Enterprise Vault™
Setting up SMTP Archiving

15.1

VERITAS™

Enterprise Vault™: Setting up SMTP Archiving

Last updated: 2024-09-02.

Legal Notice

Veritas Technologies LLC, 2625 Augustine Drive, Santa Clara, CA 95054

https://www.veritas.com

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Before you contact Technical Support, run the Veritas Quick Assist (VQA) tool to make sure that you have satisfied the system requirements that are listed in your product documentation. You can download VQA from the following article on the Veritas Support website:

https://www.veritas.com/support/en_US/vqa

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 Veritas 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:

evdocs@veritas.com

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

https://www.veritas.com/community

Contents

Chapter 1

About this guide

This chapter includes the following topics:

Introducing this guide

This guide describes how to set up Enterprise Vault SMTP Archiving to archive data that is sent to the Enterprise Vault server using the SMTP protocol.

Where to get more information about Enterprise Vault

Table 1-1 lists the documentation that accompanies Enterprise Vault. This documentation is also available in PDF and HTML format in the Veritas Documentation Library.

Table 1-1 Enterprise Vault documentation set

Document	Comments
Veritas Enterprise Vault Documentation Library	Includes all the following documents in Windows Help (`.html`) format so that you can search across them all. It also includes links to the guides in Acrobat (`.pdf`) format. You can access the library in several ways, including the following: ■ In Windows Explorer, browse to the `Documentation\`*`language`*`\Administration Guides` subfolder of the Enterprise Vault installation folder, and then open the `EVAdmin_intro.htm` file from the `EV_Help` folder. ■ On the **Help** menu in the Administration Console, click **Help on Enterprise Vault**.
Introduction and Planning	Provides an overview of Enterprise Vault functionality.
Deployment Scanner	Describes how to check the required software and settings before you install Enterprise Vault.
Installing and Configuring	Provides detailed information on setting up Enterprise Vault.
Upgrade Instructions	Describes how to upgrade an existing Enterprise Vault installation to the latest version.
Setting up Domino Server Archiving	Describes how to archive items from Domino mail files and journal databases.
Setting up Exchange Server Archiving	Describes how to archive items from Microsoft Exchange user mailboxes, journal mailboxes, and public folders.
Setting up File System Archiving	Describes how to archive files that are held on network file servers.
Setting up IMAP	Describes how to configure IMAP client access to Exchange archives and Internet Mail archives.
Setting up SharePoint Server Archiving	Describes how to archive documents from Microsoft SharePoint servers.
Setting up Skype for Business Archiving	Describes how to archive Skype for Business sessions.
Setting up SMTP Archiving	Describes how to archive SMTP messages from other messaging servers.

Table 1-1 Enterprise Vault documentation set *(continued)*

Document	Comments
Setting up Microsoft Teams Archiving	Describes how to archive Microsoft Teams data.
Classification using the Veritas Information Classifier	Describes how to use the Veritas Information Classifier to evaluate all new and archived content against a comprehensive set of industry-standard classification policies. If you are new to classification with Enterprise Vault, we recommend that you use the Veritas Information Classifier rather than the older and less intuitive File Classification Infrastructure engine.
Administrator's Guide	Describes how to perform day-to-day administration procedures.
PowerShell Cmdlets	Describes how to perform various administrative tasks by running the Enterprise Vault PowerShell cmdlets.
Auditing	Describes how to collect auditing information for events on Enterprise Vault servers.
Backup and Recovery	Describes how to implement an effective backup strategy to prevent data loss, and how to provide a means for recovery in the event of a system failure.
Reporting	Describes how to implement Enterprise Vault Reporting, which provides reports on the status of Enterprise Vault servers, archives, and archived items. If you configure FSA Reporting, additional reports are available for file servers and their volumes.
NSF Migration	Describes how to import content from Domino and Notes NSF files into Enterprise Vault archives.
PST Migration	Describes how to migrate content from Outlook PST files into Enterprise Vault archives.
Utilities	Describes Enterprise Vault tools and utilities.
Registry Values	A reference document that lists the registry values with which you can modify many aspects of Enterprise Vault behavior.
Help for Administration Console	The online Help for the Enterprise Vault Administration Console.
Help for Enterprise Vault Operations Manager	The online Help for Enterprise Vault Operations Manager.

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

Enterprise Vault training modules

Veritas Education Services provides comprehensive training for Enterprise Vault, from basic administration to advanced topics and troubleshooting. Training is available in a variety of formats, including classroom-based and virtual training.

For more information on Enterprise Vault training, curriculum paths, and certification options, see https://www.veritas.com/services/education-services.

Chapter 2

Introducing Enterprise Vault SMTP Archiving

This chapter includes the following topics:

About Enterprise Vault SMTP Archiving

Enterprise Vault SMTP Archiving enables Enterprise Vault to archive data that is sent to the Enterprise Vault server using the SMTP protocol.

Here are some example applications of SMTP Archiving:

- Ingest directly into an archive journal emails sent over SMTP from cloud-based email services, such as Office 365 and Google Mail.
- Ingest directly into an archive journal emails from on-premise email platforms, such as Exchange Server, Lotus Domino, Sun Mail System, Zimbra.
- Capture all metadata, such as BCC, point in time distribution list membership, journal report information, and so on.
- Provide additional data for supervisory sampling using Compliance Accelerator.

- Provide additional data for eDiscovery search and review using Discovery Accelerator.
- Ingest data from any other application capable of sending email, such as log files, voicemail, scanners, printers, fax machines, and so on.
- Populate mailbox archives from the journal feed, where each user's archive is a representation of their personal journal showing Inbox and Sent items.
- Replace mail-enabled Exchange Public Folders, to provide users with a more scalable, shared solution.

SMTP Archiving can be used to provide journaling for any application that can send messages over SMTP. Journal report messages (P1 messages) that are sent to Enterprise Vault SMTP servers must comply with the envelope journal report format that is described in the article, http://technet.microsoft.com/library/bb331962.aspx. The journal report messages are processed by Enterprise Vault, and available for searching using an eDiscovery application, such as Veritas Discovery Accelerator.

Note: SMTP Archiving does not currently process the journal report information in messages that are journaled by Domino Server.

Figure 2-1 SMTP Archiving overview

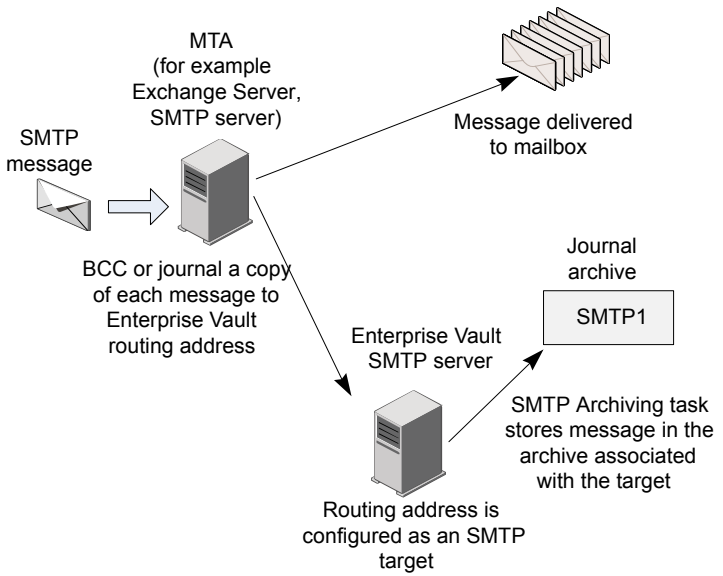


Figure 2-1 shows an example of a simple SMTP Journaling environment:

- An MTA receives an SMTP message from some application.
  The MTA could be an Exchange Server, or some other server that can route SMTP messages.
- The MTA sends the message to the destination mailbox.
- In addition, the MTA is configured to copy or journal the message to the SMTP routing address for the Enterprise Vault SMTP server. The domain used in the routing address could just be an MX record alias that you create in DNS to point to the Enterprise Vault SMTP server, for example, ev.example.com.
  In Enterprise Vault, you must configure the routing address as an SMTP target address.
- The Enterprise Vault SMTP server receives the message, and adds the routing address to the message as an X-RCPT-TO header.
  The SMTP server then places the message as an email (.eml) file in the folder that you assign as the SMTP holding folder.
- The SMTP Archiving task processes the message file in the holding folder, and archives it in the archive specified for the target address. During processing, the task applies the retention category that is specified in the target properties, and ensures that Enterprise Vault indexes any X-Headers that are listed in the policy.

An Enterprise Vault SMTP server is an Enterprise Vault server that hosts the Enterprise Vault SMTP Archiving components. The components include an SMTP server and an Enterprise Vault SMTP Archiving task. Table 2-2 provides an overview of the main components of SMTP Archiving.

An Enterprise Vault SMTP server can host only one SMTP server and one SMTP Archiving task. However, there can be multiple Enterprise Vault SMTP servers in a site. When you configure SMTP Archiving, the Enterprise Vault SMTP server settings and target configuration information are shared with all the Enterprise Vault SMTP servers in the site. This means that any Enterprise Vault SMTP server in the site can archive messages sent to any SMTP target in the site.

You can use a load balancing solution to distribute the SMTP traffic evenly across the SMTP servers in the site. A simple load balancing solution is to configure a DNS MX record for each of the Enterprise Vault SMTP servers, and give each record equal preference. If you use a single address for journaling, for example SMTPjournal@example.com, and the volume of traffic is more than one Enterprise Vault SMTP server can manage, you can either associate this routing address with multiple archives in different vault stores hosted on different Enterprise Vault storage servers, or implement address rewriting on the SMTP servers. Both these solutions enable you to spread the archiving load over several Enterprise Vault storage servers.

SMTP Archiving configurations

You can configure SMTP Archiving in different ways depending on whether you want to archive all messages that are sent to the Enterprise Vault SMTP servers, or only the messages of selected users. Table 2-1 provides a summary of the different journaling configurations that you can implement. These configurations are explained in more detail in the sections indicated.

Table 2-1 SMTP Archiving configurations

SMTP Archiving configuration	Description
SMTP Journaling	All messages that are sent to the Enterprise Vault SMTP servers are stored in one or more journal archives. The administrator needs to add access permissions to the group's archives. See "About SMTP Journaling" on page 18.
SMTP Group Journaling (previously known as Selective SMTP Journaling)	You configure the Enterprise Vault to archive only messages to or from specific target users or addresses. Enterprise Vault can store the messages from all the targets in the same archives. SMTP provisioning is the recommended way to configure groups of users for SMTP Group Journaling. The administrator needs to add access permissions to the group's archives. See "About SMTP Group Journaling" on page 20.
SMTP Mailbox Journaling	Enterprise Vault stores all messages to and from a specific target user in an archive that is exclusive to that user. SMTP provisioning is the recommended way to configure groups of users for SMTP Mailbox Journaling. For Active Directory target users, provisioning automatically gives the target user access permissions on their Internet Mail archive. See "About SMTP Mailbox Journaling" on page 22.

Table 2-1 SMTP Archiving configurations *(continued)*

SMTP Archiving configuration	Description
SMTP Journaling + SMTP Group Journaling	SMTP Journaling captures all the messages sent to the Enterprise Vault SMTP servers, and SMTP Group Journaling stores messages for a particular group of users in one or more archives assigned to the group. The SMTP site setting "Selective Journal Archiving" lets you control where the group's messages are stored; in the group's archives only, or in the general journal archives and in the group's archives. The administrator needs to add access permissions to the group's archives.
SMTP Journaling + SMTP Mailbox Journaling	SMTP Journaling captures all the messages sent to the Enterprise Vault SMTP servers, and SMTP Mailbox Journaling stores messages for SMTP Mailbox Journaling users in their personal archive. The SMTP site setting "Selective Journal Archiving" lets you control whether the SMTP Mailbox Journaling users' messages are stored in the user's personal archive only, or in the general journal archives and in the personal archive. For Active Directory target users, provisioning automatically gives the target user access permissions on their Internet Mail archive.

If you configure SMTP Journaling with either SMTP Group or Mailbox Journaling, then consider your archiving strategy when deciding where messages are stored. The following list illustrates some reasons why a combined approach may be required:

- General journaling is needed for data protection compliance, and users need access to their messages. To satisfy these requirements, you can use SMTP Journaling with SMTP Mailbox Journaling, and configure Enterprise Vault to archive messages in both journal and personal archives.
- General journaling is needed for most users, but the messages of a group of senior managers must be kept separate and confidential. To satisfy these requirements, SMTP Journaling with SMTP Group Journaling may be more appropriate. You can configure Enterprise Vault to store the senior managers' messages in the group archives only. All other messages are stored in the general journal archives. You can set the required access permissions on the group's archives to maintain confidentiality.

With SMTP Group Journaling and SMTP Mailbox Journaling, a copy of a message may be stored in multiple archives. Enterprise Vault implements single-instance storage as permitted by the vault store configuration.

If a message contains multiple target addresses that have the same destination archive, and the same retention category and policy are applied to the target addresses, only one copy of the message is stored in the archive.

SMTP Archiving components

To implement SMTP Archiving, you install the Enterprise Vault SMTP Archiving components and the Enterprise Vault server components on the computers that you want to perform SMTP Archiving. Table 2-2 provides an overview of the main components of SMTP Archiving. You can configure SMTP Archiving using the Enterprise Vault Administration Console, or Enterprise Vault PowerShell cmdlets.

Table 2-2 Overview of SMTP Archiving components

Component	Description
Enterprise Vault SMTP server	The SMTP server is implemented as the Windows service, Enterprise Vault SMTP service. This service is displayed in the Windows Services Console, but not in the Enterprise Vault Administration Console. The SMTP server manages SMTP connections, and receives messages that are sent to the Enterprise Vault SMTP server by relay Message Transfer Agents (MTAs), such as Exchange Server, or SMTP servers. The Enterprise Vault SMTP server stores the messages as .eml files in the SMTP holding folder. An Enterprise Vault SMTP server can host only one SMTP server.
SMTP Archiving task	The SMTP Archiving task processes the email files in the holding folder as follows: ■ Checks the message header for SMTP target addresses. ■ Applies the configured policy and retention, and stores the message in the archive. ■ When the message has been archived, deletes the file from the holding folder.

Table 2-2 Overview of SMTP Archiving components *(continued)*

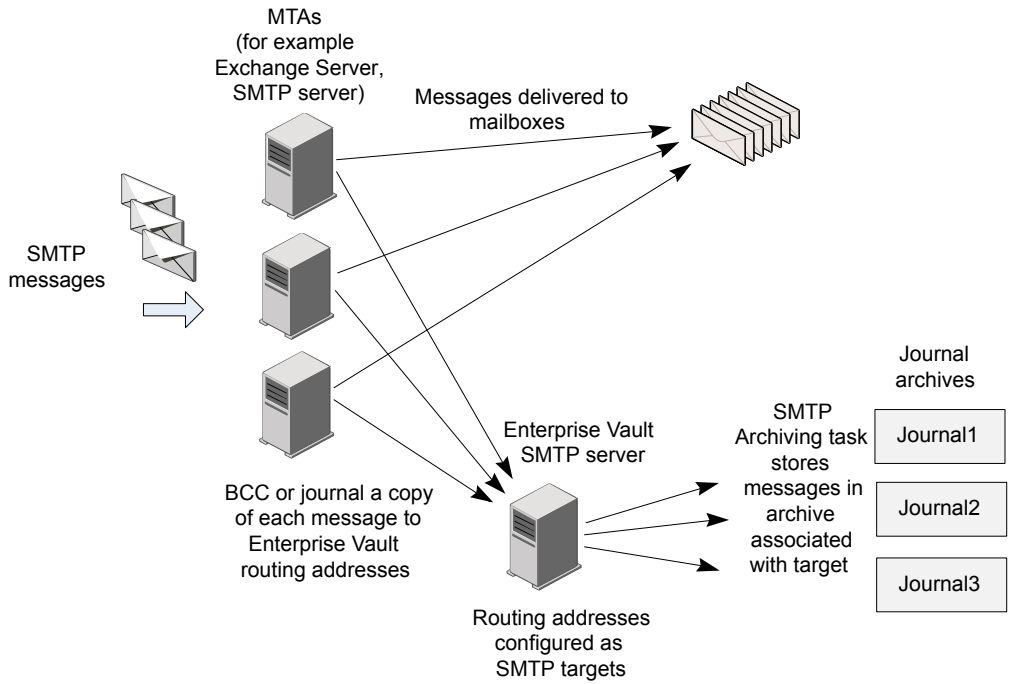
Component	Description
SMTP Provisioning task	The SMTP Provisioning task processes the members of provisioning groups. The task automatically creates SMTP targets for the users and addresses in the provisioning groups, and applies the same policy and retention to all the members of the same group. For SMTP Mailbox Journaling, the task automatically creates an Internet Mail archive for each member of the provisioning group. If an Internet Mail archive already exists for a group member, the task links the archive to the SMTP target.
SMTP holding folder	The SMTP holding folder is a local folder that is assigned to the SMTP Archiving task. The folder location is in the SMTP Archiving task properties. The Enterprise Vault SMTP server places messages in the folder for the archiving task to process. Messages that the archiving task fails to archive are not deleted automatically from the holding folder. The messages are placed in a Failed subfolder.
SMTP policies	An SMTP policy is assigned to an SMTP target address. The policy defines how the SMTP Archiving task manages journal reports and X-Headers, when archiving messages that contain the target address.
Manual targets	Manual targets are the SMTP target addresses that you add individually. For example, you add SMTP routing addresses as manual targets. Prior to Enterprise Vault 12.3, all SMTP target addresses were added as manual targets. However, in Enterprise Vault 12.3 and later, we recommend that you use provisioning groups to add target addresses other than routing addresses.
SMTP provisioning groups	SMTP provisioning groups facilitate the creation and management of large numbers of SMTP targets for SMTP Group and Mailbox Journaling. The SMTP provisioning task processes the provisioning groups.

