Enterprise Vault™ Upgrade Instructions

15.2

arctera™

Enterprise Vault™: Upgrade Instructions

Last updated: 2025-07-07.

Legal Notice

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the company website:

https://www.veritas.com/docs/100040095

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

productdocs@arctera.io

You can also see documentation information or ask a question on the Arctera (formerly Veritas) community site:

https://vox.veritas.com/category/arctera-discussions/discussions/enterprise-vault

Technical Support

Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within the company to answer your questions in a timely fashion.

Our support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about our support offerings, you can visit our website at the following URL:

www.arctera.io/support

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contents

Technical Support 4

Chapter 1 About this guide 10

Introducing this guide 10

Chapter 2 Before you begin 11

Server upgrade paths 11
Additional requirements for the Enterprise Vault index server 12
Backup strategy for Enterprise Vault indexes 12
Additional requirements for Microsoft SQL Server databases 13
Decryption of RMS-protected messages 13
Documentation 13

Chapter 3 Points to note when upgrading 14

Order of upgrade in an environment with Surveillance or eDiscovery 15
Silently installing Enterprise Vault from the command line 16
Installing Outlook on the Enterprise Vault server 16
Upgrading to a supported version of Outlook 17
Securing Enterprise Vault web applications 17
Weak protocols and ciphers are blocked 18
Improved consistency when applying a retention period to items 19
Limiting the impact when updating moved item locations 22
Automatic migration of NetApp C-Mode connection settings 22
Enterprise Vault auditing configuration 23
Amazon Simple Storage Service (S3) partition 24
Classification using Microsoft File Classification Infrastructure on Windows Server 2016 and 2019 24
Data Classification Services does not support all the types of retention categories available in Enterprise Vault 14.2 and later 24
Managing certificates for Enterprise Vault Cloud Storage Adapter 25
eDiscovery Platform compatibility with Enterprise Vault 25

Chapter 4 Steps to upgrade your system 26

Overview of the upgrade process 26

Chapter 5 Enterprise Vault server preparation 28

About Enterprise Vault server preparation 28
Backing up the system 29
Backing up Enterprise Vault data 29
Backing up changed language files 30
Updating required Windows features 30
Running Enterprise Vault Deployment Scanner 30
Setting database permissions 31
Allowing the MSMQ queues to empty 31
Checking the archiving and expiry schedules 32

Chapter 6 Single server: upgrading the Enterprise Vault server software 33

About upgrading a single Enterprise Vault server 33
Installing on a single server 33
Upgrading the Enterprise Vault databases 35
Backing up the upgraded Enterprise Vault databases 37
Configuring index data location 37
Starting all the Enterprise Vault services 38

Chapter 7 Multiple servers: upgrading the Enterprise Vault server software 39

About upgrading multiple Enterprise Vault servers 39
Installing on multiple servers 39
Upgrading the Enterprise Vault databases 42
Backing up the upgraded Enterprise Vault databases 43
Configuring index data location 43
Starting all the Enterprise Vault services 44

Chapter 8 Arctera Cluster Server: upgrading the Enterprise Vault server software 45

About upgrading an Arctera cluster 45
Installing the Enterprise Vault server software 45
Upgrading the Enterprise Vault databases 48
Backing up the upgraded Enterprise Vault databases 49
Configuring index data location 56

Starting all the Enterprise Vault services 50

Chapter 9 Windows Server Failover Clustering: upgrading the Enterprise Vault server software 51

About upgrading a Windows Server Failover Cluster 51
Installing the Enterprise Vault server software 52
Upgrading the Enterprise Vault databases 55
Backing up the upgraded Enterprise Vault databases 55
Configuring index data location 56
Starting all the Enterprise Vault services 56

Chapter 10 Upgrading standalone Administration Consoles 58

About upgrading standalone Administration Consoles 58
Upgrading a standalone Administration Console (wizard) 59
Installing Enterprise Vault (command line) 59

Chapter 11 Upgrading Enterprise Vault Reporting 61

Upgrading Enterprise Vault Reporting 61
Installing the Enterprise Vault Reporting component 62
Running the Enterprise Vault Reporting Configuration utility 62

Chapter 12 Upgrading MOM and SCOM 64

Upgrading MOM 64
Upgrading the Enterprise Vault SCOM management pack 64
About the supplied management packs 65
About the upgrade procedure 65

Chapter 13 Upgrading Exchange Server forms 66

About upgrading Exchange Server forms 66

Chapter 14 Upgrading Domino mailbox archiving 67

About upgrading Domino mailbox archiving 67
Domino client version required to run EVInstall.nsf 67
Preparing for the upgrade of Domino mailbox archiving 68
Upgrading Domino mailbox archiving 68
Granting the Domino archiving user access to mail files 70
Identifying internal mail recipients 71
Run the Domino provisioning task 73

Chapter 15 Upgrading the FSA Agent 74
Compatible versions of the FSA Agent and Enterprise Vault server 74
About upgrading the FSA Agent 74
Upgrading FSA Agent services that are clustered for high availability 76
Upgrading the FSA Agent on a target Windows file server from the Administration Console 77
Upgrading the FSA Agent on an FSA Reporting proxy server from the Administration Console 78
Upgrading the FSA Agent manually 79
Chapter 16 Upgrading Enterprise Vault Office Mail App 81
About upgrading Enterprise Vault Office Mail App 81
Chapter 17 Upgrading SharePoint Server components 82
About upgrading the SharePoint components 82
Upgrading the Enterprise Vault SharePoint components 83
Chapter 18 Upgrading SMTP archiving 84
Required and optional tasks when upgrading SMTP Archiving 84
Checking the SMTP journaling type configuration 86
Finding SMTP targets that are assigned to unsupported archive types 90
Checking the permissions of the SMTP Archiving task account 91
Checking the 'Journal report processing' advanced SMTP policy setting 92
Checking the 'Journal Reports settings' advanced SMTP policy setting 92
Checking the 'Selective Journal Archiving' site setting 93
About upgrading legacy SMTP archiving components 93
Migrating existing targets to provisioning groups 94
Reconfiguring targets that are configured for target address rewriting to use multiple archives 95
Granting the Administrators group and system account full access to the SMTP holding folder 96

Chapter 19 Upgrading your Enterprise Vault sites to use Enterprise Vault Search 97

About Enterprise Vault Search 98
Server requirements for Enterprise Vault Search 98
Defining search policies for Enterprise Vault Search 98
Allowing privileged Enterprise Vault Search users to restore items to other users' mailboxes 100
Setting up provisioning groups for Enterprise Vault Search 101
Changing the order in which Enterprise Vault processes the search provisioning groups 103
Creating and configuring Client Access Provisioning tasks for Enterprise Vault Search 103
Configuring user browsers for Enterprise Vault Search 104
Configuring the Block Untrusted Fonts feature in Windows 10 105
Configuring Enterprise Vault Search for use in Forefront TMG and similar environments 106
Setting up Enterprise Vault Search Mobile edition 107
Carrying out preinstallation tasks for Enterprise Vault Search Mobile edition 107
Installing Enterprise Vault Search Mobile edition 110
Configuring the maximum number of permitted login attempts to Enterprise Vault Search Mobile edition 111
Verifying the installation of Enterprise Vault Search Mobile edition 112

Chapter 20 Upgrading Enterprise Vault API applications 113

Upgrading any applications that use the Enterprise Vault API Runtime 113

Chapter 1

About this guide

This chapter includes the following topics:

- Introducing this guide

Introducing this guide

This guide describes how to upgrade Enterprise Vault.

If you are performing a new installation of Enterprise Vault, see the *ReadMeFirst* file. Then follow the installation instructions in the *Installing and Configuring* guide, which is in the `Arctera Enterprise Vault\Documentation` folder on the Enterprise Vault release media.

The most up-to-date versions of the *ReadMeFirst* file and *Installing and Configuring* guide are available from the Documentation Library.

Chapter 2

Before you begin

This chapter includes the following topics:

- Server upgrade paths
- Additional requirements for the Enterprise Vault index server
- Backup strategy for Enterprise Vault indexes
- Additional requirements for Microsoft SQL Server databases
- Decryption of RMS-protected messages
- Documentation

Server upgrade paths

This guide describes how to upgrade to Enterprise Vault 15.2. The only possible server upgrade paths to this version are from Enterprise Vault 14.0 original release, 14.1, 14.2, 14.3, 14.4, 14.5, 15.0, 15.1, and 15.2.

Note: Enterprise Vault release updates that you have installed do not affect the upgrades. You do not have to remove Enterprise Vault release updates before you upgrade.

Note: If Enterprise Vault Security Update exists in your environment:

♦ After an Enterprise Vault upgrade or Release Update installation, reinstall the latest Security Update.

♦ After modifying or repairing Enterprise Vault, first uninstall any existing Security Update, then install the latest Security Update.

Additional requirements for the Enterprise Vault index server

In a new installation of Enterprise Vault 14.2 or later, or an upgrade to Enterprise Vault 14.2 or later, Elasticsearch is the new indexing engine.

The Elasticsearch indexing engine has following requirements:

- Additional CPU and RAM configuration. Refer to the *Enterprise Vault hardware requirements* section in the *Installing and Configuring* guide.
- Memory is allocated and reserved for the Elasticsearch indexing engine. By default, 8 GB of memory is reserved for the Elasticsearch indexing engine. Reservation of memory for the Elasticsearch indexing engine provides lesser memory to other Enterprise Vault services if those are running on the Enterprise Vault index server. It is recommended that you increase the RAM by 8GB to ensure that all the applications run smoothly.
- By default, the Elasticsearch indexing engine supports one index location. You can configure the Elasticsearch indexing engine to support multiple index locations. It is recommended that you provision disk space considering this requirement. Additionally, it is recommended to have separate index location for storing the index data of Elasticsearch indexes. Elasticsearch index data is 8% of the total disk space of archived items. Provision disk space for index data based on future requirement.
- Additional disk requirement for storing snapshots of the Elasticsearch indexes.
- Additional two TCP ports is used by the Elasticsearch indexing engine for communication on the index server. By default, you must keep any two ports open between the range 9200-9300. The port range can be changed later.

Backup strategy for Enterprise Vault indexes

Enterprise Vault 14.2 introduces Elasticsearch as the new indexing engine which recommends to take snapshots as the only reliable way to backup the index data. Going forward, the backup strategy for newly indexed data in Elasticsearch indexes is to take snapshots.

For more information, see How to backup indexes in Enterprise Vault 14.2 and later.

Note: The backup strategy for the non-Elasticsearch indexes is unchanged and continues to support the backing up of index data through a filesystem backup.

Additional requirements for Microsoft SQL Server databases

If you use Microsoft SQL Server database mirroring with your Enterprise Vault databases, remove it before you upgrade the Enterprise Vault server software. Enterprise Vault fails to upgrade its databases if mirroring is configured. For more information, see the following article:

http://www.veritas.com/docs/100019439

Note also that, in an environment where you have implemented SQL Server log shipping as a disaster-recovery solution, the process of upgrading the Enterprise Vault databases can disrupt the log shipping operations in some circumstances. After you have completed the upgrade, it is important to check that these operations continue as scheduled.

Decryption of RMS-protected messages

This topic is applicable only if you have configured Enterprise Vault to decrypt the RMS-protected messages (that is, you have selected the **Enabled RMS Decryption** field on the Enterprise Vault site in your environment) and make those available for search and access.

To continue the decryption of protected emails, configure Microsoft Purview Information Protection (MPIP) on the Enterprise Vault site in your environment. For more information about configuring MPIP, see https://www.veritas.com/support/en_US/doc/123165319-123165378-0/index.

Note: Archiving is stopped until you configure MPIP on the Enterprise Vault site in your environment.

If you do not want to use the decryption of RMS-protected messages, clear the **Enabled RMS Decryption** field on the **RMS** tab of Enterprise Vault site properties before upgrading to Enterprise Vault 14.2 or later.

Documentation

The Enterprise Vault documentation is in the `Arctera Enterprise Vault\Documentation` folder on the Enterprise Vault media.

For the latest information on supported devices and versions of software, see the Enterprise Vault Compatibility Charts.

Chapter 3

Points to note when upgrading

This chapter includes the following topics:

- Order of upgrade in an environment with Surveillance or eDiscovery
- Silently installing Enterprise Vault from the command line
- Installing Outlook on the Enterprise Vault server
- Securing Enterprise Vault web applications
- Weak protocols and ciphers are blocked
- Improved consistency when applying a retention period to items
- Automatic migration of NetApp C-Mode connection settings
- Enterprise Vault auditing configuration
- Amazon Simple Storage Service (S3) partition
- Classification using Microsoft File Classification Infrastructure on Windows Server 2016 and 2019
- Data Classification Services does not support all the types of retention categories available in Enterprise Vault 14.2 and later
- Managing certificates for Enterprise Vault Cloud Storage Adapter
- eDiscovery Platform compatibility with Enterprise Vault

Order of upgrade in an environment with Surveillance or eDiscovery

Surveillance (formerly Compliance Accelerator) 14.5 works with Enterprise Vault 14.3 and later. eDiscovery (formerly Discovery Accelerator) 14.5 work with Enterprise Vault 14.0 and later.

Order in which to perform the upgrade

1. If your environment includes eDiscovery:
   - Install eDiscovery 15.2 on the eDiscovery server.
   - Then upgrade the eDiscovery databases.
   - Then install the eDiscovery 15.2 client software on each client computer.
2. Upgrade Enterprise Vault to version 15.2 on all Enterprise Vault servers.

   Note: If your environment includes Surveillance (formerly Compliance Accelerator), do not start the Enterprise Vault Storage service on any Enterprise Vault Storage server until you have upgraded to Surveillance 15.2. This order ensures that the random sampling feature works seamlessly before and after the upgrade.

   ---

3. Upgrade Enterprise Vault to version 15.2 on all Surveillance and eDiscovery servers.
4. If your environment includes Surveillance:
   - Install Surveillance 15.2 on the Surveillance server.
   - Then upgrade the Surveillance databases.
   - Install the Surveillance 15.2 client software on each client computer.

   Note the following:
   - Only start the Enterprise Vault Storage service on the Enterprise Vault Storage servers after you have fully upgraded Surveillance.

For more information on supported versions and upgrade paths, see the Enterprise Vault Compatibility Charts and the article about supported upgrade paths at https://www.veritas.com/docs/100023744.

For detailed instructions on how to upgrade Surveillance and eDiscovery, see their accompanying documentation.

Silently installing Enterprise Vault from the command line

The command-line syntax for silently installing Enterprise Vault has changed. You must now include two new parameters, /wait and /clone_wait. The syntax is as follows:

```
start /wait "" "setup (x64).exe" /s /clone_wait
/v"COMPONENTS=Option[|Option][...]"
```

For more information, see the "Installing Enterprise Vault (command line)" section in the *Installing and Configuring* guide.

Installing Outlook on the Enterprise Vault server

To support Exchange Server archiving, you must install Outlook on the Enterprise Vault server. Enterprise Vault currently supports the following versions of Outlook for this purpose:

- Outlook 2016, 32-bit version. You need build version 16.0.4534.1001 or later.
- Outlook 2016 Click-to-Run, 32-bit version.
- Outlook 2019, 32-bit version.
- Outlook 2019 Click-to-Run, 32-bit version.

In each case, Enterprise Vault supports the Windows Installer (MSI) version of 32-bit Outlook, which is available with the volume license. It does not support the 64-bit versions. For the latest information on supported versions of Outlook, see the Compatibility Charts.

Outlook must be the default email client on the Enterprise Vault server. When the Enterprise Vault Admin service starts, it checks that Outlook is configured as the default client and, if it is not, configures it as such.

MAPI over HTTP and Outlook Anywhere (RPC over HTTP)

Install a version of Outlook to suit the transport protocol that you have enabled in Exchange: MAPI over HTTP or Outlook Anywhere (formerly "RPC over HTTP").

Table 3-1 Exchange transport protocols and required version of Outlook

Exchange version	Outlook version on Enterprise Vault server
	Outlook 2016/2019
Exchange Server 2016/2019 with MAPI over HTTP enabled	Supported
Exchange Server 2016/2019 with Outlook Anywhere enabled	Not supported

Upgrading to a supported version of Outlook

Note: Outlook performance counters must be disabled when Outlook 2016 or 2019 is installed on the Enterprise Vault server. The Enterprise Vault Admin service automatically disables the Outlook performance counters if it detects Outlook 2016 or 2019 on the Enterprise Vault server.

To upgrade to a supported version of Outlook

1. Stop the Enterprise Vault Admin service on the Enterprise Vault server.
2. Install Outlook.
3. Restart all the Enterprise Vault services.

Securing Enterprise Vault web applications

The Enterprise Vault web applications are configured in the Default Web Site in IIS. By default in a new installation of Enterprise Vault 12.3 or later, Enterprise Vault configures HTTPS on port 443, and enables SSL on each Enterprise Vault virtual directory.

When you upgrade from a version that is earlier than Enterprise Vault 12.3, the existing configuration of the Default Web Site and Enterprise Vault virtual directories remains unchanged. To ensure the security of connections to Enterprise Vault web applications, we strongly recommend that you manually configure an HTTPS binding on the Default Web Site, and enable SSL on the Enterprise Vault virtual directories. The procedure below explains how to do this.

