



DATA SECURITY PLATFORM INSTALLATION

Publishing Information

Software Version	8.6
Publication date	February 13, 2023

Copyright © 2005 -2023 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: About Installing the Data Security Platform.....	1
Chapter 2: Issues and Limitations.....	2
Chapter 3: Antivirus and Endpoint Detection and Response Issues.....	4
Chapter 4: Installing and Configuring the Data Security Platform.....	5
Welcome and License Agreement.....	5
Main Menu.....	5
Selecting the Required Product or Service.....	6
Checking for Existing Products.....	7
Selecting the DSP Server.....	7
Configuring Your License.....	11
Installing Probes.....	12
Configuring the Installation Address for the DataPrivilege Web Application.....	15
Installing and Configuring the Varonis Web Server.....	16
Installing and Configuring Solr and ZooKeeper.....	18
Installing and Configuring DatAlert Analytics.....	20
Configuring Mail Settings.....	21
Configuring Live Updates.....	23
Live Update Security Measures.....	26
Helping to Improve the Data Security Platform.....	28
Enabling User Feedback.....	28
Sharing Data Diagnostics.....	28
Configuring the Proxy Server for Data Diagnostics.....	32
Configuring Reporting Services.....	32
Deploying the Current Tasks.....	35
Configuring Domains.....	35
Adding Active Directory Domains.....	35
Adding Active Directory Domains for Unix.....	40
Adding Azure AD Domains.....	42
Adding LDAP Domains.....	42
Adding NIS Domains.....	43
Adding Samba Domains.....	43

CONTENTS

Adding and Removing Organizational Units.	44
Adding and Removing Directory Services Containers.	45
Discovering Trusted Domains.	47
Adding New Forests.	48
Editing and Removing Domains.	49
Installing Collectors.	49
Configuring Monitored File Servers.	52
Adding Windows File Servers.	52
Adding Unix File Servers.	60
Adding NetApp File Servers.	65
Adding NetApp File Servers Operating in Cluster Mode.	79
Adding Dell File Servers.	85
Adding SharePoint File Servers.	92
Adding SharePoint Online and OneDrive File Servers.	97
Adding Exchange Storage Groups.	97
Adding Exchange Online File Servers.	107
Adding Nasuni File Servers.	108
Adding Panzura File Servers.	112
Adding Nutanix File Servers.	117
Adding Cohesity File Servers.	121
Adding CTERA File Servers.	127
Adding Hitachi NAS File Servers.	132
Adding HP-NAS File Servers.	137
Adding HPE 3PAR File Persona.	144
Adding Unix Samba File Servers.	150
Scality RING Architecture.	155
Adding Dell Fluid File Systems.	167
Adding a New Edge Data Resource.	173
Adding a Box Security Events File System.	176
Adding Shares, Mounts, Exchange Domains, or SharePoint Sites	178
Rescanning Shares.	178
Editing File Servers.	179
Removing Monitored Entities.	181

CONTENTS

Installing a DatAdvantage Windows File Server/Resource Agent	181
Installing File Servers in a Distributed Configuration.	182
Moving File Servers from One Probe to Another.	183
Partitioning Database Tables.	183
Finishing the Deployment.	184
Configuring the Search Button in the Users and Groups Pane.	184
Disabling Event Aggregation in Archiving.	185
Chapter 5: Installing DatAdvantage if DataPrivilege is Already Installed.	186
Welcome and License Agreement.	186
Main Menu.	186
Selecting the Required Product or Service.	187
Setting Existing Products.	187
Configuring Your License.	188
Helping to Improve the Data Security Platform.	189
Enabling User Feedback.	189
Sharing Data Diagnostics.	189
Configuring the Proxy Server for Data Diagnostics.	193
Configuring Reporting Services.	194
Setting Server Credentials.	196
Deploying the Current Tasks.	197
Finishing the Deployment.	197
Chapter 6: Repairing or Upgrading the Data Security Platform.	198
Welcome and License Agreement.	198
Main Menu.	198
Selecting the DSP Server.	198
Selecting the Required Product or Service for Upgrade/Repair.	199
Installing and Configuring the Varonis Web Server.	200
Installing and Configuring Solr and ZooKeeper.	201
Configuring the DSP Working Share.	203
Setting Parameters for DatAlert Analytics Installation.	204
Upgrading Varonis Servers and Monitored File Servers.	205
Configuring Live Updates.	205
Live Update Security Measures.	209

CONTENTS

Helping to Improve the Data Security Platform.	211
Enabling User Feedback.	211
Sharing Data Diagnostics.	211
Configuring the Proxy Server for Data Diagnostics.	214
Upgrading Collectors.	215
Decommissioning File Servers During Upgrade.	215
Deploying the Current Tasks.	216
Finishing the Deployment.	216
Installing or Upgrading the User Interface.	217
Repairing the User Interface.	217
Enabling History Reports for Dates Prior to Upgrade.	218
Chapter 7: SharePoint Online/OneDrive Issues After Upgrading DatAdvantage.	219
Chapter 8: Configuring the Data Security Platform.	220
Welcome and License Agreement.	220
Main Menu.	220
Selecting the DSP Server.	220
Configuring Database Users.	221
Configuring Database Security.	221
Registering Your License.	223
Configuring Your License.	223
Deploying the Current Tasks.	225
Finishing the Deployment.	225
Chapter 9: Uninstalling the Data Security Platform.	226
Main Menu.	226
Selecting the DSP Server.	226
Uninstalling Varonis Servers and Monitored File Servers.	227
Finishing the Deployment.	228
Removing the User Interface.	228
Removing the Management Console.	228
Uninstalling Optical Character Recognition (OCR).	228
Chapter 10: Advanced Configuration of the Management Console.	230
Chapter 11: Managing DSP Servers.	231
Adding DSP Connections.	231

CONTENTS

Removing DSP Connections.	231
Managing the DSP Server.	232
Configuring DSP General Settings.	232
Configuring Your License.	233
Managing DSP Server Components.	234
Adding and Removing DSP Service Components.	235
Managing Updates.	236
Chapter 12: Updating Mail Settings through the Management Console.	239
Chapter 13: Additions to the Master Database.	240
Chapter 14: Mixed Mode Environments.	242
Chapter 15: Pull Proxy Setup.	243
Chapter 16: SQL Farm Support.	247
Chapter 17: Varonis Support Website.	249

1

ABOUT INSTALLING THE 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 policy to meet business needs.

The Data Security Platform addresses the growing need for data usage regulation within organizations, enabling full visibility and accountability of data usage across legal, financial, data security, intellectual property, and data privacy requirements.

2

ISSUES AND LIMITATIONS

Data Security Platform deployment is subject to some issues and limitations.

The Enterprise Installer uses particular names for machines, components, services, and so on; they must not be changed, duplicated, or deleted.

- These include:
 - VrmsDomainDB
 - VrmsDefaultAD
 - Varonis
 - VrmsUI
 - LogicalShadowDB
- Distributed Transaction Coordinator (DTC) must be enabled (and running) on the database machine.
- The Data Security Platform requires SQL Common Language Runtime (CLR) to be enabled on SQL databases. SQL CLR hosts the .NET language engine on SQL servers and is used for adding custom-defined access control lists (ACLs), permissions, types, functions and data aggregates. The Enterprise Installer enables CLR as part of the installation process.
- Creation of DB links is required.
- For IP address resolving, it is recommended to leave the NetBIOS port open.
- IP address resolving limitations (for Windows Servers only):
 - Auditing must be enabled in order to record the log on and log off events from the server.
 - Not all logon types are supported and retrieve IP addresses (for example, Remote Desktop Protocol (RDP) and the Keyboard-Interactive authentication method).
 - The IP address information is retrieved from the Windows Security Event log, which in some cases may not report all IP addresses. This can be verified in the Windows Security Event log.
 - The IP addresses of events that flow into the logon resolver are resolved within a short period of time (a few seconds). Normally, IP addresses are resolved immediately because the logon extractor already has the IP address or logon ID mapping from the Windows Security Event log. However, if there is a large number of Windows Security events and

latency on the server, the queue size limit on unresolved events may be exceeded. The size of this queue is managed by the following registry entry (10K entries are configured by default):

```
HKLM\Software\Varonis\VrnsCifsQueue\UnresolvedEventsQueueMaxSize
```

3

ANTIVIRUS AND ENDPOINT DETECTION AND RESPONSE ISSUES

In rare cases, some Antiviruses (AV) or Endpoint Detection and Response (EDR) tools may interfere with the proper operation of the Data Security Platform. To ensure proper operation, Varonis recommends adjusting the relevant AV or EDR to prevent blocking Varonis products.

The potential AVs or EDRs that may impact Data Security Platform performance include:

- Bit9
- Bitdefender
- Carbon Black
- Cisco
- Crowdstrike
- Cylance
- FireEye
- Illumio
- Kaspersky
- McAfee
- MsSenses
- Palo Alto Networks
- SentinelOne
- Sophos
- Symantec
- Tanium
- Tivoli Monitoring Agent (IBM)
- Trend Micro
- Tripwire
- Tychon

4

INSTALLING AND CONFIGURING THE DATA SECURITY PLATFORM

Before beginning any installation or upgrade, it is strongly recommended to ensure the most updated Microsoft hotfixes and patches that suit your server versions are installed on each server.

Various steps are required for installing and configuring the Varonis Data Security Platform.

Before you begin installing and configuring the Data Security Platform, you must follow several prerequisites. For more information, see [Data Security Platform Installation Prerequisites](#).

Note: If you experience slow response times during installation, disable any personal firewall that is already installed on your machine.

Welcome And License Agreement

The Welcome and License Agreement pages of the wizard allow you to start the setup and review and accept the license agreement details.

To start the installation:

1. Run the Enterprise Installer.
The Welcome page is displayed.
2. Click Next.
The License Agreement page is displayed.
3. Select I agree.
4. Click Next.

Main Menu

You can use the Main Menu to select the required workflow.

To select the required workflow:

1. Complete the previous pages of the Enterprise Installer, until you reach the Main Menu.
2. Select the relevant option:

- Install - Select this option to install the required Data Security Platform products and services. You can use typical settings or customize the installation with more advanced configurations.
- Repair/Upgrade - Select this option to repair or upgrade your currently installed Varonis products.
- Configuration - Select this option to configure your currently installed Varonis products. You can maintain DB passwords and licenses.
- Uninstall - Select this option to remove DatAdvantage and/or DataPrivilege from your system.

3. Click Next.

Selecting The Required Product Or Service

The Product Selection page of the wizard allows you to select the Data Security Platform product or service you want to install, update, or remove.

To select the required Varonis products:

1. Complete the previous pages of the Enterprise Installer, until you reach the Product Selection page.
2. Select the relevant product or service. The available workflows and options vary per the option selected in the Main Menu page.

Important: To install DataPrivilege on a server cluster, you must select the Show advanced options checkbox in order to define the DataPrivilege Web application location.

Note: To download and use the (new) DatAdvantage GUI and the Varonis Web Interface, Solr must also be installed. Selecting the Install DatAdvantage GUI and Install Web UI checkboxes enables access to the Solr installation wizard.

Note: To install the Varonis Web Interface, you must have a license for DatAdvantage.

Note: To install the Data Classification Engine in an environment with existing Varonis products, first run the Repair/Upgrade flow and select Data Classification from the product list. Then, install the DCE from the Management Console.

3. Click Next.

Checking For Existing Products

In the Existing Products page of the wizard, you can check whether there is an existing Data Security Platform installation. This page is relevant when either selecting either DatAdvantage or DataPrivilege.

To indicate whether the Data Security Platform is already installed:

1. Complete the previous pages of the Enterprise Installer, until you reach the Existing Products page.
2. Select whether DatAdvantage or DataPrivilege is already installed.
3. If you selected Yes, DSP Server database is installed here, set the following:
 - Database Server - Enter the name of the server on which the database resides.
 - Authentication - Enter the type of authentication to use, either Windows or SQL.
 - User name - Enter the name of the user account that can access the database.
 - Password - Enter that user account's password.
4. Click Next.

Selecting The DSP Server

Before you proceed with the configurations workflows, you must specify the DSP Server you want to work with.

Note: If you selected Yes and provided the details of your DSP Server on the Existing Products page, this page is not displayed.

To select the DSP Server:

1. Complete the previous pages of the Enterprise Installer, until you reach the DSP Server Selector page.
2. Set the following parameters:
 - DSP Server Services Installation - Select the server and location of DSP services:
 - Server - Type or browse for the name of the server on which DSP services are installed.
 - To install the DSP services on a cluster, select the Cluster Name of the file server resource group to be used.
 - For a non-cluster installation, or if you are only clustering the database, enter the service machine here.

- Location - Type the path name of the folder in which the DSP services are located.
 - For a non-cluster installation, it is recommended to leave the default path displayed in this field.
 - For a cluster installation, set this to a location on the local disk, not to a shared volume.
- Working Share Settings - Select the shared working directory which stores data that is pulled by the DSP SQL database. Set the parameters in the following order:

Note: The DSP's working share is mainly for Solr event processing. The required storage is 60MB for each 1 million events per day.

- User name - The installation account's user name.
- Password - The installation account's password.

Note: Make sure to set the Windows HOMEPATH environment variable with a mounted volume. If it is set with a network path, the RabbitMQ installation will fail.

- Working share - Select the working share, click Browse to specify the working share directory. Make sure you have read and write permissions on the folder.
- Working directory - Once you have specified the working share, the working directory is automatically populated.
 - For a non-cluster installation, it is recommended to leave the default path displayed in this field.
 - For a cluster installation, select a shared volume on the File Server Cluster Application.
- DSP Server Database Installation - Select the server, location and installation credentials of the DSP SQL databases:
 - Database Server - Select or browse for the SQL server on which the DSP databases reside.
 - For cluster installation, select the Cluster Name of the file server resource group and instance name of the SQL cluster to be used. If you intend to cluster only the services, enter the SQL Server machine name and cluster name here.
 - Authentication - Select the authentication method, which can be:
 - Windows Authentication
 - SQL Authentication

Important:

Windows authentication can only be selected if either:

- All Varonis databases and services reside on one physical machine.
OR
- All Varonis databases reside on one physical machine and all Varonis services reside on one different physical machine.

When using Windows Authentication for SQL access, the "Application account" (the AD account that is used instead of the SQL user) must have local admin rights and working share permissions on the Data Security Platform and all Collectors for deployment purposes.

If you want a distributed environment (that is, Varonis databases reside on different physical hosts or Varonis services reside on different physical hosts (for example, the DSP and Probe services), you must select SQL authentication.

- User name - The installation account's user name.
- Password - The installation account's password.
- Save credentials - Select this checkbox to save the installation credentials.
- Application Account - Click this link to edit the details of the account used for all application operations, running services and updating the Varonis databases.

Set the following parameters:

- Authentication - Select the authentication method:
 - Windows Authentication
 - SQL Authentication

Note: On distributed systems, SQL authentication must be selected.

- User name - Type the account's user name (the default user name is VaronisOwner).
- Password - Type the account's password (the default password is automatically generated).
- Confirm password - If you changed the default password, retype your password.
- Custom database location - Click this link to set a customized location for the database.

Note: This option is only available if you have entered valid credentials for the database.

- SQL Server default location - Select to use the default location of the SQL Server as the location for the data files.
- Custom - Select to define a customized location for the data files. Click the Browse button to select the required location.
- General Database Security
 - Allow shrinking of the tempdb on all servers - When selected, the shrink job is performed once a week as part of the regularly scheduled maintenance and the Varonis owner is added as an owner to the tempdb on all servers.
 - Allow partitioning of the tempdb on all servers - When selected, the tempdb is partitioned when installing, repairing, upgrading, or adding a new database server, such as a distributed Probe, to the Data Security Platform. Partitioning requires 'sa' credentials.
 - Allow check disk space - When selected, disk space is checked.
 - If the application server resides on the same machine as the database server, disk space is checked by the local application server.
 - If the application server resides on a different machine, the TRUSTWORTHY database property is set to ON to allow UNSAFE permission set CRL assemblies to the check disk space. The TRUSTWORTHY property indicates whether the SQL Server instance trusts the database and its contents. Both the TRUSTWORTHY property and the UNSAFE permission set are required for checking the disk space on remote machines.

Important: When the application and database servers reside on the same machine, the application server account must be a local system account.

3. In the DataPrivilege Regional Settings area, select the default language to be used for DataPrivilege. (This area is available only when installing DataPrivilege.)
4. Click Next.
If you are installing the DSP services on a server cluster, the Resource Group Selector dialog box is displayed.
5. Do the following:
 - Select a resource group for the DSP services.

Note: Only resource groups with shared storage are displayed.

- Automatically fail over resource group - Select to automatically fail over the selected resource group.

Note: If this option is selected, all services residing on the resource group fail over, not just DSP services.

6. Click Next.

Configuring Your License

During the installation process, you can configure product license registration, automatically or manually.

If you are migrating DSP Analytics, the License Configuration page is displayed.

To configure your license:

1. Complete the previous pages of the Enterprise Installer, until you reach the License Configuration page.

2. For automatic registration:

a. Type the following parameters:

- Customer ID/email - Type the ID or the email of the customer at which the Data Security Platform is being installed.

Note: The customer ID is displayed together with the serial number you received from Varonis. The ID replaces the email as the customer identifier.

- Serial number - Type the product serial number, as supplied by Varonis upon purchase.

b. Click Register. The Varonis products and the platforms the license supports are listed at the bottom of the page.

c. Click Finish.

3. For manual registration (if a problem arises with the automatic process):

a. Type the following parameters:

- Customer ID/email - Type the ID or the email of the customer at which the Data Security Platform is being installed.

Note: The customer ID is displayed together with the serial number you received from Varonis. The ID replaces the email as the customer identifier.

- Serial number - Type the product serial number, as supplied by Varonis upon purchase.
- b. To obtain a license key:
 - i. Go to the Varonis Support Website: <https://support.varonis.com/>.
 - ii. On the Login page, enter your user credentials and click OK.
- Note:** If this is your first visit to the Varonis Support site, you must create a user account.
- iii. Select License > License Registration. The License Registration page is displayed.
 - iv. In the Enter serial field, enter your the Data Security Platform serial number.
 - v. Select one of the following options:
 - Enter unique ID - Enter your unique ID. Use this option if you have an existing DSP installation that is lower than version 5.5.
 - Enter token - Enter your registration token, available on the License Configuration page of the Enterprise Installer. Use this option if your DSP installation is version 5.5 or higher.
 - vi. Click OK. Your license key is generated and displayed at the bottom of the page, along with the details of your license.
 - vii. Copy this number into the License Key field on the License Configuration page.
- c. Click Register. The Next button is enabled.
 - d. Click Next.

Installing Probes

By default, Probes are installed on the same machine as the DSP Server.

If you are installing a distributed system, you can configure on which servers the Probe services and databases reside.

For a cluster installation, the Probe is installed automatically on the same machine as the DSP Server and cannot be changed.

To install probes:

1. Do one of the following:
 - In the Enterprise Installer, navigate to the Probe Server Selector page.

- In the Management Console, from the menu in the left pane, select Management > Components > Root > Probes. The Probes pane is displayed on the right.

Note: Alternatively, you can use the Quick Create menu on the title bar of the Management Console, and select Add New Probe.

2. Click Add.

The New Probe Details window is displayed.

3. On the left menu, click Common and set the following parameters:

- Probe Services Installation - Select the server and location on which Probe services are installed:
 - Server - Type or select the name of the server on which the Probe services are installed.

Note: Do not name the Probe varonis.

- Cluster server - Select if you are installing the Probe on a cluster server.
 - The first Probe server installed may reside in the same system as the DSP Server, or it may be installed on an entirely different machine or cluster from the DSP Server.
 - It is not possible to install the Probe databases in the same system as the DSP and the Probe services on a separate machine from the DSP services.
- Location - Type or browse to the folder on which the Probe services are installed.
- Probe Database Installation - Select the server, location and installation credentials of the Probe SQL database:
 - Database Server - Type or browse for the machine or server cluster on which the database resides.
 - Authentication - Select the required type of authentication, either SQL or Windows authentication.
 - User name - Type the installation account's user name.
 - Password - Type the installation account's password.
 - Save credentials - Select to save the installation account's credentials.
 - To set a custom location for the database, click the Custom database location link.
The Database Location window is displayed.

Set the following parameters:

- SQL Server default location - Select to use the default location of the SQL Server as the location for the data files.
- Custom - Select to define a customized location for the data files. Click the Browse button to select the required location.
- Probe Working Share Settings - Set the Working share and credentials of the account used to access the share:

Important: These credentials are only required when the DSP and Probe servers reside on different physical machines. When the servers reside on the same machine, these parameters are read-only.

- User name - The user name of the account used to access the share (Working share user).
- Password - The password of the account used to access the share (Working share user).
- Working share - Select the Working share.

Important: The Working share resides on the same machine or resource group that hosts Probe services. The folder must be shared with read and write permissions for the Working share user.

If you are installing the Probe on a server cluster, the Resource Group Selector dialog box is displayed.

- Do the following:
 - Select a resource group for the Probe services.
 - Select the Automatically fail over resource group option as necessary.
 - Click OK.
The Credentials dialog box is displayed.
- Do the following:
 - Type the installation account's user name (an account with system administration permissions on the cluster).
 - Type the installation account's password.
 - Click OK.
The Browse for Folder dialog box is displayed.
 - Select the required Working directory share and click OK.
- Working directory - A read-only field, displaying the path name of the Working directory.
- Host Servers Access Credentials - The installation account of the Probe database and serves:

Important: These credentials are only required when the DSP and Probe servers reside on different physical machines. When the servers reside on the same machine, these parameters are read-only.

Note: If you are installing the Probe on a cluster, these fields are automatically completed with the credentials used to access the resource group.

- Use "working share" access credentials - Select to use the Working share user account.

Note: If you select this option, the Working share user account must have system administration permissions on the host machine.

- User name - The installation account's user name.
- Password - The installation account's password.

4. To configure a Probe to support Varonis Edge, 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 Edge 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.

The Probe is installed.

Important: After installing the Probe, add the Probe's Working share to the unmonitored folders list (see [Configuring Unmonitored Folders](#)).

Configuring The Installation Address For The DataPrivilege Web Application

The Web Virtual Directory Configuration page is only displayed if you are installing DataPrivilege.

The DataPrivilege Web application can be installed on the cluster. However, it is not registered as a resource under the resource group. DataPrivilege services are registered as resources under the file server resource group.

To configure the installation address for the Web application:

1. Complete the previous pages of the Enterprise Installer, until you reach the first Web Virtual Directory Configuration page.
2. Set the following parameters as needed:
 - Host name - Click the Browse button to select the host on which the Web application is to be installed.
 - Website - Select the required Website for DataPrivilege.
 - Endpoint - From the drop-down list, select the required endpoint (port/hostheader/https).
 - Test URL - Click the link to test the URL that is created from the other parameters.
 - Virtual directory - Type the name of the virtual directory to be created for the Web application (for example, DP).
3. Click Next.

Installing And Configuring The Varonis Web Server

You can install the Varonis Web Server through the Enterprise Installer or Management Console.

To install and configure the Varonis Web Server:

1. Do one of the following:
 - In the Enterprise Installer, navigate to the Varonis Web Server page.

Note: The Varonis Web Server page is only displayed if you are installing the Varonis Web Interface.
 - In the Management Console, select Management > Components > Root > DSP Server > Service Components, and from the toolbar in the DSP Server - Service Components pane on the right, select Varonis Web Server. The Varonis Web Server dialog box is displayed.

Note: To configure an already installed Varonis Web Server, from the menu in the left pane, under Service Components, select Varonis Web Server to display the Varonis Web Server pane on the right. Proceed to set the parameters in the General tab.
2. Set the following parameters:
 - Installation Web Address

- Host Name - A read-only field, displaying the name of the DSP Server on which the Varonis Web Server will be installed.
- Protocol - From the drop-down list, select the required protocol for the Varonis Web Server. Options are:
 - HTTP
 - HTTPS
- Certification Thumbprint - Enter the required certificate. This option is displayed only if HTTPS is selected from the Protocol drop-down list. The default certificate is Self-signed certificate.
- Relative Path - Type the name of the directory to be created upon installation. The default option is DatAdvantage.
- Port - From the drop-down list, select the access port number of the selected protocol (by default, 443 for HTTPS and 80 for HTTP).
- URL - Click the link to test the URL that is created from the other parameters.
- Installation Credentials - Enter the credentials to be used to install the component.
- Services Installation
 - Location - The location in which the Varonis Web Server is to be installed.
 - Services Port - From the drop-down list, select the required port number to which the Varonis Web Server listens. The default and recommended port is already displayed.
- Event in Solr (Available in Web Interface)
 - Store event data for the last x days - Specify the past number of days for which event data will be stored. The default is 30 days.

Note:

- If you require more than 30 days to store event data, ensure that you have sufficient hardware for the increased number of days. You can specify up to 180 days for the storage period. For the sizing guidelines, contact Varonis Support.
- The Varonis Web Interface Events page supports only events that are available in Solr. Archived and restored events are not reflected in the Varonis Web Interface.
- When flat data is stored, the event history of filtered users is not removed. The event history will be removed according to the configured retention policy (a period of up to 14 days).

- Estimated number of Edge events per day - Specify the estimated number of Varonis Edge events that will be stored.
3. Click Next and proceed to install and configure Solr and ZooKeeper.

Installing And Configuring Solr And ZooKeeper

To install the Varonis Web Server, you must also install Solr and ZooKeeper for event flattening.

To install and configure Solr and ZooKeeper:

Note: Ensure that you have reviewed the Solr/ZooKeeper prerequisites.

1. Do one of the following:

- In the Enterprise Installer, navigate to the Solr Events page, and on the toolbar, click Add. The Solr/ZooKeeper Wizard dialog box is displayed.
- In the Management Console, complete the previous page of the Varonis Web Server installation, until you reach the Solr/ZooKeeper Wizard page.

Note: To configure an already installed Solr or ZooKeeper host, in the Flattening tab of the Varonis Web Server pane, click Add to display the Solr/ZooKeeper Wizard dialog box.

2. Set the following parameters:

Important:

- Solr and ZooKeeper must be installed on a standalone server, separate from that of the Collector and DSP.
 - .NET Framework 4.72 must be installed on the server which Solr and ZooKeeper are installed.
 - Make sure to set the hostname of the dedicated machine, and to install Java JDK 8 on it. Java JDK 9 and higher are not supported.
 - The Solr and ZooKeeper hostnames cannot include underscores (_).
 - Solr and DatAnswers cannot be installed on the same DSP machine. If DatAnswers is installed on the DSP machine, you cannot install Solr on the DSP machine as well.
- Solr Host or ZooKeeper Host - Select the host, Solr or ZooKeeper.
 - Location

- Server - The IP/name of the computer on which Solr or ZooKeeper will be installed.
 - Location - The location on which Solr will be deployed.
 - Data Location - The location on which Solr event collection will be created and saved. Make sure to set different folder locations for Solr and ZooKeeper.
 - Deployment Credentials
 - User name - The user name that will be used to install the selected host.
 - Password - The password of the selected host.
3. Click Add. The installed host is displayed in the table.

Note: Make sure to enter the host name and not an IP address in this field.

4. In the Common area, change the default ports as needed. In the Management Console, this is in the Varonis Web Server dialog box (Flattening tab).

Note: If Solr and DataAnswers are installed on the same computer, the Solr and ZooKeeper ports need to be changed to 8183 for Solr, and 2183 for the Client Communication port.

5. To install the second host (if Solr was installed, you must proceed to install ZooKeeper, and vice versa):
- a. In the Varonis Web Server dialog box, click Add.
 - b. In the Solr/ZooKeeper Wizard dialog box, select the host that was not previously selected and repeat the previous steps in this procedure.

Note: Make sure to enter the host name and not an IP address in this field.

6. Do one of the following:
- In the Enterprise Installer, click Next to continue the installation process.
 - In the Management Console, when Solr and ZooKeeper configuration is complete, click Finish.

Note:

- Upon the installation of Solr, events from the past seven days will be displayed in the Varonis Web Interface. This period will gradually increase until the configured flattening period.
- When flat data is stored, the event history of filtered users is not removed. The event history will be removed according to the configured retention policy (a period of up to 14 days).

Installing And Configuring DatAlert Analytics

You can install DatAlert Analytics through the Enterprise Installer or Management Console.

To install and configure DatAlert Analytics:

1. Do one of the following:

- In the Enterprise Installer, navigate to the DatAlert Analytics page.
- In the Management Console, select Management > Components > Root > DSP Server > Service Components, and from the toolbar in the DSP Server - Service Components pane on the right, select DatAlert Analytics. The DatAlert Analytics dialog box is displayed.

2. In the Services Installation area, set the following parameters:

- Server - Type or select the name of the server on which the DatAlert Analytics component is to be installed. By default, the DSP Server name is displayed.
- Location - Enter the path name to the folder on which the component is to be installed.

Note: After DatAlert Analytics is installed, the above fields are read-only.

3. In the Installation Credentials area, enter the credentials to be used to install the component.

Note: After DatAlert Analytics is installed, the fields in this area are read-only.

4. In the Working Share Settings area, set the following parameters as needed:

Important: The user and the system account must have Full NTFS and Share permissions to the Working share.

- Working share - Select the Working share.
- Working directory - A read-only field, which is automatically populated when a Working share is selected.
- User name - Enter the user name of the account used to access the share (Working share user).
- Password - Type the password of the account used to access the share (Working share user).

Note: Unicode characters (for example, ë, à) should not be used in the working share path when installing the DatAlert Engine, since they are not supported.

5. In the Services Configuration area, set the following:
 - Port - From the drop-down list, select the required port number to which DatAlert Analytics listens.
 - URL - Click the link to test the URL that is created from the other parameters.
6. Do one of the following:
 - In the Enterprise Installer, click Next to continue the installation process.
 - In the Management Console, click Install to install DatAlert Analytics, or click Save to save configuration changes

Configuring Mail Settings

The Mail Settings page allows you to configure email settings.

To configure email settings:

1. Complete the previous pages of the Enterprise Installer, until you reach the Mail Settings page.
2. In the Settings area, select the Server type, SMTP or Exchange Online, and set the following parameters:
For SMTP, do the following:
 - From - Type the address from which alerts are sent.
 - To - Type the list of alert recipients (to type more than one address, use a semi-colon (;) delimiter).
 - SMTP server - Type the name of the SMTP Server.

Note: The SQL Server Reporting Services configuration tool enables configuring email settings for reports. If those settings remain undefined, the Enterprise Installer sets them to the values you set on this page. However, if the Reporting Services email settings are configured correctly, no change is made.

- Port - Type the port number of the email server.
- Use Encryption - Select the SSL/TLS checkbox to use SSL encryption (or TLS for DatAlert).
- Authentication - Select Plain or Login
- Use SMTP credentials - Select to SMTP credentials to connect to the email server.
- SMTP user - Type the SMTP user name.
- SMTP password - Type the SMTP password.

- Outgoing mail bulk size - The maximum number of outgoing emails sent in bulk.
- Retry attempts - The number of retries for emails that were not sent successfully.

Note: For Office 365, use the following server and port settings:

- Use outlook.office365.com for incoming server settings.
- Use smtp.office365.com for outgoing SMTP server settings.
- Incoming Port 993 for IMAP or 995 for POP.
- Outgoing Port Number 587.

For Exchange Online:

- Endpoint - Varonis Mail Sender for all outgoing emails, and Varonis DataPrivilege Mail Reader for DataPrivilege incoming emails.
 - Authorize - Click this button to sign in with the Exchange Online account and credentials. When the authorization is successful, "Authorized as: user account" is displayed next to the Authorize button in the Mail Settings page in the Management Console, and the Save button at the top of the page is enabled.
 - To - Type the list of alert recipients (to type more than one address, use a semi-colon (;) delimiter).
3. To override the above email settings, in the DataPrivilege Mail Settings area, fill in the following Outgoing email details:
- From email – The email account from which DataPrivilege email is sent.
 - From name – A display name for the account.
4. To enable approving DataPrivilege requests by email, in the DataPrivilege Mail Settings area, set the following:
- Server Type - From the drop-down list, select the type of account. For example, POP3.
 - Use Defaults - Click this button to use the default settings defined in the system.
 - Mail server - Type the name of the server used for email.
 - Port - Type the number of the port the email server uses.
 - Use Encryption - Select the SSL checkbox to use SSL encryption or the TLS checkbox to use TLS encryption.
 - User name - Type the name of the user having privileges on the mail server.
- Note:** The account must not be a regular user in the organization.
- Password - Type the user's password.

- Processing email bulk size – The maximum number of emails sent in bulk.
5. To test the email alert settings, click Send Test Mail, located at the top of the page.
 6. Click Next.

Configuring Live Updates

The Live Update functionality enables you to automatically keep your Varonis Data Security Platform installation up to date with content, security updates, and bug fixes. You can choose whether to deploy the updates automatically or manually.

About Live Update

- Live Update is a service in the DSP Server; it uses the local system account.
- 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. A service restart might be required; a notification will be sent accordingly.
- 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.
- To receive email notifications for Live Update deployment updates, configure your email settings in the Management Console; go to Configuration > Mail Settings. For more information about the Live Update notification messages, see the Live Update Email Notifications section below.

Security

- All updates that are downloaded via Live Update are signed using cryptographic keys and verified by DatAdvantage. The update creation process for DatAdvantage prevents the injection of malicious code into these packages.

Limitations

- Some Live Update packages will require user intervention. An email notification will be sent informing that manual deployment is required.
- 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. Do one of the following:
 - In the Enterprise Installer, navigate to the Update Configuration page.
 - In the Management Console, from the menu in the left pane, select Configuration > DatAdvantage Updates. The Update Configuration page 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 Collector credentials.

Note: The user will be used to automatically deploy updates on all Collectors; therefore, the user must be a local administrator on all Collectors in the environment.

5. To configure the Web proxy server for Live Update:
 - a. Go to the DSP Server 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.config` 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"
    />
  </defaultProxy>
</system.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 registered in the Management Console > Configuration > Mail Settings.

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."

Live Update Security Measures

The Varonis Live Update component undergoes various security measures for protection.

About Live Update Protection

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.

Live Update Platform

The Live Update platform comprises the following:

- Live Update service hosted on the Azure cloud - Serves updates to Varonis customers who have the Live Update feature enabled
- Client-side component - Downloads the updates from the cloud to the application installed on the customer side

Technological Controls

Live Update Hosting Service

The Live Update server-side platform has multiple controls on the service including:

- Restricted access to updates of private APIs that are uploaded to the cloud – only specified employees can access the updates of private APIs and automated services that are uploaded to the cloud. Access is restricted from specific IP addresses within the organization; all access is monitored and alerted.
- The Public API access - is protected by a web application firewall (WAF) with profiles to prevent malicious attempts from tampering or attacking the service. The web application firewall also triggers alerts to the Security Operation Center on identified attacks.
- Updates are stored in a private cloud storage location. Access to the uploads for download is granted on the file level using a one-time token issued by the cloud API.
- Updates are hashed and signed prior to being permanently stored. The signature is verified prior to being installed.

Live Update Client Service

- The client-side application is an integral part of the Varonis Platform. The service component is installed with the application and is configurable, allowing users to enable or disable the auto-download and auto-install of the updates from the cloud service.
- The application sends its update level periodically, to identify whether there are new updates available. All Probes are sent over HTTPS to the public API of the Live Update service. When an update is identified, the client follows the configuration of the platform as to the expected behavior (see above).
- The client API verifies the certificate chain, as well as the certificate owner, thereby protecting the platform from man-in-the-middle attacks against the cloud service while working with the HTTPS endpoint.

Note: This functionality requires TLS offloading to be turned off for the Varonis Live Update domain: `liveupdate.varonis.com`.

- Every downloaded update is verified upon download with the file signature; this prevents attackers from tampering with the downloaded file.

Procedural Controls

Security and Functional Testing

- Live Update, as well as supporting services and infrastructure, undergo periodic penetration testing by a third-party security testing company. Component testing is performed in a standalone manner (on an individual basis) as well as per a whole-integrated solution. Findings undergo a triage process and are remediated.
- All updates uploaded to the Live update platform go through a series of testing phases and are deployed in a controlled rollout. The components and the code that make up the updates are managed in the central code repository.
- All software updates sent via Live Update are reviewed and undergo an approval process prior to their release.

Helping To Improve The Data Security Platform

Enabling User Feedback

Note: This functionality is not currently supported. User feedback cannot be enabled.

Sharing Data Diagnostics

By automatically allowing your Data Security Platform logs to be sent to Varonis, you can help to improve the quality, reliability, and performance of the Varonis Data Security Platform.

When you participate in Varonis log data collection, the performance of your software will not be affected in any way, and you may end your participation at any time.

The log data collection enables Varonis to readily identify issues that may arise on customer sites with Varonis system configurations, work to fix them promptly, and provide fixes as needed (as patches or version integration). Varonis will also collect feature usage statistics for reports, rule filters, and so on, to better understand the product usage, and orient the roadmap in an optimal manner.

Note: All the collected data is anonymized before it is sent to Varonis.