Table 2-2 Overview of SMTP Archiving components *(continued)*

Component	Description
SMTP archives	An SMTP archive is a journal type archive that you can use for SMTP Journaling and SMTP Group Journaling. If you create archives in the new SMTP target or new SMTP Group Journaling provisioning group wizard, you can only create SMTP archives. However, if you select existing archives for SMTP Journaling and SMTP Group Journaling targets, the following types of archive are supported: SMTP, Shared, Exchange Journal, and Domino Journal.

About SMTP Journaling

Figure 2-2 Example of SMTP Journaling



Typically within an organization, SMTP messages are delivered to user mailboxes by one or more MTAs. The MTAs are usually Exchange Servers, or SMTP servers.

You configure these MTAs to journal or BCC a copy of each message to an Enterprise Vault SMTP routing address, for example, journal1@ev.example.com.

In Enterprise Vault, you configure the routing addresses as manual SMTP targets, and associate each target address with one or more archives. In the manual target properties, ensure that the target address is enabled for archiving. The check box, **Archive messages sent from or received by this SMTP address**, must be selected to enable a target address for archiving. When you add a new manual target, the check box is selected by default. Note that you cannot use SMTP Provisioning groups to add the routing addresses.

The Enterprise Vault SMTP server checks that the recipient address in an incoming message is an SMTP target, and adds this routing address to the message as an X-RCPT-TO header. The SMTP server then places the message as an .eml file in the SMTP holding folder.

The SMTP Archiving task then processes the message file in the holding folder. As you enabled the target address for archiving, the task stores the message in one of the archives associated with the target routing address. The archive types that you can use for journal archiving are SMTP, Shared, Exchange Journal, or Domino Journal archives. In archive types that contain folders, such as SMTP archives, the SMTP Archiving task stores all messages in the Inbox. Other journal archive types, such as Shared and Exchange Journal archives, do not contain folders. In these archives, the task stores all messages in the root of the archive.

In SMTP Journaling, the SMTP Archiving task only needs to examine the X-RCPT-TO field in each message in the holding folder. The advanced SMTP site setting, **Selective Journal Archiving**, configures the archiving task to search all of the sender and recipient fields (X-RCPT-TO, To, CC, BCC, From, Sender) in each message. If you are not using SMTP Journaling in combination with another type of SMTP archiving, this advanced site setting should be set to **Non-selective**, the default value. This optimizes performance.

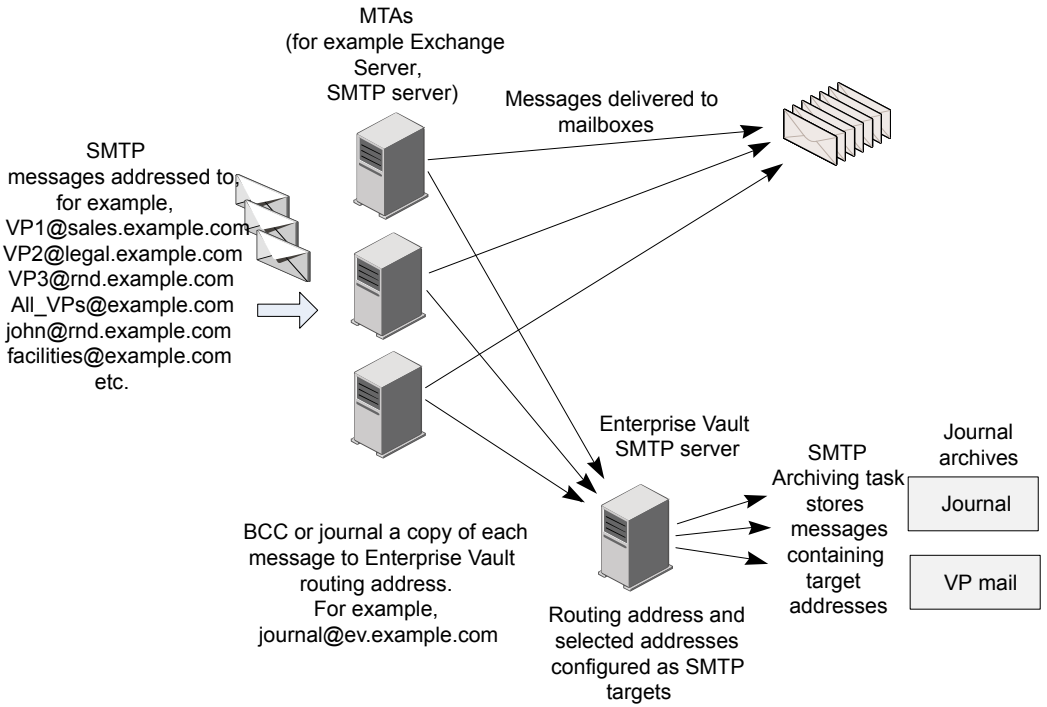
Figure 2-2 shows a simple environment with one Enterprise Vault SMTP server. (Production environments typically include several Enterprise Vault SMTP servers.) As there could be a large volume of messages for journaling, it is advisable to spread the archiving load over several Enterprise Vault storage servers. You can do this by creating several journal archives in different vault stores. A different Enterprise Vault storage service should manage each of the vault stores. If you use a single SMTP routing address, we recommend that you associate the routing address with multiple archives in different vault stores hosted on different Enterprise Vault storage servers. Enterprise Vault automatically performs load-balancing to spread the archiving load over several Enterprise Vault storage servers. Alternatively you can implement target address rewriting on the SMTP servers.

If the relay MTA is Exchange Server, you can create journal rules to select the appropriate routing address for the Enterprise Vault SMTP server.

See "Journaling messages to Enterprise Vault from Exchange Server or Office 365" on page 24.

About SMTP Group Journaling

Figure 2-3 Example of SMTP Group Journaling



Note: SMTP Group Journaling was previously known as Selective SMTP Journaling.

You can implement SMTP Group Journaling if you want Enterprise Vault to archive only messages to or from specific addresses. Enterprise Vault can store all the messages in the same archive, or in several different archives. For example, in Figure 2-3 the messages to and from all the senior managers in example.com are

archived in a separate archive. The messages to and from VP1, VP2, and VP3 are stored in the archive called VP mail. The addresses for these managers are added as SMTP targets and enabled for archiving. The addresses john@rnd.example.com and facilities@example.com are not configured as SMTP targets.

The address, All_VPs@example.com, is the SMTP address for a distribution list that includes all the senior managers in the company. To ensure that Enterprise Vault finds the selected target addresses in distribution lists, hub transport servers must expand the distribution lists in journaled messages. This must be done before the messages are sent to Enterprise Vault SMTP servers.

As in SMTP Journaling, the relay MTAs BCC or journal copies of all messages to the Enterprise Vault SMTP routing address. The Enterprise Vault SMTP server recognizes the routing address as a target address, and puts the message in the SMTP holding folder. The SMTP Archiving task then processes the messages in the holding folder, and archives them according to the target configuration settings.

To simplify the creation and maintenance of SMTP Group Journaling targets, we recommend that you create provisioning groups for the users that you want to add as targets. You can create different provisioning groups for different groups of target users. When you create a provisioning group, you select the archives for that group. Enterprise Vault automatically maintains the consistency of retention settings across the archives assigned to a group.

If you are implementing both SMTP Journaling and SMTP Group Journaling, the advanced SMTP site setting, **Selective Journal Archiving**, lets you control where messages are stored. You can archive target users' messages in the SMTP Journaling archives and in the SMTP Group Journaling archives, or only in the SMTP Group Journaling archives.

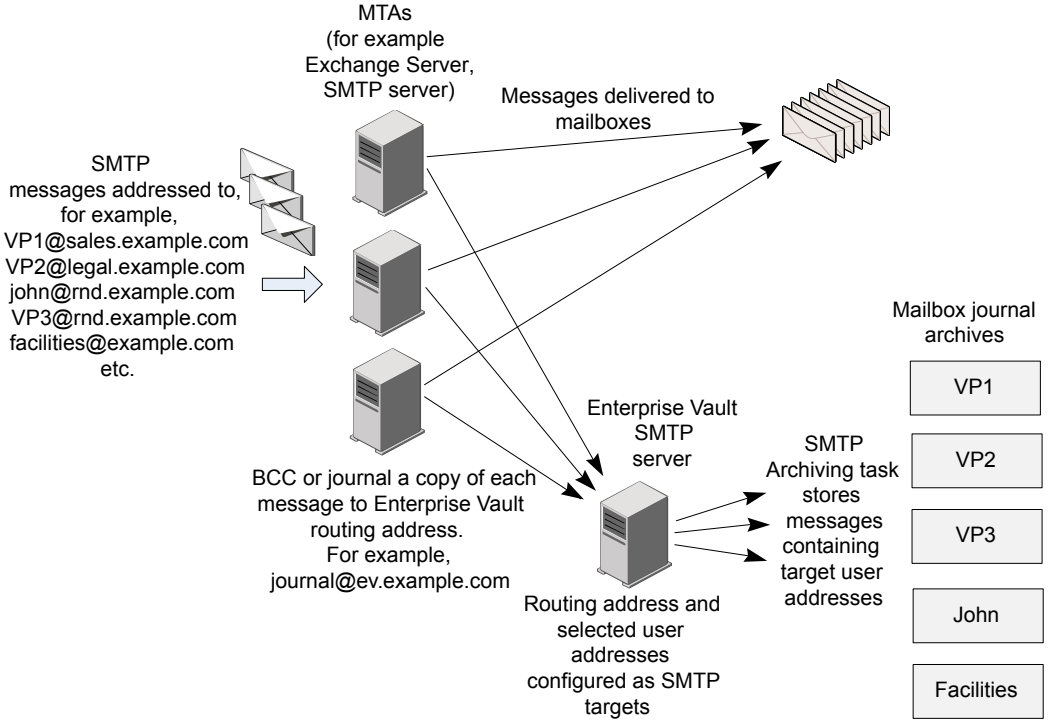
See “Configuring the SMTP site setting, Selective Journal Archiving” on page 80.

The archive types that can be used for SMTP Group Journaling are SMTP, Shared, Exchange Journal, or Domino Journal archives. In archive types that contain folders, such as SMTP archives, the SMTP Archiving task stores the messages in the Inbox. Other journal archive types, such as Shared and Exchange Journal archives, do not contain folders. In these archives, the task stores the messages in the root of the archive. If you create an archive in SMTP Group Journaling provisioning group, and create a new SMTP archive as part of the process, Enterprise Vault creates an SMTP archive.

If a message contains several of the target email addresses, a copy of the message may be stored in more than one archive. Enterprise Vault implements single-instance storage as permitted by the vault store configuration.

About SMTP Mailbox Journaling

Figure 2-4 Example of SMTP Mailbox Journaling



You can implement SMTP Mailbox Journaling if you want Enterprise Vault to store all messages to and from a specific target user in an archive that is exclusive to that user. For example, in Figure 2-4, the messages to and from VP1, VP2, and so on, are stored in separate archives, that are specifically for those addresses. The addresses for users, VP1, VP2, and so on, are added as SMTP target addresses and enabled for archiving.

We recommend that you create SMTP Mailbox Journaling provisioning groups to configure users for SMTP Mailbox Journaling. Provisioning creates targets for each user, and applies the policy and retention settings of the provisioning group. Provisioning automatically creates an Internet Mail archive for each user, or links an existing Internet Mail archive. Provisioning supports only Internet Mail archives for SMTP Mailbox Journaling.

If required, you can create manual targets for SMTP Mailbox Journaling. Exchange Mailbox archives and Internet Mail archives are supported for manual SMTP Mailbox Journaling targets.

Messages that contain a target address in a recipient field are stored in the Inbox of the archive. If a target address is found in the Sender field or From field, the message is stored in the Sent Items folder. If a target address is both the sender and recipient of a message, the message is stored in both the Inbox and the Sent Items folder.

In SMTP Mailbox Journaling, there are typically many target addresses and archives to manage. More copies of a message may be archived than in SMTP Group Journaling. As an example, take a message that contains the SMTP target addresses for user1 and user2. In SMTP Group Journaling, user1 and user2 addresses may be associated with the same journal archive, so only one copy of the message is stored. In SMTP Mailbox Journaling, user1 and user2 addresses would be associated with separate archives, so two copies of the message are stored; one in each archive. Where possible, Enterprise Vault uses single instance storage when archiving multiple copies of SMTP messages.

You can configure SMTP Journaling with SMTP Mailbox Journaling. If the advanced SMTP site setting **Selective Journal Archiving** is set to **Inclusive**, Enterprise Vault stores a target user's messages in the archive assigned to the target user, and also in the journal archive assigned to the routing address. If the setting value is **Exclusive**, Enterprise Vault stores the target user's messages in the user's archive only.

To ensure that all mail to or from a particular mailbox address is captured, it is important that hub transport servers expand distribution lists in messages before the messages are sent to Enterprise Vault SMTP servers.

About SMTP Archiving licensing

You must install an SMTP Archiving license (EVSMTPArchiving) on each Enterprise Vault server that is to perform SMTP Archiving. If you plan to implement SMTP Mailbox Journaling, you need to install both an EVSMTPArchiving license and an EVArchive license on each Enterprise Vault SMTP server. Enterprise Vault cannot archive data from SMTP targets, if valid licenses are not installed.

See *Installing and Configuring* for information about licenses.

Journaling messages to Enterprise Vault from Exchange Server or Office 365

As an alternative to Enterprise Vault Exchange Journal Archiving, you can use Enterprise Vault SMTP Archiving to store journaled messages from an Exchange Server. You can also use SMTP Archiving to store journaled messages from Office 365. For detailed instructions on how to configure Exchange Server or Office 365 to journal messages to Enterprise Vault, see the document, Setting up Exchange Server and Office 365 for Enterprise Vault SMTP Archiving.

About using SMTP Archiving to store Exchange journaled messages

If you plan to use SMTP Archiving to store journaled messages from an Exchange Server, then you do not have to set up Enterprise Vault Exchange Journal Archiving in addition to SMTP Archiving.

For SMTP Archiving, you can configure Exchange Server to journal messages to an SMTP address.

You can use either Exchange Database Journaling or Transport Rule Journaling to archive the mail of a subset of users in an Exchange database. Transport Rule Journaling requires an Exchange Enterprise CAL.

- If you use Database Journaling, then you can configure Exchange to journal all users in a particular Exchange database to Enterprise Vault.
- If you use Transport Rule Journaling, then you can create Exchange journal rules to select which users are journaled to Enterprise Vault.

Alternatively, if you use Exchange Database Journaling and want to archive the messages of selected mailboxes, you can move the mailboxes to databases that are set to journal to Enterprise Vault SMTP Archiving servers.

In SMTP Journaling, you can configure one or more routing addresses. To each routing address you can assign multiple archives. To optimize performance, the archives should be on different Enterprise Vault storage servers. Enterprise Vault automatically balances the load across the archives that are assigned to a routing address. You can use Exchange Transport Rule Journaling rules to send messages to the appropriate target routing address.

See “Assigning multiple archives to spread the archiving load across servers” on page 65.

Note that SMTP Archiving does not support messages in Transport Neutral Encapsulation Format (TNEF), also known as Outlook Rich Text Format. Messages sent by Exchange Server to Enterprise Vault must be in HTML or plain text format.

Chapter 3

Installing SMTP Archiving

This chapter includes the following topics:

About installing Enterprise Vault SMTP Archiving components

On each server that you want to perform SMTP Archiving you need to install at least the Enterprise Vault Services and the SMTP Archiving components.

See *Installing and Configuring* for the required software and settings for Enterprise Vault SMTP servers, and for detailed instructions on how to install, configure, and perform the initial set up of Enterprise Vault.

When the Enterprise Vault installation program installs the SMTP Archiving components, it installs an SMTP server. The SMTP server is implemented as a Windows service called Enterprise Vault SMTP service. This service is displayed in the Windows Services console, but not in the Enterprise Vault Administration Console.

After you have completed the initial set up of Enterprise Vault, you are ready to configure the SMTP Archiving feature as described in this guide.

If you are installing the Enterprise Vault SMTP components on an existing Enterprise Vault server, then you can either use existing vault stores and archives, or create ones specifically for the SMTP content. Enterprise Vault implements single-instance storage as permitted by the vault store configuration.

See “Configuring archives for SMTP messages” on page 63.

If you are using Enterprise Vault SMTP Archiving to store journaled messages from an Exchange Server, then you do not have to set up Enterprise Vault Exchange Journal archiving in addition to SMTP Archiving.

See "Journaling messages to Enterprise Vault from Exchange Server or Office 365" on page 24.

Reporting

The SMTP Archiving task generates summary reports and error log reports in the folder *Enterprise_Vault_installation_folder*\Reports\SMTP*SMTP_task_name*.

