the Device tab.
   The Device window is displayed.



2. From the navigation pane on the left, select Server Profiles > Syslog.
   The Syslog window is displayed.



3. Click Add (at the bottom).
   The Syslog Server Profile dialog box is displayed.



4. Click Add to add a new server. Enter the following:

- Name - Select any name such as Varonis or the name of the specific network device Collector used, for example Varonis NYC Collector.
- Syslog Server - Specify the IP address or FQDN. For the IP address, enter the same value as configured for the network device data source in the Varonis Management Console
- Transport - Select TCP or UDP as the protocol for communicating with the Syslog server. Enter the same value as configured for the network device data source in the Varonis Management Console.
- Port - Enter the same value as configured for the network device data source in the Varonis Management Console
- Format - Select BSD.
- Facility - Keep the default, LOG_USER.



5. Click OK.
   A new Syslog server profile is created.

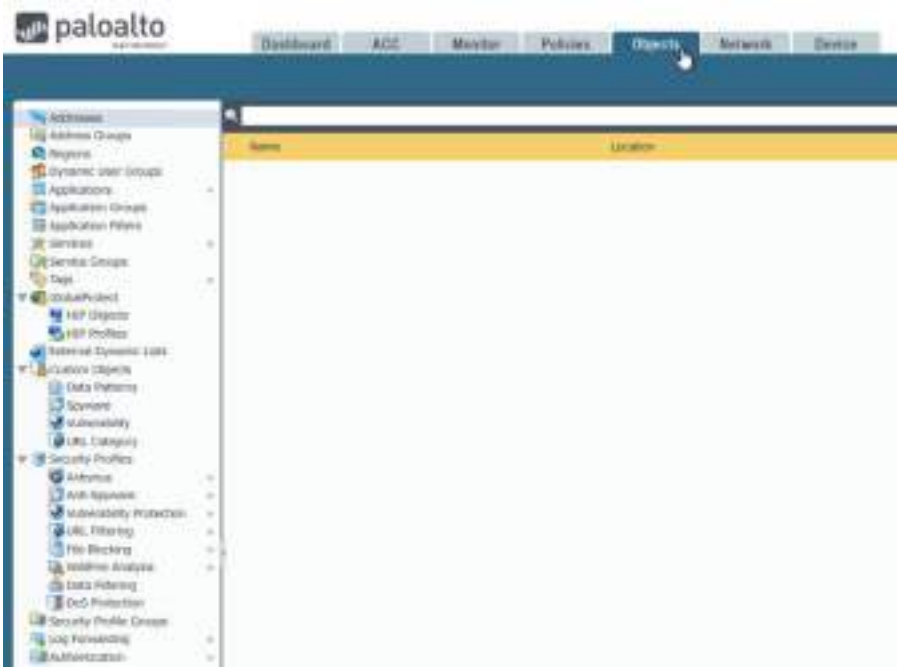
Configuring the Log Forwarding Profile

After creating a Syslog server profile, configure a log forwarding profile, as required by the Palo Alto Web Filtering configuration process.

Note: If you have already configured a log-forwarding profile, and need to configure an additional profile, for more information, see Adding a Syslog Server to an Existing Log Forwarding Profile.

1. From the Palo Alto main window, select the Objects tab.

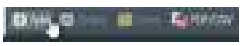
The Objects window is displayed.



2. From the navigation pane on the left, select Log Forwarding.



3. Click Add (at the bottom).

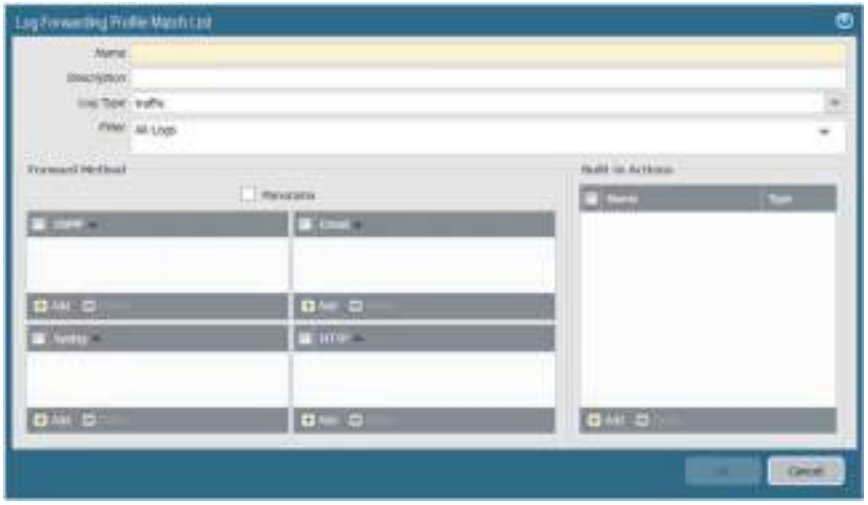


The Log Forwarding Profile dialog box is displayed.

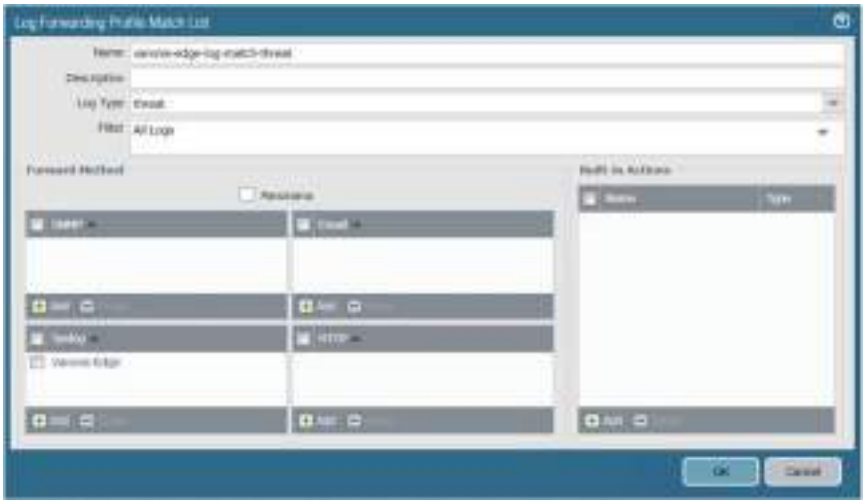


4. Click Add.

The Log Forwarding Profile Match List dialog box is displayed.

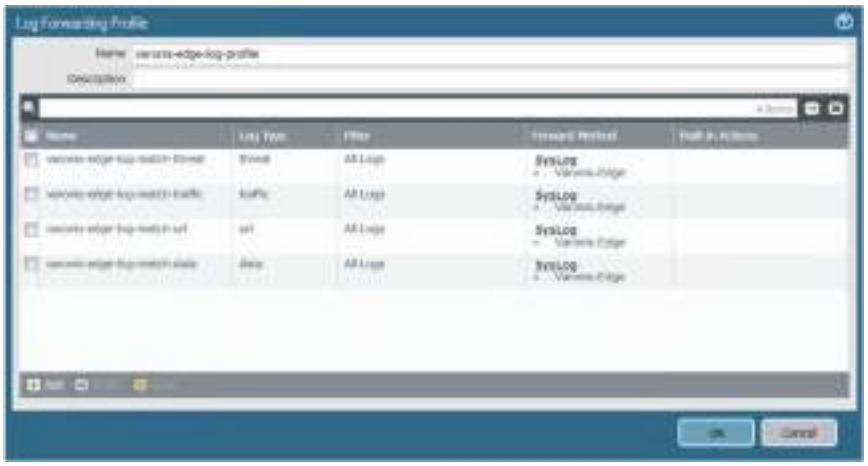


5. In the Name field, enter a name, for example varonis-log-profile.
6. Add a match list profile for each of the following log types: threat, traffic, URL, and data. For each match list profile, do the following:
   a. Click Add.
   b. In the Name field, specify a name, such as varonis-log-match-threat.
   c. In the Log Type field, select the log type.
   d. Add the Syslog server profile created above to the Syslog section.
   e. Click OK.



7. Click OK.

The profiles are displayed in the Log Forwarding Profile dialog box.



8. Click OK.

Adding a Syslog Server to an Existing Log Forwarding Profile

After configuring a log forwarding profile and performing all previous relevant procedures, it is possible to add an additional Syslog server under the existing profile.

1. From the Palo Alto main window, select the Objects tab.
   The Objects window is displayed.
2. From the navigation pane on the left, select Log Forwarding.
   The Log Forwarding window is displayed.
3. From the Name column, click the existing log forwarding profile.
   The Log Forwarding Profile dialog box is displayed.
4. In the Name column, click the object's name.
   The Log Forwarding Profile Match List dialog box is displayed.
5. In the Syslog area, click Add, and select the new Syslog profile.
6. Click OK, and repeat for all the objects in the Name column in the Log Forwarding Profile dialog box.
7. Click OK when done.
   The new profile is displayed in the Forward Method column in the Log Forwarding Profile dialog box.
8. Click OK, and from the top right of the window, click Commit.
   The new profile is displayed in the Objects tab.

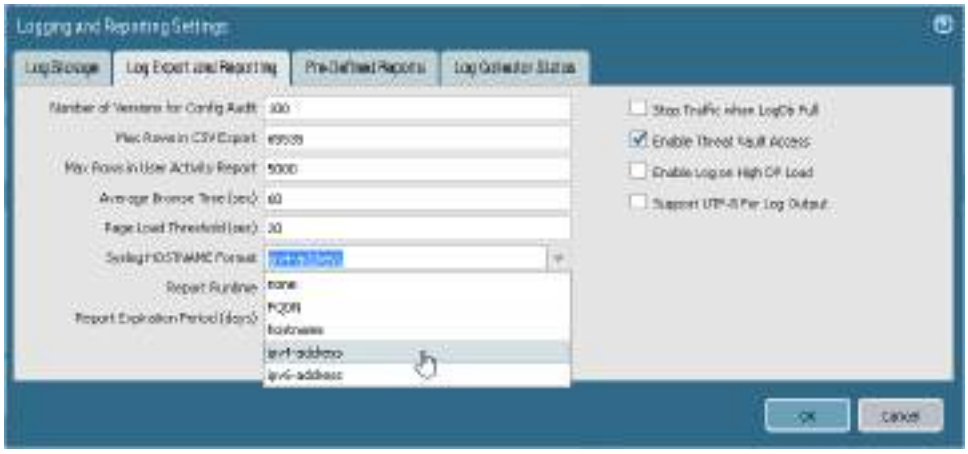
Configuring the Header Format of Syslog Messages

After configuring the log forwarding profile, it is important to configure the header format of Syslog messages.

1. Select the Device tab.
   The Device window is displayed.
2. From the navigation pane on the left, select Setup.
3. Select the Management tab.



4. In the Logging and Reporting Settings area, click the edit wheel on the upper right.
   The area is displayed in edit mode.
5. Select the Log Export and Reporting Settings tab.
6. In the Syslog HOSTNAME Format field, select ipv4-address or FQDN.



7. Click OK.

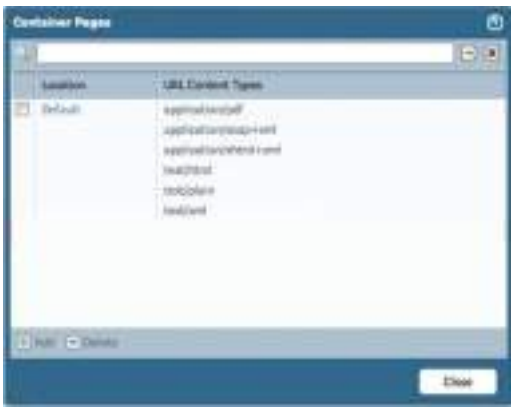
The Logging and Reporting Settings area is updated.



Adding Content Types to the Log

After configuring the header format of Syslog messages, it is necessary add the content types to the log.

1. From the Palo Alto main window, select the Device tab.
   The Device window is displayed.
2. From the navigation pane on the left, select Setup.
3. In the Device window, select the Content-ID tab.
4. In the Content-ID Features area, click Container Pages.
   The Container Pages dialog box is displayed.
5. Click Add (at the bottom).
   The Custom URL Content Type dialog box is displayed.
6. Make sure all content types from the default location exist in the container.
7. Click Add and add the following URL content types:
   - application/
   - application/octet-stream



8. Click OK, and then click Close.

Configuring URL Filtering Profiles

After adding content types to the log, it is necessary to configure the URL filtering profiles.

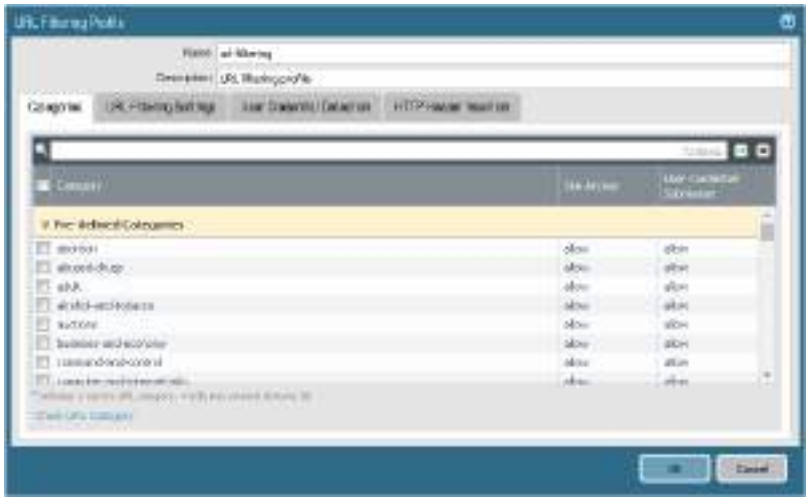
1. From the Palo Alto main window, select the Objects tab.
   The Objects window is displayed.
2. From the navigation pane on the left, select Security Profiles > URL Filtering.
   The URL Filtering window is displayed.
3. Click Add.
   The URL Filtering Profile dialog box is displayed.
4. Do the following for each URL filtering profile used in your security policy:
   a. Select the URL Filtering Settings tab.
   b. In the HTTP Header Logging area, select all available HTTP headers.



> Note: If SSL decryption is not configured, HTTP headers will not be logged for SSL requests.

   c. Ensure that Log Container page only is selected.
   d. Select the Categories tab.

e. Ensure that the associated URL filtering profile has all categories set to an action other than “none”.



5. Click OK.

Configuring Security Policy Rules

It is important to configure rules to determine your security policy.

1. From the Palo Alto main window, select the Policies tab.
2. From the navigation pane on the left, click Security.



3. For each proxy-related security policy rule, click its cell inside the Options column.

The Options dialog box is displayed.



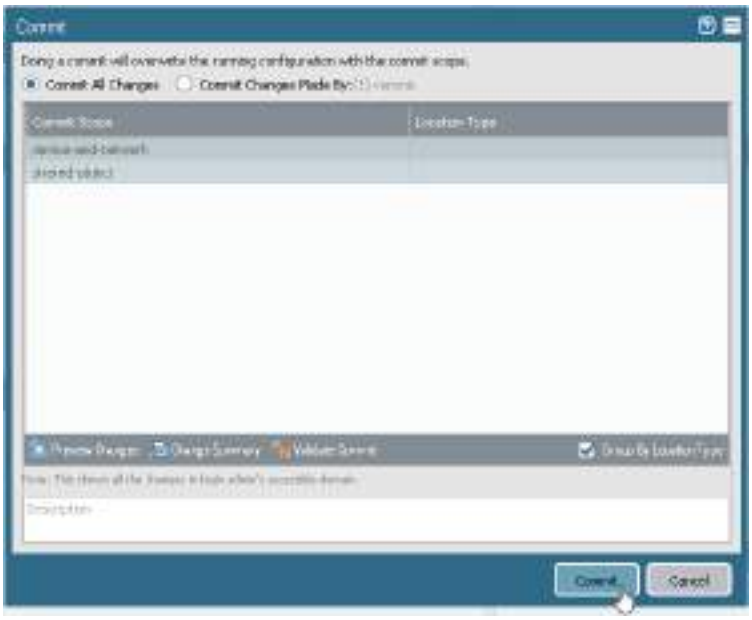
4. Select the Log at Session Start and Log at Session End checkboxes.
5. From the Log Forwarding dropdown list, select the log forwarding profile you defined previously.
6. Click OK.

Committing the Changes

After configuring Palo Alto Web Filtering and performing all the previous relevant procedures, it is necessary to commit all changes.

From of the top of the Palo Alto window, click Commit.





All changes are committed.

PAN-OS 10.x

This section describes the procedures required for PAN-OS version 10.x.

Prerequisites for Palo Alto Web Filtering

Before you begin configuring Palo Alto Web Filtering to send web proxy events to Varonis, you must follow several prerequisites.

- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.
- Setting up the Palo Alto firewall for the following will both help the firewall provide better security and help Varonis derive the maximal value from collecting the events. See these articles on the Palo Alto Networks website:
  - To configure the firewall to decrypt SSL traffic, follow the procedure in How to Implement and Test SSL Decryption.
  - To configure the firewall to map sessions to user names, follow the procedure in Configure User Mapping Using the PAN-OS Integrated User-ID Agent.

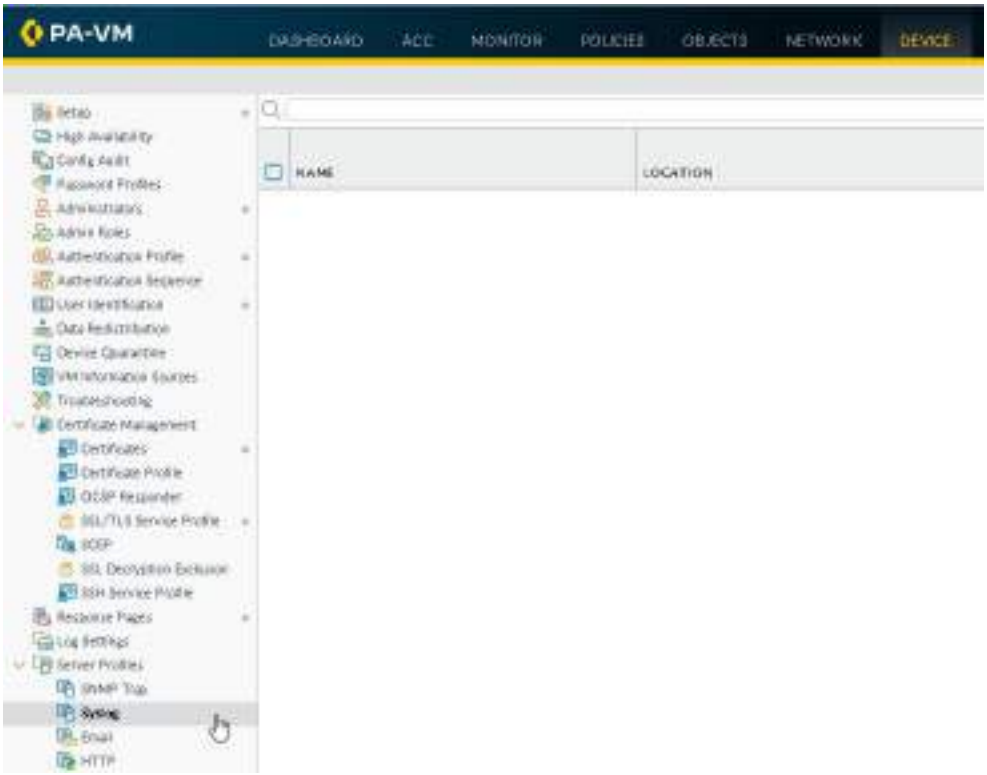
Creating a Syslog Server Profile

The Palo Alto Web Filtering configuration process requires creating a Syslog server profile.

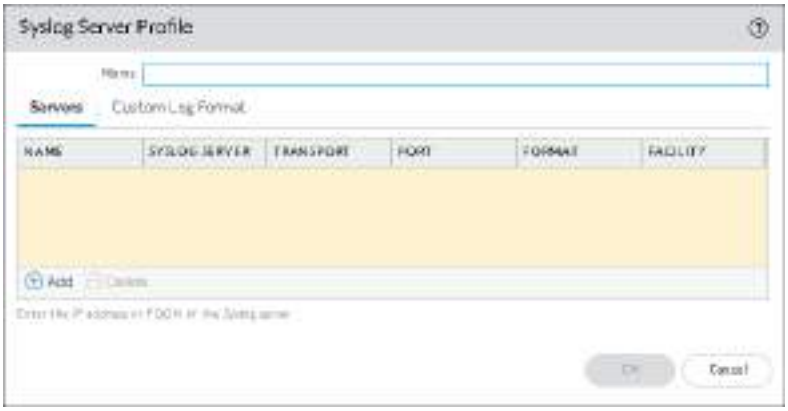
1. From the Palo Alto main window, select the Device tab.
   The Device window is displayed.



2. From the navigation pane on the left, select Server Profiles > Syslog.
   The Syslog window is displayed.



3. Click Add (at the bottom).
   The Syslog Server Profile dialog box is displayed.



4. Click Add to add a new server. For the following, if not detailed below, enter the same value as configured for the network device data source in the Varonis Management Console:
   - Name - Select any name such as Varonis or the name of the specific Varonis Collector used, for example Varonis NYC Collector.
   - Syslog Server - Specify the IP address or FQDN.
   - Transport - Select the protocol for communicating with the Syslog server.
   - Port
   - Format - Select BSD.
   - Facility - Keep the default, LOG_USER.



5. Click OK.
   A new Syslog server profile is created.

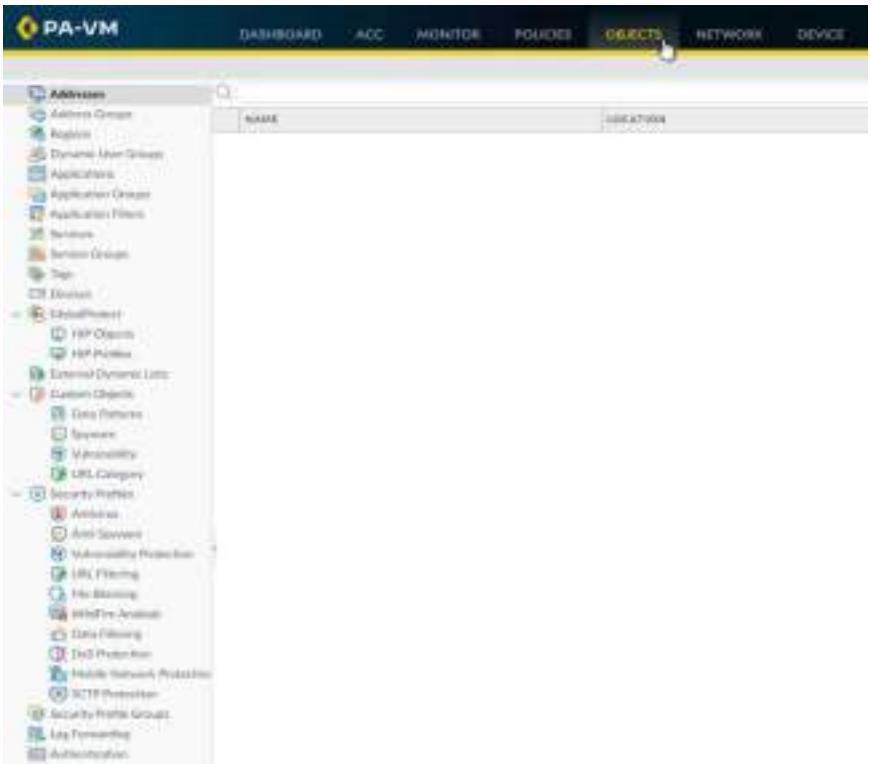
Configuring the Log Forwarding Profile

After creating a Syslog server profile, configure a log forwarding profile, as required by the Palo Alto Web Filtering configuration process.

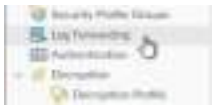
Note: If you have already configured a log-forwarding profile, and need to configure an additional profile, for more information, see Adding a Syslog Server to an Existing Log Forwarding Profile.

1. From the Palo Alto main window, select the Objects tab.

The Objects window is displayed.



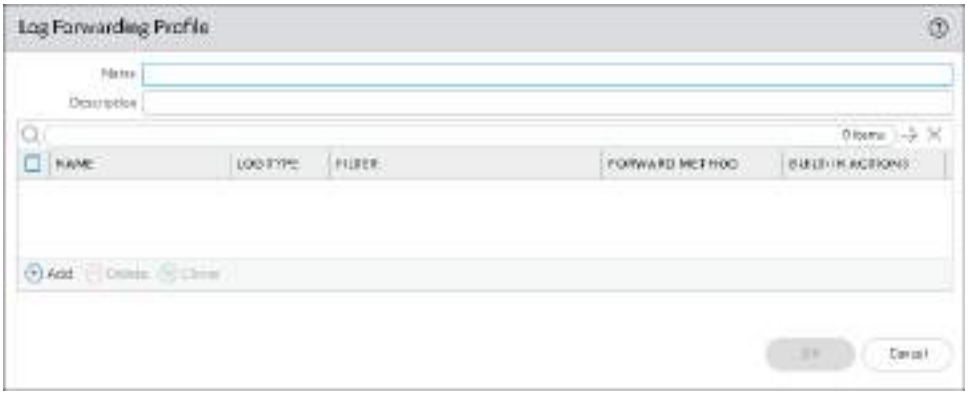
2. From the navigation pane on the left, select Log Forwarding.



3. Click Add (at the bottom).

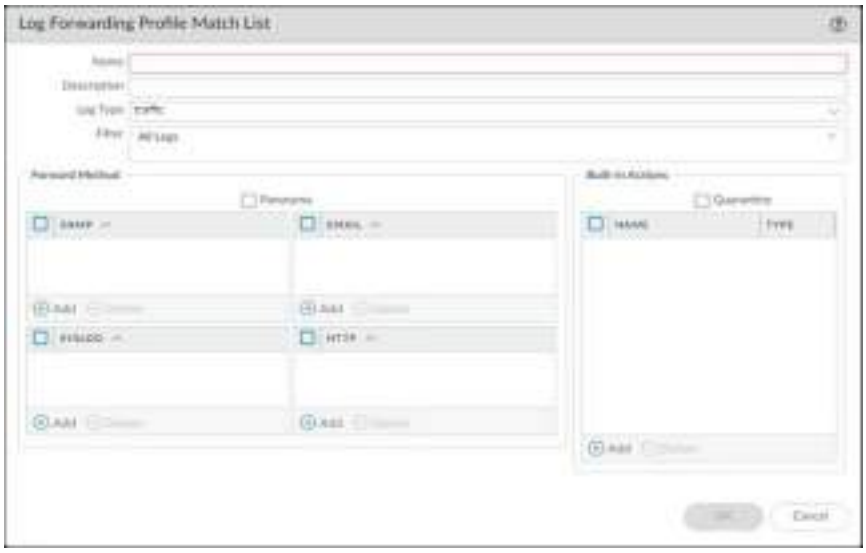


The Log Forwarding Profile dialog box is displayed.

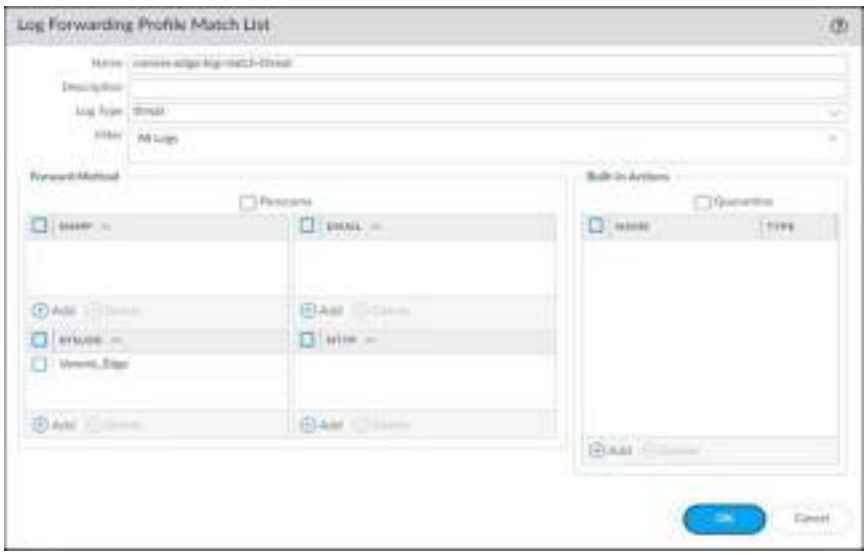


4. Click Add.

The Log Forwarding Profile Match List dialog box is displayed.

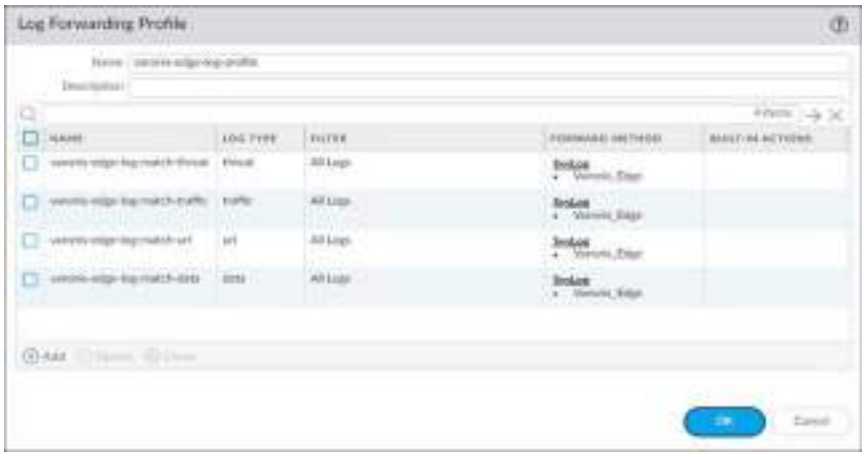


5. In the Name field, enter a name, for example varonis-log-profile.
6. Add a match list profile for each of the following log types: threat, traffic, URL, and data. For each match list profile, do the following:
   a. Click Add.
   b. In the Name field, specify a name, such as varonis-log-match-threat.
   c. In the Log Type field, select the log type.
   d. Add the Syslog server profile created above to the Syslog section.
   e. Click OK.



7. Click OK.

The profiles are displayed in the Log Forwarding Profile dialog box.



8. Click OK.

Adding a Syslog Server to an Existing Log Forwarding Profile

After configuring a log forwarding profile and performing all previous relevant procedures, it is possible to add an additional Syslog server under the existing profile.

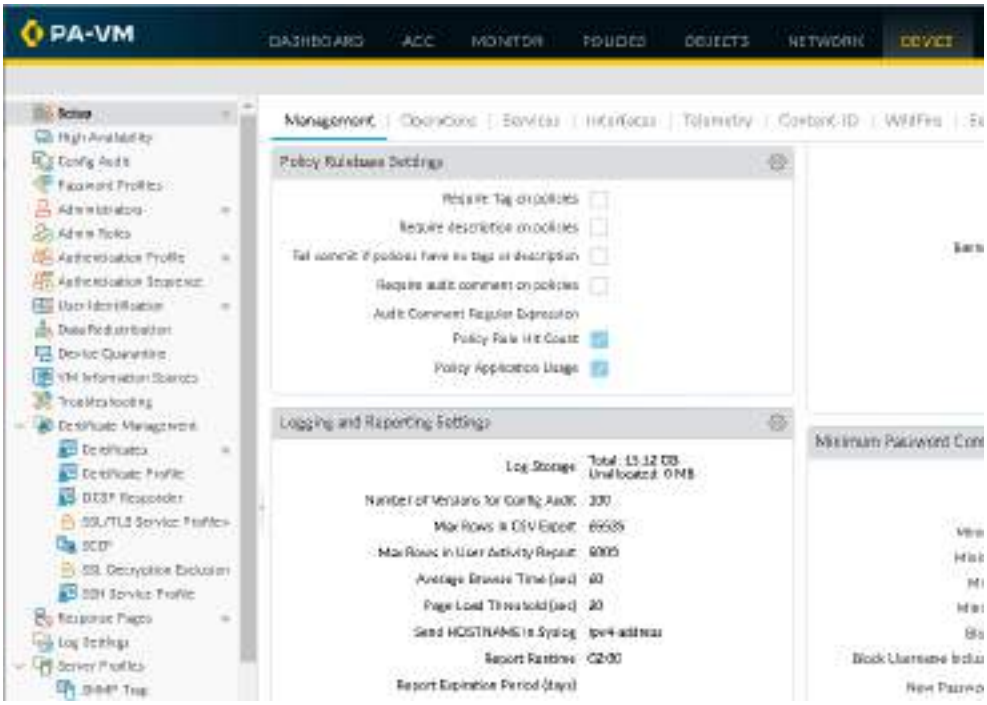
To add a Syslog Server to an existing log forwarding profile:

1. From the Palo Alto main window, select the Objects tab.
   The Objects window is displayed.
2. From the navigation pane on the left, select Log Forwarding.
   The Log Forwarding window is displayed.
3. From the Name column, click the existing log forwarding profile.
   The Log Forwarding Profile dialog box is displayed.
4. In the Name column, click the object's name.
   The Log Forwarding Profile Match List dialog box is displayed.
5. In the Syslog area, click Add, and select the new Syslog profile.
6. Click OK, and repeat for all the objects in the Name column in the Log Forwarding Profile dialog box.
7. Click OK when done.
   The new profile is displayed in the Forward Method column in the Log Forwarding Profile dialog box.
8. Click OK, and from the top right of the window, click Commit.
   The new profile is displayed in the Objects tab.

Configuring the Header Format of Syslog Messages

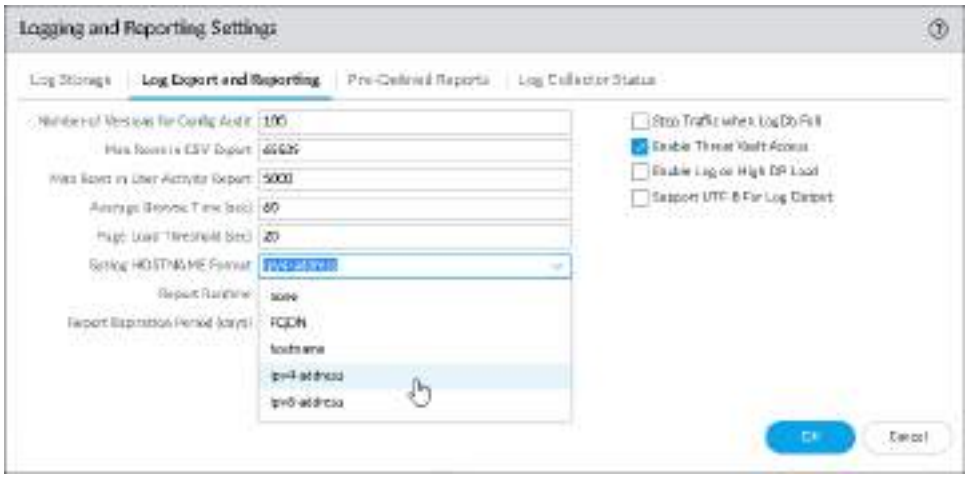
After configuring the log forwarding profile, it is important to configure the header format of Syslog messages.

1. Select the Device tab.
   The Device window is displayed.
2. From the navigation pane on the left, select Setup.
3. Select the Management tab.



4. In the Logging and Reporting Settings area, click the edit wheel on the upper right.
   The area is displayed in edit mode.
5. Select the Log Export and Reporting Settings tab.

6. In the Syslog HOSTNAME Format field, select ipv4-address or FQDN.



7. Click OK.
   The Logging and Reporting Settings area is updated.



Adding Content Types to the Log

After configuring the header format of Syslog messages, it is necessary add the content types to the log.

1. From the Palo Alto main window, select the Device tab.
   The Device window is displayed.
2. From the navigation pane on the left, select Setup.
3. In the Device window, select the Content-ID tab.
4. In the Content-ID Features area, click Container Pages.
   The Container Pages dialog box is displayed.
5. Click Add (at the bottom).
   The Custom URL Content Type dialog box is displayed.

6. Make sure all content types from the default location exist in the container.
7. Click Add and add the following URL content types:
   - application/
   - application/octet-stream



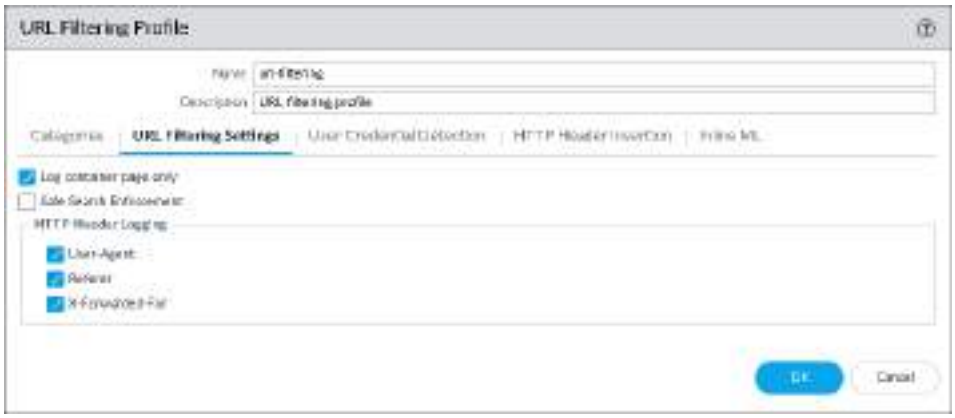
8. Click OK, and then click Close.

Configuring URL Filtering Profiles

After adding content types to the log, it is necessary to configure the URL filtering profiles.

1. From the Palo Alto main window, select the Objects tab.
   The Objects window is displayed.
2. From the navigation pane on the left, select Security Profiles > URL Filtering.
   The URL Filtering window is displayed.
3. Click Add.
   The URL Filtering Profile dialog box is displayed.
4. Do the following for each URL filtering profile used in your security policy:
   a. Select the URL Filtering Settings tab.

b. In HTTP Header Logging area, select all available HTTP headers.

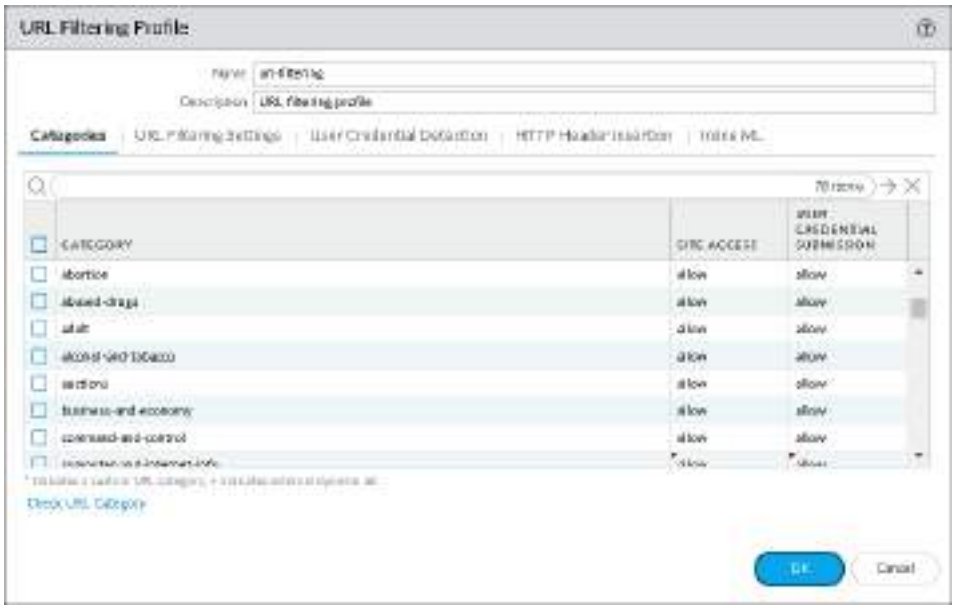


> Note: If SSL decryption is not configured, HTTP headers will not be logged for SSL requests.

c. Ensure that Log Container page only is selected.

d. Select the Categories tab.

e. Ensure that the associated URL filtering profile has all categories set to an action other than “none”.



5. Click OK.

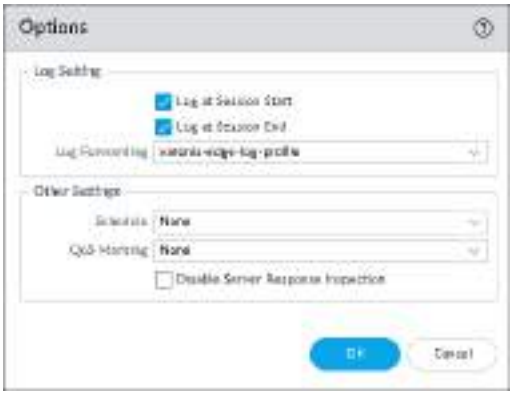
Configuring Security Policy Rules

It is important to configure rules to determine your security policy.

1. From the Palo Alto main window, select the Policies tab.
2. From the navigation pane on the left, click Security.



3. For each proxy-related security policy rule, click its cell inside the Options column. The Options dialog box is displayed.



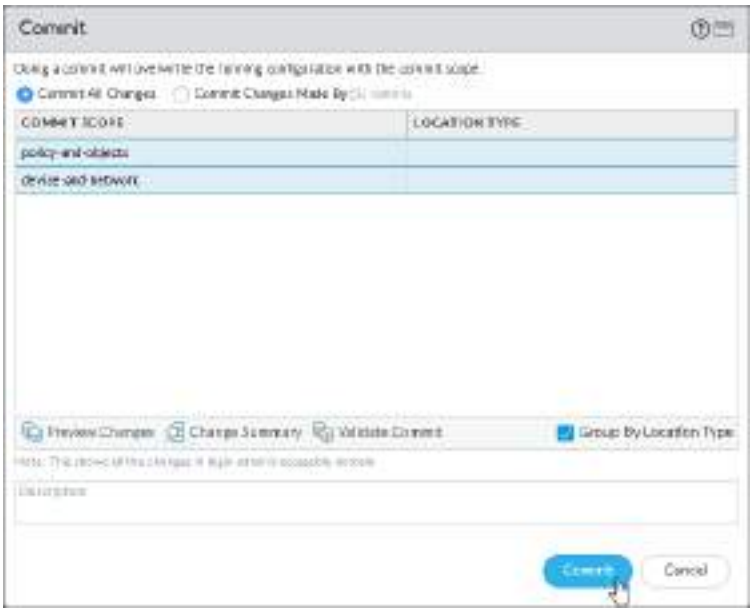
4. Select the Log at Session Start and Log at Session End checkboxes.
5. From the Log Forwarding dropdown list, select the log forwarding profile you defined previously.
6. Click OK.

Committing the Changes

After configuring Palo Alto Web Filtering and performing all the previous relevant procedures, it is necessary to commit all changes.

From of the top of the Palo Alto window, click Commit.





All changes are committed.

Cisco Firepower Threat Defense (FTD) for Proxy

Varonis supports receiving web proxy events from a Cisco Firepower Next-Generation Firewall (NGFW).
Varonis can be configured to receive Syslog messages from the Cisco ASA LINA engine that is integrated into FTD.