Connection Requirements for Data Diagnostics

- Open Port 443 to the following URLs:

- <https://authupload.varonis.net>
- <https://azcusengstorage.blob.core.windows.net>
- Connect to the Proxy server - if the DSP Server does not have an internet connection, see [Configuring the Proxy Server for Data Diagnostics](#)

Varonis Will Collect the Following Information

- Information from your environment about Varonis software and configuration
- Varonis event logs, which might include the names of servers, folders, files, and users:
 - DSP
 - Probe
 - Collector
 - Proxy
 - Windows file server
 - Solr
- All Varonis' Operational Log files
- Errors in the Varonis Notifications table - all database logs
- Hardware information from Varonis servers:
 - CPU
 - RAM
 - Disk
- Failed jobs, during a specified time period
- Failed subscriptions
- Failed sessions (reports)
- Notifications about crashes
- Varonis service states
- License information
- Customer email addresses, as recorded in the license registration
- Statistical information:
 - Data Classification Engine/DatAlert/DatAlert Analytics counters - number of rules and hits per rule, number of alerts, and so on
 - DataPrivilege configuration

- Automation Engine/Data Transport Engine counters and usage - Broken Permissions Repair, Global Access Groups Remediation, and data transport
- Varonis Edge statistics:
 - Configuration
 - Vendors
- Report statistics:
 - Filter usage
 - Template usage
- UI audit information

Data Anonymization

The logs are saved to a specified location so that the data can be reviewed locally. The following data will be anonymized before it is sent to the OMS:

- Password/connection strings
- IP addresses
- SIDs
- Server names (if De-Anonymize is not selected)
- DC names
- Users that Varonis uses for crawling/work

Varonis Will Not Collect the Following Information

- Passwords
- File content

Varonis Retention Policy

- During collection – incoming data is kept for 90 days
- Official requests to delete all data can be submitted at any time via support tickets
- Opt-out – unless requested via support to delete immediately, data collection will stop upon opt-out and will be deleted within 90 days

Data Diagnostics Flow

1. The daily job is responsible for collecting the relevant data. It uses the credentials entered for the Advanced Configuration area of the Data Diagnostics page (as described in the following procedure, Enabling Data Diagnostics via the Installer). If credentials are missing, it used the local system.
2. The logs are saved to a specified location, so that the data can be reviewed locally.
3. Data is anonymized (locally).
4. All logs are transferred over a secure channel directly to Azure Blob storage.
5. A parser service (Azure) takes the data enrichment, converts it into a universal log format, and uploads it to Azure Log Analytics located in the United States.
6. Access to logs and statistical data is based on role-based access control. The data will be used only for investigation and product optimization.

Enabling Data Diagnostics via the Management Console

To enable data diagnostics via the Installer:

1. Complete the previous pages of the Enterprise Installer, until you reach the Data Diagnostics page.
2. In the Share Log Data area, select I agree to participate in log data collection in accordance with the Varonis Privacy Policy. (Clear this checkbox to decline participation.)
3. To remove anonymization on the server, select the De-anonymize Server Names checkbox. (This checkbox is cleared by default, to ensure that the data will be anonymized before it is sent to the OMS.)
4. To change the credentials used to collect the logs, in the Advanced Configuration area, set the following:
 - Log path - By default, logs are saved in the working directory on the DSP Server. To change the location at which logs are saved, enter the preferred path.
 - User name - Enter the name of the user account that has access to the log path.
 - Password - Enter that account's password.
5. Click Next. The Check Prerequisites dialog box is displayed, indicating the validation status of each prerequisite.

Configuring the Proxy Server for Data Diagnostics

To configure the proxy server for data diagnostics:

1. Go to the DSP Server installation location. By default, it is C:\Program Files (x86)\Varonis\DatAdvantage\DSP Server.
2. Go to the subfolder, Support Assistant\LogsUploader.
3. Open the `SPUpload.exe.config` file in Notepad. (You may need to open Notepad with "Run As Administrator" if User Account Control (UAC) is configured.)
4. Find the section named `<defaultProxy>` under `<system.net>`. For more information about this section, see [Microsoft Docs](#).
 - a. If the section is commented out, uncomment it.
 - b. If the section does not exist, add it (see the example provided at the end of this procedure).
5. 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"
    />
  </defaultProxy>
</system.net>
```

Configuring Reporting Services

The Reports component enables generation of Data Security Platform reports.

This page is only displayed if you selected the Reports checkbox in the Product Selection page.

If Reporting Services were configured during a previous installation, this page is read-only.

To prevent a security loophole in which all of the Data Security Platform data could be viewed by unauthorized persons, the Data Security Platform changes the authentication and authorization methods of the Reporting Services installation to its

own methods. Therefore, other applications may have issues if installed in the same Reporting Services installation.

To configure reporting services:

1. Complete the previous pages of the Enterprise Installer, until you reach the Reporting Services Configuration page.
2. Configure the machine on which the reporting services will be installed:
 - Installation Credentials - Enter the installation account's credentials.
 - User name - Enter the installation account's user name.
 - Password - Enter the installation account's password.
 - Reporting Service Installation
 - Host name - Enter the name of the host on which the reporting service resides.
 - Instance - Select the database instance on which the reporting service resides.
 - Authentication - From the dropdown list, select the type of authentication to be used.
 - User name - Enter the user name of the reporting service's account.
 - Password - Enter the password of the reporting service's account.
 - Protocol - Select the required web interface protocol.
 - Port - Enter the number of the port to which the reporting service listens.
 - Report Configuration - Configure default report settings.
 - Report CSV export path - Enter a local or UNC path to which the CSV file containing report results will be saved if the report exceeds the maximum rows to display.
 - User name - If the export path is located on a share, enter the user name of an account having Read/Write permissions to the share.
 - Password - Enter the account's password.
 - Maximum rows to display in report - Set the maximum number of rows to be displayed in the report. If the report contains more rows than this number, the additional rows will not be displayed. Instead, a CSV file containing the full set of results will be created and saved to the designated export path.
 - Number of rows to display in short preview - Set the number of rows to be displayed in the short preview.
 - Number of executions saved in subscription history - Set the number of report executions to be saved in the subscription history. This setting

controls the results of the Execution History button in DatAdvantage's My Subscriptions page.

- Web UI Scheduled Searches
 - Maximum email size (MB) - Set the maximum size (MB) of email that can be sent by a scheduled search in the web UI. If the email size exceeds this limit, the email will not be sent. The scheduled search settings in the web UI enable saving the output to a file share if the email exceeds the maximum size limit. It is recommended to set the email size limit according to your organization's policy.
- Template Ownership and Visibility
 - The Enterprise Manager can see all templates and subscriptions - Select this option as necessary.
 - Replace template and subscription owner - Click this link to replace the original owner with a new owner for all owned templates and/or subscriptions. Selecting an option that includes "templates" will affect the templates owned by the original owner in DatAdvantage and the saved searches in the Varonis Web UI. Selecting an option that includes "subscriptions" will affect the subscriptions owned by the original owner in DatAdvantage and the scheduled searches in the Varonis Web UI.
- Report Watcher
 - Limit reports disk usage on all servers to ___ GB - Select the relevant limit on disk usage. When the reporting service uses more than the specified disk space, report processes are stopped on the relevant server until the disk usage is less than the limit; an email notification is sent to the system administrator.
 - Limit reports CPU time on all servers to ___ Minutes - Select the relevant limit for CPU time.
- Report Display Options - Configure the display options for all reports: title, subtitle, look and feel, etc.

Important: Applying these settings may take a long time, during which DatAdvantage will not be available.

- Select the custom logo for DatAdvantage
- Select the custom logo for DataPrivilege
- Advanced - Click this link to set the following display options in bulk:
 - Report Title - Click the pencil icons to set whether report names or template names are displayed for the report titles and subtitles.
 - Report Content - Click the pencil icons to set the following options:

- Display logo in report
- Display report filter
- Display the description of the report template
- Hide number of nested groups for grouped results
- Report Formatting - Set the following formatting options:
 - Look and feel
 - Date Format - Applied to all templates
 - Time Format - Applied to all templates
- Affected Report Templates - The changes set above are implemented in all the reports selected in this area. Options are:
 - User-defined report templates
 - Predefined report templates

3. Save your changes

Deploying The Current Tasks

You can deploy currently defined tasks.

To deploy the current tasks:

1. Complete the relevant pages of the Enterprise Installer, until you reach the Deployment Progress page.
2. Click Install.
The selected products and services are installed.
3. To continue defining resource and options with the Enterprise Installer, click Next.

Configuring Domains

Adding Active Directory Domains

Only an Active Directory domain can be configured as the default domain, which is the domain on which the DSP Server is installed. Other domains can be installed and used, as long as Active Directory is also installed.

You can install Active Directory domains and configure related settings including domain properties, user credentials, Directory Services options such as auditing, containers, and domain controller settings.

Note: Monitoring two domains with the same NetBIOS name is not supported.

Note: To run ADWalk on Windows 2016 and 2019 file servers, the following are required:

- A user with backup operator and power user privileges.
- Grant the Varonis service account with permissions to the SAM account database via the Microsoft Network access: Restrict clients allowed to make remote calls to SAM security policy setting, either individually via secpol.msc, the Local Security Policy editor, or in bulk via the Group Policy setting.

To add an Active Directory domain:

1. Do one of the following:

- In the Enterprise Installer, navigate to the Domain Trusts page, and on the toolbar, click Add.
- In the Management Console, 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.

2. From the Domain Type drop-down list located at the top of the page, select Active Directory.

3. Set the following parameters:

- Domain Properties
 - Domain name - Type the name of the relevant domain. The Auto-discover DC link becomes active.

Note: This option is read-only if you are editing an existing Active Directory.

- Domain controller name - Type the domain's Domain Controller name. Alternatively, enter the user credentials described below, then fill in any machine name in the remote domain and click the Auto-discover the domain controller link. The DC is saved in the database.
- Force using this specific Domain Controller - Select this checkbox to force the system to use only the DC specified above.

- Auto-discover the domain controller by any domain computer - Click the link to automatically discover the Domain Controller. The link becomes active when you enter a domain name.
- AD provider - From the drop-down list, select an Active Directory provider to override the default provider. The provider represents the technique to be used to walk the domain.

Important: Contact Varonis Support before changing the provider.

- Group types - From the drop-down list, select Only Security Groups to limit the walk to only security groups, or select All (the default option) to walk all groups, including distribution groups.
- Enable RFC 2307 - Select this checkbox to enable using LDAP as a Network Information Service (NIS) for SID resolution, according to the RFC 2307 memorandum.

Note: Be sure to select this option for HP-NAS devices.

- Domain User Credentials
 - User name - Set the name of the user that can access this domain. No special credentials are needed.

Note: If the domain is scanned by Directory Services as well, the user must be authorized to manage auditing and security logs on each DC. The domain part of the user name should be in NetBIOS format, since Directory Services auditing does not support fully-qualified domain names in the user name due to a limitation of LDAP.

- Password - Type the user's password.

4. To configure Directory Services options, do the following:

- a. On the left menu, select Directory Services.
The Directory Services settings are displayed.
- b. Set the following parameters:
 - Directory Service Auditing
 - Crawl directory services for structure and permissions - Select this checkbox to enable monitoring the domain's structure and permissions.
 - Collect Events - Select this checkbox to collect Directory Services events. This option is only available if the Crawl directory services for structure and permissions option is selected.
 - Containers


- Containers - From the drop-down list, select the Directory Services container.
- Click the Advanced Policy Settings link to configure the auditing policy. The Advanced Policy Settings dialog box is displayed.
- Apply Varonis Auditing Policy (on the Domain level) - Select to use the Varonis Auditing Policy GPO to configure the domain controller. The GPO is enforced and linked to the domain's root. This GPO does the following:
 - Adds Audit Policy:Success to the current Audit account logon events, Audit account management and Audit logon events values (previous settings are kept). These policies are located under Computer Configuration > Policies > Windows Settings > Security Settings > > Audit Policy.Local Policies.
 - Enables NTLM operational log event collection as described in [Manually Enabling NTLM Operational Log Event Collection](#).
 - Adds the user provided in the Domain User Credentials to the Event Log Reader group.
- Set Credentials - Click to set the credentials of the user who is authorized to configure GPO auditing. For this purpose, a user with domain admin credentials (or enterprise admin, for forests) is required. These credentials are not saved.

Note: If your organization's policy for this user is deny logon locally to the domain controller, you cannot configure the advanced policy settings, but will instead need to manually configure event collection for this domain. For more information, see the Directory Services Deployment Guide.

5. To configure Domain Controllers, do the following:

- a. On the left menu, select Domain Controllers.
The Domain Controllers settings are displayed.

b. Set the following parameters:

- Domain Information
 - Click the green arrow  to add additional domain controllers. Any domain controller in the domain can be added.
 - To remove domain controllers, select the domain controller and click Remove.

CAUTION: Clearing a domain controller may result in the loss of a large number of events.

- Click Manage Proxies to manage Probe proxies for Directory Services probing.
 - A Probe proxy should be located in close proximity to the resource being monitored. It can be installed on any Windows machine in the same LAN as the resource.
 - A Directory Services proxy agent functions as a local event collection process. Its use can greatly improve both performance and network data load, since it reads the logs, filters out irrelevant events and aggregates the remaining data (just as the Probe does). These activities are all carried out over a LAN (or locally if the agent is installed on the DC itself), instead of the WAN (if the Probe does not reside in the same LAN).

Important: While a single proxy can be used to monitor more than one resource, it is strongly recommended that at least one Directory Services proxy agent is defined per site, and that all the site's DC events are collected through its respective proxy agent.

- At least one directory service proxy agent is required per site (the Probe/Collector may monitor the DCs from its own site).
- It is highly recommended that a directory service proxy agent be installed on each DC having at least a medium amount of activity.
- Network traffic is best reduced by installing the directory service proxy agent on the DCs themselves, as this ensures only relevant data is passed over the network, after events have been filtered and the event log has been aggregated.
- A DC that has to withstand network communication issues must have a proxy agent installed on it.

Note: The proxy agent's buffer functions just as the agent does. If communication issues occur, the accumulated events are sent to the Probe/Collector when communication is re-established.

- Different Active Directory domains may be monitored by different Probes/Collectors (using different containers). This can help in distributing network traffic.
- Click Rescan DCs to rescan domain controllers and update their settings.
- Automatically detect Domain Controllers - Sets the system behavior when a domain controller is added to or removed from a domain. The following options are available:

- Never - New and deleted domain controllers are not detected.
 - Detect and notify by mail - New and deleted domain controllers are detected and email notifications are sent.
 - Detect and monitor automatically - New and deleted domain controllers are detected and new domain controllers are automatically monitored by DatAdvantage.
 - Detect, notify and monitor automatically - New and deleted domain controllers are detected, email notifications are sent, and new domain controllers are automatically monitored by DatAdvantage.
6. To configure the commit credentials to allow users to use different commit credentials than the configured domain user credentials, on the left menu, click Commit and set the following parameters:
- Domain Commit Credentials - Set the credentials to be used for committing DataPrivilege changes on the domain. The account used must be a member of the Administrators group.
 - Clear the Use domain user credentials checkbox to use different commit credentials than those defined for the domain user. (By default, this checkbox is selected to use the domain user credentials, and the User name and Password fields are disabled for editing.)
 - In the User name and Password fields, enter the relevant user name and password.
 - Group OU - Select the organizational unit in which DataPrivilege creates groups. Groups created by DataPrivilege reside in the default base OU, unless otherwise specified. This includes the groups created by the Automation Engine, if it is installed.
 - OU - Click the Browse button (...) to select the required OU.
7. Click Install.

Adding Active Directory Domains for Unix

You can specify the container in which the Active Directory domain resides, the technology which to map the Unix machine to the Active Directory, the zone to be monitored as a domain in DatAdvantage, and the user credentials to access the domain.

Note:

To monitor Linux data sources that have Centrify auditing enabled:

1. Before adding Linux data sources to be monitored, in the Centrify DirectAudit configuration file, disable auditing for the root user used to install the Varonis Unix agent.
2. Post-installation:
 - When running FileWalk and ADWalk with domain user credentials, disable auditing for this domain user using the Centrify Audit Manager. In this case, for the root user used to install the Varonis Unix agent, direct auditing can be enabled.
 - When running FileWalk and ADWalk with root user credentials, ensure that direct auditing is still disabled.

To add an Active Directory domain for Unix:

1. Do one of the following:
 - In the Enterprise Installer, navigate to the Domain Trusts page, and on the toolbar, click Add.
 - In the Management Console, 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.

2. From the Domain Type drop-down list located at the top of the page, select Active Directory for Unix.
3. Set the following parameters:
 - Active Directory for Unix
 - Domain container - From the drop-down list, select the container in which the Active Directory domain resides. An Active Directory domain to be mapped for Unix must be contained in an Active Directory domain that is already defined in DatAdvantage.
 - Technology - From the drop-down list, select the technology used to map the Unix machine to Active Directory. The Data Security Platform currently supports Centrify's DirectControl and Samba WinBind.
 - Zone - From the drop-down list, select a zone to be monitored as a domain in DatAdvantage. Note that several zones can be mapped to the same Active Directory.

- Domain User Credentials
 - User name - Set the name of the user that can access this domain.
 - Password - Type the user's password.
 - Use credentials of domain controller - Select this option to use the credentials defined for the domain container.
4. Click Install.

Adding Azure AD Domains

For details, see Adding and Editing an Azure AD Domain in [Azure AD Deployment](#) in the M365 Deployment Guide.

Adding LDAP Domains

You can install an LDAP domain and configure related settings, including the domain properties and user credentials.

To add an LDAP domain:

1. Do one of the following:
 - In the Enterprise Installer, navigate to the Domain Trusts page, and on the toolbar, click Add.
 - In the Management Console, 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.

2. From the Domain Type drop-down 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. Click Install.

Adding NIS Domains

You can install an NIS domain and configure related settings, including the NIS domain properties and the server on which the domain is located.

To add an NIS domain:

1. Do one of the following:
 - In the Enterprise Installer, navigate to the Domain Trusts page, and on the toolbar, click Add.
 - In the Management Console, 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.

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. Click Install.

Adding Samba Domains

You can install a Samba domain and configure related settings, including the domain properties and server on which the domain is located.

To add a Samba domain:

1. Do one of the following:

- In the Enterprise Installer, navigate to the Domain Trusts page, and on the toolbar, click Add.
- In the Management Console, 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.

2. From the Domain Type drop-down 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 drop-down list, select the required type of authentication, either Windows or SSH-keys.
- User name - Set the name of the user that can access this domain.
- Password - Type the user's password.

4. Click Install.

Adding and Removing Organizational Units

The addition of an OU allows you to limit the ADWalk to a specific OU.

Adding Organizational Units

If you select an OU, only that OU is monitored. If you do not select an OU, the entire domain is monitored.

To add an OU:

Note: You cannot add organizational units for Azure Active Directory domains.

1. Do one of the following:

- In the Enterprise Installer, navigate to the Domain Trusts page.
- In the Management Console, select Management > Components > Root > Domains. The Domains pane is displayed on the right.

2. Select the Active Directory on which you want to monitor specific OUs.

3. On the OU toolbar, click Add.
The Active Directory Selection dialog box is displayed.
4. Select the required OU from the list.
5. Click Add.
The OU is added to the domain and the dialog box is closed.

Removing Organizational Units

The definition of an OU can be removed from DatAdvantage without affecting the OU itself.

To remove an OU:

Note: You cannot remove organizational units for Azure Active Directory domains.

1. Do one of the following:
 - In the Enterprise Installer, navigate to the Domain Trusts page.
 - In the Management Console, select Management > Components > Root > Domains > <domain name>, where <domain name> is the name of domain 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 drop-down arrow.
All of the domain's OUs are listed.
3. Select the OU you want to remove, and on the OU toolbar, click Remove.
The Organizational Unit Deletion confirmation window is displayed.
4. Click Yes.
The selected OU is removed.

Adding and Removing Directory Services Containers

Directory Services containers must be defined to monitor Directory Services events (such as changes made to the users and groups repository).

Adding Directory Services Container

To add a Directory Services container:

1. Do one of the following:
 - In the Enterprise Installer, navigate to the Domain Trusts page, and on the toolbar, click Containers.

- In the Management Console, select Management > Components > Root > Domains, and on the toolbar, click Containers.

The Manage Containers dialog box is displayed.

2. Click Add.

The Container Configuration dialog box is displayed.

3. Set the following:

- General
 - Container - Type the name of the container.
 - Probe - From the drop-down list, select the name of the required Directory Services Probe.
 - Collector - From the drop-down list, select the required Collector.
 - Container Type - From the drop-down list, select the required container type, for example, Directory Services.
- Database Settings - Credentials of the account used to install the database:
 - Database Server - Type or browse for the machine on which the database resides.
 - Authentication - From the drop-down list, select the required type of authentication, either SQL or Windows authentication.
 - User name - Type the account's user name.
 - Password - Type the account's password.
 - Save credentials - Select this checkbox to save the database credentials.
 - Custom database location - Click this link to set the location of data files.
- Database Installation Credentials - Installation credentials for the machine on which the database resides:
 - User name - Type the installation account's user name.
 - Password - Type the installation account's password.

4. Click Install.

Removing Directory Services Containers

The definition of a Directory Services container can be removed from DatAdvantage without affecting the container itself.

Note: The default container cannot be removed.

To remove a directory service container:

1. Do one of the following:

- In the Enterprise Installer, navigate to the Domain Trusts page, and on the toolbar, click Containers.
- In the Management Console, select Management > Components > Root > Domains, and on the toolbar, click Containers.

The Manage Containers dialog box is displayed.

2. Select the container to be removed.

3. Click Remove.

The Container Configuration window is displayed.

4. Click Remove.

The Container Configuration closes and the container is removed.

5. In the Manage Containers window, click OK.

Discovering Trusted Domains

Domains that have been removed from DatAdvantage can easily be restored.

To discover trusted domains:

1. Do one of the following:

- In the Enterprise Installer, navigate to the Domain Trusts page, and on the toolbar, click Rediscover domains.
- In the Management Console, select Management > Components > Root > Domains, and on the toolbar, click Rediscover domains.

A message is displayed, warning that unsaved changes will be lost.

2. Click Yes to continue.

The Rediscover Domain window is displayed.


3. Do the following:

- a. Select whether you want to rediscover domains from a local or remote computer.
- b. If you select a remote computer, provide the remote computer's name and the credentials required for accessing the computer.

Important: The user name must be entered using the NetBIOS syntax. For example, domain\username not domain.com\username.

c. Click Rediscover.

The rediscovered domains are listed under the Unselected rediscovered domains area.

4. Select the domains you want to restore and click the down arrow .
The selected domains are listed in the Selected rediscovered domains area.
5. Click OK.
The domain is restored and the dialog box is closed.

Adding New Forests


You can add new domain forests and specify the machine (local or remote) on which the forest resides.

To add a new domain forest:

1. Do one of the following:
 - In the Enterprise Installer, navigate to the Domain Trusts page, and on the toolbar, click Add Forest.
 - In the Management Console, select Management > Components > Root > Domains, and on the toolbar, click Add Forest.

A message is displayed, warning you that unsaved changes will be lost.
2. Click Yes to continue.
The New Forest page is displayed.
3. Do the following:
 - a. In the Forest area, select the machine on which the forest resides.
 - b. If you select a remote computer, provide the remote computer's name and the credentials required for accessing the computer.

Important: The user name must be entered using the NetBIOS syntax. For example, `domain\username` not `domain.com\username`.

- c. Click Rediscover.
The rediscovered domains are listed in the Unselected rediscovered domains area.
4. Select the domains you want to restore and click the down arrow . At least one domain must be selected.
The selected domains are listed in the Selected rediscovered domains area.

Important: If you select domains, only the selected domains are monitored. If no domains are selected, all domains residing within the forest are monitored.

5. Click OK.

Editing and Removing Domains

You can edit defined domains.

Editing Domains

To edit defined domain trusts:

1. Do one of the following:
 - In the Enterprise Installer, navigate to the Domain Trusts page.
 - 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 domains to make sure the Data Security Platform monitors the user, group, and computer accounts from the specified domains.
3. Select the Events checkbox of the required domains to enable running FileWalk and collecting Directory Services events on them.
4. To edit a domain, double-click its row, or select the domain and click Edit. The Domain Properties page is displayed, where you can edit the domain as required.

Removing Domains

You can remove domains.

To remove a domain:

1. Do one of the following:
 - In the Enterprise Installer, navigate to the Domain Trusts page.
 - In the Management Console, select Management > Components > Root > Domains. The Domains pane is displayed on the right.
2. In the grid, select the domain you want to remove, and on the Domains toolbar, click Remove. The Domain Deletion confirmation window is displayed.
3. Click Yes. The selected domain is removed.

Installing Collectors

Collectors are optional servers that interface between monitored file servers and their Probes.

They are often deployed in environments where file servers and the Probe reside in different locations.

Each Collector can only interface with one Probe. Additionally, once a Collector has been configured to work with a specific Probe, that Collector must always be configured to work with the same Probe.

Note: Collectors installed on the supported Windows Server versions are configured to use Microsoft's LocalDB feature.

To install Collectors:

1. Do one of the following:

- In the Enterprise Installer, navigate to the Collectors page.
- In the Management Console, from the menu in the left pane, select Management > Components > Root > Collectors. The Collectors pane is displayed on the right.

Note: Alternatively, you can use the Quick Create menu on the title bar of the Management Console, and select Add New Collector.

2. Click Add.

The New Collector Details window is displayed.

3. On the left menu, click Common and then set the following parameters:

- Collector Services Installation - Select the server and location on which Collector services are installed:
 - Server - Type or select 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.
 - Cluster server - Select this checkbox if you are installing the Collector on a cluster server.
 - Location - Type or browse to the folder on which the Collector services are installed.
- Collector Working Share Settings - Set the Working share and credentials of the account used to access the share:
 - User name - Type the user name of the account used to access the share (Working share user).
 - Password - Type the password of the account used to access the share (Working share user).
 - Working share - Select the Working share.

Important: The Working share must be shared with read and write permissions for the Working share user, and its name must not include special characters or spaces.

If you are installing the Collector on a server cluster, the Resource Group Selector dialog box is displayed.

- Do the following:
 - Select a resource group for the Collector.
 - Select the Automatically fail over resource group option as necessary.
 - Click OK. The Credentials dialog box is displayed.
- Do the following:
 - Type the installation account's user name (an account with system administration permissions on the cluster).
 -
 - Click OK. The Browse for Folder dialog box is displayed. Type the installation account's password.
 - Select the required Working directory share and click OK.
- Working directory - Type the installation account's - A read-only field, displaying the path name of the Working directory.
- 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 resource group.

- Use "working share" access credentials - Select to use the Working share user account.

Note: If you select this option, the Working share user account must have system administration permissions on the host machine or resource group.

- User name - The installation account's user name.
- Password - The installation account's password.
- LocalDB Installation - Select to use LocalDB on the Collector:
 - Use LocalDB on this Collector (advanced) - Select to use a local database (LocalDB) on this Collector. By default, this option is selected. If this option is cleared, the LocalDB is not installed on the Collector.

Note: This option is only available if the relevant advanced configuration setting is enabled. Contact Varonis Support for more information.

4. To configure a Collector to support Varonis Edge, on the left menu, click Edge and then do the following:

Note: Before configuring an Edge file server, make sure to first install Java Development Kit 1.8/JRE (Java 8) 64-bit on each Edge Collector server or Probe that supports Edge, and define JAVA_HOME as a system environment variable. For more information, see the [Varonis Edge Requirements](#) and the Java documentation.

- 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 Edge 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.

The New Collector Details window is closed and the Collector is installed.

Important: If the Collector is going to be monitored, after adding it as a data source, add the Collector's Working share to the unmonitored folder.

Configuring Monitored File Servers

The Data Security Platform monitors activity on various servers and platforms. This section describes how to configure the monitored file servers and platforms.

Adding Windows File Servers

You can install Windows file servers and set the parameters for data collection, file servers, FileWalk credentials, Varonis Agent installation settings, and shares.

To add a Windows file server:

1. Do one of the following:
 - In the Enterprise Installer, navigate to the Monitored File Servers page and click Add.
 - 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.

2. On the left menu, click Common and set the following parameters:

a. Resource Type

- Select resource type - If you select a file server's type from this drop-down list, this is the type that is used no matter what type was detected earlier.

Note: If you typed the file server's name manually, you must enter the FileWalk credentials before you can use the Detect link, due to permission requirements. If the type still cannot be detected, use the override field.

- Detect resource type - Click this link to detect the type of file server you selected. (If you used the Browse button to locate the file server's name, its type is detected automatically as long as you have already entered credentials.)
- Detected resource type - Indicates the file server type, if it was automatically detected.

b. Resource Details

- Resource/Server Name - Type the resolved name or IP address of the file server to be added, or click the Browse button to locate it.

c. Data Collection Details

- Probe - From the drop-down list, select the Probe to be used with the file server.
- Collector - From the drop-down list, select the required Collector.

Important: Once you have configured a Collector to interface with a specific Probe, you must use that Collector with the same Probe. This means that if you have already configured a Collector to interface with the selected Probe while adding a monitored file server, you must either select the same Collector, a Collector that is not yet connected to a Probe, or <No Collector>. If no Collector is used with the Probe server, select <No Collector>.

d. FileWalk Credentials - File System operations include the directory crawl (FileWalk), event collection (if set) and user crawl (ADWalk) on local accounts (if set). This account must have the backup operator and power user roles (Windows or NAS devices) on the file server during installation.

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

- User name - Type the name of the user account to be used for FileWalk, event collection and local ADWalk.
- Password - Type the account's password.
- Add this user account to the Filtered Users list - This is the default user account for Data Security Platform operations. If you clear this checkbox, a large number of events generated by the Data Security Platform will be collected.

e. Varonis Agent Installation

- Do not install or upgrade the filter agent on this server - Select this checkbox if you do not want the Varonis filter agent automatically installed or upgraded on the file server.
- Do not install/upgrade/remove the Varonis FileWalk agent - Select this checkbox if you do not want the Varonis FileWalk agent automatically installed, upgraded, or removed from this file server.
- Click the Agent Deployment link to define the credentials used to install the agent on the file server. 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.

Note: If you select this option, ensure that the FileWalk 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.
- Physical Machines - Settings for adding a Windows cluster physical node
 - Server - Type or browse to the cluster's physical node name and click Add.
 - Auto detect - Click this button to automatically detect cluster physical node host name.

Note: When a cluster is detected, the word "(cluster)" is added to the Detected resource type field in the Resource Type area.

3. To select specific shares for the file server, on the left menu, click Shares and do the following:

- a. In the Available Shares area, select the required shares and click the down arrow .
The selected shares are moved to the Registered Shares area.
- b. In the Ignore Detection column, select the shares to be ignored (and not be the subject of notifications) by the resource monitor. Note the following scenarios:
 - Shares manually moved from registered shares to available shares should be selected.
 - When users manually add shares from available shares to registered shares, the checkbox must be cleared.

- c. For each share, review and set the following information as required:

Note: If the file server is installed only for use with DataPrivilege, event collection is disabled.

- Share Name - The name of the share.
- Path - The path on which the share resides.
- Protocol - The protocol defined for the share.
- Events - Select this checkbox to collect 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 collection and crawling.

- Mixed Security - In Windows environments, NT ACL extraction is always used.
- d. In the Automatic Detection area, set the following:
 - Automatically detect shares - DatAdvantage detects shares that reside at the highest level of the hierarchy and that are not already monitored. It gives preference to administrative shares over equivalent regular shares. From the drop-down list, select the relevant option:
 - Never - Select to instruct DatAdvantage not to detect shares or mounts automatically.
 - Detect and notify - Select to send users email that lists all newly detected shares or mounts. Unreachable shares and mounts are removed from DatAdvantage.
 - Detect and monitor - Select to add the newly detected shares or mounts to the Registered Shares or Registered Mounts list in the dialog box, with the Events column checked and the Crawl column set

to enable crawling. Unreachable shares and mounts are removed from DatAdvantage.

- Detect, monitor and notify - Select to add the newly detected shares or mounts as described above, and send users email listing them. Unreachable shares and mounts are (removed from DatAdvantage.

Note: Via the monitor selections, it is possible to add all the top-level shares per protocol (type) automatically as monitoring shares (for example, it is possible to add a 1st level share in CIFS protocol and 2nd level share in MIX mode). To remove a specific share from the monitoring shares list, move manually the required share from Register Shares to Available Shares, and select Ignore Detection to ensure the resource manager will not add this share automatically to the monitoring shares (relevant for NetApp only).

Note: Shares using “mixed mode” are not supported.

- Notify - From the drop-down list, select the frequency at which to send notification of new shares or mounts. Options are:
 - Always - Select to send a cumulative list of all changes made (such as detection or deletion) to all shares and mounts.
 - Once - Select to send notification of a change (that is, detection or deletion) to a share or mount only when that change occurs.
- Remove Deleted Shares - Select this checkbox to remove deleted shares. Shares that were deleted from the file server will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the file server is unavailable, the shares will not be removed.
- Enable Event Collection - Select this checkbox to collect events from all shares added from this volume/file server.

4. On the left menu, click Configuration and set the following parameters:

- File Server General Settings
 - Save file server properties history - Select this checkbox if you want DatAdvantage to monitor the changes in folder properties (size, number of nested folders, number of files, and number of nested files).

Note: Over a long period of time this data may use a large amount of storage on the database.

- Shadow Database Installation - Credentials for installing the Shadow database on the SQL server. The user must have the sysadmin role on the selected SQL server.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- Database Server - Type or browse for the machine on which the Shadow database server resides.
- Authentication - Select the required type of authentication, SQL or Windows.
- User name - Type the account's user name.
- Password - Type the account's password.
- Save credentials - Select this checkbox to save the database credentials.
- Custom database location - Click this link to set the location of data files.
- SQL Host Server Credentials - Installation credentials for the machine on which the Shadow server resides. This account must be a member of the Local Administrators group on the machine during installation. The credentials are required only when the Shadow server does not reside on the DSP Server machine.

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- User name - Type the installation account's user name.
- Password - Type the installation account's password.
- Local Accounts
 - Collect information regarding local accounts from this file server - Select this checkbox to collect user accounts from this file system.
- FileWalk Settings
 - Identify actual unique folders and file system inconsistencies - Select this checkbox to detect broken permissions in NTFS file systems.
 - FileWalk Method - Select the method to be used for the FileWalk. Changing the method entails share rescan:
 - Varonis - A method of running the FileWalk 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.
- CIFS - Uses the Common Internet File System (CIFS) protocol. The FileWalk agent need not be installed if CIFS is selected, since it uses the UNC path.
- Run FileWalk in incremental mode (hourly) - Select this checkbox to run incremental FileWalk once an hour. Incremental FileWalk runs only on folders in which events occurred. It is only supported for file servers on which all the monitored shares (CIFS and NFS) provide resolved events, with full path location information.

Note: If the Dell server is run in audit mode, incremental FileWalk does not run on new folders. This happens because the rename step of creating a new folder is not collected.

- Event Collection Parameters

Note: If the file server is installed only for use with DataPrivilege, event collection is disabled.

- Port in use - The port through which the Varonis agent on the file server communicates with the Probe.
- 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 collect 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 may 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 proceed to add the file server with the duplicated SID. You will be able to collect events and crawl the server for directory structure and permissions. The limitation will be that you cannot collect local account information on any machines that have matching SIDs in Varonis. Most of the Varonis Data Security Platform products (such as the Data Transport Engine, DataPrivilege, and DatAlert Analytics) will not be able to monitor this file server. By default, the option to Collect information regarding local accounts from this file server will become unselected if there is already a machine with that SID being monitored.

The reason for this is that when two machines have duplicate SIDs, there is no way for DatAdvantage to identify from which machine those local accounts came.

The duplicate machine will have a fake SID entry in the database 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.

5. To configure the commit credentials to allow users to use different commit credentials than the configured FileWalk credentials, on the left menu, click Commit and set the following parameters:

- File Server Commit Credentials - Set the credentials to be used for committing DataPrivilege (or Automation Engine) changes on the file server. The account used must have Backup Operator and Power User privileges. It must also be a member of the Administrators local machine group (for Windows or NAS devices), or a member of the Site Collection Administrators group (for SharePoint).

Note: In all commit operations on a NetApp CM file server, the user who executes the operation must be a CIFS superuser.

- Clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for the FileWalk job. (By default, this checkbox is selected to use the FileWalk credentials, and the User name and Password fields are disabled for editing.)
- In the User name and Password fields, enter the relevant user name and password.

- Group OU - Select the organizational unit in which DataPrivilege (or the Automation Engine, if it is installed) creates groups. Groups created by DataPrivilege (or the Automation Engine) reside in the default base OU, unless otherwise specified.
 - Inherited from domain - By default, this option is selected to use the domain's default OU.
 - Uniquely defined - Select this option to choose a different OU from those defined in the file server's domain.
 - OU - Click the Browse button (...) to select the required OU.
6. Click Install.
The file server is installed.

Adding Unix File Servers

You can install Unix file servers and set the parameters for data collection, file servers, FileWalk credentials, Varonis Agent installation settings, and mounts.

If you install the Data Security Platform on a flavor of Unix that does not support event collection, you can still configure the machine so that you can monitor it with DatAdvantage. See the description of the Varonis Agent Installation area below.
To add a Unix file server:

1. Do one of the following:
 - In the Enterprise Installer, navigate to the Monitored File Servers page and click Add.
 - 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.

2. On the left menu, click Common and set the following parameters:

- a. Resource Type

- Select resource type - If you select a file server's type from this drop-down list, this is the type that is used no matter what type was detected earlier.

Note: If you typed the file server's name manually, you must enter the FileWalk credentials before you can use the Detect link, due to permission requirements. If the type still cannot be detected, use the override field.

- Detect resource type - Click this link to detect the type of file server you selected. (If you used the Browse button to locate the file server's name, its

type is detected automatically as long as you have already entered credentials.)

- Detected resource type - Indicates the file server type, if it was automatically detected.

b. Resource Details

- Resource/Server Name - Type the resolved name or IP address of the file server to be added, or click the Browse button to locate it.

c. Data Collection Details

- Probe - From the drop-down list, select the Probe to be used with the file server.
- Collector - From the drop-down list, select the required Collector.

Important: Once you have configured a Collector to interface with a specific Probe, you must use that Collector with the same Probe. This means that if you have already configured a Collector to interface with the selected Probe while adding a monitored file server, you must either select the same Collector, a Collector that is not yet connected to a Probe, or <No Collector>. If no Collector is used with the Probe server, select <No Collector>.

d. FileWalk Credentials - File System operations include the directory crawl (FileWalk), event collection (if set) and user crawl (ADWalk) on local accounts (if set).

- Authentication - From the drop-down list, select the authentication method for the FileWalk account.

Note: These credentials must be valid Unix-style credentials.

- User name - Type the name of the user account to be used for FileWalk, event collection and local ADWalk.
- Password - Type the account's password.

Note: This field is only displayed when Unix authentication is selected

- SSH 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

e. Varonis Agent Installation

- Do not install or upgrade the filter agent on this server - Select this checkbox if you do not want the Varonis filter agent automatically installed or upgraded on the file server.


Note: If you are adding a flavor of Unix that does not support event collection, this option is disabled. However, you can continue defining the machine to enable visibility into it without event collection.

- Click the Agent Deployment link to define the credentials used to install the agent on the file server. The Agent Deployment Options window is displayed.
- Use FileWalk credentials for agent installation - Select this checkbox to install the agent using the same credentials as the FileWalk.

Note: If you select this option, ensure that the FileWalk 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.

Note: This field is only displayed when Unix authentication is selected

3. To select specific mounts for the file server, on the left menu, click Mounts and do the following:
 - a. In the Available Mounts area, select the required mounts and click the down arrow .
 - The selected mounts are moved to the Registered Mounts area.
 - b. In the Ignore Detection column, select the mounts to be ignored (and not be the subject of notifications) by the resource monitor. Note the following scenarios:
 - Mounts manually moved from registered mounts to available mounts should be selected.
 - When users manually add mounts from available shares to registered mounts, the checkbox must be cleared.
 - c. For each mount, review and set the following information as required:
 - Mount Name - The name of the mount.
 - Path - The path of the mount.
 - Protocol - The protocol defined for the mount.

Note: The Varonis FileWalk method uses the SSH protocol for this purpose.

- Events - Select this checkbox to collect events for the mount.
- Crawl - To enable or disable monitoring for the mount, in the Crawl column, select the relevant option.
- Mixed Security - In mixed NT-Unix environments, indicates the default ACL extraction.

Note: If only DataPrivilege is installed, all crawled shares of CIFS file servers (Windows, NAS) must be defined as NTFS crawled in the Management Console and not Mixed or NFS. Otherwise, DataPrivilege cannot crawl or manage them.

d. In the Automatic Detection area, set the following:

- Automatically detect mounts - DatAdvantage detects mounts that reside at the highest level of the hierarchy and that are not already monitored. It gives preference to administrative shares over equivalent regular shares. From the drop-down list, select the relevant option:
 - Never - Select to instruct DatAdvantage not to detect shares or mounts automatically.
 - Detect and notify - Select to send users email that lists all newly detected shares or mounts. Unreachable shares and mounts are removed from DatAdvantage.
 - Detect and monitor - Select to add the newly detected shares or mounts to the Registered Shares or Registered Mounts list in the dialog box, with the Events column checked and the Crawl column set to enable crawling. Unreachable shares and mounts are removed from DatAdvantage.
 - Detect, monitor and notify - Select to add the newly detected shares or mounts as described above, and send users email listing them. Unreachable shares and mounts are (removed from DatAdvantage.

Note: Via the monitor selections, it is possible to add all the top-level shares per protocol (type) automatically as monitoring shares (for example, it is possible to add a 1st level share in CIFS protocol and 2nd level share in MIX mode/ Unix mode). To remove a specific share from the monitoring shares list, move manually the required share from Register Shares to Available Shares, and select Ignore Detection to ensure the resource manager will not add this share automatically to the monitoring shares (relevant for NetApp only).

Note: Shares using “Mixed mode” are not supported for FileWalk nor for event collection

- Notify - From the drop-down list, select the frequency at which to send notification of new shares or mounts. Options are:
 - Always - Select to send a cumulative list of all changes made (such as detection or deletion) to all shares and mounts.
 - Once - Select to send notification of a change (that is, detection or deletion) to a share or mount only when that change occurs.
- Remove Deleted Shares - Select this checkbox to remove deleted shares. Shares that were deleted (and unselected) from the file server will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the file server is unavailable, the shares will not be removed.
- Enable Event Collection - Select this checkbox to collect events from all shares added from this volume/file server.

4. On the left menu, click Configuration and set the following parameters:

- Unix Domain
 - Select the affiliated Unix user repository for this file server or Samba domain - From the drop-down 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.

- File Server General Settings
 - Save file server properties history - Select this checkbox if you want DatAdvantage to monitor the changes in folder properties (size, number of nested folders, number of files, and number of nested files).

Note: Over a long period of time this data may use a large amount of storage on the database.

- Shadow Database Installation - Credentials for installing the Shadow database on the SQL server. The user must have the sysadmin role on the selected SQL server.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- Database Server - Type or browse for the machine on which the Shadow database server resides.

- Authentication - Select the required type of authentication, SQL or Windows.
- User name - Type the account's user name.
- Password - Type the account's password.
- Save credentials - Select this checkbox to save the database credentials.
- Custom database location - Click this link to set the location of data files.
- SQL Host Server Credentials - Installation credentials for the machine on which the Shadow server resides. This account must be a member of the Local Administrators group on the machine during installation. The credentials are required only when the Shadow server does not reside on the DSP Server machine.

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- User name - Type the installation account's user name.
- Password - Type the installation account's password.
- Local Accounts
 - Collect information regarding local accounts from this file server (using FS credentials) - Select this option to collect user accounts from this file system using FS credentials.
- POSIX Access Control List
 - Enable collection and management of POSIX ACLs - Select this option as relevant for Unix flavors that support POSIX ACLs.

5. Click Install.

The file server is installed.

Adding NetApp File Servers

You can install NetApp file servers and set the parameters for data collection, file servers, FileWalk credentials, and shares.

To add a NetApp file server:

1. Do one of the following:

- In the Enterprise Installer, navigate to the Monitored File Servers page and click Add.
- 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.

2. On the left menu, click Common and set the following parameters:

a. Resource Type

- Select resource type - If you select a file server's type from this drop-down list, this is the type that is used no matter what type was detected earlier.

Note: If you typed the file server's name manually, you must enter the FileWalk credentials before you can use the Detect link, due to permission requirements. If the type still cannot be detected, use the override field.

- Detect resource type - Click this link to detect the type of file server you selected. (If you used the Browse button to locate the file server's name, its type is detected automatically as long as you have already entered credentials.)
- Detected resource type - Indicates the file server type, if it was automatically detected.

b. Resource Details


- Resource/Server Name - Type the resolved name or IP address of the file server to be added, or click the Browse button to locate it.

c. Data Collection Details

- Probe - From the drop-down list, select the Probe to be used with the file server.
- Collector - From the drop-down list, select the required Collector.

Important: Once you have configured a Collector to interface with a specific Probe, you must use that Collector with the same Probe. This means that if you have already configured a Collector to interface with the selected Probe while adding a monitored file server, you must either select the same Collector, a Collector that is not yet connected to a Probe, or <No Collector>. If no Collector is used with the Probe server, select <No Collector>.

d. FileWalk Credentials - File System operations include the directory crawl (FileWalk), event collection (if set) and user crawl (ADWalk) on local accounts (if set).

- User name - Type the name of the user account to be used for FileWalk, event collection and local ADWalk.
 - Password - Type the account's password.
 - Add this user account to the Filtered Users list - This is the default user account for Data Security Platform operations. If you clear this checkbox, a large number of events generated by the Data Security Platform will be collected.
3. To select specific shares for the file server, on the left menu, click Shares and do the following:
- a. In the Available Shares area, select the required shares and click the down arrow .

Note: In addition to regular and admin shares, DatAdvantage detects nobrowse shares on servers running 7-Mode and marks them as regular shares (not admin shares). However, the NetApp API cannot supply their share permissions. As a result, the SHS FileWalk job will not find them, and their share permissions do not have any affect on their effective permissions.

The selected shares are moved to the Registered Shares area.

- b. In the Ignore Detection column, select the shares to be ignored (and not be the subject of notifications) by the resource monitor. Note the following scenarios:
 - Shares manually moved from registered shares to available shares should be selected.
 - When users manually add shares from available shares to registered shares, the checkbox must be cleared.
- c. For each share, review and set the following information as required:

Note: If the file server is installed only for use with DataPrivilege, event collection is disabled.

- Share Name - The name of the share.
- Path - The path on which the share resides.
- Protocol - The protocol defined for the share.

Note: The Varonis FileWalk method uses the SSH protocol for this purpose.

- Events - Select this checkbox to collect events for the share.
- Crawl - To enable or disable monitoring for the share, in the Crawl column, select the relevant option.

- Mixed Security - In mixed NT-Unix environments, indicates the default ACL extraction.

d. In the Automatic Detection area, set the following:

- Automatically detect shares - DatAdvantage detects shares that reside at the highest level of the hierarchy and that are not already monitored. It gives preference to administrative shares over equivalent regular shares. From the drop-down list, select the relevant option:
 - Never - Select to instruct DatAdvantage not to detect shares or mounts automatically.
 - Detect and notify - Select to send users email that lists all newly detected shares or mounts. Unreachable shares and mounts are removed from DatAdvantage.
 - Detect and monitor - Select to add the newly detected shares or mounts to the Registered Shares or Registered Mounts list in the dialog box, with the Events column checked and the Crawl column set to enable crawling. Unreachable shares and mounts are removed from DatAdvantage.
 - Detect, monitor and notify - Select to add the newly detected shares or mounts as described above, and send users email listing them. Unreachable shares and mounts are (removed from DatAdvantage).

Note: Via the monitor selections, it is possible to add all the top-level shares per protocol (type) automatically as monitoring shares (for example, it is possible to add a 1st level share in CIFS protocol and 2nd level share in MIX mode/ Unix mode). To remove a specific share from the monitoring shares list, move manually the required share from Register Shares to Available Shares, and select Ignore Detection to ensure the resource manager will not add this share automatically to the monitoring shares (relevant for NetApp only).

- Notify - From the drop-down list, select the frequency at which to send notification of new shares or mounts. Options are:
 - Always - Select to send a cumulative list of all changes made (such as detection or deletion) to all shares and mounts.
 - Once - Select to send notification of a change (that is, detection or deletion) to a share or mount only when that change occurs.
- Remove Deleted Shares - Select this checkbox to remove deleted shares. Shares that were deleted from the file server will be displayed with a strikethrough red font. They will not be removed from the "Registered" list. If the file server is unavailable, the shares will not be removed.

- Enable Event Collection - Select this checkbox to collect events from all shares added from this volume/file server.

4. On the left menu, click Configuration and set the following parameters:

- Unix Domain
 - Select the affiliated Unix user repository for this file server or Samba domain - From the drop-down 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.

- File Server General Settings
 - Save file server properties history - Select this checkbox if you want DatAdvantage to monitor the changes in folder properties (size, number of nested folders, number of files, and number of nested files).

Note: Over a long period of time this data may use a large amount of storage on the database.

- Shadow Database Installation - Credentials for installing the Shadow database on the SQL server. The user must have the sysadmin role on the selected SQL server.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- Database Server - Type or browse for the machine on which the Shadow database server resides.
- Authentication - Select the required type of authentication, SQL or Windows.
- User name - Type the account's user name.
- Password - Type the account's password.
- Save credentials - Select this checkbox to save the database credentials.
- Custom database location - Click this link to set the location of data files.
- SQL Host Server Credentials - Installation credentials for the machine on which the Shadow server resides. This account must be a member of the Local Administrators group on the machine during installation. The credentials are required only when the Shadow server does not reside on the DSP Server machine.

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- User name - Type the installation account's user name.
- Password - Type the installation account's password.
- Local Accounts
 - Collect information regarding Windows local groups - Select this checkbox to collect Windows local groups.
- FileWalk Settings
 - Identify actual unique folders and file system inconsistencies - Select this checkbox to detect broken inheritance in NTFS file systems.
 - Run FileWalk in incremental mode (hourly) - Select this checkbox to run incremental FileWalk once an hour. Incremental FileWalk runs only on folders in which events occurred. It is only supported for file servers on which all the monitored shares (CIFS and NFS) provide resolved events - with full path location information.
- Event Collection Parameters

Note: If the file server is installed only for use with DataPrivilege, event collection is disabled.

- FPolicy name - Type the name of the FPolicy policy.

Important: The name of the FPolicy is case-sensitive.

- Asynchronous mode- In asynchronous applications, the external FPolicy server does not alter access to files or directories or modify data on the Vserver. In synchronous applications, data access is altered or data is modified by the external FPolicy server. Select this option to instruct the FPolicy to send events to the Probe without waiting for acknowledgment of each event. This option is preferable for low-bandwidth/high latency networks.
- Enable full support for NFS events (using INode to PathName translation) - Select to instruct the FPolicy to translate each NFS event to the actual path (instead of just the INode number). See [INode-toPathName Translation](#).

Note: Using this feature with ONTAP 7.3 and above might affect performance.

- 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.

- Distinguish Modify operations from Read operations - Select to instruct the FPolicy to send Read and Write events separately instead of categorizing them both as Open.

Note: Selecting this option might affect performance.

- Probe Proxy Configuration - For performance reasons, it is possible to define a Probe proxy that is located near the NetApp file server. The Probe proxy can be installed on any Windows machine in the same LAN as the NetApp file server being monitored. A single proxy can be used to monitor more than one file server.
 - Proxy server- From the drop-down list, select the Probe proxy to be used to monitor the file server.
 - Manage - Click this link to add, edit, or remove Probe proxy servers.
 - Security Policy
 - Enable monitoring - Select the monitoring option from the drop-down list, NT or Unix. When this option is changed, volumes are automatically rescanned.
 - Default for mixed security - Select an option from the drop-down list, NT, Unix, Disabled, or PermissionDisabled.
 - NFS Commit - The definitions in this section enable performing commit on NFS (for Unix, Dell, NetApp, HPE 3PAR File Persona, or HP-NAS). To maintain security, the commit process must be activated through a gateway. The gateway can be any Unix machine that has access to the NFS exports on the file server and that is accessible via SSH. The gateway need only be defined for file servers on which NFS commit is available.
 - Gateway - Type the IP address of the Unix machine that acts as the gateway.
 - Via mount pattern - Type the required pattern. Can be:
 - Host name pattern - For example, HOSTNAME:/*
 - IP address pattern - For example, 10.10.10.160:/*
The asterisk (*) indicates multiple mounts on the same machine, with different exports.
5. To configure the commit credentials to allow users to use different commit credentials than the configured FileWalk credentials, on the left menu, click Commit and set the following parameters:
- File Server Commit Credentials - Set the credentials to be used for committing DataPrivilege (or Automation Engine) changes on the file server. The account

used must have Backup Operator and Power User privileges. It must also be a member of the Administrators local machine group (for Windows or NAS devices), or a member of the Site Collection Administrators group (for SharePoint).

Note: In all commit operations on a NetApp CM file server, the user who executes the operation must be a CIFS superuser.

- Clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for the FileWalk job. (By default, this checkbox is selected to use the FileWalk credentials, and the User name and Password fields are disabled for editing.)
- In the User name and Password fields, enter the relevant user name and password.
- Group OU - Select the organizational unit in which DataPrivilege (or the Automation Engine, if it is installed) creates groups. Groups created by DataPrivilege (or the Automation Engine) reside in the default base OU, unless otherwise specified.
 - Inherited from domain - By default, this option is selected to use the domain's default OU.
 - Uniquely defined - Select this option to choose a different OU from those defined in the file server's domain.
 - OU - Click the Browse button (...) to select the required OU.

6. Click Install.

The file server is installed.

Managing Probe Proxy Servers

Managing Probe Proxy Servers

You can define Probe proxy servers in order, for example, to avoid performance degradation for monitored NetApp file servers, where events can be collected by a Probe proxy that is installed together with the file servers on the LAN.

The DSP Probe crawls the file system of monitored file servers and captures events in real time. For best performance, it is highly recommended to deploy the Probes on the same LAN as the monitored file servers. However, it is not always feasible to deploy a remote Probe (given SQL Server costs, storage, and so on), so a remote connection over WAN is requested. In these cases, to avoid performance degradation for monitored NetApp file servers, events can be collected by a Probe proxy that is installed together with the file servers on the LAN. This topology does not require the same disk space or hardware resources as a regular Probe, and high performance is maintained given the proxy's position within the LAN.

If you choose to define a Probe proxy, keep the following in mind:

- The Probe proxy may be used only for event collection. It is still the regular Probe that crawls the NetApp file servers.
- Use of the Data Classification Engine (DCE) over WAN may severely impact the performance of both the file servers and the Varonis framework. To achieve classification, a real Probe must be installed on the remote LAN.

To manage Probe proxies:

1. Do one of the following:

- In the Enterprise Installer, navigate to the Monitored File Servers page.
- In the Management Console, select Management > Components > Root > File Servers. The File Servers pane is displayed on the right.

2. To add or edit a NetApp file server:

- a. On the Resources toolbar, click Add.
- b. In the File Servers grid, select the relevant NetApp file server, and on the Resources toolbar, click Edit.

The Resource Wizard is opened, where you can configure the required settings in the Common and Configuration panes. For more information, see [Adding NetApp File Servers](#).

3. To set the Probe Proxy settings, on the left menu, click Configuration, and on the right pane, scroll down to the Probe Proxy Configuration area.

4. From the Proxy server drop-down list, select the server to act as the proxy.

5. To add proxies:

- a. Click the Manage link at the bottom of the Probe Proxy Configuration area. The Manage Probe Proxies dialog box is displayed.
- b. Click New. The Probe Proxy Information dialog box is displayed.
- c. Set the following parameters:
 - Server name - Click the Browse button to select the name of the proxy server.
 - Working Credentials - Set the credentials to be used to connect to the Probe proxy server. These credentials are used for authentication to the Probe proxy server and for starting up the service; not for accessing other resources such as the event log. This account must be a member of the VaronisEventsRetrieval security group. The Data Security Platform stores these credentials in the database for future use.

- Installation Credentials - Set the credentials to be used to install the Probe proxy server. This account must be a member of the Domain Admins security group. These credentials are not stored in the database and are only used for installation.
- d. Click OK.
The Manage Probe Proxies dialog box is displayed.
 - e. Continue adding proxies as necessary.
6. To edit a proxy's information:
 - a. In the Manage Probe Proxies dialog box, select the relevant proxy.
 - b. Click Edit and edit the proxy's details.
 7. To remove a proxy:
 - a. In the Manage Probe Proxies dialog box, select the relevant proxy.
 - b. Click Remove. The proxy is removed.
 8. Click Close to return to the Configuration pane of the Resource Wizard.
 9. From the Proxy server drop-down list, select the Probe proxy to be used to monitor the file server.

Manually Installing Probe Proxies

Manually Installing Probe Proxies

You can manually install a large number of Probe proxies from the command line.

To add a large number of Probe proxies:

Run the following from the command line:

```
msiexec /i <package.msi> SMTPSERVER=<host> SMTPFROM=<from> SMTPPTO=<to>
```

Where:

- SMTPSERVER - The name of the SMTP Server
- SMTPFROM - The address from which alerts are sent
- SMTPPTO - The address from which alerts are sent

Filtering False Read Events

Filtering False Read Events

Varonis provides the ability to filter unintentional Open events.

Description

Open events may be triggered unintentionally for a variety of reasons, resulting in inaccurate analysis of file system access. Varonis has addressed this issue by providing the ability to filter unintentional Open events. With this feature, Open events are triggered only if enough file content is actually read (see below). This approach results in a dramatic reduction in the number of unintentional Open events that are collected by the Probe.

Note: Small files and certain operations (such as an antivirus scan of executables) may still trigger Read events. It is not possible to distinguish these false Read events from true ones.

Thresholds

Open 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%
32 KB	81%
64 KB	75%
128 KB	67%
1 MB	50%
4 MB	31%
16 MB	15%
256 MB	3%

File Size	Portion Read
1 GB	3%
4 GB	3%

Supported Platforms

This feature is supported by Windows and NetApp file servers.

Dell Celerra currently lacks the information needed to deploy this method.

Unix Samba and Unix-based NAS (for example, HP-NAS) will be addressed in the future.

Prerequisites

- In the Enterprise Installer, select the Distinguish Modify operations from Read operations option in the File Servers dialog box.
- The ability to filter unintentional Open events requires an FPolicy change. Change your FPolicy to the following:

```
fpolicy policy event create -vserver <Vserver Name> -event
-name fp_event_varonis_cifs -fileoperations create, create
_dir, delete, delete_dir, open, close, write, rename, rena
me_dir, setattr -protocol cifs -filters first-write, open-
with-delete-intent
```

Instructions for Use

1. Turn on/off FalseRead for any file server using the `qa_Conf_FalseRead` procedure.

Usage

```
exec qa_Conf_FalseRead [filerID: 0 to change default], [on|of
f]'
```

Example