The SMTP Provisioning task generates a summary report at the end of each run in the folder *Enterprise_Vault_installation_folder*\Reports\SMTP Provisioning.

You can configure the report options on the **Reports** tab of the SMTP Archiving task properties and the SMTP Provisioning task properties.

If you want to generate more detailed usage reports for SMTP Archiving, you need to install and configure the Enterprise Vault Reporting component. In Enterprise Vault Reporting, the report named "Content Providers Licensing and Usage Summary Report" includes information about the data that is archived using SMTP Archiving.

Monitoring

Monitoring of SMTP Archiving components is included in the automatic monitoring mechanisms that are supported by Enterprise Vault:

- Performance monitoring. The **Monitoring** tab in Site Properties lets you turn on performance monitoring for SMTP Archiving components. If a monitored item reaches its threshold, a message is logged in the application Event log and an alert is generated in Enterprise Vault system status.
- Microsoft System Center Operations Manager (SCOM). The supplied Enterprise Vault Management Pack enables you to monitor SMTP Archiving operations and performance.

For more information on monitoring Enterprise Vault, see the following article on the Veritas Support website: https://www.veritas.com/docs/100015240.

Chapter 4

Configuring SMTP Archiving

This chapter includes the following topics:

Steps to configure SMTP Archiving

Table 4-1 outlines the tasks required to configure SMTP Archiving. Some of the tasks can be performed automatically by Enterprise Vault in SMTP configuration wizards, or manually. More information about the task is provided in the section or sections that are referenced in the **Description** column of the table.

You need to perform steps 1 to 7 when setting up all types of SMTP archiving; SMTP Journaling, SMTP Group Journaling, and SMTP Mailbox Journaling.

Step 8 is required if you want to include SMTP messages in Compliance Accelerator sampling.

Step 9 completes the configuration for SMTP Journaling.

Steps 10 and 11 are required if you are setting up SMTP Group Journaling or SMTP Mailbox Journaling.

To configure SMTP Archiving, you must 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.

See "Roles-based administration" in the *Administrator's Guide*.

Table 4-1 Steps to configure SMTP Archiving

Step	Task	More information
Step 1	Plan your SMTP Archiving environment. We strongly recommend that you plan in detail your SMTP Archiving environment before starting the configuration process. The section referenced opposite provides a list of important points to consider, and best practice hints and tips.	See "Planning your configuration" on page 30.
Step 2	Configure the SMTP server settings for all the Enterprise Vault SMTP servers in the site.	See "Configuring the Enterprise Vault SMTP Servers in the site" on page 35.
Step 3	Create the SMTP Archiving task, and configure the SMTP holding folder. You can add the SMTP Archiving task manually, as described in the section opposite, or let Enterprise Vault add it automatically when you create the first SMTP routing address.	See "Adding an SMTP Archiving task and holding folder" on page 47.
Step 4	Set up suitable retention categories.	See "Configuring retention categories and retention plans" on page 51.
Step 5	Create SMTP policies.	See "Creating SMTP policies" on page 56.

Table 4-1 Steps to configure SMTP Archiving *(continued)*

Step	Task	More information
Step 6	If you want to use archives other than SMTP archives for SMTP Journaling or SMTP Group Journaling, then create these before configuring the target addresses or provisioning groups. For SMTP Journaling, you can create new SMTP archives in the New SMTP Target wizard, when you create the routing addresses. Alternatively, you can create archives of a different type beforehand, and select them in the wizard. Similarly, for SMTP Group Journaling you can create SMTP archives in the provisioning group wizard, or create archives of a different type beforehand. For SMTP Mailbox Journaling, the provisioning task assigns an Internet Mail archive to each member of the SMTP Mailbox Journaling provisioning groups. If an Internet Mail archive already exists for an SMTP address, the task automatically links it to the SMTP target. If no Internet Mail archive exists for a target address, the provisioning task automatically creates one.	See "Configuring archives for SMTP messages" on page 63.
Step 7	Add the SMTP routing addresses.	See "Adding SMTP routing addresses" on page 66.
Step 8	If you use Compliance Accelerator, add internal SMTP domains to site settings.	See "Additional configuration for Compliance Accelerator" on page 69.
Step 9	SMTP Journaling: If you are implementing SMTP Journaling, configuration is complete. We recommend that you check your configuration settings. You can skip steps 10 and 11.	See "Checking settings for SMTP Journaling" on page 67.

Table 4-1 Steps to configure SMTP Archiving *(continued)*

Step	Task	More information
Step 10	SMTP Group Journaling and SMTP Mailbox Journaling: Create SMTP Provisioning task. You can add the SMTP Provisioning task manually, as described in the section opposite, or let Enterprise Vault create it automatically when you create the first provisioning group.	See "Adding or deleting an SMTP Provisioning task" on page 79.
Step 11	SMTP Group Journaling and SMTP Mailbox Journaling: Create the required groups of users to provision for SMTP Group Journaling or SMTP Mailbox Journaling.	See "About SMTP provisioning groups" on page 70.

Planning your configuration

Before you configure SMTP Archiving, it is important to have a clear picture of how you want your SMTP archiving environment to work. This section lists aspects of the configuration that you need to plan before you begin the configuration process. The information includes recommendations to help you create an efficient environment that is easy to maintain.

Enterprise Vault SMTP servers

- Consider how many Enterprise Vault SMTP servers to configure.
  If you plan to configure multiple archives for a routing address or SMTP Group Journaling provisioning group, then consider spreading the archives across different Enterprise Vault SMTP servers that host a storage service.
- If you want to restrict connections to the Enterprise Vault SMTP servers in the site, then you need to identify the servers from which you want to allow connections.
- To support encrypted connections, you need a valid SSL/TLS certificate.
- Decide whether to implement message tracking.

See "Configuring the Enterprise Vault SMTP Servers in the site" on page 35.

Storage requirements

- Consider how much storage is needed for the vault store partitions, indexes, SQL databases, SMTP holding folders, and storage queue.
  For sizing guidance, see the document, Setting up Exchange Server and Office 365 for Enterprise Vault SMTP Archiving.

SMTP routing addresses

- Decide on the routing addresses that you want to use to send the SMTP email to Enterprise Vault SMTP servers.
- You will need to configure MTAs that send SMTP messages to Enterprise Vault to use the routing addresses.
- If you have a software or hardware load-balancing solution, you need to configure it to receive messages addressed to the routing addresses, and distribute the messages to the Enterprise Vault SMTP servers.

See "About SMTP Journaling" on page 18.

See "About SMTP Group Journaling" on page 20.

See "Journaling messages to Enterprise Vault from Exchange Server or Office 365" on page 24.

Types of SMTP Journaling to configure

- Decide on the type or types of journaling that you want to implement:
  - SMTP Journaling
  - SMTP Group Journaling
  - SMTP Mailbox Journaling
  - SMTP Journaling and SMTP Group Journaling
  - SMTP Journaling and SMTP Mailbox Journaling
- Consider what value to set for the SMTP site setting, "Selective Journal Archiving ".
  When you add the first provisioning group, Enterprise Vault automatically changes the value of this setting to **Inclusive**.

Additional hints and tips:

- If you are implementing SMTP Mailbox or Group Journaling with SMTP Journaling, consider if there are users whose personal email should not be sent to the general SMTP Journaling archives. If there are, then you can use the value **Exclusive** for the SMTP site setting, **Selective Journal Archiving**.

See "SMTP Archiving configurations" on page 14.

See "Configuring the SMTP site setting, Selective Journal Archiving" on page 80.

SMTP Group and Mailbox Journaling provisioning groups

If you are implementing SMTP Group and Mailbox Journaling, we strongly recommend that you configure target users in provisioning groups. This not only simplifies the configuration process, but ensures that retention remains consistent across your SMTP Archiving configuration.

- To determine the main provisioning groups, identify the groups of users who require the same retention and policy settings.
- Within the larger groups, identify any users who need to be excluded from archiving, or provisioned with different settings. You can then create smaller provisioning groups for these users.
- Work out the order in which you want Enterprise Vault to process the groups. The groups are processed from the top of the list down. If users appear in more than one provisioning group, they are only provisioned in the first provisioning group that includes them.
  When ordering the provisioning groups, put the most explicit group at the top of the list of groups, and the most general at the bottom of the list.

Additional hints and tips:

- The same target user cannot be provisioned for both SMTP Group and Mailbox Journaling.
- You can create disabled provisioning groups that contain the users to exclude from archiving.
- The target setting, **Target only primary email address** , defines whether targets are created for all of the Active Directory user's SMTP addresses. If you have target users who are in multiple sites, make sure this setting is consistent for these users in all the sites.
- We recommend that you always add an Active Directory target user using 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.
- Manually-added targets take precedence over provisioned targets. If a target exists in a provisioning group and in the manual target list, you need to remove the manual target before the user is provisioned in the group.

See "About SMTP provisioning groups" on page 70.

Archives

Consider the types of archives to use, and method of creation.

- SMTP Journaling and SMTP Group Journaling. You can assign multiple archives to an SMTP Journaling target routing address, or an SMTP Group Journaling provisioning group. If you want to use new SMTP archives, then you can create these in the wizards for adding the routing addresses or adding an SMTP Group Journaling provisioning group. If you want to use different types of journal archives or existing archives, you need to make sure these exist before you run the wizards.

  If you select existing archives, you can select any of the following types of archive: SMTP, Shared, Exchange Journal, or Domino Journal.
- SMTP Journaling and SMTP Group Journaling. The archives associated with a routing address or an SMTP Group Journaling provisioning group must have the same retention settings. Enterprise Vault automatically manages retention settings on these archives. If you change retention on one of the archives, then Enterprise Vault cascades the change to the other archives associated with the routing address or provisioning group. For this reason, we recommend that each routing address and each SMTP Group Journaling provisioning group use different archives.
- SMTP Mailbox Journaling. Provisioning can automatically create a new Internet Mail archive for each target user in the provisioning group. If target users in an SMTP Mailbox Journaling provisioning group were previously provisioned in IMAP provisioning groups, then Enterprise Vault links the target user to their existing Internet Mail archive.

  Exchange Mailbox archives are also supported for SMTP Mailbox Journaling, but only for manually-added target users. Only Internet Mail archives can be used for target users in SMTP Mailbox Journaling provisioning groups.

Additional hints and tips:

- SMTP Journaling and SMTP Group Journaling. Enterprise Vault automatically spreads the archiving load across servers when you assign multiple archives to a routing address or provisioning group. We recommend that you use this feature instead of address rewriting.
- If the same users are provisioned for IMAP (Internet Mail provisioning groups) and SMTP Mailbox Journaling, the provisioning groups in IMAP and SMTP Archiving must apply the same retention to the Internet Mail archives.
- If you run the SMTP Provisioning task and the Client Access Provisioning task on the same users, we recommend that you do not run both of these tasks concurrently. Change the schedules of the tasks to make sure that one task has finished before the other starts.

See "Configuring archives for SMTP messages" on page 63.

Retention settings

Decide what retention categories and retention plans to use for provisioning groups and manually-added target addresses, such as routing addresses.

- Although you can create retention categories in the new target and new provisioning group wizards, we recommend that you plan and create these beforehand.
- Keep retention simple. Consider using the same retention categories and plans across different types of archiving in your Enterprise Vault environment.
- The archives associated with a routing address or an SMTP Group Journaling provisioning group must have the same retention settings. Enterprise Vault automatically manages retention settings on these archives. If you change retention on one of the archives, then Enterprise Vault cascades the change to the other archives associated with the routing address or provisioning group.

Additional hints and tips:

- Keep the number of different retention categories and plans in your sites as few as possible, and apply them consistently. The flexibility within Enterprise Vault means that there are various ways of overriding default retention settings. If your retention model becomes too complex, retention may not be applied as you expect.
- If the same users are provisioned for IMAP (Internet Mail provisioning groups) and SMTP Mailbox Journaling, the provisioning groups in IMAP and SMTP Archiving must apply the same retention to the Internet Mail archives.

See "Configuring retention categories and retention plans" on page 51.

SMTP policies

Decide what SMTP policies to use.

- Some messages may include proprietary X-Headers that you want to index, or use to control how the messages are processed.
- Consider whether to keep or discard journal reports for the target or provisioning group. As journal reports include BCC information, the reports should not be included in archives to which end users have access, for example, SMTP Mailbox Journaling.

See "Creating SMTP policies" on page 56.

Additional configuration for Compliance Accelerator

If you use Compliance Accelerator, you need to decide which domains used in SMTP targets should be considered as internal.

See "Additional configuration for Compliance Accelerator" on page 69.

Configuring the Enterprise Vault SMTP Servers in the site

After you have completed the initial set up of Enterprise Vault, you configure the SMTP connection settings for the Enterprise Vault SMTP servers, as described in this section.

These settings are stored in the Enterprise Vault directory, and propagated to each Enterprise Vault SMTP server in the site. Starting or restarting the Enterprise Vault Admin service on an Enterprise Vault SMTP server forces the settings on that SMTP server to synchronize with the settings in the directory.

In the Enterprise Vault Administration Console, the SMTP server settings are in the properties of the container **Targets** > **SMTP**.

To configure the Enterprise Vault SMTP servers

1. On the computer that hosts the Enterprise Vault Administration Console, log on as the Vault Service account, or an account that has the SMTP Administrator role.
2. Open the Enterprise Vault Administration Console.
3. In the navigation pane, expand the site, then the **Targets** container.
4. Right-click the **SMTP** container and select **Properties**.
5. The SMTP Properties dialog box is displayed.

   When you open the dialog box for the first time, click **Configure settings...** to launch the SMTP Server Settings wizard.

   The wizard enables you to configure the following settings for the SMTP servers:

SMTP port	The port on which the SMTP server listens. By default, the SMTP server listens on port 25. Ensure that the port you specify is open on each SMTP server.
Maximum message size	The maximum size of SMTP message that the SMTP servers will accept. If you do not specify a maximum message size, there is no limit on the size of messages.

Authentication	Defines the credentials used by MTAs when connecting to the Enterprise Vault SMTP server. If you want connecting hosts to use authentication when connecting, enter the credentials that they need to use. The username should be specified in the form user@domain. There is no requirement for the username to be an existing email address, or an account in Active Directory. Authentication is required by default. You can control plain text authentication as follows: ■ Never allow plain text authentication ■ Always allow plain text authentication with or without TLS ■ Allow plain text authentication only when TLS is enabled
Connection security	Specifies which of the following connections are permitted: ■ Only encrypted ■ Only unencrypted ■ Both encrypted and unencrypted If you choose to use an encrypted connection, Enterprise Vault allows communication with the SMTP server only over encrypted channels. The Enterprise Vault SMTP server rejects messages that are sent over unencrypted channels. Veritas recommends that you configure only encrypted connections to ensure security. To support encrypted connections, you need to have a valid PFX or PKCS#12 (.p12) certificate file. See "Obtaining an SSL/TLS certificate" on page 39. The wizard enables you to install the certificates. **Note:** You can configure connection security setting at the server-level by editing the settings on the **SMTP** tab of the computer properties.

Connection control

Enables you to control which computers can connect to the Enterprise Vault SMTP servers. If you do not add any computers to the connection control list, then any computer may connect to the Enterprise Vault SMTP servers. If you add one or more computers to the list, then only the computers listed can connect.

You can specify the connecting hosts using one of the following formats:

- Host name
- Host name suffix
- Host name pattern
- IPv4
- IPv4 range in CIDR notation
- IPv6
- IPv6 range in CIDR notation

See "Entering the name or IP address of connecting hosts" on page 37.

Select the format that you want to use to enter the value. Then enter the name or IP address in the specified format.

Alternatively, you can import the values from a .csv file. Each host should be listed on a new line as *host_name_or_address, format*.

Message tracking

If you enable message tracking, Enterprise Vault logs the details of messages that each SMTP server receives. You can see the list of the SMTP servers in the site, along with the location of the message tracking log file on each server. By default, the message tracking log file is stored in the folder, `Reports\SMTP\SmtpService`, in the Enterprise Vault program folder on each SMTP server. You can change the location of the message tracking log file. You can also configure whether you want to include the subject line of the message in the message tracking log file and the DTrace logs.

See "Configuring message tracking for SMTP messages" on page 41.

Entering the name or IP address of connecting hosts

This section provides more information about the formats that you can use to specify the hosts that may connect to the SMTP servers.

