Symantec Enterprise Vault™

Setting up SMTP Archiving

11.0

Symantec

Symantec Enterprise Vault: Setting up SMTP Archiving

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Last updated: 2014-11-04.

Legal Notice

Symantec Corporation
350 Ellis Street, Mountain View, CA 94043

http://www.symantec.com

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 SMTP protocol.

Where to get more information about Enterprise Vault

Table 1-1 lists the documentation that accompanies Enterprise Vault.

Table 1-1 Enterprise Vault documentation set

Document	Comments
Symantec Enterprise Vault Documentation Library	Includes all the following documents in Windows Help (`.chm`) 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: ■ On the Windows **Start** menu, click **Start** > **Programs** > **Enterprise Vault** > **Documentation**. ■ In Windows Explorer, browse to the `Documentation\`*`language`* subfolder of the Enterprise Vault installation folder, and then open the `EV_Help.chm` file. ■ 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 Exchange Server Archiving	Describes how to archive items from Microsoft Exchange user mailboxes, journal mailboxes, and public folders.
Setting up Domino Server Archiving	Describes how to archive items from Domino mail files and journal databases.
Setting up File System Archiving	Describes how to archive the files that are held on network file servers.
Setting up IMAP	Describes how to configure IMAP client access to Exchange archives, and to Internet mail archives.
Setting up SharePoint Server Archiving	Describes how to archive content from Microsoft SharePoint servers.
Setting up SMTP Archiving	Describes how to archive SMTP messages from other messaging servers.
Administrator's Guide	Describes how to perform day-to-day administration procedures.

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

Document	Comments
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.
NSF Migration	Describes how to migrate 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.
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.
Utilities	Describes the Enterprise Vault tools and utilities.
PowerShell Cmdlets	Describes how to perform various administrative tasks by running the Enterprise Vault PowerShell cmdlets.
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* book, which is available from this address:

http://www.symantec.com/docs/TECH38537

“How To” articles on the Symantec Support website

Most of the information in the Enterprise Vault administration guides is also available online as articles on the Symantec Support website. You can access these articles by searching the Internet with any popular search engine, such as Google, or by following the procedure below.

To access the "How To" articles on the Symantec Support website

1. Type the following in the address bar of your web browser, and then press **Enter**:

   http://www.symantec.com/business/support/all_products.jsp

2. In the Supported Products A-Z page, choose the required product, such as Enterprise Vault for Microsoft Exchange.

3. Search for a word or phrase by using the Knowledge Base Search feature, or browse the list of most popular subjects.

Enterprise Vault training modules

The Enterprise Vault Tech Center (http://go.symantec.com/education_evtc) provides free, publicly available training modules for Enterprise Vault. Modules are added regularly and currently include the following:

- Installation
- Configuration
- Getting Started Wizard
- Preparing for Exchange 2010 Archiving
- Assigning Exchange 2007 and Exchange 2010 Permissions for Enterprise Vault
- Enterprise Vault File System Archiving

More advanced instructor-led training, virtual training, and on-demand classes are also available. For information about them, see http://go.symantec.com/education_enterprisevault.

Comment on the documentation

Let us know what you like and dislike about the documentation. Were you able to find the information you needed quickly? Was the information clearly presented? Report errors and omissions, or tell us what you would find useful in future versions of our guides and online help.

Please include the following information with your comment:

- The title and product version of the guide on which you want to comment.
- The topic (if relevant) on which you want to comment.
- Your name.

Email your comment to evdocs@symantec.com. Please only use this address to comment on product documentation.

We appreciate your feedback.

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 SMTP protocol. Any application that can send information to an SMTP server can send data to Enterprise Vault.

Table 2-1 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 2-1 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.

SMTP Archiving task	The SMTP Archiving task processes the email files in the holding folder as follows:
	
	■ Checks if the routing address in the message is an SMTP target that is enabled for archiving. If the advanced SMTP site setting, **Selective Journal Archiving** is **Yes**, also searches for SMTP target addresses in the To, From, CC, BCC, and Sender fields in the message file.
	■ Performs the following actions on each SMTP target address found that is enabled for archiving:
	  ■ Applies the policy associated with the target address
	  ■ Stores the message in the archive associated with the target address
	  ■ Applies the target address retention category
	■ By default, deletes the message file from the holding folder when archiving is completed successfully. If errors occur, the task does not delete the file.
	In Selective SMTP Journaling you can change the default behavior for certain messages.
	See "About the SMTP holding folder" on page 39.