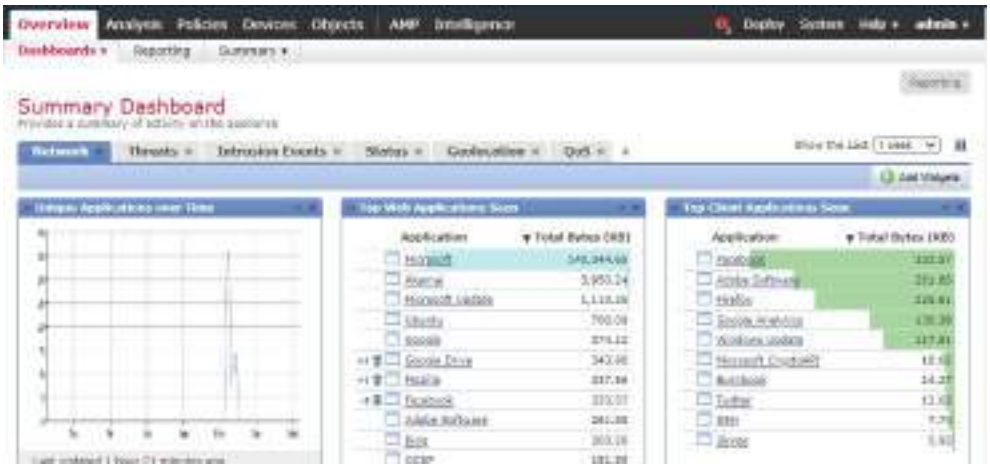
Prerequisites for Cisco Firepower Threat Defense (FTD) for Proxy

Before you begin configuring Cisco Firepower Threat Defense (FTD) to send VPN events to Varonis, you must follow several prerequisites.

- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.

Configuring Cisco Firepower FTD URL Filtering Logging

1. Open the Firepower Management Center (FMC).



2. From the FMC main window, select Devices > Platform Settings.

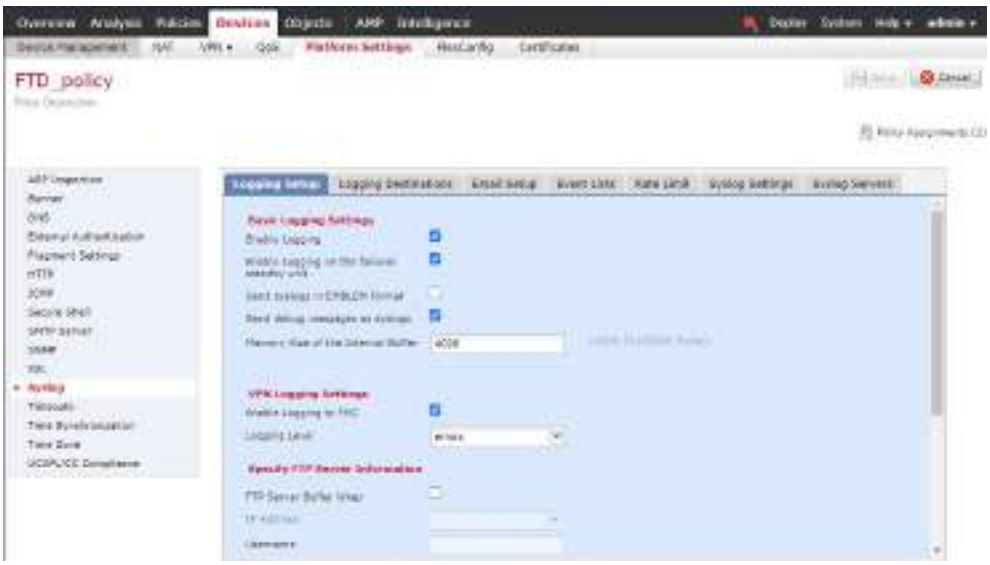


3. Select the policy related to URL filtering and click Edit.



4. From the navigation pane on the left, select Syslog.

The Logging Setup window is displayed.



5. Make sure the Enable Logging is selected.
6. Select the Event Lists tab, and click Add to create a new event list.
   The Add Event List dialog box is displayed.

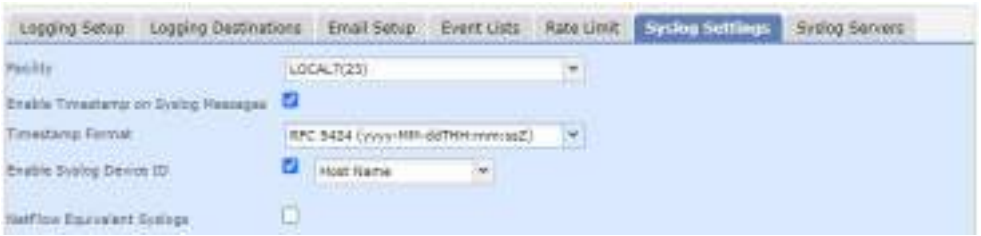


7. In the Name field, enter a name for the event list (for example, Varonis).
8. Create an event list with the following parameters and click OK:
   - Auth - Info
   - CA - Info

- Rule-engine - Info
- IDs - Info
- Session - Info
- IP - Info



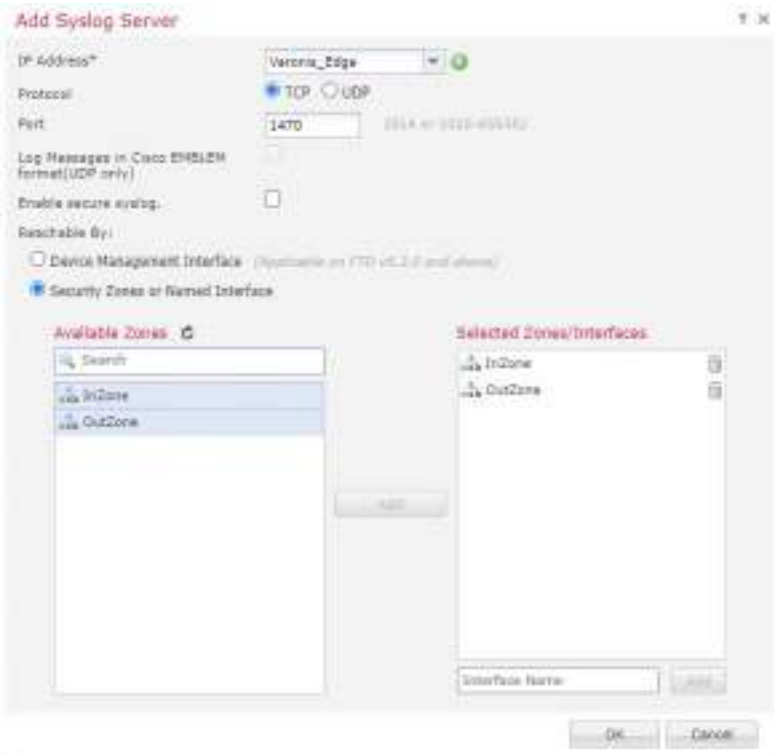
9. Select the Syslog Settings tab, and do the following:
   a. Select the Enable Timestamp on Syslog Messages checkbox.
   b. From the Timestamp Format dropdown list, select RFC 5425 as the timestamp format.
   c. Select the Enable Syslog Device ID checkbox and select Host Name from the dropdown list.



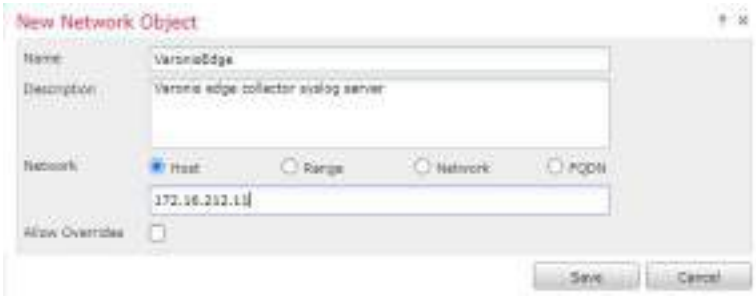
10. Select the Syslog Servers tab, and click Add.



The Add Syslog Server dialog box is displayed.



11. In the IP Address field, click the + button to add the new Syslog server. The New Network Object dialog box is displayed.



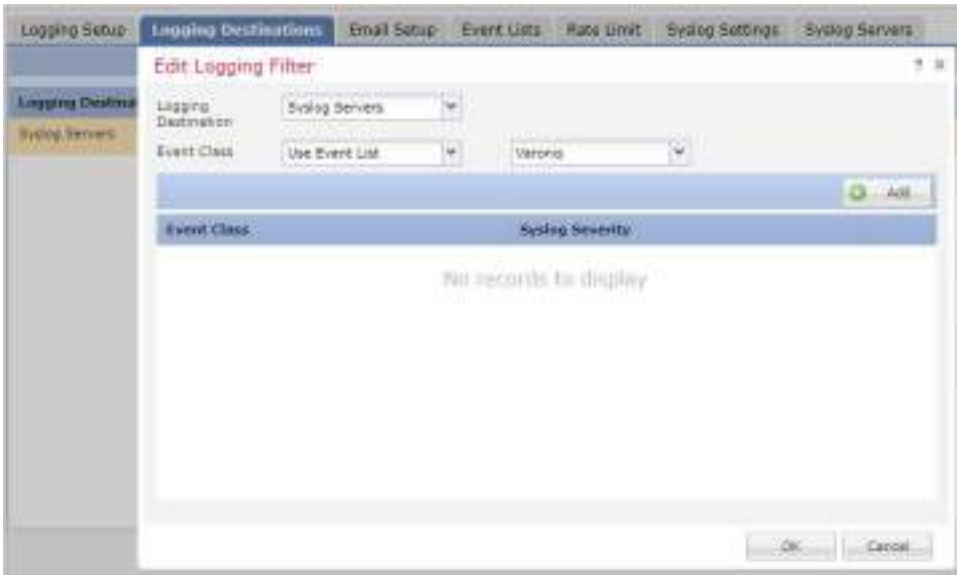
12. Enter the following:
    - Name - The name of the Syslog server.

- Description - The description of the Syslog server. (Optional)
- Network - The connection type. Select the network Host (Host 172.16.212.11 is the preferred option), Range, Network, or FQDN and fill in the relevant details.

Click Save to save the settings. Once you have added this, you can choose it from the IP Address dropdown list in the Add Syslog Server dialog box.

13. In the Add Syslog Server dialog box, do the following:
    For the following, enter the same value as configured for the network device data source in the Varonis Management Console:
    - IP Address
    - Protocol - Select UDP and use the Emblem format, or select TCP.
    - Port

    Do the following:
    - Reachable By - The interface for sending Syslog messages. Select Device Management Interface or Security Zone or Name Interface, and add the relevant Available Zones to the Selected Zones/Interface list.
14. Click OK.
15. Select the Logging Destinations tab and click Add.



16. From the Logging Destination dropdown list, select Syslog Servers.
17. From the Event Class dropdown list, select Use Event List and use the event list that was set up previously (for example, Varonis).
18. Click OK.
19. In the FTD Policy window, click Save.



20. Click Deploy (on the upper right).



21. In the Deployment tab, select the device to which to apply the changes.



22. Click the Deploy button.
    The Deployment Confirmation dialog box is displayed.



23. Click Deploy to deploy the device.

Cisco (IronPort) Web Security

Varonis supports receiving web proxy events from Cisco (IronPort) Web Security. Cisco provides information on how to send events to a third-party system such as Varonis in the User Guide for AsyncOS in the section Monitor System Activity through Logs. This document outlines the specific procedure for sending events to Varonis.

Prerequisites for Cisco (IronPort) Web Security

Before you begin configuring Cisco (IronPort) Web Security to send web proxy events to Varonis, you must follow several prerequisites.

- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.

Configuring Cisco (IronPort) Web Security

The Cisco (IronPort) Web Security configuration process requires various steps.

1. From the Cisco Web Security main window, select System Administration > Log subscriptions.
   The Log Subscriptions window is displayed.



2. Click Add Log Subscription.
   The New Log Subscription form is displayed.



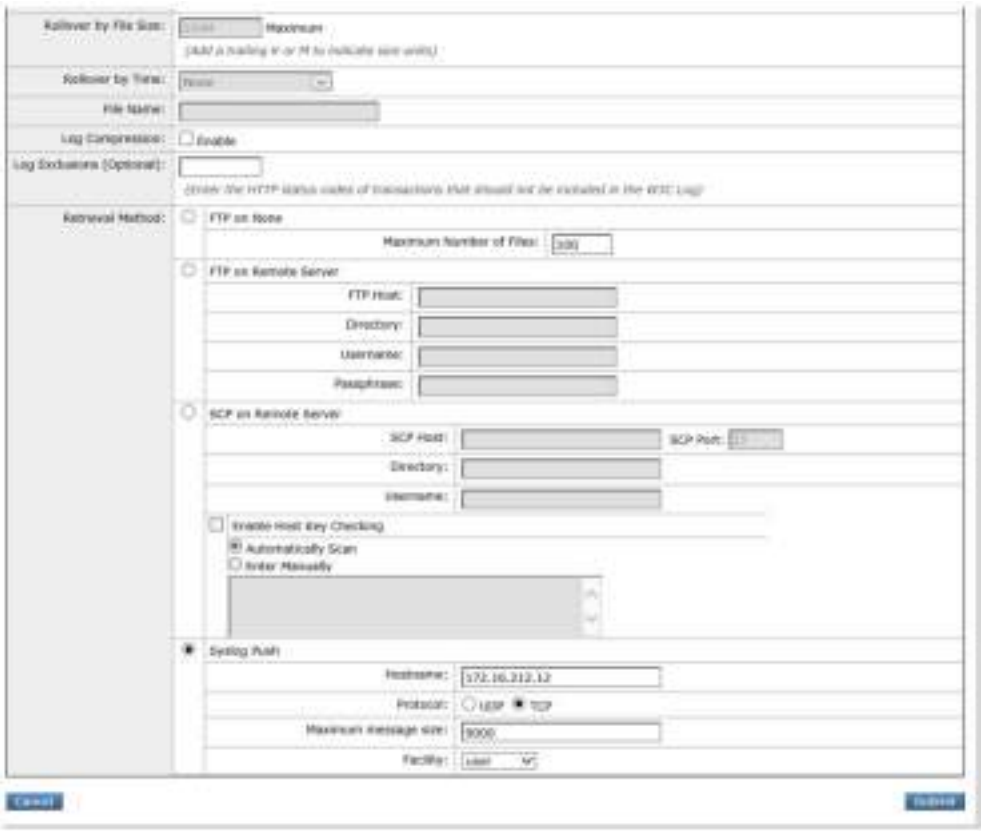
3. In the Log Fields area, add the following fields to the Selected Log Fields list, in the same order listed below:



- cs(Referer)
- c-ip
- cs-username
- cs-mime-type
- sc-http-status
- s-ip
- user-type

- cs-version
- cs-bytes
- sc-bytes
- cs(User-Agent)
- date
- time
- sc-result-code
- sc-result-code-denial
- cs-method
- cs-url

4. In the Retrieval Method area, select Syslog Push, and enter the following:
   - Hostname - The IP address or hostname of the computer hosting the Varonis connector configured for the network device data source in the Management Console. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.
   - Protocol - The protocol as configured for the network device data source in the Management Console. Note that the Cisco Web Security can only use port 514.
   - Maximum Message Size - 9000.
   - Facility - User.



5. Click Submit.

Cisco Umbrella Proxy

Varonis supports receiving proxy events from Cisco Umbrella.

This document describes how to configure Cisco Umbrella to send logs to Amazon Simple Storage Service (Amazon S3) bucket and how to set up Varonis to get the logs from AWS.

Varonis supports the following options:

- Company-managed Amazon S3 bucket
- Cisco-managed Amazon S3 bucket

Prerequisites for Cisco Umbrella Proxy

Before you begin configuring Cisco Umbrella to send proxy events to Varonis, you must follow several prerequisites.

- Ensure network connectivity between the network device Collector to the AWS site - for example: https://*.amazonaws.com.

Enable Logging to a Company-Managed Amazon S3 Bucket

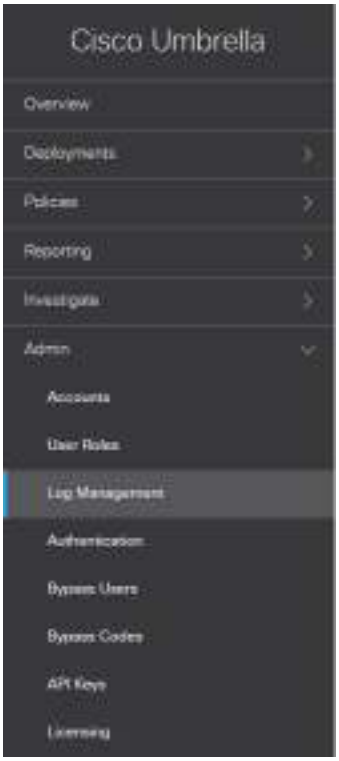
This procedure is relevant for companies that have an AWS account and want to manage their Cisco Umbrella logs under their account.

To enable logging to a company-managed Amazon S3 bucket:

1. Go to Cisco Umbrella login page.
2. Enter the credentials and click Log in.



3. In the Cisco Umbrella main window, from the navigation pane, select Admin > Log Management.



4. Select Use your company-managed Amazon S3 bucket.



5. Enter the Amazon S3 bucket name and click Verify.
   If everything is configured correctly, the following message is displayed.



6. Download the `README_FROM_UMBRELLA.txt` file from your bucket.



7. Copy the security token from the TXT file.



8. Paste the token into the token number field and click Save.



A message is displayed, confirming that the logs are sent to your Amazon S3 storage.



Enable Logging to a Cisco-Managed Amazon S3 Bucket

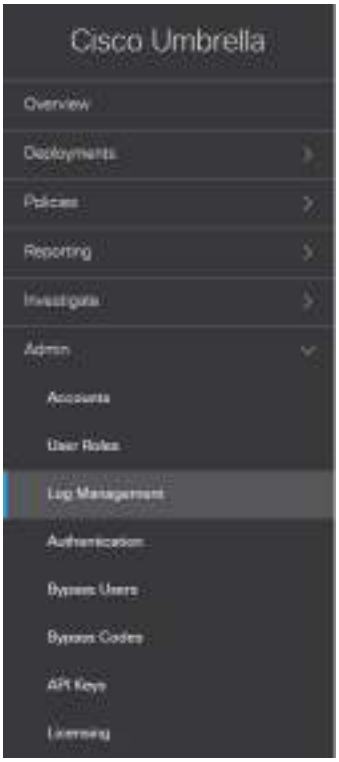
This procedure is relevant for companies that do not have an AWS account or do not want to manage Cisco Umbrella logs under their AWS account.

To enable logging to a Cisco-managed Amazon S3 bucket:

1. Go to Cisco Umbrella login page.
2. Enter the credentials and click Log in.



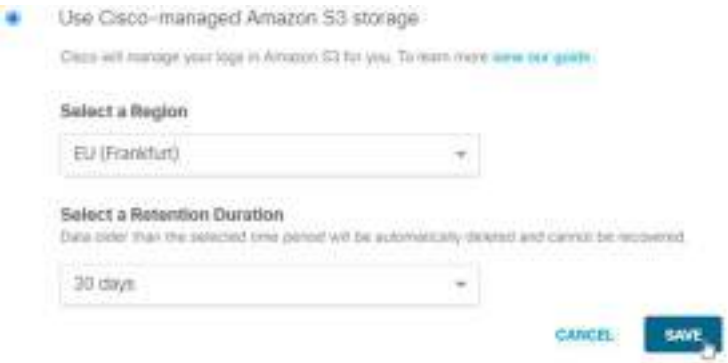
3. In the Cisco Umbrella main window, from the navigation pane, select Admin > Log Management.



4. Select Use Cisco-managed Amazon S3 storage.



5. Select the AWS region (for example, EU Frankfurt) and the desired retention duration for log files (for example, 30 days). Click Save to confirm.



6. Click Continue to proceed.



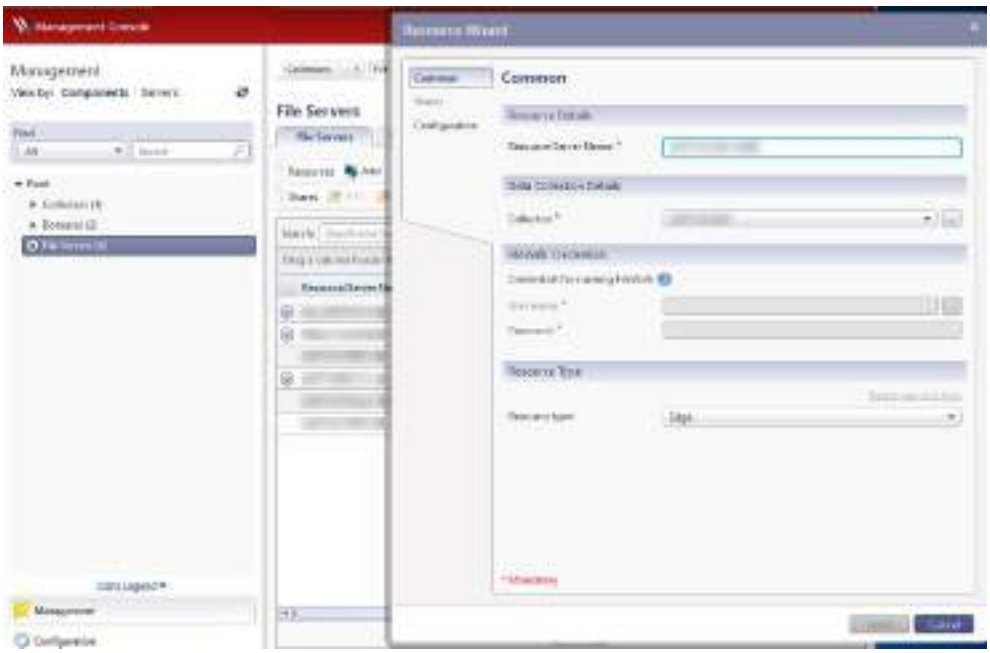
7. When activation is complete, a window is displayed, showing the credentials (Data Path, Access Key, and Secret Key). Store this information in a safe place, and then click Continue to proceed.



Configuring a Network Device Data Resource when Working with Cisco Umbrella

1. In the Management Console, from the menu in the left pane, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.

The Resource Wizard is opened to the Common pane, where you can specify the data source and set the relevant parameters.



2. In the Common pane, set the following parameters:
   a. Resource Details - Specify the data source name.
   b. Data Collection Details - Select a Collector that is configured to support network devices.
   c. Resource Type - Select Edge from the dropdown list. (The FileWalk Credentials will be disabled.)
3. On the left menu, click Configuration.
4. In the Source Device area, set the following parameters:
   - Product - Select Cisco Umbrella - Proxy.
   - Time Zone - Select UTC+0.
   - User Repository - Select the user repository with which to match user names in the events (leave the default if your installation contains only a single domain). For example, Active Directory.
   - Default Date & Time Format - Select to auto-detect the date and time format used in the logs of the monitored sources (Proxy). If the auto-detection fails, a notification is sent.

> Note: When Varonis proxy parsers based on splits is enabled (feature toggle EdgeSplitFilters=ON), auto-detection of the date and time format will not work. Only predefined default or custom dates can be used in this case.

- Custom Date & Time Format - Define the vendor's date and time format to avoid possible date format problems with Varonis servers. For information about the date and time format, see Date and Time Format Notation.

5. In the Interface Configuration area, specify the interface that Varonis will use to collect events from the source device. Options include AWS_SE or Splunk.
   To configure AWS_S3 as the interface:
   - Select an Interface - Select AWS_S3.
   - If you are working with a company-managed Amazon S3 bucket, set the following parameters:
     - Bucket - Enter the name of the Amazon S3 bucket.
     - Prefix - Leave this empty.
   - If you are using a Cisco-managed bucket, set the following parameters:
     - Bucket - Enter the name of the Cisco-managed bucket.
     - Prefix - Enter the data path within the Cisco-managed bucket (use the automatically generated data path saved from step 6 in Enable Logging to a Company-Managed Amazon S3 Bucket).
   - Access Key ID - Enter the access key ID.
   - Secret Access Key - Enter the secret access key.
   - Region - Select the bucket region.

   To configure Splunk as the interface:

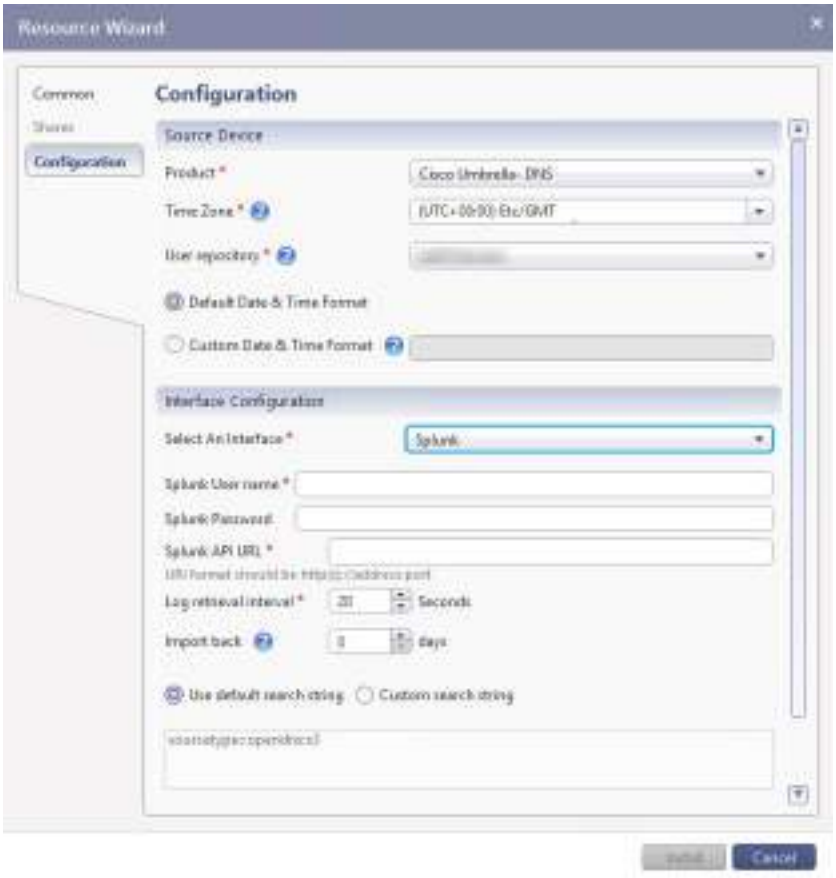
   For more information, click here. Note that Splunk does not recommend connecting third-party applications such as Varonis to Splunk Free. Since Splunk Free does not support authentication, providing such access exposes Splunk to anyone.

   a. Select an Interface - Select Splunk.
   b. Splunk User Name - Enter the Splunk API user name.
   c. Splunk Password - Enter the Splunk API password.
   d. Splunk API URL - The format is http://<host>:<port> or https://<host>:<port> where <host> is the IP address or host name of the Splunk server and <port> is the port configured in Splunk for the API. The default Splunk port is 8089 and must be specified.
   e. Log retrieval interval - Specify the interval for retrieving Splunk event logs. The default is 20 seconds. The maximum allowed is 60 seconds.

f. Import back__days - Imports past events from Splunk for network device sources which support importing real-time events. It is possible to select up to 30 days back.

g. Use default search string - Enables you to keep the provided default string (displayed at the bottom). The default search string is useful if using the standard Splunk App provided by the device to collect events.

h. Custom search string - Enables you to modify the default search string. Ensure the _raw field is returned in the search results. Test the custom search string on your Splunk Enterprise console.



Once you've configured the interface settings, the next step is to test whether the connection is working.

6. Click Test Connection. (You may need to scroll down to the bottom of the Interface Configuration area to see this button).



A message is displayed, confirming that the test connection succeeded.



If the test connection failed, see Troubleshooting SSL Certificate Issues when Using Cisco Umbrella Proxy.

7. After configuration is complete, click Install to install the data source.
   A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the File Servers pane. When the installation completes, the status shows "Installed 100%".

Troubleshooting SSL Certificate Issues when Using Cisco Umbrella Proxy

In some setups, there is no direct connectivity between the network device Collector and public Internet. If you are running SSL decryption on your network devices such as a next-generation firewall (NGFW) and presenting your own self-signed or untrusted SSL certificate, you might need to add the SSL decryption exclusion to avoid SSL certificate verification failure.

Using AWS CLI Tools for SSL Certificate Verification

To verify an SSL certificate:

1. Download and install AWS CLI tools on your Collector from https://aws.amazon.com/cli/.
2. Run the following commands on the Collector machine:

```
set AWS_ACCESS_KEY_ID=<your_access_key>
set AWS_SECRET_ACCESS_KEY=<your_secret_key>
set AWS_DEFAULT_REGION=<aws_region_for_your_s3_bucket>
```

```
aws s3 sync s3://<s3_bucket_name> . stxmsrep tvi 1 livi .
hrwpskw
```

3. For example, a bucket named varonis-test and eu-central-1 (Frankfurt) AWS region: `C:\varonis>aws s3 sync s3://varonis-test/dnslogs/`:

```
fatal error: SSL validation failed for lxxtw%..zevsrmw xi
wx#w7#iy girxvep 5#eqe3sre0w#gsq.↗pmwx x2ti 6 tvi 1 hrwps
kw 6H irgshmrk x2ti yvp [SSL: CERTIFICATE_VERIFY_FAILED]
givxm gexi verify failed: self signed givxm gexi in certif
icate chain (_ssl.c:1125)
```

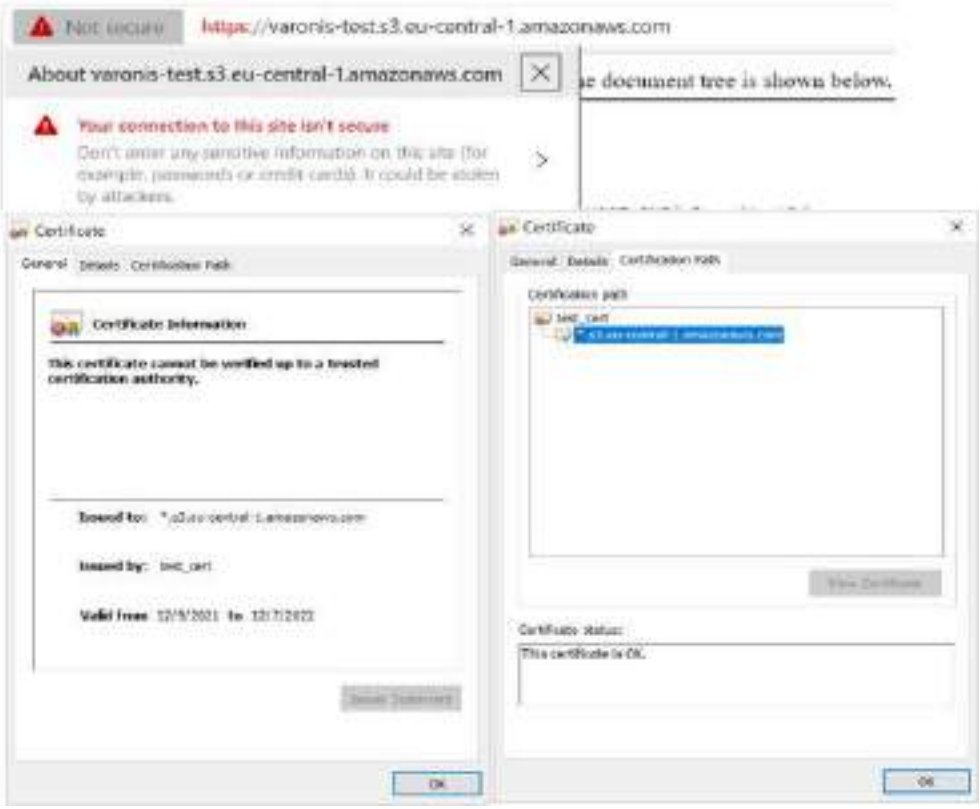
   In this case, you need to add SSL decryption exclusion for https://varonis-test.s3.eu-central-1.amazonaws.com (it can also be a wildcard for *.s3.eu-central-1.amazonaws.com or even *.amazonaws.com). For more information, see the documentation for your NGFW vendor for instructions on configuring SSL decryption exclusion.

Using the Web Browser for SSL Certificate Verification

You can also use the web browser running on the Collector machine to check the SSL certificate.
To use the web browser to verify the SSL certificate:

1. Go to https://<s3_bucket_name>.s3.<aws_region>.amazonaws.com.
2. For example, for a bucket named varonis-test and eu-central-1 (Frankfurt) AWS region, you need to go to https://varonis-test.s3.eu-central-1.amazonaws.com and check the SSL certificate.

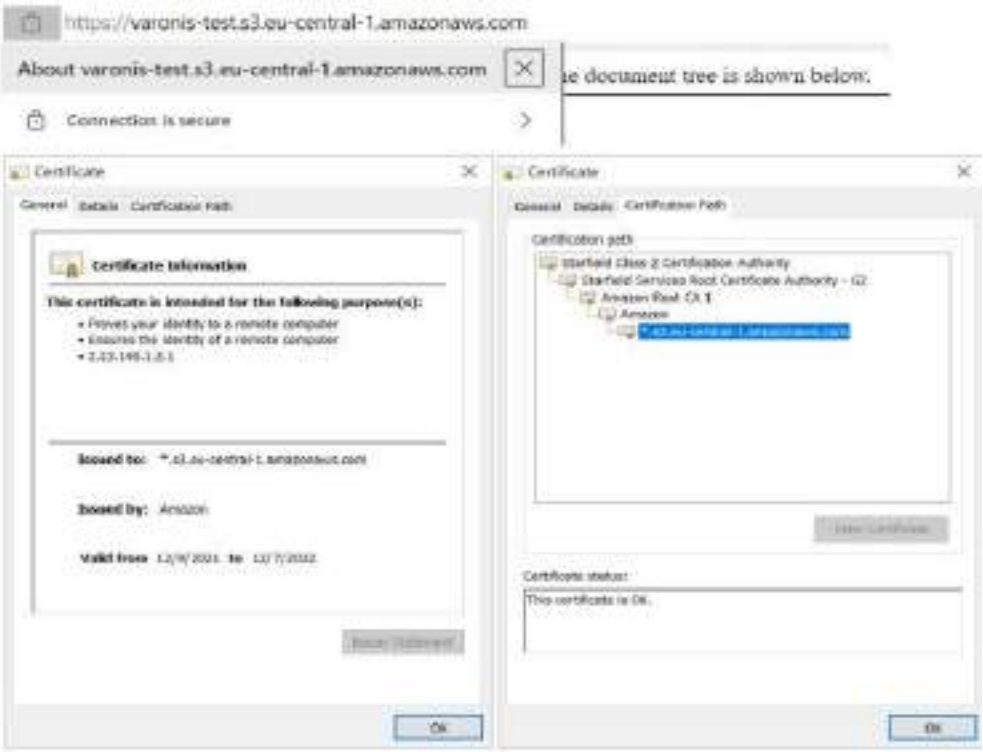
Before adding SSL decryption exclusion :



The connection is not secure, an untrusted SSL certificate was issued by test_cert, and the certification path is incomplete.

In this case, you need to add SSL decryption exclusion for https://varonis-test.s3.eu-central-1.amazonaws.com (it can also be a wildcard for *.s3.eu-central-1.amazonaws.com or even *.amazonaws.com). For more information, see the documentation for your NGFW vendor for instructions on configuring SSL decryption exclusion.

After adding SSL decryption exclusion:



The connection is secure, a trusted SSL certificate is issued by Amazon, and the full certification path is available.

Squid Proxy

Varonis supports receiving web proxy events from a Squid Proxy.
The Squid Software Foundation provides information on how to send events to a third-party system such as Varonis in the Feature: Log Modules for Squid wiki article. This document outlines the specific procedure for sending events to Varonis.

Prerequisites for Squid Proxy

Before you begin configuring the Squid Proxy to send web proxy events to Varonis, you must follow several prerequisites.

- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.

Configuring the Squid Proxy

The Squid Proxy configuration process requires various steps.

To configure the Squid Proxy:

1. Edit your Squid Proxy configuration file. The location and name of the file is specific to your deployment. It is commonly named `squid.conf` and located:
   - On Linux, under `/etc/squid` or `/usr/local/squid/etc`.
   - On Windows, in the `etc` folder under the Squid program directory.
     In Windows, you can right-click the Squid Proxy tray icon, and select Open squid configuration.
2. Add the following lines to the configuration file to define the configuration format. Make sure each line is copied as a single line and that there is a space between the parts displayed below, and that they are on separate lines.

   ```
   logformat varonis-combined %>a %[un  %[un [%tl] "%rm %ru
   HTTP/%rv" %>Hs %>st %<st "%{Referer}>h" "%{User-Agent}>h
   " %Ss:%Sh %mt %<tt
   ```

3. Add the following line to the configuration file, and set the parameters:

   ```
   access_log <protocol>://<host>:<port> combined
   ```

   For example:

   ```
   access_log tcp://172.0.0.0:568 varonis-combined
   ```

   Enter the following:
   - `<protocol>`
   - `<host>`
   - `<port>` - Enter the same value as configured for the network device data source in the Varonis Management Console.
4. Add the following lines to the configuration file, in the specified order, to connect the Squid Proxy to an LDAP directory to retrieve the user name ("xxx" below are placeholders):
   After this line:

   ```
   #
   # INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR
   CLIENTS
   #
   ```

Add the following lines:

```
auth_param basic program C:\Squid\lib\squid\basic_ldap_au
th.exe -R -b "dc=xxx,dc=xxx" -h hub-dc -D CN=xxx,CN=xxx,D
C=xxx,DC=xxx  -w passwordxxx -f (sAMAccountName=%s)
auth_param basic children 5
auth_param basic realm Web-Proxy
auth_param basic credentialsttl 1 minute
acl ldap-auth proxy_auth REQUIRED
http_access allow ldap-auth
http_access deny all
```

Note: For more information about setting the domain authentication, see http://www.squid-cache.org/Versions/v3/3.2/manuals/basic_ldap_auth.html

5. Save the configuration file.
6. Restart the Squid Proxy service:
   - On Linux, run `./squid -k vigsr kyvi` from the Squid installation directory.
   - On Windows, right-click the Squid Proxy tray icon and select Stop Squid Service, and then select Start Squid Service.

Apache Proxy

Varonis supports receiving web proxy events from an Apache Proxy.
The Apache Software Foundation provides information on how to send events to a third-party system such as Varonis in the Apache Module mod_proxy article. This article outlines the specific procedure for sending events to Varonis.

Prerequisites for Apache Proxy

Before you begin configuring the Apache Proxy to send web proxy events to Varonis, you must follow several prerequisites.

- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.

Configuring the Apache Proxy

The Apache Proxy configuration process requires various steps.

Note: Apache 2.4 does not support sending logs via the network, therefore, you need to use NXLog (a third-party tool) to send logs to Varonis, using Syslog protocol.

Varonis supports a combined log format. When configuring the Apache Proxy, ensure that you copy the strings of the log format correctly.