- **Host Name**. You specify the FQDN of the connecting host. Only alphanumeric characters and hyphen '-' are permitted. Consecutive dots are not permitted.
  Example host names:
  server.example.com
  server-NY.example.com
- **Host name suffix**. You can specify the domain name, to allow connections from all hosts in that domain.
  Example host name suffix: example.com
  This allows connections from hosts in the domain, example.com, including the host server-NY.example.com.
- **Host name pattern**. Specify the allowed host names as a regular expression, using alphanumeric characters and the characters (0-9, a-z, *, [ ]). Other special characters and consecutive dots are not permitted.
  Example host name pattern: server[1-2]*.example.com
  This allows connections from hosts with names that match the pattern, such as server1.example.com, and server2-NY.example.com.
- **IPv4**. Specify the IP address of the host using IPv4 format *nnn.nnn.nnn.nnn*, where *nnn* is a number from 0 to 255. Special characters other than the dots shown are not permitted. Consecutive dots are not permitted.
  Example IPv4 address: 192.168.1.2
- **IPv4 address ranges in CIDR notation**. Specify a range of IPv4 addresses using the format *nnn.nnn.nnn.nnn/rr*, where *nnn.nnn.nnn.nnn* is the IPv4 address of the network, and *rr* is a number from 1 to 32 that indicates the subnet mask to use to work out the permitted address range. Additional dots, forward slashes, or other special characters are not permitted.
  Example IPv4 address range in CIDR notation: 192.168.1.0/24
  This example indicates addresses in the range 192.168.1.0 to 192.168.1.255.
- **IPv6**. Specify the IP address of the host using IPv6 format *nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn*, where *nnnn* may include the hexadecimal characters (0-9,A-F,a-f). Special characters other than the colons shown are not permitted. Consecutive colons are not permitted.
  Example IPv6 address: fd9b:cd26:df9c:fb4e:0000:0000:0000:0001
- **IPv6 address ranges in CIDR notation**. Specify a range of IPv6 addresses using the format *nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn/rrr*, where *nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn* is the IPv6 address of the network, and *rrr* is a number from 1 to 128 that indicates the subnet mask to use to work out the permitted address range. Characters used must be hexadecimal characters, colons, and a forward slash, as shown. Using two consecutive colons at the end of the IPv6 range is also permitted. Any other special characters are not permitted.

Example IPv6 address range in CIDR notation: 2001:db8:1234::/48
This example indicates addresses in the range 2001:db8:1234:0000:0000:0000:0000:0000 to 2001:db8:1234:ffff:ffff:ffff:ffff:ffff.

Obtaining an SSL/TLS certificate

The following types of certificate are supported for SMTP connection security:

- Commercial certificate that is signed by a trusted third-party or Certification Authority (CA)
- Windows PKI-generated certificate (Microsoft Certificate Services)
- Private (self-signed) certificate
- Subject Alternative Name (SAN) certificate
- Wildcard certificate

You can use any suitable tool to request a certificate from a recognized certificate authority (CA). For example, you can use OpenSSL, which is installed in the Enterprise Vault installation folder.

Ensure that the certificate you request contains all the intermediate certificates you need for clients to establish a chain of trust to a root CA.

The server's certificate and private key must be presented in a PFX or PKCS#12 file. This file should be encrypted using a password.

To obtain an SSL/TLS certificate

1. If there is only one SMTP server in the site, go to Step 6.
2. Make a backup copy of `openssl.cnf` which is in the Enterprise Vault installation folder, for example `C:\Program Files (x86)\Enterprise Vault`.
3. Open `openssl.cnf` for editing.
4. Uncomment the following line in `openssl.cnf` by removing the `#` from the start of the line:

   ```
   # req_extensions = v3_req # The extensions to add to a certificate request
   ```

5 Add lines to the `[ v3_req ]` section of `openssl.cnf` as shown in the following example. Specify all the SMTP servers in the site:

```
[ v3_req ]
# Extensions to add to a certificate request

basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment

subjectAltName = @alt_names

[alt_names]
DNS.1 = evserver1.example.local
DNS.2 = evserver2.example.local
DNS.3 = evserver3.example.local
DNS.4 = evserver4.example.local
```

6 Use the following OpenSSL syntax to create a certificate request and a key:

```
openssl req -config openssl.cnf -new -nodes -keyout server.key
-out server.csr
```

Where *server*.key is the name of the file that will contain the certificate key and *server*.csr is the name of the file that will contain the certificate signing request (CSR).

You are prompted to enter information about your organization. To leave an optional field blank, enter a period. The fields are as follows:

- **Country Name** is the country in which your organization is based.
- **State or Province Name** is the state in which your organization is based. Optional.
- **Locality Name** is the town or city in which your organization is based. Optional.
- **Organization Name** is the name of your organization.
- **Organizational Unit Name** is the requesting department in your organization. Optional.
- **Common Name** is the fully qualified domain name of the alias of the Enterprise Vault server to which MTAs will make SMTP connections.
- **Email Address** is your email address. Optional.
- **Challenge password** is an extra attribute to be sent with the certificate request. Optional

- **Optional company name** is the name of the company. Optional.

Two files are generated. You should send the CSR file to the CA, and retain the key file.

7 Next use the private key to sign the CSR.

If there is only one SMTP server in the site, use the following command to sign the CSR:

```
openssl x509 -in server.csr -out server.pem -req -signkey
server.key -days 365
```

If there is more than one SMTP server in the site, use the following command to sign the CSR:

```
openssl x509 -in server.csr -out server.pem -req -signkey
server.key -days 365 -extensions v3_req -extfile openssl.cnf
```

The folder should now contain a file called *server*.pem, which is the server's certificate.

8 Use the following command to export the certificate and key into a PKCS#12 (.p12) file, and encrypt the file:

```
openssl pkcs12 -export -in server.pem -inkey server.key -out
server.p12 -descert
```

When prompted, enter a password to protect the file.

Note: Create a single SAN certificate that includes the fully qualified domain names of all the Enterprise Vault servers in the site. The Common Name for the SAN certificate can be the fully qualified domain name of the alias of any Enterprise Vault server in the site. When you import the SAN certificate to any one of the servers in the site, Enterprise Vault installs the certificate on the other servers.

Configuring message tracking for SMTP messages

Enterprise Vault SMTP message tracking helps you to track the SMTP messages that the Enterprise Vault SMTP Service receives from remote messaging servers. You configure and enable SMTP message tracking for the site using the message tracking settings in the SMTP server properties.

To access the message tracking settings in the Enterprise Vault Administration Console:

- Expand **Targets**.

- Right-click **SMTP** and select **Properties**. The SMTP server properties window is displayed.
- Click the **Message Tracking** tab to display the settings.

When you enable message tracking for the site, each Enterprise Vault SMTP server records details of each message that it receives. The SMTP server stores the message details in a message tracking log file. You can use the SMTP server log files for mail flow analysis, reporting, and troubleshooting. For example, you can compare the contents of the log files with the log file on the relay MTA to discover which messages were sent by the relay MTA but not received by an Enterprise Vault SMTP server.

Enterprise Vault generates a new message tracking log file every day. If the size of the file exceeds 10 MB, Enterprise Vault creates a new log file. The log file name format is `EVSMTPMessageTracking_DNSAliasName_ yyyymmdd_n.log`, where *n* is the incremental number that Enterprise Vault appends to the log file name if the log file size exceeds the 10-MB limit. For example, `EVSMTPMessageTracking_EV.example.com_20170128_1.log`.

The default location for the message tracking log file is `Reports\SMTP\SMTPService` in the Enterprise Vault program folder. You can change the location of the log file by editing the SMTP server properties in the Administration Console. Alternatively, you can use the cmdlet, `Set-EVSMTPMessageTrackingLogLocation`. In a Building Blocks environment, Enterprise Vault creates the log file in the message tracking log location on the active server and uses the name of the active server in the log file name.

Enterprise Vault assigns the Local System account and the local Administrators group full control on the folder that stores the message tracking log file.

You can configure the number of days to keep the log files on the server by editing the SMTP server properties in the Administration Console or using the `Set-EVSMTPServerSettings` cmdlet. Log files that are older than the specified number of days are deleted.

Table 4-2 describes the attributes in the message tracking log. The attributes in the log file are in comma-separated value (.csv) format, so that you can easily import the file contents into a spreadsheet.

Table 4-2 Attributes in message tracking log

Attribute	Description
unid	The unique ID of the message. This ID is unique to the message on each SMTP server.
qid	The ID of message in the SMTP message queue.

Table 4-2 Attributes in message tracking log *(continued)*

Attribute	Description
msgid	The Internet Message-ID of the message. This ID is present in the message header of each message that is stored in the SMTP holding folder.
subject	The subject line of the message.
mta	The name of the Message Transfer Agent (MTA) that sent the message to the SMTP server.
size	The size of the message, in bytes.
sender	The email address of the sender of the message as processed by the MTA.
submit-time	The time when the message is received by the SMTP server and placed in the SMTP holding folder.

Adding an SMTP Archiving task and holding folder

You can add the SMTP Archiving task manually, as described in this section, or let Enterprise Vault add it automatically when you create the first SMTP routing address.

An Enterprise Vault SMTP server can host only one SMTP Archiving task. Each archiving task requires its own local SMTP holding folder. The account under which the archiving task runs must have full access to the holding folder.

The SMTP Archiving task processes the .eml message files that the Enterprise Vault SMTP server has placed in the SMTP holding folder. The task examines each file, and determines if the file is eligible for archiving. The task archives messages according to the SMTP policy and target configuration.

If messages contain X-Headers that are listed in the policy, these are indexed when the message is archived. If messages contain "X-Kvs" X-Headers, then the values in these headers override policy and target configuration settings.

The archiving task deletes the message file from the holding folder when either of the following conditions is fulfilled:

- After the task has archived the message successfully.
- If the message does not contain any target addresses that are eligible for archiving. This could happen in SMTP Group or SMTP Mailbox Journaling, if the routing address is not enabled for archiving. For example, if a message in the holding folder does not contain any SMTP Group or Mailbox Journaling

target addresses, and **Archive messages sent from or received by this SMTP address** is not selected in the target properties of the routing address.

The SMTP service and SMTP Archiving task run continually. If the SMTP service stops, Enterprise Vault attempts to restart it. If you stop the archiving task, you are prompted to stop the SMTP service as well. If you leave the SMTP service running, it continues to add files to the holding folder.

When processing files in the holding folder, the archiving task performs checkpointing at regular intervals. You can change the checkpoint interval on the **Advanced** tab in the task properties.

If you want to host an SMTP Archiving task on a new server, you must delete it from the current server first. You can then add the task on the new server.

To add the SMTP Archiving task

1. Open the Administration Console, and navigate to **Enterprise Vault Servers** > ***server*** > **Tasks**.
2. Right-click the **Tasks** container and select **New** > **SMTP Archiving task** to open the new task page.
3. Enter the required information for the SMTP Archiving task, including a suitable folder for the SMTP holding folder.

To delete an SMTP Archiving task

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 from which you want to delete the SMTP Archiving task, and then click the **Tasks** container.
3. If the SMTP Archiving task is running, right-click the **SMTP Archiving Task**, and then click **Stop**.
4. Right-click the **SMTP Archiving Task**, and select **Delete** from the shortcut menu.
5. In the warning dialog box, click **Yes**.

   Enterprise Vault removes the Archiving task from the Administration Console.

About the SMTP holding folder

Each SMTP Archiving task must have its own holding folder. The Enterprise Vault SMTP service places .eml message files in this folder for the archiving task to process.

The holding folder path must comply with the following conditions:

- The folder must be on a local drive.
- The folder should be excluded from virus scanning. Scanning the holding folder can cause the corruption of items, performance issues, and data loss.
- You cannot specify a UNC path for the folder.
- The maximum permitted length of folder path is 207 characters.
- DBCS characters and non-ANSI characters are not permitted in the folder path.

The account under which the SMTP Server and the SMTP Archiving task run must have full access to the holding folder. As this folder may contain sensitive data, ensure that other accounts do not have access or inherit access to this folder.

The holding folder is organized according to the time at which message files are placed in the folder. Time is specified as UTC time. For example:

```
Mail Root (Holding folder)
   26 (day of month)
      15 (hour)
         30 (min)
            5cd6a8ba01cc51dd00000001.eml (actual email)
            6feb03d801cc2f0f00000001.eml
```

If the archiving task cannot archive an item, it moves the file to a folder named `Failed` in the holding folder. In the `Failed` folder, subfolders for day, hour, and minute are created as needed. The file is placed in the appropriate minute folder.

By default, the archiving task deletes messages in the holding folder that do not contain a target address that is enabled for archiving. You can change this behavior using the advanced SMTP site setting, **Delete messages without recipients or a matching target**. If you set this option to **No**, messages that do not contain a matching target address that is enabled for archiving are moved to the folder `NoMatchingTarget`. In the `NoMatchingTarget` folder, subfolders for day, hour, and minute are created as needed. The file is placed in the appropriate minute folder. To report such actions, you can enable the advanced SMTP site setting, **Log action when a message does not contain any archiving-enabled target**. Note that setting the option **Delete messages without recipients or a matching target** to **No** is likely to cause the holding folder space to fill quicker.

The following procedures describe how to change the location of the holding folder. The procedure differs depending on whether the site has a single or multiple Enterprise Vault SMTP servers.

To change the location of the holding folder in a site with multiple Enterprise Vault SMTP servers

1. In the Windows Services Console stop the Enterprise Vault SMTP service.

   While the SMTP service is stopped, the SMTP services and SMTP Archiving tasks on the other Enterprise Vault SMTP servers in the site continue to run and process new items.

2. Wait until the SMTP Archiving task finishes processing all of the pending files in the holding folder.

   When the SMTP Archiving task is finished processing the files, stop the task in the Enterprise Vault Administration Console.

3. In the properties of the SMTP Archiving task, change the location of the holding folder.

   Note that the new holding folder location must be excluded from virus scanning.

4. Restart the Enterprise Vault SMTP service. The archiving task is restarted automatically.

To change the location of the holding folder in a site with a single Enterprise Vault SMTP server

1. In the Enterprise Vault Administration Console stop the SMTP Archiving task.
2. Select **Stop SMTP service** and then click **Yes**.

   When you stop the SMTP service, all hosts that attempt to connect will be refused. Do not stop the SMTP service for long.

   If you do not stop the SMTP service, then it will continue to accept SMTP messages and put them in the holding folder.

3. Copy the existing SMTP holding folder tree to the new location.
4. Change the SMTP holding folder location in the Administration Console.

   Note that the new holding folder location must be excluded from virus scanning.

5. Start the Enterprise Vault SMTP Archiving task. Enterprise Vault automatically starts the SMTP service when the task starts.

Keeping safety copies of archived messages

Enterprise Vault does not use the SMTP holding folder to store safety copies of SMTP messages. When you archive SMTP messages to a vault store that has a safety copy setting of **Yes, in the original location** Enterprise Vault keeps the safety copies in the Storage queue.

You may need to check that there is sufficient space for these safety copies at the Storage queue location.

For information about the Storage queue, see the *Administrator's Guide*.

Task summary reports

The SMTP Archiving task generates summary reports and error log reports in the folder *Enterprise_Vault_installation_folder*\Reports\SMTP*SMTP_task_name*.

You can change the interval for generating summary reports on the Advanced tab in the archiving task properties.

Adding an SMTP Archiving task and holding folder

You can add the SMTP Archiving task manually, as described in this section, or let Enterprise Vault add it automatically when you create the first SMTP routing address.

An Enterprise Vault SMTP server can host only one SMTP Archiving task. Each archiving task requires its own local SMTP holding folder. The account under which the archiving task runs must have full access to the holding folder.

The SMTP Archiving task processes the .eml message files that the Enterprise Vault SMTP server has placed in the SMTP holding folder. The task examines each file, and determines if the file is eligible for archiving. The task archives messages according to the SMTP policy and target configuration.

If messages contain X-Headers that are listed in the policy, these are indexed when the message is archived. If messages contain "X-Kvs" X-Headers, then the values in these headers override policy and target configuration settings.

The archiving task deletes the message file from the holding folder when either of the following conditions is fulfilled:

- After the task has archived the message successfully.
- If the message does not contain any target addresses that are eligible for archiving. This could happen in SMTP Group or SMTP Mailbox Journaling, if the routing address is not enabled for archiving. For example, if a message in the holding folder does not contain any SMTP Group or Mailbox Journaling target addresses, and **Archive messages sent from or received by this SMTP address** is not selected in the target properties of the routing address.

The SMTP service and SMTP Archiving task run continually. If the SMTP service stops, Enterprise Vault attempts to restart it. If you stop the archiving task, you are prompted to stop the SMTP service as well. If you leave the SMTP service running, it continues to add files to the holding folder.

When processing files in the holding folder, the archiving task performs checkpointing at regular intervals. You can change the checkpoint interval on the **Advanced** tab in the task properties.

If you want to host an SMTP Archiving task on a new server, you must delete it from the current server first. You can then add the task on the new server.

To add the SMTP Archiving task

1. Open the Administration Console, and navigate to **Enterprise Vault Servers** > ***server*** > **Tasks**.
2. Right-click the **Tasks** container and select **New** > **SMTP Archiving task** to open the new task page.
3. Enter the required information for the SMTP Archiving task, including a suitable folder for the SMTP holding folder.

To delete an SMTP Archiving task

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 from which you want to delete the SMTP Archiving task, and then click the **Tasks** container.
3. If the SMTP Archiving task is running, right-click the **SMTP Archiving Task**, and then click **Stop**.
4. Right-click the **SMTP Archiving Task**, and select **Delete** from the shortcut menu.
5. In the warning dialog box, click **Yes**.

   Enterprise Vault removes the Archiving task from the Administration Console.

About the SMTP holding folder

Each SMTP Archiving task must have its own holding folder. The Enterprise Vault SMTP service places .eml message files in this folder for the archiving task to process.

The holding folder path must comply with the following conditions:

- The folder must be on a local drive.
- The folder should be excluded from virus scanning. Scanning the holding folder can cause the corruption of items, performance issues, and data loss.
- You cannot specify a UNC path for the folder.
- The maximum permitted length of folder path is 207 characters.

- DBCS characters and non-ANSI characters are not permitted in the folder path.