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.

Table 2-1 Overview of SMTP Archiving components *(continued)*

Component	Description
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. You can specify the following using policy properties: ■ The X-Headers that you want Enterprise Vault to index ■ Whether the archiving task processes or discards journal reports ■ How the archiving task processes RMS-protected items The target addresses to which the policy applies are also displayed in the policy properties. The SMTP policies are displayed in the Administration Console, under **Policies** > **SMTP**.
SMTP target addresses	The SMTP target addresses are the SMTP addresses that the Enterprise Vault SMTP server and SMTP Archiving task look for in the messages that are sent to the Enterprise Vault SMTP server. The target properties contain the following settings: ■ The SMTP address that you want to make a target address. ■ The policy to assign to messages that contain the target address. ■ The retention category to assign to the messages. ■ The archive in which to store the messages. ■ Whether to archive messages sent from or received by the target address. This option is used when configuring Selective SMTP Journaling. The SMTP targets are displayed in the Administration Console, under **Targets** > **SMTP**.
SMTP archives	The SMTP Archiving task can store SMTP messages in any type of archive. As the SMTP Archiving feature is primarily for journaling, a journal archive type is probably more suitable than a user archive type. By default, the SMTP Archiving task always stores messages in the Inbox of the archive. You can create SMTP journal archives. These are displayed in the Administration Console, under **Archives** > **SMTP**. SMTP Archiving does not create archives automatically. The required archive must exist before you add an SMTP target address.

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.

An Enterprise Vault 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, such as DNS MX records, to distribute the SMTP traffic evenly across the SMTP servers in the site.

Figure 2-1 SMTP Archiving overview

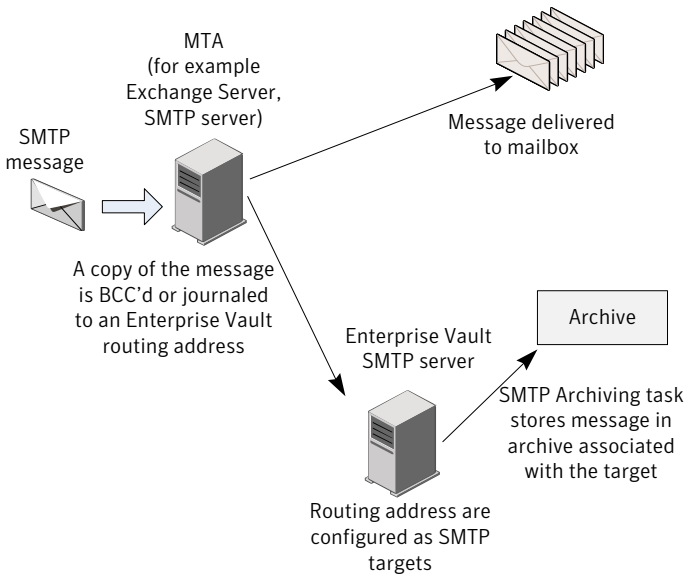


Figure 2-1 shows an example of a simple SMTP Archiving environment that performs SMTP Journaling:

- 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 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.

SMTP Archiving can be used to provide journaling for any application that can send messages over SMTP. The journaled messages are then available for searching using an eDiscovery application, such as Symantec Discovery Accelerator. Note that SMTP Archiving does not currently process the journal report information in messages that are journaled by Domino Server.

To archive messages to and from a distribution list, you need to add the SMTP address of the distribution list as an SMTP target address.

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 just selected messages. Table 2-2 provides a summary of the different journaling configurations that you can implement. These configurations are explained in more detail in the sections indicated.

Table 2-2 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. See "SMTP Journaling" on page 16.
Selective SMTP Journaling	You configure the Enterprise Vault SMTP servers 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. See "Selective SMTP Journaling" on page 18.