To configure the Apache Proxy:

1. Log in to the Apache server.
2. Go to the path: `{Apache installation path}\conf\httpd.conf`, and open the `httpd.conf` file.
3. In the `httpd.conf` file, go to the following line and uncomment it:

```
#CustomLog "logs/access.log" combined
```

4. Make sure that the `httpd.conf` file contains a section similar to the following:

```
<IfModule psk gsr k qshypi
    #
    # The following directives hi ri some format nickname
s for use with
    # a CustomLog directive (see below).
    #
    LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\"
\"%{User-Agent}i\"" combined
    LogFormat "%h %l %u %t \"%r\" %>s %b" common

    <IfModule logio_module>
      # You need to enable mod_logio.c to use %I and %O
      LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\
" \"%{User-Agent}i\" %I %O" combinedio
     LjPshypi

    #
    # The location and format of the access psk pi (Commo
n Osk pi Format).
```

```
    # If you do not hi ri any access psk piw within a <Vi
rtualHost>
    # container, they will be logged here.  Contrariwise
, if you *do*
    # hi ri per-<VirtualHost> access psk piw$ transaction
s will be
    # logged therein and *not* in this  pi#
    #
    CustomLog "logs/access.log" common

    #
    # If you prefer a psk pi with access, agent, and refe
rer information
    # (Combined Osk pi Format) you can use the following
directive.
    #
    CustomLog "logs/access.log" combined
 LjPshypi
```

5. Make sure that the following lines are present and are NOT commented out:

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{
User-Agent}i\"" combined
CustomLog "logs/access.log" common
```

6. For more information, see Log Files - Apache HTTP Server Version 2.4.

Configuring AD Authentication

After configuring the log format, you can configure AD authentication which is required for displaying the user name in the event log.

1. Add the following lines to the proxy configuration located in the `httpd.conf` file:

```
<Proxy *>
    AuthName "AD authentication"
    AuthBasicProvider ldap
    AuthType Basic
```

```
    LDAPReferrals Off
    AuthLDAPURL ldap://{domain controller url}:389/{grou
p distinguished name}?cn
    AuthLDAPBindDN {apache AD user distinguished name}
    AuthLDAPBindPassword {apache AD user password}
    Require valid-user
 Svs12
```

2. In `AuthLDAPURL` in the `httpd.conf` file shown above, replace `domain controller url` with the relevant Domain Controller server URL, and `group distinguished name` with the relevant Domain Name (DN) of an AD group with which to authenticate the user.
   For example:

```
    AuthLDAPURL ldap://172.16.212.11:389/CN=Users,DC=LH33
4,DC=com?cn
```

3. In `AuthLDAPBindDN` in the `httpd.conf` file shown above, replace the `apache AD user distinguished name` with the relevant Domain Name (DN) of an account for Apache to use for AD connection.
   For example:

```
AuthLDAPBindDN CN=Administrator,CN=Users,DC=LH334,DC=com
```

4. In `AuthLDAPBindPassword` in the `httpd.conf` file shown above, replace `apache AD user password` with the relevant password of an account for Apache to use for AD connection.
   For example:

```
AuthLDAPBindPassword "mypassword"
```

Committing the Changes

After configuring the Apache Proxy and performing all the previous relevant procedures, it is necessary to commit all changes.

Go to the path: `{Apache installation path}\bin`, and run `httpd.exe`.

Zscaler Proxy

Varonis supports receiving web proxy events from Zscaler Internet Access (ZIA). ZIA generates such events using Nanolog Streaming Service (NSS).

Zscaler provides information on how to send events to a third-party system such as Varonis on their documentation site, see NSS Deployment Guides and Adding NSS Feeds for Web Logs.

Prerequisites for Zscaler Proxy

Before you begin configuring the Zscaler Proxy to send web proxy events to Varonis, you must follow several prerequisites.

- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.
- Zscaler Proxy supports only TCP, so select TCP when configuring the Syslog interface protocol.
- Make sure to deploy the Nanolog Streaming Service (NSS) to be able to stream traffic logs in real time to Varonis.

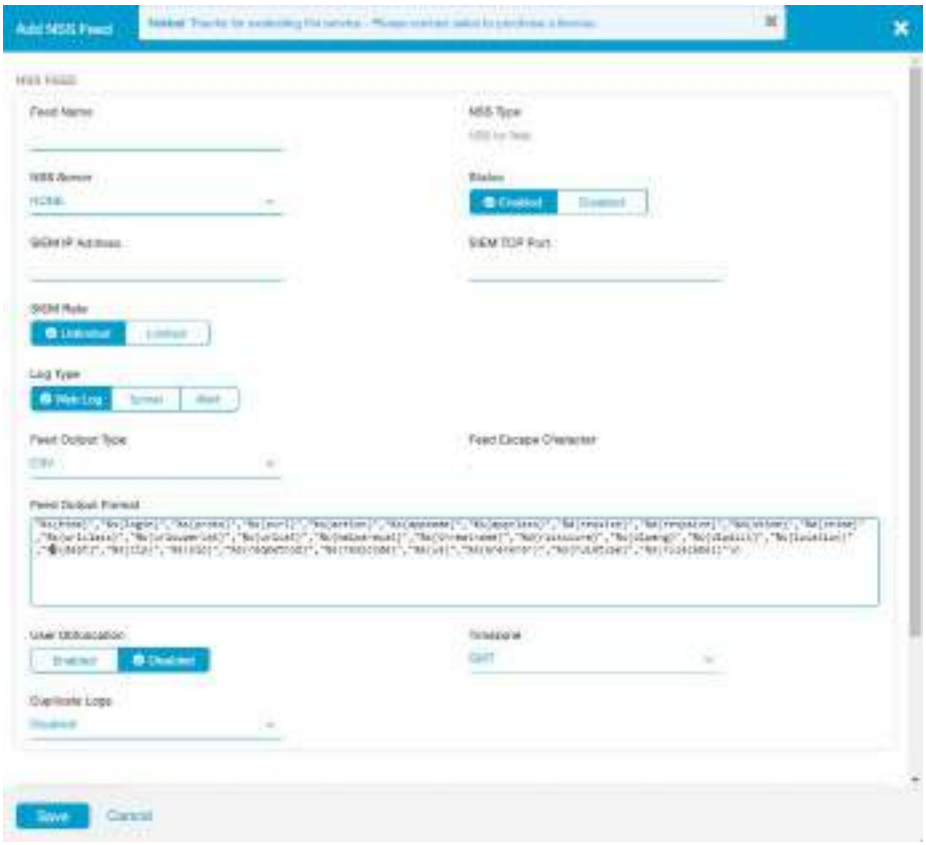
Configuring the Zscaler Proxy

The Zscaler Proxy configuration process requires various steps.

1. Log in to Zscaler with the relevant credentials.
2. From the Zscaler main window, go to Administration > Settings > Nanolog Streaming Service.



3. Make sure you have an NSS server configured. The server type must be an NSS for the Web.
4. From the NSS Feeds tab, click Add NSS Feed and configure the following parameters to add a dedicated NSS feed for Varonis:



- Feed Name - Enter the name of the feed. The feed is a connection between the NSS and Varonis.
- NSS Server - Select the NSS for the Web server.
- SIEM IP Address - The IP address of the Varonis machine in which the network device Logstash is enabled. This can be in the network device Collector or server.

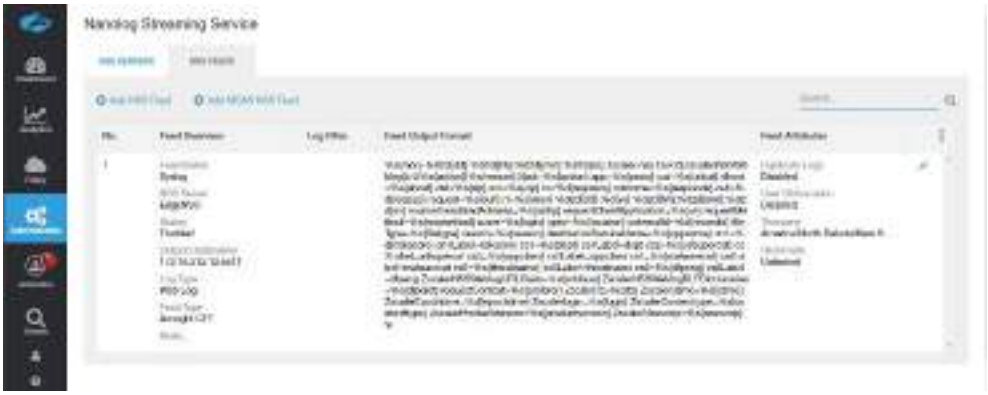
  Note: To verify where Logstash is enabled, go to the Management Console.

- SIEM TCP Port - Enter the port number of the Logstash port to which the logs are streamed.
- SIEM Rate - Select Unlimited (default).
- Log Type - Select Web Log (default).
- Feed Output Type - Select Arcsight CEF.
- Feed Output Format - Use the following format for the Varonis feed output:

```
%s{mon} %02d{dd} %02d{hh}:%02d{mm}:%02d{ss} zscaler-ns
s CEF:0|Zscaler|NSSWeblog|5.0|%s{action}|%s{reason}|3|a
```

```
ct=%s{action} app=%s{proto} cat=%s{urlcat} dhost=%s{eho
st} dst=%s{sip} src=%s{cip} in=%d{respsize} outcome=%s{
respcode} out=%d{reqsize} request=%s{eurl} rt=%s{mon} %
02d{dd} %d{yy} %02d{hh}:%02d{mm}:%02d{ss} sourceTransla
tedAddress=%s{cintip} requestClientApplication=%s{ua} r
equestMethod=%s{reqmethod} suser=%s{login} spriv=%s{loc
ation} externalId=%d{recordid}  piW2ti  w/ pix2ti| reas
on=%s{reason} destinationServiceName=%s{appname} cn1=%d
{riskscore} cn1Label=riskscore cs1=%s{dept} cs1Label=de
pt cs2=%s{urlsupercat} cs2Label=urlsupercat cs3=%s{appc
lass} cs3Label=appclass cs4=%s{malwarecat} cs4Label=mal
warecat cs5=%s{threatname} cs5Label=threatname cs6=%s{d
lpeng} cs6Label=dlpeng ZscalerNSSWeblogURLClass=%s{urlc
lass} ZscalerNSSWeblogDLPDictionaries=%s{dlpdict} reque
stContext=%s{ereferer} ZscalerTz=%s{tz} ZscalerStime=%d
{stime} ZscalerEpochtime=%d{epochtime} ZscalerOlogin=%s
{login} ZscalerContenttype=%s{contenttype} ZscalerProdu
ctversion=%s{productversion} ZscalerNsssvcip=%s{nsssvci
p}\n
```

- User Obfuscation - Select Disabled (default) to display the user names.
- Timezone - Update the relevant timezone to match that of the new network device data source added in the Management Console.
- Duplicate Logs - Select Disabled (default).



5. At the bottom of the NSS Feed page, click Save to save the changes, and activate them according to the instructions provided by Zscaler. For more information, see Saving and Activating Changes in the Admin Portal.

Barracuda Web Security Gateway

Varonis supports receiving web proxy events from the Barracuda Web Security Gateway.

Prerequisites for Barracuda Web Security Gateway

Before you begin configuring Barracuda Web Security Gateway to send web proxy events to Varonis, you must follow several prerequisites.

- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.
- Barracuda Web Security Gateway supports only UDP protocol.

Configuring Barracuda Web Security Gateway to Send Events to Varonis

Barracuda Web Security Gateway must be configured to send events to Varonis.

1. From the Barracuda Web Security Gateway main window, select the Advanced tab.



2. From the Advanced tab, select Syslog at the top.
   The Syslog Configuration page is displayed.



3. In the Enable W3C Logs field, click Yes.
4. In the Web Traffic Syslog area, enter the network device Collector IP, port number, and logical name for the Syslog server.
5. Click Add (on the right).

Sophos XG Proxy

Varonis supports receiving web proxy events from a Sophos XG Firewall. Sophos provides information on how to send events to a third-party system such as Varonis. For more information, click here.

Prerequisites for Sophos XG Proxy

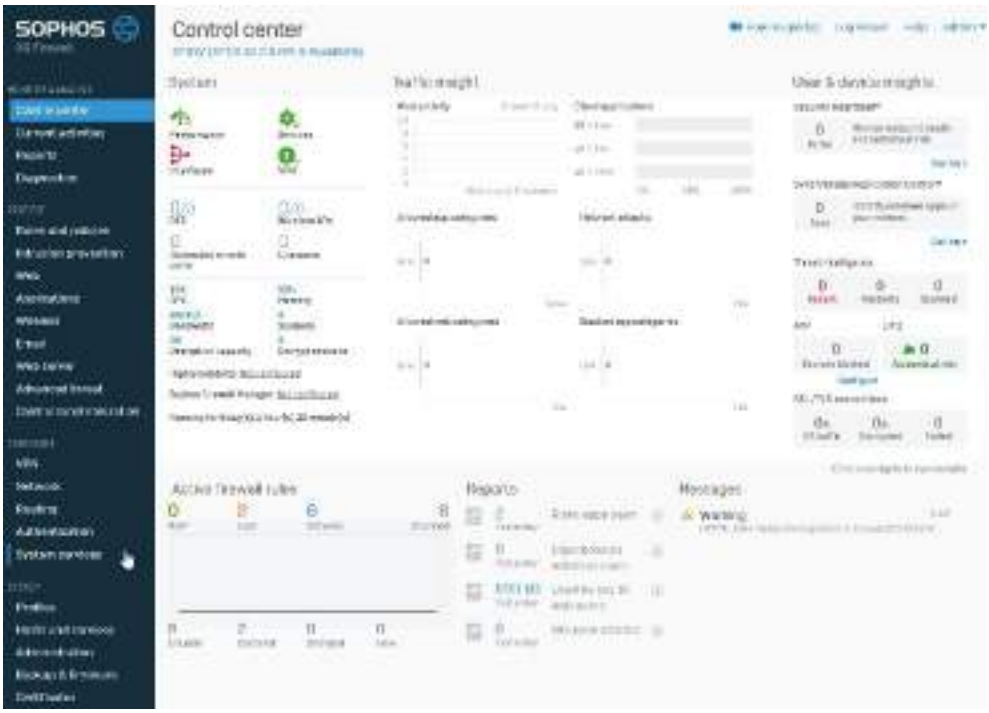
Before you begin configuring Sophos XG Firewall to send web proxy events to Varonis, you must follow several prerequisites.

- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.

Creating a Syslog Server Profile

The Sophos XG configuration process requires creating a Syslog server profile.

1. In the Sophos XG main window, from the navigation pane on the left, select Configure > System services.



2. From the menu at the top, select the Log settings tab.



3. Click Add to add a new Syslog server.



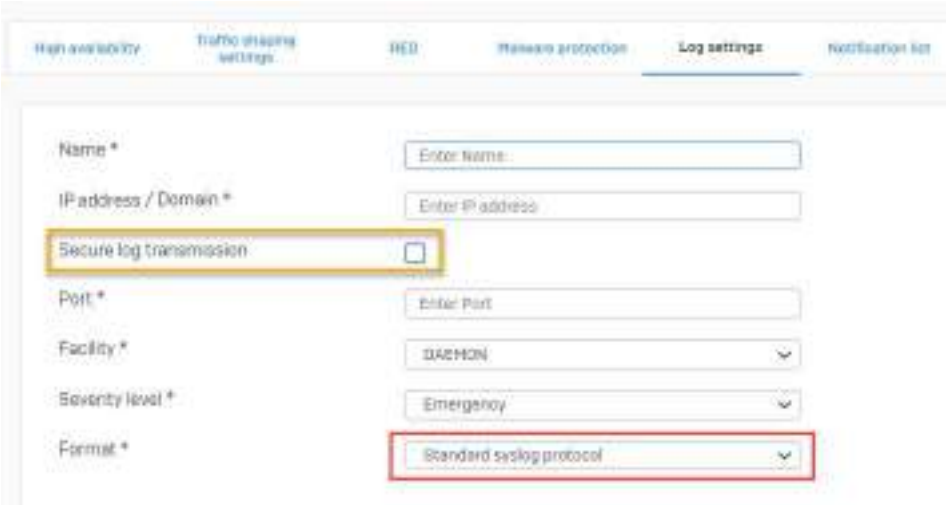
The new Syslog server window is displayed.



4. Enter the following:
   - Name - Enter any name such as Varonis or the name of the specific network device Collector used, for example Varonis NYC Collector.
   - IP address/Domain - The IP address or FQDN (for example, 192.168.57.14). For the IP address, enter the same value as configured for the network device data source in the Varonis Management Console
   - Secure log transmission - Leave the default value (cleared).
   - Port - Enter the same value as configured for the network device data source in the Varonis Management Console.

     Note: Sophos XG supports only UDP protocol.

   - Facility - Leave the default level (DAEMON).
   - Severity level - Select Information to include all informational messages.
   - Format - Select Standard syslog protocol (previously named "Central Reporting Format") which is supported by Varonis.



5. Click Save.



A new Syslog server profile is created.

Configuring Log Settings

You can configure the log settings for Sophos XG.

1. In the Sophos XG main window, from the navigation pane on the left, select Configure > System services.



2. From the menu at the top, select the Log settings tab.



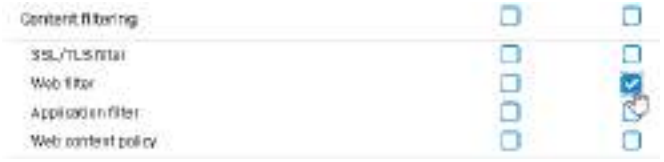
3. Make sure that you are working with the previously created profile (Varonis).



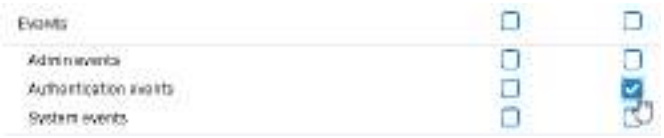
4. Select the required log categories by selecting the checkboxes:
   - For Firewall, select Firewall rules



- For Content filtering, select Web filter



- For Events, select Authentication events



5. Click Apply.



The log settings for Varonis Syslog server are applied.

6. Click OK to confirm.



Configuring DNS Sources To Send Events To Varonis

This section describes how to configure DNS Sources to send events to Varonis.

Microsoft DNS Servers

Varonis supports receiving DNS events from the supported Microsoft Windows Servers.

Prerequisites for Microsoft DNS Servers

Before you begin configuring Microsoft DNS Servers to send DNS events to Varonis, you must follow several prerequisites.

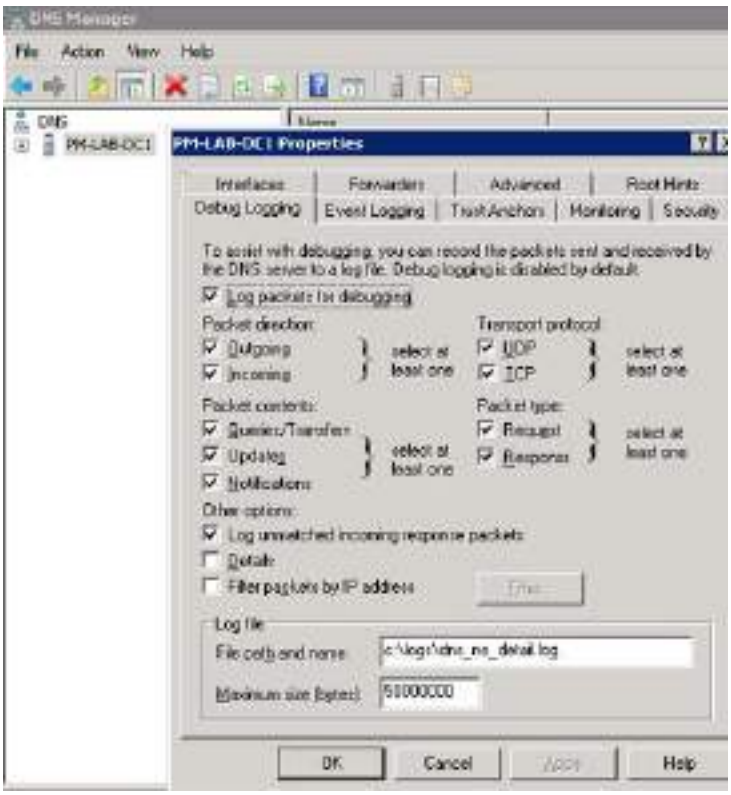
- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.

Configuring Microsoft DNS Servers to Generate Log Files

When configuring Microsoft DNS Servers to generate log files, you need to configure the DNS servers to create debug log files, and then add NXLog or Filebeat to read the log files and send the data to Varonis.

To configure the DNS servers to create debug log files:

1. Run the DNS management tool. In the elevated command prompt, type `dnsmgmt.msc`.
   For each DNS server, proceed with the following steps.
2. Select the DNS server in the navigation pane and right-click Properties.
3. Select the Debug Logging tab, and select the following:



   a. Select Log packets for debugging.
   b. In the Packet direction area, select Outgoing and Incoming.
   c. In the Transport protocol area, select UDP and TCP.
   d. In the Packet contents area, select Queries/Transfers, Updates and Notifications.
   e. In the Packet type area, select Request and Response.
   f. In Other options, select Log unmatched incoming response packets.
4. Select a file path and name in a suitable location.

   Note: The log file must be located on the Windows system drive, usually drive C.

5. Ensure the maximum size will not exhaust storage on the DNS server.

> Note: Verify that the Details checkbox is not selected. Selecting it will result in an excessive load on the domain controller, network, and the network device Collector.

6. Click OK.
7. Verify that the file is created and grows in size.
8. Proceed with one of the following options:
   - Using NXLog to Forward Log Files to Varonis
   - Configuring a New Network Device (Edge) Data Source to Use Filebeat

Using NXLog to Forward Log Files to Varonis

NXLog is a commonly used agent used to transfer log files to a Syslog server. After you have configured the DNS servers to create debug log files, you can add NXLog to read the log files and send the data to Varonis.

If you prefer not to use third-party software, click here for instructions for using the Varonis-provided Filebeat agent.

To use NXLog to forward DNS events to Varonis, for each DNS server, do the following:

1. Ensure that you configured the DNS data source to use Syslog.
2. Download the NXLog community edition from here.
3. From the command prompt, install NXLog using this command: msiexec /I <full path to downloaded file> /quiet.
4. Add the following lines to the end of the NXLog configuration file at C:\Program Files (x86)\nxlog\conf:

```
  <Input DNS_LOGS>
    Module mq  pi
    File "<full path of DNS log  pi ?
    SavePos TRUE
 Lrtyx
<Output out_syslog_server>
    Module <output module>
    Host <collector ip address>
    Port  <port>
 Ryxtyx
```

```
<Route 1>
    Path DNS_LOGS => out_syslog_server
 Usyxi
```

5. It is recommended to normalize logs to UTF-8. The xm_charconv module provides character set conversion; the convert_fields() procedure is used for converting an entire message (all event fields). To normalize logs to UTF-8 character set, it's necessary to setup the xm_charconv module in C:\Program Files (x86)\nxlog\conf\nxlog.conf:

```
<Extension converter>
    Module              xm_charconv
    AutodetectCharsets  utf-8, euc-jp, utf-16, utf-32, iso8859-2
</Extension>

<Input internal>
    Module      im_internal
</Input>

<Input file>
    Module  im_file
    File    "c:\\dns.txt"
    SavePos TRUE
    Exec    convert_fields("auto", "utf-8");
</Input>
```

- AutodetectCharsets - This optional directive accepts a comma-separated list of character set names. When auto is specified as the source encoding for `gsrzivx iphw\"`, these character sets will be tried for conversion.
- convert_fields(string srcencoding, string dstencoding) - Convert all string type fields of a log message from `srcencoding` to `dstencoding`. The `srcencoding` argument can be set to "auto" to request auto detection.

6. Change the following:

> Note: When changing, remove the "<" and ">" brackets (do not leave them in).

- <full path of DNS log file> - The full path and file name of the DNS log file (as set above), for example, "c:\logs\dns.log".
- <output module> - Whether to select `om_tcp` to use TCP (recommended) or `om_udp` to use UDP.
- <collector ip address> - The IP address configured for the network device data source in the Management Console. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.

- <port> - The port configured for the network device data source in the Management Console. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.

See the following example:

```
  <Input DNS_LOGS>
    Module mq  pi
    File "c:\logs\dns.log"
    SavePos TRUE
 Lrtyx
<Output out_syslog_server>
    Module om_tcp
    Host 10.1.2.3
    Port 5514
  Ryxtyx
 <Route 1>
    Path DNS_LOGS => out_syslog_server
  Usyxi
```

7. To allow more than one output on NXLog, you should define more than one input (one input per output).
   See the following example:

```
  <Input in_a>
  Module mq  pi
        File     "C:\dns.txt"
 Lrtyx
<Input in_b>
  Module mq  pi
        File     "C:\dns.txt"
 Lrtyx
<Output out_a>
    Module      om_tcp
    Host        10.230.78.160
    Port        520
 Ryxtyx
<Output out_b>
    Module      om_tcp
```

```
    Host        10.230.76.44
    Port        520
 Ryxtyx
<Route 1>
    Path        in_a => out_a
 Usyxi
<Route 2>
    Path        in_b => out_b
 Usyxi
```

8. Save the configuration file and restart the NXLog service.

Using NXLog on a Non-Domain Controller Windows Server

Varonis supports receiving DNS events from several Microsoft DNS Servers via NXLog running on a non-DC Windows Server. Use the procedures described in this section to deploy NXLog on a non-DC Windows Server when it not possible to deploy it on a DC server.

About NXLog

NXLog is a commonly used agent used to transfer log files to a Syslog server. After you have configured the DNS servers to create debug log files, you can configure NXLog on a non-DC Windows Server to read the log files from network shares and send the data to Varonis.

Workflow for Using NXLog on a Non-DC Windows Server

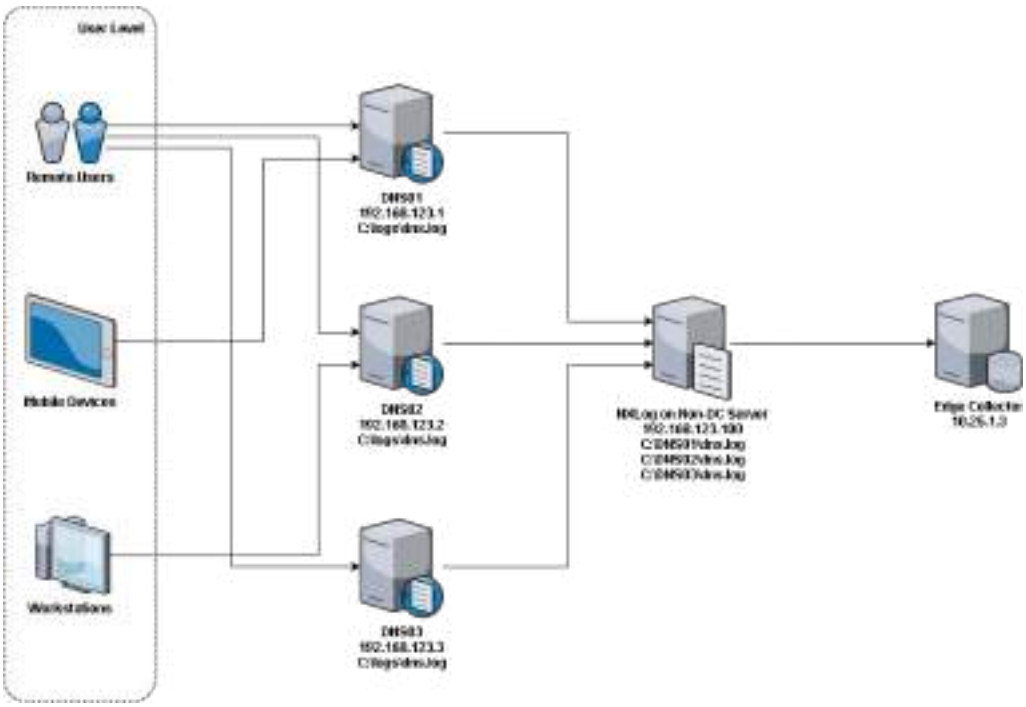
The workflow for using NXLog to forward DNS events to the network device (Edge) Collector on a non-DC Windows Server includes several steps.

1. Configure each DNS server according to the steps in Configuring Microsoft DNS Servers to Generate Log Files. For each server (for example, 192.168.123.1, 192.168.123.2, and 192.168.123.3), enable the debug logs for DNS and set the file path and file name as C:\logs\dns.log.
2. Mount the network shares on a non-DC Windows Server.
3. Use NXLog to forward DNS events to the network device (Edge) Collector on a non-DC Windows Server.

> Note: The NXLog application cannot be directly deployed on the network device (Edge) Collector.

Log Traffic Flow for DNS Events Forwarded by NXLog on a Non-DC Server

The following figure displays the log traffic flow for DNS events forwarded by NXLog on a non-DC Windows Server to the network device (Edge) Collector.



Mounting Network Shares on a Non-DC Windows Server

To mount the network shares on a non-DC Windows Server:

1. Run the following command from the command prompt:

```
net use \\192.168.123.1\c$\logs
mklink /d "C:\DNS01" \\192.168.123.1\c$\logs
net use \\192.168.123.2\c$\logs
mklink /d "C:\DNS02" \\192.168.123.2\c$\logs
```

```
net use \\192.168.123.3\c$\logs
mklink /d "C:\DNS03" \\192.168.123.3\c$\logs
```

2. If your network share requires the password to be mounted, you will be prompted accordingly.
   The log files are now accessible in C:\DNS01\dns.log, C:\DNS02\dns.log and C:\DNS03\dns.log.

Using NXLog to Forward DNS Events to Varonis on a Non-DC Windows Server

To use NXLog to forward DNS events to Varonis on a non-DC Windows Server, for each DNS server do the following :

1. Ensure that you configured the DNS data source to use Syslog.
2. Download the NXLog community edition from here.
3. From the command prompt, install NXLog using this command: msiexec /I <full path to downloaded file> /quiet.
4. Add the following lines to the end of the NXLog configuration file at C:\Program Files (x86)\nxlog\conf\nxlog.conf:

```
<Input DNS01>
     Module im_file
     File "C:\DNS01\dns.log"
     SavePos TRUE
</Input>
<Input DNS02>
     Module im_file
     File "C:\DNS02\dns.log"
     SavePos TRUE
</Input>
<Input DNS03>
     Module im_file
     File "C:\DNS03\dns.log"
     SavePos TRUE
</Input>
<Output LOGS>
     Module <output module>
     Host <ip address>
     Port <port>
</output>
<Route 1>
     Path DNS01 => LOGS
</Route>
<Route 2>
     Path DNS02 => LOGS
</Route>
<Route 3>
     Path DNS03 => LOGS
</Route>
```

5. Enter the following:

> Note: When changing the following, remove the "<" and ">" brackets (do not leave them in).

- <output module>
- <collector ip address> - Enter the same value as configured for the network device data source in the Varonis Management Console.
- <port> - Enter the same value as configured for the network device data source in the Varonis Management Console.

For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.

For example:

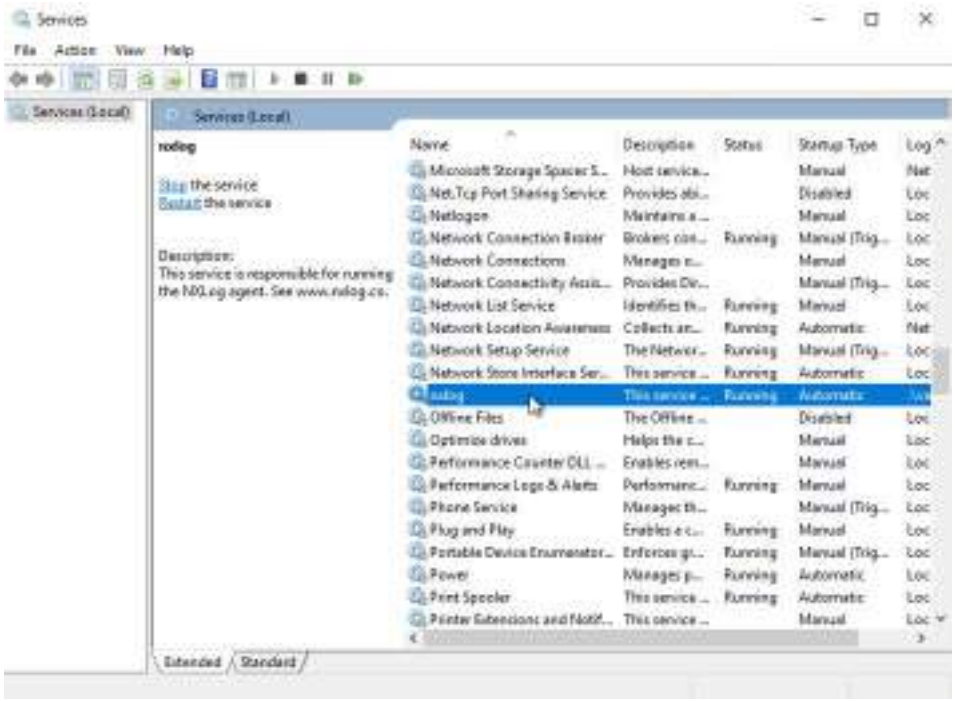
```
<Output LOGD>
    Module om_tcp
    Host 10.25.1.3
    Port 5514
</Output>
```

6. Make sure the user under which are you running NXLog has permissions to read the log files `C:\DNS01\dns.log`, `C:\DNS02\dns.log`, and `C:\DNS03\dns.log`. For example, if you are mounting the network shares using the user “varonis”, you can run the NXLog service with the same user:
   a. Open the Windows Services Manager.

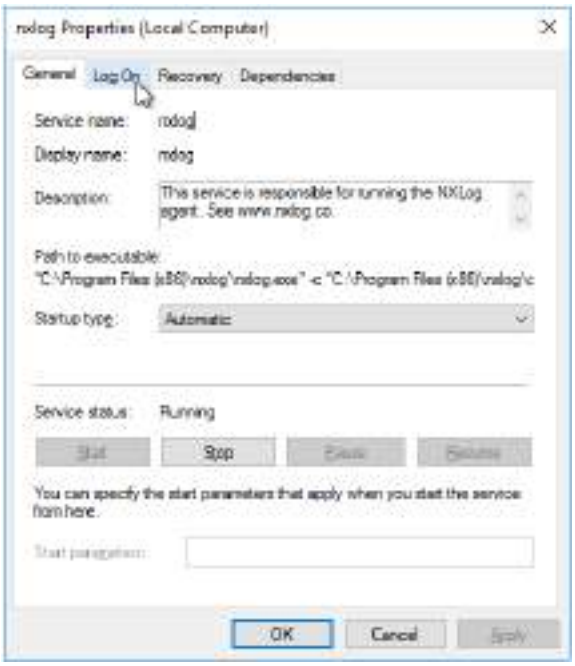


   The list of services is displayed.

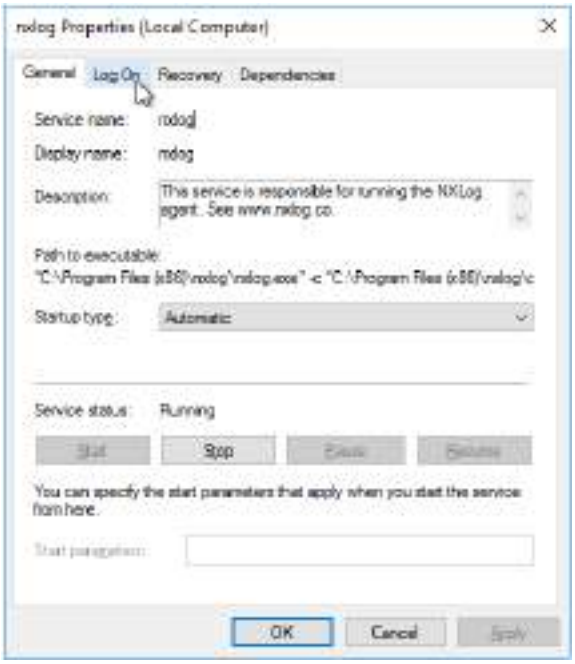
   b. Double-click nxlog.



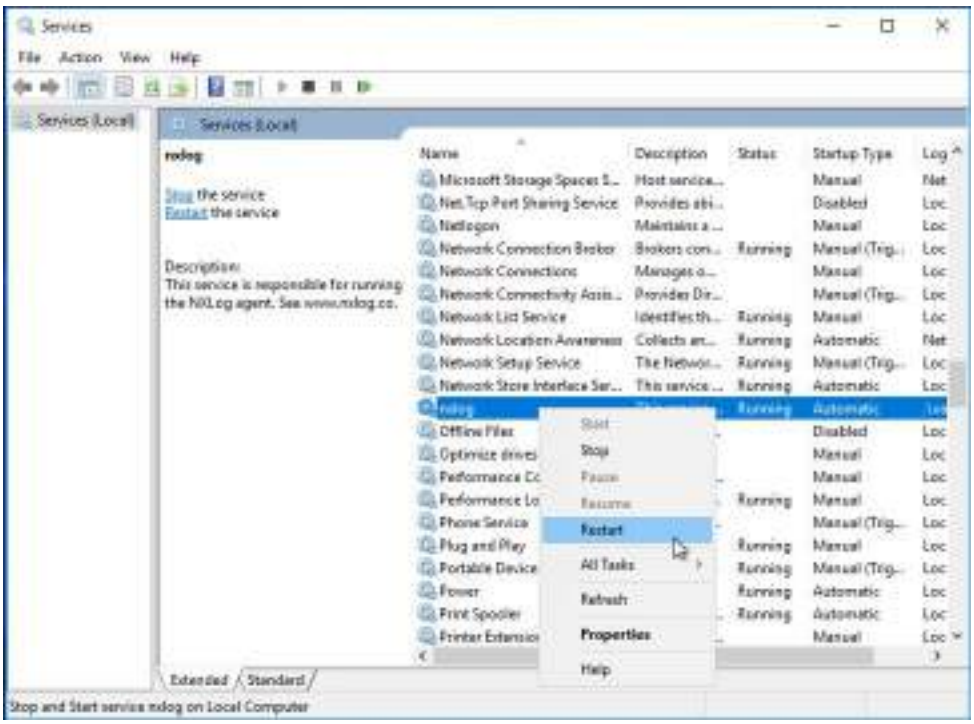
The NXLog Properties windows is displayed, showing the General tab.



c. Select the Log On tab and specify the user account (varonis) to run this service.



7. Save the configuration file and restart the NXLog service.



Infoblox DNS Servers

Varonis supports receiving events from Infoblox DNS Servers.

Infoblox provides information on how to send events to a third-party system such as Varonis in the article Using a Syslog Server.

Prerequisites for Infoblox DNS Servers

Before you begin configuring Infoblox DNS Servers to send DNS events to Varonis, you must follow several prerequisites.

- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.
- If using Splunk, ensure that the Splunk Add-on for Infoblox is installed on the Splunk machine. This is available for download from Splunk Add-on for Infoblox | Splunkbase.

Configuring Infoblox DNS Servers

When configuring Infoblox DNS Servers to send events to Varonis, you need to configure the DNS servers to create debug log files, and add Syslog Servers to send the data to Varonis.

> Note: The steps below are relevant only for on-premises Inflobox.

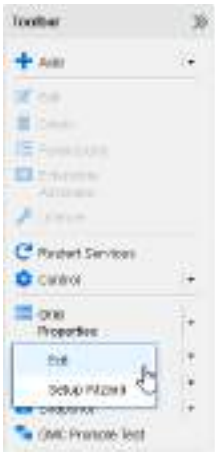
1. Log in to Infoblox with the relevant credentials.



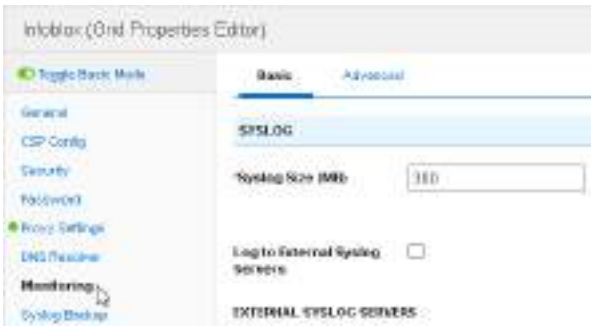
2. From the Grid tab in the Infoblox main window, select the Grid Manager > Members tab.



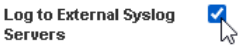
3. From the right menu bar, select Grid Properties > Edit.



4. From the left menu bar of the Grid Properties Editor, select Monitoring.



5. To enable the External Syslog Servers table, select the Log to External Syslog Servers checkbox .



6. Click + (Add) on the upper right toolbar.



The Add External Syslog Server area is displayed.



7. Fill in the fields, as follows:
   - Address - (Mandatory) The IP address of the Syslog server (Splunk server or network device Collector).
   - Transport - The transport protocol, TCP or UDP, according to the settings configured in the Management Console.
   - Interface - From the dropdown list, select the interface through which the appliance sends Syslog messages to the Syslog Server.
     - Any - The appliance chooses any port that is available for sending Syslog messages.
     - LAN - The appliance uses the LAN1 port to send Syslog messages.
     - MGMT - The appliance uses the MGMT port if it has been configured. Otherwise, it uses the LAN1 port.
   - Node ID - Specify the host or node identification string that identifies the appliance from which Syslog messages are originated. Use LAN (the default).
   - Source - From the dropdown list, select which Syslog messages the appliance sends to the external Syslog Server.
   - Severity - Info. The severity must be Info to get the debug information from the external Syslog Servers.

- Port - (Mandatory) The port number of the file server to where the Syslog messages will be published. The port is set in the Management Console for this data source. When using Splunk, this is the Splunk port.
- Logging Category - Send all (the default), to send/generate all log message types.



8. Click Add on the lower right of the Add External Syslog Server area.
   Upon successful configuration, the new Syslog server is displayed in the External Syslog Servers table.

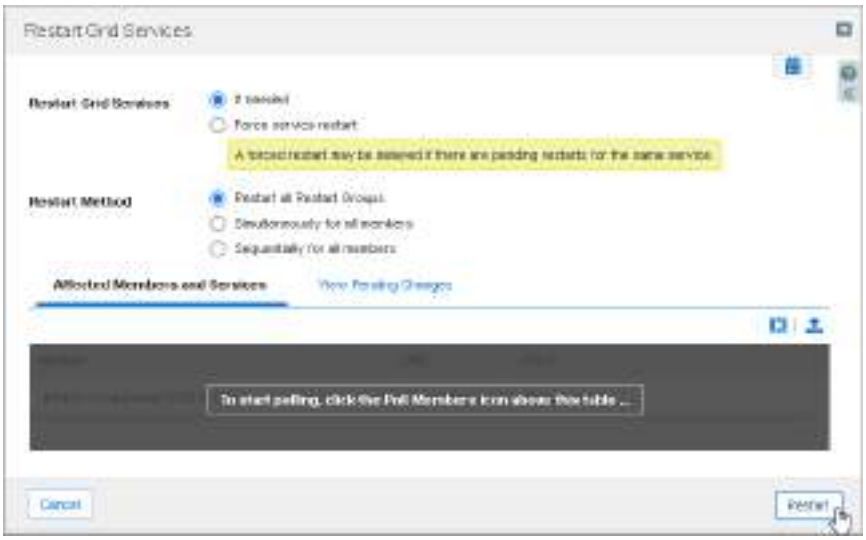


9. Click Save & Close. The system may prompt you to restart.



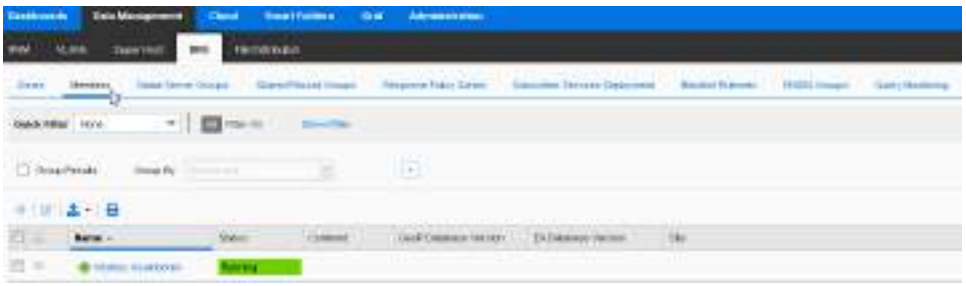
10. Restart, as needed, to apply the changes.



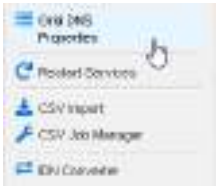


Configuring Logging DNS Query and Responses

1. From the Data Management tab, select DNS > Members.



2. From the right menu bar, select Grid DNS Properties.



3. To switch to Advanced mode, click Toggle Advanced Mode at the top of the left pane.



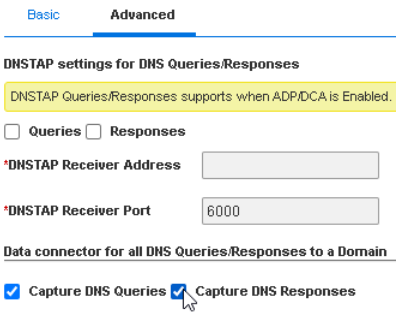
4. From the left menu bar, select Logging.



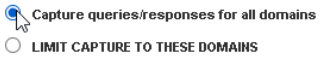
5. On the Basic tab, select the queries and responses checkboxes.



6. On the Advanced tab, in the Data connector for all DNS Queries/Responses to a Domain area, select the Capture DNS Queries and Capture DNS Responses checkboxes.



7. To capture all DNS queries and responses for all domains, select the Capture queries/responses for all domains option.



8. (Optional) To limit capturing DNS queries and responses by specific domains, select the Limit capture to these domains option and in the table below it add the domains that should be monitored.



9. To capture all DNS queries and responses from all domains except one (or several), select the Exclude the following domains checkbox.



10. To store DNS queries and responses in the Infoblox DNS server file system, select the Retain captured queries/replies on the local disk checkbox.

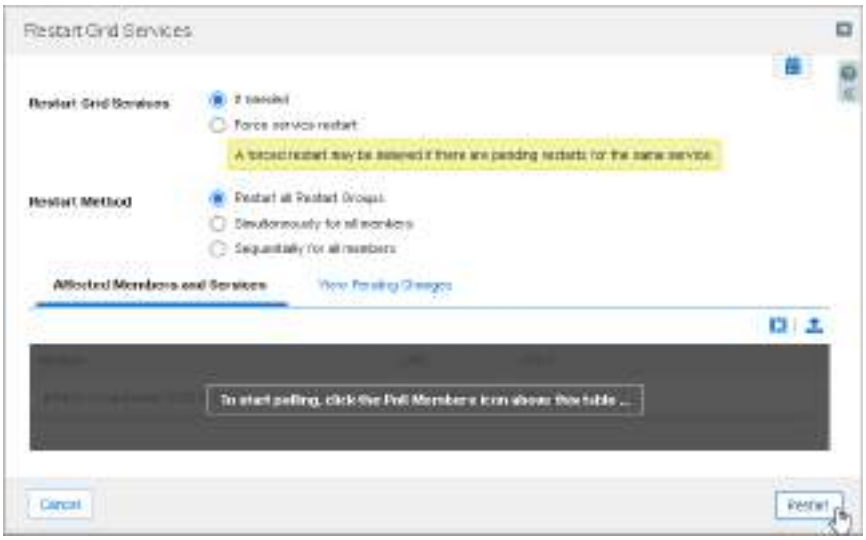


11. Click Save & Close. The system may prompt you to restart.



12. Restart, as needed, to apply the changes





Cisco Umbrella DNS Servers

Varonis supports receiving DNS events from Cisco Umbrella.

You can configure Cisco Umbrella to send DNS logs to Amazon Simple Storage Service (Amazon S3) bucket and set up Varonis to get the logs from AWS.

Varonis supports the following options:

- Company-managed Amazon S3 bucket
- Cisco-managed Amazon S3 bucket

Varonis also supports using Splunk as an interface to audit events from Cisco Umbrella source devices. For more information, see Configuring a Network Device Data Source when Working with Cisco Umbrella.

Prerequisites for Cisco Umbrella DNS Servers

Before you begin configuring Cisco Umbrella DNS Servers to send DNS events to Varonis, you must follow several prerequisites.

- Ensure network connectivity between Varonis (test connection) and the network device Collector to the AWS site.

Enable Logging to a Company-Managed Amazon S3 Bucket

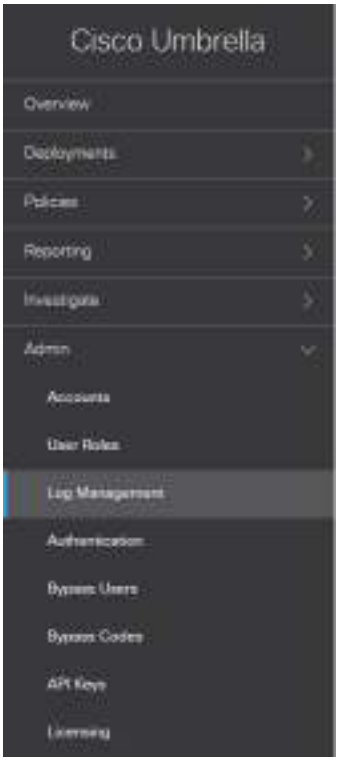
This procedure is relevant for companies that have an AWS account and want to manage their Cisco Umbrella logs under their account.

To enable logging to a company-managed Amazon S3 bucket:

1. Go to Cisco Umbrella login page.
2. Enter the credentials and click Log in.



3. In the Cisco Umbrella main window, from the navigation pane, select Admin > Log Management.



4. Select Use your company-managed Amazon S3 bucket.



5. Enter the Amazon S3 bucket name and click Verify.
   If everything is configured correctly, the following message is displayed.



6. Download the `README_FROM_UMBRELLA.txt` file from your bucket.



7. Copy the security token from the TXT file.



8. Paste the token into the token number field and click Save.



A message is displayed, confirming that the logs are sent to your Amazon S3 storage.



Enable Logging to a Cisco-Managed Amazon S3 Bucket

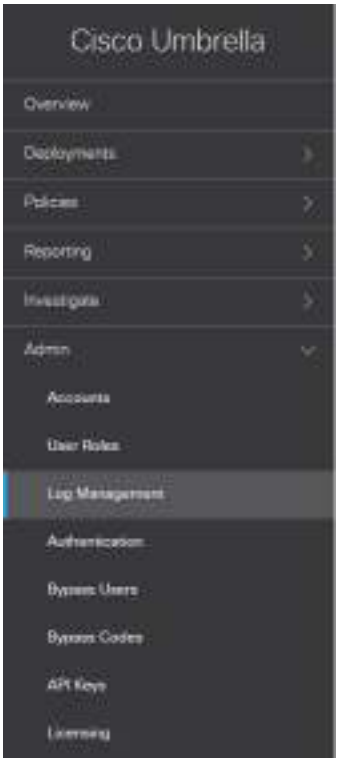
This procedure is relevant for companies that do not have an AWS account or do not want to manage Cisco Umbrella logs under their AWS account.

To enable logging to a Cisco-managed Amazon S3 bucket:

1. Go to Cisco Umbrella login page.
2. Enter the credentials and click Log in.



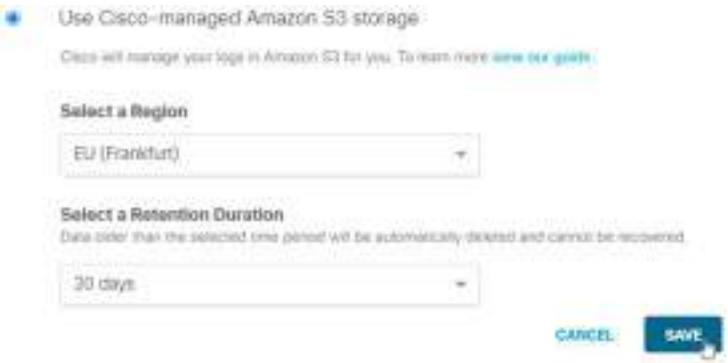
3. In the Cisco Umbrella main window, from the navigation pane, select Admin > Log Management.



4. Select Use Cisco-managed Amazon S3 storage.



5. Select the AWS region (for example, EU Frankfurt) and the desired retention duration for log files (for example, 30 days). Click Save to confirm.



6. Click Continue to proceed.



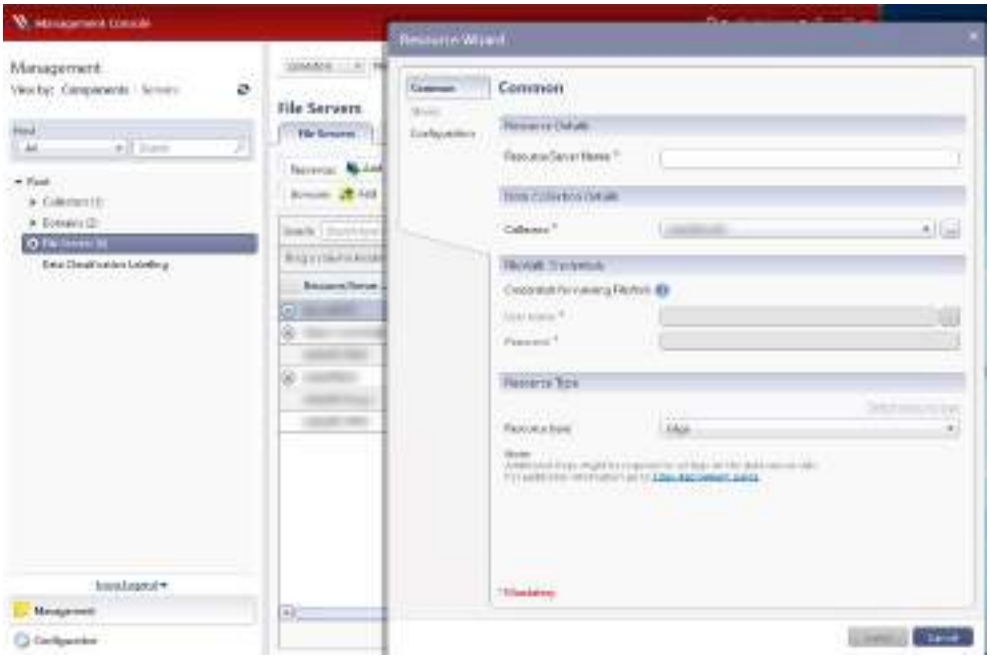
7. When activation is complete, a window is displayed, showing the credentials (Data Path, Access Key, and Secret Key). Store this information in a safe place, and then click Continue to proceed.



Configuring a Network Device Data Source when Working with Cisco Umbrella

1. In the Management Console, from the menu in the left pane, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.

The Resource Wizard is opened to the Common pane, where you can specify the data source and set the relevant parameters.



2. In the Common pane, set the following parameters:
   a. Resource Details - Specify the data source name.
   b. Data Collection Details - Select a Collector that is configured to support a network device.
   c. Resource Type - Select Edge from the dropdown list. (The FileWalk Credentials will be disabled.)
3. On the left menu, click Configuration.
4. In the Source Device area, set the following parameters:
   - Product - Select Cisco Umbrella - DNS.
   - Time Zone - Select UTC+0.
   - User Repository - Select the user repository with which to match user names in the events (leave the default if your installation contains only a single domain). For example, Active Directory.

- Default Date & Time Format - Select to auto-detect the date and time format used in the logs of the monitored sources (DNS). If the auto-detection fails, a notification is sent.

  Note: When Varonis proxy parsers based on splits is enabled (feature toggle EdgeSplitFilters=ON), auto-detection of the date and time format will not work. Only predefined default or custom dates can be used in this case.

- Custom Date & Time Format - Define the vendor's date and time format to avoid possible date format problems with Varonis servers. For information about the date and time format, see Date and Time Format Notation.



5. In the Interface Configuration area, the recommended interface will be automatically selected per the selected product. By default, AWS_S3 will be selected. The other option is Splunk.
   To configure AWS_S3 as the interface:
   - Select an Interface - Select AWS_S3.
   - If you are working with a company-managed Amazon S3 bucket, set the following parameters:

- Bucket - Enter the name of the Amazon S3 bucket.
- Prefix - Leave this empty.

- If you are using a Cisco-managed bucket, set the following parameters:
  - Bucket - Enter the name of the Cisco-managed bucket.
  - Prefix - Enter the data path within the Cisco-managed bucket (use the automatically generated data path saved from step 6 in Enable Logging to a Company-Managed Amazon S3 Bucket).
- Access Key ID - Enter the access key ID.
- Secret Access Key - Enter the secret access key.
- Region - Select the bucket region.



To configure Splunk as the interface:

Note that Splunk does not recommend connecting third-party applications such as Varonis to Splunk Free. Since Splunk Free does not support authentication, providing such access exposes Splunk to anyone.

a. Select an Interface - Select Splunk.
b. Splunk User Name - Enter the Splunk API user name.
c. Splunk Password - Enter the Splunk API password.

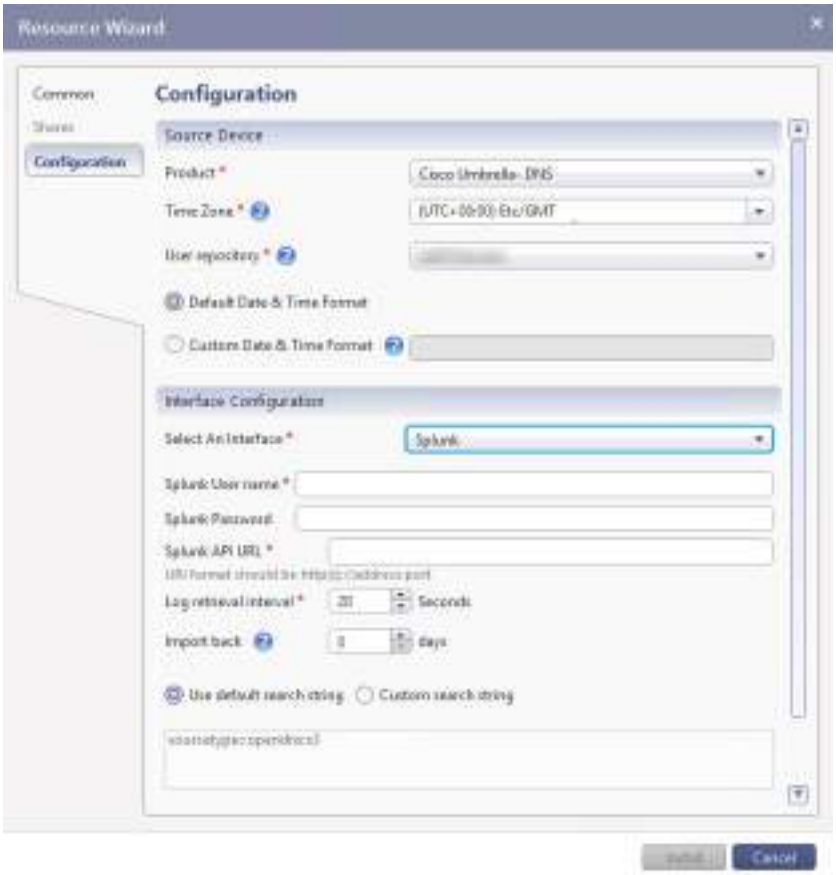
d. Splunk API URL - The format is http://<host>:<port> or https://<host>:<port> where <host> is the IP address or host name of the Splunk server and <port> is the port configured in Splunk for the API. The default Splunk port is 8089 and must be specified.

e. Log retrieval interval - Specify the interval for retrieving Splunk event logs. The default is 20 seconds. The maximum allowed is 60 seconds.

f. Import back__days - Imports past events from Splunk for network device data sources which support importing real-time events. It is possible to select up to 30 days back.

g. Use default search string - Enables you to keep the provided default string (displayed at the bottom). The default search string is useful if using the standard Splunk App provided by the device to audit events.

h. Custom search string - Enables you to modify the default search string. Ensure the _raw field is returned in the search results. Test the custom search string on your Splunk Enterprise console.



Once you've configured the interface settings, the next step is to test whether the connection is working.

6. Click Test Connection. (You may need to scroll down to the bottom of the Interface Configuration area to see this button).



A message is displayed, confirming that the test connection succeeded.



If the test connection failed, see Troubleshooting SSL Certificate Issues.

7. After configuration is complete, click Install to install the data source.
   A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the File Servers pane. When the installation completes, the status shows "Installed 100%".

Troubleshooting SSL Certificate Issues

In some setups, there is no direct connectivity between the network device Collector and public Internet. If you are running SSL decryption on your network devices such as a next-generation firewall (NGFW) and presenting your own self-signed or untrusted SSL certificate, you might need to add the SSL decryption exclusion to avoid SSL certificate verification failure.

Using AWS CLI Tools for SSL Certificate Verification

1. Download and install AWS CLI tools on your Collector from AWS Command Line Interface.
2. Run the following commands on the Collector machine:

```
set AWS_ACCESS_KEY_ID=<your_access_key>
set AWS_SECRET_ACCESS_KEY=<your_secret_key>
set AWS_DEFAULT_REGION=<aws_region_for_your_s3_bucket>
```

```
aws s3 sync s3://<s3_bucket_name> . stxmsrep tvi 1 livi .
hrwpskw
```

3. For example, a bucket named varonis-test and eu-central-1 (Frankfurt) AWS region: `C:\varonis>aws s3 sync s3://varonis-test/dnslogs/`:

```
fatal error: SSL validation failed for lxxtw%..zevsrmw xi
wx#w7#iy girxvep 5#eqe3sre0w#gsq.↗pmwx x2ti 6 tvi 1 hrwps
kw 6H irgshmrk x2ti yvp [SSL: CERTIFICATE_VERIFY_FAILED]
givxm gexi verify failed: self signed givxm gexi in certif
icate chain (_ssl.c:1125)
```

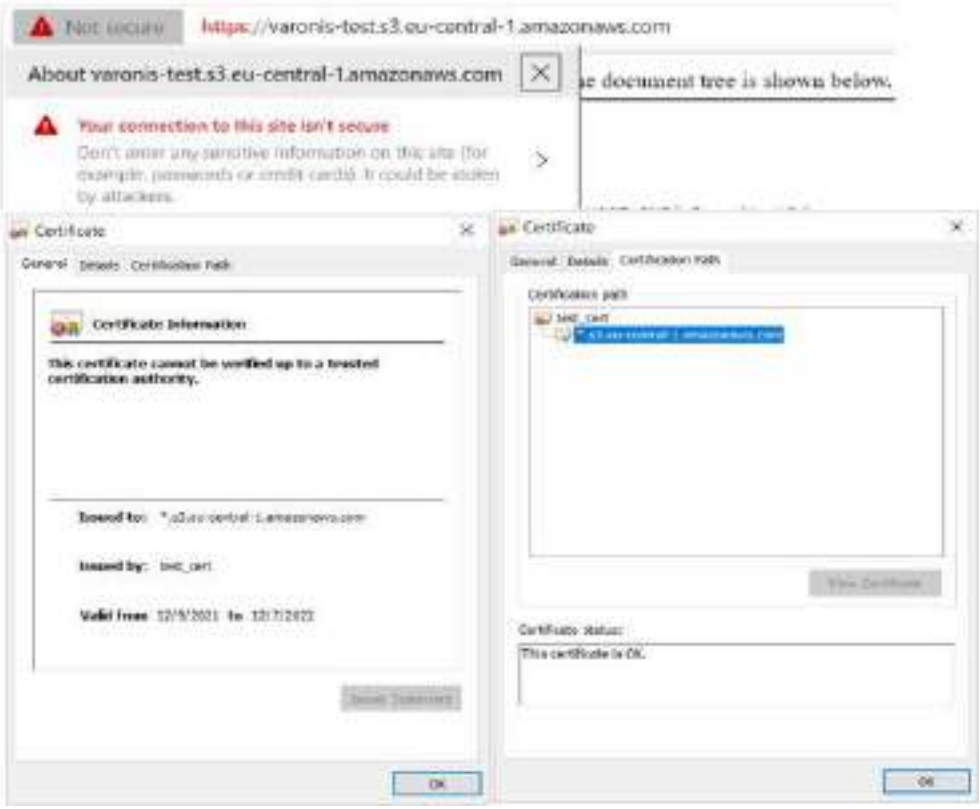
   In this case, you need to add SSL decryption exclusion for https://varonis-test.s3.eu-central-1.amazonaws.com (it can also be a wildcard for *.s3.eu-central-1.amazonaws.com or even *.amazonaws.com). For more information, see the documentation for your NGFW vendor for instructions on configuring SSL decryption exclusion.

Using the Web Browser for SSL Certificate Verification

You can also use the web browser running on the Collector machine to check the SSL certificate.

1. Go to https://<s3_bucket_name>.s3.<aws_region>.amazonaws.com.
2. For example, for a bucket named varonis-test and eu-central-1 (Frankfurt) AWS region, you need to go to https://varonis-test.s3.eu-central-1.amazonaws.com and check the SSL certificate.

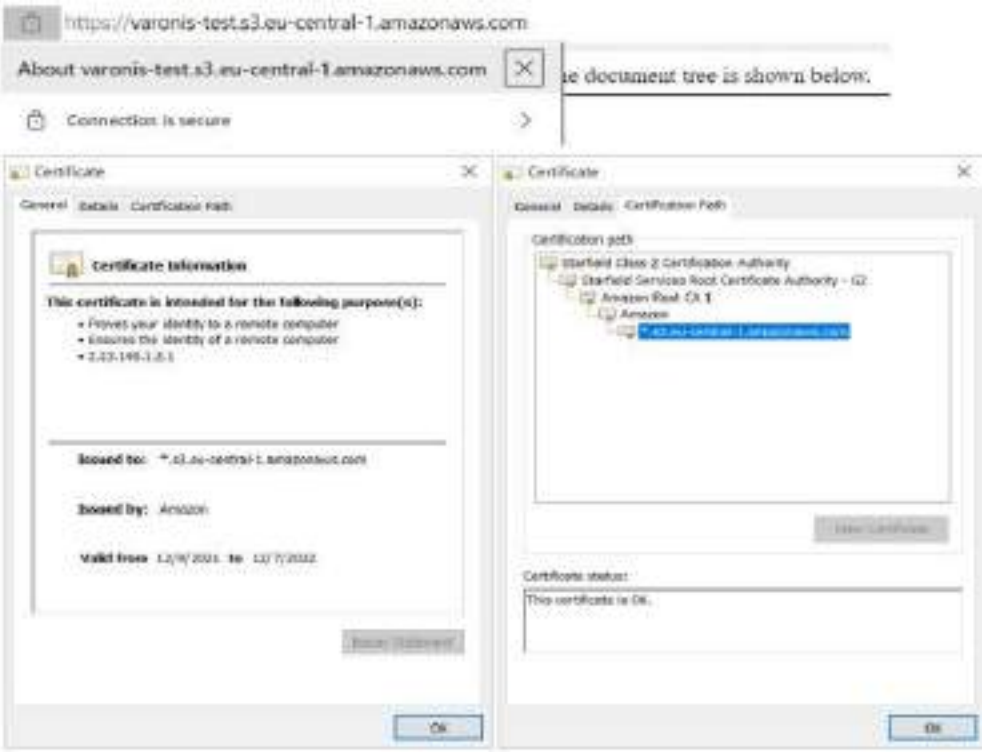
Before adding SSL decryption exclusion :



The connection is not secure, an untrusted SSL certificate was issued by test_cert, and the certification path is incomplete.

In this case, you need to add SSL decryption exclusion for https://varonis-test.s3.eu-central-1.amazonaws.com (it can also be a wildcard for *.s3.eu-central-1.amazonaws.com or even *.amazonaws.com). For more information, see the documentation for your NGFW vendor for instructions on configuring SSL decryption exclusion.

After adding SSL decryption exclusion:



The connection is secure, a trusted SSL certificate is issued by Amazon, and the full certification path is available.

BlueCat DNS Servers

Varonis supports receiving DNS events from BlueCat DNS servers.

You can configure BlueCat DNS servers to send DNS events to Varonis by using a graphical user interface.

Prerequisites for BlueCat DNS Servers

Before you begin configuring BlueCat DNS Servers to send DNS events to Varonis, you must follow several prerequisites.

- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.

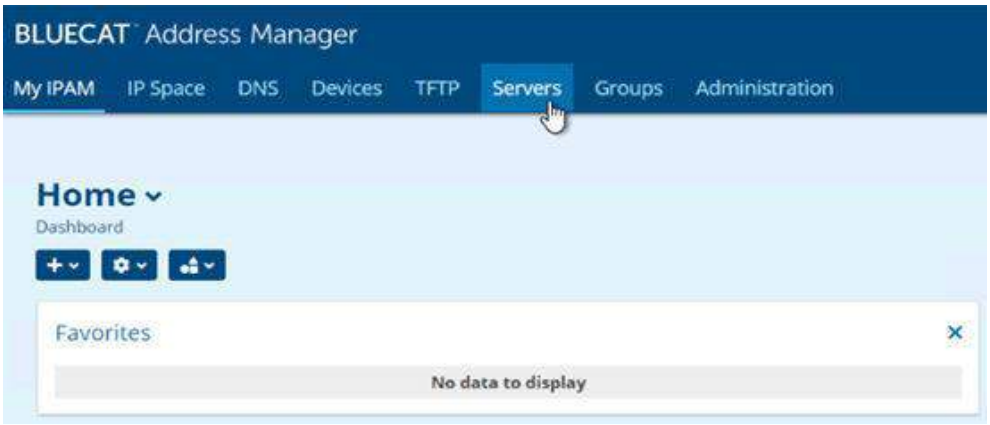
Configuring BlueCat DNS Logging Using a Graphical User Interface

To configure BlueCat Networks DNS logging using a graphical user interface:

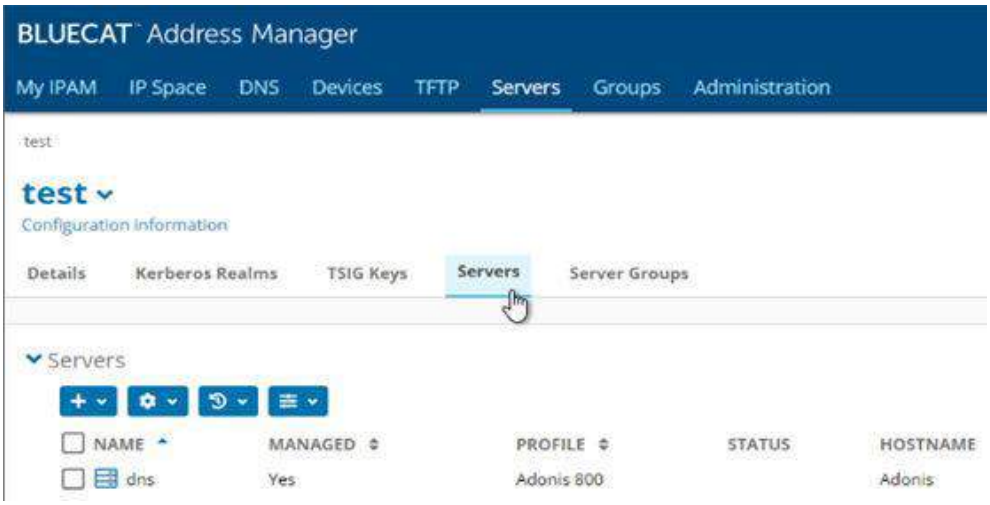
1. Log in to BlueCat Address Manager with your user name and password.



2. Navigate to the Servers tab.



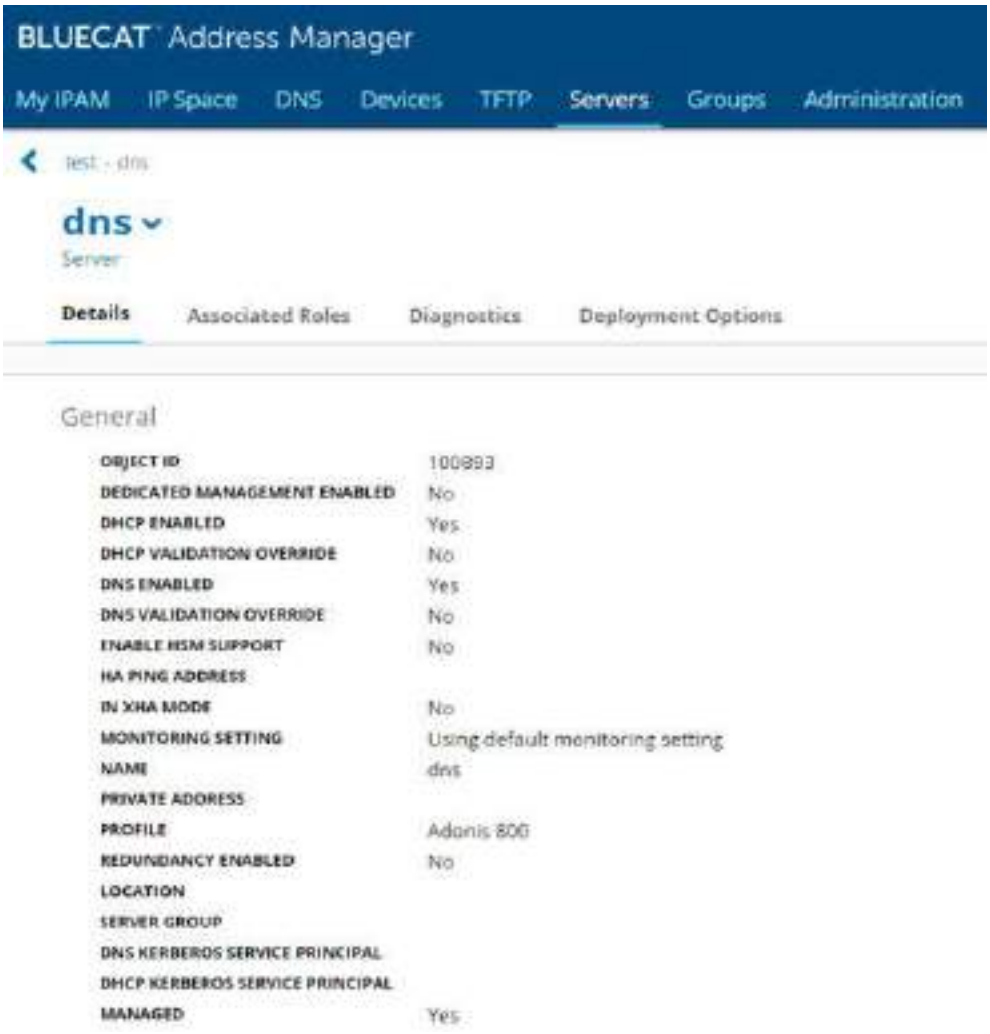
3. Make sure the Servers submenu tab is selected.



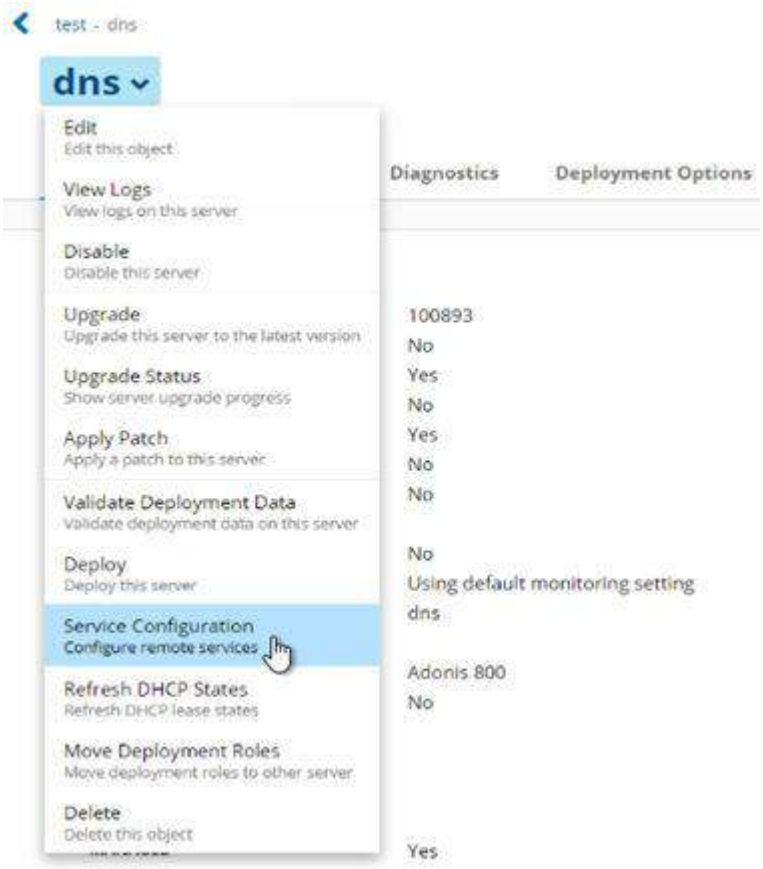
4. Click the relevant DNS server name.



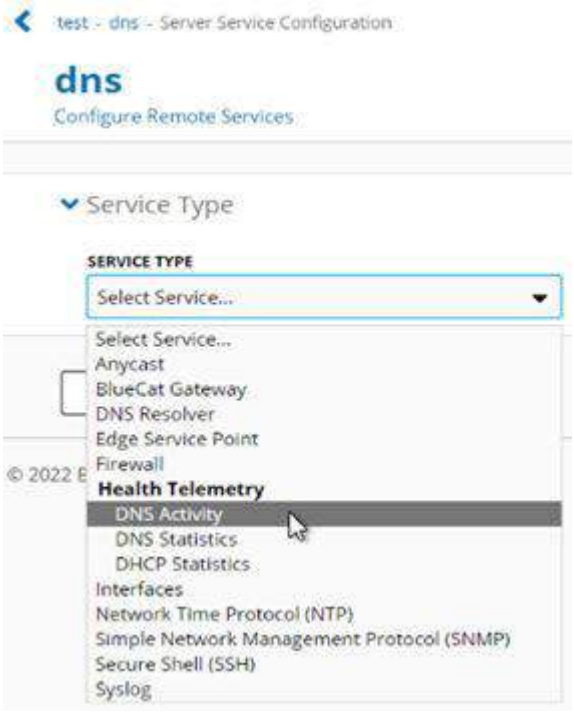
The settings page is displayed.



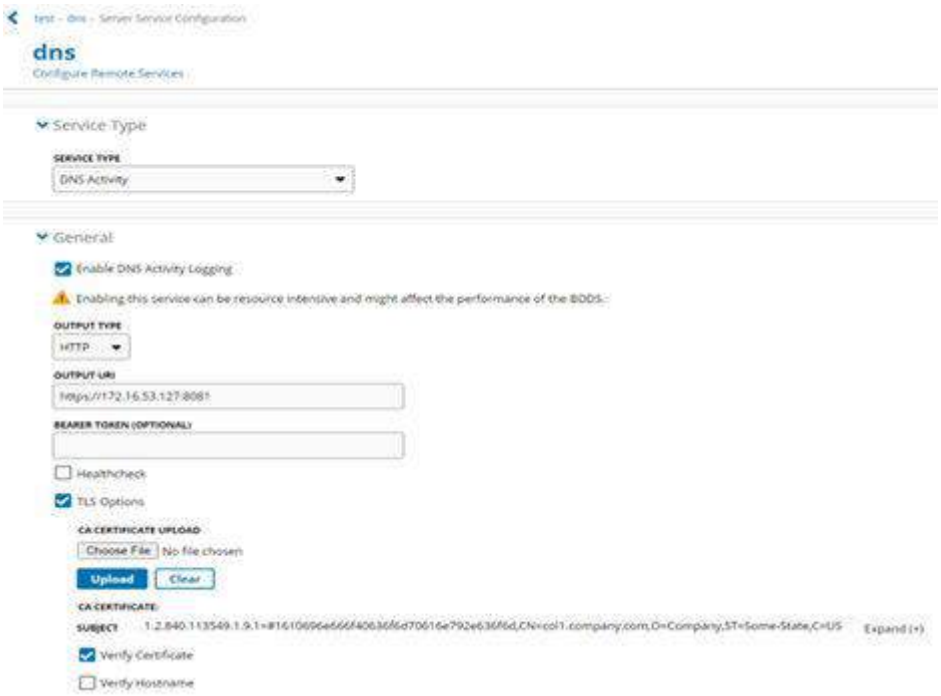
5. From the DNS server name dropdown list, select Service Configuration.



6. From the Service Type dropdown list, select DNS Activity.



7. Click Enable DNS Activity Logging and specify HTTP as the Output Type.



8. In the Output URI text box, enter the following:
   - Network devices Collector's IP address (for example, 172.16.53.127)
   - Network devices Collector's Port (for example, 8081)

> Note: If you prefer an encrypted HTTPS connection, you can enter the relevant HTTPS port number in the text box.

- TLS Options - Select this checkbox if you are planning to work with encrypted protocol:
  - Select and upload the certificate with the Choose File and Upload buttons.
  - Select Verify Certificate for certificate verification.

> Note: If you are using a passphrase for a private key, you might need to use a -v1 (PKCS#5 v1.5) algorithm due to a Java limitation (as described here).

9. Scroll down the DNS settings page and click the Update button.



DNS activity logging is now running.

Filtering DNS Events per Specified Domains

You can filter DNS events per specified domains to reduce the volume of events and suppress alerts from trusted domains. The domains can be selected from a predefined list of frequently used domains, or from a custom list of domains or domain patterns.

To filter DNS events per specified domains:

1. In the Management Console, from the menu in the left pane, select Management > Components > Root > File Servers, and select the File Servers tab.
   The File Servers settings are displayed.
2. Select the DNS data source you want to edit, and on the Resources toolbar, click Edit.
   The Editing File Server window is displayed.
3. On the left menu, click Configuration.
4. Select the Filter domains checkbox at the bottom of the pane, and click the Manage Filtered Domains link next to it, which is now enabled.
   The Filtered Domains dialog box is displayed, where you can select domains from the predefined list, or specify the list of domain filtering patterns.





Note: Filtering patterns may contain only alphanumeric characters and '*', '.', '-', '_' symbols. The wildcard is a special symbol that matches any input in the current position.

5. Click the Add Domains button to add the list of most commonly used domains.

> Note: This list is taken from the Top Sites list published by Alexa Internet.

6. Click Save in the Filtered Domains dialog box when done.
7. Click Save in the Configuration pane to update the file server configuration.

Configuring Firewall Sources To Send Events To Varonis

This section describes how to configure Firewall Sources to send events to Varonis.

> Note: Private Preview. If you'd like to monitor firewall activity, contact your Sales Engineer.

Cisco Secure Firewall Threat Defense (formerly known as Cisco Firepower Threat Defense)

> Note: Private Preview. If you'd like to monitor firewall activity, contact your Sales Engineer.

Varonis supports receiving firewall events from Cisco Secure Firewall Threat Defense.

Varonis can be configured to receive Syslog messages from the Cisco ASA LINA engine that is integrated into Cisco Secure Firewall Threat Defense.

Prerequisites for Cisco Secure Firewall Threat Defense

Before you begin configuring Cisco Secure Firewall Threat Defense to send events to Varonis, you must follow several prerequisites.

- If using Syslog, ensure that the interface configuration is properly configured to receive events. For more information, see Configuring a New Network Device (Edge) Data Source to Use Syslog.

Configuring Cisco Secure Firewall Threat Defense Filtering Logging

To configure Cisco Secure Firewall Threat Defense firewall events:

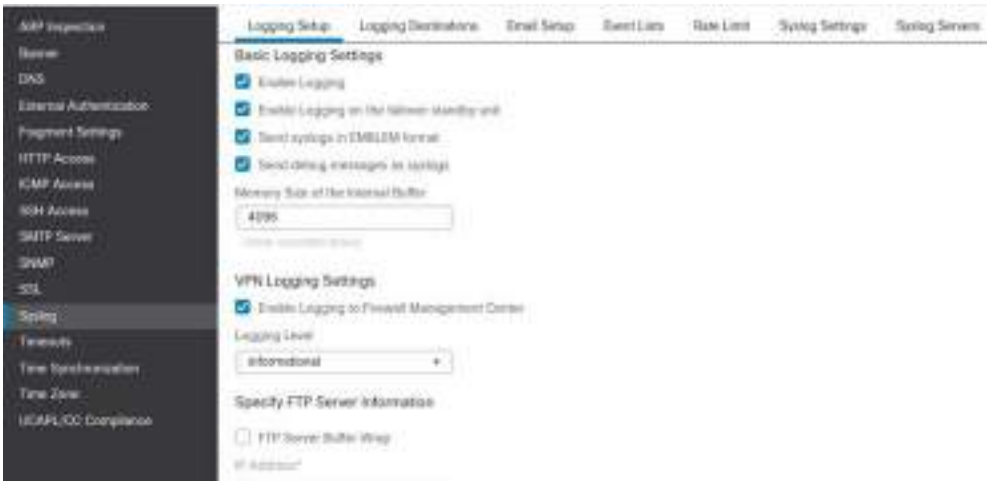
1. Open the Cisco Secure Firewall Management Center (FMC).
2. From the FMC main window, select Devices > Platform Settings.



3. Select the policy related to firewall events and click Edit.

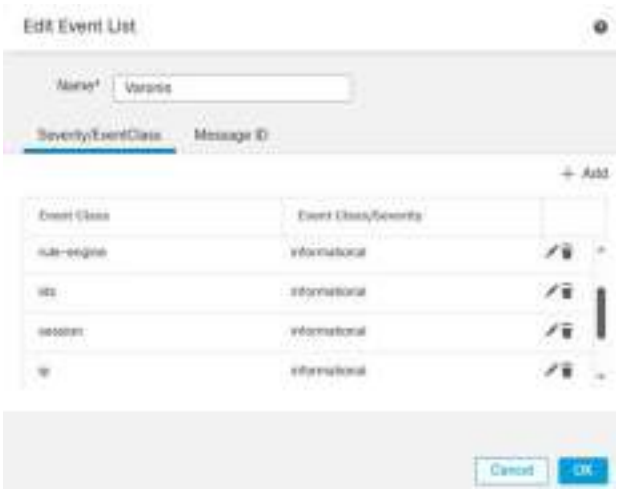


4. From the navigation pane on the left, select Syslog.
   The Logging Setup window is displayed.



5. Make sure Enable Logging is selected.
6. Select the Event Lists tab and click Add to create a new event list.
7. In the Name field, enter a name for the event list (for example, Varonis).
8. Create an event list with the following parameters and click OK:
   - auth - informational
   - ca - informational
   - rule-engine - informational
   - ids - informational

- session - informational
- ip - informational



9. Select the Syslog Settings tab, and do the following:
   a. Select the Enable Timestamp on Syslog Messages checkbox.
   b. From the Timestamp Format dropdown list, select RFC 5425 as the timestamp format.
   c. Select the Enable Syslog Device ID checkbox and select Host Name from the dropdown list.



10. Select the Syslog Servers tab and click Add.

The Add Syslog Server dialog box is displayed.



11. In the Add Syslog Server dialog box, do the following:
    For the following, enter the same value as configured for the network device data source in the Varonis Management Console:
    - IP Address - From the dropdown list, choose a network object that has the Syslog servers listed. If you have not created a network object, click the (+) icon to create a new object.
    - Protocol - Select UDP and use the Emblem format, or select TCP.
    - Port - Enter the Syslog server port number. By default, it is 514.

    Then, do the following:
    - Reachable By - The interface for sending Syslog messages. Select Device Management Interface or Security Zone or Name Interface, then add the relevant Available Zones to the Selected Zones/Interface list.
12. Click OK.
13. Select the Logging Destinations tab and click Add.
14. From the Logging Destination dropdown list, select Syslog Servers.
15. From the Event Class dropdown list, select Use Event List and use the event list that was set up previously (for example, Varonis).



16. Click OK.

To configure sending firewall events:

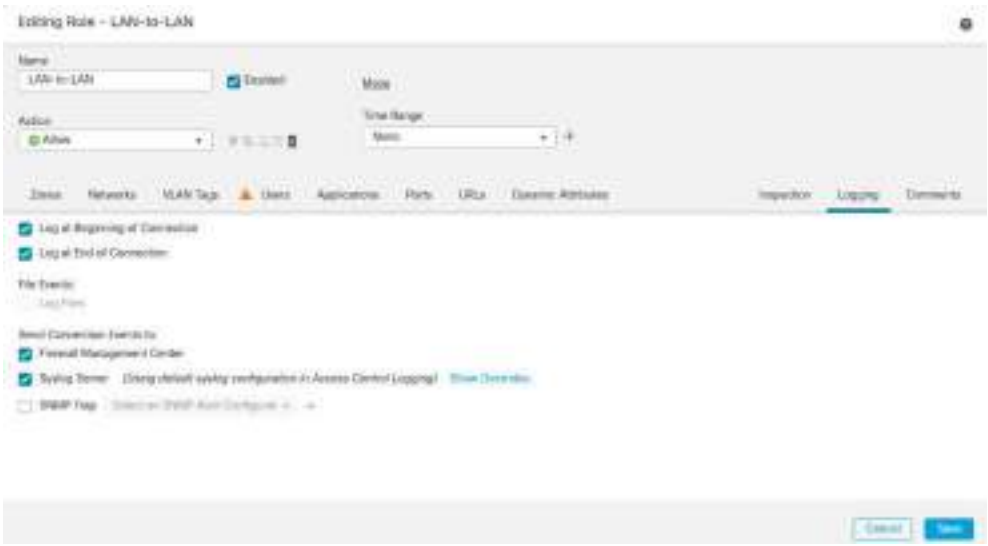
1. From the FMC main window, select Policies > Access Control.



2. Select the relevant Access Control Policy related to your firewall and click Edit.



3. Click Edit access rule and navigate to the Logging options.
4. Select Log at Beginning of Connection and Log at End of Connection.
5. Specify to send connection events to the Syslog Server (Using default syslog configuration in Access Control Logging).



6. Click Save to save the configuration.
7. In the Access Control Policy window, click Save.
8. Click Deploy (on the upper right).
9. In the Deployment tab, select the device to which to apply the changes.
10. Click the Deploy button.
11. Click Deploy to deploy the device.

Supported Events For Network Device (Edge) Data Sources

This section describes the list of events available through network devices from VPN Gateways, Web Proxies, and DNS servers activity monitoring.

VPN Gateway Events

The following events are available from Varonis monitoring activity logs from various VPN Gateways:

- VPN login request - Records an attempt to connect using the VPN, whether successful or not.
- VPN logout request - Records when a user logs out/disconnects and includes information about the session.

The VPN login request event includes the following key fields:

- User Name - The name of the authenticating user. Note that this may be an Active Directory user or a user managed using a different repository.
- External IP - The IP address of the remote device connecting. This address is used, among other things, to determine the geographic location of the user.
- Event Status and Status Reason - Whether the login was successful, and if not, what was the reason for the failure.
- User Agent, Operating System and MAC Address - Identifying properties of the connecting device.
- Connection Type - The connection method used.
- Destination IP and Destination Device Name - The destination to which the user connected if relevant to the VPN method used.
- Malicious External IP - Indicates whether the IP is known to be malicious.
- External IP Reputation - The reputation score of the IP. The score is a numeric value from 1-100.

The VPN logout request event includes the following key fields:

- User Name and External IP - Similar to those included in the login event.
- Event Status and Status Reason - Whether the connection was closed, and the reason for closure.
- Session Duration, Upload size in MB and Download size in MB - Properties of the connection.

VPN supports a wide range of modes. Not every vendor supports all features, and not all features are used by any one organization. This implies that some of the events or events fields listed would not be available in specific environments.

User names are received as part of the event and may not be related to the account enumeration users recognized by Varonis.

Varonis searches for the user in the configured User Repository. If found, the user located is used. Otherwise, the user name as specified in the event itself is used. If the user is located in the User Repository, and the user is unmonitored (pruned) or filtered for event auditing, the event is not audited.

Web Proxy Server Events

- HTTP Transaction - Created and published by Varonis from web proxy servers which reflect a single HTTP request the client made. An HTTP request does not denote a web page. Every element of a web page, such as an image or a script, requires an HTTP request. Moreover, modern web sites and mobile applications

generate HTTP requests behind the scenes without changing the displayed page, for example, to update a dropdown list based on previous input.

- Network Session – Audited only by Palo Alto; it summarizes the most recent web proxy session

To reduce the event load, facilitating easier investigation and lower resource requirements, Varonis does the following:

- Filters requests for less important page elements such as images
- Aggregates similar requests within a five-minute time window

Therefore, a single logged event may represent a number of raw events. To reflect this, the event includes the time of the first event aggregated, the time of the last event aggregated, and the count of the events aggregated in the Start Time, End Time, and Count fields respectively.

Similar requests are requests from the same source to the same server and object and with the same result.

The web proxy client request events include the following key fields:

- Object Name - The URL of the HTTP request. Varonis truncates the URL at the last slash character to the meaningful part to ensure better aggregation.
- Client IP - The source IP of the computer from which the request was initiated.
- User Name - The user name of the user initiating the request.
- The Session duration in seconds, Upload size in MB and Download size in MB - Properties of the transaction. If events are aggregated, those fields will reflect the total for all aggregated events.
- Status Reason - The HTTP status code. For a list of status codes, click here.
- URL Categorization - The type of industry or service to which the website belongs.
- URL Reputation - The risk level associated with the URL.

Note: The HTTP proxy protocol does not require transmitting a user name. Since the user name is important for applying policies and for logging activity, most proxies include a mechanism to determine the user name. However, not all organizations implement it. If a user name is not available the Client IP can serve as an indicator of the user.

DNS Server Events

The below events are available from Varonis monitoring activity logs from various DNS servers.

- DNS Query events:
  - Client DNS request - Logs a query sent by a computer to the monitored DNS server. Most commonly the query is to lookup the IP address of a domain, however it can also be a different domain-related query sent by the computer to the monitored DNS server.
  - Upstream DNS request - Logs a query sent by a monitored DNS server to its upstream DNS server when it does not have the answer available locally.
- DNS server administrative events:
  - DNS client IP update request - Logs an update message sent by a computer informing the DNS server that it receives a new IP address. Since most client computers use DHCP to get a dynamic IP address that changes from time to time, they need to inform the DNS server that their IP address has changed to ensure the DNS server can perform correct hostname to IP resolution.
  - DNS zone transfer request - Logs a request to send the entire lists of host name in a domain. While such a request can be used to replicate domain data across multiple DNS servers, it may also be used for reconnaissance.

For each event, the key fields logged are:

- Object Name - The domain or host name for which the request was made. For some DNS queries this fields might be used differently, for example, a reverse lookup query would have an IP address in this field.
- DNS Record Type - The type of information requested. Most commonly, this would be the “A” record, indicating the client asked for the IP address of the host or domain name. For a full list of record types, click here.
- Event Status and Status Reason - Whether the query was successful, and if not, why. For a list of possible status reasons, click here.
- URL Categorization - The type of industry or service to which the website belongs.
- URL Reputation - The risk level associated with the URL.

To reduce the event load, allowing easier investigation and lower resource requirements, Varonis aggregates similar DNS queries within a five-minute time window. Therefore, a single logged event may represent a number of raw events. To reflect this, the event includes the time of the first event aggregated, the time of the

last event aggregated, and the count of the events aggregated in the Start Time, End Time, and Count fields respectively.

Similar queries are queries from the same source for the same domain or host name, and with the same result.

Changing Ports For Logstash

This section describes how to change the TCP ports used for internal communication on the network device Collector.

To change ports for Logstash:

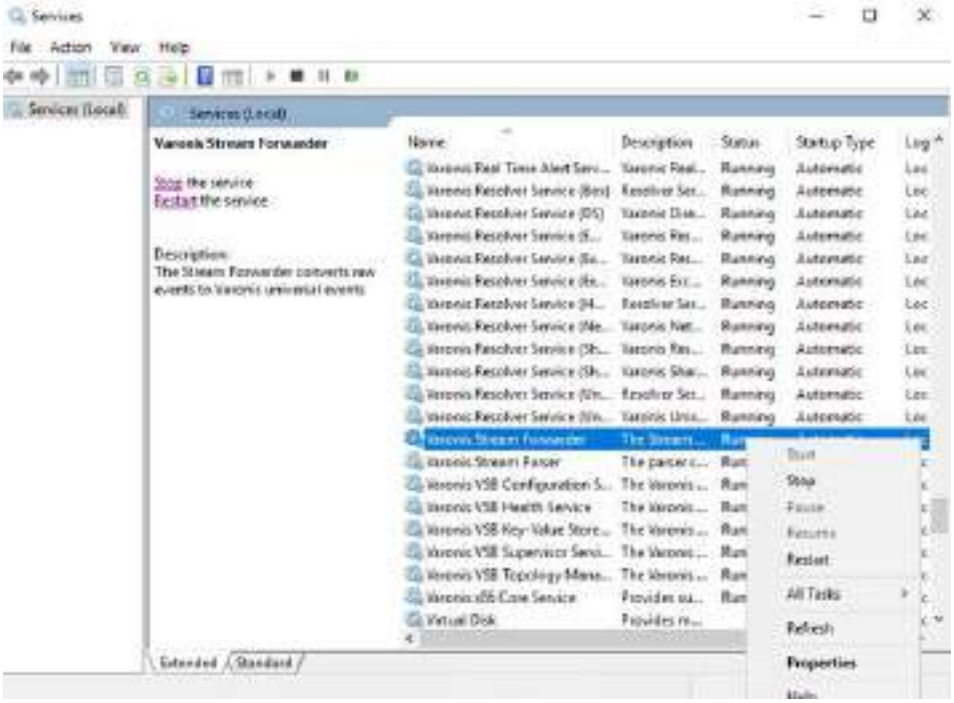
1. On the Collector, go to C:\Program Files (x86)\Varonis\DatAdvantage\Streams.
2. Open the `Varonis.Agents.Collector.Streaqw#i1i#gsr k` file.
3. Edit the following parameters:
   - `<add key="RegularEventsPort" value="34500"`
   - `<add key="UnknownEventsPort" value="34501"`
   - `<add oi2 ?Qsxm gationEventsPort" value="34502"`
   - `<add key="HeartbeatEventsPort" value="34503"`
   - `<add key="RegularDnsEventsPort" value="34504"`
   - `<add key="RegularVpnEventsPort" value="34505"`
   - `<add key="RegularProxyEventsPort" value="34506"`
   - `<add key="RegularFirewallEventsPort" value="34507"`
   - `<add key="HealthcheckEventPort" value="34508"`

   Note: Each parameter key can have only 1 port number assigned to it.
4. Go to the Logstash installation folder (for example, C:\Logstash).
5. In the config folder, open the `transport.options` file.
6. Set the port numbers for each parameter the same way as configured in step 3 above, and as shown below.

transport.options