The account under which the SMTP Server and the SMTP Archiving task run must have full access to the holding folder. As this folder may contain sensitive data, ensure that other accounts do not have access or inherit access to this folder.

The holding folder is organized according to the time at which message files are placed in the folder. Time is specified as UTC time. For example:

```
Mail Root (Holding folder)
   26 (day of month)
      15 (hour)
         30 (min)
            5cd6a8ba01cc51dd00000001.eml (actual email)
            6feb03d801cc2f0f00000001.eml
```

If the archiving task cannot archive an item, it moves the file to a folder named `Failed` in the holding folder. In the `Failed` folder, subfolders for day, hour, and minute are created as needed. The file is placed in the appropriate minute folder.

By default, the archiving task deletes messages in the holding folder that do not contain a target address that is enabled for archiving. You can change this behavior using the advanced SMTP site setting, **Delete messages without recipients or a matching target**. If you set this option to **No**, messages that do not contain a matching target address that is enabled for archiving are moved to the folder `NoMatchingTarget`. In the `NoMatchingTarget` folder, subfolders for day, hour, and minute are created as needed. The file is placed in the appropriate minute folder. To report such actions, you can enable the advanced SMTP site setting, **Log action when a message does not contain any archiving-enabled target**. Note that setting the option **Delete messages without recipients or a matching target** to **No** is likely to cause the holding folder space to fill quicker.

The following procedures describe how to change the location of the holding folder. The procedure differs depending on whether the site has a single or multiple Enterprise Vault SMTP servers.

To change the location of the holding folder in a site with multiple Enterprise Vault SMTP servers

1. In the Windows Services Console stop the Enterprise Vault SMTP service.

   While the SMTP service is stopped, the SMTP services and SMTP Archiving tasks on the other Enterprise Vault SMTP servers in the site continue to run and process new items.

2. Wait until the SMTP Archiving task finishes processing all of the pending files in the holding folder.

   When the SMTP Archiving task is finished processing the files, stop the task in the Enterprise Vault Administration Console.

3. In the properties of the SMTP Archiving task, change the location of the holding folder.

   Note that the new holding folder location must be excluded from virus scanning.

4. Restart the Enterprise Vault SMTP service. The archiving task is restarted automatically.

To change the location of the holding folder in a site with a single Enterprise Vault SMTP server

1. In the Enterprise Vault Administration Console stop the SMTP Archiving task.
2. Select **Stop SMTP service** and then click **Yes**.

   When you stop the SMTP service, all hosts that attempt to connect will be refused. Do not stop the SMTP service for long.

   If you do not stop the SMTP service, then it will continue to accept SMTP messages and put them in the holding folder.

3. Copy the existing SMTP holding folder tree to the new location.
4. Change the SMTP holding folder location in the Administration Console.

   Note that the new holding folder location must be excluded from virus scanning.

5. Start the Enterprise Vault SMTP Archiving task. Enterprise Vault automatically starts the SMTP service when the task starts.

Keeping safety copies of archived messages

Enterprise Vault does not use the SMTP holding folder to store safety copies of SMTP messages. When you archive SMTP messages to a vault store that has a safety copy setting of **Yes, in the original location** Enterprise Vault keeps the safety copies in the Storage queue.

You may need to check that there is sufficient space for these safety copies at the Storage queue location.

For information about the Storage queue, see the *Administrator's Guide*.

Task summary reports

The SMTP Archiving task generates summary reports and error log reports in the folder *Enterprise_Vault_installation_folder*\Reports\SMTP*SMTP_task_name*.

You can change the interval for generating summary reports on the Advanced tab in the archiving task properties.

Configuring retention categories and retention plans

We recommend that you plan carefully the policies, retention categories, and retention plans that you want to use in your SMTP archiving environment. You can create new policies, and retention categories when you run the wizards for adding target addresses or provisioning groups. However, you may prefer to create the required policies and retention settings beforehand, and then select them in the wizards.

For more information, see "Working with retention categories and retention plans" in the *Administrator's Guide*.

If you assign multiple archives to a routing address, then all the archives must have the same retention settings.

See “Managing cascading retention settings on multiple archives” on page 53.

About retention categories

When the archiving task stores a message, it assigns to the stored message the retention category that you configured for the target. The retention category defines the retention period, which is the minimum amount of time for which the stored message must be retained.

The retention category properties also provide other functionality, such as preventing the deletion of items with the retention category.

To change retention category settings, open the properties of the retention category in the Enterprise Vault Administration Console. Retention categories are located in the **Retention & Classification** container under **Policies**.

To create a new retention category

1. In the left pane of the Administration Console, expand the vault site hierarchy until **Policies** is visible.
2. Expand **Policies** and then expand **Retention & Classification**.
3. Right-click **Categories** and then, on the shortcut menu, click **New** > **Retention Category**.

   The New Retention Category wizard starts.
4. Work through the wizard.
5. To view or change the retention category properties, double-click the new retention category in the right-hand pane.

About retention plans

Retention plans let you define and apply the following to an archive or archive folder:

- retention category
- classification policy
- retention category usage during expiry
- retention folders

Using a retention plan gives you greater control over the retention periods of archived items. In particular, a retention plan lets you dispose of already-archived items by giving them a different retention period than the one that Enterprise Vault first gave them when it archived the items. For example, you can configure a retention plan so Enterprise Vault expires the affected items according to the retention category that you have associated with the retention plan, and not the retention categories with which Enterprise Vault originally stamped them.

We recommend that you only create retention plans after you have defined the retention categories and classification policies that you want to assign with those plans.

You can modify a retention plan after you have created it and associated it with one or more archives. You can also dissociate the plan from those archives and associate a different plan with them.

In the Enterprise Vault Administration Console, retention plans are located in the **Retention & Classification** container under **Policies**.

To create a new retention plan

1. In the left pane of the Enterprise Vault Administration Console, expand the tree view until the **Policies** container is visible.
2. Expand the **Policies** container and then expand the **Retention & Classification** container.
3. Right-click **Plans** and then point to **New** and click **Retention Plan**.

   The New Retention Plan wizard appears.
4. Work through the pages of the wizard, which prompt you to enter the following:
   - A name for the new retention plan. The name must be unique, and it can contain up to 40 alphanumeric or space characters.
     For example, you might call the retention plan "Capstone Official Plan" if it is to target users whose items are to be marked as permanent records by default. For those users whose items you want to mark as temporary records, you might create a retention plan that is called "Capstone Temporary Plan".
   - A description of the plan. The description can contain up to 127 alphanumeric, space, or special characters.
   - The required retention category: one with the record type set to Permanent or Temporary, for example.
   - Optionally, whether to allow the Enterprise Vault classification feature to classify the items that the retention plan handles. If you choose to classify the items, you must also select the required classification policy.
   - The expiry settings to assign to the affected items.

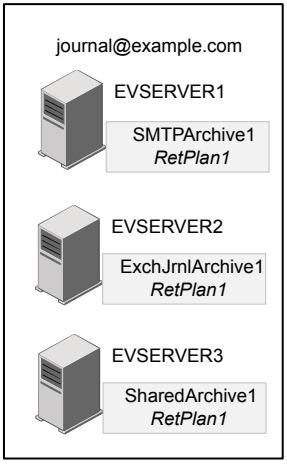
Managing cascading retention settings on multiple archives

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. All archives that are assigned to the target must have the same retention settings.

Enterprise Vault automatically manages retention settings on the archives that are assigned to a routing address or an SMTP Group Journaling provisioning group. If you change the retention settings on one of the archives assigned to a provisioning group, Enterprise Vault applies the change to the other archives in that provisioning group. If you change the retention settings on any archive or target, Enterprise Vault updates the retention settings of all associated archives. For this reason, we recommend that you configure each routing address and each SMTP Group Journaling provisioning group to use different archives or apply the same retention settings to all your groups.

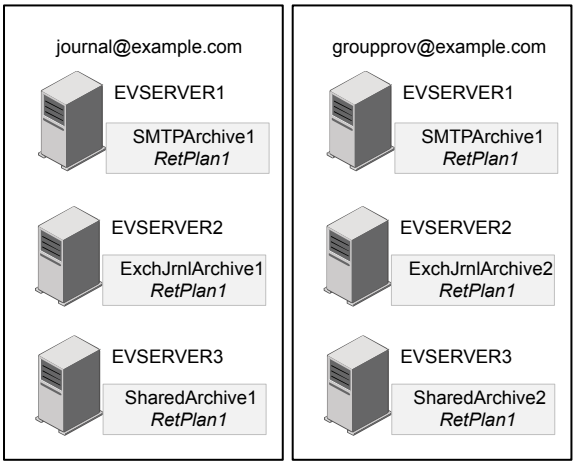
For SMTP Mailbox Journaling provisioning groups, the retention setting of the provisioning group is applied to all the targets in that group. If you change the retention settings on the archive of a target user in an SMTP Mailbox Journaling provisioning group, Enterprise Vault does not cascade the change to other archives in the group, as in SMTP Journaling and SMTP Group Journaling. However, the provisioning task restores the provisioning group retention to the archive on the next provisioning run.

Figure 4-1 Routing address assigned to multiple archives



Consider the example that is shown in Figure 4-1. If you change the retention setting of SMTPArchive1 to, say, RetPlan2; the retention setting of ExchJrnlArchive1 and SharedArchive1 will also change to RetPlan2.

Figure 4-2 Multiple targets assigned to common archives



In the example that is shown in Figure 4-2, the archive SMTPArchive1 is common to both journal@example.com and groupprov@example.com. If you change the retention setting of either target or any of the archives, say, ExchJrnlArchive1, Enterprise Vault cascades the change to all the other archives as well: SMTPArchive1, ExchJrnlArchive2, SharedArchive1, and SharedArchive2.

The retention settings cascading update can happen when you change the retention settings by editing the properties of the archive or the target. Note that if the target is associated with a retention plan, you need to edit the archive properties to change the retention settings

The retention settings cascading update applies to archive types SMTP, Shared, Exchange Journal, and Domino Journal only.

You can also update the retention settings using the Set-EVArchive, and Set-EVSMTPTarget PowerShell cmdlets.

About changing retention on SMTP Group Journaling provisioning groups

Table 4-3 describes how the retention that is set on an SMTP Group Journaling provisioning group is affected when you update the retention on the group or on one of the group's archives.

Table 4-3 Changing the effective retention set for a provisioning group

A retention plan is initially set on one of the group's archives	A retention category is initially set on the provisioning group	Administrator action	What retention is then set on the provisioning group
Yes	If an archive has a retention plan set, Enterprise Vault automatically applies the plan to the group.	Removes the retention plan from the archive.	The provisioning group uses the retention category that was associated with the retention plan.
No	Yes	Adds a retention plan to one of the group's archives.	The provisioning group uses the retention plan added.
No	Yes	Adds a retention plan to an archive, and then removes the retention plan from the archive.	The provisioning group uses the retention category that was initially set on the provisioning group.
No	Yes	Updates the provisioning group to use a retention plan.	The provisioning group uses the retention plan.
No	Yes	Updates the provisioning group to use a retention plan, and then removes the retention plan from an archive.	The provisioning group uses the retention category that was associated with the retention plan.

Creating SMTP policies

In the Enterprise Vault Administration Console, SMTP Archiving policies are located in the **SMTP** container under **Policies**.

Table 4-4 lists the settings available in the policy properties.

Table 4-4 SMTP policy properties

Property	Description
Name and Description	The policy name and a description of its application.
X-Headers	If you want Enterprise Vault to index specific X-Headers in SMTP messages, then you need to add the X-Headers to the policy. You can also use special Enterprise Vault X-Headers to customize how a message is archived. These headers begin with "X-Kvs". Enterprise Vault recognizes and processes "X-Kvs" headers, so you do not need to add these to the X-Header list. See “About X-Headers” on page 58.
Advanced	The following advanced settings control how the archiving task handles journal report messages: ■ Clear text copies of RMS Protected items. If journal report decryption is configured on Exchange Server 2016, then two messages are attached to the journal report: the original RMS-protected message and a clear text version. This policy setting controls whether Enterprise Vault uses the clear text message or the RMS-protected message as the primary message during archiving. ■ Decrypt RMS Protected Items. This setting control whether Enterprise Vault should decrypt RMS-protected messages for indexing and preview. To use this setting, you must store the RMS-protected message as the primary message during archiving. ■ Journal report processing. This setting controls whether Enterprise Vault processes journal reports and stores them with the message, or discards them. If users have access to archives that contain journaled SMTP messages, then you may want to discard the journal reports to prevent users accessing details, such as BCC recipients on messages. These advanced settings are described in detail in the "Journal Reports settings" section of the *Administrator's Guide*.
Targets	The SMTP target addresses to which this policy applies. This property is populated when you create SMTP targets and assign a policy.

To create a new SMTP policy

1. In the left pane of the Administration Console, expand the vault site hierarchy until **Policies** is visible.
2. Expand **Policies** and click **SMTP**. The existing SMTP policies are listed in the right-hand pane.

3. Right-click **SMTP** and then, on the shortcut menu, click **New** > **Policy**. The New SMTP Policy page opens.
4. Type in a name and description for the new policy, then click **OK**.
5. To view or change the policy properties, double-click the new policy in the right-hand pane.

About X-Headers

MTAs or third-party applications can add X-Headers to SMTP messages that are sent to Enterprise Vault. The format of X-Headers that are added to messages must conform to RFC 822. If non-ASCII characters are included in X-Headers, the encoding must conform to RFC 2047.

To ensure that Enterprise Vault recognizes these headers and adds them to the index for the message, you add the X-Headers to the X-Header list in the policy. Enterprise Vault treats all X-Header names and values as case-sensitive, so you must add them to the X-Header list exactly as they appear in the messages.

For each X-Header that you want to process, you specify the following information:

- The X-Header name. For example, X-Company-ID.
- The type of value that the X-Header contains; string, integer, or datetime.
- Whether the X-Header can be included in Enterprise Vault search criteria; Searchable.
- Whether the X-Header can be returned in search results; Retrievable.

If a message contains several instances of the same X-Header, Enterprise Vault indexes the first value only. If you want to add multiple values for the same X-Header, use the Enterprise Vault X-Header, X-Kvs-IndexData.

X-Kvs-IndexData is an efficient way to add to messages any custom properties that you want Enterprise Vault to index.

About X-Kvs X-Headers

This section describes the special Enterprise Vault X-Headers that third-party applications or MTAs can add to messages to override policy and target settings. These X-Headers begin with “X-Kvs”. Enterprise Vault recognizes and processes "X-Kvs" headers, so you do not need to add these to the X-Header list in the policy properties.

If a message contains multiple instances of the same X-Header, Enterprise Vault uses the first one only, and ignores the others.

As with X-Headers that you add to the X-Header list in the policy, Enterprise Vault treats the names and values of these special X-Headers as case sensitive.

X-Kvs-ArchiveId

X-Kvs-ArchiveId provides the ID of the archive in which to store the message. For example: X-Kvs-ArchiveId: 160EEB78D4253BE40AA8EBEBA09C7DFEE1210000evserver1.

This header can be used to identify a different archive from the one that is configured for the target address in the message.

For example, a message is sent to the target address journal1@example.com, and the archive configured for that target address is journal1. If X-Kvs-ArchiveId is added to the message, Enterprise Vault stores the message in the archive identified in the X-Header, rather than journal1.

X-Kvs-IndexData

You can use the Enterprise Vault X-Header, X-Kvs-IndexData, to do the following:

- Add multiple values for an X-Header. Using standard X-Headers, you can only add one value per X-Header.
- Add multiple custom index properties and property values in the one X-Header.

The header value is specified using XML. The XML element and attribute names and values are treated as case sensitive.

The following X-Kvs-IndexData example adds the X-Header, X-ExampleCorp-Dept, with multiple values:

```
X-Kvs-IndexData: <ARCHIVED_ITEM version="1.0"><PROPSET NAME="EVXHDR">
<PROP NAME=" X-ExampleCorp-Dept RESULTS="true" SEARCH="true">
<VALUE>Sales</VALUE><VALUE>Marketing</VALUE></PROP></PROPSET>
</ARCHIVED_ITEM>
```

Enterprise Vault adds X-Headers to the reserved index property set, EVXHDR. If you add other custom index properties, then you should specify a different property set for these properties. Suitable property set names for custom index properties would be your company name or the application name. The following property set names are reserved:

- Vault
- EnterpriseVault
- Any property set name starting with EV; for example, EVXHDR.
- KVS

- Veritas

In the following example, X-Kvs-IndexData is used to add two custom index properties, Dept and Region, to a message:

```
X-Kvs-IndexData: <ARCHIVED_ITEM version="1.0"><PROPSET NAME="ChatApp">
<PROP NAME="Dept" type="string" RESULTS="true" SEARCH="true">Sales</PROP>
<PROP NAME="Region" type="string" RESULTS="true" SEARCH="true">EMEA</PROP>
</PROPSET></ARCHIVED_ITEM>
```

In this example, the application name, ChatApp, is used as the property set name for the two custom index properties.

The first property, ChatApp.Dept, has the value "Sales". The property is searchable and retrievable.

The second property, ChatApp.Region, has the value "EMEA". This property is also searchable and retrievable.