```
exec qa_Conf_FalseRead 1, 'on' - turn on filer 1
exec qa_Conf_FalseRead 0, 'on' - turn on default for all file
rs
```

Instructions for Use

1. In the Enterprise Installer, access the Resource Wizard for the required Windows or NetApp file server.
2. On the left menu, click Configuration.
3. In the Event Collection Parameters area, ensure the Filter out false "File Opened" events option is selected.
4. Click Save.

Inode-to-PathName Translation

Inode-to-PathName Translation

Inode-to-PathName translation is activated (if configured) only if NFS is relevant on the NetApp file server.

4

Platform	Directory				File					
	Create	Delete	Rename	Set Security	Create	Delete	Rename	Set Security	Open	Modify
NetApp 7.3.x (NFS FullPath) ²	√	√	√	√	√	√	√	√ ¹	√	√ ³
NetApp 7.3.x (CIFS)	√	√	√	√ ¹	√	√	√	√ ¹	√	√ ³
NetApp 7.2.x (CIFS)	√	√	7.2.4+		√	√	7.2.4+		√	√ ³
NetApp 7.2.x/ (NFS)	√	√		7.3.x+	√	√				
Netapp 8.0.x/ 8.1RC (NFS FullPath)	√	√	√	√	√	√	√	√	√	√
Netapp 8.0.x/ 8.1RC (CIFS)	√	√	√	√	√	√	√	√	√	√

Limitations and Known Issues

1. For NetApp 7.2.x, 7.3.x, 8.0 and 8.1RC, SETSEC_FILE is always received for files and directories. The Probe fixes it if it does not find "FILE" addressing in its cache and the name does not include a file extension. For CIFS, it is important to enable setting security: `fpolicy options <PolicyName> cifs_setattr on`
2. NFS_FullPath with OnTap 7.3.x might add performance overhead.
3. The ability to distinguish Modify from Open events is configured through the UI (default=off) due to network issues that might affect client latency.

Adding NetApp File Servers Operating in Cluster Mode

You can configure DatAdvantage for a NetApp file server operating in Cluster Mode.

Ensure the server is defined with the same name in both the Varonis Management Console and in DFS Management, or provide the mapping of file server to its CNAME via the DFS Shares tab in the Management Console.

Important: You must create a login method before configuring DatAdvantage for a NetApp file server operating in Cluster Mode. You will need the login method to enter your FileWalk credentials.

To add a NetApp file server operating in Cluster Mode:

1. Do one of the following:
 - In the Enterprise Installer, navigate to the Monitored File Servers page and click Add.
 - 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.
2. On the left menu, click Common and set the following parameters:
 - a. Resource Type

- Detected resource type - Indicates the file server type, if it was automatically detected.
- Detect resource type - Click this button and select NetApp Cluster Mode. (If you used the Browse button to locate the file server's name, its type is detected automatically.)
- Select resource type - Select NetApp Cluster Mode from the Select file server type drop-down list.

Note: If you typed the file server name manually, you may need to enter the FileWalk credentials before you can use the Detect link, due to permission requirements. If the type still cannot be detected, use the override field.

b. Resource Details

- Resource/Server Name - Type the resolved name or IP address of the file server to be added, or click the Browse button to locate it.

c. Data Collection Details

- Probe - From the drop-down list, select the Probe to be used with the file server.
- Collector - From the drop-down list, select the required Collector.

Important: Once you have configured a Collector to interface with a specific Probe, you must use that Collector with the same Probe. This means that if you have already configured a Collector to interface with the selected Probe while adding a monitored file server, you must either select the same Collector, a Collector that is not yet connected to a Probe, or <No Collector>. If no Collector is used with the Probe server, select <No Collector>.

d. FileWalk Credentials - File System operations include the directory crawl (FileWalk), event collection (if set) and user crawl (ADWalk) on local accounts (if set).

Important: Ensure that a trust relationship exists between the DSP Server and the NetApp Cluster Mode file server.

- User name - Type the name of the user account to be used for FileWalk, event collection and local ADWalk.

Important: The user name is case-sensitive.

- Password - Type the account's password.

- Add this user account to the Filtered Users list - This is the default user account for Data Security Platform operations. If you clear this checkbox, a large number of events generated by the Data Security Platform will be collected.

3. To select specific shares for the file server, on the left menu, click Shares and do the following:

a. In the Available Shares area, select the required shares and click the down arrow .

The selected shares are moved to the Registered Shares area.

b. In the Ignore Detection column, select the shares to be ignored (and not be the subject of notifications) by the resource monitor. Note the following scenarios:

- Shares manually moved from registered shares to available shares should be selected.
- When users manually add shares from available shares to registered shares, the checkbox must be cleared.

c. For each share, review and set the following information as required:

Note: If the file server is installed only for use with DataPrivilege, event collection is disabled.

- Share Name - The name of the share.
- Path - The path on which the share resides.
- Protocol - The protocol defined for the share.

Note: The Varonis FileWalk method uses the SSH protocol for this purpose.

- Events - Select this checkbox to collect events for the share.
- Crawl - To enable or disable monitoring for the share, in the Crawl column, select the relevant option.
- Mixed Security - In mixed NT-Unix environments, indicates the default ACL extraction.

d. In the Automatic Detection area, set the following:

- Automatically detect shares - DatAdvantage detects shares that reside at the highest level of the hierarchy and that are not already monitored. It gives preference to administrative shares over equivalent regular shares. From the drop-down list, select the relevant option:
 - Never - Select to instruct DatAdvantage not to detect shares or mounts automatically.

- Detect and notify - Select to send users email that lists all newly detected shares or mounts. Unreachable shares and mounts are removed from DatAdvantage.
- Detect and monitor - Select to add the newly detected shares or mounts to the Registered Shares or Registered Mounts list in the dialog box, with the Events column checked and the Crawl column set to enable crawling. Unreachable shares and mounts are removed from DatAdvantage.
- Detect, monitor and notify - Select to add the newly detected shares or mounts as described above, and send users email listing them. Unreachable shares and mounts are (removed from DatAdvantage.

Note: Via the monitor selections, it is possible to add all the top-level shares per protocol (type) automatically as monitoring shares (for example, it is possible to add a 1st level share in CIFS protocol and 2nd level share in MIX mode/ Unix mode). To remove a specific share from the monitoring shares list, move manually the required share from Register Shares to Available Shares, and select Ignore Detection to ensure the resource manager will not add this share automatically to the monitoring shares (relevant for NetApp only).

Note: Shares using “mixed mode” are not supported.

- Notify - From the drop-down list, select the frequency at which to send notification of new shares or mounts. Options are:
 - Always - Select to send a cumulative list of all changes made (such as detection or deletion) to all shares and mounts.
 - Once - Select to send notification of a change (that is, detection or deletion) to a share or mount only when that change occurs.
- Remove Deleted Shares - Select this checkbox to remove deleted shares. Shares that were deleted from the file server will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the file server is unavailable, the shares will not be removed.
- Enable Event Collection - Select this checkbox to collect events from all shares added from this volume/file server.

4. On the left menu, click Configuration and set the following parameters:

- Unix Domain
 - Select the affiliated Unix user repository for this file server or Samba domain - From the drop-down 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.

- File Server General Settings

- Save file server properties history - Select this checkbox if you want DatAdvantage to monitor the changes in folder properties (size, number of nested folders, number of files, and number of nested files).

Note: Over a long period of time this data may use a large amount of storage on the database.

- Shadow Database Installation - Credentials for installing the Shadow database on the SQL server. The user must have the sysadmin role on the selected SQL server.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- Database Server - Type or browse for the machine on which the Shadow database server resides.
- Authentication - Select the required type of authentication, SQL or Windows.
- User name - Type the account's user name.
- Password - Type the account's password.
- Save credentials - Select this checkbox to save the database credentials.
- Custom database location - Click this link to set the location of data files.
- SQL Host Server Credentials - Installation credentials for the machine on which the Shadow server resides. This account must be a member of the Local Administrators group on the machine during installation. The credentials are required only when the Shadow server does not reside on the DSP Server machine.

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- User name - Type the installation account's user name.
- Password - Type the installation account's password.
- Local Accounts

- Collect information regarding local accounts from this file server (using FS credentials) - Select this option to collect user accounts from this file system using FS credentials.
- FileWalk Settings
 - Identify actual unique folders and file system inconsistencies - Select this option to detect broken inheritance in NTFS file systems.
 - Run FileWalk in incremental mode (hourly) - Select this option to run incremental FileWalk once an hour. Incremental FileWalk runs only on folders in which events occurred. It is only supported for file servers on which all the monitored shares (CIFS and NFS) provide resolved events - with full path location information.
- Event Collection Parameters

Note: If the file server is installed only for use with DataPrivilege, event collection is disabled.

- FPolicy name - Type the name of the FPolicy policy.
 - 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.
- Probe Proxy Configuration - For performance reasons, it is possible to define a Probe proxy that is located near the NetApp file server. The Probe proxy can be installed on any Windows machine in the same LAN as the NetApp file server being monitored. A single proxy can be used to monitor more than one file server.
 - Proxy server- From the drop-down list, select the Probe proxy to be used to monitor the file server.
 - Manage - Click this link to add, edit, or remove Probe proxy servers.
- Security Policy
 - Enable monitoring - Select the monitoring option from the drop-down list, NT or Unix. When this option is changed, volumes are automatically rescanned.
 - Default for mixed security - Select an option from the drop-down list, NT, Unix, Disabled, or PermissionDisabled.

- NFS Commit - The definitions in this section enable performing commit on NFS (for Unix, Dell, NetApp, HPE 3PAR File Persona, or HP-NAS). To maintain security, the commit process must be activated through a gateway. The gateway can be any Unix machine that has access to the NFS exports on the file server and that is accessible via SSH. The gateway need only be defined for file servers on which NFS commit is available.
 - Gateway - Type the IP address of the Unix machine that acts as the gateway.
 - Via mount pattern - Type the required pattern. Can be:
 - Host name pattern - For example, HOSTNAME:/*
 - IP address pattern - For example, 10.10.10.160:/*
The asterisk (*) indicates multiple mounts on the same machine, with different exports.

5. Click Install.

The NetApp file server operating in Cluster Mode is installed.

Adding Dell File Servers

You can install Dell file servers and set the parameters for data collection, file servers, and shares.

Note: If you do not want to open a large range of Dell ports for RPC (on the Collector or DSP Server, pending on your particular configuration), you can choose to open only specific ports. For more information, see [Restricting Active Directory RPC traffic to a specific port](#).

To add a Dell file server:

1. Do one of the following:

- In the Enterprise Installer, navigate to the Monitored File Servers page and click Add.
- 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.

2. On the left menu, click Common and set the following parameters:

- a. Resource Type

- Detected resource type - Indicates the file server type if it was automatically detected.
- Detect resource type - Click this link to detect the type of file server you selected. (If you used the Browse button to locate the file server's name, its type is detected automatically as long as you have already entered credentials.)
- Select resource type - Select the relevant Dell file server type from the drop-down list.

Note: If you typed the file server's name manually, you must enter the FileWalk credentials before you can use the Detect link, due to permission requirements. If the type still cannot be detected, use the override field.

- Dell PowerScale OneFS (Isilon) Cluster Storage - (Relevant only for Dell PowerScale OneFS (Isilon)) Select this option to monitor Dell PowerScale OneFS (Isilon) file servers by access zone, and set the following parameters:
 - Zone ID - Enter the access zone ID.
 - Storage Cluster Name - Enter the name of the storage cluster.

Note: All zones added as file servers should be allocated to the same Collector.

b. Resource Details

- Resource/Server Name - Type the resolved name or IP address of the file server to be added, or click the Browse button to locate it. For monitoring Dell PowerScale OneFS (Isilon) file servers by access zone, type FQDN for the zone DNC Delegation name.

c. Data Collection Details

- Collector - From the drop-down list, select the required Collector.

Note: For 8.6.2x versions, a Collector is required to monitor a Dell PowerScale OneFS (Isilon) Cluster Storage with a zone greater than zero.

d. FileWalk Credentials - File System operations include the directory crawl (FileWalk), event collection (if set), and user crawl (ADWalk) on local accounts (if set).

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

- User name - Type the name of the user account to be used for FileWalk, event collection and local ADWalk.
- Password - Type the account's password.
- Add this user account to the Filtered Users list - This is the default user account for Data Security Platform operations. If you clear this checkbox, a large number of events generated by the Data Security Platform will be collected.

3. To select specific shares for the file server, on the left menu, click Shares and do the following:

a. In the Available Shares area, select the required shares and then click .

The selected shares are moved to the Registered Shares area.

b. In the Ignore Detection column, select the shares to be ignored (and not be the subject of notifications) by the resource monitor. Note the following scenarios:

- Shares manually moved from registered shares to available shares should be selected.
- When users manually add shares from available shares to registered shares, the checkbox must be cleared.

c. For each share, review and set the following information as required:

Note: If the file server is installed only for use with DataPrivilege, event collection is disabled.

- Share Name - The name of the share.
- Path - The path on which the share resides.
- Protocol - The protocol defined for the share.

Note: The Varonis FileWalk method uses the SSH protocol for this purpose.

- Events - Select this checkbox to collect events for the share.
- Crawl - To enable or disable monitoring for the share, in the Crawl column, select the relevant option.
- Mixed Security - In mixed NT-Unix environments, this indicates the default ACL extraction.

d. In the Automatic Detection area, set the following:

- Automatically detect shares - DatAdvantage detects shares that reside at the highest level of the hierarchy and that are not already monitored. It gives preference to administrative shares over equivalent regular shares. From the drop-down list, select the relevant option:
 - Never - Select to instruct DatAdvantage not to detect shares or mounts automatically.
 - Detect and notify - Select to send users email that lists all newly detected shares or mounts. Unreachable shares and mounts are removed from DatAdvantage.
 - Detect and monitor - Select to add the newly detected shares or mounts to the Registered Shares or Registered Mounts list in the dialog box, with the Events column checked and the Crawl column set to enable crawling. Unreachable shares and mounts are removed from DatAdvantage.
 - Detect, monitor and notify - Select to add the newly detected shares or mounts as described above, and send users email listing them. Unreachable shares and mounts are (removed from DatAdvantage).

Note: Via the monitor selections, it is possible to add all the top-level shares per protocol (type) automatically as monitoring shares (for example, it is possible to add a 1st level share in CIFS protocol and 2nd level share in MIX mode/ Unix mode). To remove a specific share from the monitoring shares list, move manually the required share from Register Shares to Available Shares, and select Ignore Detection to ensure the resource manager will not add this share automatically to the monitoring shares (relevant for NetApp only).

Note: Shares using “mixed mode” are not supported.

- Notify - From the drop-down list, select the frequency at which to send notification of new shares or mounts. Options are:
 - Always - Select to send a cumulative list of all changes made (such as detection or deletion) to all shares and mounts.
 - Once - Select to send notification of a change (that is, detection or deletion) to a share or mount only when that change occurs.
 - Remove Deleted Shares - Select this checkbox to remove deleted shares. Shares that were deleted from the file server will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the file server is unavailable, the shares will not be removed.
 - Enable Event Collection - Select this checkbox to collect events from all shares added from this volume/file server.
4. On the left menu, click Configuration and set the following parameters:
- Unix Domain
 - Select the affiliated Unix user repository for this file server or Samba domain - From the drop-down 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.

- File Server General Settings
 - Save file server properties history - Select this checkbox if you want DatAdvantage to monitor the changes in folder properties (size, number of nested folders, number of files, and number of nested files).

Note: Over a long period of time this data may use a large amount of storage on the database.

- Shadow Database Installation - Credentials for installing the Shadow database on the SQL server. The user must have the sysadmin role on the selected SQL server.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- Database Server - Type or browse for the machine on which the Shadow database server resides.
- Authentication - Select the required type of authentication, SQL or Windows.
- User name - Type the account's user name.
- Password - Type the account's password.
- Save credentials - Select this checkbox to save the database credentials.
- Custom database location - Click this link to set the location of data files.
- SQL Host Server Credentials - Installation credentials for the machine on which the Shadow server resides. This account must be a member of the Local Administrators group on the machine during installation. The credentials are required only when the Shadow server does not reside on the DSP Server machine.

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- User name - Type the installation account's user name.

- Password - Type the installation account's password.
- Local Accounts
 - Collect information regarding local accounts from this file server (using FS credentials) - Select this option to collect user accounts from this file system using FS credentials.
- FileWalk Settings
 - Identify actual unique folders and file system inconsistencies - Select this option to detect broken inheritance in NTFS file systems.
 - Run FileWalk in incremental mode (hourly) - Select this option to run incremental FileWalk once an hour. Incremental FileWalk runs only on folders in which events occurred. For Dell except Dell PowerScale OneFS (Isilon), it is supported only for file servers on which all monitored shares use only the CIFS protocol. For Dell PowerScale OneFS (Isilon), it is only supported for file servers on which all the monitored shares (CIFS and NFS) provide resolved events - with full path location information.

Note: If the Dell server is run in audit mode, incremental FileWalk does not run on new folders. This happens because the rename step of creating a new folder is not collected.

- Event Collection Parameters

Note: If the file server is installed only for use with DataPrivilege, event collection is disabled.

- 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.
- Dell Event Collection Options
 - Method - From the drop-down list, select the method by which events will be collected. Options are:
 - Event log

- CEPA - This method makes use of the Dell APIs and requires setting up the Dell Event Enabler (CEE) and the Dell Common AntiVirus Agent (CAVA) server. Use this method if you are configuring Dell PowerScale OneFS (Isilon) or Dell PowerStore CoreOS (Unity). The event log method is not supported.
 - NFS Commit - The definitions in this section enable performing commit on NFS (for Unix, Dell, NetApp, HPE 3PAR File Persona, or HP-NAS). To maintain security, the commit process must be activated through a gateway. The gateway can be any Unix machine that has access to the NFS exports on the file server and that is accessible via SSH. The gateway need only be defined for file servers on which NFS commit is available.
 - Gateway - Type the IP address of the Unix machine that acts as the gateway.
 - Via mount pattern - Type the required pattern. Can be:
 - Host name pattern - For example, HOSTNAME:/*
 - IP address pattern - For example, 10.10.10.160:/*
The asterisk (*) indicates multiple mounts on the same machine, with different exports.
5. Relevant only for Dell PowerScale OneFS (Isilon) - To configure the commit credentials to allow users to use different commit credentials than the configured FileWalk credentials, on the left menu, click Commit and set the following parameters:
- File Server Commit Credentials - Set the credentials to be used for committing DataPrivilege (or the Automation Engine if it is installed) changes on the file server. The account used must have Backup Operator and Power User privileges. It must also be a member of the Administrators local machine group (for Windows or NAS devices), or a member of the Site Collection Administrators group (for SharePoint).
 - Clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for the FileWalk job. (By default, this checkbox is selected to use the FileWalk credentials, and the User name and Password fields are disabled for editing.)
 - In the User name and Password fields, enter the relevant user name and password.
 - Group OU - Select the organizational unit in which DataPrivilege (or the Automation Engine if it is installed) creates groups. Groups created by DataPrivilege (or the Automation Engine) reside in the default base OU, unless otherwise specified.
 - Inherited from domain - By default, this option is selected to use the domain's default OU.
 - Uniquely defined - Select this option to choose a different OU from those defined in the file server's domain.
 - OU - Click the Browse button (...) to select the required OU.
6. Click Install.

The file server is installed.

Adding SharePoint File Servers

You can install SharePoint file servers and set the parameters for data collection, file servers, FileWalk credentials, Varonis Agent installation settings, and SharePoint sites.

To add a SharePoint file server:

Note: If you intend to monitor this machine as both SharePoint and Windows, you must first install it as a Windows file server and then as a SharePoint file server.

1. Do one of the following:

- In the Enterprise Installer, navigate to the Monitored File Servers page and click Add.
- 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.

2. On the left menu, click Common and set the following parameters:

a. Resource Type

- Select resource type - If you select a file server's type from this drop-down list, this is the type that is used no matter what type was detected earlier.

Note: If you typed the file server's name manually, you must enter the FileWalk credentials before you can use the Detect link, due to permission requirements. If the type still cannot be detected, use the override field.

- Detect resource type - Click this link to detect the type of file server you selected. (If you used the Browse button to locate the file server's name, its type is detected automatically as long as you have already entered credentials.)
- Detected resource type - Indicates the file server type, if it was automatically detected.

b. Resource Details

- Resource/Server Name - Type the resolved name or IP address of the file server to be added, or click the Browse button to locate it. To enable load balancing, enter the IP address of the Network Load Balancing (NLB) machine here.

c. Data Collection Details

- Probe - From the drop-down list, select the Probe to be used with the file server.
- Collector - From the drop-down list, select the required Collector.

Important: Once you have configured a Collector to interface with a specific Probe, you must use that Collector with the same Probe. This means that if you have already configured a Collector to interface with the selected Probe while adding a monitored file server, you must either select the same Collector, a Collector that is not yet connected to a Probe, or <No Collector>. If no Collector is used with the Probe server, select <No Collector>.

d. FileWalk Credentials - File System operations include the directory crawl (FileWalk), event collection (if set) and user crawl (ADWalk) on local accounts (if set).

- User name - Type the name of the user account to be used for FileWalk, event collection and local ADWalk.
- Password - Type the account's password.

Note: These credentials must be standard Windows-style credentials (domain\user).

- Add this user account to the Filtered Users list - This is the default user account for Data Security Platform operations. If you clear this checkbox, a large number of events generated by the Data Security Platform will be collected.

e. Varonis Agent Installation

- Do not install or upgrade the filter agent on this server - Select this checkbox if you do not want the Varonis filter agent automatically installed or upgraded on the file server.
- Click the Agent Deployment link to define the credentials used to install the agent on the file server.
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.

Note: If you select this option, ensure that the FileWalk 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.

3. To add SharePoint sites, on the left menu, click Sites and do the following to define which sites and collections are monitored by DatAdvantage:
- a. Select one or more SharePoint/OneDrive web sites. After you have retrieved the list of site collections, by clicking Scan All, you can search for a specific SharePoint site or collection to monitor, or select the site in the generated list. To select SharePoint web sites:
 - i. To view a site collection, click the drop-down arrow next to the relevant SharePoint file server displayed in the Sites list. This displays a list of all the file server's site collections.

Note: If more than 1,000 site collections are retrieved for a web site, you will not be able to click the arrow to view the site collections. Additionally, if you choose to monitor a web site with over 1,000 site collections, the Detect, notify and monitor automatically option is automatically selected from the Automatically detect site collections drop-down list. If you choose to select an option other than Detect and monitor automatically or Detect, notify and monitor automatically for this web site, automatic detection will be set for all of the other monitored SharePoint web sites which have a large amount of site collections.

- ii. Select the checkboxes of the relevant sites and collections you want to monitor, or select the checkbox in the column header to select all sites and collections on the SharePoint file server.
- b. To collect events for specific sites, in the Events column select the checkboxes for the required sites.
 - c. From the Automatically detect site collections drop-down list, select one of the following options to set the system behavior when a web site is added to or deleted from a SharePoint file server:
 - Never - New and deleted web sites are not detected.
 - Detect and notify by mail - New and deleted web sites are detected and email notifications are sent.
 - Detect and monitor automatically - New and deleted web sites are detected and new web sites are automatically monitored by DatAdvantage.
 - Detect, notify and monitor automatically - New and deleted web sites are detected, email notifications are sent, and new web sites are automatically monitored by DatAdvantage.

Note: Auto-detect Resource is not supported if both the public URL and its Alternate Access Mapping (AAM) have been added to DatAdvantage.

4. On the left menu, click Configuration and set the following parameters:

- File Server General Settings
 - Save file server properties history - Select this checkbox if you want DatAdvantage to monitor the changes in folder properties (size, number of nested folders, number of files, and number of nested files).

Note: Over a long period of time this data may use a large amount of storage on the database.

- Shadow Database Installation - Credentials for installing the Shadow database on the SQL server. The user must have the sysadmin role on the selected SQL server.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- Database Server - Type or browse for the machine on which the Shadow database server resides.
- Authentication - Select the required type of authentication, SQL or Windows.
- User name - Type the account's user name.
- Password - Type the account's password.
- Save credentials - Select this checkbox to save the database credentials.
- Custom database location - Click this link to set the location of data files.
- SQL Host Server Credentials - Installation credentials for the machine on which the Shadow server resides. This account must be a member of the Local Administrators group on the machine during installation. The credentials are required only when the Shadow server does not reside on the DSP Server machine.

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- User name - Type the installation account's user name.
- Password - Type the installation account's password.
- General Agent Settings - The settings in this area affect all web applications.
 - Server
 - Click the Browse button (...) to select the relevant front-end server, and click Add to add it to the list.
 - Alternatively, click Detect Front-Ends to detect front-end servers and add them to the list automatically.
- Event Collection Settings - These settings affect selected web applications only:
 - Collect open events - Select to gather file or folder open events. Selecting this option may cause the SharePoint Web application to restart. If it does, its current state will not be saved.

Note: This option is only available when the Use legacy auditing method checkbox is cleared.

- Collect security events - Select to gather security events, such as changing permission levels or inheritance. Selecting this option may trigger the creation of a custom Varonis SharePoint database. Verify that the credentials for the database are sufficient.
- Add Varonis event handler - Select to add a Varonis event handler. This allows the interception of SharePoint folder events (such as create, modify and delete). Without it, these events are not recorded in DatAdvantage. The event handlers do not intercept security events, attachment events or generic list item open events.
- Display all files in DatAdvantage - Select to display all files in DatAdvantage.
- Leave a copy of events - Select to leave a copy of the events in the SharePoint database after the Varonis agent has processed them.
- List Item Types - Select the required options:
 - Generic type of list template used for most lists
 - Document library
 - Discussion board
 - Survey list
 - Issue-tracking list

5. To configure the commit credentials to allow users to use different commit credentials than the configured FileWalk credentials, on the left menu, click Commit and set the following parameters:

- File Server Commit Credentials - Set the credentials to be used for committing DataPrivilege changes on the file server. The account used must have Backup Operator and Power User privileges. It must also be a member of the Administrators local machine group (for Windows or NAS devices), or a member of the Site Collection Administrators group (for SharePoint).

Note: In all commit operations on a NetApp CM file server, the user who executes the operation must be a CIFS superuser.

- Clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for the FileWalk job. (By default, this checkbox is selected to use the FileWalk credentials, and the User name and Password fields are disabled for editing.)
- In the User name and Password fields, enter the relevant user name and password.
- Group OU - Select the organizational unit in which DataPrivilege creates groups. Groups created by DataPrivilege reside in the default base OU, unless otherwise specified.
 - Inherited from domain - By default, this option is selected to use the domain's default OU.
 - Uniquely defined - Select this option to choose a different OU from those defined in the file server's domain.
 - OU - Click the Browse button (...) to select the required OU.

6. Click Install.

The file server is installed.

Adding SharePoint Online and OneDrive File Servers

SharePoint Online and OneDrive file servers can only be added through the Management Console; not through the Enterprise Installer. For more information, see [Adding a SharePoint Online File Server](#) and [Adding a OneDrive File Server](#) in the M365 Deployment Guide.

Adding Exchange Storage Groups

You can install an Exchange storage group and set the parameters for data collection, file servers, Varonis Agent installation, FileWalk credentials, and domains.

Before adding an Exchange storage group, verify that the server's domain has been added to DatAdvantage.

Attention: DatAdvantage supports only manual editing for Exchange storage groups; it does not provide recommendations.

To add an Exchange storage group:

1. Do one of the following:

- In the Enterprise Installer, navigate to the Monitored File Servers page and click Add.
- 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.

2. On the left menu, click Common and set the following parameters:

a. Resource Type

- Select resource type - Select Exchange from the drop-down list.
- Detected resource type - Exchange storage groups cannot be detected automatically.

b. Resource Details

- Resource/Server Name - Type a name for the Exchange storage group.

c. Data Collection Details

- Probe - From the drop-down list, select the Probe to be used with the file server.
- Collector - From the drop-down list, select the required Collector.

Important: Once you have configured a Collector to interface with a specific Probe, you must use that Collector with the same Probe. This means that if you have already configured a Collector to interface with the selected Probe while adding a monitored file server, you must either select the same Collector, a Collector that is not yet connected to a Probe, or <No Collector>. If no Collector is used with the Probe server, select <No Collector>.

- d. FileWalk Credentials - File System operations include the directory crawl (FileWalk), event collection (if set) and user crawl (ADWalk) on local accounts (if set).

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

- User name - Type the name of the user account to be used for FileWalk, event collection and local ADWalk.
- Password - Type the account's password.

- e. Varonis Agent Installation

- Do not install or upgrade the filter agent on this server - Select this option if you do not want the Varonis filter agent automatically installed or upgraded on the Exchange storage group.
- Click the Agent Deployment link to define the credentials used to install the agent on the file server.
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.

Note: If you select this option, ensure that the FileWalk 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.

3. On the left menu, click Domains and do the following:

- a. From the Select domain forest drop-down list, select the domain on which the Exchange storage group resides. Mailboxes owned by users from the domains in the forest can be monitored and audited according to the settings below. Public folders that are stored on Exchange servers that reside in the selected domain forest are treated as domains and are also available for monitoring and auditing.
- b. In the All forest domains area, select the required domains and click the down arrow .
The selected domains are moved to the Monitored Domains List area.
- c. For each domain, review and set the following information as required:
 - Domain Name - The name of the domain.

- Events - Select the checkbox to collect events from this domain. (Select specific mailboxes from the domain in the Configuration pane.)
- Crawl - To enable or disable monitoring for the domain, click the Crawl column and select the relevant option. (Select specific mailbox servers to be crawled in the Configuration pane.)

4. On the left menu, click Configuration and set the following parameters:

- File Server General Settings
 - Save file server properties history - Select this checkbox if you want DatAdvantage to monitor the changes in folder properties (size, number of nested folders, number of files, and number of nested files).

Note: Over a long period of time this data may use a large amount of storage on the database.

- Shadow Database Installation - Credentials for installing the Shadow database on the SQL server. The user must have the sysadmin role on the selected SQL server.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- Database Server - Type or browse for the machine on which the Shadow database server resides.
- Authentication - Select the required type of authentication, SQL or Windows.
- User name - Type the account's user name.
- Password - Type the account's password.
- Save credentials - Select this checkbox to save the database credentials.
- Custom database location - Click this link to set the location of data files.
- SQL Host Server Credentials - Installation credentials for the machine on which the Shadow server resides. This account must be a member of the Local Administrators group on the machine during installation. The credentials are required only when the Shadow server does not reside on the DSP Server machine.

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- User name - Type the installation account's user name.
- Password - Type the installation account's password.
- Servers
 - Select the servers on which the Varonis auditing service (that is, the agent) will be installed. The mailboxes and public folders residing on these servers will be monitored in accordance with the options selected in the Monitored Domains list.
 - Scan for Servers - Click to find all Exchange Servers in the domain forest. Newly found servers are marked in green and placed at the top of the list.
 - To collect events for specific Exchange Servers, select the relevant servers (standard multi-select features are available) and do one of the following:
 - On the Servers toolbar, click Events and select Check or Uncheck from the drop-down list as relevant, to configure event collection for all selected Exchange Servers.
 - In the grid, select the Events checkbox for each selected server.
 - In the grid, right-click the chosen servers and select Events > Check or Events > Uncheck as relevant.
 - Select the main Events checkbox in the grid to collect events for all Exchange Servers.
 - Support additional protocols in Exchange 2010 - Select this option to support additional protocols, including ActiveSync, OWA, EWS IMAP4 and POP3.
 - Support for additional protocols can only be enabled through configuration, not during upgrade (such support requires a beta version of the Exchange agent).
 - To enable additional protocols:
 - Upgrade DatAdvantage.
 - Run the Configure File Server flow.
 - Clear the Do not install / upgrade / remove Varonis FileWalk Agent option, both here and on the Monitored File Servers page.
 - Select Support additional protocols in Exchange 2010.
 - If you do not want to enable additional protocols, auditing is enabled only for MAPI and/or OWA (according to your selection).
- Admin Event Collection

- Collect Admin Events in Exchange 2010, 2013, and 2016 - If Exchange 2010, 2013, or 2016 is in use, select this option to collect supported Admin events.
- Additional Settings
 - Install commit agent - Select to install the commit agent, which enables changing permissions on Exchange mailboxes and public folders.
 - EWS URI - Set the URI to be used by the commit agent. The server listed in the URI can also be used as the installation server.
 - Installation Server - Select the installation server, which is used for running the configuration scripts that create the mailbox for the FileWalk user. It is also the server on which the commit agent is installed.
 - FileWalk RPC Port - Enter the required RPC port (default = 135).
 - Reconnect option - Audit data is only collected for a particular mailbox when the mailbox makes a new connection to Exchange. The options below enable the Varonis Exchange agent to force the mailbox to reconnect so that auditing may commence.

Note: The selected option also takes effect if the Varonis Exchange agent must be restarted after shutdown for any reason.

- Reconnect active sessions at a given time
- Reconnect active sessions at agent startup
- Do not reconnect active sessions

5. Click Install.

The Exchange storage group is installed.

[Managing Probe Proxy Servers for Exchange Admin Events](#)

[Managing Probe Proxy Servers for Exchange Admin Events](#)

You can define Probe proxy servers in order, for example, to avoid performance degradation of the monitored file servers, where Exchange admin events can be collected by a Probe proxy that is installed together with the file servers on the LAN.

The DSP Probe crawls the file system of monitored file servers and captures events in real time. For best performance, it is highly recommended to deploy the Probes on the same LAN as the monitored file servers. However, it is not always feasible to deploy a remote Probe (given SQL Server costs, storage, and so on), so a remote connection over

WAN is requested. In these cases, to avoid performance degradation for monitored file servers, where Exchange admin events can be collected by a Probe proxy that is installed together with the file servers on the LAN. This topology does not require the same disk space or hardware resources as a regular Probe, and high performance is maintained given the proxy's position within the LAN.

If you choose to define a Probe proxy, keep the following in mind:

- The Probe proxy may be used only for event collection. It is still the regular Probe that crawls the file servers.
- Use of the Data Classification Engine (DCE) over WAN may severely impact the performance of both the file servers and the Varonis framework. To achieve classification, a real Probe must be installed on the remote LAN.

To manage Probe proxies:

1. In the Enterprise Installer, navigate to the Monitored File Servers page.
2. To add or edit a file server:
 - a. On the Resources toolbar, click Add.
 - b. In the File Servers grid, select the relevant Exchange storage group, and on the Resources toolbar, click Edit.
The Resource Wizard is opened, where you can configure the required settings in the Common and Configuration panes.
3. To set the Probe Proxy settings, on the left menu, click Configuration, and on the right pane, scroll down to the Admin Events Collection area.
4. From the Proxy server list, select the server to act as the proxy.
5. To add proxies:
 - a. Click Manage Proxies in the Admin Events Collection area.
The Manage Probe Proxies dialog box is displayed.
 - b. Click New.
The Probe Proxy Information dialog box is displayed.
 - c. Set the following parameters:

- Server name - Click the Browse button to select the name of the proxy server.
 - Working Credentials - Set the credentials to be used to connect to the Probe proxy server. This account must be a member of the VaronisEventsRetrieval security group. The Data Security Platform stores these credentials in the database for future use.
 - Installation Credentials - Set the credentials to be used to install the Probe proxy server. This account must be a member of the Domain Admins security group. These credentials are not stored in the database and are only used for installation.
- d. Click OK.
The Manage Probe Proxies dialog box is displayed.
- e. Continue adding proxies as necessary.
6. To edit a proxy's information:
- a. In the Manage Probe Proxies dialog box, select the relevant proxy.
 - b. Click Edit and edit the proxy's details.
7. To remove a proxy:
- a. In the Manage Probe Proxies dialog box, select the relevant proxy.
 - b. Click Remove. The proxy is removed.
8. Click Close to return to the Configuration pane of the Resource Wizard.
9. From the Proxy/Agent drop-down list, select the Probe proxy to be used to monitor the Exchange admin events.

[Configuring Exchange to Enable Mailbox Creation through DatAdvantage](#)

[Configuring Exchange to Enable Mailbox Creation through DatAdvantage](#)

This option can only be enabled for Exchange 2010.

To enable creating Exchange mailboxes from within DatAdvantage:

1. On the Exchange server, open the IIS manager.

2. Expand the tree: [ServerName] > Sites > Default Web Site > PowerShell.
3. Select Authentication.
4. Set Basic Authentication to Enable.

[Exchange Deployment Workaround to Bypass Prerequisite Checks for Domain Admin Permissions](#)

[Exchange Deployment Workaround to Bypass Prerequisite Checks for Domain Admin Permissions](#)

Pre-Deployment Steps

1. Disable the Exchange storage group prerequisites and commands that edit permissions automatically during deployment.
2. Disable the prerequisite for Exchange permissions.
 - a. Edit the `Prerequisite.xml` file located by default in `\\Program Files (x86)\Varonis\DatAdvantage\IDU Server\Prerequisite.xml`, and remove the section that has `ExchangePermissionsCheck` (3 instances in this file).
 - b. Restart the DSP Service.
3. Disable the command that edits permissions upon deployment.
 - a. Edit the `vip.manifest` file located in `C:\Program Files\Varonis\DatAdvantage\Domain\Repository\ExchangeFilerAgent_<version>.vip`.
 - b. In the `vip.manifest` file, remove the whole section (about 12 lines) which contains the `InstallExchangeFilerCommand` contents.
 - c. Replace the original `vip.manifest` file with the updated one, rezip it, and change it to a VIP file.

Adding an Exchange Storage Group

From the Management Console, add the Exchange storage group with the relevant users, without using Domain admin membership. For more information, see [Adding Exchange Storage Groups](#)

Post-Deployment Steps

1. Create the mailbox for FileWalk users.
2. Set all necessary permissions for the FileWalk user and the installation user:

- a. For the FileWalk user, set the following permissions

- `AccessControlModification.Add, AccessControlType.Allow, ActiveDirectorySecurityInheritance.All`
- Specify the following folder in Active Directory:

```
// organization level
"cn=Microsoft Exchange,cn=Services, objectCategory=CN=ms-Exch-Organization-Container"
// organization level
" cn=Microsoft Exchange,cn=Services, objectCategory=CN=ms-Exch-Organization-Container",
// all the private databases
" cn=Microsoft Exchange,cn=Services, objectCategory=CN=ms-Exch-Private-MDB",
// all the public databases
" cn=Microsoft Exchange,cn=Services, objectCategory=CN=ms-Exch-Public-MDB"
```

- Power users on each server on which the agent is installed.
 - Administer Information Store for the MAPI FileWalk user on each monitored mailbox database (can be assigned for the CN=<organizationname> node).
 - List contents Active Directory permissions on and under the CN=<organization name> node.
- b. For the installation user, set the following permissions:
 - Member of the Exchange Organization Management role.
 - Local administrator on all the servers on which auditing agents are installed.

3. Insert the value for EX_FileWalkUserLegacyDN in the database on VrnsDomainDB. For example:

```
exec dbo.spSetConf
    @cfgName='EX_FileWalkUserLegacyDN',
    @cfgItemID=2,
    @cfgValue='/o=First Organization/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Configuration/cn=Servers/cn=INSTALLER-XC1'
```

Where:

cfgName - name of the property, should be 'EX_FileWalkUserLegacyDN'

cfgValue - the value from LDAP

cfgItemID - filer ID

- To get the cfgValue value, run the following query:

```
select * from VrnsDomainDB.. vwConf where Name = 'EX_FileWalkUserLegacyDN'
```

If this value cannot be retrieved from the database, click this [link](#) to locate it manually via adsiedit.

4. Sync the probes by running the following stored procedure on VrnsDomainDB:

```
exec spSyncProbeConfigurations -1
```

5. Restart the DSP service.

Adding Exchange Online File Servers

Exchange Online file servers can only be added through the Management Console; not through the Enterprise Installer. For more information, see Deploying Exchange Online in the M365 Deployment Guide.

Adding Nasuni File Servers

You can install Nasuni file servers and set the parameters for data collection, file servers, FileWalk credentials, Nasuni API access management API settings, and shares.

Note: DataPrivilege only supports adding folders which reside on a cloud node server (Nasuni Edge Appliance) that is configured in the Varonis Management Console.

To add a Nasuni file server:

1. Do one of the following:

- In the Enterprise Installer, navigate to the Monitored File Servers page and click Add.
- 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.

2. On the left menu, click Common and set the following parameters:

a. Resource Type

- Select resource type - If you select a file server's type from this drop-down list, this is the type that is used no matter what type was detected earlier.

Note: If you typed the file server's name manually, you must enter the FileWalk credentials before you can use the Detect link, due to permission requirements. If the type still cannot be detected, use the override field.

- Detect resource type - Click this link to detect the type of file server you selected. (If you used the Browse button to locate the file server's name, its type is detected automatically as long as you have already entered credentials.)
- Detected resource type - Indicates the file server type, if it was automatically detected.

b. Resource Details

- Resource/Server Name - Type the resolved name or IP address of the file server to be added, or click the Browse button to locate it.

c. Data Collection Details

- Probe - From the drop-down list, select the Probe to be used with the file server.
- Collector - From the drop-down list, select the required Collector.

Important: Once you have configured a Collector to interface with a specific Probe, you must use that Collector with the same Probe. This means that if you have already configured a Collector to interface with the selected Probe while adding a monitored file server, you must either select the same Collector, a Collector that is not yet connected to a Probe, or <No Collector>. If no Collector is used with the Probe server, select <No Collector>.

Note: For Nasuni file servers, you must use a Collector in order to collect events!

d. FileWalk Credentials - File System operations include the directory crawl (FileWalk), event collection (if set) and user crawl (ADWalk) on local accounts (if set).

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

- User name - Type the name of the user account to be used for FileWalk, event collection and local ADWalk.
 - Password - Type the account's password.
 - Add this user account to the Filtered Users list - This is the default user account for Data Security Platform operations. If you clear this checkbox, a large number of events generated by the Data Security Platform will be collected.
- e. Nasuni Management Console API Access Settings - This section is displayed only if Nasuni is selected or detected as the file server type. The following are the credentials for access to the Nasuni Management Console (NMC) API, used to retrieve information about the file system, collect events, and enable critical settings:
- NMC host name
 - NMC user name
 - NMC password

- Connect & Verify – Click this button to validate the NMC credentials, retrieve the dedicated file server version, and enable adding the file server to the Management Console.

Note: For additional requirements, see Configuring the NMC User.

f. Nasuni API Access Key Settings - This section is displayed only if Nasuni is selected or detected as the file server type, and when the Varonis dedicated Edge appliance is of a Nasuni version prior to 8.5.

- API Access Key Name
- API Access Key Passcode

This Access Key is used for retrieving data on the Nasuni Filer and for collecting events using the Nasuni Filer API. Insert an Access Key Name and Passcode.

3. To select specific shares for the file server, on the left menu, click Shares and do the following:

a. In the Available Shares area, select the required shares and click the down arrow .

The selected shares are moved to the Registered Shares area.

b. In the Ignore Detection column, select the shares to be ignored (and not be the subject of notifications) by the Resource monitor. Note that shares manually moved from registered shares to available shares should be selected.

c. For each share, review and set the following information as required:

- Share Name - The name of the share.
- Path - The path on which the share resides.
- Protocol - The protocol defined for the share.
- Events - Select this checkbox to collect 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 collection and crawling.

- Mixed Security - In Windows environments, NT ACL extraction is always used.

d. In the Automatic Detection area, set the following:

- Automatically detect shares - DatAdvantage detects shares that reside at the highest level of the hierarchy and that are not already monitored. It gives preference to administrative shares over equivalent regular shares. From the drop-down list, select the relevant option:
 - Never - Select to instruct DatAdvantage not to detect shares automatically.
 - Detect and notify - Select to send users email that lists all newly detected shares. Unreachable shares are removed from DatAdvantage.
- Notify - From the drop-down list, select the frequency at which to send notification of new shares. Options are:
 - Always - Select to send a cumulative list of all changes made (such as detection or deletion) to all shares.
 - Once - Select to send notification of a change (that is, detection or deletion) to a share only when that change occurs.
- Remove Deleted Shares - Select this checkbox to remove deleted shares. Shares that were deleted from the file server will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the file server is unavailable, the shares will not be removed.
- Enable Event Collection - Select this checkbox to collect events from all shares added from this volume/file server.

4. On the left menu, click Configuration and set the following parameters:

- File Server General Settings
 - Save file server properties history - Select this checkbox if you want DatAdvantage to monitor the changes in folder properties (size, number of nested folders, number of files, and number of nested files).

Note: Over a long period of time this data may use a large amount of storage on the database.

- Shadow Database Installation - Credentials for installing the Shadow database on the SQL server. The user must have the sysadmin role on the selected SQL server.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- Database Server - Type or browse for the machine on which the Shadow database server resides.
- Authentication - Select the required type of authentication, SQL or Windows.
- User name - Type the account's user name.
- Password - Type the account's password.

- Save credentials - Select this checkbox to save the database credentials.
- Custom database location - Click this link to set the location of data files.
- SQL Host Server Credentials - Installation credentials for the machine on which the Shadow server resides. This account must be a member of the Local Administrators group on the machine during installation. The credentials are required only when the Shadow server does not reside on the DSP Server machine.

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- User name - Type the installation account's user name.
- Password - Type the installation account's password.
- Local Accounts
 - Collect information regarding local accounts from this file server - Select this checkbox to collect user accounts from this file system using FS credentials.
- FileWalk Settings
 - Identify actual unique folders and file system inconsistencies - Select this checkbox to detect broken permissions in NTFS file systems.
 - Run FileWalk in incremental mode (hourly) - Select this checkbox to run incremental FileWalk once an hour. Incremental FileWalk runs only on folders in which events occurred. It is only supported for file servers on which all the monitored shares (CIFS) provide resolved events, with full path location information.

5. Click Install.

The file server is installed.

Adding Panzura File Servers

You can install Panzura file servers and set the parameters for data collection, file servers, FileWalk credentials, Panzura API, and shares.

To add a Panzura file server:

1. Do one of the following:

- In the Enterprise Installer, navigate to the Monitored File Servers page and click Add.
- 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.

2. On the left menu, click Common and set the following parameters:

a. Resource Type

- Select resource type - If you select a file server's type from this drop-down list, this is the type that is used no matter what type was detected earlier.

Note: If you typed the file server's name manually, you must enter the FileWalk credentials before you can use the Detect link, due to permission requirements. If the type still cannot be detected, use the override field.

- Detect resource type - Click this link to detect the type of file server you selected. (If you used the Browse button to locate the file server's name, its type is detected automatically as long as you have already entered credentials.)
- Detected resource type - Indicates the file server type, if it was automatically detected.

b. Resource Details

- Resource/Server Name - Type the resolved name or IP address of the file server to be added, or click the Browse button to locate it.

Note: The Panzura dedicated file server can be either a Master file server or a subordinate.

c. Data Collection Details

- Probe - From the drop-down list, select the Probe to be used with the file server.
- Collector - From the drop-down list, select the required Collector.

Important: Once you have configured a Collector to interface with a specific Probe, you must use that Collector with the same Probe. This means that if you have already configured a Collector to interface with the selected Probe while adding a monitored file server, you must either select the same Collector, a Collector that is not yet connected to a Probe, or <No Collector>. If no Collector is used with the Probe server, select <No Collector>.


Note: For Panzura file servers, you must use a Collector in order to collect events!

- d. FileWalk Credentials - File System operations include the directory crawl (FileWalk), event collection (if set) and user crawl (ADWalk) on local accounts (if set). For more information, see [Configuring the FileWalk User for Panzura](#).

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

- User name - Type the name of the user account to be used for FileWalk, event collection and local ADWalk.
 - Password - Type the account's password.
 - Add this user account to the Filtered Users list - This is the default user account for Data Security Platform operations. If you clear this checkbox, a large number of events generated by the Data Security Platform will be collected.
- e. Panzura REST API Credentials - This section is displayed only if Panzura is selected or detected as the file server type. The following credentials are used to retrieve data about the file system and to collect 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 verify the credentials that were entered and to retrieve the dedicated file server version.
3. To select specific shares for the file server, on the left menu, click Shares and do the following:
- a. In the Available Shares area, select the required shares and click the down arrow . The selected shares are moved to the Registered Shares area.

- b. In the Ignore Detection column, select the shares to be ignored (and not be the subject of notifications) by the Resource monitor. Note that shares manually moved from registered shares to available shares should be selected.
- c. For each share, review and set the following information as required:
 - Share Name - The name of the share.
 - Path - The path on which the share resides.
 - Protocol - The protocol defined for the share.
 - Events - Select this checkbox to collect 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 collection and crawling.

- Mixed Security - In Windows environments, NT ACL extraction is always used.
- d. In the Automatic Detection area, set the following:
 - Automatically detect shares - DatAdvantage detects shares that reside at the highest level of the hierarchy and that are not already monitored. It gives preference to administrative shares over equivalent regular shares. From the drop-down list, select the relevant option:
 - Never - Select to instruct DatAdvantage not to detect shares or mounts automatically.
 - Detect and notify - Select to send users an email that lists all newly detected shares or mounts. Unreachable shares and mounts are removed from DatAdvantage.
 - Detect and monitor - Select to add the newly detected shares or mounts to the Registered Shares or Registered Mounts list in the dialog box, with the Crawl column set to enable crawling.
 - Detect, monitor, and notify - Select to add the newly detected shares or mounts as described above, and to send users an email listing them.
 - Notify - From the drop-down list, select the frequency at which to send notification of new shares or mounts. Options are:
 - Always - Select to send a cumulative list of all changes made (such as detection or deletion) to all shares and mounts.
 - Once - Select to send notification of a change (that is, detection or deletion) to a share or mount only when that change occurs.

- Remove Deleted Shares -Setting this checkbox is relevant only after selecting either Detect and monitor or Detect, monitor, and notify in the Automatically detect shares drop-down list. Select this checkbox to remove deleted shares. Shares that were deleted from the file server will be displayed with a strikethrough red font. They will not be removed from the Registered Shares list. If the file server is unavailable, the shares will not be removed.
- Enable Event Collection - Setting this checkbox is relevant only after selecting either Detect and monitor or Detect, monitor, and notify in the Automatically detect shares drop-down list. Select this checkbox to collect events from all shares added from this file server.

4. On the left menu, click Configuration and set the following parameters:

- File Server General Settings
 - Save file server properties history - Select this checkbox if you want DatAdvantage to monitor the changes in folder properties (size, number of nested folders, number of files, and number of nested files).

Note: Over a long period of time this data may use a large amount of storage on the database.

- Shadow Database Installation - Credentials for installing the Shadow database on the SQL server. The user must have the sysadmin role on the selected SQL server.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- Database Server - Type or browse for the machine on which the Shadow database server resides.
- Authentication - Select the required type of authentication, SQL or Windows.
- User name - Type the account's user name.
- Password - Type the account's password.
- Save credentials - Select this checkbox to save the database credentials.
- Custom database location - Click this link to set the location of data files.
- SQL Host Server Credentials - Installation credentials for the machine on which the Shadow server resides. This account must be a member of the Local Administrators group on the machine during installation. The credentials are required only when the Shadow server does not reside on the DSP Server machine.

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- User name - Type the installation account's user name.
- Password - Type the installation account's password.
- FileWalk Settings
 - Identify actual unique folders and file system inconsistencies - Select this checkbox to detect broken permissions in NTFS file systems.
 - Run FileWalk in incremental mode (hourly) - Select this checkbox to run incremental FileWalk once an hour. Incremental FileWalk runs only on folders in which events occurred. It is only supported for file servers on which all the monitored shares/exports provide resolved events, with full path location information.
- Event Collection Parameters
 - 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.

5. Click Install.

The file server is installed.

Adding Nutanix File Servers

You can install Nutanix file servers and set the parameters for data collection, file servers, FileWalk credentials, Nutanix REST API settings, and shares.

To add a Nutanix file server:

1. Do one of the following:

- In the Enterprise Installer, navigate to the Monitored File Servers page and click Add.
- 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.

2. On the left menu, click Common and set the following parameters:

a. Resource Type

- Select resource type - If you select a file server's type from this drop-down list, this is the type that is used no matter what type was detected earlier.

Note: If you typed the file server's name manually, you must enter the FileWalk credentials before you can use the Detect link, due to permission requirements. If the type still cannot be detected, use the override field.

- Detect resource type - Click this link to detect the type of file server you selected. (If you used the Browse button to locate the file server's name, its type is detected automatically as long as you have already entered credentials.)
- Detected resource type - Indicates the file server type, if it was automatically detected.

b. Resource Details

- Resource/Server Name - Type the resolved name or IP address of the file server to be added, or click the Browse button to locate it.

c. Data Collection Details


- Probe - From the drop-down list, select the Probe to be used with the file server.
- Collector - From the drop-down list, select the required Collector.

Important: Once you have configured a Collector to interface with a specific Probe, you must use that Collector with the same Probe. This means that if you have already configured a Collector to interface with the selected Probe while adding a monitored file server, you must either select the same Collector, a Collector that is not yet connected to a Probe, or <No Collector>. If no Collector is used with the Probe server, select <No Collector>.

d. FileWalk Credentials - File System operations include the directory crawl (FileWalk), event collection (if set) and user crawl (ADWalk) on local accounts (if set).

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

- User name - Type the name of the user account to be used for FileWalk, event collection and local ADWalk.

- Password - Type the account's password.
 - Add this user account to the Filtered Users list - This is the default user account for Data Security Platform operations. If you clear this checkbox, a large number of events generated by the Data Security Platform will be collected.
- e. Nutanix REST API Credentials - This section is displayed only if Nutanix is selected or detected as the file server type. The following credentials are used to retrieve data about the file system and to collect 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.
3. To select specific shares for the file server, on the left menu, click Shares and do the following:
- a. In the Available Shares area, select the required shares and click the down arrow .
- The selected shares are moved to the Registered Shares area.
- b. In the Ignore Detection column, select the shares to be ignored (and not be the subject of notifications) by the Resource monitor. Note that shares manually moved from registered shares to available shares should be selected.
- c. For each share, review and set the following information as required:
- Share Name - The name of the share.
 - Path - The path on which the share resides.
 - Protocol - The protocol defined for the share.
 - Events - Select this checkbox to collect 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 collection and crawling.
- Mixed Security - In Windows environments, NT ACL extraction is always used.
- d. In the Automatic Detection area, set the following:

- Automatically detect shares - DatAdvantage detects shares that reside at the highest level of the hierarchy and that are not already monitored. It gives preference to administrative shares over equivalent regular shares. From the drop-down list, select the relevant option:
 - Never - Select to instruct DatAdvantage not to detect shares automatically.
 - Detect and notify - Select to send users email that lists all newly detected shares. Unreachable shares are removed from DatAdvantage.
- Notify - From the drop-down list, select the frequency at which to send notification of new shares. Options are:
 - Always - Select to send a cumulative list of all changes made (such as detection or deletion) to all shares.
 - Once - Select to send notification of a change (that is, detection or deletion) to a share only when that change occurs.
- Remove Deleted Shares - Select this checkbox to remove deleted shares. Shares that were deleted from the file server will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the file server is unavailable, the shares will not be removed.
- Enable Event Collection - Select this checkbox to collect events from all shares added from this volume/file server.

4. On the left menu, click Configuration and set the following parameters:

- File Server General Settings
 - Save file server properties history - Select this checkbox if you want DatAdvantage to monitor the changes in folder properties (size, number of nested folders, number of files, and number of nested files).

Note: Over a long period of time this data may use a large amount of storage on the database.

- Shadow Database Installation - Credentials for installing the Shadow database on the SQL server. The user must have the sysadmin role on the selected SQL server.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- Database Server - Type or browse for the machine on which the Shadow database server resides.
- Authentication - Select the required type of authentication, SQL or Windows.
- User name - Type the account's user name.
- Password - Type the account's password.

- Save credentials - Select this checkbox to save the database credentials.
- Custom database location - Click this link to set the location of data files.
- SQL Host Server Credentials - Installation credentials for the machine on which the Shadow server resides. This account must be a member of the Local Administrators group on the machine during installation. The credentials are required only when the Shadow server does not reside on the DSP Server machine.

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- User name - Type the installation account's user name.
- Password - Type the installation account's password.
- Local Accounts
 - Collect information regarding local accounts from this file server - Select this checkbox to collect user accounts from this file system using FS credentials.
- FileWalk Settings
 - Identify actual unique folders and file system inconsistencies - Select this checkbox to detect broken permissions in NTFS file systems.

5. Click Install.

The file server is installed.

Adding Cohesity File Servers

You can install Cohesity file servers and set the parameters for data collection, file servers, FileWalk credentials, Cohesity REST API settings, and shares.

Workflow for Installing and Configuring Cohesity File Servers

The workflow for installing and configuring Cohesity file servers includes several steps:

1. [Add the relevant Cohesity file servers in the Management Console.](#)
2. [Download the Cohesity Connector for Varonis app from Cohesity Helios and install it on the Cohesity cluster.](#)

Adding a Cohesity File Server

To add a Cohesity file server:

1. Do one of the following:
 - In the Enterprise Installer, navigate to the Monitored File Servers page and click Add.
 - 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.

2. On the left menu, click Common and set the following parameters:
 - a. Resource Details
 - Resource/Server Name - Type the Cohesity cluster NetBIOS name.
 - b. Data Collection Details
 - Probe - From the drop-down list, select the Probe to be used with the file server.
 - Collector - From the drop-down list, select the required Collector.

Important: Once you have configured a Collector to interface with a specific Probe, you must use that Collector with the same Probe. This means that if you have already configured a Collector to interface with the selected Probe while adding a monitored file server, you must either select the same Collector, a Collector that is not yet connected to a Probe, or <No Collector>. If no Collector is used with the Probe server, select <No Collector>.

- c. FileWalk Credentials - File System operations include the directory crawl (FileWalk), event collection (if set) and user crawl (ADWalk) on local accounts (if set).

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

- User name - Type the name of the user account to be used for FileWalk, event collection and local ADWalk.
- Password - Type the account's password.
- Add this user account to the Filtered Users list - This is the default user account for Data Security Platform operations. If you clear this checkbox, a large number of events generated by the Data Security Platform will be collected.

d. Resource Type

- Select resource type - If you select a file server's type from this drop-down list, this is the type that is used no matter what type was detected earlier.

Note: If you typed the file server's name manually, you must enter the FileWalk credentials before you can use the Detect link, due to permission requirements. If the type still cannot be detected, use the override field.

- Detect resource type - Click this link to detect the type of file server you selected. (If you used the Browse button to locate the file server's name, its type is detected automatically as long as you have already entered credentials.)
- Detected resource type - Indicates the file server type, if it was automatically detected.

e. Cohesity REST API Credentials - This section is displayed only if Cohesity is selected or detected as the file server type. The following credentials are used to retrieve data about the file system and to collect 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.

3. To select specific shares for the file server, on the left menu, click Shares and do the following:

- a. In the Available Shares area, select the required shares and click the down arrow .

The selected shares are moved to the Registered Shares area.

Note: (Relevant for versions lower than 8.6.31) When selecting a parent volume, all child volumes must also be selected in order to collect events for the child shares.

- b. In the Ignore Detection column, select the shares to be ignored (and not be the subject of notifications) by the Resource monitor. Note that shares manually moved from registered shares to available shares should be selected.
- c. For each share, review and set the following information as required:
 - Share Name - The name of the share.
 - Path - The path on which the share resides.
 - Protocol - The protocol defined for the share.
 - Events - Select this checkbox to collect 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 collection and crawling.

- Mixed Security - In Windows environments, NT ACL extraction is always used.
- d. In the Automatic Detection area, set the following:
 - Automatically detect shares - DatAdvantage detects shares that reside at the highest level of the hierarchy and that are not already monitored. It gives preference to administrative shares over equivalent regular shares. From the drop-down list, select the relevant option:
 - Never - Select to instruct DatAdvantage not to detect shares automatically.
 - Detect and notify - Select to send users email that lists all newly detected shares. Unreachable shares are removed from DatAdvantage.
 - Notify - From the drop-down list, select the frequency at which to send notification of new shares. Options are:
 - Always - Select to send a cumulative list of all changes made (such as detection or deletion) to all shares.
 - Once - Select to send notification of a change (that is, detection or deletion) to a share only when that change occurs.
 - Remove Deleted Shares - Select this checkbox to remove deleted shares. Shares that were deleted from the file server will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the file server is unavailable, the shares will not be removed.
 - Enable Event Collection - Select this checkbox to collect events from all shares added from this volume/file server.

Note: When selecting a parent volume, all child volumes must be selected also in order to collect events for the child shares.

4. On the left menu, click Configuration and set the following parameters:

- File Server General Settings
 - Save file server properties history - Select this checkbox if you want DatAdvantage to monitor the changes in folder properties (size, number of nested folders, number of files, and number of nested files).

Note: Over a long period of time this data may use a large amount of storage on the database.

- Shadow Database Installation - Credentials for installing the Shadow database on the SQL server. The user must have the sysadmin role on the selected SQL server.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- Database Server - Type or browse for the machine on which the Shadow database server resides.
- Authentication - Select the required type of authentication, SQL or Windows.
- User name - Type the account's user name.
- Password - Type the account's password.
- Save credentials - Select this checkbox to save the database credentials.
- Custom database location - Click this link to set the location of data files.
- SQL Host Server Credentials - Installation credentials for the machine on which the Shadow server resides. This account must be a member of the Local Administrators group on the machine during installation. The credentials are required only when the Shadow server does not reside on the DSP Server machine.

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- User name - Type the installation account's user name.
- Password - Type the installation account's password.
- Local Accounts
 - Collect information regarding local accounts from this file server - Select this checkbox to collect user accounts from this file system using FS credentials.
- FileWalk Settings
 - Identify actual unique folders and file system inconsistencies - Select this checkbox to detect broken permissions in NTFS file systems.

5. Click Install.

The file server is installed.

Downloading the Cohesity Connector for Varonis App from Cohesity Helios and Installing it on the Cohesity Cluster

To install 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.
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.

To download and install 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. Click Upload App.
10. 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.
11. Navigate to the All Instances tab and click Open App to launch the app in a new tab.
12. 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](#).

Adding CTERA File Servers

You can install CTERA file servers and set the parameters for data collection, file servers, FileWalk credentials, CTERA REST API settings, and shares.

To add a CTERA file server:

1. Do one of the following:

- In the Enterprise Installer, navigate to the Monitored File Servers page and click Add.
- 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.

2. On the left menu, click Common and set the following parameters:

a. Resource Details

- Resource/Server Name - Type the resolved name or IP address of the file server to be added, or click the Browse button to locate it.

b. Data Collection Details

- Probe - From the drop-down list, select the Probe to be used with the file server.
- Collector - From the drop-down list, select the required Collector. - From the drop-down list, select the required Collector.

Important: Once you have configured a Collector to interface with a specific Probe, you must use that Collector with the same Probe. This means that if you have already configured a Collector to interface with the selected Probe while adding a monitored file server, you must either select the same Collector, a Collector that is not yet connected to a Probe, or <No Collector>. If no Collector is used with the Probe server, select <No Collector>.

Note: For CTERA file servers, you must use a Collector in order to collect events!

c. FileWalk Credentials - File System operations include the directory crawl (FileWalk), event collection (if set) and user crawl (ADWalk) on local accounts (if set).

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

- User name - Type the name of the user account to be used for FileWalk, event collection and local ADWalk.

- Password - Type the account's password.
- Add this user account to the Filtered Users list - This is the default user account for Data Security Platform operations. If you clear this checkbox, a large number of events generated by the Data Security Platform will be collected.

d. Resource Type

- Select resource type - If you select a file server's type from this drop-down list, this is the type that is used no matter what type was detected earlier.
- Detect resource type - Click this link to detect the type of file server you selected. (If you used the Browse button to locate the file server's name, its type is detected automatically as long as you have already entered credentials.)

Note: If you typed the file server's name manually, you must enter the FileWalk credentials before you can use the Detect link, due to permission requirements. If the type still cannot be detected, use the override field.

- Detected resource type - Indicates the file server type, if it was automatically detected.

e. CTERA REST API Credentials - This section is displayed only if CTERA is selected or detected as the file server type. The following credentials are used to retrieve data about the file system and to collect events.

Note: This is not a domain user.

- Virtual Portal DNS Name - Insert the portal name in DNS format. This attribute should not be updated after the file server was installed.

Note: The Virtual Portal DNS Name attribute is available starting from version 8.6.25. For versions lower than 8.6.25, the Gateway Forwarder IP attribute is used.

- 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.

3. To select specific shares for the file server, on the left menu, click Shares and do the following:

- a. In the Available Shares area, select the required shares and click the down arrow .

The selected shares are moved to the Registered Shares area.

- b. In the Ignore Detection column, select the shares to be ignored (and not be the subject of notifications) by the Resource monitor. Note that shares manually moved from registered shares to available shares should be selected.
- c. For each share, review and set the following information as required:
 - Share Name - The name of the share.
 - Path - The path on which the share resides.
 - Protocol - The protocol defined for the share.
 - Events - Select this checkbox to collect 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 collection and crawling.

- Mixed Security - In Windows environments, NT ACL extraction is always used.
 - d. In the Automatic Detection area, set the following:
 - Automatically detect shares - DatAdvantage detects shares that reside at the highest level of the hierarchy and that are not already monitored. It gives preference to administrative shares over equivalent regular shares. From the drop-down list, select the relevant option:
 - Never - Select to instruct DatAdvantage not to detect shares automatically.
 - Detect and notify - Select to send users email that lists all newly detected shares. Unreachable shares are removed from DatAdvantage.
 - Notify - From the drop-down list, select the frequency at which to send notification of new shares. Options are:
 - Always - Select to send a cumulative list of all changes made (such as detection or deletion) to all shares.
 - Once - Select to send notification of a change (that is, detection or deletion) to a share only when that change occurs.
 - Remove Deleted Shares - Select this checkbox to remove deleted shares. Shares that were deleted from the file server will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the file server is unavailable, the shares will not be removed.
 - Enable Event Collection - Select this checkbox to collect events from all shares added from this volume/file server.
4. On the left menu, click Configuration and set the following parameters:

- File Server General Settings
 - Save file server properties history - Select this checkbox if you want DatAdvantage to monitor the changes in folder properties (size, number of nested folders, number of files, and number of nested files).

Note: Over a long period of time this data may use a large amount of storage on the database.

- Shadow Database Installation - Credentials for installing the Shadow database on the SQL server. The user must have the sysadmin role on the selected SQL server.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- Database Server - Type or browse for the machine on which the Shadow database server resides.
- Authentication - Select the required type of authentication, SQL or Windows.
- User name - Type the account's user name.
- Password - Type the account's password.
- Save credentials - Select this checkbox to save the database credentials.
- Custom database location - Click this link to set the location of data files.
- SQL Host Server Credentials - Installation credentials for the machine on which the Shadow server resides. This account must be a member of the Local Administrators group on the machine during installation. The credentials are required only when the Shadow server does not reside on the DSP Server machine.

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- User name - Type the installation account's user name.
- Password - Type the installation account's password.
- FileWalk Settings

- Identify actual unique folders and file system inconsistencies - Select this checkbox to detect broken permissions in NTFS file systems.

5. Click Install.

The file server is installed.

Adding Hitachi NAS File Servers

You can install Hitachi NAS file servers and set the parameters for data collection, file servers, FileWalk credentials, and shares.

To add a Hitachi NAS file server:

1. Do one of the following:

- In the Enterprise Installer, navigate to the Monitored File Servers page and click Add.
- 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.

2. On the left menu, click Common and set the following parameters:

a. Resource Type

- Select resource type - If you select a file server's type from this drop-down list, this is the type that is used no matter what type was detected earlier.

Note: If you typed the file server's name manually, you must enter the FileWalk credentials before you can use the Detect link, due to permission requirements. If the type still cannot be detected, use the override field.

- Detect resource type - Click this link to detect the type of file server you selected. (If you used the Browse button to locate the file server's name, its type is detected automatically as long as you have already entered credentials.)
- Detected resource type - Indicates the file server type, if it was automatically detected.

b. Resource Details

- Resource/Server Name - Type the resolved name or IP address of the file server to be added, or click the Browse button to locate it.

c. Data Collection Details

- Probe - From the drop-down list, select the Probe to be used with the file server.
- Collector - From the drop-down list, select the required Collector.

Important: Once you have configured a Collector to interface with a specific Probe, you must use that Collector with the same Probe. This means that if you have already configured a Collector to interface with the selected Probe while adding a monitored file server, you must either select the same Collector, a Collector that is not yet connected to a Probe, or <No Collector>. If no Collector is used with the Probe server, select <No Collector>.

d. FileWalk Credentials - File System operations include the directory crawl (FileWalk), event collection (if set) and user crawl (ADWalk) on local accounts (if set).

- User name - Type the name of the user account to be used for FileWalk, event collection and local ADWalk.
- Password - Type the account's password.

Note: These credentials must be standard Windows-style credentials (domain\user).

- Add this user account to the Filtered Users list - This is the default user account for Data Security Platform operations. If you clear this checkbox, a large number of events generated by the Data Security Platform will be collected.

e. Hitachi NAS Rest API Server Settings - To enable full NFS functionality on pure NFS and mixed volumes, select the Add NFS support checkbox, and fill in the following fields:

- Administrative EVS address - Type the Hitachi NAS Administrative Enterprise Virtual Server address.
- REST API Server user name - Type the user name for REST API server. The user must have a supervisor role.
- REST API Server password- Type the password for the REST API server.

3. To select specific shares for the file server, on the left menu, click Shares and do the following:

a. In the Available Shares area, select the required shares and click the down arrow .

The selected shares are moved to the Registered Shares area.

b. In the Ignore Detection column, select the shares to be ignored (and not be the subject of notifications) by the resource monitor. Note the following scenarios:

- Shares manually moved from registered shares to available shares should be selected.

- When users manually add shares from available shares to registered shares, the checkbox must be cleared.

c. For each share, review and set the following information as required:

Note: If the file server is installed only for use with DataPrivilege, event collection is disabled.

- Share Name - The name of the share.
- Path - The path on which the share resides.
- Protocol - The protocol defined for the share.

Note: The Varonis FileWalk method uses the SSH protocol for this purpose.

- Events - Select this checkbox to collect events for the share.
- Crawl - To enable or disable monitoring for the share, in the Crawl column, select the relevant option.
- Mixed Security - In mixed NT-Unix environments, indicates the default ACL extraction.

d. In the Automatic Detection area, set the following:

- Automatically detect shares - DatAdvantage detects shares that reside at the highest level of the hierarchy and that are not already monitored. It gives preference to administrative shares over equivalent regular shares. From the drop-down list, select the relevant option:
 - Never - Select to instruct DatAdvantage not to detect shares or mounts automatically.
 - Detect and notify - Select to send users email that lists all newly detected shares or mounts. Unreachable shares and mounts are removed from DatAdvantage.
 - Detect and monitor - Select to add the newly detected shares or mounts to the Registered Shares or Registered Mounts list in the dialog box, with the Events column checked and the Crawl column set to enable crawling. Unreachable shares and mounts are removed from DatAdvantage.
 - Detect, monitor and notify - Select to add the newly detected shares or mounts as described above, and send users email listing them. Unreachable shares and mounts are (removed from DatAdvantage.

Note: Via the monitor selections, it is possible to add all the top-level shares per protocol (type) automatically as monitoring shares (for example, it is possible to add a 1st level share in CIFS protocol and 2nd level share in MIX mode/ Unix mode). To remove a specific share from the monitoring shares list, move manually the required share from Register Shares to Available Shares, and select Ignore Detection to ensure the resource manager will not add this share automatically to the monitoring shares (relevant for NetApp only).

Note: Shares using “mixed mode” are not supported.

- Notify - From the drop-down list, select the frequency at which to send notification of new shares or mounts. Options are:
 - Always - Select to send a cumulative list of all changes made (such as detection or deletion) to all shares and mounts.
 - Once - Select to send notification of a change (that is, detection or deletion) to a share or mount only when that change occurs.
- Remove Deleted Shares - Select this checkbox to remove deleted shares. Shares that were deleted from the file server will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the file server is unavailable, the shares will not be removed.
- Enable Event Collection - Select this checkbox to collect events from all shares added from this volume/file server.

4. On the left menu, click Configuration and set the following parameters:

- Unix Domain
 - Select the affiliated Unix user repository for this file server or Samba domain - From the drop-down 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.

- File Server General Settings
 - Save file server properties history - Select this checkbox if you want DatAdvantage to monitor the changes in folder properties (size, number of nested folders, number of files, and number of nested files).

Note: Over a long period of time this data may use a large amount of storage on the database.

- Shadow Database Installation - Credentials for installing the Shadow database on the SQL server. The user must have the sysadmin role on the selected SQL server.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- Database Server - Type or browse for the machine on which the Shadow database server resides.
- Authentication - Select the required type of authentication, SQL or Windows.
- User name - Type the account's user name.
- Password - Type the account's password.
- Save credentials - Select this checkbox to save the database credentials.
- Custom database location - Click this link to set the location of data files.
- SQL Host Server Credentials - Installation credentials for the machine on which the Shadow server resides. This account must be a member of the Local Administrators group on the machine during installation. The credentials are required only when the Shadow server does not reside on the DSP Server machine.

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- User name - Type the installation account's user name.
- Password - Type the installation account's password.
- FileWalk Settings
 - Identify actual unique folders and file system inconsistencies - Select this checkbox to detect broken permissions in NTFS file systems.
 - Run FileWalk in incremental mode (hourly) - Select this checkbox to run incremental FileWalk once an hour. Incremental FileWalk runs only on folders in which events occurred. It is only supported for file servers on which all the monitored shares (CIFS and NFS) provide resolved events, with full path location information.
- Event Collection Parameters
 - 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. Access Denied events must be enabled on the Hitachi NAS auditing system.

5. To configure the commit credentials to allow users to use different commit credentials than the configured FileWalk credentials, on the left menu, click Commit and set the following parameters:

- File Server Commit Credentials - Set the credentials to be used for committing DataPrivilege changes on the file server. The account used must have Backup Operator and Power User privileges. It must also be a member of the Administrators local machine group (for Windows or NAS devices), or a member of the Site Collection Administrators group (for SharePoint).

Note: In all commit operations on a NetApp CM file server, the user who executes the operation must be a CIFS superuser.

- Clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for the FileWalk job. (By default, this checkbox is selected to use the FileWalk credentials, and the User name and Password fields are disabled for editing.)
- In the User name and Password fields, enter the relevant user name and password.
- Group OU - Select the organizational unit in which DataPrivilege creates groups. Groups created by DataPrivilege reside in the default base OU, unless otherwise specified.
 - Inherited from domain - By default, this option is selected to use the domain's default OU.
 - Uniquely defined - Select this option to choose a different OU from those defined in the file server's domain.
 - OU - Click the Browse button (...) to select the required OU.

6. Click Install.

The file server is installed.

Adding HP-NAS File Servers

You can install HP-NAS file servers and set the parameters for data collection, file servers, FileWalk credentials, and shares.

HP-NAS is a multi-protocol file server accessible by both CIFS and NFS (like NetApp and Dell Celerra). It consists of a cluster of Linux nodes. The file server must be a member of a regular Active Directory domain with an RFC2307 extension.

To add an HP-NAS file server:

1. Do one of the following:

- In the Enterprise Installer, navigate to the Monitored File Servers page and click Add.
- 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.

2. On the left menu, click Common and set the following parameters:

a. Resource Type

- Select resource type - If you select a file server's type from this drop-down list, this is the type that is used no matter what type was detected earlier.

Note: If you typed the file server's name manually, you must enter the FileWalk credentials before you can use the Detect link, due to permission requirements. If the type still cannot be detected, use the override field.

- Detected resource type - - Indicates the file server type, if it was automatically detected.
- Detect resource type - Click this link to detect the type of file server you selected. (If you used the Browse button to locate the file server's name, its type is detected automatically as long as you have already entered credentials.)

b. Resource Details

- Resource/Server Name - Type the resolved name or IP address of the file server to be added, or click the Browse button to locate it.

c. Data Collection Details

- Probe - From the drop-down list, select the Probe to be used with the file server.
- Collector - From the drop-down list, select the required Collector.

Important: Once you have configured a Collector to interface with a specific Probe, you must use that Collector with the same Probe. This means that if you have already configured a Collector to interface with the selected Probe while adding a monitored file server, you must either select the same Collector, a Collector that is not yet connected to a Probe, or <No Collector>. If no Collector is used with the Probe server, select <No Collector>.

- d. FileWalk Credentials - File System operations include the directory crawl (FileWalk), event collection (if set) and user crawl (ADWalk) on local accounts (if set).

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

- User name - Type the name of the user account to be used for FileWalk, event collection and local ADWalk.
- Password - Type the account's password.

Note: These credentials must be standard Windows-style credentials (domain\user).

- Add this user account to the Filtered Users list - This is the default user account for Data Security Platform operations. If you clear this checkbox, a large number of events generated by the Data Security Platform will be collected.

- e. Varonis Agent Installation

- Do not install or upgrade the filter agent on this server - Select this checkbox if you do not want the Varonis filter agent automatically installed or upgraded on the file server.
- Click the Agent Deployment link to define the credentials used to install the agent on the file server. The Agent Deployment Options window is displayed. Set the following parameters.

- Agent Installation Credentials


- Use FileWalk credentials for agent installation - Select this checkbox to install the agent using the same credentials as the FileWalk.

Note: If you select this option, ensure that the FileWalk 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.

Note: For HP-NAS devices, specify root user credentials (Unix-style) to ensure the driver is installed correctly on the target server.

Note: If a root user is not specified, the driver package is copied to the `/tmp/Varonis.<user name>` folder on the file server and can be locally installed.

- Physical Machines - Settings for adding load-balancing cluster or redundant failover
 - Server - Type or browse to the cluster's physical node name and click Add.
3. To select specific shares for the file serverShares and do the following:, on the left menu, click
- a. In the Available Shares area, select the required shares and click the down arrow .
The selected shares are moved to the Registered Shares area.
 - b. In the Ignore Detection column, select the shares to be ignored (and not be the subject of notifications) by the resource monitor. Note the following scenarios:
 - Shares manually moved from registered shares to available shares should be selected.
 - When users manually add shares from available shares to registered shares, the checkbox must be cleared.
 - c. For each share, review and set the following information as required:

Note: If the file server is installed only for use with DataPrivilege, event collection is disabled.

- Share Name - The name of the share.
- Path - The path on which the share resides.
- Protocol - The protocol defined for the share.

Note: The Varonis FileWalk method uses the SSH protocol for this purpose.

- Events - Select this checkbox to collect events for the share.
 - Crawl - To enable or disable monitoring for the share, in the Crawl column, select the relevant option.
 - Mixed Security - In mixed NT-Unix environments, indicates the default ACL extraction.
- d. In the ,Automatic Detection area, set the following:

- Automatically detect shares - DatAdvantage detects shares that reside at the highest level of the hierarchy and that are not already monitored. It gives preference to administrative shares over equivalent regular shares. From the drop-down list, select the relevant option:
 - Never - Select to instruct DatAdvantage not to detect shares or mounts automatically.
 - Detect and notify - Select to send users email that lists all newly detected shares or mounts. Unreachable shares and mounts are removed from DatAdvantage.
 - Detect and monitor - Select to add the newly detected shares or mounts to the Registered Shares or Registered Mounts list in the dialog box, with the Events column checked and the Crawl column set to enable crawling. Unreachable shares and mounts are removed from DatAdvantage.
 - Detect, monitor and notify - Select to add the newly detected shares or mounts as described above, and send users email listing them. Unreachable shares and mounts are (removed from DatAdvantage).

Note: Via the monitor selections, it is possible to add all the top-level shares per protocol (type) automatically as monitoring shares (for example, it is possible to add a 1st level share in CIFS protocol and 2nd level share in MIX mode/ Unix mode). To remove a specific share from the monitoring shares list, move manually the required share from Register Shares to Available Shares, and select Ignore Detection to ensure the resource manager will not add this share automatically to the monitoring shares (relevant for NetApp only).

Note: Shares using “mixed mode” are not supported.

- Notify - From the drop-down list, select the frequency at which to send notification of new shares or mounts. Options are:
 - Always - Select to send a cumulative list of all changes made (such as detection or deletion) to all shares and mounts.
 - Once - Select to send notification of a change (that is, detection or deletion) to a share or mount only when that change occurs.
 - Remove Deleted Shares - Select this checkbox to remove deleted shares. Shares that were deleted from the file server will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the file server is unavailable, the shares will not be removed.
 - Enable Event Collection - Select this checkbox to collect events from all shares added from this volume/file server.
4. On the left menu, click Configuration and set the following parameters:
- Unix Domain
 - Select the affiliated Unix user repository for this file server or Samba domain - From the drop-down 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.

- File Server General Settings
 - Save file server properties history - Select this checkbox if you want DatAdvantage to monitor the changes in folder properties (size, number of nested folders, number of files, and number of nested files).

Note: Over a long period of time this data may use a large amount of storage on the database.

- Shadow Database Installation - Credentials for installing the Shadow database on the SQL server. The user must have the sysadmin role on the selected SQL server.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- Database Server - Type or browse for the machine on which the Shadow database server resides.
- Authentication - Select the required type of authentication, SQL or Windows.
- User name - Type the account's user name.
- Password - Type the account's password.
- Save credentials - Select this checkbox to save the database credentials.
- Custom database location - Click this link to set the location of data files.
- SQL Host Server Credentials - Installation credentials for the machine on which the Shadow server resides. This account must be a member of the Local Administrators group on the machine during installation. The credentials are required only when the Shadow server does not reside on the DSP Server machine.

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- User name - Type the installation account's user name.

- Password - Type the installation account's password.
 - Security Policy
 - Enable monitoring - Select the monitoring option from the drop-down list, NT or Unix. When this option is changed, volumes are automatically rescanned.
 - Default for mixed security - Select an option from the drop-down list, NT, Unix, Disabled, or PermissionDisabled.
 - POSIX Access Control List
 - Enable collection and management of POSIX ACLs - Select this option as relevant for Unix flavors that support POSIX ACLs.
5. Click Install.
The file server is installed.
6. Proceed to [HP-NAS Post-Installation Activities](#).

HP-NAS Post-Installation Activities

HP-NAS Post-Installation Activities

For each node in the cluster, there are various steps to perform after installing HP-NAS, including setting the cache size and other config file parameters, and adding the users to the Varonis group.

Do the following for each node in the cluster:

1. Install the RHEL5-SMP-2.6.18-x86-64 package (already copied to the node).
2. In the `/opt/varonis/varonis_drv.conf` file, set `uidCacheSize` to 1024.
3. Run `/opt/varonis/vrns_drv_adm.sh reload`.
4. In the `/opt/varonis/varonis.conf` file, do the following:
 - Set `<lstatKernel>` to 1.
 - Set `<forcedFsuidFile>` to `/var/lib/likewise/requestor`.

5. Run `touch /var/lib/likewise/requestor` .
6. Do the following to add the user to the varonis group.
 - a. Open the `/etc/group` file.
 - b. Find the entry for the varonis group.
 - c. Add the user after the last colon (:) using the `<DOMAIN_NAME>\<username>` format, where:
 - `<DOMAIN_NAME>` is the name of the domain in upper case.
 - `<username>` is the name of the user in lower case.

Note: Multiple group members are defined using a comma-delimited list.

Example:

```
varonis:x:1801: DEVCORE\administrator
```

- d. Save and close the file.
7. Execute the following command to ensure the user is recognized by `getent`:

```
getent passwd <domain>\\<user>
```

Adding HPE 3PAR File Persona

You can install HPE 3PAR File Persona and set the parameters for data collection, file servers, FileWalk credentials, connection settings, and shares.

1. Do one of the following:

- In the Enterprise Installer, navigate to the Monitored File Servers page and click Add.
- 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.

2. On the left menu, click Common and set the following parameters:

a. Resource Type

- Select resource type - Select HPE 3PAR File Persona from the drop-down list. - If you select a file server's type from this drop-down list, this is the type that is used no matter what type was detected earlier.

Note: If you typed the file server's name manually, you must enter the FileWalk credentials before you can use the Detect link, due to permission requirements. If the type still cannot be detected, use the override field.

- Detect resource type - Click this link to detect the type of file server you selected. (If you used the Browse button to locate the file server's name, its type is detected automatically as long as you have already entered credentials.)
- Detected resource type - - Indicates the file server type, if it was automatically detected.

b. Resource Details

- Resource/Server Name - Type the resolved name or IP address of the file server to be added, or click the Browse button to locate it.

c. Data Collection Details


- Probe - From the drop-down list, select the Probe to be used with the file server.
- Collector - From the drop-down list, select the required Collector.

Important: Once you have configured a Collector to interface with a specific Probe, you must use that Collector with the same Probe. This means that if you have already configured a Collector to interface with the selected Probe while adding a monitored file server, you must either select the same Collector, a Collector that is not yet connected to a Probe, or <No Collector>. If no Collector is used with the Probe server, select <No Collector>.

Note: The "one-minute cache" filter, available in the Collector, can be disabled to improve performance (but disabling it will create more events in the DB. If you need to do so, contact Varonis Support.

- d. FileWalk Credentials - File System operations include the directory crawl (FileWalk), event collection (if set) and user crawl (ADWalk) on local accounts (if set).

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

- User name - Type the name of the user account to be used for FileWalk, event collection and local ADWalk. Note that this user must be entered in the HPE 3PAR CLI, as described in [step 3e in Configuring HPE 3PAR SSMC and HPE 3PAR CLI](#).
 - Password - Type the account's password.
- e. Connection Settings - This section is displayed only if HPE 3PAR is selected as the file server type.
- File Server GUID - Enter the GUID of the Virtual File Server (VFS) in this field. DatAdvantage uses this GUID to connect and collect events from the HPE 3PAR file server. You can extract the GUID from the HPE 3PAR CLI, by typing the command `showfsaudit pol`. For more details, see [Configuring HPE 3PAR SSMC and HPE 3PAR CLI](#).
3. To select specific shares for the file server, on the left menu, click Shares and do the following:
- a. In the Available Shares area, select the required shares and click the down arrow .
The selected shares are moved to the Registered Shares area.
 - b. In the Ignore Detection column, select the shares to be ignored (and not be the subject of notifications) by the resource monitor. Note the following scenarios:
 - Shares manually moved from registered shares to available shares should be selected.
 - When users manually add shares from available shares to registered shares, the checkbox must be cleared.
 - c. For each share, review and set the following information as required:
 - Share Name - The name of the share.
 - Path - The path on which the share resides.
 - Protocol - The protocol defined for the share.

Note: The Varonis FileWalk method uses the SSH protocol for this purpose.

- Events - Select the checkbox to collect events for the share.
- Crawl - To enable or disable monitoring for the share, in the Crawl column, select the relevant option.

d. In the Automatic Detection area, set the following:

- Automatically detect shares - DatAdvantage detects shares that reside at the highest level of the hierarchy and that are not already monitored. It gives preference to administrative shares over equivalent regular shares. From the drop-down list, select the relevant option:
 - Never - Select to instruct DatAdvantage not to detect shares or mounts automatically.
 - Detect and notify - Select to send users email that lists all newly detected shares or mounts. Unreachable shares and mounts are removed from DatAdvantage.
 - Detect and monitor - Select to add the newly detected shares or mounts to the Registered Shares or Registered Mounts list in the dialog box, with the Events column checked and the Crawl column set to enable crawling. Unreachable shares and mounts are removed from DatAdvantage.
 - Detect, monitor and notify - Select to add the newly detected shares or mounts as described above, and send users email listing them. Unreachable shares and mounts are (removed from DatAdvantage.

Note: Via the monitor selections, it is possible to add all the top-level shares per protocol (type) automatically as monitoring shares (for example, it is possible to add a 1st level share in CIFS protocol and 2nd level share in MIX mode/ Unix mode). To remove a specific share from the monitoring shares list, move manually the required share from Register Shares to Available Shares, and select Ignore Detection to ensure the resource manager will not add this share automatically to the monitoring shares (relevant for NetApp only).

Note: Shares using “mixed mode” are not supported.

- Notify - From the drop-down list, select the frequency at which to send notification of new shares or mounts. Options are:
 - Always - Select to send a cumulative list of all changes made (such as detection or deletion) to all shares and mounts.
 - Once - Select to send notification of a change (that is, detection or deletion) to a share or mount only when that change occurs.

- Remove Deleted Shares - Select this checkbox to remove deleted shares. Shares that were deleted from the file server will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the file server is unavailable, the shares will not be removed.
- Enable Event Collection - Select this checkbox to collect events from all shares added from this volume/file server.

4. On the left menu, click Configuration and set the following parameters:

- Unix Domain
 - Select the affiliated Unix user repository for this file server or Samba domain - From the drop-down 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.

- File Server General Settings
 - Save file server properties history - Select this checkbox if you want DatAdvantage to monitor the changes in folder properties (size, number of nested folders, number of files, and number of nested files).

Note: Over a long period of time this data may use a large amount of storage on the database.

- Shadow Database Installation - Credentials for installing the Shadow database on the SQL server. The user must have the sysadmin role on the selected SQL server.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- Database Server - Type or browse for the machine on which the Shadow database server resides.
- Authentication - Select the required type of authentication, SQL or Windows.
- User name - Type the account's user name.
- Password - Type the account's password.
- Save credentials - Select this checkbox to save the database credentials.
- Custom database location - Click this link to set the location of data files.

- SQL Host Server Credentials - Installation credentials for the machine on which the Shadow server resides. This account must be a member of the Local Administrators group on the machine during installation. The credentials are required only when the Shadow server does not reside on the DSP Server machine.

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- User name - Type the installation account's user name.
- Password - Type the installation account's password.
- Local Accounts
 - Collect information regarding local accounts from this resource local groups - Select this option to collect local accounts.
- FileWalk Settings
 - Identify actual unique folders and file system inconsistencies - Select this option to detect broken inheritance in NTFS file systems.
 - Run FileWalk in incremental mode (hourly) - Select this option to run incremental FileWalk once an hour. Incremental FileWalk runs only on folders in which events occurred. It is only supported for file servers on which all the monitored shares (CIFS and NFS) provide resolved events - with full path location information.
- NFS Commit - The definitions in this section enable performing commit on NFS (for Unix, Dell, NetApp, HPE 3PAR File Persona, or HP-NAS). To maintain security, the commit process must be activated through a gateway. The gateway can be any Unix machine that has access to the NFS exports on the file server and that is accessible via SSH. The gateway need only be defined for file servers on which NFS commit is available.
 - Gateway - Type the IP address of the Unix machine that acts as the gateway.
 - Via mount pattern - Type the required pattern. Can be:
 - Host name pattern - For example, HOSTNAME:/*
 - IP address pattern - For example, 10.10.10.160:/*
The asterisk (*) indicates multiple mounts on the same machine, with different exports.

5. Click Install.

The file server is installed.

Adding Unix Samba File Servers

IBM AIX file servers are based on Unix. You can install Unix Samba file servers and set the parameters for data collection, file servers, FileWalk credentials, Varonis Agent installation settings, shares, and mounts.

To add a Unix Samba (SMB) file server:

1. Do one of the following:

- In the Enterprise Installer, navigate to the Monitored File Servers page and click Add.
- 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.

2. On the left menu, click Common and set the following parameters:

a. Resource Type

- Select resource type - If you select a file server's type from this drop-down list, this is the type that is used no matter what type was detected earlier.

Note: If you typed the file server's name manually, you must enter the FileWalk credentials before you can use the Detect link, due to permission requirements. If the type still cannot be detected, use the override field.

- Detect resource type - Click this link to detect the type of file server you selected. (If you used the Browse button to locate the file server's name, its type is detected automatically as long as you have already entered credentials.)
- Detected resource type - Indicates the file server type, if it was automatically detected.

b. Resource Details

- Resource/Server Name - Type the resolved name or IP address of the file server to be added, or click the Browse button to locate it.

c. Data Collection Details

- Probe - From the drop-down list, select the Probe to be used with the file server.

- Collector - From the drop-down list, select the required Collector.

Important: Once you have configured a Collector to interface with a specific Probe, you must use that Collector with the same Probe. This means that if you have already configured a Collector to interface with the selected Probe while adding a monitored file server, you must either select the same Collector, a Collector that is not yet connected to a Probe, or <No Collector>. If no Collector is used with the Probe server, select <No Collector>.

d. FileWalk Credentials - File System operations include the directory crawl (FileWalk), event collection (if set) and user crawl (ADWalk) on local accounts (if set).


- User name - Type the name of the user account to be used for FileWalk, event collection and local ADWalk.
- Password - Type the account's password.

Note: These credentials must be standard Windows-style credentials (domain\user).

- Add this user account to the Filtered Users list - This is the default user account for Data Security Platform operations. If you clear this checkbox, a large number of events generated by the Data Security Platform will be collected.

e. Varonis Agent Installation

- Do not install or upgrade the filter agent on this server - Select this checkbox if you do not want the Varonis filter agent automatically installed or upgraded on the file server.
- Click the Agent Deployment link to define the credentials used to install the agent on the file server. The Agent Deployment Options window is displayed.
 - Agent Installation Credentials
 - User name - Type the agent installation account's user name.
 - Password - Type the agent installation account's password.
 - Physical Machines - Settings for adding load-balancing cluster or redundant failover
 - Server - Type or browse to the cluster's physical node name and click Add.

3. To select specific shares for the file server, on the left menu, click Shares and do the following:
- a. In the Available Mounts area, select the required mounts and click the down arrow .

The selected mounts are moved to the Registered Mounts area.

b. In the Ignore Detection column, select the mounts to be ignored (and not be the subject of notifications) by the resource monitor. Note the following scenarios:

- Mounts manually moved from registered mounts to available mounts should be selected.
- When users manually add mounts from available shares to registered mounts, the checkbox must be cleared.

c. For each share, review and set the following information as required:

- Share Name - The name of the share.
- Path - The path on which the share resides.
- Protocol - The protocol defined for the share.

Note: The Varonis FileWalk method uses the SSH protocol for this purpose.

- Events - Select this checkbox to collect events for the share.
- Crawl - To enable or disable monitoring for the share, in the Crawl column, select the relevant option.
- Mixed Security - In mixed NT-Unix environments, indicates the default ACL extraction.

d. In the Automatic Detection area, set the following:

- Automatically detect shares - DatAdvantage detects shares that reside at the highest level of the hierarchy and that are not already monitored. It gives preference to administrative shares over equivalent regular shares. From the drop-down list, select the relevant option:
 - Never - Select to instruct DatAdvantage not to detect shares or mounts automatically.
 - Detect and notify - Select to send users email that lists all newly detected shares or mounts. Unreachable shares and mounts are removed from DatAdvantage.
 - Detect and monitor - Select to add the newly detected shares or mounts to the Registered Shares or Registered Mounts list in the dialog box, with the Events column checked and the Crawl column set to enable crawling. Unreachable shares and mounts are removed from DatAdvantage.
 - Detect, monitor and notify - Select to add the newly detected shares or mounts as described above, and send users email listing them. Unreachable shares and mounts are (removed from DatAdvantage.

Note: Via the monitor selections, it is possible to add all the top-level shares per protocol (type) automatically as monitoring shares (for example, it is possible to add a 1st level share in CIFS protocol and 2nd level share in MIX mode/ Unix mode). To remove a specific share from the monitoring shares list, move manually the required share from Register Shares to Available Shares, and select Ignore Detection to ensure the resource manager will not add this share automatically to the monitoring shares (relevant for NetApp only).

Note: Shares using “mixed mode” are not supported.

- Notify - From the drop-down list, select the frequency at which to send notification of new shares or mounts. Options are:
 - Always - Select to send a cumulative list of all changes made (such as detection or deletion) to all shares and mounts.
 - Once - Select to send notification of a change (that is, detection or deletion) to a share or mount only when that change occurs.
- Remove Deleted Shares - Select this checkbox to remove deleted shares. Shares that were deleted from the file server will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the file server is unavailable, the shares will not be removed.
- Enable Event Collection - Select this checkbox to collect events from all shares added from this volume/file server.

4. On the left menu, click Configuration and set the following parameters:

- Unix Domain
 - Select the affiliated Unix user repository for this file server or Samba domain - From the drop-down 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.

- File Server General Settings
 - Save file server properties history - Select this checkbox if you want DatAdvantage to monitor the changes in folder properties (size, number of nested folders, number of files, and number of nested files).

Note: Over a long period of time this data may use a large amount of storage on the database.

- Shadow Database Installation - Credentials for installing the Shadow database on the SQL server. The user must have the sysadmin role on the selected SQL server.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- Database Server - Type or browse for the machine on which the Shadow database server resides.
- Authentication - Select the required type of authentication, SQL or Windows.
- User name - Type the account's user name.
- Password - Type the account's password.
- Save credentials - Select this checkbox to save the database credentials.
- Custom database location - Click this link to set the location of data files.
- SQL Host Server Credentials - Installation credentials for the machine on which the Shadow server resides. This account must be a member of the Local Administrators group on the machine during installation. The credentials are required only when the Shadow server does not reside on the DSP Server machine.

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- User name - Type the installation account's user name.
- Password - Type the installation account's password.
- Security Policy
 - Enable monitoring - Select the monitoring option from the drop-down list, NT or Unix. When this option is changed, volumes are automatically rescanned.
 - Default for mixed security - Select an option from the drop-down list, NT, Unix, Disabled, or PermissionDisabled.
- POSIX Access Control List
 - Enable collection and management of POSIX ACLs - Select this option as relevant for Unix flavors that support POSIX ACLs.

- NFS Commit - The definitions in this section enable performing commit on NFS (for Unix, Dell, NetApp, HPE 3PAR File Persona, or HP-NAS). To maintain security, the commit process must be activated through a gateway. The gateway can be any Unix machine that has access to the NFS exports on the file server and that is accessible via SSH. The gateway need only be defined for file servers on which NFS commit is available.
 - Gateway - Type the IP address of the Unix machine that acts as the gateway.
 - Via mount pattern - Type the required pattern. Can be:
 - Host name pattern - For example, HOSTNAME:/*
 - IP address pattern - For example, 10.10.10.160:/*
The asterisk (*) indicates multiple mounts on the same machine, with different exports.

5. Click Install.

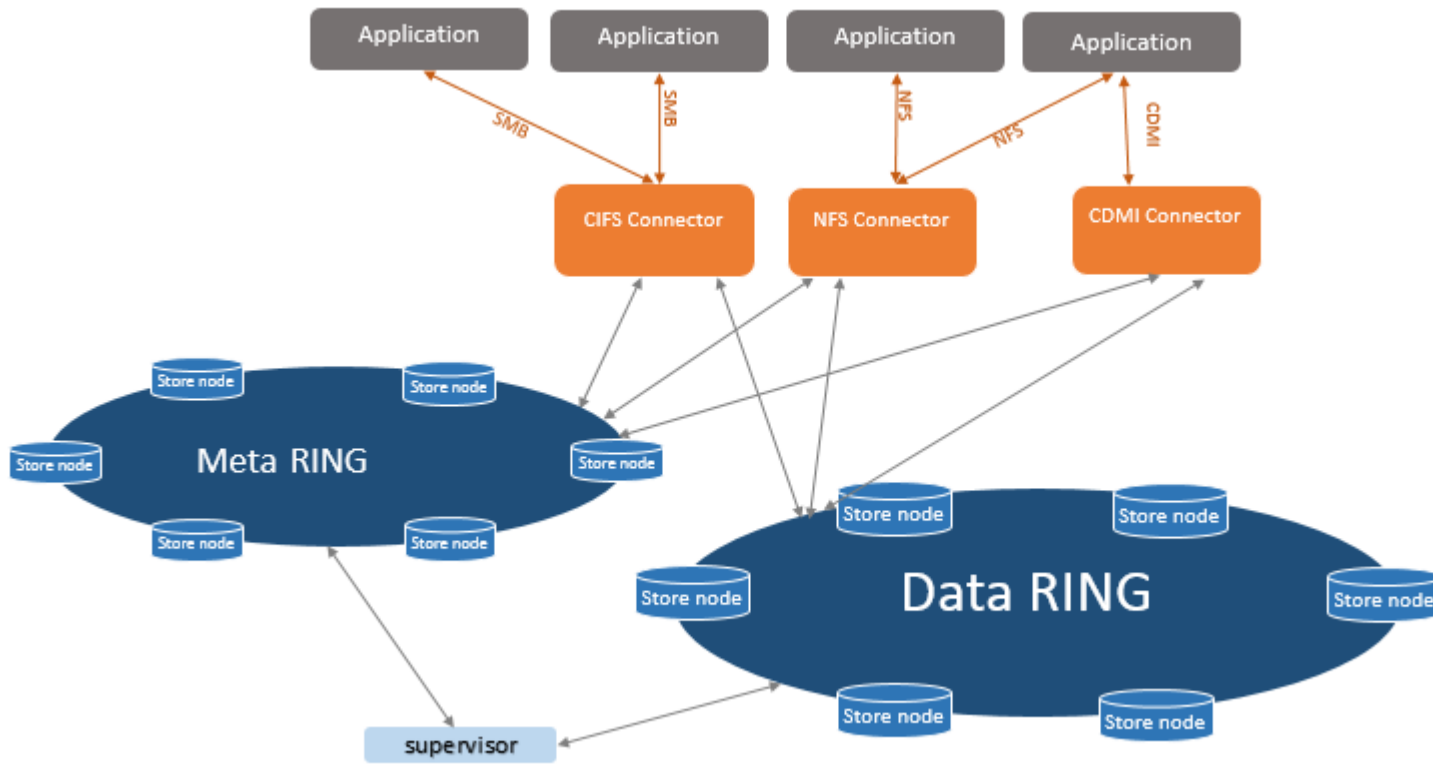
The file server is installed.

Scality RING Architecture

The Scality RING architecture includes various components.

These include:

- CIFS connector - A Linux machine with a Samba service, used for CIFS access to the RING. Several CIFS connectors can be configured.
- NFS connector - A Linux machine with an NFS service, used for NFS access to the RING. Several NFS connectors can be configured.
- CDMI connector - A Linux machine with a CDMI (Cloud Data Management Interface) service, used for HTTP access to the RING. Several CDMI connectors can be configured.
- Data RING - Distributed data storage.
- Meta RING - Distributed metadata storage. A customer can choose to store the metadata together with the data on the data ring.
- Supervisor - Monitors and controls the nodes in the rings, contains a local fuse connector for backups.



Prerequisites/Limitations

- The Data Security Platform monitors only CIFS events from the CIFS connectors.
- CIFS connectors are added as Unix Samba file servers.

- The Linux version used for the CIFS connector must be a version that is supported.

Adding Scality RING File Servers

Adding Scality RING File Servers

When adding a Scality RING file server, make sure to choose NTFS and NFS as the crawling method for all the shares.

To add a Scality RING file server, add each connector as a different file server:

1. Do one of the following:

- In the Enterprise Installer, navigate to the Monitored File Servers page and click Add.
- 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.

2. On the left menu, click Common and set the following parameters:

a. Resource Type

- Select resource type - If you select a file server's type from this drop-down list, this is the type that is used no matter what type was detected earlier.

Note: If you typed the file server's name manually, you must enter the FileWalk credentials before you can use the Detect link, due to permission requirements. If the type still cannot be detected, use the override field.

- Detect resource type - Click this link to detect the type of file server you selected. (If you used the Browse button to locate the file server's name, its type is detected automatically as long as you have already entered credentials.)
- Detected resource type - - Indicates the file server type, if it was automatically detected.

b. Resource Details

- Resource/Server Name - Type the resolved name or IP address of the file server to be added, or click the Browse button to locate it.

c. Data Collection Details

- Probe - From the drop-down list, select the Probe to be used with the file server.
- Collector - From the drop-down list, select the required Collector.

Important: Once you have configured a Collector to interface with a specific Probe, you must use that Collector with the same Probe. This means that if you have already configured a Collector to interface with the selected Probe while adding a monitored file server, you must either select the same Collector, a Collector that is not yet connected to a Probe, or <No Collector>. If no Collector is used with the Probe server, select <No Collector>.

d. FileWalk Credentials - File System operations include the directory crawl (FileWalk), event collection (if set) and user crawl (ADWalk) on local accounts (if set).

- User name - Type the name of the user account to be used for FileWalk, event collection and local ADWalk.
- Password - Type the account's password.

Note: These credentials must be standard Windows-style credentials (domain\user).

- Add this user account to the Filtered Users list - This is the default user account for Data Security Platform operations. If you clear this checkbox, a large number of events generated by the Data Security Platform will be collected.

e. Varonis Agent Installation

- Do not install or upgrade the filter agent on this server - Select this checkbox if you do not want the Varonis filter agent automatically installed or upgraded on the file server.
- Click the Agent Deployment link to define the credentials used to install the agent on the file server. The Agent Deployment Options window is displayed.
 - Agent Installation Credentials
 - User name - Type the agent installation account's user name.
 - Password - Type the agent installation account's password.
 - Physical Machines - Settings for adding load-balancing cluster or redundant failover
 - Server - Type or browse to the cluster's physical node name and click Add.

3. To select specific shares for the file server, on the left menu, click Shares and do the following:

- a. In the Available Mounts area, select the required mounts and then click .

The selected mounts are moved to the Registered Mounts area.

- b. In the Ignore Detection column, select the mounts to be ignored (and not be the subject of notifications) by the resource monitor. Note the following scenarios:

- Mounts manually moved from registered mounts to available mounts should be selected.
- When users manually add mounts from available shares to registered mounts, the checkbox must be cleared.

- c. For each share, review and set the following information as required:

- Share Name - The name of the share.
- Path - The path on which the share resides.
- Protocol - The protocol defined for the share.

Note: The Varonis FileWalk method uses the SSH protocol for this purpose.

- Events - Select this checkbox to collect events for the share.
- Crawl - Select NTFS & NFS.
- Mixed Security - In mixed NT-Unix environments, indicates the default ACL extraction.

- d. In the Automatic Detection area, set the following:

- Automatically detect shares - DatAdvantage detects shares that reside at the highest level of the hierarchy and that are not already monitored. It gives preference to administrative shares over equivalent regular shares. From the drop-down list, select the relevant option:
 - Never - Select to instruct DatAdvantage not to detect shares or mounts automatically.
 - Detect and notify - Select to send users email that lists all newly detected shares or mounts. Unreachable shares and mounts are removed from DatAdvantage.
 - Detect and monitor - Select to add the newly detected shares or mounts to the Registered Shares or Registered Mounts list in the dialog box, with the Events column checked and the Crawl column set to enable crawling. Unreachable shares and mounts are removed from DatAdvantage.
 - Detect, monitor and notify - Select to add the newly detected shares or mounts as described above, and send users email listing them. Unreachable shares and mounts are (removed from DatAdvantage.

Note: Via the monitor selections, it is possible to add all the top-level shares per protocol (type) automatically as monitoring shares (for example, it is possible to add a 1st level share in CIFS protocol and 2nd level share in MIX mode/ Unix mode). To remove a specific share from the monitoring shares list, move manually the required share from Register Shares to Available Shares, and select Ignore Detection to ensure the resource manager will not add this share automatically to the monitoring shares (relevant for NetApp only).

Note: Shares using “mixed mode” are not supported.

- Notify - From the drop-down list, select the frequency at which to send notification of new shares or mounts. Options are:
 - Always - Select to send a cumulative list of all changes made (such as detection or deletion) to all shares and mounts.
 - Once - Select to send notification of a change (that is, detection or deletion) to a share or mount only when that change occurs.
- Remove Deleted Shares - Select this checkbox to remove deleted shares. Shares that were deleted from the file server will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the file server is unavailable, the shares will not be removed.
- Enable Event Collection - Select this checkbox to collect events from all shares added from this volume/file server.

4. On the left menu, click Configuration and set the following parameters:

- Unix Domain
 - Select the affiliated Unix user repository for this file server or Samba domain - From the drop-down 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.

- File Server General Settings
 - Save file server properties history - Select this checkbox if you want DatAdvantage to monitor the changes in folder properties (size, number of nested folders, number of files, and number of nested files).

Note: Over a long period of time this data may use a large amount of storage on the database.

- Shadow Database Installation - Credentials for installing the Shadow database on the SQL server. The user must have the sysadmin role on the selected SQL server.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- Database Server - Type or browse for the machine on which the Shadow database server resides.
- Authentication - Select the required type of authentication, SQL or Windows.
- User name - Type the account's user name.
- Password - Type the account's password.
- Save credentials - Select this checkbox to save the database credentials.
- Custom database location - Click this link to set the location of data files.
- SQL Host Server Credentials - Installation credentials for the machine on which the Shadow server resides. This account must be a member of the Local Administrators group on the machine during installation. The credentials are required only when the Shadow server does not reside on the DSP Server machine.

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- User name - Type the installation account's user name.
- Password - Type the installation account's password.
- POSIX Access Control List
 - Enable collection and management of POSIX ACLs - Select this option as relevant for Unix flavors that support POSIX ACLs.

5. Click Install.

The file server is installed.

[Adding Scality RING File Servers for Identical Connectors](#)

Adding Scality RING File Servers for Identical Connectors

There are additional prerequisites for identical CIFS connectors.

In addition to other [prerequisites](#), identical CIFS connectors must have:

- The same SID-to-UID mapping (related to the Samba configuration file)
- The same volumes, mounted on the same physical path (defined in: `/run/scality/connectors/<connector name>/config/transport/mountpoint`)
- The same device ID (`stat -c '%d' <mount path>`)
- Same Samba shares (related to the Samba configuration file)
- Same FileWalk user with the same password

To add Scality RING file servers for identical connectors:

1. Add a new file server. In the Management Console or in the Enterprise Installer, navigate to the Monitored File Servers page and click Add. The Resource Wizard is opened.
2. On the left menu, click Common. The Common settings are displayed.
3. In the Resource/Server Name field, add the name of one of the connectors.
4. In the FileWalk Details area, add the FileWalk credentials.
5. In the Resource Type area, click the Detect resource type link. Ensure that the type is detected as Unix SMB.
6. In the Varonis Agent Installation area, click the Agent Deployment link and add all the CIFS connectors as physical machines.
7. Complete the installation process (install the agent on all the connectors).

Important: Make sure to choose NTFS & NFS as the crawling method for all the shares.

To add a Scality RING file server, add each connector as a different file server:

1. Do one of the following:

- In the Enterprise Installer, navigate to the Monitored File Servers page and click Add.
- 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.

2. On the left menu, click Common and set the following parameters:

a. Resource Type

- Detected resource type - - Indicates the file server type, if it was automatically detected.
- Detect resource type - Click this link to detect the type of file server you selected. (If you used the Browse button to locate the file server's name, its type is detected automatically as long as you have already entered credentials.)
- Select resource type - If you select a file server's type from this drop-down list, this is the type that is used no matter what type was detected earlier.

Note: If you typed the file server's name manually, you must enter the FileWalk credentials before you can use the Detect link, due to permission requirements. If the type still cannot be detected, use the override field.

b. Resource Details

- Resource/Server Name - Type the name of one of the connectors.

c.

- Probe - From the drop-down list, select the Probe to be used with the file server.
- - From the drop-down list, select the required Collector.

Important: Once you have configured a Collector to interface with a specific Probe, you must use that Collector with the same Probe. This means that if you have already configured a Collector to interface with the selected Probe while adding a monitored file server, you must either select the same Collector, a Collector that is not yet connected to a Probe, or <No Collector>. If no Collector is used with the Probe server, select <No Collector>.

d. FileWalk Credentials - File System operations include the directory crawl (FileWalk), event collection (if set) and user crawl (ADWalk) on local accounts (if set).

- User name - Type the name of the user account to be used for FileWalk, event collection and local ADWalk.
- Password - Type the account's password.

Note: These credentials must be standard Windows-style credentials (domain\user).

- Add this user account to the Filtered Users list - This is the default user account for Data Security Platform operations. If you clear this checkbox, a large number of events generated by the Data Security Platform will be collected.

e. Varonis Agent Installation

- Do not install or upgrade the filter agent on this server - Select this checkbox if you do not want the Varonis filter agent automatically installed or upgraded on the file server.
- Click the Agent Deployment link to define the credentials used to install the agent on the file server. The Agent Deployment Options window is displayed.
 - Agent Installation Credentials
 - User name - Type the agent installation account's user name.
 - Password - Type the agent installation account's password.
 - Physical Machines - Add all the CIFS connectors as physical machines.
 - Server - Enter the name of a CIFS connector and click Add. Repeat to enter the remaining CIFS connectors.

3. To select specific shares for the file server, on the left menu, click Shares and do the following:

a. In the Available Mounts area, select the required mounts and then click the down arrow .

The selected mounts are moved to the Registered Mounts area.

b. In the Ignore Detection column, select the mounts to be ignored (and not be the subject of notifications) by the resource monitor. Note the following scenarios:

- Mounts manually moved from registered mounts to available mounts should be selected.
- When users manually add mounts from available shares to registered mounts, the checkbox must be cleared.

c. For each share, review and set the following information as required:

- Share Name - The name of the share.
- Path - The path on which the share resides.
- Protocol - The protocol defined for the share.

Note: The Varonis FileWalk method uses the SSH protocol for this purpose.

- Events - Select this checkbox to collect events for the share.
- Crawl - Select NTFS & NFS.
- Mixed Security - In mixed NT-Unix environments, indicates the default ACL extraction.

d. In the Automatic Detection area, set the following:

- Automatically detect shares - DatAdvantage detects shares that reside at the highest level of the hierarchy and that are not already monitored. It gives preference to administrative shares over equivalent regular shares. From the drop-down list, select the relevant option:
 - Never - Select to instruct DatAdvantage not to detect shares or mounts automatically.
 - Detect and notify - Select to send users email that lists all newly detected shares or mounts. Unreachable shares and mounts are removed from DatAdvantage.
 - Detect and monitor - Select to add the newly detected shares or mounts to the Registered Shares or Registered Mounts list in the dialog box, with the Events column checked and the Crawl column set to enable crawling. Unreachable shares and mounts are removed from DatAdvantage.
 - Detect, monitor and notify - Select to add the newly detected shares or mounts as described above, and send users email listing them. Unreachable shares and mounts are (removed from DatAdvantage).

Note: Via the monitor selections, it is possible to add all the top-level shares per protocol (type) automatically as monitoring shares (for example, it is possible to add a 1st level share in CIFS protocol and 2nd level share in MIX mode/ Unix mode). To remove a specific share from the monitoring shares list, move manually the required share from Register Shares to Available Shares, and select Ignore Detection to ensure the resource manager will not add this share automatically to the monitoring shares (relevant for NetApp only).

Note: Shares using “mixed mode” are not supported.

- Notify - From the drop-down list, select the frequency at which to send notification of new shares or mounts. Options are:
 - Always - Select to send a cumulative list of all changes made (such as detection or deletion) to all shares and mounts.
 - Once - Select to send notification of a change (that is, detection or deletion) to a share or mount only when that change occurs.
- Remove Deleted Shares - Select this checkbox to remove deleted shares. Shares that were deleted from the file server will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the file server is unavailable, the shares will not be removed.
- Enable Event Collection - Select this checkbox to collect events from all shares added from this volume/file server.

4. On the left menu, click Configuration and set the following parameters:

- Unix Domain
 - Select the affiliated Unix user repository for this file server or Samba domain - From the drop-down 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.

- File Server General Settings
 - Save file server properties history - Select this checkbox if you want DatAdvantage to monitor the changes in folder properties (size, number of nested folders, number of files, and number of nested files).

Note: Over a long period of time this data may use a large amount of storage on the database.

- Shadow Database Installation - Credentials for installing the Shadow database on the SQL server. The user must have the sysadmin role on the selected SQL server.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- Database Server - Type or browse for the machine on which the Shadow database server resides.
- Authentication - Select the required type of authentication, SQL or Windows.
- User name - Type the account's user name.
- Password - Type the account's password.

- Save credentials - Select this checkbox to save the database credentials.
- Custom database location - Click this link to set the location of data files.
- SQL Host Server Credentials - Installation credentials for the machine on which the Shadow server resides. This account must be a member of the Local Administrators group on the machine during installation. The credentials are required only when the Shadow server does not reside on the DSP Server machine.

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- User name - Type the installation account's user name.
- Password - Type the installation account's password.
- POSIX Access Control List
 - Enable collection and management of POSIX ACLs - Select this option as relevant for Unix flavors that support POSIX ACLs.

5. Click Install.

The file server is installed.

Adding Dell Fluid File Systems

You can install Dell Fluid file systems and set the parameters for data collection, file servers, and shares.

To add a Dell Fluid file system:

1. Do one of the following:

- In the Enterprise Installer, navigate to the Monitored File Servers page and click Add.
- 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.

2. On the left menu, click Common and set the following parameters:

a. Resource Type

- Detected resource type - Indicates the file server type, if it was automatically detected.
- Detect resource type - Click this link to detect the type of file server you selected. (If you used the Browse button to locate the file server's name, its type is detected automatically as long as you have already entered credentials.)
- Select resource type - If you select a file server's type from this drop-down list, this is the type that is used no matter what type was detected earlier.

Note: If you typed the file server's name manually, you must enter the FileWalk credentials before you can use the Detect link, due to permission requirements. If the type still cannot be detected, use the override field.

b. Resource Details

- Resource/Server Name - Type the resolved name or IP address of the file server to be added, or click the Browse button to locate it.
- Cluster ID - To find the cluster ID, run the `Get-DellFluidFsCluster` cmdlet from the FluidFS domain controller and look for the relevant ClusterID value. This value can also be found in the FluidFS GUI and in the FluidFS CLI by running the following command: `CLI/Maintenance> view-cluster-id`.

c. Data Collection Details

- Probe - From the drop-down list, select the Probe to be used with the file server.
- Collector - From the drop-down list, select the required Collector.

Important: Once you have configured a Collector to interface with a specific Probe, you must use that Collector with the same Probe. This means that if you have already configured a Collector to interface with the selected Probe while adding a monitored file server, you must either select the same Collector, a Collector that is not yet connected to a Probe, or <No Collector>. If no Collector is used with the Probe server, select <No Collector>.

d. FileWalk Credentials - File System operations include the directory crawl (FileWalk), event collection (if set) and user crawl (ADWalk) on local accounts (if set).

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

- - Type the name of the user account to be used for FileWalk, event collection and local ADWalk.
- - Type the account's password.
- Add this user account to the Filtered Users list - This is the default user account for Data Security Platform operations. If you clear this checkbox, a large number of events generated by the Data Security Platform will be collected.

3. To select specific shares for the file server, on the left menu, click Shares and do the following:

a. In the Available Shares area, select the required shares and click the down arrow .

The selected shares are moved to the Registered Shares area.

b. In the Ignore Detection column, select the shares to be ignored (and not be the subject of notifications) by the resource monitor. Note the following scenarios:

- Shares manually moved from registered shares to available shares should be selected.
- When users manually add shares from available shares to registered shares, the checkbox must be cleared.

c. For each share, review and set the following information as required:

Note: If the file server is installed only for use with DataPrivilege, event collection is disabled.

- Share Name - The name of the share.
- Path - The path on which the share resides.
- Protocol - The protocol defined for the share.
- Events - Select this checkbox to collect 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 collection and crawling.

- Mixed Security - In Windows environments, NT ACL extraction is always used.

d. In the Automatic Detection area, set the following:

- Automatically detect shares - DatAdvantage detects shares that reside at the highest level of the hierarchy and that are not already monitored. It gives preference to administrative shares over equivalent regular shares. From the drop-down list, select the relevant option:
 - Never - Select to instruct DatAdvantage not to detect shares or mounts automatically.
 - Detect and notify - Select to send users email that lists all newly detected shares or mounts. Unreachable shares and mounts are removed from DatAdvantage.
 - Detect and monitor - Select to add the newly detected shares or mounts to the Registered Shares or Registered Mounts list in the dialog box, with the Events column checked and the Crawl column set to enable crawling. Unreachable shares and mounts are removed from DatAdvantage.
 - Detect, monitor and notify - Select to add the newly detected shares or mounts as described above, and send users email listing them. Unreachable shares and mounts are (removed from DatAdvantage).

Note: Via the monitor selections, it is possible to add all the top-level shares per protocol (type) automatically as monitoring shares (for example, it is possible to add a 1st level share in CIFS protocol and 2nd level share in MIX mode/ Unix mode). To remove a specific share from the monitoring shares list, move manually the required share from Register Shares to Available Shares, and select Ignore Detection to ensure the resource manager will not add this share automatically to the monitoring shares (relevant for NetApp only).

Note: Shares using “mixed mode” are not supported.

- Notify - From the drop-down list, select the frequency at which to send notification of new shares or mounts. Options are:
 - Always - Select to send a cumulative list of all changes made (such as detection or deletion) to all shares and mounts.
 - Once - Select to send notification of a change (that is, detection or deletion) to a share or mount only when that change occurs.
 - Remove Deleted Shares - Select this checkbox to remove deleted shares. Shares that were deleted from the file server will be displayed with a strikethrough red font. They will not be removed from the “Registered” list. If the file server is unavailable, the shares will not be removed.
 - Enable Event Collection - Select this checkbox to collect events from all shares added from this volume/file server.
4. On the left menu, click Configuration and set the following parameters:
- Unix Domain
 - Select the affiliated Unix user repository for this file server or Samba domain - From the drop-down 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.

- File Server General Settings
 - Save file server properties history - Select this checkbox if you want DatAdvantage to monitor the changes in folder properties (size, number of nested folders, number of files, and number of nested files).

Note: Over a long period of time this data may use a large amount of storage on the database.

- Shadow Database Installation - Credentials for installing the Shadow database on the SQL server. The user must have the sysadmin role on the selected SQL server.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- Database Server - Type or browse for the machine on which the Shadow database server resides.
- Authentication - Select the required type of authentication, SQL or Windows.
- User name - Type the account's user name.
- Password - Type the account's password.
- Save credentials - Select this checkbox to save the database credentials.
- Custom database location - Click this link to set the location of data files.
- SQL Host Server Credentials - Installation credentials for the machine on which the Shadow server resides. This account must be a member of the Local Administrators group on the machine during installation. The credentials are required only when the Shadow server does not reside on the DSP Server machine.

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- User name - Type the installation account's user name.

- Password - Type the installation account's password.
 - FileWalk Settings
 - Identify actual unique folders and file system inconsistencies - Select this checkbox to detect broken permissions in NTFS file systems.
 - Run FileWalk in incremental mode (hourly) - Select this checkbox to run incremental FileWalk once an hour. Incremental FileWalk runs only on folders in which events occurred. It is only supported for file servers on which all the monitored shares (CIFS and NFS) provide resolved events, with full path location information.
 - Security Policy
 - Enable monitoring - Select the monitoring option from the drop-down list, NT or Unix. When this option is changed, volumes are automatically rescanned.
 - Default for mixed security - Select an option from the drop-down list, NT, Unix, Disabled, or PermissionDisabled.
 - NFS Commit - The definitions in this section enable performing commit on NFS (for Unix, Dell, NetApp, HPE 3PAR File Persona, or HP-NAS). To maintain security, the commit process must be activated through a gateway. The gateway can be any Unix machine that has access to the NFS exports on the file server and that is accessible via SSH. The gateway need only be defined for file servers on which NFS commit is available.
 - Gateway - Type the IP address of the Unix machine that acts as the gateway.
 - Via mount pattern - Type the required pattern. Can be:
 - Host name pattern - For example, CELERRA10:/*
 - IP address pattern - For example, 10.10.10.160:/*
The asterisk (*) indicates multiple mounts on the same machine, with different exports.
5. To configure the commit credentials to allow users to use different commit credentials than the configured FileWalk credentials, on the left menu, click Commit and set the following parameters:
- File Server Commit Credentials - Set the credentials to be used for committing DataPrivilege changes on the file server. The account used must have Backup Operator and Power User privileges. It must also be a member of the Administrators local machine group (for Windows or NAS devices), or a member of the Site Collection Administrators group (for SharePoint).

Note: In all commit operations on a NetApp CM file server, the user who executes the operation must be a CIFS superuser.

- Clear the Use FileWalk credentials checkbox to use different commit credentials than those defined for the FileWalk job. (By default, this checkbox is selected to use the FileWalk credentials, and the User name and Password fields are disabled for editing.)
- In the User name and Password fields, enter the relevant user name and password.
- Group OU - Select the organizational unit in which DataPrivilege creates groups. Groups created by DataPrivilege reside in the default base OU, unless otherwise specified.
 - Inherited from domain - By default, this option is selected to use the domain's default OU.
 - Uniquely defined - Select this option to choose a different OU from those defined in the file server's domain.
 - OU - Click the Browse button (...) to select the required OU.

6. Click Install.

The file server is installed.

Adding a New Edge Data Resource

You can add a new Edge data resource for a specific device.

A separate Edge data resource 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 Edge data resource.

Note: In the Enterprise Installer and Management Console, the term file server may be used to describe an Edge source device, even if it is not actually a file server.

To add a new Edge data resource:

1. Do one of the following:

- In the Enterprise Installer, navigate to the Monitored File Servers page, and click Add.
- 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.

2. On the left menu, click Common, and set the following parameters:

a. Specify the resource:

- i. In the Resource Details area, enter the name of the monitored resource. For example, North America Office VPN.
- ii. In the Resource Type area at the bottom, select VPN, Proxy, or DNS from the drop-down list.

b. In the Data Collection Details area, from the Collector drop-down list, select a Collector which is configured to support Edge.

3. On the left menu, click Configuration, and set the following parameters:

- File Server General Settings - The Save File Server Properties History checkbox is cleared by default. Leave as is.
- Shadow Database Installation - Enter the credentials for installing the Shadow database on the SQL server. The user must have the sysadmin role on the selected SQL Server.

Note: This area is only displayed when the data resource is initially installed; it is not displayed during subsequent editing.

- Database Server - Enter or browse for the computer on which the Shadow database server resides.
- Authentication - Select the required type of authentication, either SQL or Windows authentication.
- User name - Enter the account's user name.
- Password - Enter the account's password.
- Save credentials - Select this checkbox to save the database credentials.
- Custom database location - Click this link to set the custom location of the data files.
- SQL Host Server Credentials - Installation credentials for the machine on which the Shadow server resides. This account must be a member of the Local Administrators group on the computer during installation. The credentials are required only when the Shadow server does not reside on the DSP computer.

Note: This area is only displayed when the data resource is initially added. It is not displayed during subsequent editing.

- User name - Enter the installation account's user name.

- Password - Enter the installation account's password.
- Source Device
 - Product - Select the relevant vendor product from the drop-down list. The options vary according to the resource type selected in the Common pane.
 - 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 Edge data resource to use Filebeat or NXLog, it is not necessary to configure the time zone.

- 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.
- Auto-detect the date and 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 Edge 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 and 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..
- Interface Configuration - Specify the interface that Edge will use to collect events from the source device. Options are: Splunk, Syslog, and Filebeat. The additional parameters to configure vary according to the selected option:
 - To use Splunk to collect events, see Configuring a New Edge Data Resource to Use Splunk.
 - To use Syslog to collect events directly from the source device, see Configuring a New Edge Data Resource to Use Syslog.
 - To use Filebeat to collect events from the source device, see Configuring a New Edge Data Resource to Use Filebeat.

Note:

For more information on configuring the source devices to send events to Edge, see the relevant sections:

- Configuring VPN Sources to Send Events to Edge

- Configuring Web Proxy Sources to Send Events to Edge
- Configuring DNS Sources to Send Events to Edge

4. When you have completed all the required configurations, click Install.
The Edge data resource is installed.

Adding a Box Security Events File System

You can install a Box Security Events file system and set the parameters for data collection, file server, and configuration.

To add a Box Security Events file system:

1. Do one of the following:
 - In the Enterprise Installer, navigate to the Monitored File Servers page and click Add.
 - 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.

2. On the left menu, click Common and set the following parameters:
 - a. Specify the resource:

- i. In the Resource Details area, enter a name for the Box Security Events file system. For example, box-varonis.

Note: Make sure that the name is meaningful, since it will be displayed across the relevant Varonis products, such as analytics, reports, alerts, and so on.

- ii. In the Resource Type area at the bottom, select Box from the drop-down list. Note that this selection disables the FileWalk Credentials area.
The RSA key pair file field is added at the bottom.

- b. In the Data Collection Details area:

- i. From the Probe drop-down list, select the Probe to be used with the file server.

- ii. From the Collector drop-down list, select the required Collector.

Important: Once you have configured a Collector to interface with a specific Probe, you must use that Collector with the same Probe. This means that if you have already configured a Collector to interface with the selected Probe while adding a monitored file server, you must either select the same Collector, a Collector that is not yet connected to a Probe, or <No Collector>. If no Collector is used with the Probe server, select <No Collector>.

- 3. On the left menu, click Configuration and set the following parameters:

- Shadow Database Installation - Credentials for installing the Shadow database on the SQL Server. The user must have the sysadmin role on the selected SQL server.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- Database Server - Type or browse for the machine on which the Shadow database server resides.
- Authentication - Select the required type of authentication, either SQL or Windows authentication.
- User name - Type the account's user name.
- Password - Type the account's password.
- Save credentials - Select this checkbox to save the database credentials.
- Custom database location - Click this link to set the location of data files.
- SQL Host Server Credentials - Installation credentials for the machine on which the Shadow server resides. This account must be a member of the Local Administrators group on the machine during installation. The credentials are required only when the Shadow server does not reside on the DSP Server machine.

Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.

Note: This area is only displayed when the file server is initially installed. It is not displayed during subsequent editing.

- User name - Type the installation account's user name.
- Password - Type the installation account's password.

4. Click Install.

The file server is installed.

Adding Shares, Mounts, Exchange Domains, or SharePoint Sites

You can add shares, mounts, Exchange domains or SharePoint sites as needed.

To add shares, mounts, Exchange domains or SharePoint sites:

1. Do one of the following:

- In the Enterprise Installer, navigate to the Monitored File Servers page.
- In the Management Console, select Management > Components > Root > File Servers, and select the File Servers tab.

2. In the File Servers grid, select the row of the file server to which you want to add an item.

3. On the toolbar, click the Add button for the type of item you want to add (the name of the toolbar changes to reflect the type of resource you are working with: Shares, Mounts, Domains, or Sites).

The Editing File Server window is displayed.

4. Edit the item according to the instructions for the relevant resource.

Rescanning Shares

You can rescan shares in order to refresh them.

To rescan shares:

1. Do one of the following:

- In the Enterprise Installer, navigate to the Monitored File Servers page.
- In the Management Console, select Management > Components > Root > File Servers, and select the File Servers tab.

2. In the File Servers grid, select the row of the file server on which the relevant shares are located.
3. On the toolbar, click the relevant Rescan button (Rescan Shares, Rescan Mounts or Rescan Exports) to refresh the share.

Changes in the existing list are color-coded as follows:

- Red - The share was removed.
- Green - The share was added.

Editing File Servers

You can edit defined file servers.

To edit a file server:

1. Do one of the following:
 - In the Enterprise Installer, navigate to the Monitored File Servers page.
 - In the Management Console, select Management > Components > Root > File Servers, and select the File Servers tab.
2. In the File Servers grid, do one of the following:
 - Double-click the file server you want to edit.
 - Select the file server you want to edit, and on the Resources toolbar, click Edit.

The Editing File Server window is displayed.
3. Edit according to instructions provided in the relevant file server topics in this installation guide.
4. In the File Servers grid in the Monitored File Servers page, in the grid, you can set the following parameters for file servers and volumes:
 - For file servers:
 - Collect Events - Select the checkbox to collect events for the file server.
 - A non-monitored file server does not collect events. Its directory structure is updated according to the Crawl definitions for the shares, but the services (for Windows, SharePoint and Unix file servers) are not upgraded during future upgrades.

- For Unix flavors that do not support event collection, this checkbox is available but selecting it has no effect in the system.

Note: If the file server is installed only for use with DataPrivilege, event collection is disabled.

- Resource/Server Name - The name of the file server (read-only).
- Type - The file server type (read-only).
- IP Address - The file server IP address (read-only).
- Mixed Security - In mixed NT-Unix environments, indicates the default ACL extraction.
- Access Denied Events - Select the checkbox to collect events in which a user attempted to carry out an operation on a file or folder, but lacked sufficient permission to do so.

Note: The Data Security Platform does not identify access events which were denied due to lack of share permissions.

- Azure AD Tenant - The name of the Azure AD tenant.
- For shares, mounts, exports, domains, and sites:
 - Collect Events - Select the checkbox to collect events for the share.
 - Crawl - To enable or disable monitoring for the share, click the Crawl File System column and select the relevant option.
 - Path - The path on which the share resides.
 - Share Name - The name of the share.
 - Protocol - The protocol by which the entry point into the system is discovered.

Note: The Varonis FileWalk method uses the SSH protocol for this purpose.

- Mixed Security - In mixed NT-Unix environments, indicates the default ACL extraction.

5. To prevent updating the agent, if relevant for the selected data source type, select the Do not install or upgrade the filter agent on this server and Do not install/upgrade/remove the Varonis FileWalk agent checkboxes.

Removing Monitored Entities

When SharePoint volumes and file servers are removed, the volumes are also removed from the Domain table.

To remove a monitored entity:

1. Do one of the following:
 - In the Enterprise Installer, navigate to the Monitored File Servers page.
 - In the Management Console, select Management > Components > Root > File Servers, and select the File Servers tab.
2. In the File Servers grid, select the checkbox of the relevant entity, or select the entity's row.
3. On the Resources toolbar, click Remove.

Installing a DatAdvantage Windows File Server/Resource Agent

To perform a silent installation from an MSI:

Run the following from the command line:

```
msiexec /i <package.msi> SMTPSERVER=<host> SMTPFROM=<from> SMTPTO=<to> ADDLOCAL=<agent> /norestart /qb
```

Where:

- ADDLOCAL - A comma-separated list of the agents to be installed. Required parameter. Valid values:
 - WinAgent
 - ExchangeAgent
 - SharePointAgent

- SMTPSERVER - The name of the SMTP Server. Optional parameter.
- SMTPFROM - The address from which alerts are sent. Optional parameter.
- SMTPTO - The address from which alerts are sent. Optional parameter.

Installing File Servers in a Distributed Configuration

System administrators can install file servers in a distributed configuration.

To install file servers in a distributed configuration:

1. Do one of the following:
 - In the Enterprise Installer, navigate to the Monitored File Servers page.
 - In the Management Console, select Management > Components > Root > File Servers, and select the File Servers tab.
2. In the File Servers grid, select the relevant file server, and on the Resources toolbar, click Edit.
The Editing File Server window is displayed.
3. In the Distributed DB Configuration area, click Settings.
The Distributed File Server Configuration dialog box is displayed.
4. Select the Distributed file server installation option.
5. In the Available servers field, type the name of the required DSP Server instance or select it from the drop-down list. If the relevant server is not listed, click the Browse button to locate it.
6. In the Use SQL Server authentication area, set the SQL Server user name and password.

Note: The user must have system administrator privileges on the selected server.

7. Click Advanced Settings.
The Advanced Database Settings dialog box is displayed.

8. Set the following parameters as needed:

- SQL Server default location - Select to use the default location of the SQL Server as the location for the data files.
- Custom - Select to define a customized location for the data files. Click the Browse button to select the required location.

9. Click OK.

Moving File Servers from One Probe to Another

You can move file servers from one Probe to another as needed.

To move a file server from one Probe to another:

1. Do one of the following:

- In the Enterprise Installer, navigate to the Monitored File Servers page.
- In the Management Console, select Management > Components > Root > File Servers, and select the File Servers tab.

2. In the File Servers grid, select the file server to be moved, and on the Resource toolbar, click Edit.

3. In the Editing File Server window, select the new Probe from the Probe drop-down list.

4. Click OK.

Partitioning Database Tables

You can partition databases when using Microsoft SQL 2014 Enterprise Edition and above, or SQL 2016 SP1 Standard Edition and above.

Activation

After a clean installation, before any job is run: set `UsePartitionedTable=1` in the local `dbo.keyvalue` table.

Configuration

- Table types are defined in `Hist__ArchTypes`.
- All partitions and detached tables from partition tables are listed in `Hist__Archive`.
- The maximum number of partitions per table is defined in `MaxPartitionsInTable` in `vrnsDomainDB.dbo.keyValue`. The maximum permitted number of partitions is 1000.

Finishing The Deployment

When the deployment is finished, you can return to the main menu, view an error log, or close the Enterprise Installer.

To finish the deployment:

Select the relevant option from the Installation Complete page:

- Return to Main Menu
- Show Error Log
- Close the Enterprise Installer; alternatively, click Finish.

Configuring The Search Button In The Users And Groups Pane

You can configure a Search button in the Users and Groups pane of DatAdvantage to perform manual searches implemented by clicking the button, instead of automatic searches that are activated by the auto-complete feature.

When a user types a few letters in the Look For field of the Users and Groups pane, DatAdvantage performs the search automatically. However, it is possible to configure a Search button that disables this auto-complete feature, such that the search is only performed after the button is clicked.

To configure the Search button in the Users and Groups pane:

- In `vrnsDomainDB`, set the `IsShowSearchButtonUG` key in the `KeyValue` table to 1.

Disabling Event Aggregation In Archiving

It is possible to prevent event aggregation in the Archiving job for Windows, NFS, and SharePoint.

By default, the Data Security Platform aggregates events to save disk space.

Keep in mind that disabling aggregation can result in up to 100% growth in disk space usage.

To disable event aggregation:

1. Ensure you are logged in with the `sa` account to enable synchronization with remote Probes.
2. For each file server on which you want to disable event aggregation, run the following commands:

```
Use [vrnsDomainDB]
Exec [spSetConf] 'AggregateEvents',#FilerID,0
Exec [spSyncProbeConfigurations] -1
```


5

INSTALLING DATADVANTAGE IF DATAPRIVILEGE IS ALREADY INSTALLED

Before beginning any installation or upgrade, it is strongly recommended to ensure the most updated Microsoft hotfixes and patches that suit your server versions are installed on each server.

Various steps are required for installing DatAdvantage if DataPrivilege is already installed.

Note: If you experience slow response times during installation, disable any personal firewall that is already installed on your machine.

Welcome And License Agreement

The Welcome and License Agreement pages of the wizard allow you to start the setup and review and accept the license agreement details.

To start the installation:

1. Run the Enterprise Installer.
The Welcome page is displayed.
2. Click Next.
The License Agreement page is displayed.
3. Select I agree.
4. Click Next.

Main Menu

You can use the Main Menu to select the required workflow.

To select the required workflow:

1. Complete the previous pages of the Enterprise Installer, until you reach the Main Menu.
2. Select the relevant option:

- Install - Select this option to install the required Data Security Platform products and services. You can use typical settings or customize the installation with more advanced configurations.
- Repair/Upgrade - Select this option to repair or upgrade your currently installed Varonis products.
- DataPrivilege Schema Converter - Select this option to convert the DataPrivilege metadata to the new database schema. This is relevant for migrating DataPrivilege from 6.0 to 6.3, and from 6.3 to 6.4.
- Configuration - Select this option to configure your currently installed Varonis products. You can maintain DB passwords and licenses.
- Uninstall - Select this option to remove DatAdvantage and/or DataPrivilege from your system.

3. Click Next.

Selecting The Required Product Or Service

You can select the Data Security Platform product or service you want to install, update or remove from the Product Selection page.

To select the required Varonis products:

1. Complete the previous pages of the Enterprise Installer, until you reach the Product Selection page.
2. Select the products and services you want to work with.

Important: To install DataPrivilege on a server cluster, you must select the Show advanced options checkbox in order to define the DataPrivilege Web application location.

3. Click Next.

Setting Existing Products

The Existing Products page allows you to set various parameters for existing Varonis products.

To set parameters for existing Varonis products:

1. Complete the previous pages of the Enterprise Installer, until you reach the Existing Products page.
2. Select whether DatAdvantage or DataPrivilege is currently installed.

3. If you selected Yes in the previous step, set the required parameters for the existing DSP database server:
 - Database server - Enter the name of the server on which the DSP database is installed.
 - Authentication - Select the type of authentication used with the database.
 - User name - Enter the name of the user having privileges to the database.
 - Password - Enter the user's password.
4. In DataPrivilege Regional Settings, select the language to be used for DataPrivilege.
5. Click Next.

Configuring Your License

During the installation process, you can configure product license registration, automatically or manually.

If you are migrating DSP Analytics, the License Configuration page is displayed.

To configure your license:

1. Complete the previous pages of the Enterprise Installer, until you reach the License Configuration page.
2. For automatic registration:
 - a. Type the following parameters:
 - Customer ID/email - Type the ID or the email of the customer at which the Data Security Platform is being installed.

Note: The customer ID is displayed together with the serial number you received from Varonis. The ID replaces the email as the customer identifier.

 - b. Click Register. The Varonis products and the platforms the license supports are listed at the bottom of the page.
 - c. Click Finish.
3. For manual registration (if a problem arises with the automatic process):
 - a. Type the following parameters:
 - Customer ID/email - Type the ID or the email of the customer at which the Data Security Platform is being installed.

Note: The customer ID is displayed together with the serial number you received from Varonis. The ID replaces the email as the customer identifier.

- Serial number - Type the product serial number, as supplied by Varonis upon purchase.
- b. To obtain a license key:
- i. Go to the Varonis Support Website: <https://support.varonis.com/>.
 - ii. On the Login page, enter your user credentials and click OK.

Note: If this is your first visit to the Varonis Support site, you must create a user account.

- iii. Select License > License Registration. The License Registration page is displayed.
 - iv. In the Enter serial field, enter your the Data Security Platform serial number.
 - v. Select one of the following options:
 - Enter unique ID - Enter your unique ID. Use this option if you have an existing DSP installation that is lower than version 5.5.
 - Enter token - Enter your registration token, available on the License Configuration page of the Enterprise Installer. Use this option if your DSP installation is version 5.5 or higher.
 - vi. Click OK. Your license key is generated and displayed at the bottom of the page, along with the details of your license.
 - vii. Copy this number into the License Key field on the License Configuration page.
- c. Click Register. The Next button is enabled.
- d. Click Next.

Helping To Improve The Data Security Platform

Enabling User Feedback

Note: This functionality is not currently supported. User feedback cannot be enabled.

Sharing Data Diagnostics

By automatically allowing your Data Security Platform logs to be sent to Varonis, you can help to improve the quality, reliability, and performance of the Varonis Data Security Platform.

When you participate in Varonis log data collection, the performance of your software will not be affected in any way, and you may end your participation at any time.

The log data collection enables Varonis to readily identify issues that may arise on customer sites with Varonis system configurations, work to fix them promptly, and provide fixes as needed (as patches or version integration). Varonis will also collect feature usage statistics for reports, rule filters, and so on, to better understand the product usage, and orient the roadmap in an optimal manner.

Note: All the collected data is anonymized before it is sent to Varonis.

Connection Requirements for Data Diagnostics

- Open Port 443 to the following URLs:
 - <https://authupload.varonis.net>
 - <https://azcusengstorage.blob.core.windows.net>
- Connect to the Proxy server - if the DSP Server does not have an internet connection, see [Configuring the Proxy Server for Data Diagnostics](#)

Varonis Will Collect the Following Information

- Information from your environment about Varonis software and configuration
- Varonis event logs, which might include the names of servers, folders, files, and users:
 - DSP
 - Probe
 - Collector
 - Proxy
 - Windows file server
 - Solr
- All Varonis' Operational Log files
- Errors in the Varonis Notifications table - all database logs
- Hardware information from Varonis servers:
 - CPU

- RAM
- Disk
- Failed jobs, during a specified time period
- Failed subscriptions
- Failed sessions (reports)
- Notifications about crashes
- Varonis service states
- License information
- Customer email addresses, as recorded in the license registration
- Statistical information:
 - Data Classification Engine/DatAlert/DatAlert Analytics counters - number of rules and hits per rule, number of alerts, and so on
 - DataPrivilege configuration
 - Automation Engine/Data Transport Engine counters and usage - Broken Permissions Repair, Global Access Groups Remediation, and data transport
 - Varonis Edge statistics:
 - Configuration
 - Vendors
 - Report statistics:
 - Filter usage
 - Template usage
 - UI audit information

Data Anonymization

The logs are saved to a specified location so that the data can be reviewed locally. The following data will be anonymized before it is sent to the OMS:

- Password/connection strings
- IP addresses
- SIDs
- Server names (if De-Anonymize is not selected)
- DC names
- Users that Varonis uses for crawling/work

Varonis Will Not Collect the Following Information

- Passwords
- File content

Varonis Retention Policy

- During collection – incoming data is kept for 90 days
- Official requests to delete all data can be submitted at any time via support tickets
- Opt-out – unless requested via support to delete immediately, data collection will stop upon opt-out and will be deleted within 90 days

Data Diagnostics Flow

1. The daily job is responsible for collecting the relevant data. It uses the credentials entered for the Advanced Configuration area of the Data Diagnostics page (as described in the following procedure, Enabling Data Diagnostics via the Installer). If credentials are missing, it used the local system.
2. The logs are saved to a specified location, so that the data can be reviewed locally.
3. Data is anonymized (locally).
4. All logs are transferred over a secure channel directly to Azure Blob storage.
5. A parser service (Azure) takes the data enrichment, converts it into a universal log format, and uploads it to Azure Log Analytics located in the United States.
6. Access to logs and statistical data is based on role-based access control. The data will be used only for investigation and product optimization.

Enabling Data Diagnostics via the Management Console

To enable data diagnostics via the Installer:

1. Complete the previous pages of the Enterprise Installer, until you reach the Data Diagnostics page.
2. In the Share Log Data area, select I agree to participate in log data collection in accordance with the Varonis Privacy Policy. (Clear this checkbox to decline participation.)

3. To remove anonymization on the server, select the De-anonymize Server Names checkbox. (This checkbox is cleared by default, to ensure that the data will be anonymized before it is sent to the OMS.)
4. To change the credentials used to collect the logs, in the Advanced Configuration area, set the following:
 - Log path - By default, logs are saved in the working directory on the DSP Server. To change the location at which logs are saved, enter the preferred path.
 - User name - Enter the name of the user account that has access to the log path.
 - Password - Enter that account's password.
5. Click Next. The Check Prerequisites dialog box is displayed, indicating the validation status of each prerequisite.

Configuring the Proxy Server for Data Diagnostics

To configure the proxy server for data diagnostics:

1. Go to the DSP Server installation location. By default, it is C:\Program Files (x86)\Varonis\DatAdvantage\DSP Server.
2. Go to the subfolder, Support Assistant\LogsUploader.
3. Open the `SPUpload.exe.config` file in Notepad. (You may need to open Notepad with "Run As Administrator" if User Account Control (UAC) is configured.)
4. Find the section named `<defaultProxy>` under `<system.net>`. For more information about this section, see [Microsoft Docs](#).
 - a. If the section is commented out, uncomment it.
 - b. If the section does not exist, add it (see the example provided at the end of this procedure).
5. 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"
```



```
    />  
  </defaultProxy>  
</system.net>
```

Configuring Reporting Services

The Reports component enables generation of Data Security Platform reports.

This page is only displayed if you selected the Reports checkbox in the Product Selection page.

If Reporting Services were configured during a previous installation, this page is read-only.

To prevent a security loophole in which all of the Data Security Platform data could be viewed by unauthorized persons, the Data Security Platform changes the authentication and authorization methods of the Reporting Services installation to its own methods. Therefore, other applications may have issues if installed in the same Reporting Services installation.

To configure reporting services:

1. Complete the previous pages of the Enterprise Installer, until you reach the Reporting Services Configuration page.
2. Configure the machine on which the reporting services will be installed:
 - Installation Credentials - Enter the installation account's credentials.
 - User name - Enter the installation account's user name.
 - Password - Enter the installation account's password.
 - Reporting Service Installation
 - Host name - Enter the name of the host on which the reporting service resides.
 - Instance - Select the database instance on which the reporting service resides.
 - Authentication - From the dropdown list, select the type of authentication to be used.
 - User name - Enter the user name of the reporting service's account.
 - Password - Enter the password of the reporting service's account.
 - Protocol - Select the required web interface protocol.
 - Port - Enter the number of the port to which the reporting service listens.
 - Report Configuration - Configure default report settings.

- Report CSV export path - Enter a local or UNC path to which the CSV file containing report results will be saved if the report exceeds the maximum rows to display.
- User name - If the export path is located on a share, enter the user name of an account having Read/Write permissions to the share.
- Password - Enter the account's password.
- Maximum rows to display in report - Set the maximum number of rows to be displayed in the report. If the report contains more rows than this number, the additional rows will not be displayed. Instead, a CSV file containing the full set of results will be created and saved to the designated export path.
- Number of rows to display in short preview - Set the number of rows to be displayed in the short preview.
- Number of executions saved in subscription history - Set the number of report executions to be saved in the subscription history. This setting controls the results of the Execution History button in DatAdvantage's My Subscriptions page.
- Web UI Scheduled Searches
 - Maximum email size (MB) - Set the maximum size (MB) of email that can be sent by a scheduled search in the web UI. If the email size exceeds this limit, the email will not be sent. The scheduled search settings in the web UI enable saving the output to a file share if the email exceeds the maximum size limit. It is recommended to set the email size limit according to your organization's policy.
- Template Ownership and Visibility
 - The Enterprise Manager can see all templates and subscriptions - Select this option as necessary.
 - Replace template and subscription owner - Click this link to replace the original owner with a new owner for all owned templates and/or subscriptions. Selecting an option that includes "templates" will affect the templates owned by the original owner in DatAdvantage and the saved searches in the Varonis Web UI. Selecting an option that includes "subscriptions" will affect the subscriptions owned by the original owner in DatAdvantage and the scheduled searches in the Varonis Web UI.
- Report Watcher
 - Limit reports disk usage on all servers to ___ GB - Select the relevant limit on disk usage. When the reporting service uses more than the specified disk space, report processes are stopped on the relevant server until the disk usage is less than the limit; an email notification is sent to the system administrator.

- Limit reports CPU time on all servers to ___ Minutes - Select the relevant limit for CPU time.
- Report Display Options - Configure the display options for all reports: title, subtitle, look and feel, etc.

Important: Applying these settings may take a long time, during which DatAdvantage will not be available.

- Select the custom logo for DatAdvantage
- Select the custom logo for DataPrivilege
- Advanced - Click this link to set the following display options in bulk:
 - Report Title - Click the pencil icons to set whether report names or template names are displayed for the report titles and subtitles.
 - Report Content - Click the pencil icons to set the following options:
 - Display logo in report
 - Display report filter
 - Display the description of the report template
 - Hide number of nested groups for grouped results
 - Report Formatting - Set the following formatting options:
 - Look and feel
 - Date Format - Applied to all templates
 - Time Format - Applied to all templates
 - Affected Report Templates - The changes set above are implemented in all the reports selected in this area. Options are:
 - User-defined report templates
 - Predefined report templates

3. Save your changes

Setting Server Credentials

The Security Configuration page allows you to set credentials and agent options for monitored file servers.

To set credentials and agent options for monitored file servers:

1. Complete the previous pages of the Enterprise Installer, until you reach the Security Configuration page.
2. If any server is lacking credentials, select the server and click Edit Credentials.

3. To prevent upgrading or removing any agents, select the following options as necessary in the Agent Options pane:

- SharePoint agent
- Varonis FileWalk agent

Note: The Data Security Platform supports data deduplication on Windows 2012 when both the CIFS and the Varonis FileWalk methods are in use. To enable use of the Varonis method, the agent needs to be upgraded.

- Directory Services proxy agents
- Other file server agents

4. Click Next.

Deploying The Current Tasks

You can deploy currently defined tasks.

To deploy the current tasks:

1. Complete the relevant pages of the Enterprise Installer, until you reach the Deployment Progress page.
2. Click Install.
The selected products and services are installed.
3. To continue defining resource and options with the Enterprise Installer, click Next.

Finishing The Deployment

When the deployment is finished, you can return to the main menu, view an error log, or close the Enterprise Installer.

To finish the deployment:

Select the relevant option from the Installation Complete page:

- Return to Main Menu
- Show Error Log
- Close the Enterprise Installer; alternatively, click Finish.

6

REPAIRING OR UPGRADING THE DATA SECURITY PLATFORM

You can run the Varonis Repair/Upgrade flow or the Report Deployment tool to repair and upgrade the Data Security Platform.

Before beginning any installation or upgrade, it is strongly recommended to ensure the most updated Microsoft hotfixes and patches that suit your server versions are installed on each server.

Welcome And License Agreement

The Welcome and License Agreement pages of the wizard allow you to start the setup and review and accept the license agreement details.

To start the installation:

1. Run the Enterprise Installer.
The Welcome page is displayed.
2. Click Next.
The License Agreement page is displayed.
3. Select I agree.
4. Click Next.

Main Menu

You can use the Main Menu to select the required workflow.

To select the required workflow:

1. Complete the previous pages of the Enterprise Installer, until you reach the Main Menu.
2. Select Repair/Upgrade to repair or upgrade a Data Security Platform product or service.
3. Click Next.

Selecting The DSP Server

The DSP Server Selection page allows you to select the DSP Server and set the required parameters.

To select the DSP Server:

1. Complete the previous pages of the Enterprise Installer, until you reach the DSP Server Selection page.
2. Set the following parameters:
 - Database Server - Type the name of the required DSP Server database instance or select it from the drop-down list. If the relevant server is not listed, click the Browse button to locate it.
 - Authentication - Select the required authentication type, which can be either Windows or SQL.
 - User name - Type the user name for the DSP database.
 - Password - Type the password.

Important: If you plan to select the Maintain Database Passwords flow and change the sa credentials used to access the DSP Server, you must enter the new credentials on this page of the wizard - even though you have not yet changed them. The credentials you enter here are stored, and appear on the Database Security Configuration page when you set the database credentials for the sa account.

3. Click Next.

Selecting The Required Product Or Service For Upgrade/Repair

The Product Selection page of the wizard allows you to select the Data Security Platform product or service you want to install, update, or remove.

To select the required Varonis products:

1. Complete the previous pages of the Enterprise Installer, until you reach the Product Selection page.
2. Select the product or service you want to work.

Note: To install the Data Classification Engine in an environment with existing Varonis products, first run the Repair/Upgrade flow and select Data Classification from the product list. Then, install the DCE from the Management Console.

Note: To download and use the (new) DatAdvantage GUI and the Varonis Web Interface, Solr must also be installed. Selecting the Install DatAdvantage GUI and Install Web UI checkboxes enables access to the Solr installation wizard.

3. Click Next.

Installing And Configuring The Varonis Web Server

You can install the Varonis Web Server through the Enterprise Installer or Management Console.

To install and configure the Varonis Web Server:

1. Do one of the following:

- In the Enterprise Installer, navigate to the Varonis Web Server page.

Note: The Varonis Web Server page is only displayed if you are installing the Varonis Web Interface.

- In the Management Console, select Management > Components > Root > DSP Server > Service Components, and from the toolbar in the DSP Server - Service Components pane on the right, select Varonis Web Server. The Varonis Web Server dialog box is displayed.

Note: To configure an already installed Varonis Web Server, from the menu in the left pane, under Service Components, select Varonis Web Server to display the Varonis Web Server pane on the right. Proceed to set the parameters in the General tab.

2. Set the following parameters:

- Installation Web Address
 - Host Name - A read-only field, displaying the name of the DSP Server on which the Varonis Web Server will be installed.
 - Protocol - From the drop-down list, select the required protocol for the Varonis Web Server. Options are:
 - HTTP
 - HTTPS
 - Certification Thumbprint - Enter the required certificate. This option is displayed only if HTTPS is selected from the Protocol drop-down list. The default certificate is Self-signed certificate.

- Relative Path - Type the name of the directory to be created upon installation. The default option is DatAdvantage.
- Port - From the drop-down list, select the access port number of the selected protocol (by default, 443 for HTTPS and 80 for HTTP).
- URL - Click the link to test the URL that is created from the other parameters.
- Installation Credentials - Enter the credentials to be used to install the component.
- Services Installation
 - Location - The location in which the Varonis Web Server is to be installed.
 - Services Port - From the drop-down list, select the required port number to which the Varonis Web Server listens. The default and recommended port is already displayed.
- Event in Solr (Available in Web Interface)
 - Store event data for the last x days - Specify the past number of days for which event data will be stored. The default is 30 days.

Note:

- If you require more than 30 days to store event data, ensure that you have sufficient hardware for the increased number of days. You can specify up to 180 days for the storage period. For the sizing guidelines, contact Varonis Support.
 - The Varonis Web Interface Events page supports only events that are available in Solr. Archived and restored events are not reflected in the Varonis Web Interface.
 - When flat data is stored, the event history of filtered users is not removed. The event history will be removed according to the configured retention policy (a period of up to 14 days).
- Estimated number of Edge events per day - Specify the estimated number of Varonis Edge events that will be stored.

3. Click Next and proceed to install and configure Solr and ZooKeeper.

Installing And Configuring Solr And ZooKeeper

To install the Varonis Web Server, you must also install Solr and ZooKeeper for event flattening.

To install and configure Solr and ZooKeeper:

Note: Ensure that you have reviewed the Solr/ZooKeeper prerequisites.

1. Do one of the following:

- In the Enterprise Installer, navigate to the Solr Events page, and on the toolbar, click Add. The Solr/ZooKeeper Wizard dialog box is displayed.
- In the Management Console, complete the previous page of the Varonis Web Server installation, until you reach the Solr/ZooKeeper Wizard page.

Note: To configure an already installed Solr or ZooKeeper host, in the Flattening tab of the Varonis Web Server pane, click Add to display the Solr/ZooKeeper Wizard dialog box.

2. Set the following parameters:

Important:

- Solr and ZooKeeper must be installed on a standalone server, separate from that of the Collector and DSP.
 - .NET Framework 4.72 must be installed on the server which Solr and ZooKeeper are installed.
 - Make sure to set the hostname of the dedicated machine, and to install Java JDK 8 on it. Java JDK 9 and higher are not supported.
 - The Solr and ZooKeeper hostnames cannot include underscores (_).
 - Solr and DatAnswers cannot be installed on the same DSP machine. If DatAnswers is installed on the DSP machine, you cannot install Solr on the DSP machine as well.
- Solr Host or ZooKeeper Host - Select the host, Solr or ZooKeeper.
 - Location
 - Server - The IP/name of the computer on which Solr or ZooKeeper will be installed.
 - Location - The location on which Solr will be deployed.
 - Data Location - The location on which Solr event collection will be created and saved. Make sure to set different folder locations for Solr and ZooKeeper.
 - Deployment Credentials
 - User name - The user name that will be used to install the selected host.
 - Password - The password of the selected host.

3. Click Add. The installed host is displayed in the table.

Note: Make sure to enter the host name and not an IP address in this field.

4. In the Common area, change the default ports as needed. In the Management Console, this is in the Varonis Web Server dialog box (Flattening tab).

Note: If Solr and DatAnswers are installed on the same computer, the Solr and ZooKeeper ports need to be changed to 8183 for Solr, and 2183 for the Client Communication port.

5. To install the second host (if Solr was installed, you must proceed to install ZooKeeper, and vice versa):
 - a. In the Varonis Web Server dialog box, click Add.
 - b. In the Solr/ZooKeeper Wizard dialog box, select the host that was not previously selected and repeat the previous steps in this procedure.

Note: Make sure to enter the host name and not an IP address in this field.

6. Do one of the following:
 - In the Enterprise Installer, click Next to continue the installation process.
 - In the Management Console, when Solr and ZooKeeper configuration is complete, click Finish.

Note:

- Upon the installation of Solr, events from the past seven days will be displayed in the Varonis Web Interface. This period will gradually increase until the configured flattening period.
- When flat data is stored, the event history of filtered users is not removed. The event history will be removed according to the configured retention policy (a period of up to 14 days).

Configuring The DSP Working Share

The DSP Working Share page allows you to configure Data Security Platform working share settings.

To configure the DSP working share:

1. Complete the previous pages of the Enterprise Installer, until you reach the DSP Working Share page.
2. In the Working Share Settings area, set the following parameters as needed:

- Working share - Select the Working share.
- Working directory - Enter the path name of the Working directory.
- User name - Enter the user name of the account used to access the share (Working share user).
- Password - Type the password of the account used to access the share (Working share user).

3. Click Next.

Setting Parameters For DatAlert Analytics Installation

The DatAlert Analytics page allows you to set the parameters for DatAlert Analytics installation.

To set the parameters for DatAlert Analytics installation:

1. Complete the previous pages of the Enterprise Installer, until you reach the DatAlert Analytics page.
2. Set the following:
 - Services Installation
 - Server - The server on which DatAlert Analytics is installed.
 - Location - The location on the server in which the DatAlert Analytics services are installed.
 - Installation Credentials
 - User name - The name of the account that performs the installation.
 - Password - That account's password.
 - Working Share Settings
 - Working share - Set the DatAlert Analytics working share.
 - Working directory - Set the DatAlert Analytics working directory, if different from the working share.
 - User name - Set the user account that has access to the working share.
 - Password - Set that account's password.
 - Services Configuration
 - Port - Set the port used by DatAlert Analytics.
 - Protocol - Set the protocol used by DatAlert Analytics.
 - URL - The URL of the web UI.
3. Click Next.

Upgrading Varonis Servers And Monitored File Servers

The Data Security Platform Configuration page allows you to upgrade Varonis servers, databases, and monitored file servers.

To upgrade Varonis servers, databases, and monitored file servers:

1. Complete the previous pages of the Enterprise Installer, until you reach the Data Security Platform Configuration page.
2. To find or update user credentials for each server, do the following:
 - a. To find a specific server, type the name of the server in the Search Server text box, and click Apply.
 - b. To find servers using a specific type of account credentials, select the required type from the Credentials type drop-down list, and click Apply.
 - c. To find servers for which there are no user credentials, select the Show only empty checkbox, and click Apply.

Note: You can combine any of the search methods to filter the list of servers.

Only servers that match your search criteria are displayed in the Server Name column.

3. To add or edit server credentials:
 - a. Select the server you want to edit, and click Edit Credentials.
 - b. In the Credentials dialog box, set the user name and password of the user account.
4. To clear credentials, select the required server, and click Clear Credentials.
5. To prevent upgrading or removing any agents, select the following options as necessary in the Agent Options pane:
 - SharePoint agent
 - Varonis FileWalk agent

Note: The Data Security Platform supports data deduplication on Windows 2012 when both the CIFS and the Varonis FileWalk methods are in use. To enable use of the Varonis method, the agent needs to be upgraded.

- Directory Services proxy agents
 - Other file server agents
6. Click Next.

Configuring Live Updates

The Live Update functionality enables you to automatically keep your Varonis Data Security Platform installation up to date with content, security updates, and bug fixes. You can choose whether to deploy the updates automatically or manually.

About Live Update

- Live Update is a service in the DSP Server; it uses the local system account.
- 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. A service restart might be required; a notification will be sent accordingly.
- 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.
- To receive email notifications for Live Update deployment updates, configure your email settings in the Management Console; go to Configuration > Mail Settings. For more information about the Live Update notification messages, see the Live Update Email Notifications section below.

Security

- All updates that are downloaded via Live Update are signed using cryptographic keys and verified by DatAdvantage. The update creation process for DatAdvantage prevents the injection of malicious code into these packages.

Limitations

- Some Live Update packages will require user intervention. An email notification will be sent informing that manual deployment is required.
- 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. Do one of the following:
 - In the Enterprise Installer, navigate to the Update Configuration page.
 - In the Management Console, from the menu in the left pane, select Configuration > DatAdvantage Updates. The Update Configuration page 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 Collector credentials.

Note: The user will be used to automatically deploy updates on all Collectors; therefore, the user must be a local administrator on all Collectors in the environment.

5. To configure the Web proxy server for Live Update:
 - a. Go to the DSP Server 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.config` 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"
    />
  </defaultProxy>
</system.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 registered in the Management Console > Configuration > Mail Settings.

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."

Live Update Security Measures

The Varonis Live Update component undergoes various security measures for protection.

About Live Update Protection

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.

Live Update Platform

The Live Update platform comprises the following:

- Live Update service hosted on the Azure cloud - Serves updates to Varonis customers who have the Live Update feature enabled
- Client-side component - Downloads the updates from the cloud to the application installed on the customer side

Technological Controls

Live Update Hosting Service

The Live Update server-side platform has multiple controls on the service including:

- Restricted access to updates of private APIs that are uploaded to the cloud – only specified employees can access the updates of private APIs and automated services that are uploaded to the cloud. Access is restricted from specific IP addresses within the organization; all access is monitored and alerted.

- The Public API access - is protected by a web application firewall (WAF) with profiles to prevent malicious attempts from tampering or attacking the service. The web application firewall also triggers alerts to the Security Operation Center on identified attacks.
- Updates are stored in a private cloud storage location. Access to the uploads for download is granted on the file level using a one-time token issued by the cloud API.
- Updates are hashed and signed prior to being permanently stored. The signature is verified prior to being installed.

Live Update Client Service

- The client-side application is an integral part of the Varonis Platform. The service component is installed with the application and is configurable, allowing users to enable or disable the auto-download and auto-install of the updates from the cloud service.
- The application sends its update level periodically, to identify whether there are new updates available. All Probes are sent over HTTPS to the public API of the Live Update service. When an update is identified, the client follows the configuration of the platform as to the expected behavior (see above).
- The client API verifies the certificate chain, as well as the certificate owner, thereby protecting the platform from man-in-the-middle attacks against the cloud service while working with the HTTPS endpoint.

Note: This functionality requires TLS offloading to be turned off for the Varonis Live Update domain: `liveupdate.varonis.com`.

- Every downloaded update is verified upon download with the file signature; this prevents attackers from tampering with the downloaded file.

Procedural Controls

Security and Functional Testing

- Live Update, as well as supporting services and infrastructure, undergo periodic penetration testing by a third-party security testing company. Component testing is performed in a standalone manner (on an individual basis) as well as per a whole-integrated solution. Findings undergo a triage process and are remediated.
- All updates uploaded to the Live update platform go through a series of testing phases and are deployed in a controlled rollout. The components and the code that make up the updates are managed in the central code repository.

- All software updates sent via Live Update are reviewed and undergo an approval process prior to their release.

Helping To Improve The Data Security Platform

Enabling User Feedback

Note: This functionality is not currently supported. User feedback cannot be enabled.

Sharing Data Diagnostics

By automatically allowing your Data Security Platform logs to be sent to Varonis, you can help to improve the quality, reliability, and performance of the Varonis Data Security Platform.

When you participate in Varonis log data collection, the performance of your software will not be affected in any way, and you may end your participation at any time.

The log data collection enables Varonis to readily identify issues that may arise on customer sites with Varonis system configurations, work to fix them promptly, and provide fixes as needed (as patches or version integration). Varonis will also collect feature usage statistics for reports, rule filters, and so on, to better understand the product usage, and orient the roadmap in an optimal manner.

Note: All the collected data is anonymized before it is sent to Varonis.

Connection Requirements for Data Diagnostics

- Open Port 443 to the following URLs:
 - <https://authupload.varonis.net>
 - <https://azcusengstorage.blob.core.windows.net>
- Connect to the Proxy server - if the DSP Server does not have an internet connection, see [Configuring the Proxy Server for Data Diagnostics](#)

Varonis Will Collect the Following Information

- Information from your environment about Varonis software and configuration
- Varonis event logs, which might include the names of servers, folders, files, and users:
 - DSP

- Probe
- Collector
 - Proxy
 - Windows file server
 - Solr
- All Varonis' Operational Log files
- Errors in the Varonis Notifications table - all database logs
- Hardware information from Varonis servers:
 - CPU
 - RAM
 - Disk
- Failed jobs, during a specified time period
- Failed subscriptions
- Failed sessions (reports)
- Notifications about crashes
- Varonis service states
- License information
- Customer email addresses, as recorded in the license registration
- Statistical information:
 - Data Classification Engine/DatAlert/DatAlert Analytics counters - number of rules and hits per rule, number of alerts, and so on
 - DataPrivilege configuration
 - Automation Engine/Data Transport Engine counters and usage - Broken Permissions Repair, Global Access Groups Remediation, and data transport
 - Varonis Edge statistics:
 - Configuration
 - Vendors
 - Report statistics:
 - Filter usage
 - Template usage
 - UI audit information

Data Anonymization

The logs are saved to a specified location so that the data can be reviewed locally.

The following data will be anonymized before it is sent to the OMS:

- Password/connection strings
- IP addresses
- SIDs
- Server names (if De-Anonymize is not selected)
- DC names
- Users that Varonis uses for crawling/work

Varonis Will Not Collect the Following Information

- Passwords
- File content

Varonis Retention Policy

- During collection – incoming data is kept for 90 days
- Official requests to delete all data can be submitted at any time via support tickets
- Opt-out – unless requested via support to delete immediately, data collection will stop upon opt-out and will be deleted within 90 days

Data Diagnostics Flow

1. The daily job is responsible for collecting the relevant data. It uses the credentials entered for the Advanced Configuration area of the Data Diagnostics page (as described in the following procedure, Enabling Data Diagnostics via the Installer). If credentials are missing, it used the local system.
2. The logs are saved to a specified location, so that the data can be reviewed locally.
3. Data is anonymized (locally).
4. All logs are transferred over a secure channel directly to Azure Blob storage.

5. A parser service (Azure) takes the data enrichment, converts it into a universal log format, and uploads it to Azure Log Analytics located in the United States.
6. Access to logs and statistical data is based on role-based access control. The data will be used only for investigation and product optimization.