The port and protocol that clients use to access the `EnterpriseVault` virtual directory is displayed on the **General** tab of site properties in the Enterprise Vault Administration Console. Before you change this setting, you must first make the

required changes to the Default Web Site in IIS for each server in the Enterprise Vault site.

If you change the port or protocol setting in site properties after items have been archived, existing shortcuts will no longer work. Shortcuts in Outlook and Notes can be updated with the new protocol or port information by synchronizing mailboxes in the Enterprise Vault Administration Console, but customized shortcuts, FSA shortcuts and SharePoint shortcuts cannot be updated.

To create a certificate request, and implement SSL in IIS

1. Create and submit an SSL certificate request to a trusted certificate authority. Your certificate must include both the short names and fully qualified domain names of the Vault Site alias (that is, the DNS alias for the Enterprise Vault site). For example, **EVServer1** and **EVServer1.domain.com**.

   You can use any suitable tool to request the certificate. For example, you can use OpenSSL, which is installed in the Enterprise Vault installation folder. How to create a certificate request using Microsoft Management Console (MMC) is described in the document, https://www.veritas.com/docs/100038186.

2. On the Enterprise Vault server, perform the following steps in IIS Manager:

   - Use the **Server Certificates** feature to install the new certificate.
   - In the site bindings for the Default Web Site, add a binding for the HTTPS protocol and link it to the new certificate. Bear in mind, if you change the protocol or port for the Default Web Site, it will affect all virtual directories in the website.
   - In the **SSL Settings** pane for each Enterprise Vault virtual directory, select **Require SSL**.

   These tasks are also described in the document, https://www.veritas.com/support/en_US/doc/85434533-129299639-0/index.

3. When you have made the necessary changes in IIS, change the port or protocol setting on the **General** tab of site properties in the Enterprise Vault Administration Console.

Weak protocols and ciphers are blocked

In a new installation of Enterprise Vault 12.4 or later, or an upgrade to Enterprise Vault 12.4 or later, the Enterprise Vault installer now disables weak protocols and ciphers. Enterprise Vault disables the following protocols, if you have not enabled them manually:

- SSL 2.0

- SSL 3.0
- TLS 1.0

Weak protocols are managed using registry settings under `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols`. If you have manually enabled the weak protocols listed above, a registry setting will exist under the `Protocols` subkey. Enterprise Vault does not disable a protocol that you have enabled in this way.

Enterprise Vault disables the following ciphers:

- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Ciphers are managed using registry settings under `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Cryptography\Configuration\SSL\00010002`. Enterprise Vault disables all of the weak ciphers listed above, even if you have enabled any of them using a registry setting under the `Ciphers` subkey.

Improved consistency when applying a retention period to items

Changes to the Vault Administration Console provide improved consistency and clarity in the way that Enterprise Vault applies a retention period to items. Some of these changes include changes to default behavior.

Table 3-2 Changes to Administration Console elements

Administration Console element	Changes made
Exchange Mailbox Policy dialog box > Existing Items tab	This tab has been removed. The settings on the tab related to how retention was assigned to items whose shortcuts were moved from one mailbox folder to another. The settings also applied to existing shortcut items in the mailbox folder. On the **Archive Settings** tab of the **Site Properties** dialog box, the **Update the category for existing items** setting also controlled how retention was assigned to such items. The various setting names and their combined effect caused confusion. In this release, the item movement behavior has been standardized across Enterprise Vault. That is: ■ The location of a moved item is always updated. See "Limiting the impact when updating moved item locations" on page 22. ■ The category of a moved item is updated. This is subject to site archive settings and classification policy settings. ■ The category of other, existing items in the folder is never changed. ■ The category of a moved item is updated, even if the original category was selected by a user, set by a custom filter, or set by PST migration. Again, this is subject to site archive settings and classification policy settings.
Site Properties dialog box > Archive Settings tab	The Allow user actions to update categories setting on this tab determines whether, when users perform actions that could potentially update the retention categories of their archived items, Enterprise Vault allows the updates to take place. For example, users may move archived items between folders to which you have applied different retention categories, or change the retention categories of items in Enterprise Vault Search, if permitted. Both actions can cause the retention categories of the items to change. The following options now let you control when Enterprise Vault updates the retention category of such items: ■ **Always** ■ **If item expiry is the same or later, or the record type changes**

Table 3-2 Changes to Administration Console elements *(continued)*

Administration Console element	Changes made
Classification Policy Properties dialog box > Settings tab	This tab now provides an option, **Prevent user actions from updating retention categories**, with which you can block unwanted changes to the retention categories that the Enterprise Vault classification feature has assigned to archived items. For example, users can potentially update the retention categories by moving the items from one folder to another. You can choose to block retention category updates in all instances or, if you use the Enterprise Vault records management feature, you can allow them in instances where this also causes the record types of the items to change.
Retention Category Properties dialog box > Details tab	The following options are available on this tab: ■ **Prevent automatic deletion of expired items with this category** ■ **Prevent user deletion of items with this category** Consider the following situation: ■ An item in a mailbox folder has a retention category with a hold set on automatic deletion of expired items. ■ The user moves the item shortcut to a folder that has a different category assigned. The folder category does not have any holds set. In previous releases, Enterprise Vault did not update the category in this situation. This behavior has now changed. Enterprise Vault updates the item category, subject to site and classification policy settings for allowing user actions to update categories on items. In this example, updating the category means that the hold on automatic deletion on expiry is removed. Similarly, a user action may cause a change of retention category from one that specifies a hold on user deletion to one that does not. This can lead to the removal of the hold on user deletion.
Search Policy Properties dialog box > Features tab	This tab now contains an option, **Allow Retention Category to be changed**, with which you can allow Enterprise Vault Search users to change the retention categories of the items in their archives. By default, this option is turned off. This setting is subject to the site and classification policy settings that are described above.

For an overview of retention in Enterprise Vault 14.2 and later, see the technical note Managing Retention.

Limiting the impact when updating moved item locations

Previously, you could prevent Enterprise Vault from updating an item's location in the archive when a user moved the shortcut to a different folder in their mailbox. To disable this feature, you cleared **Update archive location for items moved in the mailbox** in the Exchange Mailbox policy.

In this release, Enterprise Vault always updates the archive location of moved items. If you had previously disabled this feature, and mailboxes contain lots of shortcuts, then Enterprise Vault attempts to update the archive location for moved items after you upgrade. If the mailboxes include historical shortcuts to Enterprise Vault servers that are no longer reachable, then long network timeouts may occur.

To prevent these timeouts, configure a list of valid site aliases as described in the following procedure.

Configuring a list of valid site aliases

1. In the Enterprise Vault Administration Console, open the **Advanced** tab in the Exchange Mailbox policy.
2. In **List settings from:**, select **Archiving General**.
3. Select **Valid Enterprise Vault site aliases** and click **Modify**.
4. Enter a semi-colon separated list of valid site aliases. During shortcut processing, Enterprise Vault does not attempt to contact any site whose alias does not appear in the list.
5. Click **OK** to close the dialog box, and then again to close the properties.
6. Repeat the above steps for each Exchange Mailbox policy.

Automatic migration of NetApp C-Mode connection settings

Previously, you could configure NetApp C-Mode connection settings only at the server-level using registry settings. In Enterprise Vault 12.4 and later, these settings have moved to the advanced File System Archiving site setting and the advanced File System Archiving computer setting in the Enterprise Vault Administration Console. This provides a convenient way to configure the setting at the site-level and then apply common configuration across all the servers in the site.

These settings are as follows:

- NetApp C-Mode server certificate verification
  This is the equivalent of the `CModeIgnoreServerCertVerification` registry setting.
- NetApp C-Mode server port number
  This is the equivalent of the `CModeServerPort` registry setting.
- NetApp C-Mode server transport type
  This is the equivalent of the `CModeServerTransportStyle` registry setting.
- Use site settings for NetApp C-Mode server configuration
  This setting is only available in the computer properties advanced settings. The value is set to **No** on servers where you had previously configured connection settings.

During the upgrade process, the NetApp C-Mode connection settings are added to each site with default values. If you previously configured registry settings on any Enterprise Vault servers, the setting values are populated on each server accordingly during upgrade. After the upgrade, the registry keys are no longer available.

Enterprise Vault auditing configuration

In Enterprise Vault 12.3 and earlier releases, you could configure auditing settings only at the server-level. Enterprise Vault 12.4 onwards, you can configure auditing at the site-level. The **Configure Auditing** option in the Enterprise Vault servers container in the Administration Console lets you enable and configure auditing for all the available Enterprise Vault servers in the site. Note that the option to enable auditing is no longer available from the **Auditing** tab of the **Computer Properties** of the Enterprise Vault server.

In Enterprise Vault 12.3 and earlier, the auditing configuration was stored as registry settings under `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KVS\Enterprise Vault\Admin\Auditing` on each server. During the upgrade to Enterprise Vault 12.4 or later, these settings are migrated from each server's registry to the Enterprise Vault Directory database. After the successful migration of the settings, these registry keys are no longer available.

Note that auditing category settings are stored at the server-level whereas connection pool size settings are available at the site-level only. You can no longer configure separate connection pool sizes at the server-level. If you previously configured different connection pool sizes for each server, then the upgrade process stores the minimum configured value as the default connection pool size

at the site-level, which applies to all the servers in the site. For example, if the Indexing service connection pool size for EVServer1 was 6, and the Indexing service connection pool size for EVServer2 was 3, then the upgrade process chooses 3 as the default Indexing service connection pool size. Additionally, if you had turned on connection information logging for any of the servers, then the **Log database information** option is enabled for all the servers in the site.

Amazon Simple Storage Service (S3) partition

In case a primary vault store or smart partition is created for Amazon Simple Storage Service (S3) in Enterprise Vault 14.0, you must provide additional permissions when the IAM Role or STS Assume Role authentication is used before you upgrade to Enterprise Vault 14.1.

For details, refer to Using Amazon Simple Storage Service (S3) as a primary storage for Enterprise Vault.

Classification using Microsoft File Classification Infrastructure on Windows Server 2016 and 2019

Enterprise Vault classification using the Microsoft File Classification Infrastructure is not supported on Windows Server 2016 and 2019.

Data Classification Services does not support all the types of retention categories available in Enterprise Vault 14.2 and later

Enterprise Vault 12.2 introduced the option to configure retention categories that have a fixed expiry date rather than a retention period. For example, you can create a retention category that has a fixed expiry date of 31 December 2021, and then assign the retention category to the items that you want to expire on this date.

The Enterprise Vault Data Classification Services feature does not support retention categories with fixed expiry dates. Therefore, when you define the list of available retention categories in Data Classification Services, you must omit those that have fixed expiry dates.

Managing certificates for Enterprise Vault Cloud Storage Adapter

Certificate file for Enterprise Vault Cloud Storage Adapter, which stores the PEM certificates, gets overwritten during the Enterprise Vault upgrade.

In order to retain the certificates that you have explicitly added, follow steps mentioned in following knowledge base article:

https://www.veritas.com/content/support/en_US/article.100051774

eDiscovery Platform compatibility with Enterprise Vault

Before you upgrade Enterprise Vault, see the eDiscovery Platform Compatibility Matrix for details of compatibility with Enterprise Vault.

Chapter 4

Steps to upgrade your system

This chapter includes the following topics:

- Overview of the upgrade process

Overview of the upgrade process

Overview of the upgrade process

1. If your environment includes Surveillance or eDiscovery, familiarize yourself with the order in which you must upgrade these applications and Enterprise Vault.

   See "Order of upgrade in an environment with Surveillance or eDiscovery" on page 15.

2. Prepare the Enterprise Vault servers for the upgrade:

   See "About Enterprise Vault server preparation" on page 28.

3. Install and configure the Enterprise Vault server software as described in the appropriate chapter for your installation.

   See "About upgrading a single Enterprise Vault server" on page 33.

   See "About upgrading multiple Enterprise Vault servers" on page 39.

   See "About upgrading an Arctera cluster" on page 45.

   See "About upgrading a Windows Server Failover Cluster" on page 51.

4. Upgrade any computers that are running just the Enterprise Vault Administration Console.

   See "About upgrading standalone Administration Consoles" on page 58.

5 Upgrade any computers that are running Enterprise Vault Reporting.

See "Upgrading Enterprise Vault Reporting" on page 61.

6 Perform the post-installation tasks as necessary:

- Upgrade MOM and SCOM.
  See "Upgrading MOM" on page 64.
- Upgrade Exchange Server forms.
  See "About upgrading Exchange Server forms" on page 66.
- Upgrade Domino mailbox archiving.
  See "About upgrading Domino mailbox archiving" on page 67.
- Upgrade the FSA Agent on the Windows servers on which it is installed.
  See "About upgrading the FSA Agent" on page 74.
- Upgrade the Enterprise Vault Office Mail App.
  See "About upgrading Enterprise Vault Office Mail App" on page 81.
- Upgrade SharePoint Server components.
  See "About upgrading the SharePoint components" on page 82.
- Upgrade SMTP archiving.
  See "Checking the permissions of the SMTP Archiving task account" on page 91.
- Upgrade your Enterprise Vault sites to use Enterprise Vault Search.
  See "About Enterprise Vault Search" on page 98.
- Upgrade Enterprise Vault API applications.
  See "Upgrading any applications that use the Enterprise Vault API Runtime" on page 113.

Chapter 5

Enterprise Vault server preparation

This chapter includes the following topics:

- About Enterprise Vault server preparation
- Backing up the system
- Updating required Windows features
- Running Enterprise Vault Deployment Scanner
- Setting database permissions
- Allowing the MSMQ queues to empty
- Checking the archiving and expiry schedules

About Enterprise Vault server preparation

Before you upgrade the Enterprise Vault software you must prepare for the upgrade, as described in this chapter.

Perform the following actions in the order they are listed:

- Back up the system.
  See "Backing up the system" on page 29.
- Run Enterprise Vault Deployment Scanner.
  See "Running Enterprise Vault Deployment Scanner" on page 30.
- Set database permissions.
  See "Setting database permissions" on page 31.
- Allow the MSMQ queues to empty.

See "Allowing the MSMQ queues to empty" on page 31.

- Check the archiving and expiry schedules.
  See "Checking the archiving and expiry schedules" on page 32.
- Configure valid site aliases to limit the impact when Enterprise Vault updates the archive location of moved items.
  See "Improved consistency when applying a retention period to items" on page 19.

Backing up the system

You need to back up your Enterprise Vault data and any changed language files.

If you use SCOM, you may want to back up the management pack.

Backing up Enterprise Vault data

Before upgrading your Enterprise Vault environment, back up all Enterprise Vault data in accordance with your normal backup procedures.

See the *Backup and Recovery* guide.

Note: When you back up your databases, perform the recommended database maintenance steps that are described in the following technical note on the Arctera Support website:

https://www.veritas.com/docs/100022023

These maintenance steps shrink the database, rebuild the table indexes, and update the database statistics. Such actions enable the upgrade of the databases to proceed more quickly.

When you have backed up your vault store partitions, the Storage service marks the relevant files as backed up, and this removes the entries from the WatchFile table. The Storage service performs these tasks at preconfigured intervals. You should wait for the WatchFile table to reduce in size before you proceed with the upgrade. If you do not wait, the Storage service can take some time to restart after the upgrade is complete. You can use the usage report at http://*evserver*/enterprisevault/usage.asp to check the number of files in the **Awaiting Backup** column.

Backing up changed language files

The installation procedure overwrites the files in the following Enterprise Vault server language folders:

`Enterprise Vault\Languages\Mailbox Messages\`*`language`*

Where *`language`* indicates the language used.

The installation does not modify the live versions of these files that you have in the Enterprise Vault folder, for example `C:\Program Files (x86)\Enterprise Vault`.

If you have made changes that you want to keep to the files in the language folders, copy the files to another location.

Updating required Windows features

The Enterprise Vault Install Launcher can automatically check that a server has the required Windows features and can add any features that are missing.

For details of the features that the Install Launcher can add, see "Automatically preparing an Enterprise Vault server" in the *Installing and Configuring* guide.

To run the Prepare My System option

1. Load the Enterprise Vault media on to the server.
2. If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.

   If AutoPlay is not enabled, use Windows Explorer to open the root folder of the installation media and then double-click the file `Setup.exe`.

   The Install Launcher opens.
3. In the list in the left pane of the Install Launcher, click **Enterprise Vault**.
4. Click **Server Preparation**.
5. Click **Windows features**, and then click **Prepare my system**. The Windows features are added immediately, with no further prompts. The server may restart automatically after the features have been added.

Running Enterprise Vault Deployment Scanner

Before you upgrade Enterprise Vault, we strongly recommend that you run Deployment Scanner to check required software and settings.

Use the Vault Service account when running Deployment Scanner.

Note: If you choose to check SQL Server, the report may show a warning that "SQL databases contain entities with mixed collations". See the following technical note for details of how to fix the problem:

https://www.veritas.com/docs/100023860

If you make changes to your configuration as a result of running Deployment Scanner, repeat your system backup if necessary.

To run the Deployment Scanner

1. Log in to the Vault Service account.
2. Load the Enterprise Vault media.
3. If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.