The following example uses X-Kvs-IndexData to add the custom index property, ChatApp.Region, with multiple values:

```
X-Kvs-IndexData: <ARCHIVED_ITEM version="1.0"><PROPSET NAME="ChatApp">
<PROP NAME="Region" type="string" RESULTS="true" SEARCH="true">
<VALUE>USA</VALUE><VALUE>EMEA</VALUE><VALUE>ASIA</VALUE></PROP>
</PROPSET></ARCHIVED_ITEM>
```

In this example, the ChatApp.Region property has the values, "USA", "EMEA", and "ASIA". The property is searchable and retrievable.

It is advisable to reduce the header size as much as possible. If the default values for attributes are required, you can omit the attributes from the header. Table 4-5 lists the default values for the XML attributes.

Table 4-5 Default values for XML attributes

Attribute	Default value
RESULTS	"false"
SEARCH	"true"
type	"string"

In the previous example, the default values for SEARCH and type attributes are required, so you can omit these attributes:

```
X-Kvs-IndexData: <ARCHIVED_ITEM version="1.0"><PROPSET NAME="ChatApp">
<PROP NAME="Region" RESULTS="true"><VALUE>USA</VALUE><VALUE>EMEA</VALUE>
<VALUE>ASIA</VALUE></PROP></PROPSET></ARCHIVED_ITEM>
```

When searching for a custom index property that has been added using X-Kvs-IndexData, you specify the property in the form *property_set_name*.*property_name*, for example ChatApp.Region.

When searching for an X-Header that has been added using X-Kvs-IndexData, you specify the X-Header in the form EVXHDR.*X-Header_name*, for example EVXHDR.X-ExampleCorp-Dept.

See "Searching archives for messages with specific X-Headers" on page 63.

Note the following points about the value specified in the X-Kvs-IndexData header:

- The XML value can be folded according to the syntax rules in RFC 822.
- To support the use of international characters in the XML, the entire header value must be encoded as specified in RFC 2047.
  The following example shows how the header value might look when UTF-8 character set and BASE64 encoding is used:

  ```
  X-Kvs-IndexData: =?UTF-8"?B?PEFSQ0hJVkVEX0lURU0+PFBST1BTRVQgTkFNRT0i
  Q2hhdEFwcCI+PFBST1AgTkFNRT0iRGVwdCI+PFZBTFVFPlNhbGVzPC9WQUxVRT48L1BS
  T1A+PC9QUk9QU0VUPjwvQVJDSElWRURfSVRFTT4=?=
  ```

  Encoding only certain words in the XML is not supported. Similarly, specifying the encoding in the XML prolog is not adequate. For example,
  X-Kvs-IndexData: <ARCHIVED_ITEM version="1.0" encoding="UTF-8"> ... </ARCHIVED_ITEM>

X-Kvs-MessageType

X-Kvs-MessageType identifies the type of the message. For example: X-Kvs-MessageType: Bloomberg.

This header is used to override the value of the Vault.MsgType property that Enterprise Vault assigns to the message when it is archived. By default, if a message is archived using SMTP Archiving, Enterprise Vault assigns the value SMTP.Mail to the Vault.MsgType property.

The value of the Vault.MsgType property can be used in search applications, such as Discovery Accelerator, to filter the messages to search. If, for example, SMTP Archiving is used to archive Bloomberg messages, then the message type needs to be identified as Bloomberg. If the message type is not set to Bloomberg, the messages will not be included in Discovery Accelerator searches of Bloomberg messages.

X-Kvs-OriginalLocation

X-Kvs-OriginalLocation identifies the location in the content source to set for the message. Original location refers to the folder in the content source where the message resides. This could be set to the name of a top-level folder, or a folder path. For example: X-Kvs-OriginalLocation: CompanyA\ProductB\CustomerC.

You can add this X-Header to a message to specify a different archive folder for the message. If a message contains the example X-Header shown above, and the target archive type can contain folders, then the task would store the message in the following location:

Top-level folder: CompanyA

Subfolder: ProductB

Subfolder: CustomerC

If the folder structure does not exist, the task creates the folders when it stores the message.

This X-Header is only effective if the target archive type can contain folders.

In SMTP Journaling and SMTP Group Journaling, the SMTP Archiving task archives messages in the Inbox, if the archive type can contain folders. If the message contains an X-Kvs-OriginalLocation header, and the archive can contain folders, then the task stores the message in the location indicated in the X-Header instead of the Inbox.

Typically the type of archives used for SMTP Mailbox Journaling can contain folders; for example, Exchange mailbox, or Internet mail archives. The task stores messages in the Inbox, or Sent Items folder, or both, depending on whether a target address is the sender, recipient, or both. If the message contains an X-Kvs-OriginalLocation header, then the task stores the message in the location indicated in the X-Header instead of the Inbox or Sent Items folders.

X-Kvs-RetentionCategory

X-Kvs-RetentionCategory provides the ID of the retention category to assign to the message. For example: X-Kvs-RetentionCategory: 1505EB2CDB9C6AA44B30335E4A785F98C1b10000evserver1.

This header can be used to identify a different retention category from the one that is configured for the target address in the message.

For example, a message is sent to the target address journal1@example.com, and the retention category configured for that target address is 7years. If X-Kvs-RetentionCategory is added to the message, Enterprise Vault applies the retention category identified in the X-Header, rather than 7years.

Searching archives for messages with specific X-Headers

You can use Discovery Accelerator or the Advanced Search facility in Enterprise Vault Search to search archives for messages that contain a specific X-Header name and value. In Enterprise Vault Search, first turn on the display of custom fields in the **Preferences** dialog box. See the online Help for Enterprise Vault Search for instructions on how to do this.

When Enterprise Vault indexes a message that contains a header in the X-Header list, or an X-Kvs header, it adds the X-Header name to the index property set, EVXHDR. In the search criteria, you specify the X-Header name in the form **EVXHDR.*X-Header_name***; for example, **EVXHDR.X-CompanyID** or **EVXHDR.X-Kvs-ArchiveId**.

The X-Header name and value are case-sensitive.

Configuring archives for SMTP messages

When you create SMTP target addresses, you associate an archive with the target address. The archive can be an existing archive. Alternatively, you may want to create new archives to hold the items that are stored using SMTP Archiving.

The archive types that you can use for SMTP Journaling and SMTP Group Journaling are SMTP, Shared, Exchange Journal, or Domino Journal archives. When you create an SMTP routing address, or an SMTP Group Journaling provisioning group, Enterprise Vault prompts you to choose an existing archive, or to create a new SMTP archive.

You can assign multiple archives to an SMTP Journaling routing address, or an SMTP Group Journaling provisioning group to spread the archiving load.

See “Assigning multiple archives to spread the archiving load across servers” on page 65.

Note that all archives associated with the target must have the same retention settings. Enterprise Vault automatically manages retention settings on the archives that are assigned to a routing address or an SMTP Group Journaling provisioning group.

See “Managing cascading retention settings on multiple archives” on page 53.

User archive types that can contain folders, such as Exchange Mailbox or Internet Mail archives, can only be used for SMTP Mailbox Journaling. If you plan to add a manual target for SMTP Mailbox Journaling, the required archive must already exist. When you create an SMTP Mailbox Journaling provisioning group, Enterprise Vault prompts you to select the vault store where the Internet Mail archives are created. For users that do not have an Internet Mail archive already assigned, Enterprise Vault creates new ones in the selected vault store.

For example, say, you add 20 users to a new SMTP Mailbox Journaling provisioning group, out of which 5 users already have Internet Mail archives on VaultStore1. If you choose VaultStore2 as the vault store for the group, Enterprise Vault creates Internet Mail archives for the other users on VaultStore2. When the provisioning task runs, Enterprise Vault searches for the name of the user in Active Directory, retrieves all the SMTP addresses for that user, and checks whether the user has an Internet mail archive. If not, Enterprise Vault creates a new archive in VaultStore2 for this user.

Table 4-6 shows which types of archives can contain a folder structure.

Table 4-6 Structure of the different archive types

Archive type	Can contain folders
Exchange Mailbox	Yes
Exchange Journal	No
Domino Journal	No
SMTP	Yes
Internet Mail	Yes
Shared	Yes

There are some types of archives, including Exchange Mailbox and Internet Mail, that you cannot create manually. For more information, refer to the "Setting up" guides.

With SMTP Group Journaling and SMTP Mailbox Journaling, a copy of a message may be stored in multiple archives.

Enterprise Vault implements single-instance storage as permitted by the vault store configuration. To enable single-instance storage across vault stores in a vault store group, the following conditions must be fulfilled:

- The archives must be in the same vault store group.
- Configuration on the vault store group must allow sharing within the group.

To enable single-instance storage within a vault store, the following conditions must be fulfilled:

- The archives must be in the same vault store.
- Configuration on the parent vault store group must allow sharing within the vault store.

In SMTP Journaling and SMTP Group Journaling, messages are stored in the Inbox of the archive, if the archive type contains folders. In SMTP Mailbox Journaling, the following rules apply:

- All messages that contain a target address in a recipient field are stored in the Inbox of the archive.
- If a target address is found in the Sender or From fields, the message is stored in the Sent Items folder.
- If a target address is both the sender and recipient of a message, the message is stored in both the Inbox and the Sent Items folder.

You can use the special X-Header, X-Kvs-OriginalLocation, to change the behavior of the archiving task. This X-Header can be used to specify the archive folder in which to store the message. This X-Header is only effective if the target archive type can contain a folder structure.

Note that the SMTP Archiving task cannot synchronize archive folders with the folders in the original mailbox.

To create an SMTP archive

1. In the left pane of the Administration Console, expand the hierarchy until **Archives** is visible.
2. Expand **Archives**.
3. Right-click **SMTP** and, on the shortcut menu, click **New** and then **Archive**.

   The **New SMTP Archive** wizard starts.
4. Work through the wizard.

   You need to provide the following information:

   - The vault store in which to create the archive
   - The required Indexing service
   - The indexing level
   - A billing account
   - The retention settings to apply to the items that Enterprise Vault stores in the archive

Assigning multiple archives to spread the archiving load across servers

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.

The SMTP Archiving task stores messages that are sent to the SMTP target address based on the following criteria:

- If the SMTP target address is assigned to multiple archives, the task running on the server always archives to the archive that is local to that server.
- If multiple local archives are found on the server, the task chooses the archive that has the least number of items.
- If any of the local archives are not available due to temporary errors such as storage is busy, the vault store is in backup mode, and so on, the task chooses a remote archive that is assigned to the SMTP target address.

As archiving continues, the task maintains a cache of archives along with the number of items in each archive. This cache is refreshed every 10 minutes. The task then switches to the archive that has the least number of items.

When the temporary errors are resolved, the task starts archiving to the local archive. If none of the assigned archives are available, the SMTP task reports an error in the event log.

You can assign multiple archives when you create the routing address or provisioning group, or by editing the target properties.

To spread the archiving load optimally, we recommend that you assign each routing address or provisioning group to archives in different vault stores hosted on different Enterprise Vault storage servers.

Note: If you have a software or hardware load-balancing solution, you need to configure it to receive messages addressed to the routing addresses, and distribute the messages to the Enterprise Vault SMTP servers.

Adding SMTP routing addresses

Routing addresses are used to direct SMTP email messages to the Enterprise Vault SMTP servers. If you are configuring SMTP Journaling, then the routing addresses are the only target addresses that you add. If you are configuring SMTP Group or Mailbox Journaling, you need to add the required routing addresses before you configure additional target addresses.

We recommend that you create provisioning groups to add the additional target addresses for SMTP Group or Mailbox Journaling. You cannot use provisioning groups to add routing addresses.

SMTP routing addresses are added as manual SMTP target addresses. You can use the Enterprise Vault Administration Console, as described in this section, or the PowerShell cmdlet New-EVSMTPTarget.

To add an SMTP routing address using the Enterprise Vault Administration Console

1. In the navigation pane, navigate to **Targets** > **SMTP** > **Manual Targets**.
2. Right-click the **Manual Targets** container, and select **New** > **Target Email Address**.

   The New SMTP target wizard starts.
3. Enter the routing address in the form *user@domain*. Wildcard characters are not permitted when specifying SMTP target addresses.
4. For now, leave the type of journaling option set to **SMTP Journaling**, even if you are implementing SMTP Group or Mailbox Journaling.
5. Select the SMTP policy to apply to messages that include the routing address. Click **Next**.
6. Click **Add** to select the archives in which to store these messages. Click **New** if you want to associate this target with a new SMTP archive. Click **Next**.
7. Select the retention settings to apply to the messages. Click **Next**.

   Note: Changes to the retention settings may apply to multiple archives, if the target's archive is also associated with other targets that are in turn associated with other archives.
8. A summary of the target properties is displayed. Click **Finish**.
9. If you are adding this routing address after you have configured SMTP Group or Mailbox Journaling, then rerun the SMTP Provisioning task using the **Run now** option on the task properties or context menu.
10. When the SMTP Provisioning task run has completed, restart the SMTP Archiving task on the Enterprise Vault SMTP server. If there are multiple Enterprise Vault SMTP servers in the site, then you need to start the SMTP Archiving task on each SMTP server.

Checking settings for SMTP Journaling

The following list summarizes configuration settings that you need to check when implementing SMTP Journaling:

- Check that the relay MTAs are configured to BCC or journal copies of all messages to the Enterprise Vault SMTP routing address or addresses.
- Check that any load-balancing solution is correctly set up for the Enterprise Vault SMTP servers.
- Check SMTP server settings, such as which servers can connect to Enterprise Vault servers. The SMTP server settings are applied to all of the Enterprise Vault SMTP servers in the site.

  In the Enterprise Vault Administration Console, the SMTP server settings are in the properties of the container **Targets** > **SMTP**.
- Check the value set for the advanced SMTP site setting, **Selective Journal Archiving**. If you are implementing SMTP Journaling only, and not in combination with another type of SMTP journaling, then set the value to **Non-selective**. This ensures that the SMTP Archiving task only examines the X-RCPT-TO field in each message in the holding folder. Searching for the target address in all of the sender and recipient fields (X-RCPT-TO, To, CC, BCC, From, Sender) is only necessary if you implement selective journaling, such as SMTP Group or Mailbox Journaling.

  In the Enterprise Vault Administration Console, **Selective Journal Archiving** is on the **Advanced** tab of Site properties. Open the Site properties, and select the **Advanced** tab. In the **List settings from** box, select **SMTP**, and **Selective Journal Archiving** is included in the settings listed.
- Check that the routing addresses are correctly configured with the required policy, retention settings, and archives.

  If you have not configured address rewriting, all the routing addresses should be enabled for archiving; that is, **Archive messages sent from or received by this SMTP address** in the properties of the target should be selected.
- If you have assigned multiple archives to a routing address, check that the location of these archives is as expected.

  If there is a large volume of messages for journaling, it is advisable to spread the archiving load over several Enterprise Vault storage servers. You can do this by creating several journal archives in different vault stores. Each of the vault stores should be managed by a different Enterprise Vault storage service.
- If multiple archives are assigned to a routing address, then all the archives must have the same retention settings.

Additional configuration for Compliance Accelerator

If you use Compliance Accelerator in your environment then, before you start to archive SMTP messages, it is essential to configure the SMTP settings of your Enterprise Vault site appropriately.

For Compliance Accelerator to determine whether the senders and recipients of SMTP messages are internal or external to your company, you must inform Enterprise Vault of the SMTP domains that it should treat as internal domains. This enables Enterprise Vault to set the correct value for the index property Vault.MsgDirection on each message that it archives. When Compliance Accelerator subsequently processes these messages, it can determine their direction of travel from the Vault.MsgDirection property value.

For more information, see "Configuring how Compliance Accelerator handles email addresses" in the Compliance Accelerator *Administrator's Guide*.

To submit a list of internal SMTP domains

1. In the Enterprise Vault Administration Console, open the **Site Properties** dialog box for the Enterprise Vault site.
2. On the **Advanced** tab, choose **SMTP** in the **List settings from** box.
3. Click **List of internal SMTP domains**, and then click **Modify**.
4. Type the list of internal domains, and then click **OK**.

Chapter 5

Provisioning users for SMTP Group or SMTP Mailbox Journaling

This chapter includes the following topics:

About SMTP provisioning groups

SMTP provisioning groups facilitate the initial configuration and ongoing management of large numbers of target users for SMTP Group Journaling and SMTP Mailbox Journaling. You can create multiple provisioning groups to apply different policy and retention settings to different groups of users. For example, you could create one provisioning group for sales users, and a different one for engineering users.

Before creating provisioning groups for SMTP Group or Mailbox Journaling, you need to add the required SMTP routing addresses. The routing addresses are added as manual SMTP target addresses. You cannot use provisioning groups to add routing addresses.

See "Adding SMTP routing addresses" on page 66.

When you create the first provisioning group, Enterprise Vault offers to create the SMTP Provisioning task, if it does not exist. When the provisioning task runs, it configures each target user in the group with the provisioning group archiving and retention settings. The provisioning task creates a report on how it has provisioned target users in each group. The provisioning reports include details of any issues that arise during the provisioning run.

See "SMTP Provisioning task summary reports" on page 80.

There are two different types of provisioning group: one to configure users for SMTP Group Journaling, and another to configure users for SMTP Mailbox Journaling. You create new provisioning groups in the Administration Console, under **Targets** > **SMTP** > **Provisioning Groups**.

The order of SMTP provisioning groups is significant. Enterprise Vault processes the groups from the top of the list down. If you add target users in large groups, you can use group ordering to process certain users differently.

See "Changing the order of the SMTP provisioning groups" on page 77.