```
regularEventPort,34500
unknownEventPort,34501
notificationEventPort,34502
heartbeatEventPort,34503
dnsEventPort,34504
vpnEventPort,34505
proxyEventPort,34506
firewallEventPort,34507
shouldUseTcp,1
host,127.0.0.1
healthcheckPort,34508
```

7. Restart the Varonis Stream Forwarder and Varonis Stream Parser services:
   a. Run the Windows Services Manager:
      i. Select Start > Run.
      ii. In the Run field, type `services.msc`.
   b. In the list of services, right-click Varonis Stream Forwarder and select Stop. Then right-click it again and select Start.
   c. Right-click Varonis Stream Parser and select Stop. Then right-click it again and select Start.



24 GENERIC DATA SOURCES

What This Section Contains

This section describes how to deploy and monitor Generic data sources; the requirements, deployment and configuration steps.

What To Do Next

First, make sure you fulfill the Generic data source requirements.

Generic Data Source Requirements

Varonis Service Account

Varonis requires a dedicated service account. The service account can be reused for multiple data source installations and configurations.

- Service Account Read Operations:
  - Traverse and enumerate files, folders, directory structures, users, and groups.
  - Gather data source, user, and group metadata as part of normal system operations.
- Service Account Write Operations:
  - Used for executing Varonis Policies, if policies are defined.

Varonis Installation and Requirements

- The Varonis service account requires permissions to read all files. Varonis Policies require write permissions to perform changes.

Data Discovery and Classification

- Varonis supports data classification on files that reside in the monitored data sources.

Notes

- IMPORTANT: Generic data sources can only be used for data sources that support SMB and WINAPI.
- Event auditing is not supported.
- When deploying a resource using a Generic data source, no agent is installed. Since event auditing is not supported on Generic data sources, there is no event agent. Instead, directory structure monitoring is conducted via the CIFS method, not the Varonis agent method.
- When monitoring Azure NetApp Files using a Generic data source, the Varonis service account should be added to the Domain Admins group to ensure proper access and functionality.

What To Do Next

Now that you've fulfilled the requirements, it's time to add a monitored generic data source. First familiarize yourself with the deployment steps summary and then dive into the detailed procedure.

Adding a Generic Data Source - Summary

Now that you've fulfilled the requirements, you can deploy a Generic data source. This section summarizes the procedure for deploying generic data sources.

1. Run the Management Console as an administrator.
2. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.
3. In the Resource Wizard's Common pane, specify the data source name, check the Collector selected by default and change it if needed, and enter the credentials for running directory structure monitoring (FileWalk).
4. In the Resource Type area, select Generic Data Source from the dropdown list.
5. In the Generic Data Source Settings area, specify the data source type. This field helps track usage and identify demand for new platforms.
6. In the Monitored Shares area, select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source is installed and share detection is completed.
7. In the Configuration pane, review the Local Accounts settings and FileWalk Settings.
8. (Optional) In the Commit pane, clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials.

   Note:

   - If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
   - If the Collector is in a lower version than 8, the FileWalk credentials will be used.

   In the Group OU area, if required, select Uniquely defined to choose a different OU from that defined in the data source's domain.
9. After configuration is complete, click Install to add the data source.

10. After the data source installation and share detection are completed, in the Shares pane, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. If you chose to monitor selected shares, you can select and register the required shares.

What To Do Next

Now that you're familiar with the deployment steps, it's time to dive into the detailed procedure.

Adding a Generic Data Source - Detailed Procedure

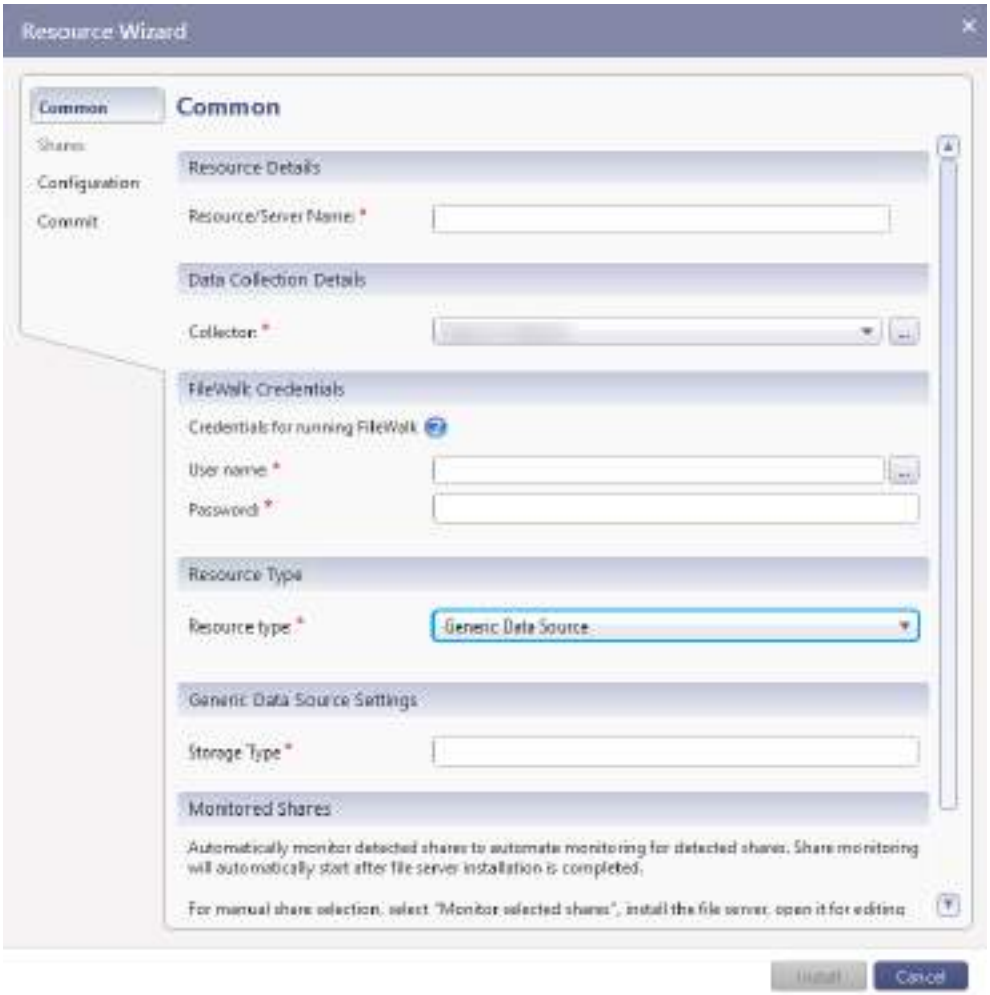
Now that you've fulfilled the requirements, you can deploy a Generic data source.

> Note: Each Generic data source represents a monitored Generic Server. In some cases, the Varonis UI displays the term File Server or Resource instead of Data Source. To monitor multiple Generic servers, add a Generic data source per Generic server.

1. Set common data source parameters

1. In the Management Console, select Management > Components > Root > File Servers, and on the Resources toolbar on the File Servers tab, click Add.

The Resource Wizard is opened to the Common pane, where you can specify the data source and set the relevant parameters.



2. In the Common pane, set the following parameters:
   a. Resource Details - Specify the data source name.
   b. Data Collection Details - Select the relevant Collector from the dropdown list.
   c. FileWalk Credentials - Enter the credentials for running directory structure monitoring. File System operations include directory structure monitoring, event auditing (if set) and account enumeration on local accounts (if set).

      Note:
      - These credentials are cached, so that they are automatically entered if another data source is added during the same session.

      - User name - Type the name of the user account to be used for directory structure monitoring, event auditing, and local account enumeration.
      - Password - Type the account's password.

d. Resource Type - Select Generic Data Source from the dropdown list.

e. Generic Data Source Settings - Specify the data source type. The Storage Type field helps track usage and identify demand for new platforms.

f. Monitored Shares - Select whether to automatically monitor all detected shares or to monitor selected shares. Share monitoring will only start after the data source installation is completed, and share selection is only available after the data source installed and share detection is completed.

- Automatically monitor detected shares - Select this option to automate monitoring for all detected shares. Share monitoring will automatically start after the data source installation is completed. Varonis will monitor all shares that aren't marked as "ignored". When this option is selected, click the Advanced setting link to modify share detection preferences. By default, the option is set to Prefer regular shares over equivalent admin shares. In this case, an admin share that has an equivalent regular share will be marked as "ignored" and the equivalent regular share will be detected for monitoring. Note: Any change in the monitored shares configuration, including the detection method, admin shares configuration, and selected shares, requires rerunning the resource detection.
- Monitor selected shares - This option is selected by default. You can manually select the shares to be monitored only after the data source is installed and share detection is completed. You'll need to open the Edit window for the installed data source and select the shares. For more information, see Post-installation share detection and registration.

Once the above settings are configured, you can proceed to review and adjust configuration settings.

2. Review and adjust configuration settings

1. On the left menu, click Configuration and confirm the information.
   The general configuration settings are displayed.
2. In the Local Accounts area, review the options:
   - Collect information regarding local accounts from this file server - Select this checkbox to collect user accounts from this file system.
3. In the FileWalk Settings area, review the options:
   - Identify actual unique folders and file system inconsistencies - Select this checkbox (if it not already selected) to detect broken permissions in NTFS file systems.

3. (Optional) Customize commit credentials

You can use different commit credentials instead of the default FileWalk credentials.

1. On the left menu, select Commit.
   The commit settings are displayed.
2. (Optional) Clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for running directory structure monitoring (FileWalk) and enter the relevant credentials. (By default, this checkbox is selected to use the FileWalk credentials, and the User name and Password fields are disabled for editing.)

   Note:
   - If credentials were not entered but the checkbox was cleared, the FileWalk credentials in the Common pane will be used instead.
   - If the Collector is in a lower version than 8, the FileWalk credentials will be used.
3. In the Group OU area, if required, select Uniquely defined to choose a different OU from that defined in the data source's domain. Click the Browse button (...) to select the required OU.

4. Install the data source

After configuration is complete, click Install to install the data source.

A prerequisite check is run. When completed, the Prerequisite window closes, and the installation status is displayed in the Status column in the File Servers pane. When the installation completes, the status shows "Installed 100%".

5. Post-installation share detection and registration

After the data source installation and share detection are completed, you can select the shares to be monitored. If, when adding the data source, you chose to automate monitoring for detected shares, all shares will be monitored. The following procedure describes the manual registration and automatic share detection flows.

Important: If after the data source is installed, share detection fails for any reason, the Share Detection Status column will remain "In Progress" until the issue is fixed, and share detection completes successfully at least once.

After the data source is installed, the Shares pane is enabled, and you can view the share settings.

1. On the left menu, click Shares.
   The share settings are displayed. The pane's heading indicates the option you selected when adding a data source.
2. In the Available Shares area, you can filter the shares based on the reason they are not registered for monitoring and easily identify the shares that can be added. The default filter is Accessible Shares. You can change the filter to see the rest of the shares. Options include:
   - Accessible shares - Can be added for monitoring (this option is selected by default)
   - Ignored shares - Are marked as "ignored"
   - Incompatible and inaccessible shares - Cannot be monitored since the exposed protocol does not match the security style of the volume (relevant to multiprotocol platforms only) or the Varonis service account does not have access to this share
   - Child share of a monitored share - Is monitored via its parent folder
3. Do one of the following:
   - If you chose to monitor selected shares, in the Available Shares area, select the required shares and click the down arrow. The selected shares are moved to the Registered Shares area. (The registered shares list is empty until you make your selections.)
   - If you chose to automatically monitor detected shares, Varonis will monitor all shares that aren't marked as "ignored". The automated share detection runs every few hours. The Registered Shares area is autopopulated with the shares to be monitored.
4. For each share, review and set the following information as required:
   - Ignore Detection - Select the shares to be ignored (and not be the subject of automatic detection and notifications) by the data source monitor.
   - Events - Select this checkbox to audit events for the share.
   - Crawl - To enable or disable monitoring for the share, in the Crawl column, select the relevant option.

     Note: You can also right-click the grid and select the required options for event auditing and crawling.
5. In the Additional Share Settings area, review the options:

- Remove deleted shares - Select this checkbox to remove deleted shares. Shares that were deleted from the data source will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the data source is unavailable, the shares will not be removed.
- Enable event auditing - Select this checkbox to audit events from all shares added from this data source.

After share detection and registration are completed, the status and number of registered volumes are respectively displayed in the Share Detection Status and Registered Shares columns in the File Servers pane.

25 APPENDIX - CREATING AN ENTRA ID APPLICATION FOR MONITORING M365 VIA THE ADMIN CENTER

We recommend that you create a new Entra ID application "automatically" via the Varonis Management Console, as described in the detailed procedures for adding an Entra ID, SharePoint Onine, OneDrive, and Exchange Online data source. However, if you prefer to use an existing Entra ID application, you need to manually create it via the Microsoft Entra admin center, as described in the following topics:

- Creating an Entra ID Application for Monitoring Entra ID via the Admin Center
- Creating an Entra ID Application for Monitoring SharePoint Online via the Admin Center
- Creating an Entra ID Application for Monitoring OneDrive via the Admin Center
- Creating an Entra ID Application for Monitoring Exchange Online via the Admin Center

Creating An Entra ID Application For Monitoring Entra ID Via The Admin Center

We recommend that you create a new Entra ID application "automatically" via the Varonis Management Console, as described in Adding an Entra ID Data Source. However, if you prefer to use an existing Entra ID application, you need to manually create it via the Microsoft Entra admin center, as described in the following topics:

- Creating an Entra ID Application for Monitoring Entra ID - Summary
- Creating an Entra ID Application for Monitoring Entra ID - Detailed Procedure

Creating an Entra ID Application for Monitoring Entra ID - Summary

This section describes the procedure for manually creating the Entra ID application in the Microsoft Entra admin center. The Entra ID application will be used by Varonis to monitor Entra ID.

1. Go to the Microsoft Entra admin center.
2. In Entra ID, go to App registrations > New registration > Accounts in this organizational directory only > Register.
3. Set a name for this application.
4. Copy and save the following values for later use:
   a. Application ID = Application (client) ID
   b. Tenant ID = Directory (tenant) ID
5. Add permissions as explained in Entra ID Requirements.
6. Click Grant admin consent for (your tenant name) and confirm your request.
7. Create a secret as follows:
   a. API permissions > Certificates & secrets > New client secret.
   b. Add a description for the client secret and set the Expires dropdown list to 24 months.
   c. Click Add.
   d. Copy and save the Value string.
8. Add a platform as follows:
   a. Authentication > Add a platform > Mobile and desktop applications.
   b. Enter https://login.microsoftonline.com/common/oauth2/nativeclient in the Custom redirect URIs field, and then click Configure.

What To Do Next

Now that you're familiar with the deployment steps, it's time to dive into the detailed procedure.

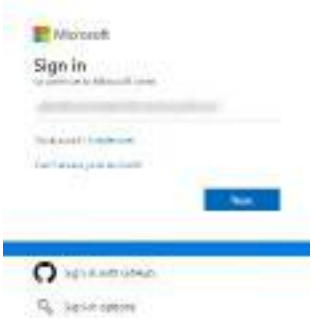
Creating an Entra ID Application for Monitoring Entra ID - Detailed Procedure

This section describes the procedure for manually creating the Entra ID application in the Microsoft Entra admin center. The Entra ID application will be used by Varonis to monitor Entra ID.

1. Access the Microsoft Entra admin center

1. Go to the Microsoft Entra admin center.
2. Log in using an account with permissions to create applications in Entra ID.

> Note: To complete the Entra ID application creation process, one of the following user accounts is required:
>
> - Global Administrator
> - Application administrator
> - Application developer
> - Cloud application administrator
>
> To grant consent to an application, a user account with Global Administrator privileges is required.
>
> If you are not using one of these accounts, make sure the holder of a suitable account is present during the session.





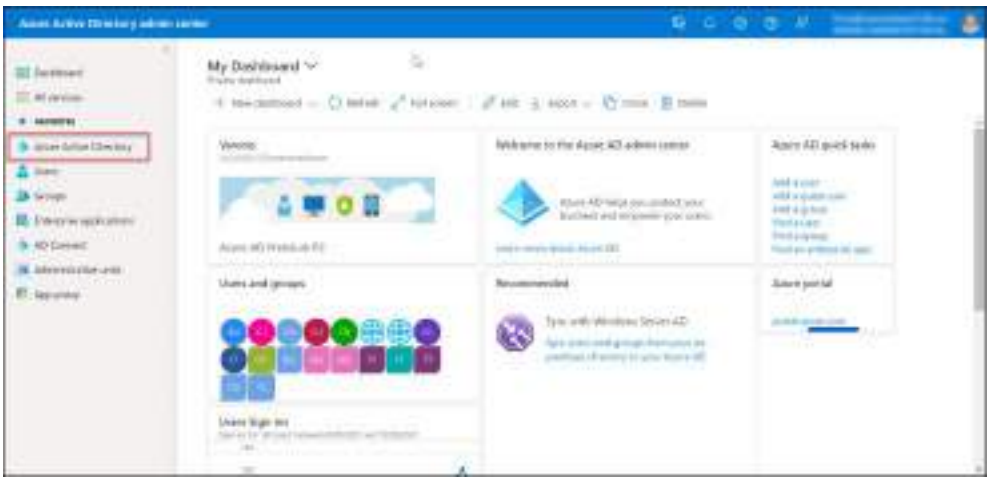
3. If you are using an account with MFA enabled, you will be prompted to enter a code. Enter the code and click Verify.



The Home page is displayed.

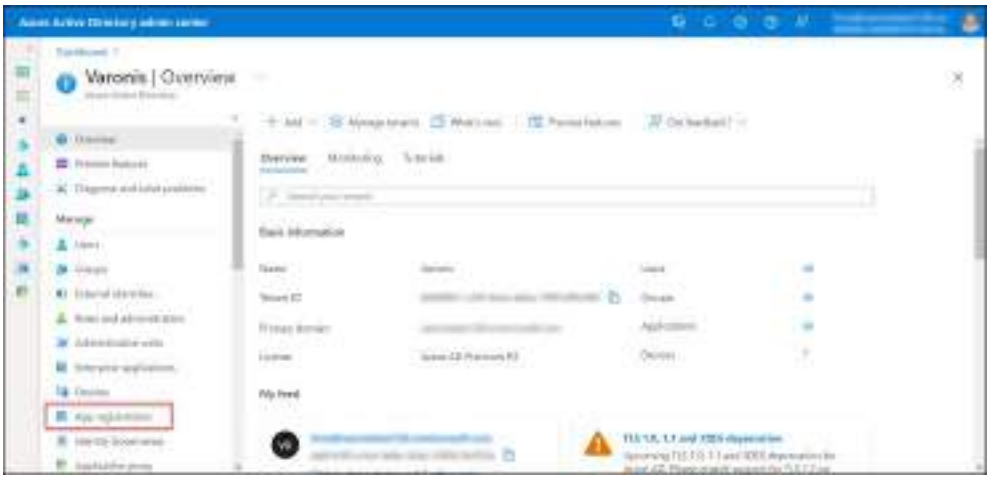
2. Create a new application

1. Select Azure Active Directory.



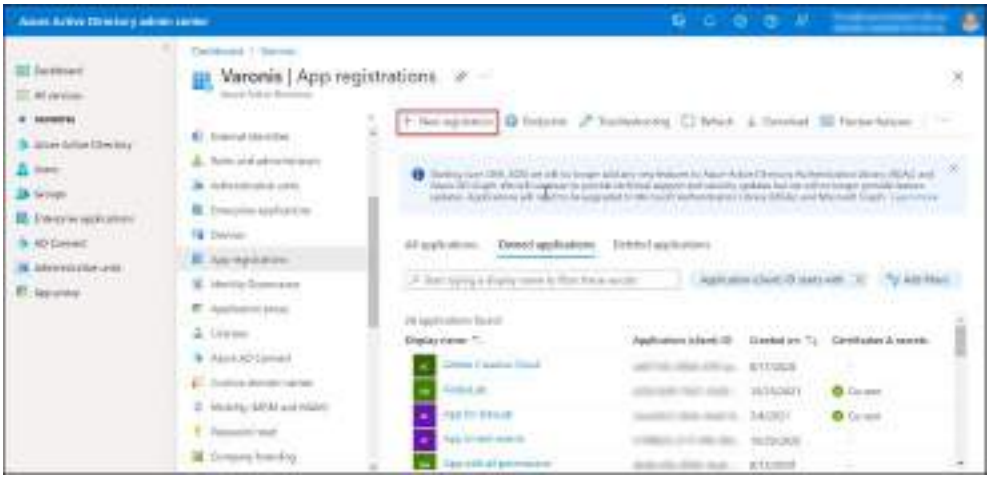
The Overview page is displayed.

2. Select App Registrations.



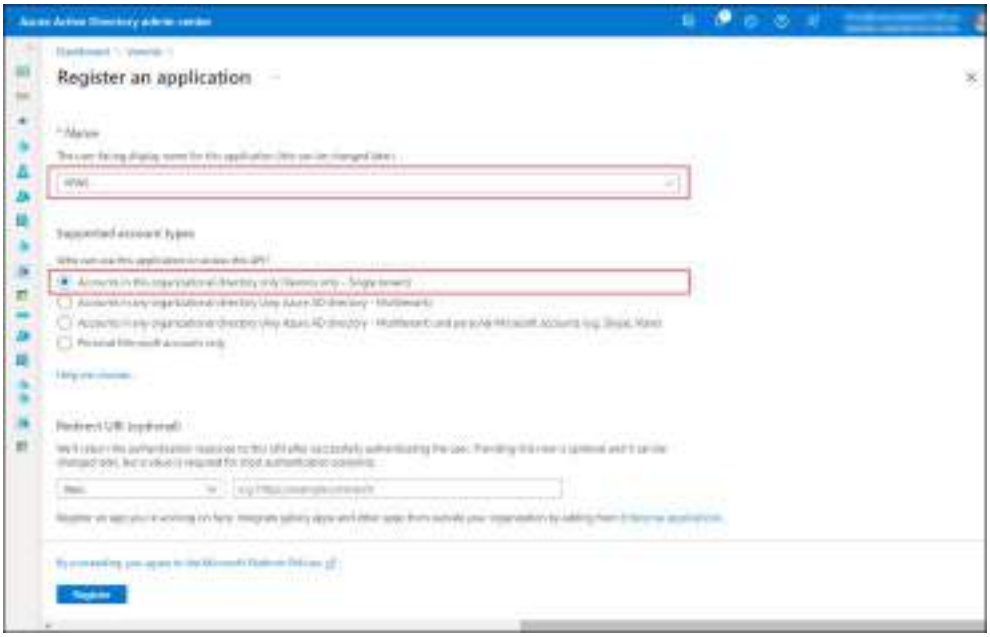
The App registrations page is displayed.

3. Select New registration.

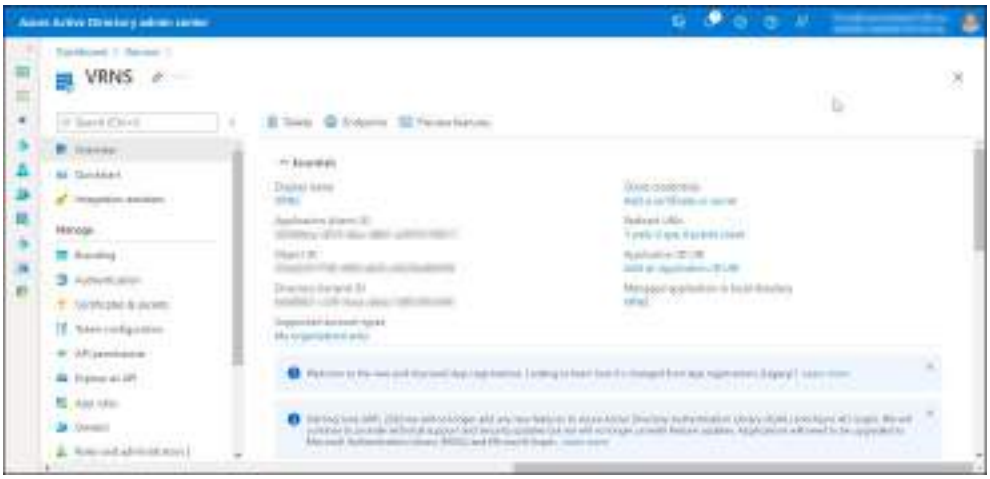


The Register an application page is displayed.

4. Configure the application as follows:
   - In the Name field, set a name for this application. For example, VRNS.
   - In the Supported account types section, select Accounts in this organizational directory only (… Single tenant).

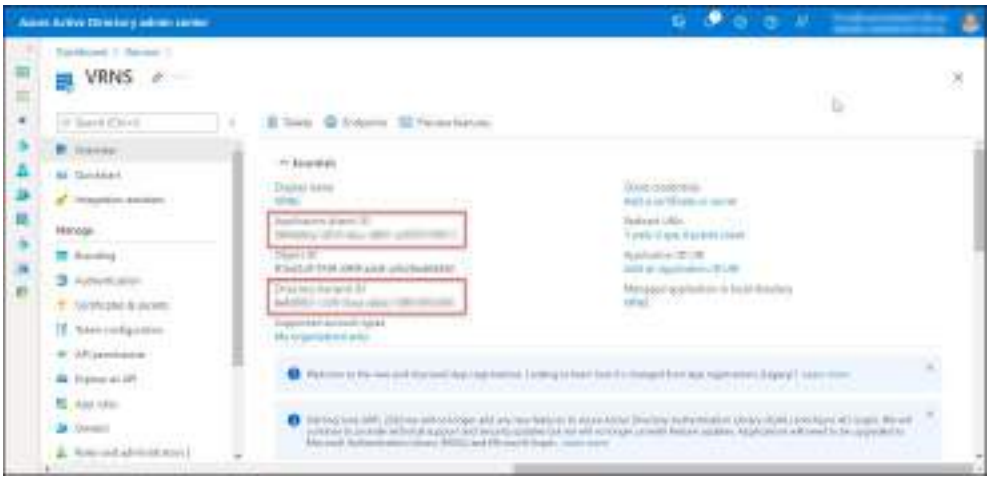


5. Click Register.
   The application is created and the application configuration page is displayed.



6. Copy and save the Application (client) ID (the application ID) and Directory (tenant) ID (the tenant ID) for later use.

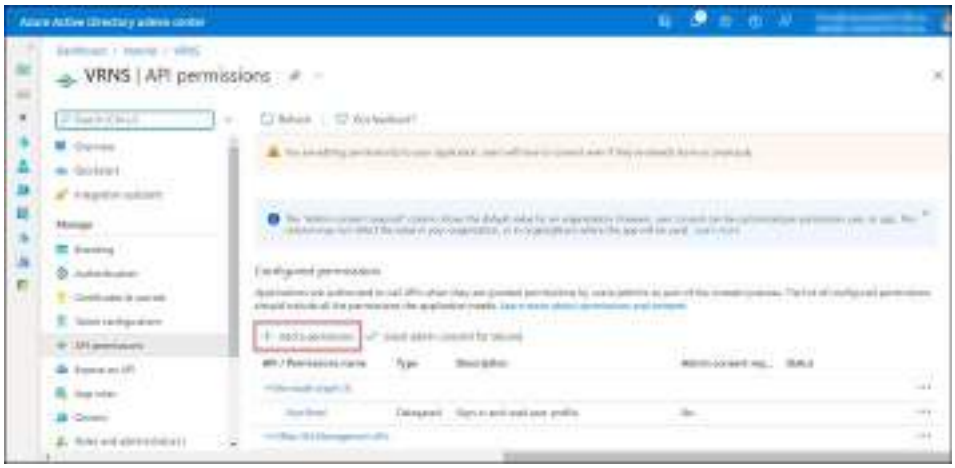
Note: The application ID and the tenant ID are required when adding the Entra ID application to the Entra ID domain in the Management Console.



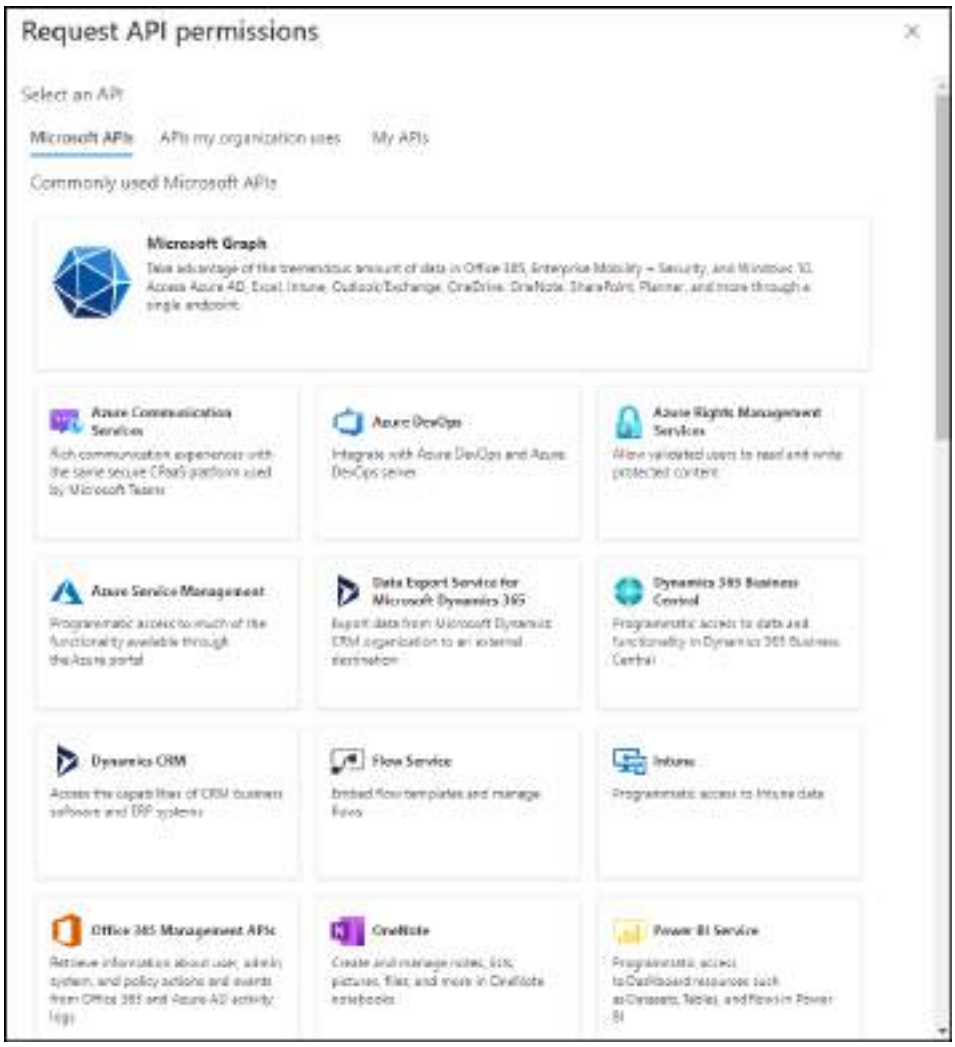
3. Add and grant API permissions

1. Click API permissions to set up permissions for the application.
   The API permissions page is displayed.
   You will now add the permissions as explained in Entra ID Requirements.
2. Add all the required Microsoft Graph or Office 365 Management API permissions.
   For example, to add the Microsoft Graph - Directory.ReadWrite.All permission (for reading writing directory data):

a. Click Add a permission.



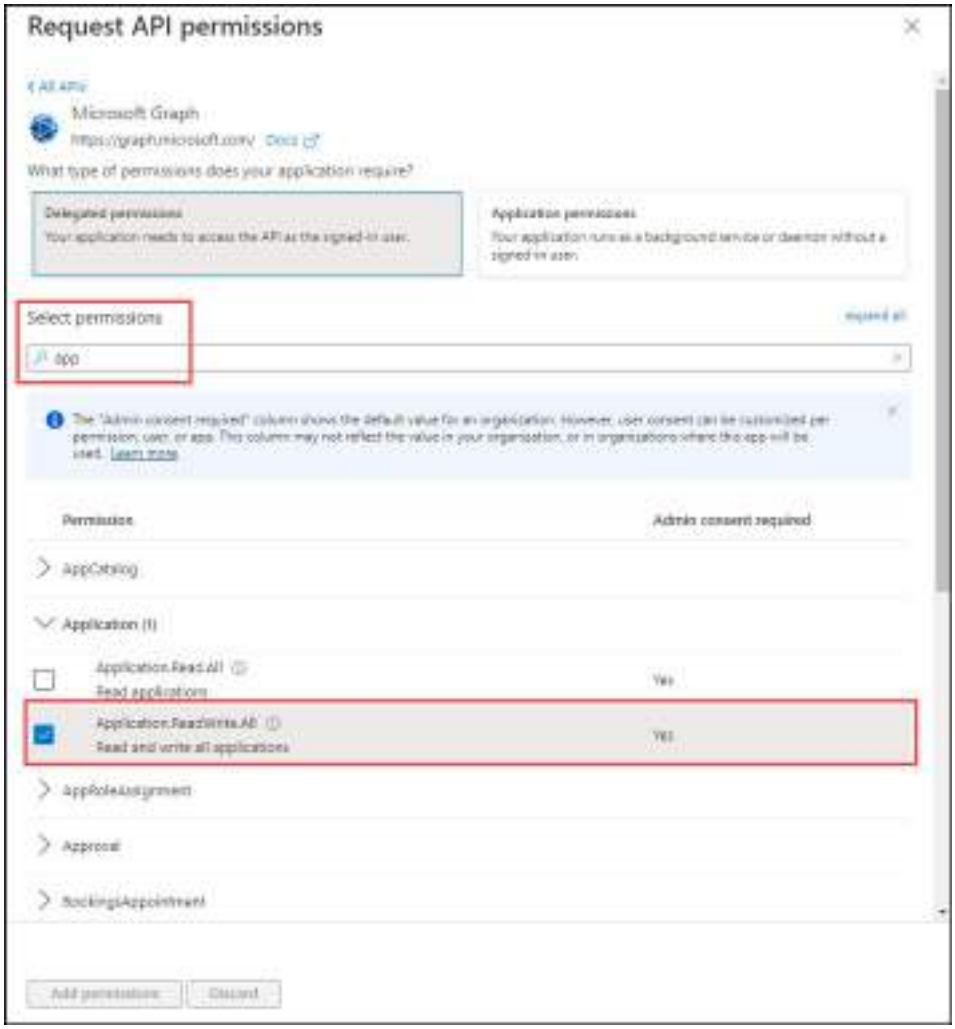
The Request API permissions page is displayed.



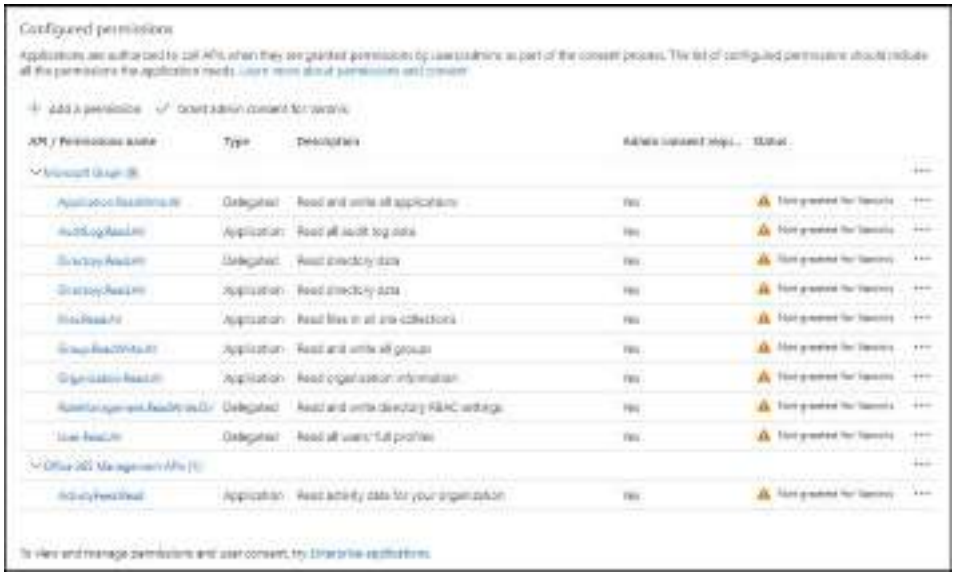
b. In the Request API permissions page, click the relevant API pane (Microsoft Graph or Office 365 Management API).

c. Select Delegated permissions or Application permissions, as necessary.

d. In the Select permissions search box, start typing the name of the permission, then select the permission from the Permission list. For example:

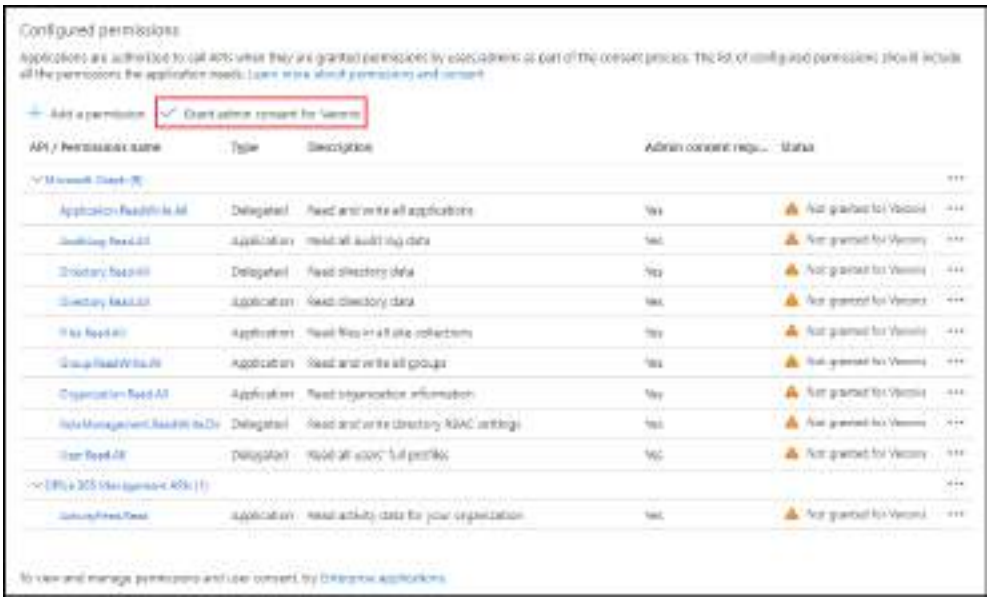


e. Click Add permissions.
The newly added permission is displayed in the Configured permissions table.



3. Once you are done adding all the required permissions, in the Configured permissions section of the API permissions page, click Grant admin consent for (your tenant name).
   To grant consent to an application, a user account with Global Administrator privileges is required.

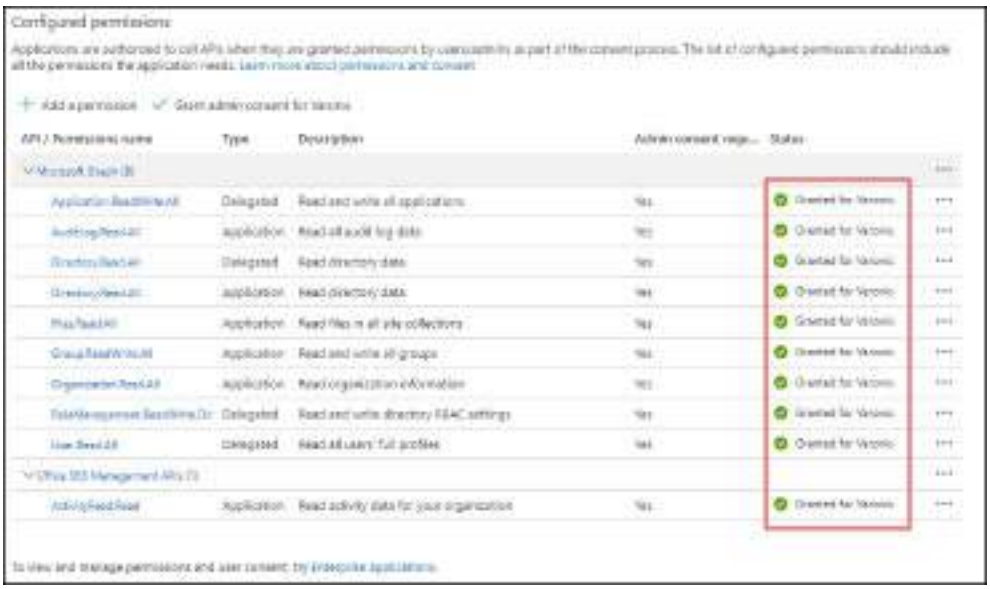
   > Important: Until consent is granted, Varonis flows cannot use the Entra ID applications and will fail.



4. Click Yes to confirm your request.

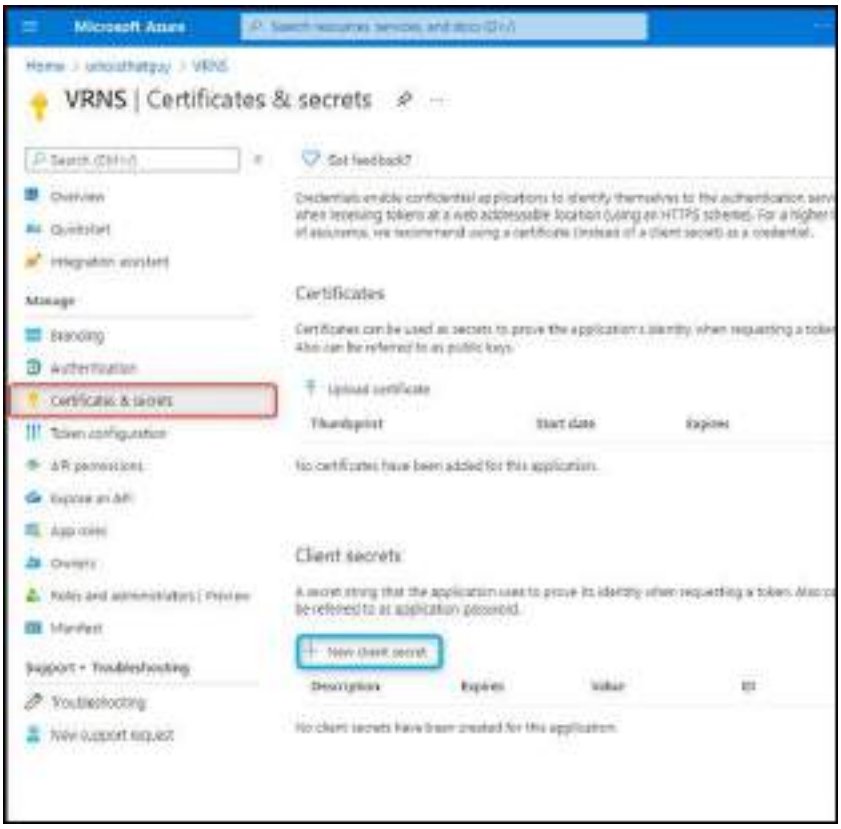


Administrator consent is granted for the permissions.



4. Add a client secret

1. Click Certificates & secrets to add a client secret.
   The Certificates & secrets page is displayed.



2. Click New client secret.
3. Type a description for the client secret and select 24 months (the maximum allowed) from the Expires dropdown list.



4. Click Add.
   The secret key is displayed in the Value column of the Client secrets table.



5. Copy the key value to the clipboard and then to a text file.

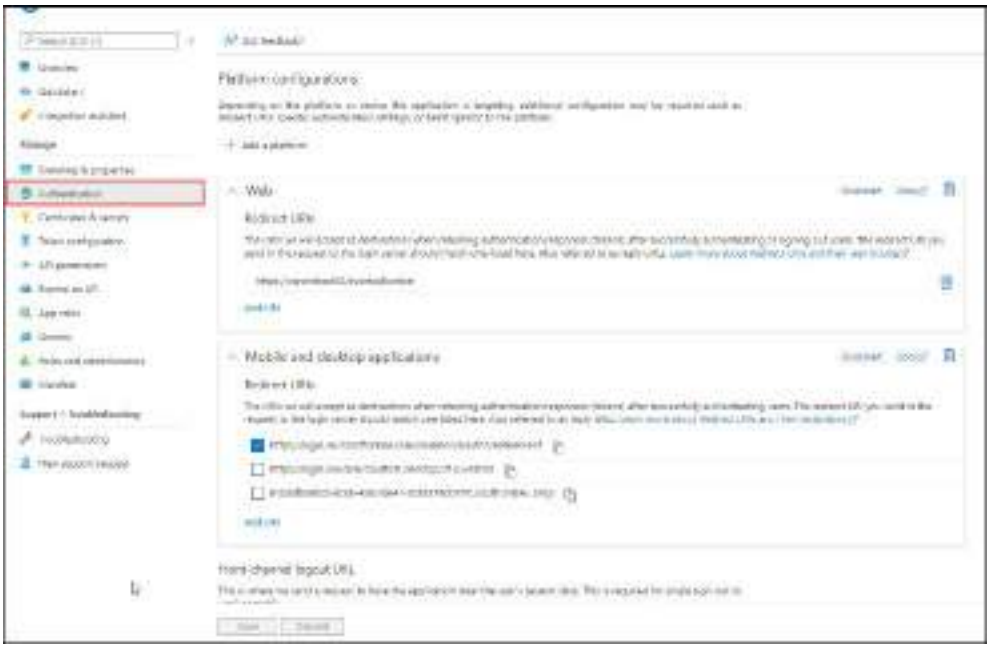
> Note: You cannot copy the secret key value after you have finished the Entra ID application creation procedure. If you do not copy the secret key value, you will need to create a new secret key later.

This secret will be used during the Entra ID domain configuration in the Management Console, along with application ID. Since the secret is set to expire after 24 months, be sure to renew it both in the Microsoft Entra admin center and in the Varonis Management Console, as explained in Renewing the Secret of your Entra ID Application.

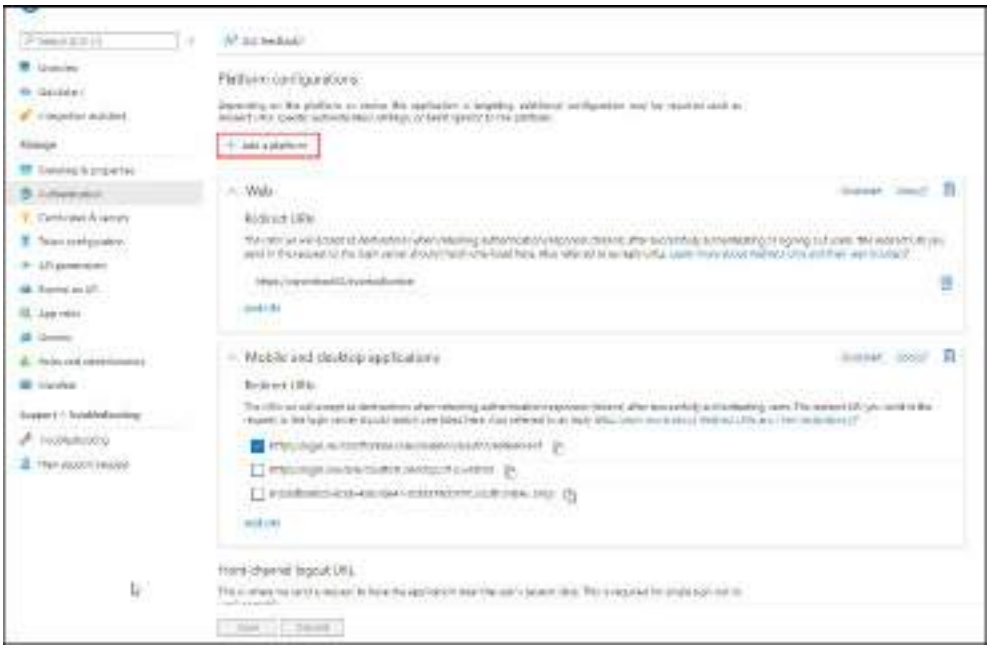
5. Configure Authentication for a platform

Now you must configure authentication for a platform to allow Varonis to use the permissions for automatically creating SharePoint Online and OneDrive applications.

1. Click Authentication to add a platform.



2. Click Add a platform.



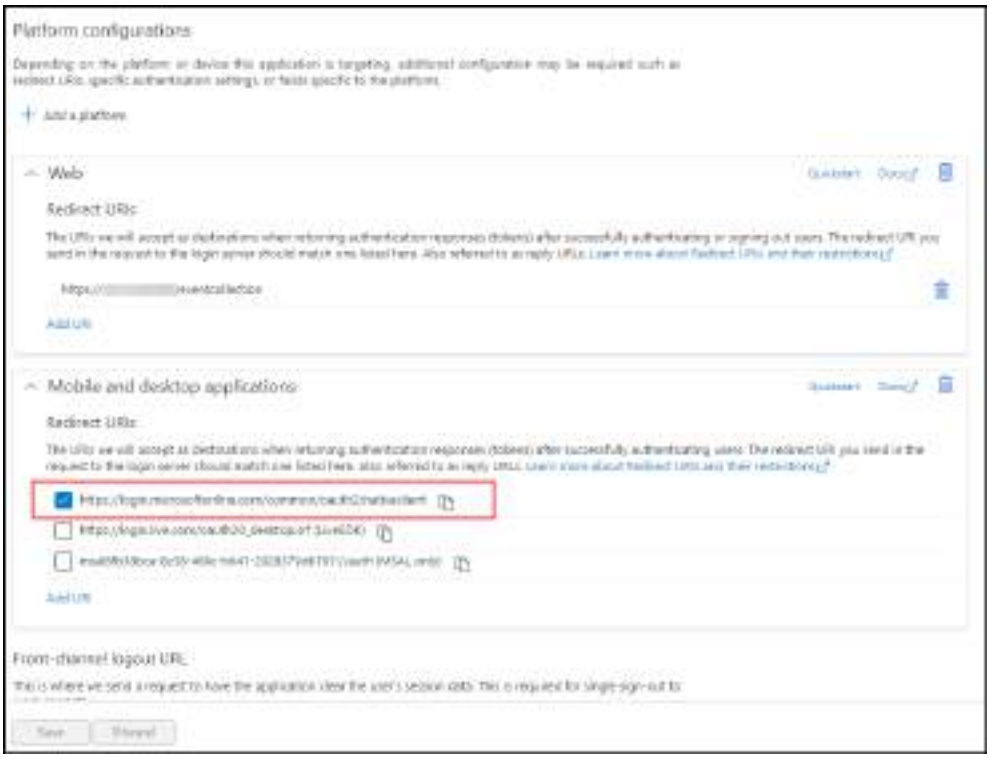
3. In the Configure platforms page, select Mobile and desktop applications.



4. In the Configure Desktop + devices page, enter https://login.microsoftonline.com/common/oauth2/nativeclient in the Custom redirect URIs field, and then click Configure.



The new URI appears in the Mobile and desktop applications section of the Platform configurations page.



What To Do Next

Remember: To add the Entra ID data source in the Management Console, have the following values ready from this procedure:

- Tenant ID from the Directory (tenant) ID value
- Application ID from the Application (client) ID value
- Secret key value

Creating An Entra ID Application For Monitoring SharePoint Online Via The Admin Center

We recommend that you create a new Entra ID application "automatically" via the Varonis Management Console, as described in Adding a SharePoint Online Data

Source - Detailed Procedure. However, if you prefer to use an existing Entra ID application, you need to manually create it via the Microsoft Entra admin center, as described in the following topics:

- Creating an Entra ID Application for Monitoring SharePoint Online - Summary
- Creating an Entra ID Application for Monitoring SharePoint Online - Detailed Procedure

Creating an Entra ID Application for Monitoring SharePoint Online - Summary

This section describes the procedure for manually creating the Entra ID application in the Microsoft Entra admin center. The Entra ID application will be used by Varonis to monitor SharePoint Online.

1. Go to the Microsoft Entra admin center.
2. In Entra ID, go to App registrations > New registration > Accounts in this organizational directory only > Register.
3. Set a name for this application.
4. Copy and save the Application (client) ID (the application ID) for later use.
5. Add permissions as explained in SharePoint Online Requirements.
6. Add a certificate.

What To Do Next

Now that you're familiar with the deployment steps, it's time to dive into the detailed procedure.

Creating an Entra ID Application for Monitoring SharePoint Online - Detailed Procedure

This section describes the procedure for manually creating the Entra ID application in the Microsoft Entra admin center. The Entra ID application will be used by Varonis to monitor SharePoint Online.

1. Access the Microsoft Entra admin center

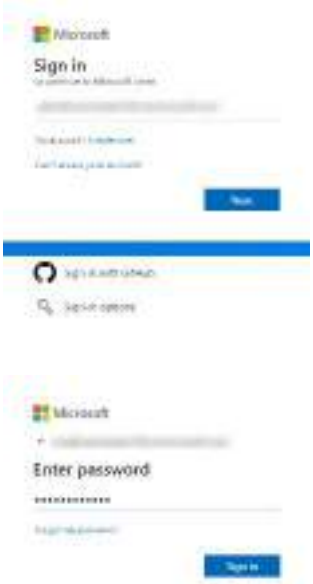
1. Go to the Microsoft Entra admin center.
2. Log in using an account with permissions to create applications in Entra ID.

Note: To complete the Entra ID application creation process, one of the following user accounts is required:

- Global Administrator
- Application administrator
- Application developer
- Cloud application administrator

To grant consent to an application, a user account with Global Administrator privileges is required.

If you are not using one of these accounts, make sure the holder of a suitable account is present during the session.



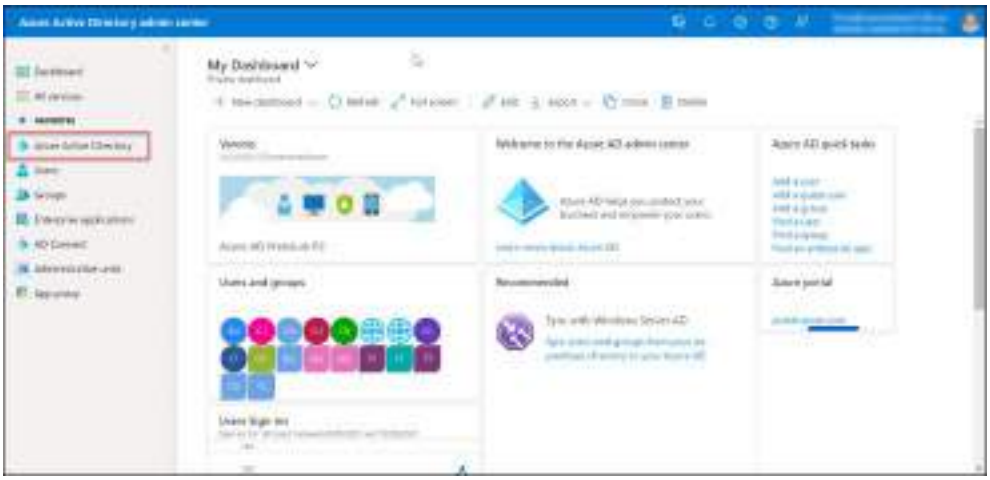
3. If you are using an account with MFA enabled, you will be prompted to enter a code. Enter the code and click Verify.



The Home page is displayed.

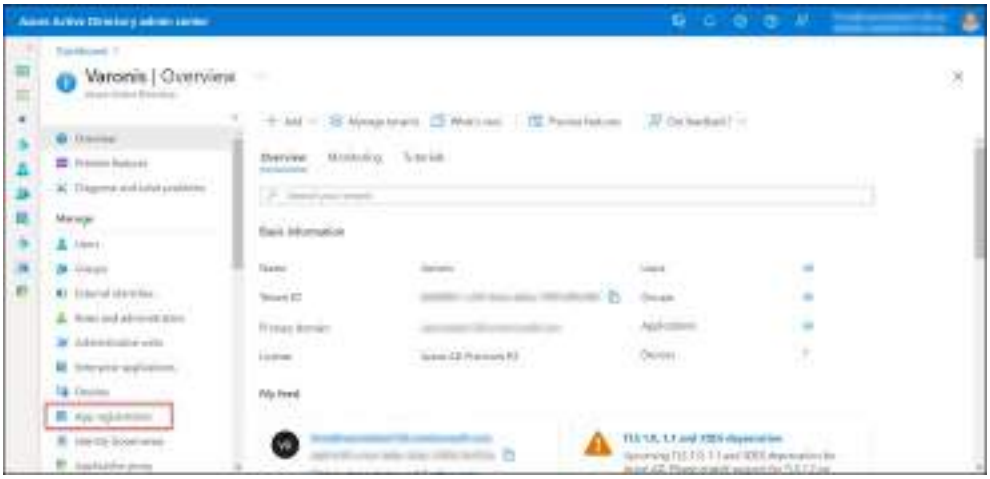
2. Create a new application

1. Select Azure Active Directory.



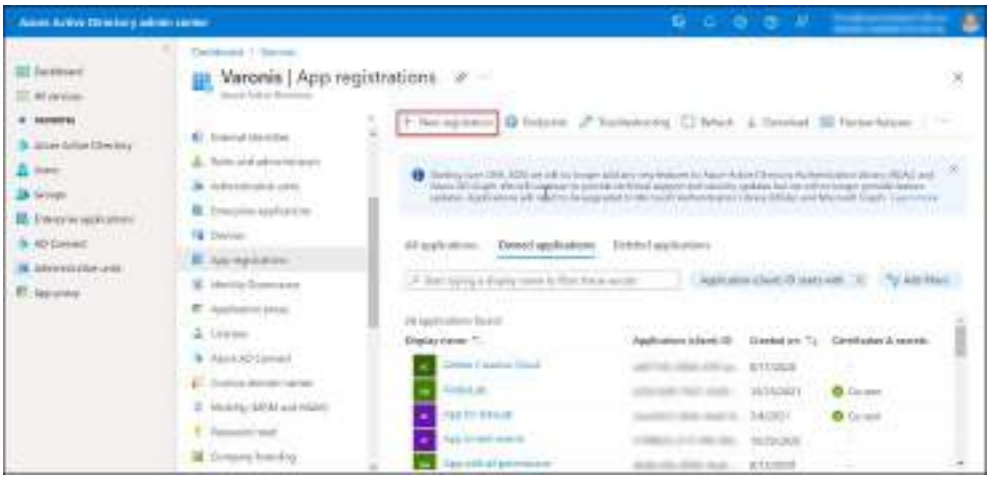
The Overview page is displayed.

2. Select App Registrations.



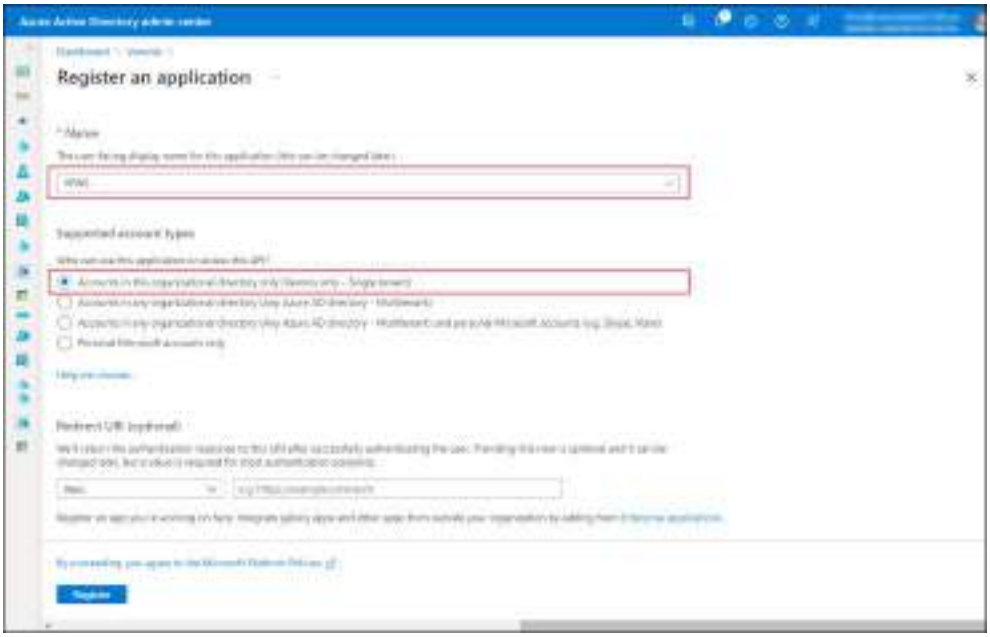
The App registrations page is displayed.

3. Select New registration.

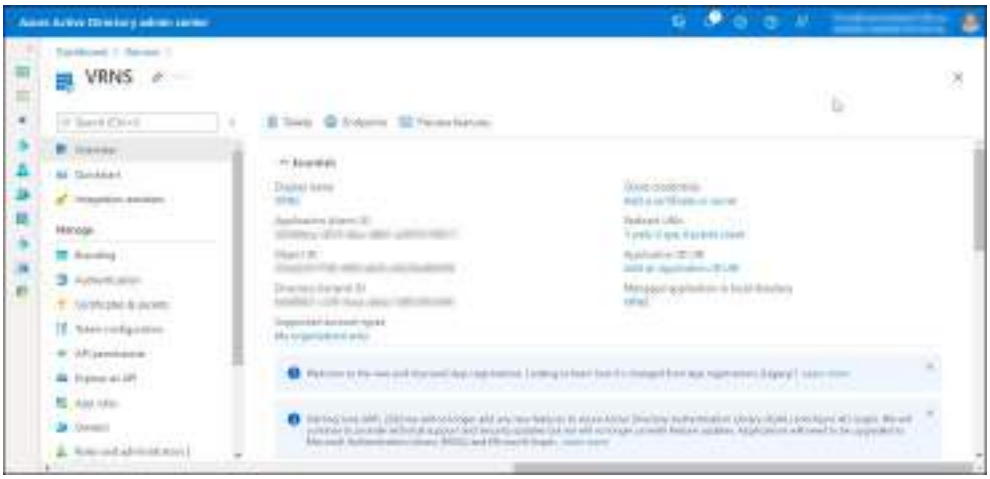


The Register an application page is displayed.

4. Configure the application as follows:
   - In the Name field, set a name for this application. For example, VRNS.
   - In the Supported account types section, select Accounts in this organizational directory only (… Single tenant).

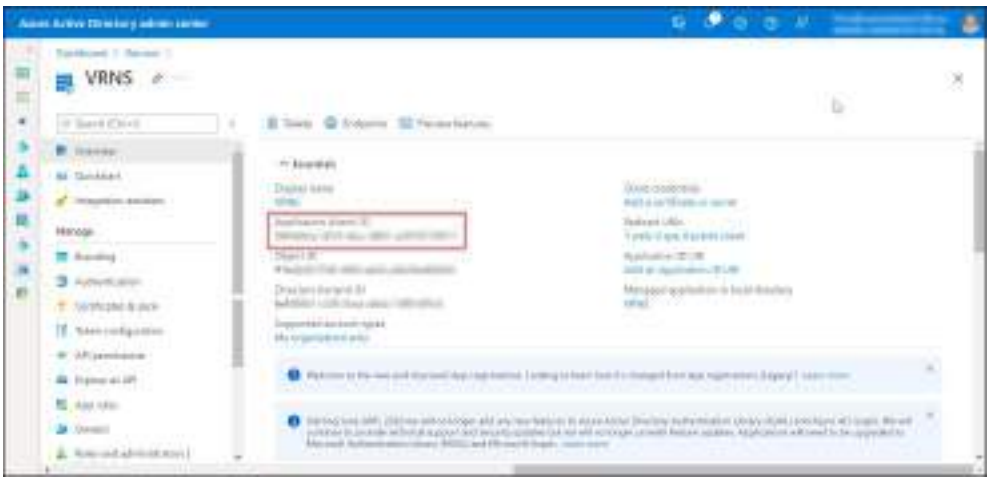


5. Click Register.
   The application is created and the application configuration page is displayed.



6. Copy and save the Application (client) ID (the application ID) value for later use.

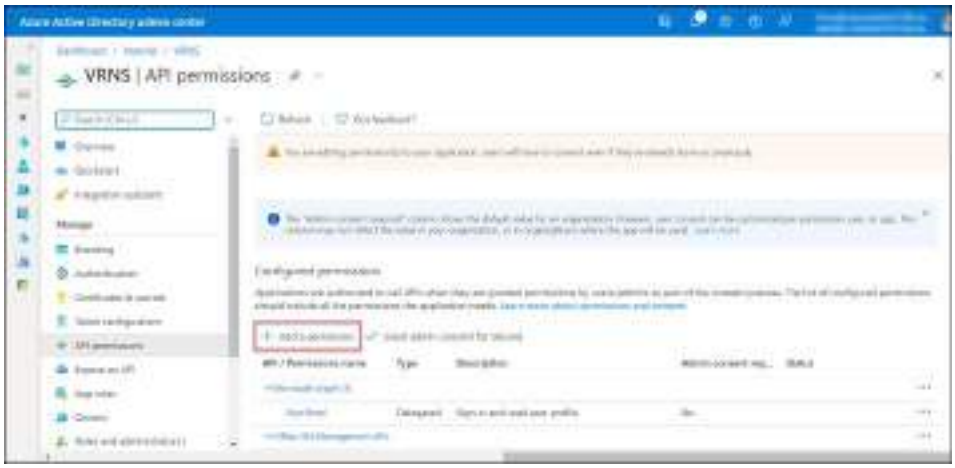
Note: The application ID is required when adding the Entra ID application to the SharePoint Online data source in the Management Console.



3. Add and grant API permissions

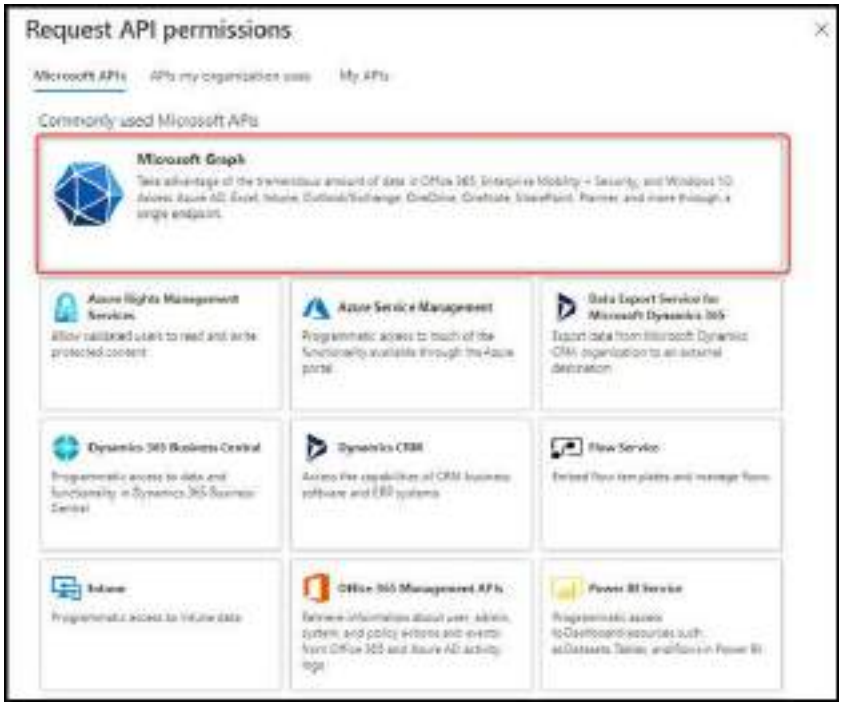
1. Click API permissions to set up permissions for the application.
   The API permissions page is displayed.
   You will now add permissions as explained in SharePoint Online Requirements.
2. Add all the required permissions.
   For example, to add the Microsoft Graph - Directory.Read.All permission (for reading directory data):

a. Click Add a permission.



The Request API permissions page is displayed.

b. Select Microsoft Graph.

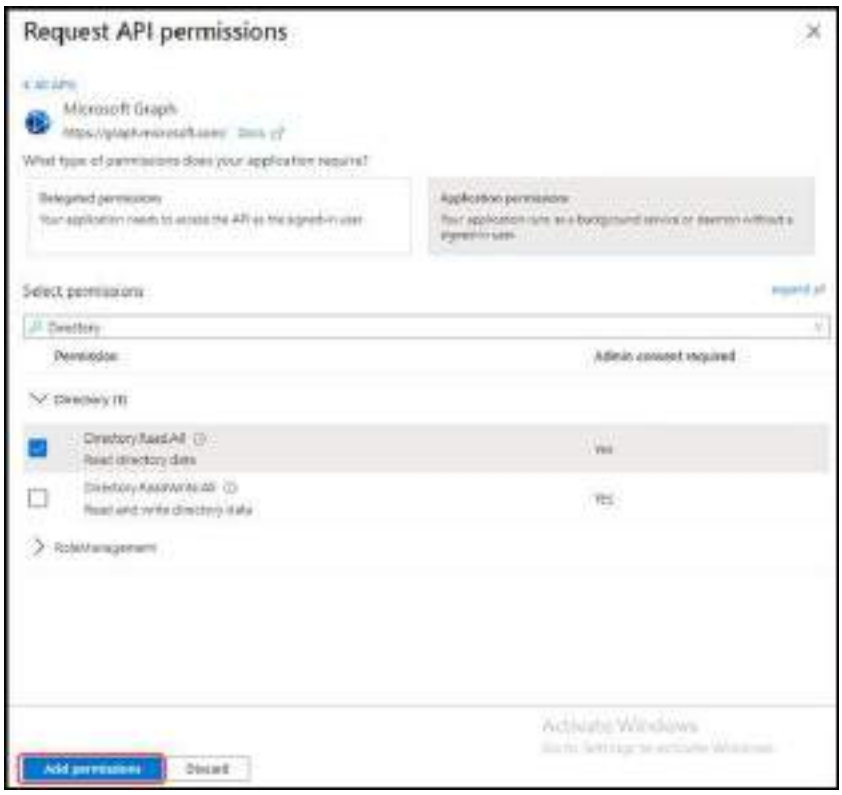


c. Select Application permissions.



d. In the search field, type Directory.

e. Under Directory, select Directory.Read.All and click Add permissions.



The newly added permission is displayed in the Configured permissions table.



3. Once you are done adding all the required permissions, in the Configured permissions section of the API permissions page, click Grant consent for (your tenant name).
   To grant consent to an application, a user account with Global Administrator privileges is required.

   > Important: Until consent is granted, Varonis flows cannot use the Entra ID applications and will fail.

4. Click Yes to confirm your request.



Administrator consent is granted for the permissions.



4. Add a certificate

1. Click Certificates & secrets to add a certificate.



You can use a purchased certificate signed by a certificate authority (recommended), or create a self-signed certificate.
For certificate authentication, Entra ID requires the following:

- Certificates in X.509 V3 format for client and server authentication.
- A key length of 2048 bits.
- Key usage digital signature and key encipherment.
- The RSA cryptographic algorithm.

- Certificates signed with the SHA256 hash algorithm.
- The CN (subject), issuer, and validity period fields should be set.

Note: Certificates exported without a private key in the CER or PEM file should be uploaded to the App registrations screen in Entra ID. Certificates with a password-encrypted private key in PFX format should be uploaded to the Collector when adding a file server (including the password of the PFX file).

To purchase a certificate signed by a certificate authority, see this example.
To create a self-signed certificate, follow these steps:

Note: The following PowerShell commands are compatible with PowerShell 5.1 and Windows Server 2016. For older Windows Server versions, see Microsoft documentation.

a. Open Windows PowerShell Integrated Scripting Environment (ISE) as an administrator.

b. Run the following commands:

Important: When copying the following PowerShell commands from this document, line breaks may be mistakenly added. Make sure to remove the line breaks, so that each command line resides on a single line. Otherwise, the commands may fail.