   If AutoPlay is not enabled, use Windows Explorer to open the root folder of the installation media and then double-click the file `Setup.exe`.
4. In the left pane of the **Arctera Enterprise Vault Install Launcher** window, click **Enterprise Vault** and then click **Server Preparation**.
5. In the right pane, click **Deployment Scanner** and then click **Run the Deployment Scanner**. The Deployment Scanner starts.

Setting database permissions

Before you upgrade Enterprise Vault, you must ensure that the Vault Service account has all the necessary permissions.

You can verify the Vault Service account's permissions against the procedure in "Creating a SQL login account", in the *Installing and Configuring* guide.

Allowing the MSMQ queues to empty

Before you upgrade Enterprise Vault, we recommend that you allow the MSMQ queues to empty. If you upgrade Enterprise Vault with items still on the queues, the Enterprise Vault services may log error events the first time they start after the upgrade.

Checking the archiving and expiry schedules

To allow time to examine the new installation before archiving starts, you may want to disable archiving and expiry before you upgrade the servers. You can enable the servers again when you have checked the installation.

Chapter 6

Single server: upgrading the Enterprise Vault server software

This chapter includes the following topics:

- About upgrading a single Enterprise Vault server
- Installing on a single server
- Upgrading the Enterprise Vault databases
- Backing up the upgraded Enterprise Vault databases
- Configuring index data location
- Starting all the Enterprise Vault services

About upgrading a single Enterprise Vault server

This chapter describes how to upgrade the Enterprise Vault server software and databases when you have only one server that runs Enterprise Vault services.

Perform the procedures in this chapter in the order that they are listed.

Installing on a single server

This section describes how to install the Enterprise Vault server software when you have only one server that runs Enterprise Vault services.

Preparation

To prepare to upgrade the Enterprise Vault server software on a single server

1. Log on to the Enterprise Vault server as the Vault Service account.
2. Stop the Enterprise Vault Admin service. This stops the Admin service itself, and any other Enterprise Vault services.
3. Stop any other local or remote services or applications that can lock Enterprise Vault files. For example:
   - Enterprise Vault Administration Console
   - Enterprise Vault Accelerator Manager service
4. Close any other applications that may be running on the server, including the Control Panel, Computer Management, Windows Services, and the Windows Event Viewer.
5. If you are installing on an Enterprise Vault Domino Gateway, make sure that the Domino server on the Enterprise Vault Domino Gateway is shut down and that `EVInstall.nsf` is not being accessed locally.

Installing Enterprise Vault (wizard)

To use the wizard to install Enterprise Vault

1. Load the Enterprise Vault media.
2. If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.

   If AutoPlay is not enabled, use Windows Explorer to open the root folder of the installation media and then double-click the file `Setup.exe`.
3. In the list in the left pane of the **Arctera Enterprise Vault Install Launcher** window, click **Enterprise Vault**.
4. Click **Server Installation**.
5. In the right pane, click **Upgrade existing server**.
6. Click **Install**. The Enterprise Vault installation wizard starts.
7. Work through the installation wizard to upgrade the Enterprise Vault components.
8. If the installation wizard prompts you to restart the server, restart and then log on again as the Vault Service account so that the installer can complete the upgrade.

Installing Enterprise Vault (command line)

The following procedure describes how to upgrade the Enterprise Vault installation. If you want to add or remove components, see the "Installing Enterprise Vault" chapter in the *Installing and Configuring* guide for a complete description of the command-line options.

Caution: If a system restart is needed during silent installation, the server restarts automatically. If the server restarts, log on again as the Vault Service account so that the installer can complete the upgrade.

To install Enterprise Vault from the command line

1. Log on to the Enterprise Vault server as the Vault Service account.
2. Load the Enterprise Vault media.
3. If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Close the AutoPlay dialog box.
4. Open a command prompt window and navigate to the following folder on the Enterprise Vault media:

   ```
   \Arctera Enterprise Vault\Server\x64
   ```

5. Run `setup (x64).exe` as follows:

   ```
   start /wait "" "setup (x64).exe" /s /clone_wait
   /v"COMPONENTS=Option[|Option][...]"
   ```

6. If the server restarts, log on again as the Vault Service account so that the installer can complete the upgrade.

Upgrading the Enterprise Vault databases

Before you start any Enterprise Vault services on the target server, you must upgrade the Enterprise Vault databases.

Note: After upgrading Enterprise Vault databases to version 14.2 or later, all the existing index locations will be closed for new index additions. A new index location must be configured to store new Elasticsearch indexes. The Enterprise Vault Indexing service does not start until a new index location has been configured.

Enterprise Vault provides a PowerShell cmdlet called `Start-EVDatabaseUpgrade`, which you can use to upgrade all Enterprise Vault databases.

The upgrade of the Directory database schema requires additional disk space on the SQL Server computer, mainly for log file growth. You can reclaim most of this additional space by routine database maintenance after the upgrade.

The required amount of space for the upgrade depends on which recovery model the database uses.

Table 6-1 lists the additional space requirements.

Table 6-1 Space required for the upgrade of the Directory database

Directory database recovery model	Required additional space on the volume that holds the database transaction log files
Simple or Bulk-logged	Twice the combined size of the Directory database data files
Full	Four times the combined size of the Directory database data files

Note: Enterprise Vault does not let you proceed with the upgrade unless this additional space is available.

These estimated space requirements are based on the assumption that you perform the recommended maintenance activities when you back up the database before the upgrade.

See "Backing up the upgraded Enterprise Vault databases" on page 37.

The upgrade of a large Directory database may take a long time to complete. The upgrade time depends on the size of the database, the database recovery model, the upgrade path, and the available resources.

To upgrade Enterprise Vault's databases

1 On the target Enterprise Vault server, log in using the Vault Service account.

2 Run the Enterprise Vault Management Shell.

3 In the Enterprise Vault Management Shell, run the following command:

```
Start-EVDatabaseUpgrade
```

Note that you can also run `Start-EVDatabaseUpgrade -verbose` if you want to see detailed output.

4 Wait for `Start-EVDatabaseUpgrade` to complete the upgrade of all the databases.

When the upgrade is complete, you can examine the upgrade reports for errors.

`Start-EVDatabaseUpgrade` writes the reports in the `Reports\DBUpgrade` subfolder of the Enterprise Vault installation folder (for example `C:\Program Files (x86)\Enterprise Vault`).

Backing up the upgraded Enterprise Vault databases

Back up the upgraded Enterprise Vault databases as follows.

To back up the upgraded Enterprise Vault databases

1. Stop any running Enterprise Vault services on the Enterprise Vault server.
2. Back up all Enterprise Vault databases.

Configuring index data location

The Enterprise Vault administrator must configure an index data location from the Enterprise Vault Administration Console or by running the Getting Started wizard. The Enterprise Vault Admin service and the Enterprise Vault Directory service must be running before configuring the index data location.

To set up the Enterprise Vault index data location through Enterprise Vault Administration Console, perform the following steps:

1. In the left pane, expand the Enterprise Vault site hierarchy until the Indexing container is visible.
2. Expand the Indexing container.
3. Expand the index server to which you want to add an index data location.
4. Right-click the index server, click **Properties**, and then click the **Elasticsearch Index Locations** tab.
5. Click **Browse** to choose an empty folder in which index data can be stored.
6. Click **OK** to apply the changes.
7. Start Enterprise Vault indexing service once the configuration is done.

If you want to backup the newly created Elasticsearch indexes, you first need to set up an index snapshot location through PowerShell using the following steps:

1. Run the Enterprise Vault Management Shell.
2. In the Enterprise Vault Management Shell, run the following command:

   ```
   Set-EVIndexSnapshotLocation -SnapshotLocationPath "I:\"
   ```

   For more information, see the *PowerShell Cmdlets* guide.

3. Restart the Enterprise Vault Indexing service.

Starting all the Enterprise Vault services

Start all the Enterprise Vault services on the target server.

Chapter 7

Multiple servers: upgrading the Enterprise Vault server software

This chapter includes the following topics:

- About upgrading multiple Enterprise Vault servers
- Installing on multiple servers
- Upgrading the Enterprise Vault databases
- Backing up the upgraded Enterprise Vault databases
- Configuring index data location
- Starting all the Enterprise Vault services

About upgrading multiple Enterprise Vault servers

This chapter describes how to upgrade the Enterprise Vault server software and databases, when you have multiple servers that run Enterprise Vault services.

Perform the procedures in this chapter in the order that they are listed.

Installing on multiple servers

The following procedure describes how to install the Enterprise Vault server software on all the servers that run Enterprise Vault services.

Perform the following procedure on each computer on which the Enterprise Vault services are installed.

Preparation

To prepare to upgrade the Enterprise Vault server software

1. Log on to the Enterprise Vault server as the Vault Service account.
2. Stop the Enterprise Vault Admin service. This stops the Admin service itself, and any other Enterprise Vault services.
3. Stop any other local or remote services or applications that can lock Enterprise Vault files. For example:
   - Enterprise Vault Administration Console
   - Enterprise Vault Accelerator Manager service
4. Close any other applications that may be running on the server, including the Control Panel, Computer Management, Windows Services, and the Windows Event Viewer.
5. If you are installing on an Enterprise Vault Domino Gateway, make sure that the Domino server on the Enterprise Vault Domino Gateway is shut down and that `EVInstall.nsf` is not being accessed locally.

Installing Enterprise Vault (wizard)

To use the wizard to install Enterprise Vault

1. Load the Enterprise Vault media.
2. If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.

   If AutoPlay is not enabled, use Windows Explorer to open the root folder of the installation media and then double-click the file `Setup.exe`.
3. In the list in the left pane of the **Arctera Enterprise Vault Install Launcher** window, click **Enterprise Vault**.
4. Click **Server Installation**.
5. In the right pane, click **Upgrade existing server**.
6. Click **Install**. The Enterprise Vault installation wizard starts.
7. Work through the installation wizard to upgrade the Enterprise Vault components.

8 If the installation wizard prompts you to restart the server, restart and then log on again as the Vault Service account so that the installer can complete the upgrade.

9 When the installation is complete, the installer re-enables the Enterprise Vault services. Do not start any Enterprise Vault services at this time.

Installing Enterprise Vault (command line)

The following procedure describes how to upgrade the Enterprise Vault installation. If you want to add or remove components, see the "Installing Enterprise Vault" chapter in the *Installing and Configuring* guide for a complete description of the command-line options.

Caution: If a system restart is needed during silent installation, the server restarts automatically. If the server restarts, log on again as the Vault Service account so that the installer can complete the upgrade.

To install Enterprise Vault from the command line

1 Log on to the Enterprise Vault server as the Vault Service account.

2 Load the Enterprise Vault media.

3 If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Close the AutoPlay dialog box.

4 Open a Command Prompt window and navigate to the following folder on the Enterprise Vault media:

```
\Arctera Enterprise Vault\Server\x64
```

5 Run `setup (x64).exe` as follows:

```
start /wait "" "setup (x64).exe" /s /clone_wait
/v"COMPONENTS=Option[|Option][...]"
```

6 If the server restarts, log on again as the Vault Service account so that the installer can complete the upgrade.

7 When the installation is complete, the installer re-enables the Enterprise Vault services. Do not start any Enterprise Vault services at this time.

8 Repeat this procedure on every computer on which the Enterprise Vault services are installed.

Upgrading the Enterprise Vault databases

Before you start any Enterprise Vault services, you must upgrade the Enterprise Vault databases.

Note: You only need to complete this procedure on one Enterprise Vault server.

Enterprise Vault provides a PowerShell cmdlet called `Start-EVDatabaseUpgrade`, which you can use to upgrade all Enterprise Vault databases.

Note: After upgrading Enterprise Vault databases to version 14.2 and later, all the existing index locations will be closed for new index additions. A new index location must be configured to store new Elasticsearch indexes. The Enterprise Vault Indexing service does not start until a new index location has been configured.

The upgrade of the Directory database schema requires additional disk space on the SQL Server computer, mainly for log file growth. You can reclaim most of this additional space by routine database maintenance after the upgrade.

The required amount of space for the upgrade depends on which recovery model the database uses.

Table 7-1 lists the additional space requirements.

Table 7-1 Space required for the upgrade of the Directory database

Directory database recovery model	Required additional space on the volume that holds the database transaction log files
Simple or Bulk-logged	Twice the combined size of the Directory database data files
Full	Four times the combined size of the Directory database data files

---

Note: Enterprise Vault does not let you proceed with the upgrade unless this additional space is available.

These estimated space requirements are based on the assumption that you perform the recommended maintenance activities when you back up the database before the upgrade.

See "Backing up the upgraded Enterprise Vault databases" on page 43.

The upgrade of a large Directory database may take a long time to complete. The upgrade time depends on the size of the database, the database recovery model, the upgrade path, and the available resources.

To upgrade Enterprise Vault's databases

1. On any Enterprise Vault server, log in using the Vault Service account.
2. Run the Enterprise Vault Management Shell.
3. In the Enterprise Vault Management Shell, run the following command:

   ```
   Start-EVDatabaseUpgrade
   ```

   Note that you can also run `Start-EVDatabaseUpgrade -verbose` if you want to see detailed output.
4. Wait for `Start-EVDatabaseUpgrade` to complete the upgrade of all the databases.

When the upgrade is complete, you can examine the upgrade reports for errors.

`Start-EVDatabaseUpgrade` writes the reports in the `Reports\DBUpgrade` subfolder of the Enterprise Vault installation folder (for example `C:\Program Files (x86)\Enterprise Vault`).

Backing up the upgraded Enterprise Vault databases

Back up the upgraded Enterprise Vault databases as follows.

To back up the upgraded Enterprise Vault databases

1. Stop any running Enterprise Vault services on the Enterprise Vault servers.
2. Back up all Enterprise Vault databases.

Configuring index data location

The Enterprise Vault administrator must configure an index data location from the Enterprise Vault Administration Console or by running the Getting Started wizard. The Enterprise Vault Admin service and the Enterprise Vault Directory service must be running before configuring the index data location.

To set up the Enterprise Vault index data location through Enterprise Vault Administration Console, perform the following steps:

1. In the left pane, expand the Enterprise Vault site hierarchy until the Indexing container is visible.
2. Expand the Indexing container.

3. Expand the index server to which you want to add an index data location.
4. Right-click the index server, click **Properties**, and then click the **Elasticsearch Index Locations** tab.
5. Click **Browse** to choose an empty folder in which index data can be stored.
6. Click **OK** to apply the changes.
7. Start Enterprise Vault indexing service once the configuration is done.
8. Repeat this procedure on every computer on which the Enterprise Vault Indexing service is installed.

If you want to backup the newly created Elasticsearch indexes, you first need to set up an index snapshot location through PowerShell using the following steps:

1. Run the Enterprise Vault Management Shell.
2. In the Enterprise Vault Management Shell, run the following command:

   ```
   Set-EVIndexSnapshotLocation -SnapshotLocationPath "I:\" -SiteId
   <EV site id>
   ```

   For more information, see the *PowerShell Cmdlets* guide.
3. Restart the Enterprise Vault Indexing service on every computer on which the Enterprise Vault Indexing service is installed..

Starting all the Enterprise Vault services

Start all the Enterprise Vault services on all the Enterprise Vault servers in the site.

Chapter 8

Arctera Cluster Server: upgrading the Enterprise Vault server software

This chapter includes the following topics:

- About upgrading an Arctera cluster
- Installing the Enterprise Vault server software
- Upgrading the Enterprise Vault databases
- Backing up the upgraded Enterprise Vault databases
- Configuring index data location
- Starting all the Enterprise Vault services

About upgrading an Arctera cluster

This chapter describes how to upgrade the Enterprise Vault server software and databases, when the servers that run Enterprise Vault tasks are part of an Arctera cluster.

Perform the procedures in this chapter in the order that they are listed.

Installing the Enterprise Vault server software

This section describes how to install the Enterprise Vault server software when the servers that run Enterprise Vault tasks are part of an Arctera cluster.

Note that Enterprise Vault does not support high-availability upgrades. You must install the server software on all nodes in the cluster before you start Enterprise Vault services or run the configuration wizard.

Preparation

To prepare to upgrade the Enterprise Vault server software

1. Log on to the active node as the Vault Service account.
2. Use the VCS cluster administration tools to take all the Enterprise Vault service resources offline.

   Note the following important points:

   - You must stop all Enterprise Vault services in the Enterprise Vault site. For example, stop the services on non-clustered servers, such as an Enterprise Vault Domino Gateway.
   - If you install on an Enterprise Vault Domino Gateway, make sure that the Domino server on the Enterprise Vault Domino Gateway is shut down and that `EVInstall.nsf` is not accessed locally.
   - If there are multiple sites that share the Enterprise Vault Directory, you must also stop all Enterprise Vault services in the other sites.
3. Stop any other local or remote services or applications that can lock Enterprise Vault files. For example:
   - Enterprise Vault Administration Console
   - Enterprise Vault Accelerator Manager service
4. Close any applications that may be running on the server, including the Control Panel, Computer Management, Windows Services, and the Windows Event Viewer.