About SMTP Group Journaling provisioning groups

Use SMTP Group Journaling provisioning groups when you want the group members' messages archived together in the archive or archives that you assign to the provisioning group.

In the new provisioning group wizard for this type of group, you select or create one or more archives in which you want Enterprise Vault to store the messages. All the archives assigned to an SMTP Group Journaling provisioning group must have the same retention settings. Enterprise Vault enforces this requirement. If you change the retention on one of the group archives, Enterprise Vault propagates the change to all of the other archives assigned to the group.

See "Managing cascading retention settings on multiple archives" on page 53.

If you create archives in the new provisioning group wizard, you can only create SMTP archives. However, if you select existing archives, you can select any of the following types of archive: SMTP, Shared, Exchange Journal, or Domino Journal.

If you assign multiple archives to a provisioning group, Enterprise Vault spreads the archiving load across the archives.

About SMTP Mailbox Journaling provisioning groups

Use SMTP Mailbox Journaling provisioning groups when you want each group member's messages archived in a separate, personal Internet Mail archive. Enterprise Vault creates and configures the Internet Mail archives automatically.

In the new provisioning group wizard for this type of provisioning group, you select the vault store in which you want Enterprise Vault to create any new Internet Mail archives.

When provisioning a target user or address in an SMTP Mailbox Journaling provisioning group, the SMTP provisioning task tries to resolve the target user or address to an Active Directory user account. Provisioning then checks the Enterprise Vault configuration to see if an Internet Mail archive already exists for the user. If an Internet Mail archive exists, then provisioning assigns the archive for the user's SMTP messages. If an Internet Mail archive does not exist, then provisioning creates a new one in the vault store that you selected. The user is given access permissions to the new archive.

If provisioning cannot find an Active Directory account for the target, it uses the target SMTP address as the archive name. For example, if the target email address is john.doe@example.com, then the archive name is john.doe@example.com. In this situation, you have to add access permissions to the archive manually.

If you have previously configured the target users for IMAP access in Enterprise Vault, then they will already have an Internet Mail archive. When the same Internet Mail archives are used for both SMTP Archiving and IMAP access, then you need to set the same retention settings for the archives in both IMAP and SMTP provisioning groups.

If you schedule both the Client Access Provisioning task for IMAP access, and the SMTP Provisioning task for the same target users, then we recommend that you stagger the schedules so that both tasks do not run at the same time.

If you change the retention settings on the archive of a target user in an SMTP Mailbox Journaling provisioning group, Enterprise Vault does not cascade the change to other archives in the group, as in SMTP Journaling and SMTP Group Journaling. However, the provisioning task restores the provisioning group retention to the archive on the next provisioning run.

About adding target users to provisioning groups

You can add target users to a provisioning group in the new provisioning group wizard. After you have created a provisioning group, you can add or remove group members using the provisioning group **Targets** properties. The following options are available in the wizard and in the group properties:

- Windows group

- Windows user
- LDAP query
- Organizational unit
- Distribution group
- Email address

When you add a target user to a group, we recommend that you always add an Active Directory target user using 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. You can also use this option to add to the group an existing target address that is listed under **Manual Targets**. Enterprise Vault cannot provision the target address as a member of the group until you delete the existing target under **Manual Targets**.

To include as targets all of the SMTP addresses for the Active Directory user's, clear the check box, **Target only primary email address**, if it is selected. This option is in the wizard, and on the **General** tab of the provisioning group properties. If the target user has no SMTP addresses in Active Directory, the target is created, but disabled for archiving.

If the same target user is included in more than one provisioning group, then the user is provisioned according to the first group processed. You can change the order in which Enterprise Vault processes the provisioning groups. As provisioning groups for both SMTP Group and Mailbox Journaling are listed together, the same user cannot be provisioned for both types of journaling.

If you have a multi-site SMTP Archiving environment, and some target users are in more than one site, then **Target only primary email address** must be set consistently across the sites.

You can use the dashboard to list the SMTP target users in the provisioning group, and view their configuration details. To open the dashboard, click **Targets** > **SMTP** in the navigation pane of the Administration Console.

Excluding members' messages from the general journal archive

If you are implementing SMTP Group or Mailbox Journaling with SMTP Journaling, the setting, **Selective Journal Archiving**, lets you control whether target users' messages are archived in both the SMTP Journaling archives and the SMTP Group or Mailbox Journaling archives. For example, your provisioned target users may

be senior managers, who want their messages archived in the provisioning group archives only, and not in the general journal archives. In this case, you can use the value, **Exclusive**, to limit where target users' messages are stored.

For SMTP Group or Mailbox Journaling, the value of the advanced SMTP site setting, **Selective Journal Archiving**, must be **Inclusive** or **Exclusive**. When you create the first provisioning group, Enterprise Vault automatically sets the value to **Inclusive**. If you subsequently change the setting value, Enterprise Vault does not update it automatically.

See "Configuring the SMTP site setting, Selective Journal Archiving" on page 80.

Enabling or disabling archiving for all members in a provisioning group

You can create a provisioning group as enabled or disabled for archiving. In the new provisioning group wizard, this is controlled by the setting, **Archive messages sent from or received by these users**.

Creating a disabled provisioning group is useful if you have added a large group of target users to a provisioning group, and you want to exclude certain users in that group from archiving. You can create a disabled provisioning group, and add as targets the users that you want to exclude. Make sure that this provisioning group is first in the list of provisioning groups.

After you create a provisioning group, you can control whether the group members are enabled for archiving using the setting, **Archive messages for provisioned users**, in the **General** tab of the provisioning group properties

About manually-added targets

We strongly recommend that you use SMTP provisioning groups to configure users for SMTP Group and Mailbox Journaling. If necessary, you can use the **Manual Targets** node to add target SMTP addresses for SMTP Group or Mailbox Journaling. Note that targets that you add in this way are not associated with any provisioning group.

See "Adding SMTP target addresses manually" on page 82.

Adding an SMTP Group Journaling provisioning group

To add an SMTP Group Journaling provisioning group

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

3 Right-click the **Provisioning Groups** container, and then click **New > Provisioning Group > SMTP Group Journaling**.

The wizard starts.

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

- The name of the provisioning group.
- Whether SMTP archiving is enabled or disabled for the provisioning group members. This is controlled by the setting, **Archive messages for provisioned users**.
- The SMTP policy to assign to the target users in the provisioning group.
- For the SMTP email addresses that are associated with each Active Directory account, whether to create a target for each of the addresses or only the primary address.
- The domain to which the provisioning group applies. You can enter the details of a new Active Directory domain, if necessary.
  You must choose a trusted domain in your environment. Optionally, you can specify the required Global Catalog server.
- The target users who are members of the provisioning group.
- The archives in which to store the group members' messages. You can select archives of type SMTP, Shared, Exchange Journal, or Domino Journal, or create new SMTP archives in the wizard.
- The retention category to assign to the group. If you have assigned a retention plan to the selected archive, Enterprise Vault applies the retention category that is defined in the plan. To change the retention setting, you must edit the properties of the archive or choose an archive to which you have not assigned a retention plan.
- The Enterprise Vault server that is to host the SMTP Provisioning task for all the SMTP provisioning groups. You have the option to create the SMTP Provisioning task when you create the first provisioning group. This task applies the required policy to the targets of the provisioning group. You can host the task on any Enterprise Vault server in your site.

5 The new provisioning group is configured when the SMTP Provisioning task next runs. You can use the **Run Now** option on the provisioning task properties or context menu to run the task immediately.

6 When the provisioning task run has finished, restart the SMTP Archiving task on the Enterprise Vault SMTP server. If there are multiple Enterprise Vault SMTP servers in the site, then you need to start the SMTP Archiving task on each SMTP server.

Adding an SMTP Mailbox Journaling provisioning group

To add an SMTP Mailbox Journaling provisioning group

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

2 Expand the **Targets** container, and then expand the **SMTP** container.

3 Right-click the **Provisioning Groups** container, and then click **New > Provisioning Group > SMTP Mailbox Journaling**.

The 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.
- Whether SMTP archiving is enabled or disabled for the provisioning group members. This is controlled by the setting, **Archive messages for provisioned users**.
- The SMTP policy to assign to the target users in the provisioning group.
- For the SMTP email addresses that are associated with each Active Directory account, whether to create a target for each of the addresses or only the primary address.
- The domain to which the provisioning group applies. You can enter the details of a new Active Directory domain, if necessary.
  You must choose a trusted domain in your environment. Optionally, you can specify the required Global Catalog server.
- The target users who are members of the provisioning group.
- The vault store in which to create any new Internet Mail archives for the target users. If an Internet Mail archive already exists for any of the target users, then Enterprise Vault uses that archive.

If you enter an email address for a target user, then Enterprise Vault searches Active Directory for an account with that address. If found, the archive is given the Active Directory user's name. If no Active Directory account is found, then the email address is used for the archive name. The administrator will need to give user permissions to any archive created with an email address name.

- The retention category to assign to the group. If you have assigned a retention plan to the selected archive, Enterprise Vault applies the retention category that is defined in the plan. To change the retention setting, you must edit the properties of the archive or choose an archive to which you have not assigned a retention plan.
- The indexing settings to apply to new Internet Mail archives that provisioning creates for members of the group.
- The Enterprise Vault server that is to host the SMTP Provisioning task for all the SMTP provisioning groups. This task applies the required policy to the targets of the provisioning group. You can host the task on any Enterprise Vault server in your site.

5. The new provisioning group is configured when the SMTP Provisioning task next runs. You can use the **Run Now** option on the provisioning task properties or context menu to run the task immediately.
6. When the provisioning task run has finished, restart the SMTP Archiving task on the Enterprise Vault SMTP server. If there are multiple Enterprise Vault SMTP servers in the site, then you need to start the SMTP Archiving task on each SMTP server.

Changing the order of the SMTP provisioning groups

The order in which the provisioning groups are listed is significant. Provisioning processes the groups from the top of the list down. This section explains how you can change the order in which Enterprise Vault processes the provisioning groups.

You can use ordering of provisioning groups to exclude or include Windows users in provisioning:

- Excluding certain users in a selected Windows group.
  Multiple provisioning groups can include the same users, but Enterprise Vault provisions users only once; using the first group that includes them. This feature is useful if you want to provision users in a particular Windows security group, but exclude a subset of these users.

You can do this by creating a provisioning group that targets the users that you want to exclude. Configure this provisioning group so that archiving is not enabled. If you give this provisioning group the highest priority, it prevents any other provisioning group from enabling archiving for the targeted users.

- Provisioning previously excluded users in the same way as the rest of the selected Windows group.
  You can remove a provisioning group, or remove target users from a provisioning group. If a lower priority provisioning group also targets these users, the next run of the SMTP Provisioning task creates targets for the users.

The list of SMTP provisioning groups includes both SMTP Group and Mailbox Journaling provisioning groups. If users are included in multiple provisioning groups, provisioning processes them as members of the topmost group only. Provisioning then ignores these users when it processes lower priority provisioning groups that contain the users. This means that a target user cannot be provisioned for both SMTP Group Journaling and SMTP Mailbox Journaling.

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

1. In Administration Console tree, right-click the **Provisioning Groups** node and select **Properties**.
2. In the **Domain** list, select a domain to view the provisioning groups that it contains.
3. Use **Move Up** and **Move Down** buttons to rearrange the groups.

   Ensure that the most specific group is at the top of the list, and the least specific is at the bottom.

   The changes take effect the next time the SMTP Provisioning task runs.

Deleting an SMTP provisioning group

You can delete an SMTP provisioning group. When you delete a provisioning group, all the SMTP targets in the group are removed from Enterprise Vault, unless they are present in another group.

You can delete a target user or group from a provisioning group. If the user or group is an Active Directory user or group, then all the target SMTP addresses for that user or group are removed. Enterprise Vault does not delete the destination archive or archives, nor any of the archives' contents.

The targets are deleted the next time the SMTP Provisioning task runs. Enterprise Vault stops archiving items for the deleted targets.

To delete an SMTP provisioning group

1. In the left pane of the Administration Console, expand your Enterprise Vault site.
2. Expand the **Targets** container, and then expand the **SMTP** container.
3. Click the **Provisioning Groups** container.
4. Right-click the provisioning group that you want to delete and select **Delete** from the shortcut menu.
5. In the warning dialog box, click **Yes**.

   Enterprise Vault removes the provisioning group from the Administration Console.
6. Run the SMTP Provisioning task.

Adding or deleting an SMTP Provisioning task

An SMTP Provisioning task applies the provisioning group configuration to each target user in the provisioning group. This includes linking the target user with the required archive or archives, and applying the group's policy and retention settings to the group members and archives. When processing an SMTP Mailbox Journaling provisioning group, the provisioning task creates a new Internet Mail archive for any group member that does not have an existing Internet Mail archive.

You can add an SMTP Provisioning task manually, as described in this section, or you can let Enterprise Vault add one automatically when you add the first SMTP provisioning group.

The task runs once or twice each day, processing the provisioning groups in the order in which they are listed in the Administration Console. You can also use the **Run Now** option on the task properties or context menu to run the task immediately.

If you want to host an SMTP Provisioning task on a new server, you must delete it from the current server first. You can then add the task on the new server.

To add an SMTP Provisioning task

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 SMTP Provisioning task.
3. Right-click the **Tasks** container, and then click **New** > **SMTP Provisioning Task**.

   The **New SMTP 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 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.

To delete an SMTP Provisioning task

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 from which you want to delete the SMTP Provisioning task, and then click the **Tasks** container.
3. If the SMTP Provisioning task is running, right-click the **SMTP Provisioning Task for *domain***, and then click **Stop**.
4. Right-click the **SMTP Provisioning Task for *domain***, and select **Delete** from the shortcut menu.
5. In the warning dialog box, click **Yes**.

   Enterprise Vault removes the Provisioning task from the Administration Console.

SMTP Provisioning task summary reports

The SMTP Provisioning task generates a summary report at the end of each run in the folder *Enterprise_Vault_installation_folder*\Reports\SMTP Provisioning. You can configure the report options on the Reports tab of the SMTP Provisioning task properties.

Configuring the SMTP site setting, Selective Journal Archiving

For SMTP Group Journaling and SMTP Mailbox Journaling, the value of the advanced SMTP site setting, **Selective Journal Archiving**, must be either **Inclusive**

or **Exclusive**. When you create the first provisioning group, Enterprise Vault automatically sets the value to **Inclusive**.

If you implement general SMTP Journaling together with either SMTP Group or Mailbox Journaling, this setting controls where messages that contain target addresses are stored:

- **Inclusive**. A message that contains a target user address may be stored in both of the following archives:
  - An SMTP Journaling archive that is assigned to the routing address.
  - The archive that is assigned to the target user (SMTP Mailbox Journaling), or an archive that is assigned to the group that includes the target user (SMTP Group Journaling).
- **Exclusive**. A message that contains a target user address is only stored in the archive that is assigned to the target user (SMTP Mailbox Journaling), or an archive assigned to the group that includes the target user (SMTP Group Journaling).
  Any message that does not contain a target user address is stored in an SMTP Journaling archive that is assigned to the routing address.

You may want to set the **Exclusive** value if your target users have sensitive data that you want to keep separate from the general SMTP journaled data.

Table 5-1 describes in more detail how the SMTP Archiving task determines where to archive messages depending on the value of **Selective Journal Archiving** and whether routing addresses are enabled or disabled for archiving. In the information given, assume that the messages contain the correct routing address for the Enterprise Vault SMTP server.

Table 5-1 How **Inclusive** and **Exclusive** values affect the archiving task behavior

Configuration of SMTP Journaling and SMTP Group or Mailbox Journaling	SMTP Archiving task behavior
■ **Selective Journal Archiving** is set to **Inclusive**. ■ The provisioning group or manual targets, and routing address are enabled for archiving.	The task searches the sender and recipient fields (X-RCPT-TO, To, CC, BCC, From, Sender) in each message for any of the SMTP Group or Mailbox Journaling target addresses. If the task finds a target address, it stores the message in the archive that is associated with the target address it finds. The archive may be an archive associated with an SMTP Group Journaling group, or the archive associated with an SMTP Mailbox Journaling target user. A copy of the message is also stored in an archive associated with the routing address (SMTP Journaling).

Table 5-1 How **Inclusive** and **Exclusive** values affect the archiving task behavior *(continued)*

Configuration of SMTP Journaling and SMTP Group or Mailbox Journaling	SMTP Archiving task behavior
■ **Selective Journal Archiving** is set to **Inclusive**. ■ The provisioning group or manual targets are enabled for archiving. ■ The routing address is disabled for archiving.	The task searches the sender and recipient fields (X-RCPT-TO, To, CC, BCC, From, Sender) in each message for any of the SMTP Group or Mailbox Journaling target addresses. If the task finds a target address, it stores the message in the archive that is associated with the target address it finds. The archive may be an archive associated with an SMTP Group Journaling group, or the archive associated with an SMTP Mailbox Journaling target user. The task does not store the messages in an archive that is associated with the routing address (SMTP Journaling).
■ **Selective Journal Archiving** is set to **Exclusive**. ■ The provisioning group or manual targets, and routing address are enabled for archiving.	The task first searches the sender and recipient fields (To, CC, BCC, From, Sender) in each message for any of the SMTP Group or Mailbox Journaling target addresses. If the task finds a target address, it stores the message in the archive that is associated with the target address it finds. The archive may be an archive associated with an SMTP Group Journaling group, or the archive associated with an SMTP Mailbox Journaling target user. If no target user addresses are found in the message recipient fields (To, CC, BCC, From, Sender), then the archiving task stores the message in an archive that is associated with the routing address.