```
$notAfter = (Get-Date).AddMonths(24) # Valid for 24 mon
ths
```

```
$cer = \Qi0 VipjVmkrihEivxm gate -Subject "CN=MyService
" -Provider "Microsoft Enhanced RSA and AES Cryptograph
ic Provider" -CertStoreLocation "cert:\LocalMachine\My"
 -KeyExportPolicy Exportable -NotAfter $notAfter -KeyLe
ngth 2048 -HashAlgorithm SHA256)
```

```
G1tsvx Eivxm gate -Type CERT -FilePath c:\cert5.cer -Ce
rt $cer
```

```
$mypwd = ConvertTo-SecureString -String "1234" -Force -
AsPlainText
```

```
G1tsvx Sj1Eivxm gate -FilePath c:\cert5.pfx -Password $
mypwd -Cert $cer
```

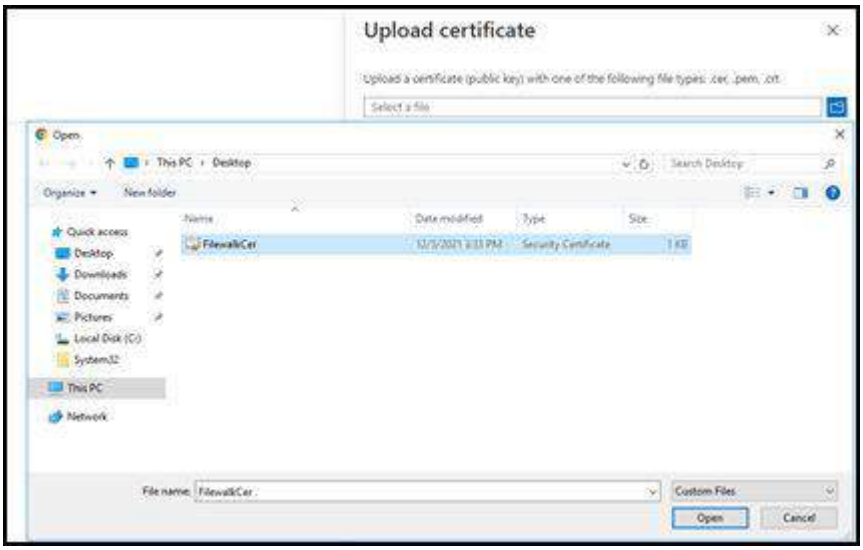
c. Configure the script as follows:

- In the first command line, set the expiration time of the certificate.
- In the second command line, the certificate is created.
- In the third command line, set the path to which to export the certificate CER file. This file will be uploaded later to Entra ID as part of the Entra ID application creation.
- In the fourth command line, set the password for encrypting the certificate PFX file.
- In the fifth command line, set the path to which to export the certificate PFX file. This file will be uploaded later to the Management Console.

2. When you have an available certificate, select the Certificates tab and click Upload certificate.



3. Select the certificate CER file, click Open and then click Add.



The certificate displays in the Certificates tab.



The application creation process is now complete.

What To Do Next

Remember: To add the SharePoint Online data source in the Management Console, have the following values ready from this procedure:

- Tenant ID from the Directory (tenant) ID value
- Application ID from the Application (client) ID value
- Certificate

Creating An Entra ID Application For Monitoring OneDrive Via The Admin Center

We recommend that you create a new Entra ID application "automatically" via the Varonis Management Console, as described in Adding a OneDrive Data Source - Detailed Procedure. However, if you prefer to use an existing Entra ID application, you

need to manually create it via the Microsoft Entra admin center, as described in the following topics:

- Creating an Entra ID Application for Monitoring OneDrive - Summary
- Creating an Entra ID Application for Monitoring OneDrive - Detailed Procedure

Creating an Entra ID Application for Monitoring OneDrive - Summary

This section describes the procedure for manually creating the Entra ID application in the Microsoft Entra admin center. The Entra ID application will be used by Varonis to monitor OneDrive.

1. Go to the Microsoft Entra admin center.
2. In Entra ID, go to App registrations > New registration > Accounts in this organizational directory only > Register.
3. Set a name for this application.
4. Copy and save the Application (client) ID (the application ID) for later use.
5. Add permissions as explained in OneDrive Requirements.
6. Add a certificate.

What To Do Next

Now that you're familiar with the deployment steps, it's time to dive into the detailed procedure.

Creating an Entra ID Application for Monitoring OneDrive - Detailed Procedure

This section describes the procedure for manually creating the Entra ID application in the Microsoft Entra admin center. The Entra ID application will be used by Varonis to monitor OneDrive.

1. Access the Microsoft Entra admin center

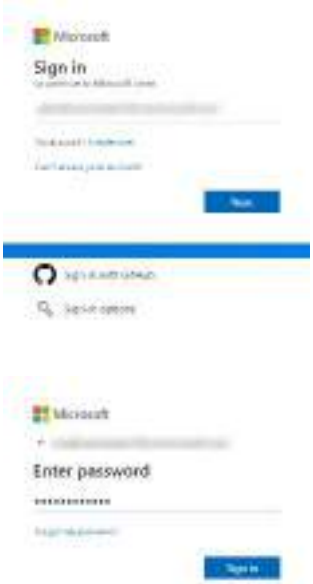
1. Go to the Microsoft Entra admin center.
2. Log in using an account with permissions to create applications in Entra ID.

> Note: To complete the Entra ID application creation process, one of the following user accounts is required:
>
> - Global Administrator

- Application administrator
- Application developer
- Cloud application administrator

To grant consent to an application, a user account with Global Administrator privileges is required.

If you are not using one of these accounts, make sure the holder of a suitable account is present during the session.



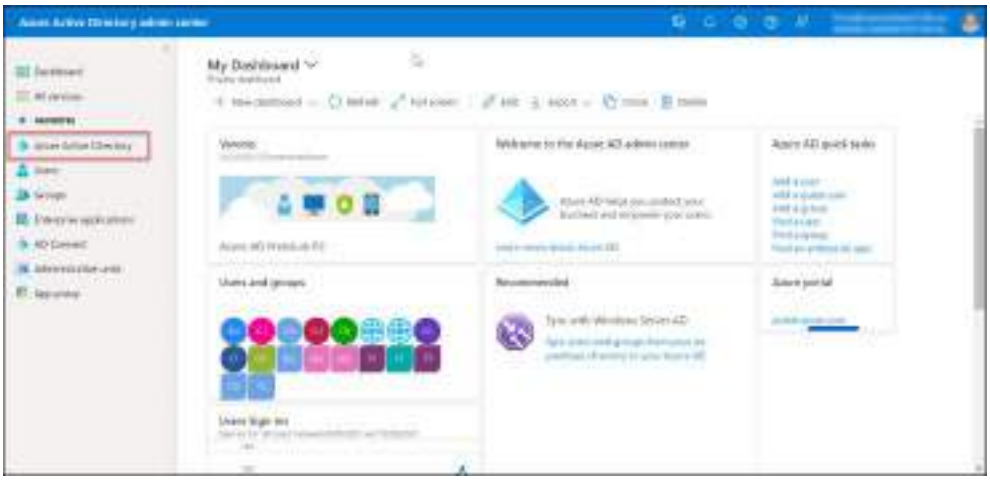
3. If you are using an account with MFA enabled, you will be prompted to enter a code. Enter the code and click Verify.



The Home page is displayed.

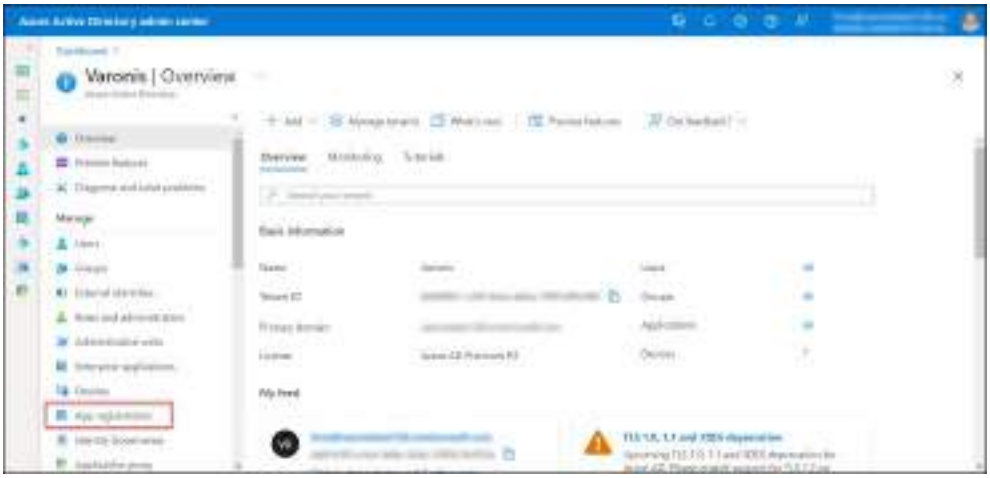
2. Create a new application

1. Select Azure Active Directory.



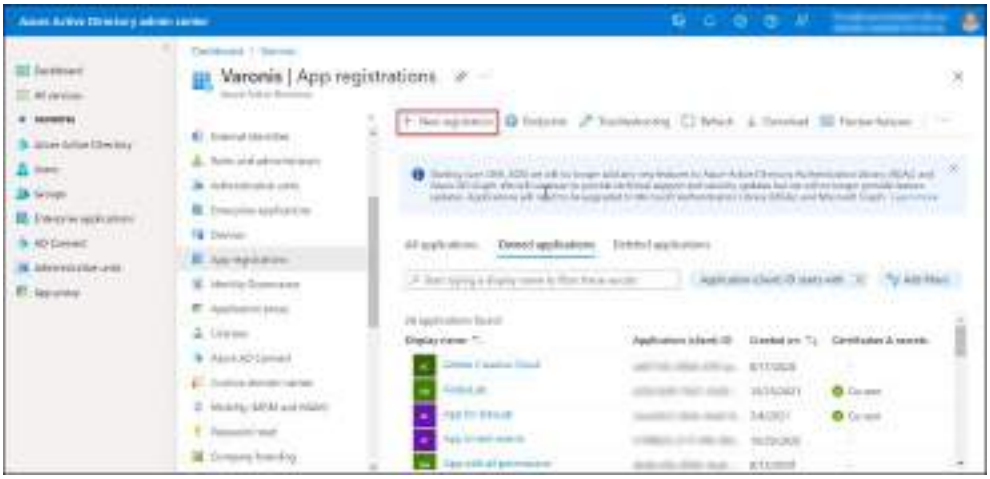
The Overview page is displayed.

2. Select App Registrations.



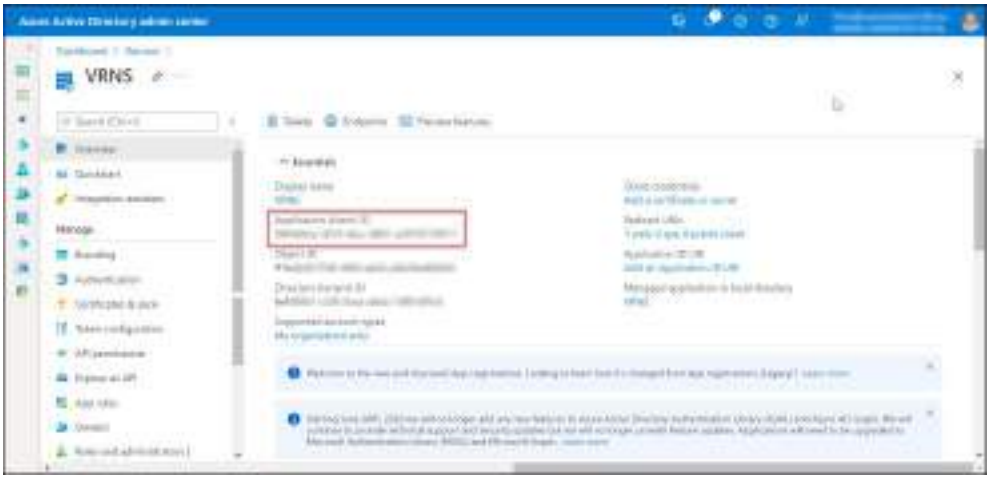
The App registrations page is displayed.

3. Select New registration.

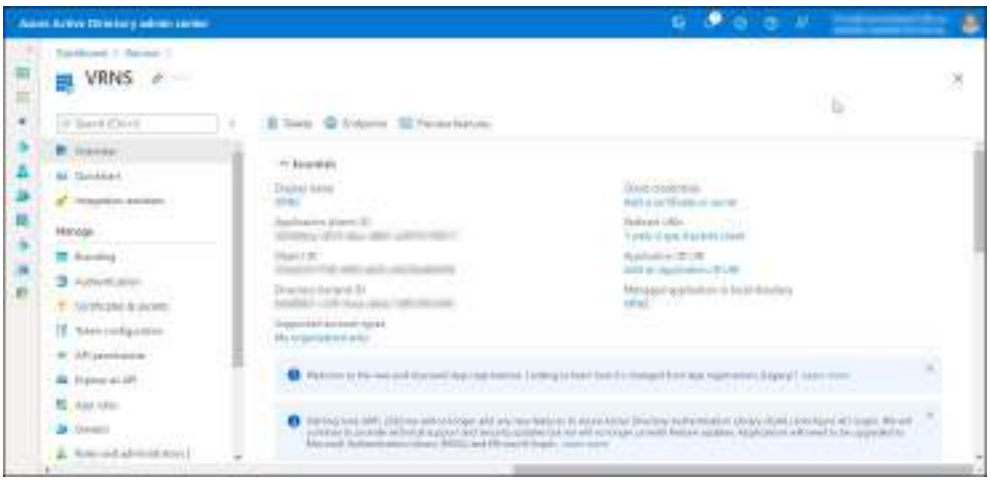


The Register an application page is displayed.

4. Configure the application as follows:
   - In the Name field, set a name for this application. For example, VRNS.
   - In the Supported account types section, select Accounts in this organizational directory only (… Single tenant).

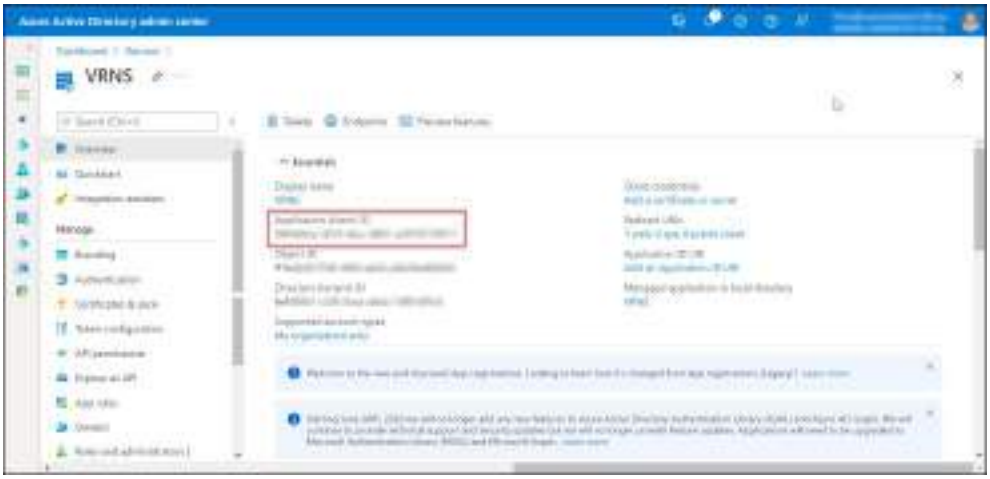


5. Click Register.
   The application is created and the application configuration page is displayed.



6. Copy and save the Application (client) ID (the application ID) value for later use.

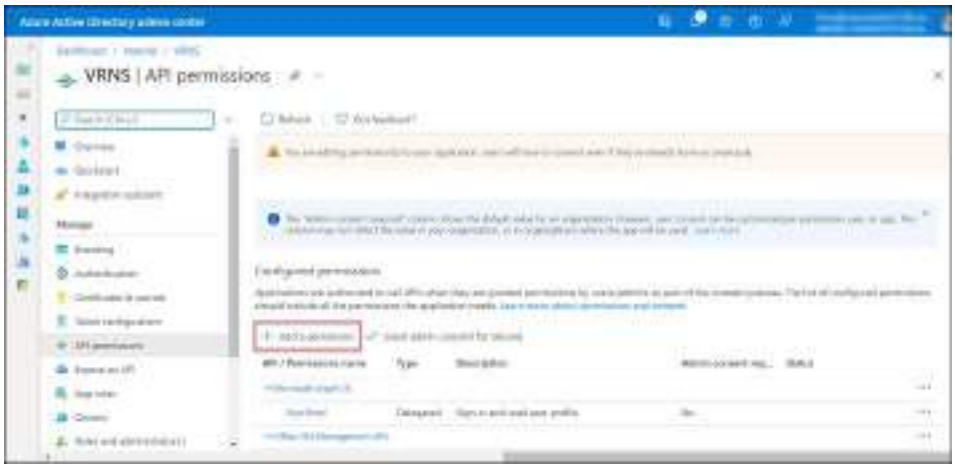
> Note: The application ID is required when adding the Entra ID application to the OneDrive data source in the Management Console.



3. Add and grant API permissions

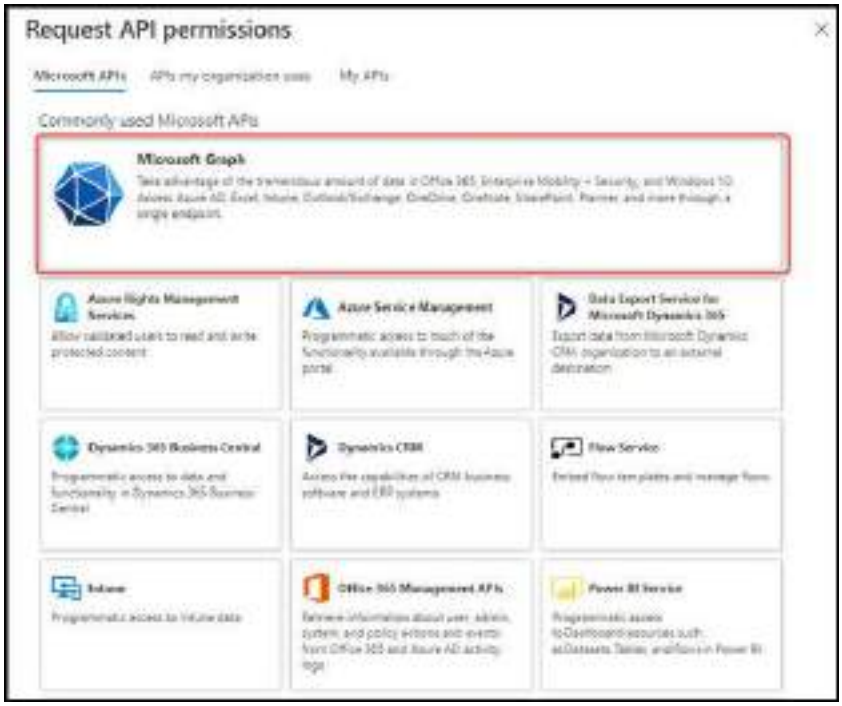
1. Click API permissions to set up permissions for the application.
   The API permissions page is displayed.
   You will now add permissions as explained in OneDrive Requirements.
2. Add all the required permissions.
   For example, to add the Microsoft Graph - Directory.Read.All permission (for reading directory data):

a. Click Add a permission.



The Request API permissions page is displayed.

b. Select Microsoft Graph.

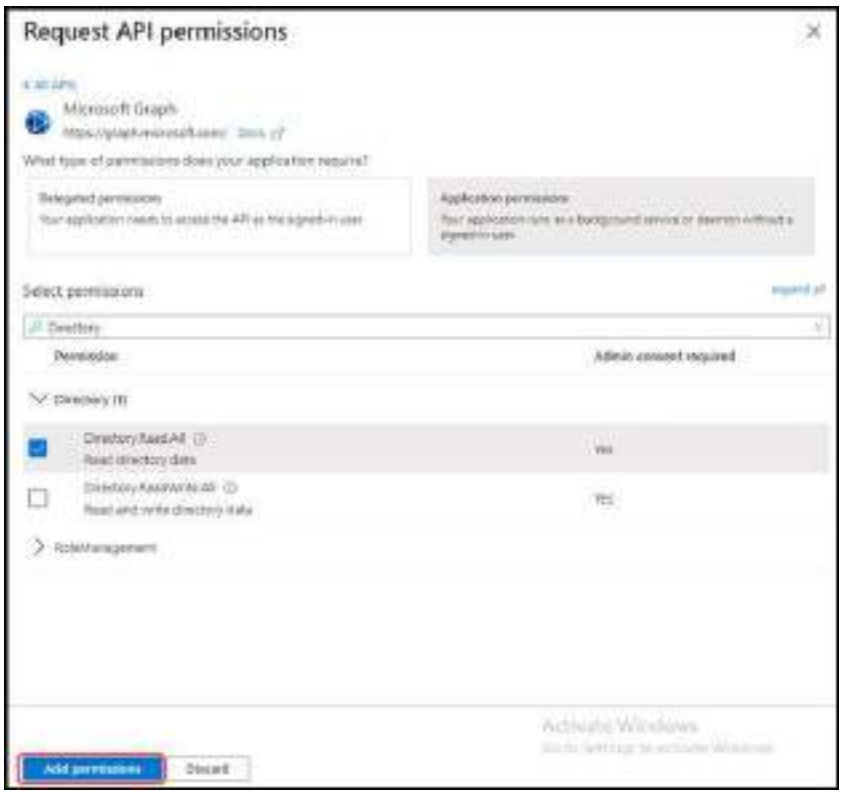


c. Select Application permissions.



d. In the search field, type Directory.

e. Under Directory, select Directory.Read.All and click Add permissions.



The newly added permission is displayed in the Configured permissions table.



3. Once you are done adding all the required permissions, in the Configured permissions section of the API permissions page, click Grant consent for (your tenant name).
   To grant consent to an application, a user account with Global Administrator privileges is required.

   > Important: Until consent is granted, Varonis flows cannot use the Entra ID applications and will fail.

4. Click Yes to confirm your request.



Administrator consent is granted for the permissions.



4. Add a certificate

1. Click Certificates & secrets to add a certificate.



You can use a purchased certificate signed by a certificate authority (recommended), or create a self-signed certificate.
For certificate authentication, Entra ID requires the following:

- Certificates in X.509 V3 format for client and server authentication.
- A key length of 2048 bits.
- Key usage digital signature and key encipherment.
- The RSA cryptographic algorithm.
- Certificates signed with the SHA256 hash algorithm.
- The CN (subject), issuer, and validity period fields should be set.

Note: Certificates exported without a private key in the CER or PEM file should be uploaded to the App registrations screen in Entra ID. Certificates with a password-encrypted private key in PFX format should be uploaded to the Collector when adding a file server (including the password of the PFX file).

To purchase a certificate signed by a certificate authority, see this example.
To create a self-signed certificate, follow these steps:

Note: The following PowerShell commands are compatible with PowerShell 5.1 and Windows Server 2016. For older Windows Server versions, see Microsoft documentation.

a. Open Windows PowerShell Integrated Scripting Environment (ISE) as an administrator.

b. Run the following commands:

> Important: When copying the following PowerShell commands from this document, line breaks may be mistakenly added. Make sure to remove the line breaks, so that each command line resides on a single line. Otherwise, the commands may fail.

```
$notAfter = (Get-Date).AddMonths(24) # Valid for 24 mon
ths
```

```
$cer = \Qi0 VipjVmkrihEivxm gate -Subject "CN=MyService
" -Provider "Microsoft Enhanced RSA and AES Cryptograph
ic Provider" -CertStoreLocation "cert:\LocalMachine\My"
 -KeyExportPolicy Exportable -NotAfter $notAfter -KeyLe
ngth 2048 -HashAlgorithm SHA256)
```

```
G1tsvx Eivxm gate -Type CERT -FilePath c:\cert5.cer -Ce
rt $cer
```

```
$mypwd = ConvertTo-SecureString -String "1234" -Force -
AsPlainText
```

```
G1tsvx Sj1Eivxm gate -FilePath c:\cert5.pfx -Password $
mypwd -Cert $cer
```

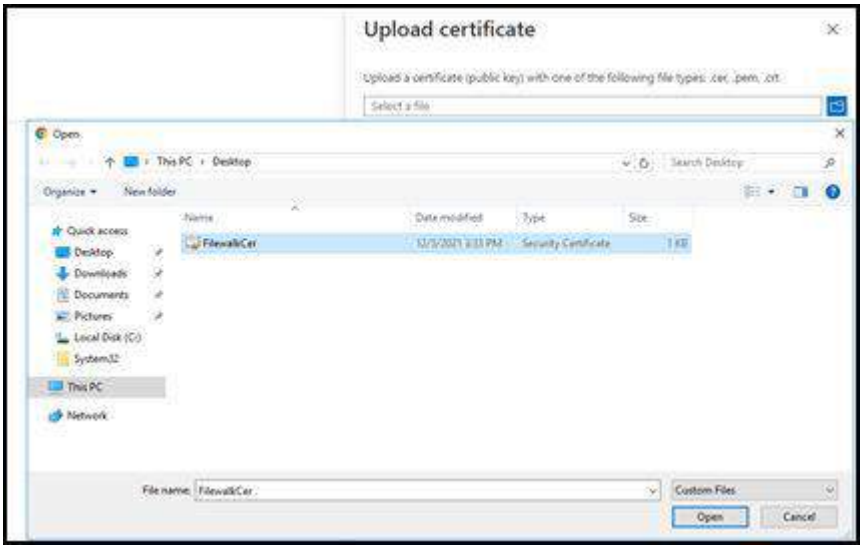
c. Configure the script as follows:

- In the first command line, set the expiration time of the certificate.
- In the second command line, the certificate is created.
- In the third command line, set the path to which to export the certificate CER file. This file will be uploaded later to Entra ID as part of the Entra ID application creation.
- In the fourth command line, set the password for encrypting the certificate PFX file.
- In the fifth command line, set the path to which to export the certificate PFX file. This file will be uploaded later to the Management Console.

2. When you have an available certificate, select the Certificates tab and click Upload certificate.



3. Select the certificate CER file, click Open and then click Add.



The certificate displays in the Certificates tab.



The application creation process is now complete.

What To Do Next

Remember: To add the OneDrive data source in the Management Console, have the following values ready from this procedure:

- Tenant ID from the Directory (tenant) ID value
- Application ID from the Application (client) ID value
- Certificate

Creating An Entra ID Application For Monitoring Exchange Online Via The Admin Center

We recommend that you create a new Entra ID application "automatically" via the Varonis Management Console, as described in Adding an Exchange Online Data Source. However, if you prefer to use an existing Entra ID application, you need to manually create it via the Microsoft Entra admin center, as described in the following topics:

- Creating an Entra ID Application for Monitoring Exchange Online - Summary
- Creating an Entra ID Application for Monitoring Exchange Online - Detailed Procedure

Creating an Entra ID Application for Monitoring Exchange Online - Summary

This section describes the procedure for manually creating the Entra ID application in the Microsoft Entra admin center. The Entra ID application will be used by Varonis to monitor Exchange Online.

1. Go to the Microsoft Entra admin center.

2. In Entra ID, go to App registrations > New registration > Accounts in this organizational directory only > Register.
3. Set a name for this application.
4. Copy and save the Application (client) ID (the application ID) for later use.
5. Add permissions as explained in Exchange Online Requirements.
6. Assign the Exchange Administrator role.
7. Add a certificate.

What To Do Next

Now that you're familiar with the deployment steps, it's time to dive into the detailed procedure.

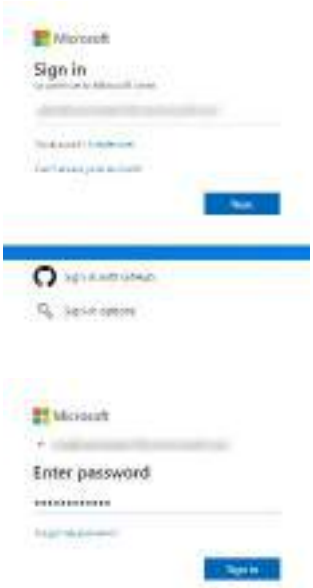
Creating an Entra ID Application for Monitoring Exchange Online - Detailed Procedure

This section describes the procedure for manually creating the Entra ID application in the Microsoft Entra admin center. The Entra ID application will be used by Varonis to monitor Exchange Online.

1. Access the Microsoft Entra admin center

1. Go to the Microsoft Entra admin center.
2. Log in using an account with permissions to create applications in Entra ID.

> Note: To complete the Entra ID application creation process, one of the following user accounts is required:
>
> - Global Administrator
> - Application administrator
> - Application developer
> - Cloud application administrator
>
> To grant consent to an application, a user account with Global Administrator privileges is required.
>
> If you are not using one of these accounts, make sure the holder of a suitable account is present during the session.



3. If you are using an account with MFA enabled, you will be prompted to enter a code. Enter the code and click Verify.



The Home page is displayed.

2. Create a new application

1. Go to Identity > Applications > App registrations.

The App registrations page is displayed.



2. Click New registration.
   The Register an application page is displayed.



3. Configure the application as follows:
   - In the Name field, set a name for this application. For example, VRNS.
   - In the Supported account types section, select Accounts in this organizational directory only (… Single tenant).
4. Click Register.

The application is created, and the application configuration page is displayed.



5. Copy and save the Application (client) ID value for later use.

> Note: The application ID is required when adding the Entra ID application to the Exchange Online data source in the Management Console.

3. Add and grant API permissions

1. Click API permissions to set up permissions for the application.



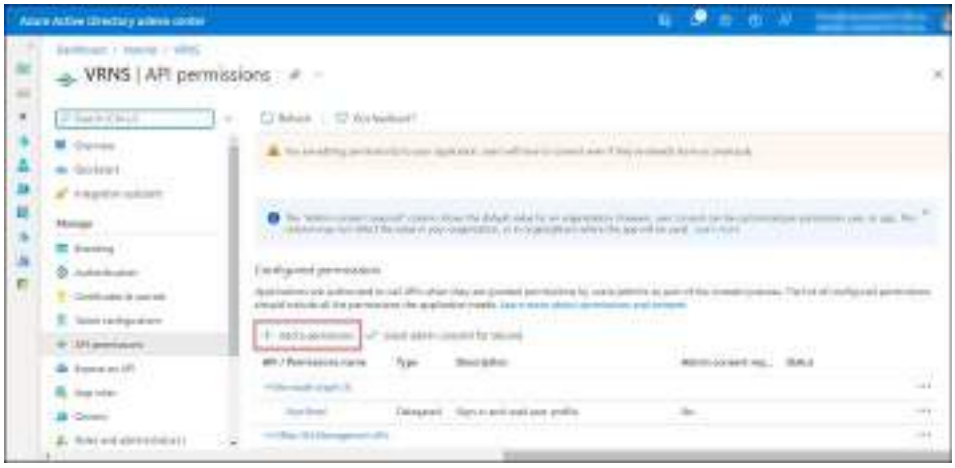
The API permissions page is displayed.



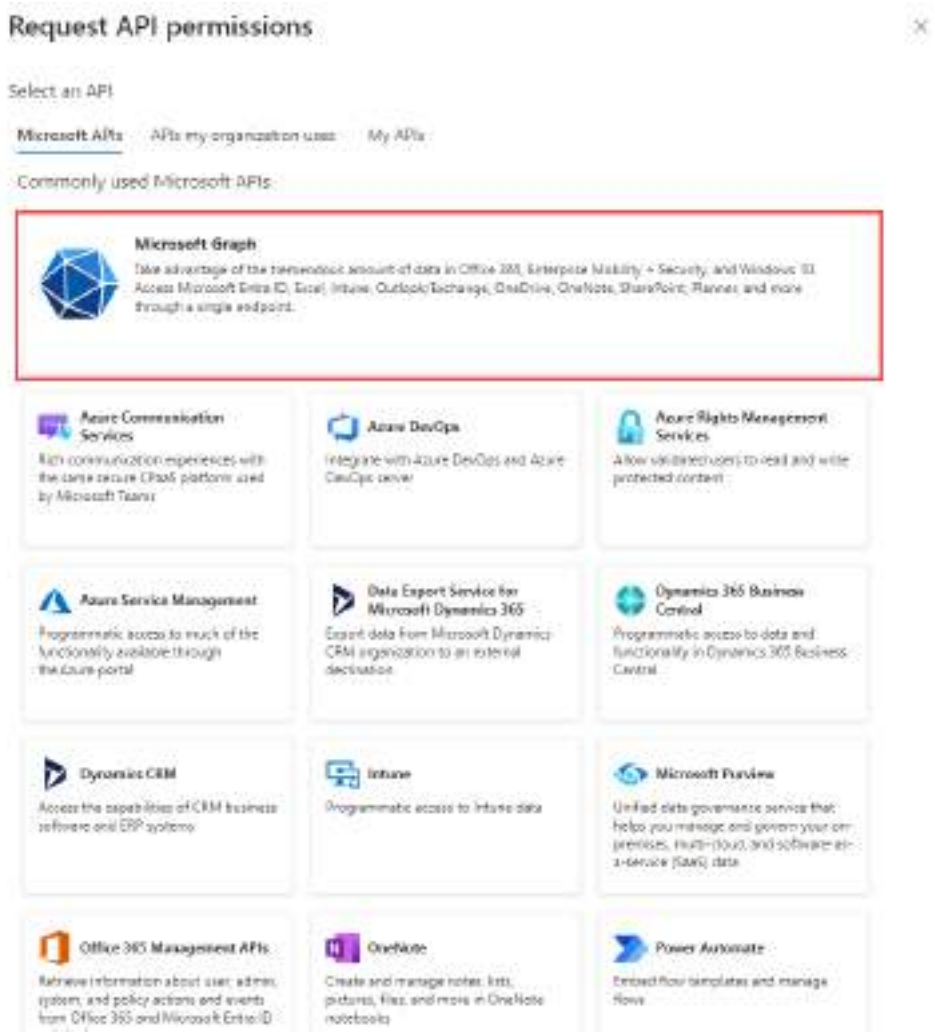
You will now add permissions as explained in Exchange Online Requirements. The permissions include:

- For reading directory data: Microsoft Graph - Directory.Read.All.
- For retrieving email attachment information: Microsoft Graph - Mail.Read.
- For accessing Exchange Online resources: Office 365 Exchange Online - Exchange.ManageAsApp.
- For granting full access to all Exchange mailboxes: Office 365 Exchange Online - full_access_as_app.

2. Add all the required permissions.
   For example, to add the Microsoft Graph - Directory.Read.All permission and Microsoft Graph - Mail.Read permission:
   a. Click Add a permission.



The Request API permissions page is displayed.



b. Select Microsoft Graph.



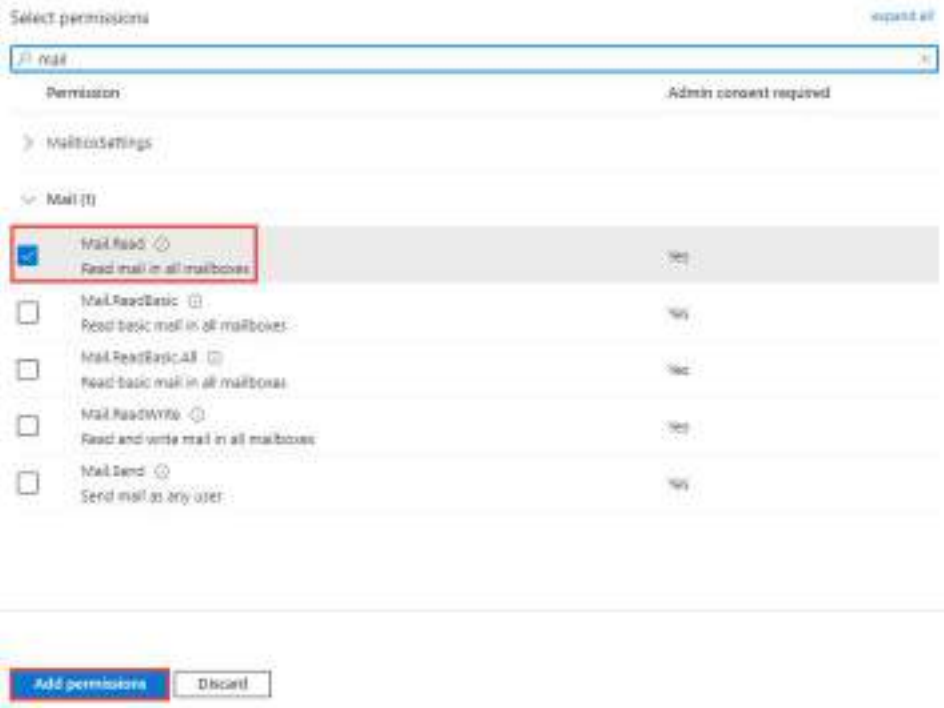
c. Select Application permissions.

d. In the search field, type Directory, and under Directory, select Directory.Read.All.

The Directory.Read.All permission is required for reading directory data.



e. In the search field, type Mail.Read, and under Mail, select Mail.Read.
The Mail.Read permission is required for message classification and to retrieve attachment information as part of Exchange Online Message Delivered events.



f. Click Add permissions.

The newly added permissions are displayed in the Configured permissions table.



3. Once you are done adding all the required permissions, in the Configured permissions section of the API permissions page, click Grant consent for (your tenant name).
   To grant consent to an application, a user account with Global Administrator privileges is required.

   Important: Until consent is granted, Varonis flows cannot use the Entra ID applications and will fail.

4. Click Yes to confirm your request.



Administrator consent is granted for the permissions.



4. Assign the Exchange Administrator role

1. Go to Identity > Roles & admins > Roles & admins.
   The Roles and administrators page is displayed.



2. In the search field, type Exchange Administrator.
3. Select Exchange Administrator and click it to open the Exchange Administrators > Assignments page.

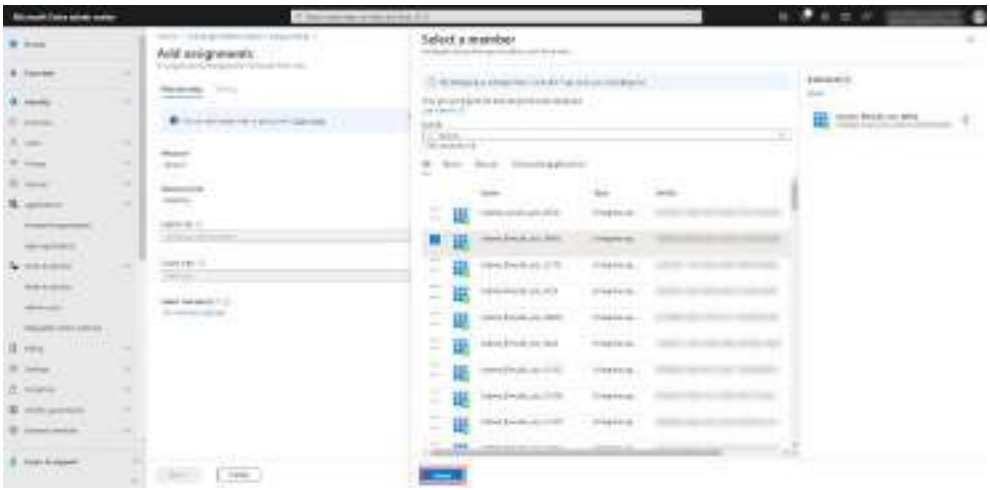


4. Click Add Assignment.

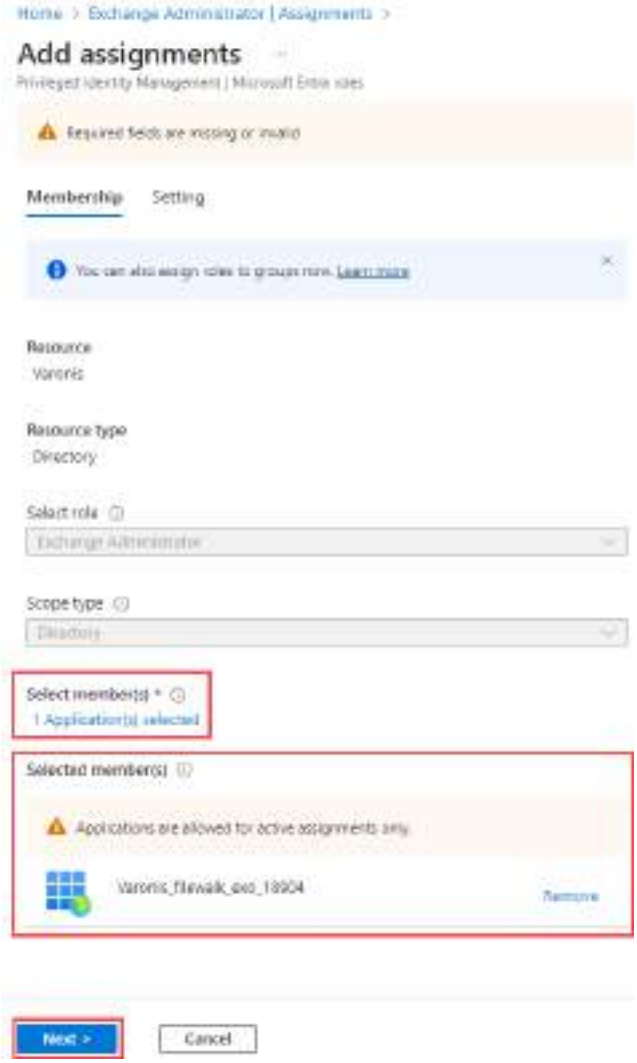
The Add assignments pane is displayed, opened to the Membership tab. You need to designate your application as a member.



5. In the Select members area, click the link.
   The Select a member pane is displayed on the right.
6. In the search field, type the name of the application you created, select the relevant Entra ID application, and click Select.


Add assignments
Select a member

The application is shown as selected in the Add assignments pane on the left.



7. Click Next

The Setting tab is displayed.



8. Make sure that Active and Permanently assigned are both selected, enter the justification, and click Assign.
   The Exchange Administrators > Assignments page is displayed, showing a confirmation message in the upper right corner indicating that the Entra ID application was successfully assigned to the Exchange Administrator role.
   The application is displayed in the Active assignments list; its State is marked Assigned.



5. Add a certificate

1. Click Certificates & secrets to add a certificate.



You can use a purchased certificate signed by a certificate authority (recommended), or create a self-signed certificate.
For certificate authentication, Entra ID requires the following:

- Certificates in X.509 V3 format for client and server authentication.
- A key length of 2048 bits.
- Key usage digital signature and key encipherment.
- The RSA cryptographic algorithm.
- Certificates signed with the SHA256 hash algorithm.
- The CN (subject), issuer, and validity period fields should be set.

Note: Certificates exported without a private key in the CER or PEM file should be uploaded to the App registrations screen in Entra ID. Certificates with a password-encrypted private key in PFX format should be uploaded to the Collector when adding a file server (including the password of the PFX file).

To purchase a certificate signed by a certificate authority, see this example.
To create a self-signed certificate, follow these steps:

Note: The following PowerShell commands are compatible with PowerShell 5.1 and Windows Server 2016. For older Windows Server versions, see Microsoft documentation.

a. Open Windows PowerShell Integrated Scripting Environment (ISE) as an administrator.

b. Run the following commands:

Important: When copying the following PowerShell commands from this document, line breaks may be mistakenly added. Make sure to remove the line breaks, so that each command line resides on a single line. Otherwise, the commands may fail.

```
$notAfter = (Get-Date).AddMonths(24) # Valid for 24 mon
ths
```

```
$cer = \Qi0 VipjVmkrihEivxm gate -Subject "CN=MyService
" -Provider "Microsoft Enhanced RSA and AES Cryptograph
ic Provider" -CertStoreLocation "cert:\LocalMachine\My"
 -KeyExportPolicy Exportable -NotAfter $notAfter -KeyLe
ngth 2048 -HashAlgorithm SHA256)
```