To prepare to upgrade to Enterprise Vault 15.0 or later from EV 14.x with standalone Enterprise Vault Usage Analyzer

Before upgrading to Enterprise Vault 15.0 or later from EV 14.x with the standalone Enterprise Vault Usage Analyzer (EVUA), you need to perform the following steps to remove EVUA Service from the VCS cluster:

1. Start the **VCS Cluster Manager**.
2. Login with cluster administrator credentials. On successful login, the **Cluster Explorer** window is launched.
3. In **Cluster Explorer**, navigate to the existing **Service Group > GenericService**.

   Check if **EVUsageAnalyzerService** is present.

4. Right-click **EVUsageAnalyzerService** and select **Offline** to bring the service offline.
5. Once the service is offline, right-click **EVUsageAnalyzerService** and select **Unlink**.

   Click **Yes** if prompted to switch to read/write mode.
6. Click **OK** on the **Unlink Resource** prompt.
7. Right-click **EVUsageAnalyzerService** and select **Delete**.
8. Click **OK** to confirm deletion.
9. Once **EVUSageAnalyzerService** is deleted from **Generic Service**, right-click on the root node and select **Save Configuration**.
10. Right-click on the root node and select **Close Configuration** to switch to read-only mode.
11. Proceed with upgrading to Enterprise Vault 15.0 or later.

Installing Enterprise Vault (wizard)

To use the wizard to install Enterprise Vault

1 Load the Enterprise Vault media.

2 If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.

   If AutoPlay is not enabled, use Windows Explorer to open the root folder of the installation media and then double-click the file `Setup.exe`.

3 In the list in the left pane of the **Arctera Enterprise Vault Install Launcher** window, click **Enterprise Vault**.

4 Click **Server Installation**.

5 In the right pane, click **Upgrade existing server**.

6 Click **Install**. The Enterprise Vault installation wizard starts.

7 Work through the installation wizard to upgrade the Enterprise Vault components.

8 If the installation wizard prompts you to restart the server, restart and then log on again as the Vault Service account so that the installer can complete the upgrade.

9 Install the Enterprise Vault software on the other servers in your Enterprise Vault environment, including any cluster failover nodes.

Installing Enterprise Vault (command line)

The following procedure describes how to upgrade the Enterprise Vault installation. If you want to add or remove components, see the "Installing Enterprise Vault" chapter in the *Installing and Configuring* guide for a complete description of the command-line options.

Caution: If a system restart is needed during silent installation, the server restarts automatically. If the server restarts, log on again as the Vault Service account so that the installer can complete the upgrade.

To install Enterprise Vault from the command line

1. Log on to the active node as the Vault Service account.
2. Load the Enterprise Vault media.
3. If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Close the AutoPlay dialog box.
4. Open a command prompt window and navigate to the following folder on the Enterprise Vault media:

   ```
   \Arctera Enterprise Vault\Server\x64
   ```

5. Run `setup (x64).exe` as follows:

   ```
   start /wait "" "setup (x64).exe" /s /clone_wait /v"COMPONENTS=
   Option [| Option ][...]"
   ```

6. When the installation is complete, the installer re-enables the Enterprise Vault services. Do not start any Enterprise Vault services at this time.
7. Install the Enterprise Vault software on the other servers in your Enterprise Vault environment, including any cluster failover nodes.

Upgrading the Enterprise Vault databases

Before you start any Enterprise Vault services, you must upgrade the Enterprise Vault databases.

Note: You only need to complete this procedure on the active node.

Enterprise Vault provides a PowerShell cmdlet called `Start-EVDatabaseUpgrade`, which you can use to upgrade all Enterprise Vault databases.

Note: After upgrading Enterprise Vault databases to version 14.2 and later, all the existing index locations will be closed for new index additions. A new index location must be configured to store new Elasticsearch indexes. The Enterprise Vault Indexing service does not start until a new index location has been configured.

To upgrade Enterprise Vault's databases

1. On the active node, log in using the Vault Service account.
2. Run the Enterprise Vault Management Shell.
3. In the Enterprise Vault Management Shell, run the following command:

   ```
   Start-EVDatabaseUpgrade
   ```

   Note that you can also run `Start-EVDatabaseUpgrade -verbose` if you want to see detailed output.
4. Wait for `Start-EVDatabaseUpgrade` to complete the upgrade of all the databases.

When the upgrade is complete, you can examine the upgrade reports for errors.

`Start-EVDatabaseUpgrade` writes the reports in the `Reports\DBUpgrade` subfolder of the Enterprise Vault installation folder (for example `C:\Program Files (x86)\Enterprise Vault`).

Backing up the upgraded Enterprise Vault databases

Back up the upgraded Enterprise Vault databases as follows.

To back up the upgraded Enterprise Vault databases

1. Use the cluster administration tool to take any running Enterprise Vault services offline.
2. Back up all Enterprise Vault databases.

Configuring index data location

Note: You must complete this procedure on the active node.

The Enterprise Vault administrator must configure an index data location from the Enterprise Vault Administration Console or by running the Getting Started

wizard. The Enterprise Vault Admin service and the Enterprise Vault Directory service must be running before configuring the index data location.

To set up the Enterprise Vault index data location through Enterprise Vault Administration Console, perform the following steps:

1. In the left pane, expand the Enterprise Vault site hierarchy until the Indexing container is visible.
2. Expand the Indexing container.
3. Expand the index server to which you want to add an index data location.
4. Right-click the index server, click **Properties**, and then click the **Elasticsearch Index Locations** tab.
5. Click **Browse** to choose an empty folder in which index data can be stored.
6. Click **OK** to apply the changes.
7. Start Enterprise Vault indexing service once the configuration is done.

If you want to backup the newly created Elasticsearch indexes, you first need to set up an index snapshot location through PowerShell using the following steps:

1. Run the Enterprise Vault Management Shell.
2. In the Enterprise Vault Management Shell, run the following command:

   ```
   Set-EVIndexSnapshotLocation -SnapshotLocationPath "I:\" -SiteId
   <EV site id>
   ```

   For more information, see the *PowerShell Cmdlets* guide.
3. Restart the Enterprise Vault Indexing service.

Starting all the Enterprise Vault services

Start the Enterprise Vault services on all the servers in the site.

Use the cluster administration tools to bring all the Enterprise Vault services online.

If there are multiple sites that share the Enterprise Vault Directory, you can start all Enterprise Vault services in the other sites.

Test that the cluster failover works correctly for Enterprise Vault.

Chapter 9

Windows Server Failover Clustering: upgrading the Enterprise Vault server software

This chapter includes the following topics:

- About upgrading a Windows Server Failover Cluster
- Installing the Enterprise Vault server software
- Upgrading the Enterprise Vault databases
- Backing up the upgraded Enterprise Vault databases
- Configuring index data location
- Starting all the Enterprise Vault services

About upgrading a Windows Server Failover Cluster

This chapter describes how to upgrade the Enterprise Vault server software and databases, when the servers that run Enterprise Vault tasks are part of a Windows cluster.

Perform the procedures in this chapter in the order that they are listed.

Installing the Enterprise Vault server software

This section describes how to install the Enterprise Vault server software when the servers that run Enterprise Vault tasks are part of a Windows Server failover cluster.

Note that Enterprise Vault does not support high-availability upgrades. You must install the server software on all nodes in the cluster before you start Enterprise Vault services or run the configuration wizard.

Preparation

To prepare to upgrade the Enterprise Vault server software

1. Log on to the active node as the Vault Service account.
2. Use Failover Cluster Manager or the command-line utility `cluster` to take the Admin service resource offline. This takes all the Enterprise Vault services offline.

   Note the following important points:

   - Do not take the EnterpriseVaultServerInstance offline.
   - You must stop all Enterprise Vault services in the Enterprise Vault site. For example, stop the services on non-clustered servers, such as an Enterprise Vault Domino Gateway.
   - If you install on an Enterprise Vault Domino Gateway, make sure that the Domino server on the Enterprise Vault Domino Gateway is shut down and that `EVInstall.nsf` is not accessed locally.
   - If there are multiple sites that share the Enterprise Vault Directory, you must also stop all Enterprise Vault services in the other sites.
3. Stop any other local or remote services or applications that can lock Enterprise Vault files. Use Failover Cluster Manager to stop clustered services. For example:

   - Enterprise Vault Administration Console
   - Enterprise Vault Accelerator Manager service
4. Close any applications that may be running on the server, including the Control Panel, Computer Management, Windows Services, and the Windows Event Viewer.

To prepare to upgrade to Enterprise Vault 15.0 or later from EV 14.x with standalone Enterprise Vault Usage Analyzer

1. Start the **MSCS failover Cluster Manager**.
2. Select the **Roles** displayed in the left pane; it shows the cluster information.
3. Select the **Resource** tab in the bottom pane display in-between **Summary and Shares**.

   The **Resource** tab shows all the resources created under the cluster.
4. Select **Enterprise Vault Usage Analyzer Service**, right-click and select **Take Offline**.
5. Once offline, select **Enterprise Vault Usage Analyzer Service**, right-click and select the **Properties** option.
6. Clear the **Use Network Name for computer name** option on the **General** page.
7. Click the **Dependencies** tab, select **<Role name> -Enterprise Vault Indexing Service**, click **Delete**, and then click **OK**.
8. Select the **Enterprise Vault Usage Analyzer Service** service and remove it.
9. Proceed with upgrading to Enterprise Vault 15.0 or later.

Installing Enterprise Vault (wizard)

To use the wizard to install Enterprise Vault

1. Load the Enterprise Vault media.
2. If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.

   If AutoPlay is not enabled, use Windows Explorer to open the root folder of the installation media and then double-click the file `Setup.exe`.
3. In the list in the left pane of the **Arctera Enterprise Vault Install Launcher** window, click **Enterprise Vault**.
4. Click **Server Installation**.
5. In the right pane, click **Upgrade existing server**.
6. Click **Install**. The Enterprise Vault installation wizard starts.
7. Work through the installation wizard to upgrade the Enterprise Vault components.

8 If the installation wizard prompts you to restart the server, restart and then log on again as the Vault Service account so that the installer can complete the upgrade.

9 Install the Enterprise Vault software on the other servers in your Enterprise Vault environment, including any cluster failover nodes.

Installing Enterprise Vault (command line)

The following procedure describes how to upgrade the Enterprise Vault installation. If you want to add or remove components, see the "Installing Enterprise Vault" chapter in the *Installing and Configuring* guide for a complete description of the command-line options.

Caution: If a system restart is needed during silent installation, the server restarts automatically. If the server restarts, log on again as the Vault Service account so that the installer can complete the upgrade.

To install Enterprise Vault from the command line

1 Log on to the active node as the Vault Service account.

2 Load the Enterprise Vault media.

3 If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Close the AutoPlay dialog box.

4 Open a command prompt window and navigate to the following folder on the Enterprise Vault media:

```
\Arctera Enterprise Vault\Server\x64
```

5 Run `setup (x64).exe` as follows:

```
start /wait "" "setup (x64).exe" /s /clone_wait
/v"COMPONENTS=Option[|Option][...]"
```

6 If the server restarts, log on again as the Vault Service account so that the installer can complete the upgrade.

7 When the installation is complete, the installer re-enables the Enterprise Vault services. Do not start any Enterprise Vault services at this time.

8 Install the Enterprise Vault software on the other servers in your Enterprise Vault environment, including any cluster failover nodes.

Upgrading the Enterprise Vault databases

Before you start any Enterprise Vault services, you must upgrade the Enterprise Vault databases.

Note: You only need to complete this procedure on the active node.

Enterprise Vault provides a PowerShell cmdlet called `Start-EVDatabaseUpgrade`, which you can use to upgrade all Enterprise Vault databases.

Note: After upgrading Enterprise Vault databases to version 14.2 and later, all the existing index locations will be closed for new index additions. A new index location must be configured to store new Elasticsearch indexes. The Enterprise Vault Indexing service does not start until a new index location has been configured.

To upgrade Enterprise Vault's databases

1. On the active node, log in using the Vault Service account.
2. Run the Enterprise Vault Management Shell.
3. In the Enterprise Vault Management Shell, run the following command:

   ```
   Start-EVDatabaseUpgrade
   ```

   Note that you can also run `Start-EVDatabaseUpgrade -verbose` if you want to see detailed output.
4. Wait for `Start-EVDatabaseUpgrade` to complete the upgrade of all the databases.

When the upgrade is complete, you can examine the upgrade reports for errors.

`Start-EVDatabaseUpgrade` writes the reports in the `Reports\DBUpgrade` subfolder of the Enterprise Vault installation folder (for example `C:\Program Files (x86)\Enterprise Vault`).

Backing up the upgraded Enterprise Vault databases

Back up the upgraded Enterprise Vault databases as follows.

To back up the upgraded Enterprise Vault databases

1. Stop any running Enterprise Vault services.
2. Back up all Enterprise Vault databases.

Configuring index data location

Note: You must complete this procedure on the active node.

The Enterprise Vault administrator must configure an index data location from the Enterprise Vault Administration Console or by running the Getting Started wizard. The Enterprise Vault Admin service and the Enterprise Vault Directory service must be running before configuring the index data location.

To set up the Enterprise Vault index data location through Enterprise Vault Administration Console, perform the following steps:

1. In the left pane, expand the Enterprise Vault site hierarchy until the Indexing container is visible.
2. Expand the Indexing container.
3. Expand the index server to which you want to add an index data location.
4. Right-click the index server, click **Properties**, and then click the **Elasticsearch Index Locations** tab.
5. Click **Browse** to choose an empty folder in which index data can be stored.
6. Click **OK** to apply the changes.
7. Start Enterprise Vault indexing service once the configuration is done.

If you want to backup the newly created Elasticsearch indexes, you first need to set up an index snapshot location through PowerShell using the following steps:

1. Run the Enterprise Vault Management Shell.
2. In the Enterprise Vault Management Shell, run the following command:

   ```
   Set-EVIndexSnapshotLocation -SnapshotLocationPath "I:\" -SiteId
   <EV site id>
   ```

   For more information, see the *PowerShell Cmdlets* guide.
3. Restart the Enterprise Vault Indexing service.

Starting all the Enterprise Vault services

Start the Enterprise Vault services on all the servers in the site.

Use the cluster administration tools to bring all the Enterprise Vault services online.

If there are multiple sites that share the Enterprise Vault Directory, you can start all Enterprise Vault services in the other sites.

Test that the cluster failover works correctly for Enterprise Vault.

Chapter 10

Upgrading standalone Administration Consoles

This chapter includes the following topics:

- About upgrading standalone Administration Consoles
- Upgrading a standalone Administration Console (wizard)
- Installing Enterprise Vault (command line)

About upgrading standalone Administration Consoles

If you have any computers on which you have installed the Enterprise Vault Administration Console component only, you must upgrade it. Note that the supported versions of Windows for standalone Administration Consoles are as follows:

- Windows 10
- Windows 11
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

You must have local administrator rights to install and run the Enterprise Vault Administration Console on a separate computer.

Upgrading a standalone Administration Console (wizard)

To upgrade a standalone Administration Console

1. Log on to the computer as the Vault Service account.
2. Make sure that the Administration Console is not running.
3. Load the Enterprise Vault media.
4. If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.

   If AutoPlay is not enabled, use Windows Explorer to open the root folder of the installation media and then double-click the file `Setup.exe`.
5. In the list in the left pane of the **Arctera Enterprise Vault Install Launcher** window, click **Enterprise Vault**.
6. Click **Server Installation**.
7. In the right pane, click **Upgrade existing server**.
8. Click **Install**. The Enterprise Vault installation wizard starts.
9. Work through the installation to upgrade the Administration Console component.

Installing Enterprise Vault (command line)

To upgrade the Administration Console from the command line

1. Log on to the computer as the Vault Service account.
2. Load the Enterprise Vault media.
3. If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Close the AutoPlay dialog box.
4. Open a Command Prompt window and navigate to the following folder on the Enterprise Vault media:

   ```
   \Arctera Enterprise Vault\Server
   ```
5. Run the appropriate setup file, as follows:
   - On a computer that runs 64-bit version of Windows:

     ```
     start /wait "" "setup (x64).exe" /s /clone_wait
     /v"COMPONENTS=VAC"
     ```
   - On a computer that runs 32-bit version of Windows:

```
start /wait "" "setup (x86).exe" /s /clone_wait
/v"COMPONENTS=VAC"
```

Chapter 11

Upgrading Enterprise Vault Reporting

This chapter includes the following topics:

- Upgrading Enterprise Vault Reporting
- Installing the Enterprise Vault Reporting component
- Running the Enterprise Vault Reporting Configuration utility

Upgrading Enterprise Vault Reporting

You must upgrade Enterprise Vault Reporting on the computers on which it is installed.

Table 11-1 lists the steps that are required to upgrade Enterprise Vault Reporting.

Table 11-1 Steps to install Enterprise Vault Reporting

Step	Action	Description
Step 2	Install the Enterprise Vault 15.2 Reporting component on each computer on which the Enterprise Vault Reporting component is installed.	See "Installing the Enterprise Vault Reporting component" on page 62.
Step 3	Run the Enterprise Vault Reporting Configuration utility on each computer on which the Enterprise Vault Reporting component is installed.	See "Running the Enterprise Vault Reporting Configuration utility" on page 62.

Installing the Enterprise Vault Reporting component

You must install the Enterprise Vault 15.2 Reporting component on each computer on which the Enterprise Vault Reporting component is already installed.