To configure the SMTP site setting, Selective Journal Archiving

1. Open site properties, and select the **Advanced** tab.

   In the **List settings from** box, select **SMTP**.
2. Click **Selective Journal Archiving**, and then click **Modify**.
3. Set the value to **Inclusive** or **Exclusive**, as required.
4. Apply the setting changes, and close the site properties dialog.
5. These configuration changes become effective when you restart the SMTP Archiving task on the Enterprise Vault SMTP server. If there are multiple Enterprise Vault SMTP servers in the site, then you need to start the SMTP Archiving task on each SMTP server.

Adding SMTP target addresses manually

For SMTP Group and Mailbox Journaling, we recommend that you use SMTP provisioning groups to add and manage the SMTP target addresses.

If necessary, you can add SMTP target addresses manually, as described in this section, or use the PowerShell cmdlet, New-EVSMTPTarget.

To add an SMTP target address using the Enterprise Vault Administration Console

1. In the navigation pane, navigate to **Targets** > **SMTP** > **Manual Targets**.
2. Right-click the **Manual Targets** container, and select **New** > **Target Email Address**.

   The New SMTP target wizard starts.
3. Enter the target address in the form *user@domain*. Wildcard characters are not permitted when specifying SMTP target addresses.
4. Select the type of journaling for the target address.

   The types of journaling that are available on this screen depend on the value of the SMTP site setting, **Selective Journal Archiving**. To select Group or Mailbox Journaling, the site setting value must be either Inclusive or Exclusive.

   See "Configuring the SMTP site setting, Selective Journal Archiving" on page 80.
5. Select the SMTP policy to apply to messages that include the target address. Click **Next**.
6. Click **Add** to select one or more archives in which to store the target's messages. Click **New** if you want to create a new SMTP archive for this target. Click **Next**.
7. Select the retention settings to apply to the messages. Click **Next**.

   Note: Changes to the retention settings may apply to multiple archives, if the target's archive is also associated with other targets that are in turn associated with other archives.

   ---
8. A summary of the target properties is displayed. Click **Finish**.
9. If you are adding this target address after you have configured SMTP Group or Mailbox Journaling, then rerun the SMTP Provisioning task using the **Run Now** option on the task properties or context menu.
10. When the SMTP Provisioning task run is finished, restart the SMTP Archiving task on the Enterprise Vault SMTP server. If there are multiple Enterprise Vault SMTP servers in the site, then you need to start the SMTP Archiving task on each SMTP server.

Chapter 6

Using the SMTP dashboard

This chapter includes the following topics:

About the SMTP dashboard

The SMTP dashboard in the Administration Console lets you search for SMTP targets that you have configured using SMTP provisioning. You can use the dashboard to list SMTP targets, search for targets, and view the configuration details of targets. To open the dashboard, click the **SMTP** node under **Targets**.

The dashboard has the following pages:

- **Summary**. Click the **Summary** tab in the dashboard to see this page. The page lists available provisioning groups, and shows summary information about provisioned targets.
- **Search**. Click the **Search** tab in the dashboard to see this page. The page lets you search for provisioned SMTP targets.
- **SMTP Archiving**. This page opens when you click a target in the search results. The SMTP Archiving page lists detailed configuration information for the target.

Using the Summary page

The **Summary** page shows summary information about the SMTP target configuration. The information includes the number of SMTP Group Journaling and SMTP Mailbox Journaling provisioning groups, the number of Active Directory and non-Active Directory users provisioned, and the number of targets enabled for archiving.

The configured provisioning groups are also listed on the page. When you click the provisioning group name, the **Search** page opens. The targets in the group are listed as search results on the page.

Using the Search page

The **Search** page lets you search for provisioned SMTP targets, view search results, and export search results to a file.

- To list all of the provisioned SMTP targets, click **Search** without selecting criteria.
- To list the targets in a provisioning group, click the provisioning group name on the **Summary** page. The **Search** page opens to show all the targets in the group.
  Alternatively, on the **Search** page, select **Provisioning group** in the search drop-down box. Enter the name of the provisioning group to search for, and click **Search**. The targets in the provisioning group are listed as search results.
- To search for an individual target, select **Archive name**, **User name**, or **Email address** in the search drop-down box, and enter all or part of the value for the target.

If there are a large number of search results, they are displayed in pages. Each page lists 250 search results.

You can filter search results using the criteria available in the drop-down boxes. For example, you can filter the results by provisioning group type or archive status.

Click the required column header to sort the results in ascending or descending order.

The **Export as CSV** option, at the top right-hand side of the search results, lets you save the search results to a CSV file. All pages are exported. The contents of the file reflect any sorting or filtering that you have applied to the results.

When you click the name of a target in the search results, the **SMTP Archiving** page opens in your browser. The **SMTP Archiving** page shows detailed configuration information for the target.

Using the SMTP Archiving page

When you click a target name in search results on the **Search** page of the dashboard, the **SMTP Archiving** page opens in your default browser.

The **SMTP Archiving** page lists the SMTP archiving settings for the target. The information includes the following details:

- The provisioning group that is associated with the target.
- The retention category and policy that are assigned to target.
- The SMTP addresses that are associated with the target.
- Details of the archives that are associated with the target.

Chapter 7

PowerShell cmdlets

This chapter includes the following topics:

About the PowerShell cmdlets for SMTP Archiving

Table 7-1 lists the PowerShell cmdlets that the Enterprise Vault Management Shell provides for managing the SMTP Archiving configuration. See the *PowerShell Cmdlets* guide for more information on them.

Table 7-1 PowerShell cmdlets for SMTP Archiving

PowerShell cmdlet	Description
Get-EVSMTPHoldingFolder	Retrieves details of the SMTP holding folder that is configured for the SMTP Archiving task on the current Enterprise Vault server.
Get-EVSMTPMessageTrackingLogLocation	Displays the location of the message tracking log file.
Set-EVSMTPMessageTrackingLogLocation	Updates the location of the message tracking log file.
Get-EVSMTPPolicy	Retrieves the properties of an existing SMTP policy.
New-EVSMTPPolicy	Creates a new SMTP policy.
Remove-EVSMTPPolicy	Deletes an SMTP policy.
Set-EVSMTPPolicy	Updates the properties of an existing SMTP policy.

Table 7-1 PowerShell cmdlets for SMTP Archiving *(continued)*

PowerShell cmdlet	Description
Get-EVSMTPTarget	Retrieves the properties of an existing SMTP target.
New-EVSMTPTarget	Adds a new SMTP target address.
Remove-EVSMTPTarget	Deletes an SMTP target address.
Set-EVSMTPTarget	Updates the properties of an existing SMTP target address.
Get-EVSMTPServerSettings	Retrieves the SMTP server settings that apply to all the Enterprise Vault SMTP servers in the site.
New-EVSMTPServerSettings	Creates the SMTP server settings that apply to all Enterprise Vault SMTP servers in the site.
Set-EVSMTPServerSettings	Updates the SMTP server settings that apply to all Enterprise Vault SMTP servers in the site.
Sync-EVSMTPServerSettings	Synchronizes SMTP server settings from the Enterprise Vault directory to the specified Enterprise Vault SMTP server.

For information on how to manage X-Header lists, type `get-help about_SMTPXHeaders`.

The following commands provide information on managing the authentication of incoming connections to the SMTP servers:

- `get-help about_SMTPConnectionControlList`
- `get-help about_SMTPEnumerations`
- `get-help about_TlsCertificate`

Appendix A

Configuring target address rewriting

This appendix includes the following topics:

About target address rewriting

If a high volume of SMTP traffic is sent to Enterprise Vault using one or two SMTP routing addresses, you can use a load balancing solution to distribute the incoming messages across a number of Enterprise Vault SMTP servers. For example, a simple load balancing solution is to configure equal preference MX records in DNS for the Enterprise Vault SMTP servers.

In Enterprise Vault SMTP Journaling configurations that use a single SMTP routing address to send messages to Enterprise Vault, all the messages are stored in the archive that is associated with the routing address. You can implement target address rewriting on each SMTP server to distribute the archiving load over several archives and Enterprise Vault storage servers. With target address rewriting, the messages that arrive at each SMTP server are redirected to a different target address and archive.

In Enterprise Vault SMTP Journaling configurations that use a single SMTP routing address to send messages to Enterprise Vault, all the messages are stored in the archive that is associated with the routing address. 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.

See "Assigning multiple archives to spread the archiving load across servers" on page 65.

In previous releases of Enterprise Vault, you could only implement target address rewriting to do this.

The instructions in these sections describe how to set up target address rewriting on the Enterprise Vault SMTP servers. Instructions on how to set up DNS MX records for load balancing are not included in this guide.

Figure A-1 SMTP Journaling without address rewriting

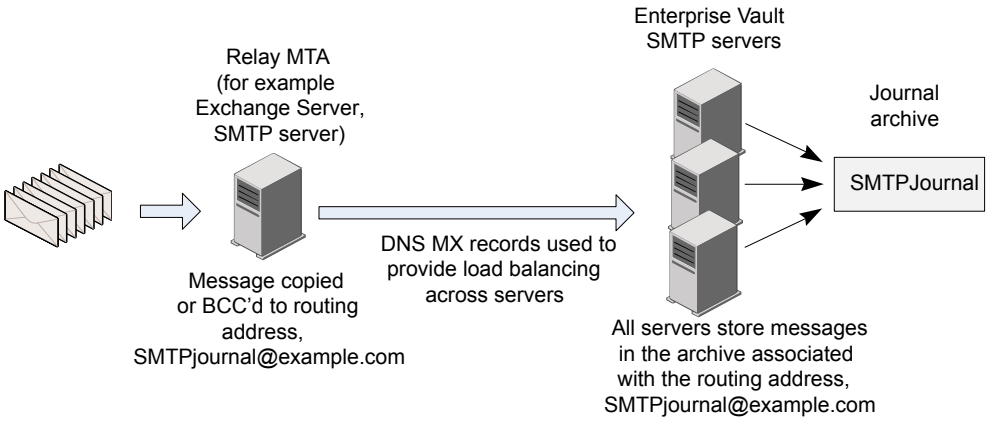
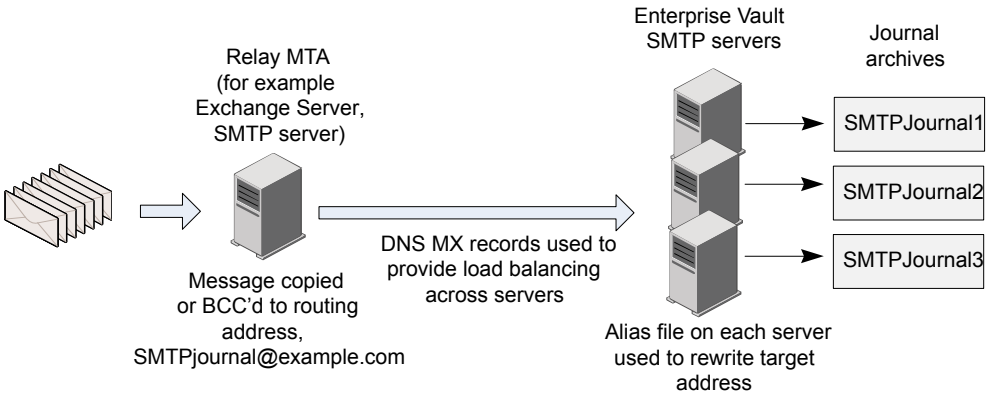


Figure A-1 shows an example environment where equal preference MX records provide basic load balancing of incoming messages across several Enterprise Vault SMTP servers. The example Enterprise Vault environment is configured as follows:

- All SMTP messages are sent to the same SMTP routing address, SMTPjournal@example.com.
- SMTP messages for SMTPjournal@example.com are evenly distributed across the different Enterprise Vault SMTP servers.
- In the Enterprise Vault Administration Console, SMTPjournal@example.com is configured as an SMTP target address, and enabled for archiving. The archive that is configured for this target is SMTPjournal.
  With this configuration, all the SMTP messages are stored in the one archive, SMTPjournal.

In the above example, the SMTP traffic is distributed across several Enterprise Vault SMTP servers, but all of the servers store the messages in the same archive. To spread the archiving load over several archives, you can implement target address rewriting on the SMTP servers. This is illustrated in the following example.

Figure A-2 SMTP Journaling with address rewriting



The example environment in Figure A-2 is configured as follows:

- As in the previous example, all SMTP messages are sent to the same SMTP routing address, SMTPjournal@example.com.
- In the Enterprise Vault Administration Console, SMTPjournal@example.com is configured as an SMTP target address. As address rewriting will send the messages to different target addresses and archives, this target address is not enabled for archiving.
- To implement address rewriting, alias entries are added manually to the aliases files on each of the SMTP servers. On the first SMTP server, for example, the alias might be SMTPserver1. The target routing address in each message that is received by this server is then rewritten as SMTPserver1@example.com. On the second SMTP server, if the alias is SMTPserver2, the target routing address in each message that is received by this server is rewritten as SMTPserver2@example.com, and so on.
- In the Enterprise Vault Administration Console, the alias address for each server, SMTPserver1@example.com, SMTPserver2@example.com, and SMTPserver3@example.com, is configured as an SMTP target address, and enabled for archiving.

Enterprise Vault stores the messages in the archive that is associated with the target address. The archive SMTPjournal1 is associated with the target SMTPserver1@example.com, the archive SMTPjournal2 is associated with the target SMTPserver2@example.com, and so on.

Steps to configure target address rewriting

This section lists the steps for setting up target address rewriting on the Enterprise Vault SMTP servers. Perform the tasks in the order shown.

Table A-1 Steps to configure target address rewriting

Step	Task	More information
Step 1	Decide which archive to assign to each SMTP routing address and alias address. Create the archive if it does not exist.	See "Configuring archives for SMTP messages" on page 63.
Step 2	In the Enterprise Vault Administration Console, add the routing addresses and alias addresses as SMTP targets.	See "Adding SMTP target addresses" on page 92.
Step 3	On each Enterprise Vault SMTP server, add target address aliases to the appropriate aliases files.	See "Adding target address aliases" on page 93.

Adding SMTP target addresses

Before you configure the SMTP target addresses, decide which archives to assign to each target address, and create the archives if they do not exist. An existing archive must be assigned to each SMTP routing address, even if you use address rewriting to redirect the messages to a different archive.

Add each routing address and each alias address as an SMTP target using the Enterprise Vault Administration Console. A domain aliases file is created automatically when you add an SMTP target address with a new domain.

To add an SMTP target address

1. In the navigation pane, navigate to **Targets** > **SMTP** > **Manual Targets**.
2. Right-click the **Manual Targets** container, and select **New** > **Target Email Address**.

   The New SMTP target wizard starts.

3. Enter the target address in the form *user@domain*. Wildcard characters are not permitted when specifying SMTP target addresses.
4. Select the type of SMTP journaling that you want to configure for the target.
5. Select the SMTP policy to apply to messages that include the target address. Click **Next**.
6. Select the archive in which to store these messages. Click **Next**.
7. Select the retention settings to apply to the messages. Click **Next**.
8. A summary of the target properties is displayed. Click **Finish**.
9. Open the properties dialog box for the SMTP target address.

   If the target is an SMTP routing address for which you want to create an alias, then clear the check box, **Archive messages sent from or received by this SMTP address**.

   If the target is an alias address, then ensure that the check box, **Archive messages sent from or received by this SMTP address** is selected.

Adding target address aliases

When you add an SMTP target address using the Enterprise Vault Administration Console, an aliases file is automatically added to the following folder on each Enterprise Vault SMTP server in the site:

Enterprise Vault installation folder\SMTP\DATA\etc\switch

The name of the aliases file is the domain part of the target address. For example, if you add the target address, SMTPjournal@example.com, then the aliases file name is `example.com`. If you then add a target with a different domain, Enterprise Vault adds another aliases file with the new domain as the file name.

Although the aliases files are added automatically to all the SMTP servers, any entries that you add to an aliases file on one of the SMTP servers are not propagated to the aliases files on the other SMTP servers.

You must configure each alias address as an SMTP target address in the Enterprise Vault Administration Console.

See "Adding SMTP target addresses" on page 92.

In a building blocks environment, you do not need to copy the aliases files to the new SMTP server, as the messages can be archived by any of the SMTP servers in the site.

To add a target address alias

1. Log on to the Enterprise Vault SMTP server for which you want to create an 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. Navigate to the folder, *`Enterprise Vault installation folder`*`\SMTP\DATA\etc\switch`.
3. Locate the aliases file that has the target address domain as its filename. Open the file using a standard text editor.
4. Add an alias entry in the form,

   incoming_name:alias *redirect_name*

   Where *incoming_name* is the local name part of the incoming routing address.

   redirect_name is the local name part of the target address to which you want to redirect messages.

   For example, to rewrite the target address in incoming messages from SMTPjournal@example.com to SMTPserver1@example.com, you add the following entry to the aliases file called `example.com`:

   SMTPjournal:alias SMTPserver1
5. Save the file.
6. Restart the Enterprise Vault SMTP service. This service is displayed in the Windows Services Console.