```
G1tsvx Eivxm gate -Type CERT -FilePath c:\cert5.cer -Ce
rt $cer
```

```
$mypwd = ConvertTo-SecureString -String "1234" -Force -
AsPlainText
```

```
G1tsvx Sj1Eivxm gate -FilePath c:\cert5.pfx -Password $
mypwd -Cert $cer
```

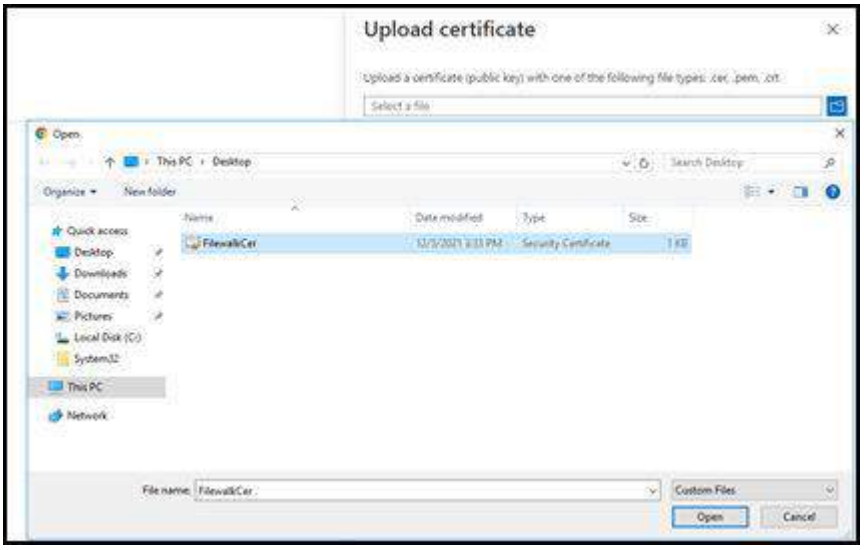
c. Configure the script as follows:

- In the first command line, set the expiration time of the certificate.
- In the second command line, the certificate is created.
- In the third command line, set the path to which to export the certificate CER file. This file will be uploaded later to Entra ID as part of the Entra ID application creation.
- In the fourth command line, set the password for encrypting the certificate PFX file.
- In the fifth command line, set the path to which to export the certificate PFX file. This file will be uploaded later to the Management Console.

2. When you have an available certificate, select the Certificates tab and click Upload certificate.



3. Select the certificate CER file, click Open and then click Add.



The certificate displays in the Certificates tab.



The application creation process is now complete.

What To Do Next

Remember: To add the Exchange Online data source in the Management Console, have the following values ready from this procedure:

- Tenant ID from the Directory (tenant) ID value
- Application ID from the Application (client) ID value
- Certificate

26 APPENDIX - RENEWING THE SECRET OR CERTIFICATE OF YOUR ENTRA ID APPLICATIONS

Varonis uses Entra ID applications to monitor your M365 data sources. These applications require a secret or a certificate, which expire after a maximum of 24 months.

Make sure to renew the expired secret or certificate both in the Microsoft Entra admin center and in the Varonis Management Console. Follow the instructions in the relevant procedure:

- Renewing the Secret of your Entra ID Application
- Renewing the Certificate of your Entra ID Application

Renewing The Secret Of Your Entra ID Application

Overview

Varonis uses an Entra ID application to monitor your Entra ID domain. This application requires a secret, which expires after a maximum of 24 months.

Make sure to renew the expired secret both in the Microsoft Entra admin center and in the Varonis Management Console as follows:

1. Find the name of your Entra ID application in the Management Console.
2. Use this name to find your application and renew its secret in the Microsoft Entra admin center.
3. Use this new secret to replace the expired one back in the Management Console.

The following sections provide step-by-step instructions on how to renew your secret.

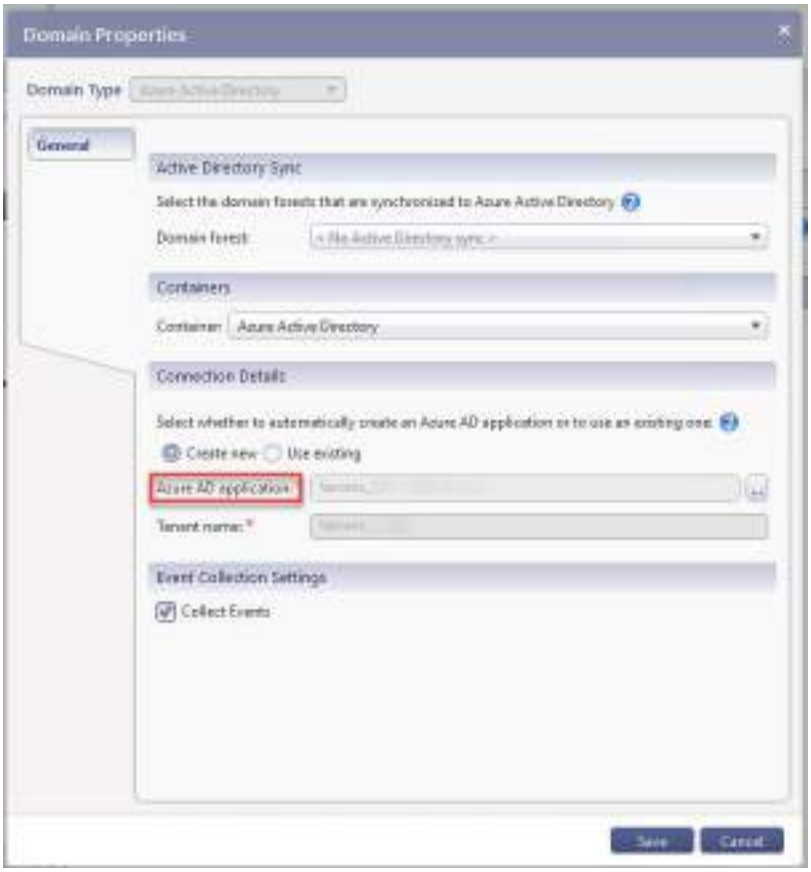
> Note: Alternatively, create a new application for monitoring your Entra ID domain. This process automatically includes the creation of a new secret.

1. Find the name of your Entra ID application in the Management Console

1. Run the Management Console as an administrator.
2. Select Management > Components > Root > Domains. The Domains pane is displayed on the right.
3. In the grid, select your Entra ID domain and then go to the Domains toolbar and click Edit.



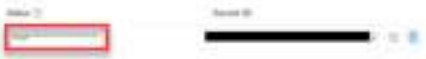
The Domain Properties window is displayed, showing the General tab.



4. Go to the Connection Details section and find the Entra ID application name - to be used to search for this application in the Microsoft Entra admin center.

2. Renew your secret in the Entra ID portal

1. Log in to Microsoft Entra admin center.
2. Search for your Entra ID application using the name you found in the Management Console.
3. Click your application to display its settings and then click Certificates & Secrets.
4. Confirm that the Expires date shows your secret is about to expire and then click New client secret.
5. In Add a client secret, add a Description for your secret and set its Expires date to 24 months (or the maximum time allowed).
6. Copy the secret's Value - to be pasted in the Management Console.



> Note: Make sure to copy the new secret immediately, as it is hidden once the page reloads.

3. Update your secret in the Management Console

1. Back in the Management Console, select your domain and click Edit.The Domain Properties window is displayed, showing the General tab.
2. In the Connection Details section, click the Use Existing button. The Use Existing Entra ID Application window is displayed.
3. In the Secret key field, override the current value with the new secret key that you copied from the Entra ID portal and click OK.
4. Back in the General window, click Save.
5. If you have more than one Entra ID domain, make sure to repeat this procedure per-domain.

Renewing The Certificate Of Your Entra ID Application

Overview

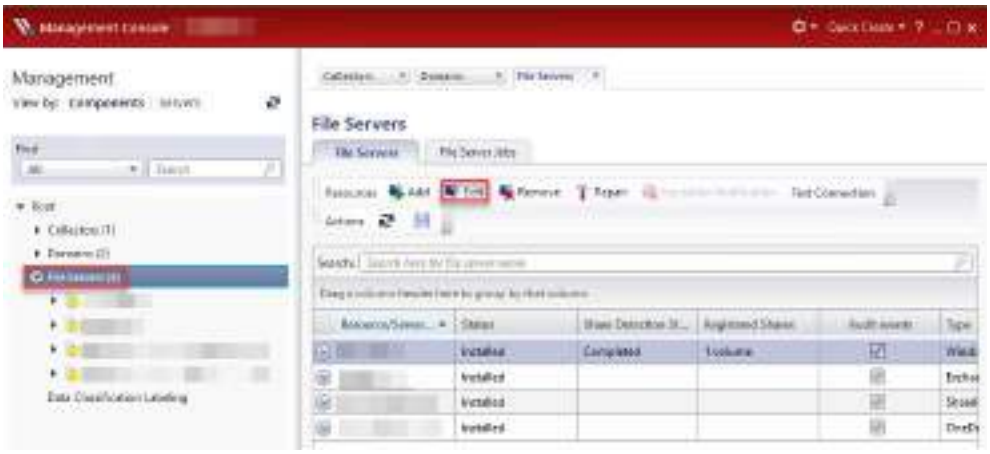
Varonis uses an Entra ID application to monitor your M365 data source. This application requires a certificate, which expires after a maximum of 24 months.

Once a certificate expires, you are required to create a new Entra ID application that has a new certificate. Varonis can automatically create this application and its certificate for you. Alternatively, you can create the application and its certificate manually.

The following procedure explains how to replace the Entra ID application whose certificate expired with a new Entra ID application that has a valid certificate.

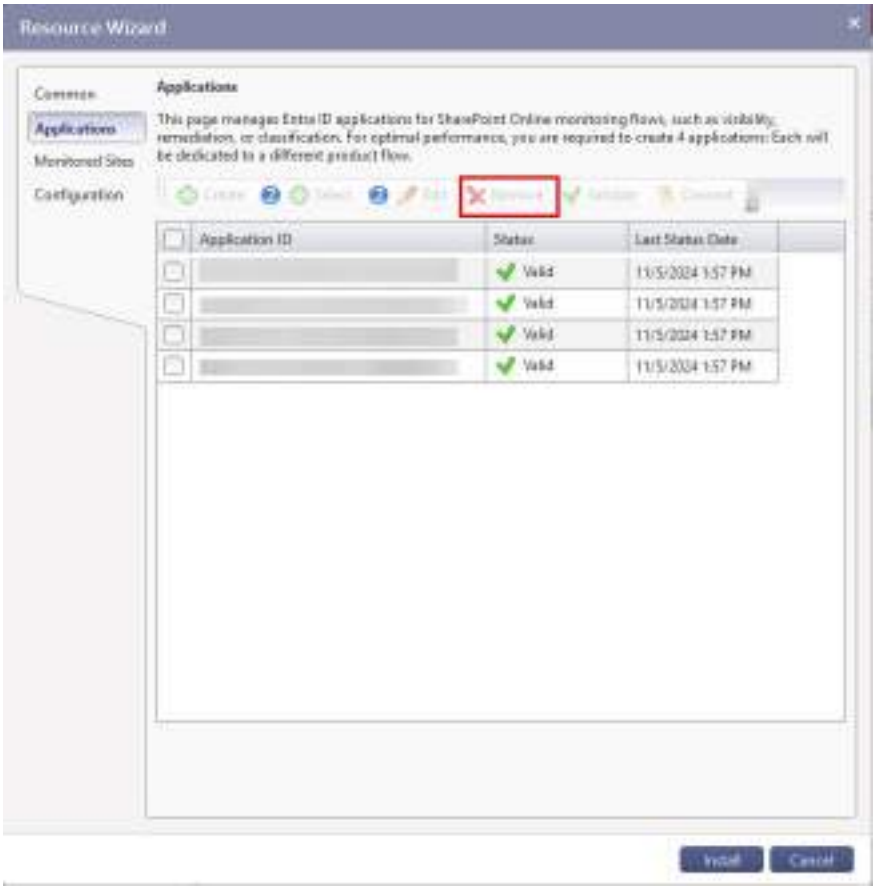
Replace the Entra ID application whose certificate expired

1. Run the Management Console as an administrator.
2. Select Management > Components > Root > File Servers and then the File Servers tab. The File Servers pane is displayed on the right.
3. In the grid, select one of your data sources and then go to the Resources toolbar and click Edit.



The Editing file server window is displayed, showing the Common tab.

4. Go to the Applications tab.



5. Select the application whose certificate expired and click Remove.
6. Choose one of the following options:

- To allow Varonis to automatically create a new application and its certificate, click Create.
- To manually replace the certificate and use your own application:
  - Create a new valid certificate.
  - In the Microsoft Entra admin center, go to your tenant and select App registrations.
  - Find your application and go to its Certificates & secrets > Certificates and click Upload certificate.
  - Upload the new certificate to install it on your application.
  - In the Management Console, return to the Editing file server window 's Applications tab and click Select.

  These procedures are described in the "Configure Entra ID applications" section of Adding a SharePoint Online Data Source - Detailed Procedure (the same instructions apply to OneDrive data sources).

If you have more than one data source, make sure to repeat this procedure per data source.

27 APPENDIX - ADDITIONAL CONFIGURATIONS AND OPERATIONS

This section describes some additional procedures for configuring and managing monitored data sources.

Testing Connectivity to Data Sources and Domains

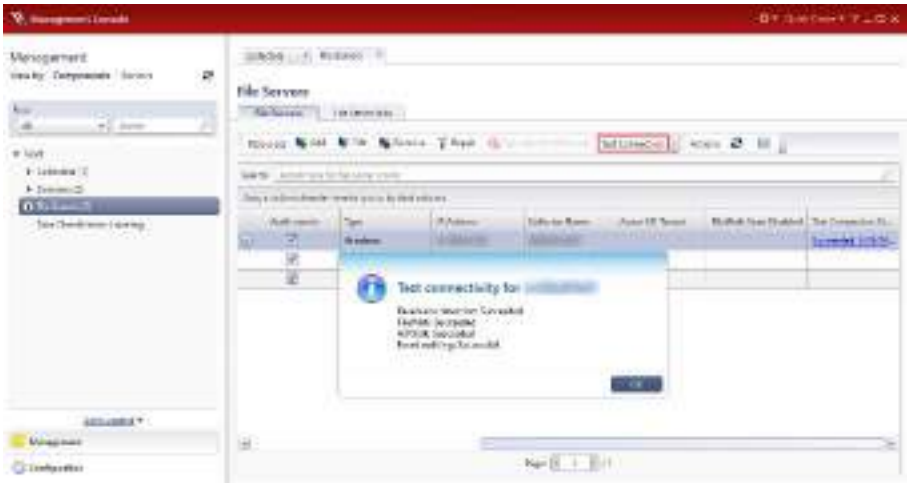
You can test the Varonis connection to installed data sources and domains, and connectivity health of the core processes (Resource Detection, FileWalk, ADWalk, Event Auditing) required for monitoring structure and permissions, local accounts, and events.

> Note: The test connectivity functionality is not supported for Varonis Edge.

1. From the File Servers grid (or from the Domains grid), select one data source (or AD domain) to test.

   > Note: The Test Connection button is enabled when only one data source is selected.

2. On the Resources toolbar, click Test Connection.
   The Test Connectivity dialog box is displayed, prompting you to confirm.
3. Click OK.
   When testing has completed, a link to access the results is displayed in the Test Connection Status column.



Repairing a Data Source

You can repair the Varonis agent along with the data source.

1. From the File Servers grid, select the data source to be repaired.
2. On the Resources toolbar, click Repair.
   The Repair File Server window is displayed.
3. Set the following:
   - File Server Credentials - The credentials of a user with access to the data source. The account must be a member of the Local Administrators group on the machine during installation.
     - User name - Set the account's user name.
     - Password - Set the account's password.
   - Repair Varonis File Server agent - Select this option to repair the Varonis agent along with the data source itself.
4. Click Continue.
   A prerequisite check is run. When completed, the Prerequisite window closes, and the repair Update status is displayed in the Status column in the File Servers page. When the update completes, the status shows 100%, indicating that the selected items are repaired.

Decommissioning Data Sources

When a data source is decommissioned, historical data is saved. Event auditing and crawling are disabled for a decommissioned data source.

Once a data source is decommissioned, you can edit only the Collector to which it is connected.

> Important: If you choose to restore a decommissioned data source, you must also restore event auditing and crawling on the data source. To restore event auditing and crawling, select the Collect Events and Crawl options in the File Servers grid or in the Editing File Server window.

1. From the File Servers grid, select the data source to be decommissioned.
2. On the Resources toolbar, click Edit.
   The Editing File Server window is displayed.
3. In the Resource Details area, select the Set file server as decommissioned checkbox.

4. Click Save.
   A prerequisite check is run. When completed, the Prerequisite window closes, and the decommissioned Update status is displayed in the Status column in the File Servers page. When the update completes, the status shows 100%, indicating that the selected data source is decommissioned. The data source is grayed out in the grid.

   Note:
   - You can restore a decommissioned data source by clearing the Set file server as decommissioned checkbox in the Editing File Server window.
   - Decommissioning a data source does not release its allocated license from the monitoring Collector.

Removing a Data Source

1. From the File Servers grid, select the data source to be removed.
2. On the Resources toolbar, click Remove.
   The Remove File Server window is displayed.
3. Set the following:
   - File Server Credentials - The credentials of a user with access to the data source. The account must be a member of the Local Administrators group on the machine during installation.
     - User name - Set the account's user name.
     - Password - Set the account's password.
   - Remove Varonis File Server agent - Select this option to remove the Varonis agent along with the data source itself.
4. Click Continue.
   A prerequisite check is run. When completed, the Prerequisite window closes, and the remove Update status is displayed in the Status column in the File Servers page. When the update completes, the status shows 100%, indicating that the selected items are removed.

Configuring Unmonitored Folders

When a data source is monitored by Varonis, all the folders it contains are automatically monitored. However, collection of data for data sources can result in a good deal of needless overhead in terms of storage space and licensing costs.

Therefore, Varonis enables you to select entities you do not want to monitor and remove them from Varonis storage, either temporarily or permanently.

The list of unmonitored entities is easily configurable and can be changed on the fly. The Unmonitored panes also provide information about the amount of data or number of users your DatAdvantage license permits you to store, and the amount or number you are currently using.

Note: If you make a change to resume monitoring an unmonitored entity, the change takes effect either after the nightly run of FileWalk or ADWalk (as relevant) and PullWalk, or after these jobs are run manually.

1. In the Management Console, from the menu in the left pane, select Configuration > Unmonitored Folders.
   The Unmonitored Folders settings are displayed, listing entities that are currently not being monitored.
2. To locate the entities you want to configure, set the filters above the list and click Search.
   - Access Path - The full path on which the folders reside
   - File Server - The data source on which the folders reside
   - Size (MB)- The size of the folders
   - Last monitored - The date on which the folder was last monitored
3. To add folders, click Add on the toolbar.
   The Directory Picker dialog box is displayed, where you can browse to the required folders.
4. To make entities monitored again, select the required entity and click Remove.
5. To upload a file containing a list of entities to designate as unmonitored, on the toolbar in the main page, click Import and browse to the relevant file.
   The file entries must be in the following format.

   ```
   pi wivziv rame|full access_path
   ```

   Note: Imported folders must be initially crawled by FileWalk.

Proteção de dados em Tenants do Microsoft 365

Proteja os seus dados do Microsoft 365 contra a sobreexposição e ameaças cibernéticas.

Desafio

As organizações costumavam manter os seus dados isolados, para que os utilizadores de um departamento não pudessem aceder aos dados pertencentes a outro. Mas, à medida que as organizações internacionais migram os seus dados para grandes e consolidados tenants de Microsoft 365 — cada um contendo milhares de utilizadores e múltiplas suborganizações — a segurança dos dados tornou-se mais desafiante.

Uma vez que os controlos administrativos e de segurança são geridos a nível do tenant, as suborganizações individuais não têm visibilidade sobre quem pode aceder aos dados, onde são armazenados os dados críticos ou mesmo sobre a forma como esses dados são utilizados. Sem limites administrativos adequados, as organizações individuais não podem proteger os dados armazenados em tenants consolidados ou cumprir as leis de privacidade.

Em média

7% das empresas que utilizam o Microsoft 365 tinham mais de 10 mil ficheiros expostos[1]

9% dos ficheiros confidenciais no Microsoft 365 são expostos em toda a organização[1]

São necessárias **12 horas** para investigar um incidente de segurança sem a Varonis[2]

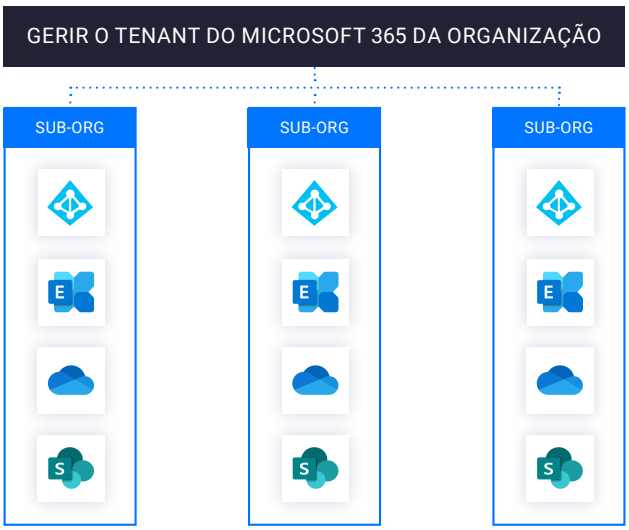
Solução

A Varonis permite que organizações individuais protejam e assegurem os seus dados hospedados em grandes tenants consolidados da Microsoft. Com a Varonis, as suborganizações podem:

- Visualizar e corrigir riscos de dados
- Descobrir dados confidenciais e regulamentados em escala
- Prevenir ataques de dados

A Varonis permite a segmentação de dados para Teams, SharePoint Online e OneDrive através de vários mecanismos diferentes, incluindo:

- Proprietário do site/criador do site
- Adesão e atributos do grupo do Azure Active Directory
- Convenção de nomenclatura do site
- Permissões de utilizador



[1] Relatório global de riscos de dados da Varonis 2022
[2] Estudo da Forrester de Impacto Económico Total da Varonis

EXPOSIÇÃO DE LINKS

1.294
PARTILHADO COM TODO O TENANT

23.321
PARTILHADO COM OUTRAS SUBORGANIZAÇÕES

4.234
UTILIZADORES ESPECÍFICOS

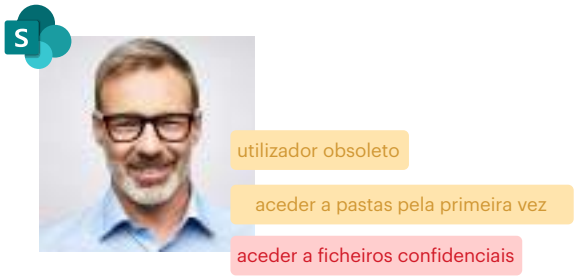
Evite a fuga de dados.

A Varonis ajuda a evitar a fuga de dados, identificando onde os dados são sobreexpostos. Rastreamos e analisamos continuamente as permissões — incluindo associações a grupos, permissões diretas e links de partilha entre departamentos — e apresentamos onde os dados são expostos. Os limites do departamento são respeitados e protegidos em grandes tenants multiorganizacionais, através de uma solução de segmentação única.

Detete ameaças proativamente.

A Varonis combina atividades do Microsoft 365 e Azure AD com telemetria local e de perímetro para proporcionar uma visão mais holística de possíveis ameaças e tentativas de exfiltração. As nossas deteções baseadas no comportamento fornecem apenas alerts que importam e somente ao pessoal competente.

Acesso anormal a ficheiros confidenciais



Serviço	Nome	Acesso	Classificação
	Conta na Califórnia		CCPA PHI
	Q12021.xls	Todos	PCI
	Transações	Todos	PCI PII

Não se contente com classificações "quase" precisas.

A Microsoft confia em grande parte em uma pequena biblioteca de regras de classificação e classificação manual, que não cresce. A vasta biblioteca de políticas da Varonis usa lógica sofisticada para gerar resultados precisos. Emparelhamos resultados de classificação com permissões para revelar onde os dados confidenciais estão sobre-expostos, fornecendo uma ideia clara do risco.

Experimente a Varonis gratuitamente.

Todos os produtos Varonis podem ser testados gratuitamente e incluem uma avaliação de risco conduzida por engenheiros. A maneira mais fácil de começar é com uma pequena demo 1:1 e uma conversa de descoberta.

Contacte-nos

Varonis na nuvem

A nossa nova plataforma nativa da nuvem é implementada em minutos e oferece retorno sobre o investimento imediato. Sem hardware. Sem despesas gerais. Apenas resultados.

A Plataforma de Segurança de Dados SaaS da Varonis simplifica a implementação, fornecendo resultados quantificáveis de segurança dos dados com o mínimo esforço manual e um baixo custo total de propriedade (TCO).

Com o SaaS, pode esperar os seguintes benefícios:

- Mais fácil de implementar
- Mais fácil de manter e atualizar
- Requisitos mínimos de infraestrutura (sem SQL, Solr, etc.)
- Dimensiona dinamicamente com base nas necessidades do cliente
- Mais fácil de sustentar



Poupança média de SaaS

100% de redução nos custos de licenciamento da SQL

75% de redução de servidores geridos

67% de redução nos custos de CPU

87% de redução nos custos de memória

92% de redução nos custos de disco

"A Varonis poupa-nos facilmente algumas centenas de milhares de dólares por ano em termos de custos com pessoal e em recuperação de custos de hardware. Se também nos salva de um incidente de segurança — não tem preço".

Mike Taylor
CIO, Setor Federal

Leia o estudo de caso →

A nova oferta SaaS da Varonis fornece

Resultados significativos em matéria de segurança em piloto automático

A nossa missão é fornecer resultados de segurança precisos e de baixo contacto. Com novas e poderosas capacidades de automatização, os seus dados tornam-se mais seguros a cada minuto. Mesmo quando não está ligado, a Varonis está a classificar mais dados, a revogar permissões, a aplicar políticas, e a acionar alertas para que a nossa equipa de resposta a incidentes possa fazer análises em seu nome.

Implementação rápida, insights instantâneos

A plataforma Varonis SaaS pode ser implementada em minutos. As insights, alertas, e exposições são completados instantaneamente, fornecendo valor rapidamente. Um engenheiro dedicado ajuda com a integração, formação e configuração. A monitorização Cloud-to-cloud é feita sem agentes e fora da banda.

Baixo custo total de propriedade

Não há necessidade de fornecer hardware, comprar licenças de SQL Server, ou instalar máquinas virtuais complicadas. SaaS reduz o seu TCO ao eliminar os custos operacionais de self-hosting.

Resposta proativa a incidentes

Quando se liga à nuvem de Varonis, a nossa equipa de ciber-segurança pode estar atenta aos seus alertas. Se virmos algo alarmante, alertá-lo-emos. Além disso, a nossa equipa de apoio pode resolver rapidamente problemas sem aceder à sua rede corporativa.

Uma Subscrição, funcionalidade infinita

Simplificámos drasticamente o nosso modelo de licenciamento. Ao comprar uma subscrição da Plataforma de Segurança de Dados Varonis SaaS, obtém todas as nossas funcionalidades principais por defeito: classificação de dados, inteligência de acesso, automatização de privilégios mínimos, monitorização da atividade de dados, UEBA, etiquetagem de sensibilidade, e muito mais.

Modelo de ameaça contínua e atualizações de políticas

Obtenha acesso imediato às funcionalidades mais recentes do produto, incluindo os mais recentes modelos de ameaça e políticas de classificação. Não há necessidade de atualizações, downloads de pacotes ou patches

Experimente a Varonis gratuitamente.

Todos os produtos Varonis podem ser testados gratuitamente e incluem uma avaliação de risco conduzida por engenheiros. A maneira mais fácil de começar é com uma pequena demo 1:1 e uma conversa de descoberta.

Contacte-nos

CERTIDÃO NEGATIVA DE DISTRIBUIÇÃO (AÇÕES DE FALÊNCIAS E RECUPERAÇÕES JUDICIAIS)
1ª e 2ª Instâncias

CERTIFICAMOS que, após consulta aos registros eletrônicos de distribuição de ações de falências e recuperações judiciais disponíveis até 15/10/2026, **NADA CONSTA** contra o nome por extenso e CPF/CNPJ de:

JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA
24.425.034/0001-96

OBSERVAÇÕES:
a) Os dados de identificação são de responsabilidade do solicitante da certidão, devendo a titularidade ser conferida pelo interessado e pelo destinatário.
b) A certidão será emitida de acordo com as informações inseridas no banco de dados. Em caso de exibição de processos com dados desatualizados, o interessado deverá requerer a atualização junto ao juízo ou órgão julgador.
c) A certidão será negativa quando não for possível a individualização dos processos por carência de dados do Poder Judiciário. (artigo 8o, § 2o da Resolução 121/CNJ).
d) A certidão cível contempla ações cíveis, execuções fiscais, execuções e insolvências civis, falências, recuperações judiciais, recuperações extrajudiciais, inventários, interdições, tutelas e curatelas. A certidão criminal compreende os processos criminais, os processos criminais militares e as execuções penais. Demais informações sobre o conteúdo das certidões, consultar em www.tjdft.jus.br, no menu Serviços, Certidões, Certidão Nada Consta, Tipos de Certidão.
e) As certidões de Falência e Recuperação Judicial, Cível ou Especial atendem ao disposto no inciso II do artigo 69 da Lei 14133/2021.
f) Medida prevista no artigo 26 do Código Penal, sentença não transitada em julgado.

A autenticidade deverá ser confirmada no site do TJDFT (www.tjdft.jus.br), no menu Serviços, Certidões, Certidão Nada Consta, Validar Certidão - autenticar, informando-se o número do selo digital de segurança impresso.

Emitida gratuitamente pela internet em: 15/10/2026
Selo digital de segurança: **2026.CTD.FSZW.Z20O.8182.MQVO.YDXL**
*** VÁLIDA POR 30 (TRINTA) DIAS ***

NUCER - Núcleo de Emissão de Certidões do TJDFT
Fórum de Brasília - Milton Sebastião Barbosa, Praça Municipal - Lote 1, Bloco A, Ala B - Térreo.
Brasília - DF
Horário de Atendimento: 7h às 19h, de segunda a sexta-feira, exceto feriados.

BALANÇO PATRIMONIAL

Entidade:	JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA
Período da Escrituração:	01/01/2025 a 31/12/2025
CNPJ:	24.425.034/0001-96
Número de Ordem do Livro:	14
Período Selecionado:	01 de janeiro de 2025 a 31 de dezembro de 2025

DEMONSTRAÇÕES CONTÁBEIS DO EXERCÍCIO CONSOLIDADO

Descrição	Nota	Saldo Inicial	Saldo Final
ATIVO		R$ 116.735.515,00	R$ 298.454.976,34
ATIVO CIRCULANTE		R$ 115.773.925,87	R$ 297.454.393,83
CAIXA E EQUIVALENTES DE CAIXA		R$ 74.591.000,24	R$ 97.973.497,43
BENS NUMERARIOS		R$ 2.671,86	R$ 2.671,86
CONTAS CORRENTES		R$ 12.547.357,63	R$ 8.888.470,87
APLICACOES DE LIQUIDEZ IMEDIATA		R$ 62.040.970,75	R$ 89.082.354,70
CLIENTES		R$ 23.961.288,95	R$ 170.542.485,49
DUPLICATAS A RECEBER		R$ 23.961.288,95	R$ 170.542.485,49
OUTROS CREDITOS		R$ 17.219.195,45	R$ 27.048.792,50
BANCOS CONTAS VINCULADAS		R$ 97.413,50	R$ 102.674,95
OUTROS CREDITOS E VALORES		R$ 3.209.294,37	R$ 2.739.983,48
ADIANTAMENTOS A TERCEIROS		R$ 13.565.502,71	R$ 22.993.880,52
ADIANT. A FUNCIONARIOS, SOCIOS E DIRETORES		R$ 0,00	R$ 16.740,81
LUCROS DISTRIBUIDOS NO EXERCICIO		R$ 0,00	R$ 0,00
TRIBUTOS A RECUPERAR		R$ 346.984,87	R$ 1.195.512,74
IMPOSTOS A COMPENSAR		R$ 0,00	R$ 0,00
ESTOQUES		R$ 2.441,23	R$ 1.889.618,41
ESTOQUES DIVERSOS		R$ 2.441,23	R$ 1.889.618,41
NAO CIRCULANTE		R$ 961.589,13	R$ 1.000.582,51
INVESTIMENTOS		R$ 37.082,90	R$ 38.702,90
OUTROS INVESTIMENTOS		R$ 37.082,90	R$ 38.702,90
IMOBILIZADO		R$ 922.116,93	R$ 960.684,91
IMOVEIS		R$ 750.000,00	R$ 750.000,00
BENS EM OPERACAO		R$ 317.782,80	R$ 432.853,18
(-) (-) DEPREC/AMORTIZ/EXAUSTAO ACUMULADA		R$ (145.665,87)	R$ (222.168,27)
INTANGIVEL		R$ 2.389,30	R$ 1.194,70
CUSTO		R$ 5.973,12	R$ 5.973,12
(-) (-) AMORTIZACOES		R$ (3.583,82)	R$ (4.778,42)
ATIVO COMPENSATORIO		R$ 0,00	R$ 0,00
DEMONSTRACOES DIVERSAS		R$ 0,00	R$ 0,00
TRANSFERENCIAS		R$ 0,00	R$ 0,00
PASSIVO		R$ 116.735.515,00	R$ 298.454.976,34
CIRCULANTE		R$ 38.834.659,68	R$ 178.956.187,72
FORNECEDORES		R$ 29.331.285,74	R$ 81.437.674,89
FORNECEDORES NACIONAIS		R$ 29.331.285,74	R$ 81.437.674,89
OBRIGACOES TRIBUTARIAS		R$ 9.119.646,73	R$ 24.092.630,91
IMPOSTOS E CONTRIBUICOES A RECOLHER		R$ 9.118.880,12	R$ 24.091.224,78
TRIBUTOS RETIDOS A RECOLHER		R$ 766,61	R$ 1.406,13
OBRIGACOES TRABALHISTAS E PREVIDENCIARIAS		R$ 134.539,53	R$ 783.849,29
OBRIGACOES COM O PESSOAL		R$ 121.411,70	R$ 4.151,78
ENCARGOS SOCIAIS		R$ 13.127,83	R$ 13.572,37
PROVISOES		R$ 0,00	R$ 766.125,14
PARCELAMENTOS		R$ 242.287,68	R$ 107.525,27
PARCELAMENTOS RFB		R$ 242.287,68	R$ 107.525,27
OUTRAS OBRIGACOES		R$ 6.900,00	R$ 72.534.507,36
ADIANTAMENTOS DE CLIENTES		R$ 0,00	R$ 65.934.419,06
CONTAS A PAGAR		R$ 6.900,00	R$ (0,00)
OUTROS DEBITOS		R$ 0,00	R$ 6.600.088,30
NAO CIRCULANTE		R$ 948.960,08	R$ 822.808,98
OBRIGACOES A LONGO PRAZO		R$ 948.960,08	R$ 822.808,98
PARCELAMENTOS		R$ 948.960,08	R$ 822.808,98
PATRIMONIO LIQUIDO		R$ 76.951.895,24	R$ 118.675.979,64
CAPITAL SOCIAL		R$ 1.000.000,00	R$ 1.000.000,00
CAPITAL SUBSCRITO		R$ 1.000.000,00	R$ 1.000.000,00
LUCROS E PREJUIZOS ACUMULADOS		R$ 75.951.895,24	R$ 117.675.979,64
LUCROS E PREJUIZOS ACUMULADOS		R$ 75.951.895,24	R$ 40.959.540,94
LUCROS E PREJUIZOS DO EXERCICIO		R$ 0,00	R$ 76.716.438,70

Este documento é parte integrante de escrituração cuja autenticação se comprova pelo recibo de número 55.B8.6D.57.3D.5F.65.05.31.5C.F6.AA.1B.C4.8C.75.DC.A5.D1.9F-5, nos termos do Decreto nº 8.683/2016.

Este relatório foi gerado pelo Sistema Público de Escrituração Digital – Sped

Versão 10.4.1 do Visualizador

DEMONSTRAÇÃO DE RESULTADO DO EXERCÍCIO

Entidade:	JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA
Período da Escrituração:	01/01/2025 a 31/12/2025
CNPJ:	24.425.034/0001-96
Número de Ordem do Livro:	14
Período Selecionado:	01 de janeiro de 2025 a 31 de dezembro de 2025

DEMONSTRAÇÕES CONTÁBEIS DO EXERCÍCIO CONSOLIDADO

Descrição	Nota	Saldo anterior	Saldo atual
RECEITAS OPERACIONAIS BRUTAS		R$ 0,00	R$ 339.768.060,24
VENDAS DE SERVICOS		R$ 0,00	R$ 269.939.920,13
REVENDA DE MERCADORIAS		R$ 0,00	R$ 69.828.140,11
(-) (-) DEDUÇÕES DA RECEITA		R$ (0,00)	R$ (40.239.347,12)
(-) TRIBUTOS INCIDENTES SOBRE A RECEITA		R$ (0,00)	R$ (40.239.347,12)
(-) CUSTOS		R$ (0,00)	R$ (156.863.699,08)
(-) CUSTO DOS SERVIÇOS		R$ (0,00)	R$ (119.515.588,68)
(-) CUSTO DE MERCADORIA		R$ (0,00)	R$ (36.842.411,26)
(-) CUSTO DE PRODUÇÃO INDUSTRIAL		R$ (0,00)	R$ (505.699,14)
(-) DESPESAS/RECEITAS OPERACIONAIS		R$ (0,00)	R$ (27.347.583,01)
(-) DESPESAS ADMINISTRATIVAS		R$ (0,00)	R$ (27.114.087,98)
(-) DESPESAS TRIBUTARIAS		R$ (0,00)	R$ (233.902,00)
OUTRAS RECEITAS OPERACIONAIS		R$ 0,00	R$ 406,97
(=) RESULTADO FINANCEIRO LÍQUIDO		R$ 0,00	R$ 630.514,66
RECEITAS FINANCEIRAS		R$ 0,00	R$ 3.398.058,24
(-) DESPESAS FINANCEIRAS		R$ (0,00)	R$ (2.767.543,58)
(-) PROVISÃO IR E CSLL		R$ (0,00)	R$ (39.231.506,99)
(-) CSLL		R$ (0,00)	R$ (10.486.457,73)
(-) IRPJ		R$ (0,00)	R$ (28.745.049,26)
(=) LUCRO/PREJUÍZO LÍQUIDO DO PERÍODO		R$ (0,00)	R$ 76.716.438,70

Este documento é parte integrante de escrituração cuja autenticação se comprova pelo recibo de número 55.B8.6D.57.3D.5F.65.05.31.5C.F6.AA.1B.C4.8C.75.DC.A5.D1.9F-5, nos termos do Decreto nº 8.683/2016.

Este relatório foi gerado pelo Sistema Público de Escrituração Digital – Sped

Versão 10.4.1 do Visualizador

TERMOS DE ABERTURA E ENCERRAMENTO

Entidade:	JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA
Período da Escrituração:	01/01/2025 a 31/12/2025
CNPJ:	24.425.034/0001-96
Número de Ordem do Livro:	14
Período Selecionado:	01 de janeiro de 2025 a 31 de dezembro de 2025

TERMO DE ABERTURA

Nome Empresarial	JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA
NIRE	53202049896
CNPJ	24.425.034/0001-96
Número de Ordem	14
Natureza do Livro	LIVRO DIARIO GERAL
Município	BRASILIA
Data do arquivamento dos atos constitutivos	24/05/2024
Data de arquivamento do ato de conversão de sociedade simples em sociedade empresária	
Data de encerramento do exercício social	31/12/2025
Quantidade total de linhas do arquivo digital	48472

TERMO DE ENCERRAMENTO

Nome Empresarial	JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA
Natureza do Livro	LIVRO DIARIO GERAL
Número de ordem	14
Quantidade total de linhas do arquivo digital	48472
Data de inicio	01/01/2025
Data de término	31/12/2025

Este documento é parte integrante de escrituração cuja autenticação se comprova pelo recibo de número 55.B8.6D.57.3D.5F.65.05.31.5C.F6.AA.1B.C4.8C.75.DC.A5.D1.9F-5, nos termos do Decreto nº 8.683/2016.

Este relatório foi gerado pelo Sistema Público de Escrituração Digital – Sped

MINISTÉRIO DA FAZENDA
SECRETARIA DA RECEITA FEDERAL DO BRASIL
SISTEMA PÚBLICO DE ESCRITURAÇÃO DIGITAL – Sped **Versão: 10.4.1**

RECIBO DE ENTREGA DE ESCRITURAÇÃO CONTÁBIL DIGITAL

IDENTIFICAÇÃO DO TITULAR DA ESCRITURAÇÃO

NIRE	CNPJ	
53202049896	24.425.034/0001-96	

NOME EMPRESARIAL
JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA

IDENTIFICAÇÃO DA ESCRITURAÇÃO

FORMA DA ESCRITURAÇÃO CONTÁBIL	PERÍODO DA ESCRITURAÇÃO
Livro Diário (Completo - sem escrituração Auxiliar)	01/01/2025 a 31/12/2025
NATUREZA DO LIVRO	**NÚMERO DO LIVRO**
LIVRO DIARIO GERAL	14

IDENTIFICAÇÃO DO ARQUIVO (HASH)
55.B8.6D.57.3D.5F.65.05.31.5C.F6.AA.1B.C4.8C.75.DC.A5.D1.9F

ARQUIVOS SUBSTITUÍDOS (HASH)

ESTE LIVRO FOI ASSINADO COM OS SEGUINTES CERTIFICADOS DIGITAIS:

QUALIFICAÇÃO DO SIGNATARIO	CPF/CNPJ	NOME	Nº SÉRIE DO CERTIFICADO	VALIDADE	RESPONSÁVEL LEGAL
Pessoa Jurídica (e-CNPJ ou e-PJ)	24425034000196	JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA: 24425034000196	759095425634695267 9	11/06/2025 a 11/06/2026	Sim
Contador	72802600125	GLEICE FARIAS VIEIRA: 72802600125	829261212944687281 675654	10/07/2025 a 10/07/2026	Não

NÚMERO DO RECIBO:

55.B8.6D.57.3D.5F.65.05.31.5C.F6.AA.
1B.C4.8C.75.DC.A5.D1.9F-5

Escrituração recebida via Internet
pelo Agente Receptor SERPRO

em 28/05/2026 às 09:53:50

47.F7.2D.61.B2.98.4E.E4
FC.11.8E.58.6C.BF.6D.BA

Considera-se autenticado o livro contábil a que se refere este recibo, dispensando-se a autenticação de que trata o art. 39 da Lei nº 8.934/1994. Este recibo comprova a autenticação.

BASE LEGAL: Decreto nº 1.800/1996, com a alteração do Decreto nº 8.683/2016, e arts. 39, 39-A, 39-B da Lei nº 8.934/1994 com a alteração da Lei Complementar nº 1247/2014.

INDICES ECONOMICOS FINANCEIROS

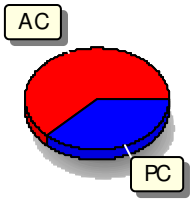
Referência: 01/JAN/2025 até 31/DEZ/2025 - CONSOLIDADO

Liquidez Corrente

Ativo Circulante	297.454.393,83
Passivo Circulante	178.956.187,72
Indice	**1,66**

Interpretação:

Conclui-se que para cada real de dívida de curto prazo (Passivo Circulante), a empresa dispõe de R$ 1,66 de bens e direitos de curto prazo (Ativo Circulante) para pagar a cada R$ 1,00 de dívidas de curto prazo.

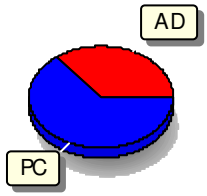


Liquidez Imediata

Ativo Disponível	97.973.497,43
Passivo Circulante	178.956.187,72
Indice	**0,55**

Interpretação:

Demonstra a disponibilidade em R$ 0,55 para cada R$ 1,00 de dívida a curto prazo. Observa-se porem que estamos considerando valores disponíveis no momento para saldar dívidas vencíveis em até 365 dias.

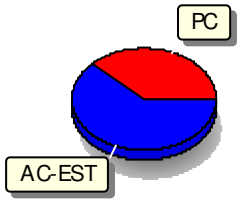


Liquidez Seca

AT.Circulante - Estoque	295.564.775,42
Passivo Circulante	178.956.187,72
Indice	**1,65**

Interpretação:

Conclui-se que ao se excluir os estoques, para cada R$ 1,00 de dívida de curto prazo com terceiros (passivo circulante) a empresa dispõe de R$ 1,65 de bens e direitos de curto prazo.



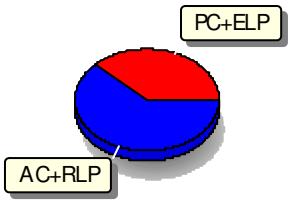
Liquidez Geral

AT.Circulante + Realiz. L/Prazo	297454393,83
Passivo Circul. + Passivo não Circulante	179.778.996,70
Indice	**1,65**

Interpretação: Observa-se que para cada real de dívidas totais (sejam de curto ou longo prazo) com terceiros (passivo exigível), a empresa dispõe de R$ 1,65 de bens e direitos de curto e longo prazo (AC+RLP), para saldar cada R$ 1,00 de suas dívidas vencíveis a longo prazo.

INDICES ECONOMICOS FINANCEIROS

Referência: 01/JAN/2025 até 31/DEZ/2025 - CONSOLIDADO

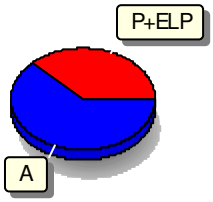


Solvencia Geral

Ativo Total	298.454.976,34
Passivo Circulante + Passivo não Circulante	179.778.996,70
Indice	**1,66**

Interpretação:

Este índice demonstra a capacidade de pagamento da empresa tomando como base o seu ativo total. Nesta situação observa-se que para cada R$ 1,00, de dívidas vencíveis a curto e longo prazo, a empresa dispõe de R$ 1,66 para garantir sua capacidade de pagamento e honrar seus compromissos.

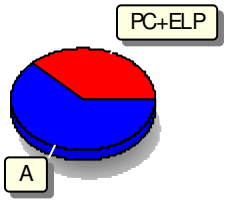


Endividamento

Passivo Circulante + Passivo não Circulante	179.778.996,70
Ativo Total	298.454.976,34
Indice	**0,60**

Interpretação:

Este índice indica a dependência de recursos de terceiros (Passivo Exigível) no financiamento do Ativo. Observa-se, assim, que para cada R$ 1,00 de Capital Próprio, a empresa tomou R$ 0,6 de Capital de Terceiros.



BRASILIA-DF, 31 de Dezembro de 2025

GLEICE FARIAS VIEIRA LIMA:72802600125 Assinado de forma digital por GLEICE FARIAS VIEIRA LIMA:72802600125 Dados: 2026.05.29 10:41:16 -03'00'

CENTROCON CONTABILIDADE E ASSESSORIA EMPRESARIAL LTDA
Contador(a): GLEICE FARIAS VIEIRA LIMA
CPF: 728.026.001-25
CRC/DF: 021005O8

JOSE ANDRE MENDES COIMBRA:47153989153 Assinado de forma digital por JOSE ANDRE MENDES COIMBRA:47153989153 Dados: 2026.06.12 15:35:28 -03'00'

JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA
JOSE ANDRE MENDES COIMBRA
CPF: 471.539.891-53
Sócio Administrador

Brasília, 20 de outubro de 2026.

DECLARAÇÃO DE ACEITAÇÃO E CONHECIMENTO

COMPANHIA DE SANEAMENTO DE SERGIPE – DESO,

ARACAJU – SERGIPE,

Processo PAE nº 528/2026

Pregão Eletrônico SRP nº 44/2026

Prezados Senhores,

A empresa **JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA**, pessoa jurídica de direito privado, inscrita no CNPJ/MF sob o nº 24.425.034/0001-96, portadora da inscrição estadual nº 0776048100140, sediada no SCES Trecho 2, Centro de Lazer Beira Lago, Conj 08, Loja 03, Asa Sul, Brasília/DF, CEP: 70.200-002, por meio de seu representante legal José André Mendes Coimbra, brasileiro, solteiro, sócio-diretor, inscrito no CPF/MF sob o nº 471.539.891-53, pela presente, apresentamos e submetemos à apreciação de V.Sª., nossa Proposta relativa ao PREGÃO ELETRÔNICO Nº 044/2026 em epígrafe, assumindo inteira responsabilidade por quaisquer erros ou omissões que venham a ser verificados na preparação da mesma.

Em tempo, manifestamos nossa expressa aceitação das condições do referido PREGÃO ELETRÔNICO e com a emissão de Notas Fiscais e Fatura diretamente à DESO.

A validade desta Proposta é de 90 (noventa) dias, a contar desta data, de acordo com as disposições do item 10, subitem 10.1.14 deste Edital.

Atenciosamente,

JOSE ANDRE MENDES COIMBRA:47153989153

Assinado de forma digital por JOSE ANDRE MENDES COIMBRA:47153989153
Dados: 2026.10.20 10:52:04 -03'00'

JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA
Sócio-diretor: José André Mendes Coimbra
CPF: 471.539.891-53 / RG: 1179715 - SSP/DF

DECLARAÇÃO INEXISTÊNCIA DE FATO IMPEDITIVO

À

COMPANHIA DE SANEAMENTO DE SERGIPE – DESO,

RUA CAMPO DO BRITO Nº 331 – ARACAJU/SE,

Processo PAE nº 528/2026

Pregão Eletrônico SRP nº 44/2026

OBJETO: Contratação de solução de detecção e resposta a incidentes, auditoria e proteção de dados, detecção e resposta a ameaças baseadas em dados, coleta de fluxos de metadados, e analise constante de dados e de seus repositórios de dados corporativos, plataforma de compartilhamento colaborativo, incluindo prestação de serviço de instalação e configuração, com garantia técnica de 12 (doze meses) meses, com treinamento para capacitação de técnicos da companhia de saneamento de sergipe e serviço de operação assistida e apoio operacional.

JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, pessoa jurídica de direito privado, inscrita no CNPJ/MF sob o nº 24.425.034/0001-96, portadora da inscrição estadual nº 0776048100140, sediada no SCES Trecho 2, Centro de Lazer Beira Lago, Conj 08, Loja 03, Asa Sul, Brasília/DF, CEP: 70.200-002, por meio de seu representante legal José André Mendes Coimbra, brasileiro, solteiro, sócio-diretor, inscrito no CPF/MF sob o nº 471.539.891-53, declara, sob as penalidades cabíveis, que inexiste qualquer fato impeditivo da habilitação de nossa empresa para apresentar proposta na licitação em referência.

Por ser verdade, firmamos a presente declaração para que produza seus efeitos de direito.

Brasília, 20 de outubro de 2026.

_____

JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA
Sócio-diretor: José André Mendes Coimbra
CPF: 471.539.891-53 / RG: 1179715 - SSP/DF

DECLARAÇÃO DE REGULARIDADE QUANTO AO TRABALHO DO MENOR

Processo PAE nº 528/2026

Pregão Eletrônico SRP nº 44/2026

JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA, pessoa jurídica de direito privado, inscrita no CNPJ/MF sob o nº 24.425.034/0001-96, portadora da inscrição estadual nº 0776048100140, sediada no SCES Trecho 2, Centro de Lazer Beira Lago, Conj 08, Loja 03, Asa Sul, Brasília/DF, CEP: 70.200-002, por meio de seu representante legal José André Mendes Coimbra, brasileiro, solteiro, sócio-diretor, inscrito no CPF/MF sob o nº 471.539.891-53, declara que:

Está em comprimento com à pela Lei nº 9.854/99, de 27 de outubro de 1999, que não emprega menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 (dezesseis) anos, salvo menor a partir de 14 (quatorze) anos na condição de aprendiz, nos termos do art. 7º, inciso XXXIII da Constituição Federal do Brasil.

Emprega menor a partir de quatorze anos, na condição de aprendiz?

SIM (X) OU NÃO ( )

Brasília, 20 de outubro de 2026

JOSE ANDRE MENDES COIMBRA:47153989153

Assinado de forma digital por JOSE ANDRE MENDES COIMBRA:47153989153
Dados: 2026.10.20 10:49:33 -03'00'

JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA
Sócio-diretor: José André Mendes Coimbra
CPF: 471.539.891-53 / RG: 1179715 - SSP/DF

DECLARAÇÕES

Pregão Eletrônico SRP nº 44/2026 – DESO,

PAE nº 528/2026,

A empresa **JAMC CONSULTORIA E REPRESENTACAO DE SOFTWARE LTDA**, pessoa jurídica de direito privado, inscrita no CNPJ/MF sob o nº 24.425.034/0001-96, portadora da inscrição estadual nº 0776048100140, sediada no SCES Trecho 2, Centro de Lazer Beira Lago, Conj 08, Loja 03, Asa Sul, Brasília/DF, CEP: 70.200-002, por meio de seu representante legal José André Mendes Coimbra, brasileiro, solteiro, sócio-diretor, inscrito no CPF/MF sob o nº 471.539.891-53, declara que:

a) está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

b) não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;

c) não possui empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

d) cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

e) inexistem fatos supervenientes impeditivos para a sua habilitação na licitação em epígrafe, contendo o compromisso de comunicar eventual superveniência de fato dessa natureza.

f) Suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas

infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

Brasília, 20 de outubro de 2026.

JOSE ANDRE MENDES COIMBRA:47153989153

Assinado de forma digital por JOSE ANDRE MENDES COIMBRA:47153989153
Dados: 2026.10.20 10:02:55 -03'00'

JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA
Sócio-diretor: José André Mendes Coimbra
CPF: 471.539.891-53 / RG: 1179715 - SSP/DF