If the Reporting component is installed on an Enterprise Vault server, you can install the Enterprise Vault 15.2 Reporting component when you install the other Enterprise Vault components.

Use the following procedure to install the Enterprise Vault Reporting component on any additional computers on which it is installed.

To install the Enterprise Vault Reporting component

1. Log on to the computer with the Vault Service account.
2. Load the Enterprise Vault media.
3. If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.

   If AutoPlay is not enabled, use Windows Explorer to open the root folder of the installation media and then double-click the file `Setup.exe`.
4. In the list in the left pane of the **Arctera Enterprise Vault Install Launcher** window, click **Enterprise Vault**.
5. Click **Server Installation**.
6. In the right pane, click **Upgrade existing server**.
7. Click **Install**. The Enterprise Vault installation wizard starts.
8. Work through the installation to upgrade the Enterprise Vault Reporting component.

Running the Enterprise Vault Reporting Configuration utility

Perform the following procedure on each computer on which the Enterprise Vault Reporting component is installed. Do not run the utility until you have done the following:

- Installed the Enterprise Vault 15.2 software on the Enterprise Vault servers.
- Installed the Enterprise Vault 15.2 Reporting component on each computer on which the Reporting component is installed.

To run the Enterprise Vault Reporting Configuration utility

1. Start the Reporting Configuration utility, **Enterprise Vault Reports Configuration**.
2. Select **Configure Reporting and deploy or upgrade reports**.
3. Type the domain, user name, and password for the Reporting user account.
4. Select the SQL Server Reporting Services instance.
5. Select the language in which to deploy the reports.
6. Select or type in the name of the Directory database SQL Server.
7. Click **Configure** to deploy the reports.

   If the Reporting Configuration utility indicates that there was an error deploying Enterprise Vault reports, see the following technical note on the Arctera Support website:

   https://www.veritas.com/docs/100018177

   The Enterprise Vault Reporting Configuration utility synchronizes the report security settings with the current administrator roles. If you subsequently add, remove, or modify roles, Enterprise Vault must synchronize Enterprise Vault Reporting again to reflect the changes.

   See "Enabling the synchronization of Enterprise Vault Reporting roles-based security" in the *Reporting* guide.

Chapter 12

Upgrading MOM and SCOM

This chapter includes the following topics:

- Upgrading MOM
- Upgrading the Enterprise Vault SCOM management pack

Upgrading MOM

If you use Microsoft Operations Manager (MOM) to monitor Enterprise Vault events then you must install the new management pack.

To install the Enterprise Vault MOM management pack

1. Start the MOM Administrator Console.
2. In the left pane, right-click **Processing Rule Groups** and, on the shortcut menu, click **Import Management Pack**.
3. Select the Enterprise Vault Management Pack, `EnterpriseVault.akm`, and work through the rest of the **Import Options** wizard.

Upgrading the Enterprise Vault SCOM management pack

You must install the new Enterprise Vault management pack to use the improved monitoring.

About the supplied management packs

Table 12-1 describes the management packs that come with Enterprise Vault 15.2.

Table 12-1 SCOM management packs in Enterprise Vault

Management pack	Description
Arctera.EnterpriseVault.mp	Required for monitoring Enterprise Vault 15.2. Importing the pack creates an **Enterprise Vault** node under the **Arctera Enterprise Vault** node in SCOM. This node contains all the servers with Enterprise Vault 15.2.
Arctera.EnterpriseVault.Library.mp	A common library that is required for monitoring all versions of Enterprise Vault.
Arctera.EnterpriseVault.Reports.mp	Required so that reports can be viewed.

You must import both the Arctera.EnterpriseVault.mp and Arctera.EnterpriseVault.Library.mp packs to implement the monitoring facilities in Enterprise Vault 15.2.

About the upgrade procedure

To upgrade the SCOM management packs from version 14.x to 15.2, you must install the Enterprise Vault 15.2 management packs.

Chapter 13

Upgrading Exchange Server forms

This chapter includes the following topics:

- About upgrading Exchange Server forms

About upgrading Exchange Server forms

By default, Enterprise Vault deploys the Exchange Server forms to users' computers automatically.

If you use forms from the Organization Forms Library instead of using the Enterprise Vault client to deploy the forms automatically then you must upgrade the forms in the Organization Forms Library.

If you decide to upgrade the forms that are in the Organization Forms Library, follow the instructions in the "Distributing Exchange Server Forms" chapter of *Setting up Exchange Server Archiving*.

Note the following:

- When you upgrade or reinstall the Enterprise Vault forms `EVPendingArchive.fdm`, `EVShortcut.fdm`, `EVPendingDelete.fdm`, `EVPendingRestore.fdm`, and `EVPendingArchiveHTTP.fdm`, always uninstall the existing copies first. Do not install the new forms on top of the existing copies.
- By default, Enterprise Vault deploys the forms automatically into personal forms libraries.

Chapter 14

Upgrading Domino mailbox archiving

This chapter includes the following topics:

- About upgrading Domino mailbox archiving
- Domino client version required to run EVInstall.nsf
- Preparing for the upgrade of Domino mailbox archiving
- Upgrading Domino mailbox archiving
- Granting the Domino archiving user access to mail files
- Identifying internal mail recipients
- Run the Domino provisioning task

About upgrading Domino mailbox archiving

You must follow the instructions in this chapter to upgrade Domino mailbox archiving after you have upgraded the Enterprise Vault server software.

Domino client version required to run EVInstall.nsf

You must use a suitable version of the Notes client on the workstation from which you run `EVInstall.nsf`.

The version of the Notes client must be no older than the newest version of the Domino Server that is installed on the Enterprise Vault Domino Gateway and the Domino mail servers.

Preparing for the upgrade of Domino mailbox archiving

This section describes how to prepare your Domino servers for the upgrade of Domino mailbox archiving.

Complete the following procedure on all Enterprise Vault Domino Gateway servers and on all Domino mail servers on which you have updated these forms to include the Enterprise Vault customizations:

- `Forms9.nsf`
- `Forms85.nsf`

Note: The following procedure requires you to replace the forms files with the original Domino versions. When you replace the forms files you lose any non-Enterprise Vault customizations that you made to them. If you made any non-Enterprise Vault customizations to the forms files, you must reapply these changes to the files after you have upgraded Enterprise Vault.

To prepare for the upgrade of Domino mailbox archiving

1. Stop the HTTP task.
2. Skip this step for Domino 9 and later.

   Delete `Forms85_x.nsf` if it exists on the server.
3. Skip this step for Domino 9 and later.

   Replace the `Forms85.nsf` file with the original Domino versions that you backed up before you installed the previous version of Enterprise Vault.
4. If the forms databases have replication enabled, the changes that EVInstall makes are replicated to all Domino mail servers. If you want to prevent the replication to other mail servers, disable the replication of `Forms85.nsf` and `Forms9.nsf`.
5. Update the ACLs on the original Domino `.nsf` files to give Manager access to the ID of the user that will run EVInstall.

Upgrading Domino mailbox archiving

This section describes how to upgrade Domino mailbox archiving.

To upgrade Domino mailbox archiving

1 Make sure that you have a suitable version of the Notes client installed on the workstation from which you want to run `EVInstall.nsf`.

See "Domino client version required to run EVInstall.nsf" on page 67.

2 Do the following in the order listed:

- From your chosen workstation, connect to the Enterprise Vault Domino Gateway server and run `EVInstall.nsf`.
- In the application page, select the Enterprise Vault Domino Gateway and a target Domino mail server.
- If you use the browser-based Enterprise Vault Search facilities or you require iNotes (DWA), select **Modify Domino Web Access Forms Files**.
- Click **Install Arctera Enterprise Vault 15.2 database design templates** to start the process.
  The application takes several minutes to create the new Enterprise Vault templates.

3 Deploy the templates created on the Domino mail server to each target Domino mail server that has the same Domino Server version. For example, if you ran `EVInstall.nsf` against a Domino Server 9.0 target server, deploy the templates to all Domino Server 9.0 mail servers.

Deploy the templates by creating replicas of the Enterprise Vault mail templates and running `Load Design` on each mail server.

It is important that you copy the templates created on the Domino mail server and not those created on the Enterprise Vault Domino Gateway.

Note that the command `Load Design` updates all databases on the server. It may be quicker to restrict the scope of the command so that it updates just those databases that need changing. In this case, use the command's `-I` or `-d` or `-f` switches to update all Enterprise Vault mail databases that have had any of the following templates applied to them:

- `ev_dwa*.ntf`
- `ev_iNotes*.ntf`
- `ev_Mail*.ntf`

See the Domino help for more information about Load Design switches.

4 If you have other target mail servers with different Domino Server versions, do the following until you have deployed the templates to all mail server targets:

- Run `EVInstall.nsf` again.
- In the application page, clear the **Enterprise Vault Domino Gateway** selection.
- Select a target Domino mail server.
- If you require iNotes (DWA), select **Modify Domino Web Access Forms Files**.
- Click **Install Arctera Enterprise Vault 15.2 database design templates** to start the process.
  The application takes several minutes to create the new Enterprise Vault templates.
- Deploy the templates and run `Load Design` as before, on each mail server.

Granting the Domino archiving user access to mail files

The Domino archiving user account needs permissions to all the mail files to be archived. We recommend that you provide **Manager** access to the mail files.

The account requires a minimum of **Editor** access with **Delete Documents** and **Create shared folders/views**.

Note: If you intend not to archive unread items then the Domino archiving user requires Manager access to the mail files. This is because Domino requires Manager access in order to determine which items are unread.

If Domino administrators have Manager access to all mail files, you can use the Manage ACL tool in the Domino Administrator client to add the Domino archiving user to all mail databases.

Repeat the following steps for each target Domino mail server.

To add the Domino archiving user to all mail databases

1. In the Domino Administrator client, navigate to the Domino mail server and click the **Files** tab.
2. In the tasks pane, click the **Mail** folder to display a list of all the mail databases in the results pane.
3. Select the first mail database, and then press Shift+End to select all the mail databases.
4. Right-click and select **Access Control** > **Manage**.

5 Click **Add** and then click the person icon to select the Domino archiving user from the Domino directory list. Click **OK**.

6 When the user is in the **Access Control List** dialog box, change the set **User Type** to **Person** and **Access** to **Manager**.

7 Select **Delete documents**.

8 Click **OK** to add the user to the ACL of all mail databases selected.

If no user has Manager access to every mail database, then do the following:

- Place the Domino server administrator's user name in the Full Access Administrators field in the server document.
- Restart the Domino server.
- In the Domino Administrator client, choose **Administration** > **Full Access Administration** and complete the procedure described above.
- If necessary, the administrator can then be removed from the Full Access Administrators field.

Identifying internal mail recipients

You can specify that Enterprise Vault must perform a local address lookup for specific Notes domains. The local lookup enables Enterprise Vault to identify the Notes user name for messages that are addressed to alternate email addresses. The local lookup results can aid searching in the web applications and in Surveillance and eDiscovery.

In order to specify the domains that require local address lookup, you must make some changes to the registry on the Enterprise Vault servers that run the journaling and archiving tasks.

To specify local lookup domains

1 On an Enterprise Vault server that runs a Domino archiving or journaling task, create a new registry key named **NotesDomains** in the following location:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \Agents
```

2 Under the new **NotesDomains** key, create a subkey for each Notes domain. For example, if you have Notes domains 'MyNotesDomain1' and 'MyNotesDomain2' you create subkeys 'MyNotesDomain1' and 'MyNotesDomain2'.

3 Under each of the Notes domain subkeys, create a new String value named **InternalSMTPDomains**.

4 Assign to each InternalSMTPDomains value a string that lists the domains for which you want to use local lookup. Use semi-colons (;) to separate domains. For example:

```
exampledomain1.com;exampledomain2.com
```

5 Under each of the Notes domain subkeys, create a new DWORD value called **EnableLocalPartLookup**.

6 Give **EnableLocalPartLookup** one of the following values:

- 0 to disable local part lookup
- 1 to enable local part lookup

7 Repeat all these steps for other Enterprise Vault servers that run Domino archiving or journaling tasks.

Table 14-1 shows how the NotesDomains registry key controls how Enterprise Vault identifies internal mail recipients.

Table 14-1 Effects of NotesDomains registry key

Registry key or value	Effect on Enterprise Vault behavior
NotesDomains key is missing	Full address lookup and a warning in the event log.

Table 14-1 Effects of NotesDomains registry key *(continued)*

Registry key or value	Effect on Enterprise Vault behavior
NotesDomains key is present but has no key for the current Notes domain	Original address is recorded. No lookup.
NotesDomains key is present and has a key for the current Notes domain	■ If EnableLocalPartLookup is set to 0, perform a full address lookup. ■ If EnableLocalPartLookup is set to 1, perform a full address and local part lookup for addresses that match the Domain. If the InternalSMTPDomains list is present and the SMTP domain matches a domain in the list, SMTP messages being archived from journals are checked with full address and local part lookup. If the InternalSMTPDomains list is not present or there is no match, full address lookup is used.

Run the Domino provisioning task

When you have completed the upgrade of Domino mailbox archiving, you must run the Domino provisioning task to synchronize Domino permissions to Enterprise Vault archives.

Chapter 15

Upgrading the FSA Agent

This chapter includes the following topics:

- Compatible versions of the FSA Agent and Enterprise Vault server
- About upgrading the FSA Agent
- Upgrading FSA Agent services that are clustered for high availability
- Upgrading the FSA Agent on a target Windows file server from the Administration Console
- Upgrading the FSA Agent on an FSA Reporting proxy server from the Administration Console
- Upgrading the FSA Agent manually

Compatible versions of the FSA Agent and Enterprise Vault server

Enterprise Vault 15.2 does not support File Blocking.

For more details of the compatible versions of the FSA Agent and Enterprise Vault server, see the following documents:

- The Enterprise Vault Compatibility Charts.
- For compatibility with Enterprise Vault Reporting, the technical note at https://www.veritas.com/docs/100030221.

About upgrading the FSA Agent

We recommend that you upgrade the FSA Agent on the Windows computers on which it is installed. Support is provided for backward compatibility, but new

features may not be available until the FSA Agent version is aligned with the Enterprise Vault server version.

Note the following:

- Do not install the FSA Agent on Enterprise Vault servers. Enterprise Vault servers do not require the FSA Agent.
- As part of the upgrade process, you are prompted for a compulsory restart of the file server.
- Enterprise Vault 15.2 does not support File Blocking.

FSA Agent installation requires an up-to-date root certificate on the target computer. Certificate updates usually happen automatically over the Internet. If the certificate is out-of-date, for example because the computer has no Internet connection, the FSA Agent installation fails with a "Signature verification failed" error in the FSA Agent installation log. For more details and for instructions on how to update the root certificate, see the following technical note on the Arctera Support website:

https://www.veritas.com/docs/100023437

You can upgrade the FSA Agent from an Enterprise Vault Administration Console, or by installing the files manually on the file server.

To install or upgrade the FSA Agent you must use an account that is a member of the local Administrators group on the file server.

If you upgrade the FSA Agent from the Administration Console then if the file server's firewall is enabled it must be suitably configured. Otherwise the Administration Console wizard fails with the message "Error: The RPC server is unavailable". See the following technical note on the Arctera Support website:

https://www.veritas.com/docs/100022335

Table 15-1 describes the options for upgrading the FSA Agent.

Table 15-1 Upgrading the FSA Agent

To do this	See this section
Upgrade FSA Agent services that are clustered for high availability.	See "Upgrading FSA Agent services that are clustered for high availability" on page 76.
Upgrade the FSA Agent on target Windows file servers from the Administration Console.	See "Upgrading the FSA Agent on a target Windows file server from the Administration Console" on page 77.

Table 15-1 Upgrading the FSA Agent *(continued)*

To do this	See this section
Upgrade the FSA Agent on FSA Reporting proxy servers from the Administration Console.	See "Upgrading the FSA Agent on an FSA Reporting proxy server from the Administration Console" on page 78.
Upgrade the FSA Agent manually.	See "Upgrading the FSA Agent manually" on page 79.

Upgrading FSA Agent services that are clustered for high availability

Note that Enterprise Vault 14.5 does not support File Blocking. If you are upgrading from Enterprise Vault 12.1 or earlier, the upgrade process removes the Enterprise Vault File Blocking service from the file server.

Use this procedure to upgrade FSA Agent services that are clustered for high availability.

To upgrade FSA Agent services that are clustered for high availability

1 Perform these steps in the order shown:

- Run the Enterprise Vault Administration Console with an account that is a member of the local Administrators group on each file server node. The account must also have Full Control permission on the Enterprise Vault server's `FSA Cluster` folder. This folder is in the `Utilities` subfolder of the Enterprise Vault installation folder; for example, `C:\Program Files (x86)\Enterprise Vault\Utilities\FSA Cluster`.
- In the Administration Console, expand the Enterprise Vault site.
- Expand the **Targets** container and then the **File Servers** container.
- Right-click the clustered file server and then, on the shortcut menu, click **FSA Cluster Configuration**.
- Select the option **Remove the FSA resource from all groups** to remove the FSA resource.

2 Upgrade the FSA Agent on the clustered file server by using one of the following methods:

- Upgrade the FSA Agent from the Administration Console.
  See "Upgrading the FSA Agent on a target Windows file server from the Administration Console" on page 77.

- Upgrade the FSA Agent manually on each file server node.
  See "Upgrading the FSA Agent manually" on page 79.

3 Perform the following steps in the order shown to reconfigure the FSA services for high availability:

- Run the Enterprise Vault Administration Console with an account that is a member of the local Administrators group on each file server node. The account must also have Full Control permission on the Enterprise Vault server's `FSA Cluster` folder. This folder is in the `Utilities` subfolder of the Enterprise Vault installation folder, for example `C:\Program Files (x86)\Enterprise Vault\Utilities\FSA Cluster`.
- In the Administration Console, expand the Enterprise Vault site.
- Expand the **Targets** container and then the **File Servers** container.
- Right-click the clustered file server and then, on the shortcut menu, click **FSA Cluster Configuration**.
- Select the option **Add, remove or reconfigure the FSA resource for groups that have shared disks**, and add the FSA resource back to the groups that have a shared disk.

Upgrading the FSA Agent on a target Windows file server from the Administration Console

Use the following procedure to upgrade the FSA Agent by using the Administration Console's Install FSA Agent wizard.

Before you upgrade the FSA Agent on a target Windows file server, note that while the upgrade proceeds, Enterprise Vault stops the following FSA Agent services on the file server:

- Enterprise Vault File Placeholder service. While this service is stopped, Enterprise Vault cannot create placeholders or perform placeholder recalls on the Windows file server.
- Enterprise Vault File Collector service. While this service is stopped, no FSA Reporting scans run on the following:
  - The file server.
  - Any non-Windows file servers for which the file server acts as the FSA Reporting proxy server.
- Enterprise Vault 15.2 does not support File Blocking.

To upgrade the FSA Agent on a target Windows file server from the Administration Console

1. Run the Enterprise Vault Administration Console with an account that is a member of the local Administrators group on the file server.
2. In the Administration Console, expand the Enterprise Vault site until the **Targets** container is visible.
3. Expand the **Targets** container.
4. Expand the **File Servers** container.
5. Right-click the file server on which you want to upgrade the FSA Agent and then, on the shortcut menu click **Install FSA Agent**.
6. Work through the wizard.

Note: As part of the upgrade process, you may be prompted to restart the file server.

Upgrading the FSA Agent on an FSA Reporting proxy server from the Administration Console

This section applies if you use FSA Reporting with non-Windows file servers.

If you have configured any target Windows file servers or other Windows servers as FSA Reporting proxy servers, you can upgrade the FSA Agent on the proxy servers from the Administration Console.

Before you upgrade the FSA Agent on a target Windows file server, note that while the upgrade proceeds, Enterprise Vault stops the following FSA Agent services on the file server:

- Enterprise Vault File Placeholder service. While this service is stopped, Enterprise Vault cannot create placeholders or perform placeholder recalls on the Windows file server.
- Enterprise Vault File Collector service. While this service is stopped, no FSA Reporting scans run on the following:
  - The file server.
  - Any non-Windows file servers for which the file server acts as the FSA Reporting proxy server.
- Enterprise Vault 15.2 does not support File Blocking.

To upgrade the FSA Agent on an FSA Reporting proxy server from the Administration Console

1. Run the Enterprise Vault Administration Console with an account that is a member of the local Administrators group on the FSA Reporting proxy server.
2. In the Administration Console, expand the Enterprise Vault site until the **Targets** container is visible.
3. Expand the **Targets** container.
4. Expand the **File Servers** container.
5. Right-click the target non-Windows file server and on the shortcut menu click **Upgrade FSA Agent on proxy server for FSA Reporting**.

   This option is not available if the FSA Reporting proxy server is an Enterprise Vault server. Enterprise Vault servers do not require the FSA Agent.

   If the proxy server is a target Windows file server, Enterprise Vault displays a dialog box to warn that the FSA Agent services stop while the upgrade proceeds. Click **Yes** if you want to continue.
6. Work through the wizard to upgrade the version of the FSA Agent on the FSA Reporting proxy server.

Note: As part of the upgrade process, you may be prompted to restart the file server.

Upgrading the FSA Agent manually

Use the following procedure to upgrade the FSA Agent on a server by installing the required files manually.

Before you upgrade the FSA Agent on a target Windows file server, note that while the upgrade proceeds, Enterprise Vault stops the following FSA Agent services on the file server:

- Enterprise Vault File Placeholder service. While this service is stopped, Enterprise Vault cannot create placeholders or perform placeholder recalls on the Windows file server.
- Enterprise Vault File Collector service. While this service is stopped, no FSA Reporting scans run on the following:
  - The file server.

  - Any non-Windows file servers for which the file server acts as the FSA Reporting proxy server.

- Enterprise Vault 14.5 does not support File Blocking. If you are upgrading from Enterprise Vault 12.1 or earlier, the upgrade process removes the Enterprise Vault File Blocking service from the file server.

To upgrade the FSA Agent manually

1. Find the required files on the Enterprise Vault server. The files are in the `evpush\Agent` folder under the Enterprise Vault installation folder; for example, `C:\Program Files (x86)\Enterprise Vault\evpush\Agent`.
2. Install the required Microsoft Visual C++ redistributable packages on the file server:
   - `VC_redist.x86.exe`
   - `VC_redist.x64.exe`
3. Log on to the file server with an account that is a member of the local Administrators group on the file server.
4. Run the `Enterprise Vault File System Archiving x64.msi` file on the file server.

Note: As part of the upgrade process, you may be prompted to restart the file server.

Chapter 16

Upgrading Enterprise Vault Office Mail App

This chapter includes the following topics:

- About upgrading Enterprise Vault Office Mail App

About upgrading Enterprise Vault Office Mail App

If you have deployed the Enterprise Vault Office Mail App, then you need to upgrade the deployed version after you have upgraded the Enterprise Vault server.

To upgrade Enterprise Vault Office Mail App

1. On the Exchange Server, rerun the New-App command that you originally used to deploy the Enterprise Vault Office Mail App.

   The New-App command lines for deploying the application to individual or multiple users are given in the section, "Deploying the Enterprise Vault Office Mail App", in *Setting up Exchange Server Archiving*.

2. On the Enterprise Vault server, synchronize the mailboxes to which you have deployed the Enterprise Vault Office Mail App.

   If the Exchange Mailbox Archiving task is set to run automatically, it synchronizes mailboxes the next time it runs. Alternatively, you can synchronize the mailboxes manually using the Arctera Administration Console. Open the properties dialog box of the Exchange Mailbox Archiving task, and select the **Synchronization** tab for the manual synchronization options.

Chapter 17

Upgrading SharePoint Server components

This chapter includes the following topics:

- About upgrading the SharePoint components
- Upgrading the Enterprise Vault SharePoint components

About upgrading the SharePoint components

This chapter describes how to upgrade Enterprise Vault SharePoint components.

Note: You must upgrade the SharePoint components. The version of the SharePoint components must match the version of Enterprise Vault that is installed on the Enterprise Vault servers.

The upgrade path depends on your version of SharePoint, as follows:

- You can upgrade Enterprise Vault components on any of the following:
  - Microsoft SharePoint Server 2019
  - Microsoft SharePoint Server Subscription Edition
  - Microsoft SharePoint Server 2016

  See "Upgrading the Enterprise Vault SharePoint components" on page 83.
- If you have started a gradual migration to upgrade SharePoint, finish the migration before you upgrade Enterprise Vault.

Upgrading the Enterprise Vault SharePoint components

Upgrade the Enterprise Vault SharePoint components on each of your SharePoint Server computers.

To upgrade the Enterprise Vault SharePoint components

1. Log on to the SharePoint Server as one of the following:
   - The SharePoint Server farm account. This account is sometimes known as the SharePoint database access account.
   - An account that has sufficient permissions to the SharePoint_Config database (the configuration database). The account must be a member of the following SQL Server security roles on the SharePoint_Config database: SharePoint_Shell_Access and WSS_Content_Application_Pools.
     The Vault Service account can be used provided it has these permissions.
2. On your SharePoint Server computer, load the Enterprise Vault media.
3. If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.

   If AutoPlay is not enabled, use Windows Explorer to open the root folder of the installation media and then double-click the file `Setup.exe`.
4. In the list in the left pane of the **Arctera Enterprise Vault Install Launcher** window, click **Enterprise Vault**.
5. Click **Server Installation**.
6. In the right pane, click **Upgrade existing server** to start the installation.
7. On the **Select Components to Install** screen, ensure that only **Microsoft SharePoint Components** is selected.
8. Click **Next**.
9. Work through the remainder of the installation wizard.

Chapter 18

Upgrading SMTP archiving

This chapter includes the following topics:

- Required and optional tasks when upgrading SMTP Archiving
- Checking the SMTP journaling type configuration
- Checking the permissions of the SMTP Archiving task account
- Checking the 'Journal report processing' advanced SMTP policy setting
- Checking the 'Journal Reports settings' advanced SMTP policy setting
- Checking the 'Selective Journal Archiving' site setting
- About upgrading legacy SMTP archiving components
- Migrating existing targets to provisioning groups
- Reconfiguring targets that are configured for target address rewriting to use multiple archives
- Granting the Administrators group and system account full access to the SMTP holding folder

Required and optional tasks when upgrading SMTP Archiving

The SMTP Archiving feature was introduced at Enterprise Vault 11.0.1. Subsequent releases have improved and expanded the feature considerably. Enterprise Vault applies some of these improvements automatically to your configuration during the upgrade procedure.

After you upgrade the SMTP Archiving components, we recommend that you perform the tasks listed in Table 18-1. The sections listed under the column heading, **More information**, provide detailed information about each task.

Table 18-2 lists some optional changes that you may want to make to take advantage of improved functionality.

"Legacy SMTP archiving" refers to the SMTP archiving solution in Enterprise Vault 11.0.0 and earlier. SMTP Archiving was completely redesigned in Enterprise Vault 11.0.1. Although the legacy SMTP archiving components are still supported at this release, we strongly recommend that you use the current SMTP Archiving feature instead.

Table 18-1 Checks and tasks to perform after you upgrade Enterprise Vault

Task	More information
Check that the type of SMTP journaling assigned to existing targets is correct.	See "Checking the SMTP journaling type configuration " on page 86.
Check that only supported archive types are assigned to existing targets.	See "Checking the SMTP journaling type configuration " on page 86.
Check the permissions of the SMTP Archiving task account, if the Vault Service account is not used.	See "Checking the permissions of the SMTP Archiving task account" on page 91.
Check the configuration setting for Journal reports.	See "Checking the 'Journal report processing' advanced SMTP policy setting" on page 92.
Check the value of the **Selective Journal Archiving** site setting.	See "Checking the 'Selective Journal Archiving' site setting" on page 93.
If you use the legacy SMTP archiving solution, re-configure the legacy SMTP archiving components.	If you want to continue running the legacy SMTP archiving components, then you need to rerun the legacy SMTP archiving configuration process. See "About upgrading legacy SMTP archiving components" on page 93.

Table 18-2 Optional checks and tasks to perform after you upgrade Enterprise Vault

Task	More information
Migrate targets to provisioning groups.	See "Migrating existing targets to provisioning groups" on page 94.

Table 18-2 Optional checks and tasks to perform after you upgrade Enterprise Vault *(continued)*

Task	More information
Replace address rewriting with targets that have multiple archives assigned.	See "Reconfiguring targets that are configured for target address rewriting to use multiple archives" on page 95.
Upgrade a legacy SMTP archiving configuration.	For guidance on how to migrate a legacy SMTP archiving solution to the current implementation, see Migrating from the Legacy SMTP Archiving Solution.

Checking the SMTP journaling type configuration

From Enterprise Vault 12.3 and later, the type of journaling formerly known as "Selective SMTP Journaling" is called "SMTP Group Journaling".

Enterprise Vault 12.3 onwards, you must specify the type of SMTP journaling that you want to configure for new SMTP target addresses. For existing SMTP addresses, the upgrade process determines the journaling type based on the advanced SMTP site setting, **Selective Journal Archiving**, and the archiving configuration of each SMTP target address.

Additionally, the supported archive types for each type of SMTP journaling are as follows:

- SMTP, Shared, Exchange Journal, and Domino Journal archives - For SMTP addresses that are configured for SMTP Journaling and SMTP Group Journaling.
- Exchange Mailbox and Internet Mail archives - For SMTP addresses that are configured for SMTP Mailbox Journaling.

After the upgrade is complete, if any targets are linked to unsupported archives, such as File System or SharePoint, you need to assign the appropriate archives manually. You can use SQL queries to retrieve details of such archives.

See "Finding SMTP targets that are assigned to unsupported archive types" on page 90.

Table 18-3 details how Enterprise Vault determines the journaling type of existing SMTP target addresses.

Table 18-3 How Enterprise Vault determines the SMTP journaling type

"Selective Journal Archiving" site setting	Archive configuration	Determined Target Type
Non-selective	■ Archive type is Domino Journal, Exchange Journal, Shared, or SMTP.	SMTP Journaling. For example, SMTPTarget1 > SMTPArchive SMTPTarget2 > SharedArchive SMTPTarget3 > ExchangeJournalArchive SMTPTarget4 > DominoJournalArchive In this case, SMTPTarget1, SMTPTarget2, SMTPTarget3, and SMTPTarget4 will be considered as SMTP Journaling targets.
Non-selective	■ Archive type is other than Domino Journal, Exchange Journal, Shared, or SMTP.	SMTP Journaling. For example, SMTPTarget1 > ExchangeMailboxArchive SMTPTarget2 > InternetMailArchive SMTPTarget3 > FSAArchive Enterprise Vault continues to archive messages from these SMTP target addresses to the existing unsupported archive. However, if you want to assign multiple archives to this target, you need to delete the address and add it again with the supported archive types.

Table 18-3 How Enterprise Vault determines the SMTP journaling type *(continued)*

"Selective Journal Archiving" site setting	Archive configuration	Determined Target Type
Inclusive or Exclusive	■ SMTP target addresses are associated with a single archive each. ■ Archive type is Domino Journal, Exchange Journal, Shared, or SMTP.	SMTP Journaling. For example, SMTPTarget1 > SMTPArchive SMTPTarget2 > SharedArchive SMTPTarget3 > ExchangeJournalArchive In this case, SMTPTarget1, SMTPTarget2, and SMTPTarget3 will be considered as SMTP Journaling targets.
Inclusive or Exclusive	■ SMTP target addresses are associated with a single archive each. ■ Archive type is Exchange Mailbox or Internet Mail archives.	SMTP Mailbox Journaling. For example, SMTPTarget1 > ExchangeMailboxArchive SMTPTarget2 > InternetMailArchive In this case, SMTPTarget1, and SMTPTarget2 will be considered as SMTP Mailbox Journaling targets.

Table 18-3 How Enterprise Vault determines the SMTP journaling type *(continued)*

"Selective Journal Archiving" site setting	Archive configuration	Determined Target Type
Inclusive or Exclusive	■ SMTP target addresses are associated with a single archive each. ■ Archive type is other than SMTP, Shared, Exchange Journal, Domino Journal, Exchange Mailbox, or Internet Mail archives.	SMTP Mailbox Journaling. For example, SMTPTarget1 > SharePointArchive SMTPTarget2 > ExchangePublicFolderArchive SMTPTarget3 > FSAArchive Enterprise Vault continues to archive messages from these SMTP target addresses to the existing unsupported archive. However, if you want to assign multiple archives to this target, you need to delete the address and add it again with the supported archive types.
Inclusive or Exclusive	■ Multiple SMTP target addresses are associated with the same archive. ■ Archive type is Domino Journal, Exchange Journal, Shared, or SMTP.	SMTP Group Journaling. For example, SMTPTarget1, SMTPTarget2, and SMTPTarget3 > SMTPArchive In this case, SMTPTarget1, SMTPTarget2, and SMTPTarget3 will be considered as SMTP Group Journaling targets.

Table 18-3 How Enterprise Vault determines the SMTP journaling type *(continued)*

"Selective Journal Archiving" site setting	Archive configuration	Determined Target Type
Inclusive or Exclusive	■ Multiple SMTP target addresses are associated with the same archive. ■ Archive type is other than SMTP, Shared, Exchange Journal, or Domino Journal.	SMTP Group Journaling. For example, SMTPTarget1, SMTPTarget2, and SMTPTarget3 > SharePointArchive Enterprise Vault continues to archive messages from these SMTP target addresses to the existing unsupported archive. However, if you want to assign multiple archives to this target, you need to delete the address and add it again with the supported archive types.

Finding SMTP targets that are assigned to unsupported archive types

Enterprise Vault 12.3 and later support only archive types Exchange Mailbox and Internet Mail archives for SMTP Mailbox Journaling. The archive types that you can use for SMTP Journaling and SMTP Group Journaling are SMTP, Shared, or Exchange Journal, or Domino Journal archives.

After the upgrade is complete, if any of the existing SMTP targets are assigned to unsupported archive types, such as File System or SharePoint, you need to associate them with valid archive types.

On the SQL server that hosts the Directory database, run the following SQL query to retrieve the list of targets that are assigned to unsupported archive types:

```
USE EnterpriseVaultDirectory
SELECT ST.TargetId, ST.Address, A.ArchiveName, AT.Name AS 'ArchiveType',
CASE      WHEN ST.TargetType = 1 THEN 'SMTP Journaling'
WHEN ST.TargetType = 2 THEN 'SMTP Mailbox Journaling'
WHEN ST.TargetType = 3 THEN 'SMTP Group Journaling'
ELSE 'Legacy'
END AS WronglyDetectedTargetType
FROM SmtpTarget ST
INNER JOIN SmtpTargetArchives STA ON STA.TargetId = ST.TargetId
INNER JOIN Root R ON R.RootIdentity = STA.RootIdentity
```

```
INNER JOIN Archive A ON A.RootIdentity = STA.RootIdentity
INNER JOIN ArchiveType AT ON AT.Type = R.Type
WHERE R.Type NOT IN (5, 17, 513, 2049) AND ST.TargetType IN (1, 3)
UNION
SELECT ST.TargetId, ST.Address, A.ArchiveName, AT.Name AS 'ArchiveType',
CASE      WHEN ST.TargetType = 1 THEN 'SMTP Journaling'
WHEN ST.TargetType = 2 THEN 'SMTP Mailbox Journaling'
WHEN ST.TargetType = 3 THEN 'SMTP Group Journaling'
ELSE 'Legacy'
END AS WronglyDetectedTargetType
FROM SmtpTarget ST
INNER JOIN SmtpTargetArchives STA ON STA.TargetId = ST.TargetId
INNER JOIN Root R ON R.RootIdentity = STA.RootIdentity
INNER JOIN Archive A ON A.RootIdentity = STA.RootIdentity
INNER JOIN ArchiveType AT ON AT.Type = R.Type
WHERE R.Type NOT IN(9, 4097) AND ST.TargetType = 2
```

This query returns information about each target such as the ID of the target, the SMTP target address, name of the archive, and the archive type. You can export the retrieved results to a CSV or TXT file.

If you want to assign multiple archives to this target, you need to delete the address and add it again with the supported archive types.

Checking the permissions of the SMTP Archiving task account

Adjustments have been made to the permissions that are required to run the SMTP Archiving task. The advice in this section only applies if your configuration fulfils the following criteria:

- The SMTP Archiving task runs under an account other that the Vault Service account
- Your environment contains Enterprise Vault storage servers that do not host an SMTP Archiving task

After you have upgraded Enterprise Vault, check the members of the local Administrators group on any Enterprise Vault storage servers that do not host an SMTP Archiving task. If the group includes the SMTP Archiving task account, then we recommend that you remove it from the group if there is no other reason for the account having this permission. Obviously you should not remove the account from the group if, for example, another Enterprise Vault task on that server is configured to run under the account.

Checking the 'Journal report processing' advanced SMTP policy setting

The new value, **Process journal reports for journal archives only**, has been added to the advanced SMTP policy setting, **Journal report processing**. When this value is set, journal reports are only processed for the following archive types: SMTP, Exchange Journal, Domino Journal, and Shared. Journal reports are discarded for user archive types, such as Exchange Mailbox and Internet Mail. This new value is now the default value for journal report processing.

After you have upgraded, check that the value that is assigned to the **Journal report processing** setting is the one that you want. It can have the following values:

- **Process journal reports for journal archives only**
  This is the new value and the default setting. If the value was **Process journal reports** before upgrading, then this value is assigned during the upgrade.
- **Process journal reports for all archives**
  This is the equivalent of **Process journal reports** in Enterprise Vault 12.2 or earlier releases.
- **Discard journal reports for all archives**
  This is the equivalent of **Discard journal reports** in Enterprise Vault 12.2 or earlier releases.

For information about each of these values, see the section, "Journal report processing (Advanced SMTP policy setting)", in the *Administrator's Guide*.

Checking the 'Journal Reports settings' advanced SMTP policy setting

Enterprise Vault 12.4 and later support the decryption of Office 365 RMS encrypted messages by using Azure Rights Management Services (RMS). The setting, **Decrypt RMS Protected Items**, has been added to the advanced SMTP policy setting, **Journal Reports settings**.

To allow Enterprise Vault to decrypt RMS-protected messages, check that the following settings are applied:

- **ClearText copies of RMS Protected items**
  This is an existing setting. Set this to **Treat as Secondary**.
- **Decrypt RMS Protected Items**
  This is the new setting. Set this to **Decrypt for journal archives only**.

For information about these values, see the section, "Journal Reports settings" (Advanced SMTP policy settings)", in the *Administrator's Guide*.

Checking the 'Selective Journal Archiving' site setting

In Enterprise Vault 12.3 and later, the upgrade process uses the value of the advanced SMTP site setting, **Selective Journal Archiving**, when determining the journaling type to apply to existing SMTP addresses. In Enterprise Vault 12.2, this setting was enhanced to give greater control over where the archiving task stores messages. After you upgrade the SMTP Archiving components, check that the value that is assigned to the site setting is the one that you want.

The **Selective Journal Archiving** site setting can have the following values:

- **Non-selective**
  This is the equivalent of **No** in Enterprise Vault 12.1 or earlier releases. If the setting value was **No** before upgrading, then the value **Non-selective** is assigned during the upgrade.
- **Inclusive**
  This is the equivalent of **Yes** in Enterprise Vault 12.1 or earlier releases. If the setting value was **Yes** before upgrading, then the value **Inclusive** is assigned during the upgrade.
- **Exclusive**
  This value was introduced at Enterprise Vault 12.2.

A detailed description of the effect of these values is provided in the section, "Configuring the SMTP site setting, Selective Journal Archiving", in the *Setting up SMTP Archiving* guide.

About upgrading legacy SMTP archiving components

Enterprise Vault 11.0.1 introduced a completely new version of SMTP Archiving. The new implementation does not require the Windows SMTP service or File System Archiving.

If you use a legacy version of Enterprise Vault SMTP Archiving, that version can run concurrently with the new version. The legacy version and the new version must use different port numbers.

If you want to continue to use the legacy Enterprise Vault SMTP Archiving components, install the Enterprise Vault 14.5 SMTP Archiving components, and rerun the legacy Enterprise Vault SMTP Archiving configuration process as follows:

- Open a command prompt window and change to the folder, *Enterprise Vault_installation_folder*\x64.
- Enter the following command:

  EVSMTPArchiveConfig *config_file*

  Where *config_file* is the name of the required configuration file. The default file is EVSMTPArchiveConfig.ini.

For guidance on how to migrate from the legacy version of SMTP Archiving to the new version, see Migrating from the Legacy SMTP Archiving Solution.

Migrating existing targets to provisioning groups

SMTP targets that you added in a previous release of Enterprise Vault will continue to work in Enterprise Vault 12.3 and later. In the Arctera Administration Console, existing targets are located under **Targets** > **SMTP** > **Manual targets**.

To take advantage of the easier maintenance provided by the SMTP provisioning feature in Enterprise Vault 12.3 and later, you may decide to migrate some or all of your existing targets to SMTP provisioning groups. Before you migrate targets to provisioning groups, read the "Planning your configuration" topic and "Provisioning users for SMTP Group or SMTP Mailbox Journaling" chapter in the *Setting up SMTP Archiving* guide.

Points to note when you configure the provisioning groups for the target users:

- In Enterprise Vault 12.3 and later, you can assign multiple archives to a single SMTP Group Journaling provisioning group.
- Only Internet Mail archives are supported in SMTP Mailbox Journaling provisioning groups. If your existing SMTP Mailbox Journaling targets use Exchange Mailbox archives for SMTP messages, these archives are no longer used under provisioning. Instead, provisioning creates new Internet Mail archives for each of these users. If a user already has an Internet Mail archive, then Enterprise Vault links that archive to the SMTP target.

To migrate existing targets to provisioning groups

1. Create the required SMTP Group or Mailbox Journaling provisioning groups, and add the target users. Add Active Directory target users by selecting one of the menu options other than **Email address**.

   Use the **Email address** option to add to the provisioning group the target SMTP address of a user who is not associated with an Active Directory account. For example, you can use this option to add to the group users who are external to your organization.
2. Check that the target users are in the correct provisioning groups.

3 Check that the provisioning groups are in the required order.

Enterprise Vault processes the groups from the top of the list down. If a user appears in more than one provisioning group, they are only provisioned in the first group in which they appear.

4 We strongly recommend that you stop the SMTP Archiving task until the provisioning run below has finished. This ensures that messages that arrive during the period when the original targets are deleted and the users are provisioned are not lost.

5 When you have checked that a user in the manual targets is included in a provisioning group, you can delete the manual target. Enterprise Vault does not provision the target user as a member of the group until you delete the existing target under **Manual targets**.

6 Run the SMTP provisioning task, and then check the provisioning task reports.

Reconfiguring targets that are configured for target address rewriting to use multiple archives

In Enterprise Vault 12.3 and later, you can assign multiple archives to an SMTP Journaling routing address, or an SMTP Group Journaling provisioning group to spread the archiving load over several archives and Enterprise Vault storage servers. In previous releases of Enterprise Vault, you could only implement target address rewriting to do this.

For existing targets that have been configured for target address rewriting, you can assign them to multiple archives instead. To do this, follow these steps on all the Enterprise Vault SMTP servers that you have configured for target address rewriting.

To reconfigure existing targets to use multiple archives

1 Log on to the Enterprise Vault SMTP server for which you have created the alias. Log in using the Vault Service account, or an account that is assigned to the SMTP Administrator role. The SMTP Administrator role is also included in the Messaging Administrator role and the Power Administrator role.

2 Stop the SMTP Archiving task.

3 Navigate to the folder, *Enterprise Vault installation folder*\SMTP\DATA\etc\switch.

4 Take a backup of the aliases file that has the target address domain as its filename. Remove the alias entry of the routing address and rename the file.

5 Update the properties of the routing address to assign multiple archives.

6 Restart the SMTP Archiving task.

Granting the Administrators group and system account full access to the SMTP holding folder

If you are upgrading from Enterprise Vault 12.4 or earlier, and have already configured an SMTP holding folder, you need to assign the Local System account and the local Administrators group full control on the SMTP holding folder.

Chapter 19

Upgrading your Enterprise Vault sites to use Enterprise Vault Search

This chapter includes the following topics:

- About Enterprise Vault Search
- Server requirements for Enterprise Vault Search
- Defining search policies for Enterprise Vault Search
- Allowing privileged Enterprise Vault Search users to restore items to other users' mailboxes
- Setting up provisioning groups for Enterprise Vault Search
- Creating and configuring Client Access Provisioning tasks for Enterprise Vault Search
- Configuring user browsers for Enterprise Vault Search
- Configuring Enterprise Vault Search for use in Forefront TMG and similar environments
- Setting up Enterprise Vault Search Mobile edition

About Enterprise Vault Search

Note: You need only follow the instructions in this chapter if you want to upgrade an Enterprise Vault site in which Enterprise Vault Search was not previously available.

Enterprise Vault Search enables client users to browse and search their archives. This feature replaces the legacy search applications: Archive Explorer, Browser Search, and Integrated Search, which are no longer available.

Server requirements for Enterprise Vault Search

Each Enterprise Vault server requires the Net.Tcp Listener Adapter service (NetTcpActivator) for Enterprise Vault Search. This service requires the following Windows Communication Foundation (WCF) Activation features:

- HTTP Activation
- Non-HTTP Activation

The Prepare My System option in the Enterprise Vault Install Launcher automatically installs these features, if they are not already installed. However, if you do not want to use the Prepare My System option, you can manually install the WCF Activation features.

To add the requirements for Enterprise Vault Search manually

1. Click **Start** > **Control Panel** > **Turn Windows features on or off**.

   The **Add Roles and Features** wizard starts.
2. Click **Next** until the **Features** page is shown.
3. Expand **.NET Framework 4.5 Features**.
4. Expand **WCF Services**.
5. Select **HTTP Activation** and then click **Install**.
6. Work through to the end of the wizard.

Defining search policies for Enterprise Vault Search

A search policy defines the range of Enterprise Vault Search facilities that you want to make available to users. With a search policy, you can choose to let Enterprise Vault Search users do the following:

- Show the reading pane. This pane displays a preview of the currently selected item in Enterprise Vault Search. For performance reasons, you may want to hide the reading pane to stop recalls from slow storage media, such as tape or optical disks.
- Export the items that are listed in Enterprise Vault Search to an `.nsf`, `.pst`, or `.zip` file, depending on the archive type.

  Some export formats are appropriate for use with certain types of items only. For example, it is not possible to export Outlook messages to a `.nsf` file, or Notes messages to a `.pst` file. A user who chooses to export both Outlook and Notes messages to a single file can export them to a `.zip` file only.
- Choose to allow the Enterprise Vault Search users generate an expiry report. An expiry report lists all archived items from Enterprise Vault, whose retention period is about to end. It lists the items that are about to expire in 60 days. Administrators can also generate the expiry report from the Enterprise Vault Administration Console so that the expiry report gets loaded in Enterprise Vault Search.
- Change the retention categories of the items in their archives. Note that some Enterprise Vault features, such as the retention folders and classification features, can override the changes that users make to the retention categories of items. For more information on retention, see the *Administrator's Guide*.
- Copy and move archived items out of an archive, within an archive, and from one archive to another. Choosing to allow these actions also allows users to create, rename, move, and delete folders in their archives.

  In addition, choosing to allow users to copy and move archived items out of an archive provides certain privileged users with an additional facility: users who have full access rights to other users' Exchange mailboxes can also restore items from Enterprise Vault journal archives to the **Restored Items** folders in these mailboxes.

  See "Allowing privileged Enterprise Vault Search users to restore items to other users' mailboxes" on page 100.
- Delete archived items. Note that, even if you define a search policy to grant delete permissions, users can only delete items if you have configured the Enterprise Vault site appropriately. In the Administration Console, open the **Site Properties** dialog box for the Enterprise Vault site and then, on the **Archive Settings** tab, ensure that **Users can delete items from their archives** is selected.
- When using the advanced search facilities in Enterprise Vault Search, choose from extra options on the **Select search property** drop-down list. These extra properties make it easier to build search queries for the items that the Enterprise Vault records management and classification features have tagged.

Installing Enterprise Vault creates a default search policy automatically. You can modify the properties of this default policy and define custom search policies. Then you can assign each policy to a different search provisioning group.

To view and modify the properties of the default search policy

1. In the left pane of the Administration Console, expand your Enterprise Vault site.
2. Expand the **Policies** container.
3. Click the **Search** container.
4. In the right pane, right-click **Default Search Policy** and then click **Properties**.

   You can change the settings on the **Features** and **Advanced Search** tabs, but you cannot change the settings on the other tabs.

To define a new search policy

1. In the left pane of the Administration Console, expand your Enterprise Vault site.
2. Expand the **Policies** container.
3. Right-click the **Search** container, and then click **New** > **Policy**.

   The **New Search Policy** wizard appears.
4. Follow the on-screen instructions. The wizard prompts you to specify the following:
   - The name of the policy and an optional description of it.
   - The Enterprise Vault Search facilities that you want to make available to users.

Allowing privileged Enterprise Vault Search users to restore items to other users' mailboxes

You may want to allow certain privileged users to restore items from Enterprise Vault journal archives to the **Restored Items** folders in other users' Exchange mailboxes. For example, if a user accidentally deletes an important email, a privileged user can search for it in a journal archive and copy the email back into the first user's mailbox. The online Help for Enterprise Vault Search provides instructions on how to do this.

We recommend that you set up dedicated user accounts for these privileged users, instead of extending the privileges that you have awarded to their normal user accounts. This enables the selected users to run Enterprise Vault Search in

the normal way for their own purposes, and only log in to it as a privileged user when they need to restore items to other users' mailboxes.

To allow privileged Enterprise Vault Search users to restore items to other users' mailboxes

1. In your search policy, enable the option **Allow copy and move out of an archive (Restore)**.
2. Ensure that the privileged users have at least Read access to the journal archives. You can do this by editing the properties of each archive with the Vault Administration Console.
3. Ensure that the privileged users have full access rights to the Exchange mailboxes to which they may need to restore items.

   For example, you can run the `Add-MailboxPermission` cmdlet in the Exchange Management Shell to grant one user full access to another's mailbox. For more information on this cmdlet, see the following article on the Microsoft website:

   https://technet.microsoft.com/en-us/library/bb124097.aspx

Setting up provisioning groups for Enterprise Vault Search

A search provisioning group identifies the users and user groups to whom you want to assign a search policy for Enterprise Vault Search. After you install Enterprise Vault, a default search provisioning group is available with which you can assign the default search policy to all users. If you want to assign a custom search policy to selected users or groups, you must set up a custom provisioning group. The default provisioning group continues to target those users whom you do not assign to a custom provisioning group.

You can set up any number of custom provisioning groups for different sets of targets. However, each provisioning group can target the users in one Active Directory domain or Domino domain, so you require at least as many groups as you have domains.

To view the properties of the default search provisioning group

1. In the left pane of the Administration Console, expand your Enterprise Vault site.
2. Expand the **Client Access** container and then expand the **Search** container.

3 Click the **Provisioning Groups** container.

4 In the right pane, right-click **Default Search Provisioning Group** and then click **Properties**.

You cannot amend any of the properties.

To set up a custom search provisioning group

1 In the left pane of the Administration Console, expand your Enterprise Vault site.

2 Expand the **Client Access** container and then expand the **Search** container.

3 Right-click the **Provisioning Groups** container, and then click **New** > **Active Directory Provisioning Group** or **New** > **Domino Provisioning Group**.

The **New Search Provisioning Group** wizard appears.

4 Complete the fields and then click **Create Provisioning Group**. The wizard prompts you to specify the following:

- The name of the provisioning group.
- The search policy to assign.
- The domain to which the provisioning group applies. You can enter the details of a new domain, if necessary.
  For an Active Directory domain, you must choose a trusted domain in your environment and optionally specify the required Global Catalog server. For a Domino domain, you must specify the name and password for the ID file that Enterprise Vault will use to access the domain, and the fully-distinguished name of any Domino server in the domain.
- The targets (individual users and user groups) of the provisioning group.
- The Enterprise Vault server that is to host the Client Access Provisioning task for this provisioning group. This task applies the required search policy to the targets of the provisioning group. You can host the task on any Enterprise Vault server in your site. However, if the task is to provision a Domino domain then you must ensure that Notes is installed on the server.
  Enterprise Vault creates the task automatically if one does not already exist for the nominated domain.

The provisioning group takes effect when the Client Access Provisioning task has run.

Changing the order in which Enterprise Vault processes the search provisioning groups

When you set up a search provisioning group, it automatically has the highest ranking in its domain. In consequence, Enterprise Vault processes the new provisioning group before it processes any other groups in the domain. You can change the order in which Enterprise Vault processes the provisioning groups, if necessary.

To change the order in which Enterprise Vault processes the search provisioning groups

1. In the left pane of the Administration Console, expand your Enterprise Vault site.
2. Expand the **Client Access** container and then expand the **Search** container.
3. Click the **Provisioning Groups** container.
4. Right-click a blank area of the right pane, and then click **Properties**.

   The **Provisioning Groups Properties** dialog box appears.
5. In the **Provisioning Groups** list, click a group and then click **Move Up** or **Move Down** to raise or lower its priority.

   If users are the targets of multiple provisioning groups, Enterprise Vault processes them as members of the topmost group only. Thereafter, Enterprise Vault ignores these users when it processes the lower priority provisioning groups.

Creating and configuring Client Access Provisioning tasks for Enterprise Vault Search

You require one Client Access Provisioning task for each Active Directory domain or Domino domain in which you want to apply search policies for Enterprise Vault Search. At specified times each day, the task applies the required search policy to users who are the targets of a provisioning group with which you have associated the task. You can host the task on any Enterprise Vault server in your site. However, if the task is to provision a Domino domain then you must ensure that Notes is installed on the server.

Besides processing the search provisioning groups for a domain, a Client Access Provisioning task also processes the domain's IMAP (Exchange Mailbox or Internet Mail) provisioning groups. These two types of provisioning group differ slightly in how the task processes them, in the event that the task is stopped before it has finished assigning the required policies to the target users.

- For a search provisioning group, the task does not assign the search policy to any users. When the task next runs, it starts from the beginning and assigns the policy to all users.
- For an IMAP provisioning group, those users to whom the task assigned a policy before it stopped retain that policy; the other users are not provisioned. However, when the task next runs, it starts from the beginning and reassigns the policy to all users.

If a suitable Client Access Provisioning task does not exist when you set up a search provisioning group, Enterprise Vault automatically creates one. However, you can manually create and configure this task at any time.

To create and configure a Client Access Provisioning task for Enterprise Vault Search

1. In the left pane of the Administration Console, find and then expand the **Enterprise Vault Servers** container.
2. Expand the container for the server to which you want to add the Client Access Provisioning task.
3. Right-click the **Tasks** container, and then click **New** > **Client Access Provisioning Task**.

   The **New Client Access Provisioning Task** dialog box appears.
4. Complete the fields and then click **OK**. The dialog box prompts you to specify the following:
   - The domain with which to associate the task.
   - The name of the task.
   - Whether to start the task now. If you want to configure the task before it starts, turn off this option and follow the instructions in step 5.
     The settings that you can configure include the times at which the task runs each day and the level of reporting that it undertakes for each provisioning run.
5. To configure the task, right-click it in the right pane, and then click **Properties**.

   The online Help provides detailed information on each field in the properties dialog box.

Configuring user browsers for Enterprise Vault Search

Client users require an HTML5-compatible web browser to benefit from all the new features in Enterprise Vault Search. Older browsers are supported, but the client experience may be compromised.

For the latest information on supported web browsers, see the Enterprise Vault Compatibility Charts.

Enterprise Vault Search uses the browser's language for the default time and date format in advanced search, the reading pane, and search results. If the browser is set to a language that is not supported, Enterprise Vault Search defaults to English (US). You may want to use a Group Policy Object (GPO) to set the Internet Explorer language for users. Note that users can change their Enterprise Vault Search language in their Enterprise Vault Search regional preferences.

Most users should not experience any problems when they access Enterprise Vault Search. However, they must set the following in their browsers to use Enterprise Vault Search:

- Allow cookies and local storage.
- Enable JavaScript.
- Disable private browsing or the settings that prevent their browsers from storing data about their browsing.
- If an option to not save encrypted pages to disk is available, disable it.

You can also minimize potential problems by configuring their web browsers to treat Enterprise Vault Search as a trusted site. How you do this varies from one browser to another, but the procedure for Internet Explorer is as described below.

If you use Active Directory, you can employ a group policy to apply the zone change to all the domain users. To do this, you must edit the Internet Explorer Maintenance settings within the policy.

To configure Internet Explorer to trust Enterprise Vault Search

1. On the client computer, open Internet Explorer.
2. On the **Tools** menu, click **Internet Options**.
3. Click the **Security** tab.
4. Click **Trusted sites**, and then click **Sites**.
5. Enter the fully-qualified domain name of the server on which you installed Enterprise Vault Search, and then click **Add**. For example, you might type **vault.company.com**.
6. Close the **Trusted sites** dialog box, and then close the **Internet Options** dialog box.

Configuring the Block Untrusted Fonts feature in Windows 10

Enterprise Vault Search uses font icons from the third-party Font Awesome toolkit. Windows 10 includes a Block Untrusted Fonts feature which stops

applications from loading untrusted fonts (third-party fonts that are not installed in the `%windir%/Fonts` folder). Turning on this feature may cause the font icons in Enterprise Vault Search to disappear.

For information on the Block Untrusted Fonts feature, and guidelines on how to stop it from being applied to selected applications, see the following article on the Microsoft website:

https://technet.microsoft.com/en-us/itpro/windows/keep-secure/block-untrusted-fonts-in-enterprise

Configuring Enterprise Vault Search for use in Forefront TMG and similar environments

By default, Enterprise Vault Search implements security best practices for all supported browsers. In some environments, these restrictions can affect the functionality of Enterprise Vault Search. For example, if you implement forms-based authentication through Forefront Threat Management Gateway (TMG), the reading pane of Enterprise Vault Search may contain the logon screen rather than a preview of the selected item.

This issue arises because Enterprise Vault Search uses an attribute to enforce the Restricted Sites zone settings in the reading pane. In fact, this mechanism is needed for Internet Explorer 9 and earlier only; version 10 and later uses a different security mechanism, which Enterprise Vault Search also implements. However, because version 10 and later still respects the older security mechanism, the reading pane does not work in these later versions either. So, if your users do not run Internet Explorer 9 and earlier, you can configure Enterprise Vault to not use the attribute to enforce the Restricted Sites zone settings. The reading pane then works without reducing security.

To configure Enterprise Vault Search for use in Forefront TMG and similar environments

1. Locate the following file on the Enterprise Vault server:

   ```
   C:\Program Files (x86)\Enterprise Vault\EVSearch\EVSearchClient\Web.config
   ```

2. Open the file in a text editor such as Windows Notepad.

3 Find the following line, and change the value from 1 to 0:

```
<add key="UseRestrictedSecurity" value="1"/>
```

A value of 1 enforces the security restrictions, whereas 0 relaxes them.

4 Save and close the file.

Setting up Enterprise Vault Search Mobile edition

Designed for use on Android, iOS, and Windows Mobile devices, Enterprise Vault Search Mobile edition enables users to access their archives through the web browsers on their smartphones. Those users for whom you provision Enterprise Vault Search on the desktop and tablet can also run the Mobile edition on their smartphones.

Enterprise Vault Search Mobile edition is a browser-based application that you deploy for intranet or Internet access using Microsoft Internet Information Services (IIS).

Caution: You can install the required components on the Enterprise Vault server. However, if you want to give your users Internet access to Enterprise Vault Search without exposing your Enterprise Vault server to unnecessary security risks, it is advisable to install the components on a proxy server.

Carrying out preinstallation tasks for Enterprise Vault Search Mobile edition

Before installing Enterprise Vault Search Mobile edition, you must perform the following tasks:

- If you want to install Enterprise Vault Search Mobile edition on a proxy server, ensure that the server meets the minimum requirements.
  See "Requirements for installing Enterprise Vault Search Mobile edition on a proxy server" on page 108.
- Obtain a digital certificate from a certification authority for setting up HTTPS.
- In a configuration providing direct access to the Enterprise Vault Search web server from the Internet, do the following:
  - Verify that the firewall or firewalls are configured to allow HTTPS access to the server on which you plan to install Enterprise Vault Search Mobile edition.
  - Configure any reverse proxy server that is installed in the DMZ.

- Ensure that the browsers of end-users are configured to allow cookies and local storage, enable JavaScript, and disable private browsing.

Requirements for installing Enterprise Vault Search Mobile edition on a proxy server

---

Caution: To maximize security, install Enterprise Vault Search on a reverse proxy server or protect the server with Microsoft Threat Management Gateway (TMG).

You can install Enterprise Vault Search Mobile edition on a proxy server on which you have also installed the following:

- One of the following versions of Windows:
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019

  The server must have an NTFS file system.
- The Enterprise Vault API Runtime. The process of installing Enterprise Vault Search Mobile edition on the proxy server automatically installs the API Runtime, if it is not already present.
- Internet Information Services (IIS) 8.0 or later.
  The following table lists the minimum set of role services that you must install for the Web Server (IIS) role.

Common HTTP Features	■ Static Content ■ Directory Browsing ■ HTTP Errors ■ HTTP Redirection
Application Development	■ ASP.NET ■ ISAPI Extensions ■ ISAPI Filters
Health and Diagnostics	■ HTTP Logging ■ Logging Tools
Security	■ Request Filtering
Performance	■ Static Content Compression

Management Tools
- IIS Management Console

- Microsoft .NET Framework 4.5.2.
  The Windows Communication Foundation (WCF) HTTP Activation feature must be installed and enabled. You do not need to install and enable the non-HTTP Activation feature.

In addition, you must ensure the following:

- The proxy server is part of a Windows domain.
- Distributed COM (DCOM) is enabled.
- Port 135 is open on the firewall.
- None of the following is also installed on the proxy server:
  - The Enterprise Vault server software
  - Microsoft SQL Server
  - Microsoft Exchange Server (the target system for Enterprise Vault archiving)

Disabling unsafe cryptographic protocols and cipher suites

If you want to give your users Internet access to Enterprise Vault Search without exposing your proxy server to unnecessary security risks, you can disable unsafe cryptographic protocols and cipher suites on the server.

When a client device uses HTTPS to connect to Enterprise Vault Search on a proxy server, the client and server negotiate a common cryptographic protocol to help secure the channel. If the client and server have multiple protocols in common, Internet Information Services (IIS) tries to secure the channel with one of the protocols that IIS supports. However, some protocols are stronger than others; to maximize the security of your environment, you may therefore want to disable the weak protocols in favor of stronger, Arctera-approved alternatives.

You can comply with Arctera recommendations by configuring the cryptographic protocols and cipher suites on your proxy server as follows:

- Enable the TLS 1.1 and 1.2 protocols.
- Disable the SSL 2.0 and 3.0 protocols.
- Disable the RC2, RC4, and DES cipher suites.

The following articles in the Microsoft Knowledge Base provide guidelines on how to implement these changes:

- http://support.microsoft.com/kb/187498

- http://support.microsoft.com/kb/245030

Installing Enterprise Vault Search Mobile edition

Whether you want to install the required components for Enterprise Vault Search Mobile edition on the Enterprise Vault server or on a proxy server, follow the steps below.

To install Enterprise Vault Search Mobile edition

1. On the server where you want to install Enterprise Vault Search Mobile edition, log in as the Vault Service account.
2. Load the Enterprise Vault installation media.
3. Do one of the following:
   - If an AutoPlay dialog box appears, click **Run Setup.exe**.
   - If AutoPlay is not enabled, use Windows Explorer to open the root folder of the installation media and then double-click the file `Setup.exe`.
4. In the left pane of the Arctera Enterprise Vault Install Launcher, click **Enterprise Vault**.
5. Click **Server Installation**.
6. Choose the required installation option.

   To install Enterprise Vault Search Mobile edition on a proxy server, choose **Installation on an additional server**.
7. Follow the instructions in the Enterprise Vault installation wizard.

   When the wizard prompts you to select the features that you want to install, do one of the following:
   - For installation on a proxy server, clear all the options except for **Search Access Components**.
     When you click **Next**, the wizard requests the Vault Site alias. This alias is the DNS alias for the Enterprise Vault site.
   - For installation on an Enterprise Vault server, choose all the required components.
     If you choose to install the Enterprise Vault services, or you have previously installed them on this server, then you cannot clear the **Search Access Components** option. The components will be automatically installed.

8 Follow the on-screen instructions to complete the remaining steps in the installation wizard.

9 Ensure the Enterprise Vault Search web application is configured for HTTPS to secure transmitted data.

On the Enterprise Vault server and on the proxy server, the Enterprise Vault Search web application is configured in the Default Web Site in IIS. In a new Enterprise Vault installation of 12.3 or later, Enterprise Vault automatically configures HTTPS on port 443 as default. If SSL is not already configured on the Default Web Site, Enterprise Vault configuration creates and installs a self-signed certificate, and adds an HTTPS binding on port 443 using the certificate. On an Enterprise Vault server, the configuration wizard then enables SSL on all of the Enterprise Vault virtual directories. On a proxy server, the configuration wizard enables SSL on the virtual directory, `EnterpriseVault\Search`.

We recommend that you replace the self-signed certificate as soon as possible with one obtained from a trusted authority.

If you have already installed a certificate and configured a valid HTTPS binding on port 443, then Enterprise Vault configuration uses the existing binding.

If you are upgrading from a version of Enterprise Vault that is earlier than 12.3, then Enterprise Vault does not change the existing IIS configuration on the Enterprise Vault server or proxy server. If HTTPS is not already configured for Enterprise Vault virtual directories, then you need to do this manually on the Enterprise Vault server and on the proxy server.

Configuring the maximum number of permitted login attempts to Enterprise Vault Search Mobile edition

By default, users who make five unsuccessful attempts to log in to Enterprise Vault Search Mobile edition are barred for 24 hours from making further login attempts from the same device. You can configure the maximum number of login attempts that you want to permit and the number of hours for which barred users are locked out.

To configure the maximum number of permitted login attempts

1 Locate the following file on the Enterprise Vault server:

```
C:\Program Files (x86)\Enterprise
Vault\EVSearch\EVSearchClient\Web.config
```

2 Open the file in a text editor such as Windows Notepad.

3 Find the following lines and change the values to the required ones.

```
<add key="EVSMobileMaxFailedAttemptsAllowed" value="5" />
<add key="EVSMobileLoginRestrictedTimeoutInHours" value="24" />
```

4 Save and close the file.

Verifying the installation of Enterprise Vault Search Mobile edition

Before you make Enterprise Vault Search Mobile edition available to users, follow the steps below to verify the installation.

To verify the installation of Enterprise Vault Search Mobile edition

1 Open a web browser on a smartphone that has Internet access.

2 In the **Address** field, enter the Mobile Search URL as follows:

https://*server*/enterprisevault/search

Where *server* is the name or IP address of the server on which you installed the search components.

3 Click **Go** or press **Enter** to display the Sign In page.

4 Enter the details of a user who has access to at least one archive.

5 Click **Sign In**.

If your authentication is valid, you see the home page of Enterprise Vault Search.

6 Perform a search to verify that Enterprise Vault Search can return search results.

7 Click a message in the search results and verify that you can see its contents.

Chapter 20

Upgrading Enterprise Vault API applications

This chapter includes the following topics:

- Upgrading any applications that use the Enterprise Vault API Runtime

Upgrading any applications that use the Enterprise Vault API Runtime

You may have installed a third-party application that uses the Enterprise Vault API to archive proprietary data or filter the data that Enterprise Vault stores. After upgrading Enterprise Vault, you may need to perform the following additional tasks to upgrade these applications:

- If the application uses the Enterprise Vault API Runtime, you need to update the API Runtime on each computer that hosts the application.
- For a .NET application that uses a specific version of the Enterprise Vault API Runtime, you need to update the binding redirections in the application's configuration file.
  For instructions on how to update the binding redirections, see the document `ReadMeFirst_en.htm`. The document is located with the API Runtime kit in the `API Runtime` folder on the Enterprise Vault media.