Enabling Data Diagnostics via the Management Console

To enable data diagnostics via the Installer:

1. Complete the previous pages of the Enterprise Installer, until you reach the Data Diagnostics page.
2. In the Share Log Data area, select I agree to participate in log data collection in accordance with the Varonis Privacy Policy. (Clear this checkbox to decline participation.)
3. To remove anonymization on the server, select the De-anonymize Server Names checkbox. (This checkbox is cleared by default, to ensure that the data will be anonymized before it is sent to the OMS.)
4. To change the credentials used to collect the logs, in the Advanced Configuration area, set the following:
 - Log path - By default, logs are saved in the working directory on the DSP Server. To change the location at which logs are saved, enter the preferred path.
 - User name - Enter the name of the user account that has access to the log path.
 - Password - Enter that account's password.
5. Click Next. The Check Prerequisites dialog box is displayed, indicating the validation status of each prerequisite.

Configuring the Proxy Server for Data Diagnostics

To configure the proxy server for data diagnostics:

1. Go to the DSP Server installation location. By default, it is C:\Program Files (x86)\Varonis\DatAdvantage\DSP Server.
2. Go to the subfolder, Support Assistant\LogsUploader.
3. Open the `SPUpload.exe.config` file in Notepad. (You may need to open Notepad with "Run As Administrator" if User Account Control (UAC) is configured.)

4. Find the section named `<defaultProxy>` under `<system.net>`. For more information about this section, see [Microsoft Docs](#).
 - a. If the section is commented out, uncomment it.
 - b. If the section does not exist, add it (see the example provided at the end of this procedure).
5. 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"
    />
  </defaultProxy>
</system.net>
```

Upgrading Collectors

The Collector Upgrade page allows you to upgrade the Collectors and specify the required credentials.

To upgrade Collectors:

1. Complete the previous pages of the Enterprise Installer, until you reach the Collector Upgrade page.
2. If the Wrong credentials status is displayed for one or more of the Collectors, do the following:
 - a. In the Status column, click the relevant pencil icon. The Credentials dialog box is displayed.
 - b. In the Credentials dialog box, set the user name and password of the user account.
 - c. Click OK.
3. To continue deploying the currently defined tasks, click Next.

Decommissioning File Servers During Upgrade

You can decommission a file server that no longer exists.

When a file server is decommissioned, historical data is saved. Event collection and crawling are disabled for decommissioned file server.

To decommission file servers:

1. Complete the previous pages of the Enterprise Installer, until you reach the Set Servers as Decommissioned page.

Note: The following page appears only if event collection and crawling are disabled for one or more file servers. In addition, file servers that are already decommissioned are not displayed on this page.

2. Select the relevant file server to be decommissioned. You can select more than one file sever.
3. Click Next.

Deploying The Current Tasks

You can deploy currently defined tasks.

To deploy the current tasks:

1. Complete the relevant pages of the Enterprise Installer, until you reach the Deployment Progress page.
2. Click Install.
The selected products and services are installed.
3. To continue defining resource and options with the Enterprise Installer, click Next.

Finishing The Deployment

When the deployment is finished, you can return to the main menu, view an error log, or close the Enterprise Installer.

To finish the deployment:

Select the relevant option from the Installation Complete page:

- Return to Main Menu
- Show Error Log
- Close the Enterprise Installer; alternatively, click Finish.

Installing Or Upgrading The User Interface

The Select Installation Folder page allows you to install or upgrade the user interface.

To install or upgrade the UI:

1. Navigate to the GUI installation folder and double-click `setup.exe` to start the Enterprise Installer.
The Welcome page is displayed.
2. Click Next.
The License Agreement page is displayed.
3. To accept the agreement, select I agree and click Next. Otherwise, click Cancel.
The Select Installation Folder page is displayed.
4. On this page, set the following parameters:
 - a. Click the Browse button to select the folder in which to install the DatAdvantage UI.
 - b. Click Disk Cost to view available space and required space for each physical drive.
 - c. Select whether to install the DatAdvantage UI for yourself or for anyone who uses the computer.
5. Click Next.
The Confirm Installation page is displayed.
6. Click Next to begin the installation.
When it is finished, the Installation Complete page is displayed.
7. Click Close.
The UI Enterprise Installer exits.
8. Double-click the DatAdvantage icon on the desktop to start DatAdvantage.
9. Configure the required DSPs.

Repairing The User Interface

The Repair function allows you to repair problems that occur with the user interface.

To repair problems that occur with the UI:

1. Navigate to the GUI installation folder located and double-click `setup.exe` to start the Enterprise Installer. A page is displayed prompting you to repair or remove the installed application.
2. Click Repair.
3. Click Next.

The Ready to repair page is displayed.

4. Click Repair. The repair progress is displayed.

When it is finished, the Installation Complete page is displayed.

Enabling History Reports For Dates Prior To Upgrade

The history reports (reports 3e and 4k) can be generated out of the box on all data stored starting from the same version in which the history reports were first included.

To enable generating history reports for dates prior to upgrade:

Run the following script from `vrsnDomainDB`:

```
exec spUpgradeForReport41
```

7

SHAREPOINT ONLINE/ONEDRIVE ISSUES AFTER UPGRADING DATADVANTAGE

FileWalk and event collection are performed by an Azure application.

When adding a SharePoint Online/OneDrive file server, this application is created automatically. After upgrading DatAdvantage, it is necessary to replace the existing SharePoint/OneDrive FileWalk user with this application. Do as follows:

1. In the Management Console, under Management > Root > File Servers, find the SharePoint Online/OneDrive file server and click Edit.
The Edit File Server Wizard is displayed.
2. In the Common tab, in FileWalk credentials, click Update Settings.
The Create FileWalk Application dialog box is displayed.
3. Enter a user name and password to create a new FileWalk application in the tenant. The credentials must be from a user who has privileges to create applications in Azure Active Directory. The user name must be in the following format: username@domain.com.
4. Click OK.
The application is created and the (original) FileWalk user is deleted.

8

CONFIGURING THE DATA SECURITY PLATFORM

You can change the configuration options you set during the installation and add or remove components by running the Enterprise Installer again and selecting the Configuration option.

Before beginning any installation or upgrade, it is strongly recommended to ensure the most updated Microsoft hotfixes and patches that suit your server versions are installed on each server.

Welcome And License Agreement

The Welcome and License Agreement pages of the wizard allow you to start the setup and review and accept the license agreement details.

To start the installation:

1. Run the Enterprise Installer.
The Welcome page is displayed.
2. Click Next.
The License Agreement page is displayed.
3. Select I agree.
4. Click Next.

Main Menu

You can use the Main Menu to select the required workflow.

To select the required workflow:

1. Complete the previous pages of the Enterprise Installer, until you reach the Main Menu.
2. Select Configuration to configure your currently installed Varonis products.
You can maintain DB passwords and licenses.
3. Click Next.

Selecting The DSP Server

The DSP Server Selection page allows you to select the DSP Server and set the required parameters.

To select the DSP Server:

1. Complete the previous pages of the Enterprise Installer, until you reach the DSP Server Selection page.
2. Set the following parameters:
 - Database Server - Type the name of the required DSP Server database instance or select it from the drop-down list. If the relevant server is not listed, click the Browse button to locate it.
 - Authentication - Select the required authentication type, which can be either Windows or SQL.
 - User name - Type the user name for the DSP database.
 - Password - Type the password.

Important: If you plan to select the Maintain Database Passwords flow and change the sa credentials used to access the DSP Server, you must enter the new credentials on this page of the wizard - even though you have not yet changed them. The credentials you enter here are stored, and appear on the Database Security Configuration page when you set the database credentials for the sa account.

3. Click Next.

Configuring Database Users

The Configuration Options page allows you to select the required configuration flow. You can proceed to configure database users or register your license.

To configure database users:

1. Complete the previous pages of the Enterprise Installer, until you reach the Configuration Options page.
2. Select Database users configuration.
3. Click Next.

Configuring Database Security

The Database Users page allows you to configure database security options.

To configure database security options:

1. Complete the previous pages of the Enterprise Installer, until you reach the Database Users page.
2. To add the current user as a Varonis administrator, click Assign new admin.
3. To edit the permanent database account:
 - Click Edit. The Application account dialog box is displayed.

Note:

- This is the account used to retrieve data from all Varonis databases.
- When SQL authentication is selected, this account has a predefined user name and automatically generated password.
- Updating the application account will update the Log On As account for several Varonis services, such as Varonis Forwarder, DSP Server, Infra Logging, License, and so on.

The Permanent Database Account window is displayed.

Set the following parameter:

- Authentication - Select the authentication method, which can be:
 - Windows Authentication
 - SQL Authentication

Note:

- On distributed systems, SQL authentication must be selected.
- When using Windows Authentication for SQL access, the "Application account" (the AD account that is used instead of the SQL user) must have local admin rights and working share permissions on the Data Security Platform and all Collectors for deployment purposes.
- When using Windows Authentication on Solr/ZooKeeper servers (the AD account that is used manage the Solr/ZooKeeper component), the user must have local admin rights on the server.

- User name - Type the account's user name (the default user name is VaronisOwner).
- Password - Type the account's password (the default password is automatically generated).

Note: The SQL account password cannot contain the following characters: [{}(),;?*').

- Confirm password - If you changed the default password, retype your password.
 - Click OK. The Database Users page is displayed.
4. Click Next.
The Varonis Data Security Platform Configuration page is displayed, where you can insert or update the server's credentials.
 5. Click Next.
The Check prerequisites page is displayed. Wait while the Enterprise Installer proceeds to verify the prerequisites.
 6. Click Next.

Registering Your License

The Configuration Options page allows you to select the required configuration flow. You can proceed to configure database users or register your license.

To register your license:

1. Complete the previous pages of the Enterprise Installer, until you reach the Configuration Options page.
2. Select License Registration.
3. Click Next.

Configuring Your License

During the installation process, you can configure product license registration, automatically or manually.

If you are migrating DSP Analytics, the License Configuration page is displayed.

To configure your license:

1. Complete the previous pages of the Enterprise Installer, until you reach the License Configuration page.
2. For automatic registration:
 - a. Type the following parameters:
 - Customer ID/email - Type the ID or the email of the customer at which the Data Security Platform is being installed.

Note: The customer ID is displayed together with the serial number you received from Varonis. The ID replaces the email as the customer identifier.

- Serial number - Type the product serial number, as supplied by Varonis upon purchase.
 - b. Click Register. The Varonis products and the platforms the license supports are listed at the bottom of the page.
 - c. Click Finish.
3. For manual registration (if a problem arises with the automatic process):
- a. Type the following parameters:

- Customer ID/email - Type the ID or the email of the customer at which the Data Security Platform is being installed.

Note: The customer ID is displayed together with the serial number you received from Varonis. The ID replaces the email as the customer identifier.

- Serial number - Type the product serial number, as supplied by Varonis upon purchase.
 - b. To obtain a license key:
 - i. Go to the Varonis Support Website: <https://support.varonis.com/>.
 - ii. On the Login page, enter your user credentials and click OK.
- Note:** If this is your first visit to the Varonis Support site, you must create a user account.
- iii. Select License > License Registration. The License Registration page is displayed.
 - iv. In the Enter serial field, enter your the Data Security Platform serial number.
 - v. Select one of the following options:
 - Enter unique ID - Enter your unique ID. Use this option if you have an existing DSP installation that is lower than version 5.5.
 - Enter token - Enter your registration token, available on the License Configuration page of the Enterprise Installer. Use this option if your DSP installation is version 5.5 or higher.
 - vi. Click OK. Your license key is generated and displayed at the bottom of the page, along with the details of your license.
 - vii. Copy this number into the License Key field on the License Configuration page.
- c. Click Register. The Next button is enabled.
 - d. Click Next.

Deploying The Current Tasks

You can deploy currently defined tasks.

To deploy the current tasks:

1. Complete the relevant pages of the Enterprise Installer, until you reach the Deployment Progress page.
2. Click Install.
The selected products and services are installed.
3. To continue defining resource and options with the Enterprise Installer, click Next.

Finishing The Deployment

When the deployment is finished, you can return to the main menu, view an error log, or close the Enterprise Installer.

To finish the deployment:

Select the relevant option from the Installation Complete page:

- Return to Main Menu
- Show Error Log
- Close the Enterprise Installer; alternatively, click Finish.

9

UNINSTALLING THE DATA SECURITY PLATFORM

Proceed to perform the steps required to uninstall the Data Security Platform.

Main Menu

You can use the Main Menu to select the required workflow.

To select the required workflow:

1. Complete the previous pages of the Enterprise Installer, until you reach the Main Menu.
2. Select Uninstall to remove a Data Security Platform product or service from your system.
3. Click Next.

Selecting The DSP Server

The DSP Server Selection page allows you to select the DSP Server and set the required parameters.

To select the DSP Server:

1. Complete the previous pages of the Enterprise Installer, until you reach the DSP Server Selection page.
2. Set the following parameters:
 - Database Server - Type the name of the required DSP Server database instance or select it from the drop-down list. If the relevant server is not listed, click the Browse button to locate it.
 - Authentication - Select the required authentication type, which can be either Windows or SQL.
 - User name - Type the user name for the DSP database.
 - Password - Type the password.

Important: If you plan to select the Maintain Database Passwords flow and change the sa credentials used to access the DSP Server, you must enter the new credentials on this page of the wizard - even though you have not yet changed them. The credentials you enter here are stored,

and appear on the Database Security Configuration page when you set the database credentials for the sa account.

3. Click Next.

Uninstalling Varonis Servers And Monitored File Servers

The Security Configuration page allows you to uninstall Varonis servers, databases, and monitored file servers.

To uninstall Varonis servers, databases, and monitored file servers:

1. Complete the previous pages of the Enterprise Installer, until you reach the Security Configuration page.
2. To find or update user credentials for each server, do the following:
 - a. To find a specific server, type the name of the server in the Search Server text box and click Apply.
 - b. To find servers using a specific type of account credentials, select the required type from the Credentials type drop-down list and click Apply.
 - c. To find servers for which there are no user credentials, select the Show only empty checkbox and click Apply.

Note: You can combine any of the search methods to filter the list of servers.

Only servers that match your search criteria are displayed in the Server Name column.

3. To add or edit server credentials:
 - a. Select the server you want to edit and click Edit Credentials.
 - b. In the Credentials dialog box, set the user name and password of the user account.
4. To clear credentials, select the required server and click Clear Credentials.
5. To prevent removing any agents, select the following options as necessary in the Agent Options pane:
 - SharePoint agent
 - Varonis FileWalk agent
 - Directory Services proxy agents
 - Other file server agents
6. Click Next.

Finishing The Deployment

When the deployment is finished, you can return to the main menu, view an error log, or close the Enterprise Installer.

To finish the deployment:

Select the relevant option from the Installation Complete page:

- Return to Main Menu
- Show Error Log
- Close the Enterprise Installer; alternatively, click Finish.

Removing The User Interface

You can remove the user interface following the uninstallation of DatAdvantage.

To remove the user interface following the uninstallation of DatAdvantage:

1. Navigate to the GUI installation folder and double-click `setup.exe` to start the Enterprise Installer. The Welcome page is displayed.
2. Select Remove DatAdvantage UI <version>.
3. Click Finish.

Removing The Management Console

You can remove the Management Console user interface following the uninstallation of DatAdvantage.

To remove the user interface following the uninstallation of DatAdvantage:

1. Navigate to the Management Console installation folder and double-click `setup.exe` to start the Management Console installer.
The Varonis Management Console Setup page is displayed.
2. Click Remove.
The Ready to remove page is displayed.
3. Click Remove.
The Management Console is uninstalled.
4. Click Finish.

Uninstalling Optical Character Recognition (OCR)

If the Data Security Platform is uninstalled after the OCR mechanism (ABBYY) is installed, the OCR remains and is not uninstalled.


To uninstall the OCR mechanism:

1. On each Probe/Collector, go to C:\Program Files (x86).
2. Delete the ABBYY folder.

10

ADVANCED CONFIGURATION OF THE MANAGEMENT CONSOLE

The advanced configuration settings require in-depth knowledge of the Management Console. Do not change the settings unless instructed to do so by Varonis Support.

The advanced configuration settings are available in the Management Console through Tools  > Advanced Application Configuration.

11

MANAGING DSP SERVERS

The Management Console enables you to connect to various monitored DSP Servers.

Organizations that have several DSP Servers can define connection parameters for each server and switch between them.


The Management Console enables you to connect to various monitored DSP Servers. Use this option if you have several DSP Servers in your organization, in order to define connection parameters for each server and switch between them.

Note: The Management Console installation requires .NET Framework 3.5 SP1 and PowerShell 5.0.

Adding DSP Connections

Administrators can add connections to DSP Servers.


To add a connection to an DSP:

1. On the title bar, click the Tools button  and choose Select DSP Server. The DSP Server Selection dialog box is displayed.
2. Click Servers. The DSP Server Editor dialog box is displayed.
3. To add another DSP Server to the list:
 - a. Click Add. The Server Information dialog box is displayed.
 - b. Set the following:
 - DSP Server address - Type the name or IP Address of the DSP Server to be added.
 - Port number - Type the port number to which the DSP Server listens.
 - c. Click OK. The DSP Server is added to the list.

Removing DSP Connections

Administrators can delete connections to DSP Servers.

To delete a DSP connection:

1. On the title bar, click the Tools button  and choose Select DSP Server. The DSP Server Selection dialog box is displayed.
2. Click Servers. The DSP Server Editor dialog box is displayed.
3. From the list, select the DSP to be removed. You cannot remove the currently active DSP.
4. Click Remove.

Managing The DSP Server

Configuring DSP General Settings

You can view and configure general settings including information about the DSP Server itself, such as its name, installation path and port number, and to configure general database security.

To view or configure the general settings for the DSP server:

1. From the menu in the left pane, select Management > Components > Root > DSP. The DSP settings are displayed in the right pane.
2. In the right pane, select the General tab.
3. Select or clear one or more of the following checkboxes.

- Allow shrinking of the tempdb on all servers - When selected, the shrink job is performed once a week as part of the regularly scheduled maintenance and the Varonis owner is added as an owner to the tempdb on all servers.

Important: This option must have been selected when the DSP server was installed. Otherwise the shrink job will fail when it is selected here.

- Allow partitioning of the tempdb on all servers - When selected, the tempdb is partitioned when installing, repairing, upgrading, or adding a new database server, such as a distributed Probe, to the Data Security Platform. Partitioning requires 'sa' credentials.
- Allow check disk space - When selected, disk space is checked. If the application server resides on the same machine as the database server, disk space is checked by the local application server. If the application server resides on a different machine, UNSAFE CLR is used to check disk space.

Important: When the application and database servers reside on the same machine, the application server account must be a local system account.

4. Click Save.

Configuring Your License

During the installation process, you can configure product license registration, automatically or manually.

If you are migrating DSP Analytics, the License Configuration page is displayed.

To configure your license:

1. Complete the previous pages of the Enterprise Installer, until you reach the License Configuration page.

2. For automatic registration:

a. Type the following parameters:

- Customer ID/email - Type the ID or the email of the customer at which the Data Security Platform is being installed.

Note: The customer ID is displayed together with the serial number you received from Varonis. The ID replaces the email as the customer identifier.

- Serial number - Type the product serial number, as supplied by Varonis upon purchase.

b. Click Register. The Varonis products and the platforms the license supports are listed at the bottom of the page.

c. Click Finish.

3. For manual registration (if a problem arises with the automatic process):

a. Type the following parameters:

- Customer ID/email - Type the ID or the email of the customer at which the Data Security Platform is being installed.

Note: The customer ID is displayed together with the serial number you received from Varonis. The ID replaces the email as the customer identifier.

- Serial number - Type the product serial number, as supplied by Varonis upon purchase.

b. To obtain a license key:

- i. Go to the Varonis Support Website: <https://support.varonis.com/>.
- ii. On the Login page, enter your user credentials and click OK.

Note: If this is your first visit to the Varonis Support site, you must create a user account.

- iii. Select License > License Registration. The License Registration page is displayed.
 - iv. In the Enter serial field, enter your the Data Security Platform serial number.
 - v. Select one of the following options:
 - Enter unique ID - Enter your unique ID. Use this option if you have an existing DSP installation that is lower than version 5.5.
 - Enter token - Enter your registration token, available on the License Configuration page of the Enterprise Installer. Use this option if your DSP installation is version 5.5 or higher.
 - vi. Click OK. Your license key is generated and displayed at the bottom of the page, along with the details of your license.
 - vii. Copy this number into the License Key field on the License Configuration page.
- c. Click Register. The Next button is enabled.
 - d. Click Next.

Managing DSP Server Components

DSP Server Component Management enables managing various aspects of DSP Server components, including the Reports component, the Data Classification Engine, and DatAnswers.

- Reports - Install and configure the Reports component, to enable generation of reports.
- DCE and DatAnswers - Install and configure the following:
 - Data Classification Engine - Monitors access to files containing sensitive data.
 - DatAnswers (DW) - Enables users to search an organization's Varonis-monitored file systems for the information they need, while ensuring only the right users have access to the right data. DatAnswers uses the Varonis classification engine to filter results according to file system permissions and index the data.
- Data Transport Engine - Install and configure the Data Transport Engine, to enable secure transport of data within the organization's servers.

- **DatAlert Web Server** - Install and configure the Web Interface server to enable monitoring and investigating the various alerts generated by DatAlert and DatAlert Analytics in the Varonis Web Interface.
- **DatAlert Analytics** - Install and configure DatAlert Analytics, to enable receiving DatAlert Analytics alerts on important events in real-time (or nearly so).

For information about how to add and remove components, see [Adding and Removing DSP Service Components](#).

Adding and Removing DSP Service Components

You can install licensed DSP Server components.

For information about how to configure DSP Server components, see [Managing DSP Server Components](#).

To add or remove DSP Server components:

Important: You can only add licensed service components.

1. In the Management Console, from the menu in the left pane, select Management > Components > Root > DSP > Service Components.
The Service Components settings are displayed in the right pane.
2. To install a component, from the toolbar, click the required component.
The following options are available:

Note: Only licensed components are available.

- **Data Classification and DatAnswers** - Installs the following components:
 - **Data Classification Engine (DCE)** - Monitors access to files containing sensitive data.
 - **DatAnswers (DW)** - An enterprise search engine that enables users to search an organization's Varonis-monitored file systems for the information they need, while ensuring only the right users have access to the search results.
- **DatAlert and DatAlert Analytics** - Installs DatAlert and DatAlert Analytics, which enable defining rules and threat models to identify problematic activity in a company's data assets.
- **Data Transport Engine** - Installs the Data Transport Engine service, which enables migration of files, folders and file servers.
- **Reports** - Installs the reporting services.

3. To remove a component, select the required component and click Remove.

Managing Updates

You can deploy updates for each component, server, and client application.

The Update Manager tab allows deploying updates for each component, server, and client application. The updates are created by Varonis and sent to customers as VIP files.

To deploy Varonis updates:

1. In the Management Console, from the menu in the left pane, select Management > Components > Root.
2. In the right pane, select the Update Manager tab.
The Update Manager pane is displayed on the right.
3. Click Load File and browse to select the relevant Varonis Package VIP file.
The Windows Open dialog box opens with the Varonis Package *.vip file as the default file type. This is the only file type that is supported for upload.
4. After you have selected the Varonis Package VIP file, click Open.
The Update Details dialog box is displayed, where you can choose whether to deploy the VIP file now or at a later time.
5. At this stage, you can run the deployment immediately, or register it and run it later.
 - To run the deployment now:
 - a. Click Register and Deploy.
 - b. Proceed to [step 6](#) if the Update type is either Server and client or Server only. Otherwise, skip ahead to [step 7](#), if the Update type is Client only.
 - To run the deployment later:
 - a. Click Register only.
The Update Details window closes, and the update is added to the list in the main Update Manager page with "Pending Deployment" status.
6. If the update is "Server and client" or "Server only": The Update Deployment dialog box is displayed. Choose whether to install the update on all servers or on specific ones:
 - a. Select the relevant checkboxes, and click Deploy to run the update on the selected servers.

The Fill Credentials dialog box is displayed, where you can view and edit server credentials.
 - b. Set the server credentials, as needed. Click Continue to proceed.

The Update Deployment dialog box is displayed, showing the deployment progress in the Status column: Pending, Installing, or Installed.

Note: While the deployment is running, the checkboxes are disabled, and the Management Console cannot be used.

- c. When the installation completes, the Status column displays warning icons for viewing error status details. Click the icon in the relevant row to view a summary of the status details, indicating whether the deployment is successful. If unsuccessful, relevant errors or warnings are displayed, and you can review them and redeploy the update as required.

When the deployment is successful, the Status column displays Successfully deployed.

7. If the update type is "client only": You will need to register the update on the DSP server. A pop-up window is displayed, showing that the update was successfully deployed on the DSP server. Click OK to close the pop-up window. The update is added to the list with "Fully Deployed" status.

The deployment on the client-side is as follows:

- When an update is detected, a notification will be displayed in the Management Console title bar. You can click this text to view the list of available updates in the Varonis Update dialog box.

Note: The client applications will be updated the next time they are launched.

8. To view the details of an update, in the Update Manager page, select the relevant update and click Show Details.

The [Update Details page](#) is displayed.

9. To export the update details to a CSV file, in the Update Manager page, select the relevant update and click Export. Save the file to the required directory.

In the CSV file, additional details, beyond those shown in the Update Manager page, will be displayed. The data will be comma-separated, and multiple values will be separated by semicolons (;).

10. To redeploy an update, for example, that has partial, error, or pending status, in the Update Manager page, select the relevant update and click Deploy.

Note: Only a single update can be deployed at a time. Bulk deployment is not supported.

11. To search for updates per specific statuses or types, select the relevant filters and click Apply.

The Status options include:

- Successfully Deployed - The update was successfully deployed.

- In Progress - The update is in progress.
- Partially Deployed - The update is in progress on the selected servers.
- Pending Deployment - The update is designated to be deployed later. This occurs when a VIP file was loaded, and Deploy Later was selected.
- Deployment Error -
 - When an error occurred while deploying (either deploying a new update from scratch or redeploying a previously partially deployed update).
 - The error caused the update to be partially installed or not installed at all (these have the same error status).
- All (default) - All update statuses will be displayed in the list.

The Type options include:

- Client Only
- Server Only
- Server and Client

12. To remove "pending" deployment" updates that have not been deployed yet, in the Update Manager page, select the relevant update(s) with "pending deployment" status, and click Remove Pending.

12

UPDATING MAIL SETTINGS THROUGH THE MANAGEMENT CONSOLE

You can update Data Security Platform email settings through the Management Console, and specify whether to send file server connectivity notifications.

To update Data Security Platform email settings:

1. In the Management Console, from the menu in the left pane, select Configuration > Mail Settings.
The Mail Settings pane is displayed.
2. Set the relevant parameters. For more information, see [Configuring Mail Settings](#).
3. To update the email settings on all monitored file servers, select the Update email settings on all monitored file servers checkbox.
4. To prevent Probes from sending email notifications regarding file server connectivity issues, clear the Send file server connectivity notifications checkbox.

Note: The Probe service must be restarted before changes to this setting take effect on the relevant Probes and Collectors.

5. Click Save.

13

ADDITIONS TO THE MASTER DATABASE

During installation (or upgrade), the Enterprise Installer adds objects to the master database.

These include:

Tables

HardwareInfo([Key] nvarchar(128),[Value] nvarchar(128))

Views

Only temporary for archiving purposes

Stored Procedures and Functions

- spHardwareInfo
- fnSmallDateTimeRange
- fn_YearMonth2Str
- fn_YearMonth2Date
- fn_YearMonthStr2Date
- fn_Date2YearMonthStr
- fn_Date2YearMonthDayStr
- fn_AgentDateTime2DateTime
- fn_DateTime2AgentDate
- fn_DateTime2AgentTime
- fn_DateTime2ANSI
- spSecurity_Notification
- fnclsSecureMode
- spSecurity_AddMemberToRoleSQLAgentOperatorRole
- spSecurity_AddMemberToRoleViewServerState
- spSecurity_AddMemberToRoleGUI
- spSecurity_AddMemberToRoleOWNER

- spSecurity_RemoveMember
- spSecurity_DropMemberFromRoles
- spSecurity_DropAllMembersFromRoles
- spSecurity_AddWinUserToRoleGUI
- spSecurity_AddWinUserToRoleOWNER
- Security_RemoveWinUser
- splsAdmin
- spSecurity_MasterDropLogin
- Security_UpdateJobsOwner
- spCheckDiskSpace
- spGenerateView (create temporary view for archiving purposes)
- spDropView (remove temporary view for archiving purposes)
- spCreateCheckDiskSpaceJob
- spSecurity_MasterGrantLogin
- spSecurity_MasterAddLogin
- spSecurity_Master_ProxyAccount_Set
- spSecurity_Master_ProxyAccount_Del
- spSecurity_Master_ProxyAccount_Get spKillUserProcesses

Roles

GUI

Jobs

Maintain_tempdb

Configuration

- Ole Automation Procedures = 1
- Cross DB ownership chaining = 1

MIXED MODE ENVIRONMENTS

DatAdvantage supports mixed-mode environments, in which it is possible to set permissions from different protocols.

For each entry point, you must set the security that DatAdvantage should extract for mixed folders under that point. This is required since DatAdvantage can maintain only one set of permissions per folder.

DatAdvantage handles security modes as follows:

- Unix security mode - Handled as regular Unix security
- NT security mode - Handled as regular NT security
- All other security modes - Handled as mixed security

Note: The term mixed mode should not be confused with the term multi-protocol, which refers to the ability to authenticate and access the same files from different client file systems.

15 PULL PROXY SETUP

Varonis enables reliable transfer of large tables that are pulled from the Probe servers to the Shadow servers over high-latency, low-bandwidth connections.

The basic concept of this architecture is that a temporary zipped file is stored on the Probe machine and pushed to the Shadow machine over CIFS, thereby reducing SQL statement overhead.

- A new folder with executables is added to the Probes, Shadows and the DSP, under the existing Varonis folder. This folder will be named "SQLMover".
- Every Probe and Shadow server has a new temporary folder (called "temp") to be used during the pull process.
- A dedicated Active Directory account (called "Proxy user") is responsible for transferring the zipped files.

To install and configure the pull proxy setup:

1. Create the Active Directory proxy account.
 - a. Select or create an Active Directory account to be used as the proxy user (no special credentials or roles are needed).
 - b. If needed, a separate proxy account can be chosen for each server with Shadow databases (all Shadows on the same server use a common proxy account).
2. Create the temporary folder on every Probe and Shadow server.
 - a. Create a new folder to handle the temporary transferred data (be sure to name it "temp").
 - b. Set Read and Write permissions on the temp folder for the account used by the SQL instance service and the SQL agent service (no change is required if using Local System).
 - c. Set Read and Write permissions on the temp folder for the Active Directory proxy account.
 - d. Create a windows share leading to the temporary folder that is accessible by the proxy account. If the proxy account is a local administrator on the probe, the administrative share "c\$" can be used.
3. Copy the executable folder.

- a. Copy the SQLFHandler folder provided in the DSP installation "C:\Program Files\Varonis\DatAdvantage\Domain\SQLFHandler" to the Probe servers, to the Varonis program directory (by default this is "C:\Program Files\Varonis").
 - b. Copy the SQLFHandler folder provided in the DSP installation "C:\Program Files\Varonis\DatAdvantage\Domain\SQLFHandler" to the Shadow servers. It is recommended to create a directory called "C:\Program Files\Varonis" and place "SQLFHandler" there.
4. Ensure permissions on the executable folder, on every Probe and Shadow server:
 - a. Set Read, Write, and Execute permissions on the SQLFHandler folder for the account used by the SQL instance service and the SQL agent service (no change is required if using Local System).
 - b. Set Read, Write, and Execute permissions on the SQLFHandler folder for the Active Directory proxy account.
 5. Ensure permissions on the SQL Server tools folder, on every Probe and Shadow server:
 - a. Find the SQL Server tools folder on each computer.
 - b. Set Read, Write, and Execute permissions on the tools folder for the account used by the SQL instance service and the SQL agent service.
 - c. Set Read, Write, and Execute permissions on the tools folder for the Active Directory proxy account.
 6. Ensure Read permissions on the Windows\temp folder:
 - a. On every Probe server, set Read permissions on the Windows\temp folder for the account used by the SQL instance service and the SQL agent service.
 - b. On every Shadow server, set Read permissions on the Windows\temp folder for the Active Directory proxy account.
 7. Set the proxy account on all Shadow servers:
 - a. Execute the following procedure to configure the account you chose above (all three parameters are required):

```
master..spSecurity_Master_ProxyAccount_Set @Domain, @User, @password
```

Where:

- @Domain = Proxy user's domain (NetBIOS name)
- @User = Proxy user name
- @password = Proxy user's password

- b. Use the procedure `master..spSecurity_Master_ProxyAccount_Get` to show the current proxy account.
 - c. Use the procedure `master..spSecurity_Master_ProxyAccount_del` to remove the proxy account. Only remove the proxy account from a Shadow server if you do not plan to use the ZIP feature on that server.
 - d. Execute the procedure once per SQL instance on which Shadow databases are installed. It does not need to be run more than once if several Shadow databases are installed on the same instance.
8. For each Shadow, run the commands below on the DSP database (`VrnsDomainDB`), making sure to enter the correct path for your configuration and file locations, and correcting the key name for each Shadow server:
- a. Run the following command:

```
update keyvalue set [value] = 'C:\Program Files\Varonis\SQLFShandler\SQLFShandler.exe' where [key] = 'SQLMoverPath_<shadowserver\instance>'
```

- b. For shadows located on the DSP Server, the value can be copied from the predefined key used by the DSP itself using the following commands:

```
update keyvalue set [value] = (select [value] from keyvalue where [key] = 'SQLMoverPath') where [key] = 'SQLMoverPath_<shadowserver\instance>'
```

```
update keyvalue set [value] = 'C:\Program Files\Varonis\SQLMoverData' where [key] = 'SQLMoverShadowSharePath_<shadowserver\instance>'
```

- c. Replace the string `<shadowserver\instance>` with the Shadow server's name and instance.
 - d. Note that the path in step a points to the `SQLFShandler.exe` file, whereas the path in step b points to the temp data directory.
9. On each Probe run the commands below, making sure to enter the correct path for your configuration and file locations:
- a. Run the following commands:

```
update keyvalue set [value] = 'C:\Program Files\Varonis\
SQLFShandler \SQLFShandler.exe' where [key] = 'SQLMoverP
ath'
```

```
update keyvalue set [value] = '\\16-probe2k3\c$\Program
Files\Varonis\SQLMoverData' where [key] = 'SQLMoverProbe
SharePath'
```

- b. Note that the path in step a must point to the `SQLFShandler.exe` file.
- c. Note that the path in step b must be a CIFS/UNC path, including the machine name, pointing to the temp data directory on the Probe. The format is `\<machine name>\<share>\<path>`.
- d. To enable the use of the SQL Mover feature for this Probe, run the following command:

```
update keyvalue set [value] = 1 where [key] = 'SQLMoverI
nUse'
```

- e. To disable the feature for this Probe, run the above command with `[value]` set to 0.
10. On the `VrnsDomainDB` database (on the DSP), run the following command to enable use of the SQL Mover feature:

```
update keyvalue set [value] = 1 where [key] = 'SQLMoverInUs
e'
```

Note: If this main flag is disabled but the flags on the Probes are enabled, zip files are still created.

11. To verify configuration, check the `[keyvalue]` table on the DSP) and the Probes; the relevant keys begin with "SQLMover".
12. Enable the SQLMover job on the DSP database.
 - a. In the SQL Server Enterprise Manager, select SQL Server Agent > Jobs.
 - b. Right-click the job name SQLMover and select Enable from the context menu.

Note: The key `SQLMoverInUse` is the flag that enables the fix, and it can be configured individually on each Probe.

16 SQL FARM SUPPORT

An SQL farm is a main DB server (clustered or not) that serves different applications. It is not defined per application (DatAdvantage can use it alongside other enterprise applications).

DatAdvantage can work with either a physical database server (for example, the local machine's database, a single remote database server or a non-clustered farm) or a federated/clustered farm/virtual DB server that represents multiple servers under the same management system. Since SQL farms do not allow direct interaction with the file server and operating system, an application layer is used (in DatAdvantage, the DSP Server is used).

What Is Supported

- Database and services separation for the DSP and Probe servers (reside on different machines).

Important: When DatAdvantage is configured in this way, SQL authentication is required for all databases.

- Databases installed on a non-clustered (single physical machine) SQL farm.

Important: All MS SQL installations in the DatAdvantage system must use the simple recovery mode. For more information about MS recovery modes, see the relevant Microsoft documentation.

CAUTION: Changing the recovery mode of Varonis databases can damage DatAdvantage's functionality and may result in loss of data.

Database Credentials

Two accounts are required for the SQL database, one for the initial installation (SA account) and one accessing the account to carry out tasks such as accessing the database, performing select operations and updating data (work account).

The following table summarizes the required credentials:

Account	Services	Database	Reporting Services
Installation	Local administrator on the machine	N/A	Local administrator
Administrator	Local administrator on the machine on which the installer is running	SQL Server system administrator	User with access to the reporting services database tables (simple select and update)
Work	Local administrator on the machine	Permissions granted via the Enterprise Installer	None

17

VARONIS SUPPORT WEBSITE

Log in to the Varonis Support website for technical assistance.

Logging In to the Support Site

To log in to the support site:

1. Go to the Varonis Support Website:<https://support.varonis.com/>.
2. If you already have a user account, enter your email address and password, or follow the instructions below to create a user account.
3. Click Sign In.

Creating a User Account

Create a user account on the Varonis Support website to obtain technical assistance.

To create a user account for the Varonis Support site:

1. In the top right corner of the Varonis Support page, click the relevant link:
 - Partner Registration
 - Customer Registration
 - Secondary Customer Registration - To create a user account that is linked to the primary customer account, with the same visibility and permissions as the primary account. The secondary account is bound by the license belonging to the primary account, and can only be created after the primary account possesses a license.

The relevant registration page is displayed.

2. Complete the information.
3. Click OK.
The account is created.