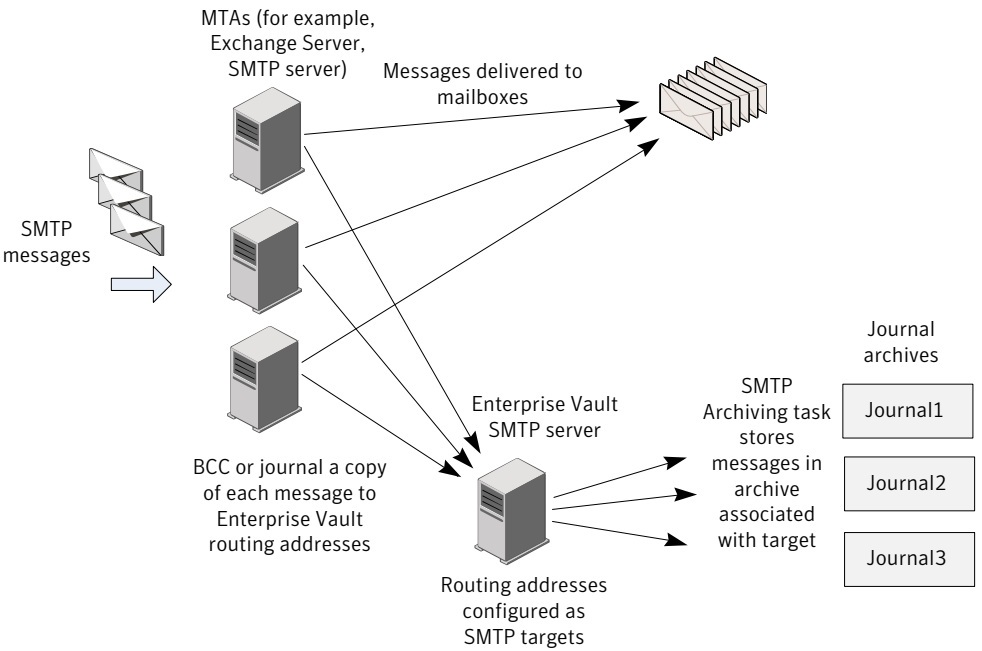
With Selective SMTP Journaling, a copy of a message may be stored in multiple archives. Enterprise Vault implements single-instance storage as permitted by the vault store configuration.

See "Creating archives for SMTP messages" on page 26.

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

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 SMTP targets, and associate each target address with an archive. In the SMTP 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 target address, the check box is selected by default.

The Enterprise Vault SMTP server checks that the routing address is an SMTP target, and adds the 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 the archive that is associated with the target routing address. The archive can be of any type. The archive types that are typically used for journal archiving are SMTP, Shared, and Exchange Journal archives.

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. To optimize performance for SMTP Journaling, ensure that this advanced site setting is set to **No**.

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.

In DNS you can configure MX record aliases to support the target routing addresses that are associated with the different journal archives. You can then configure the MTAs to use the appropriate target routing address to send messages to the Enterprise Vault SMTP server. SMTP Archiving stores the messages in the archive that is associated with the target routing address.

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 "Using Exchange Server to journal messages to Enterprise Vault" on page 20.

There are load balancing solutions available that you can use to distribute journaled messages over several Enterprise Vault SMTP servers. For example, basic load balancing can be implemented using DNS MX records.

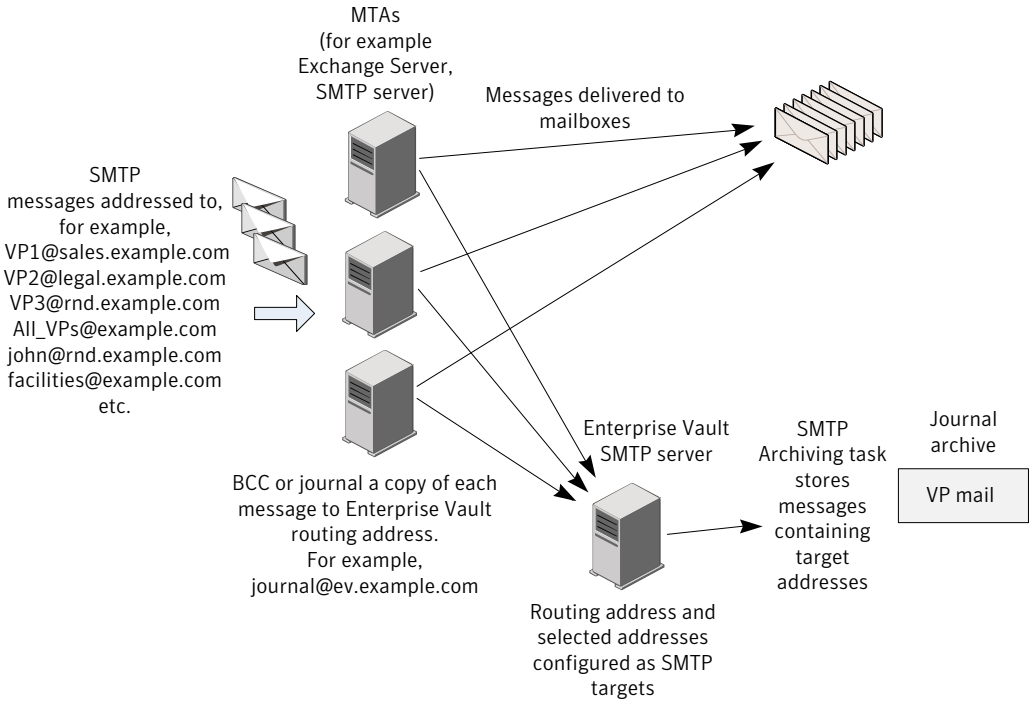
The following points summarize key tasks that you need to consider when implementing SMTP Journaling:

- Configure the relay MTAs to BCC or journal copies of all messages to the Enterprise Vault SMTP routing address.

- In Enterprise Vault decide which archives to use. These can be of any type. The archives must exist before you configure the routing addresses as SMTP target addresses.
- In Enterprise Vault configure the routing addresses as SMTP targets, and ensure that they are enabled for archiving; that is, ensure that the check box, **Archive messages sent from or received by this SMTP address**, in the properties of the target is selected.
- Ensure that the advanced SMTP site setting, **Selective Journal Archiving**, is set to **No**.

Selective SMTP Journaling

Figure 2-3 Example of Selective SMTP Journaling



You can implement Selective SMTP Journaling if you want to archive only messages that are sent to and from particular email addresses. For example, in Figure 2-3 only the messages to and from all the senior managers in example.com are archived. Messages to and from VP1, VP2, and VP3 are stored in the archive called VP mail.

The addresses for these managers, VP1@sales.example.com, VP2@legal.example.com, and VP3@rnd.example.com, are added as SMTP target addresses and enabled for archiving. The address, All_VPs@example.com, is the SMTP address for a distribution list that includes all the senior managers in the company. To archive messages to and from the distribution list, this address must also be added as a target and enabled for archiving.

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. However, in Selective SMTP Journaling, you do not enable the target routing address for archiving, so the archiving task does not store messages in the archive associated with the routing address. Instead, the task searches each message for any of the selected target addresses, and stores the message in the archive that is associated with the target address it finds.

In the example above, messages to and from VP1@sales.example.com, VP2@legal.example.com, VP3@rnd.example.com, and All_VPs@example.com are stored in the one archive, VP mail. However, target addresses could be associated with different archives. If a message contains several of the selected target 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.

Messages that do not contain any of the selected target addresses are not archived. In the example above, john@rnd.example.com and facilities@example.com are not configured as selected target addresses. The archiving task only archives messages to and from john and facilities if they contain any of the selected target addresses.

The following points summarize key tasks that you need to consider when implementing Selective SMTP Journaling:

- Configure the relay MTAs BCC or journal copies of all messages to the Enterprise Vault SMTP routing address.
- In Enterprise Vault decide which archives to use. These can be of any type. The archives must exist before you configure the SMTP target addresses.
- In Enterprise Vault configure the routing address as an SMTP target, but do not enable it for archiving; that is, do not select the check box, **Archive messages sent from or received by this SMTP address**, in the properties of this target.
- Configure as SMTP targets the selected addresses that you want to archive. In the properties of these targets, enable the targets for archiving; that is, select the check box, **Archive messages sent from or received by this SMTP address**.

If you want to archive messages to and from a distribution list, then you must add the SMTP address of the distribution list as a target, and enable it for archiving.

- Ensure that the advanced SMTP site setting, **Selective Journal Archiving**, is set to **Yes**. This ensures that the SMTP archiving task includes all of the sender and recipient fields (X-RCPT-TO, To, CC, BCC, From, Sender) in its searches.
- Decide what to do with messages in the holding folder that do not contain any selected target addresses. By default, the archiving task deletes such messages. You can change this behavior using the advanced SMTP site setting, **Delete messages without recipients or a matching target**.
  See "About the SMTP holding folder" on page 39.

You can spread the archiving load over several Enterprise Vault SMTP servers, and load-balance the distribution of messages as described for SMTP Journaling.

See "SMTP Journaling" on page 16.

Using Exchange Server to journal messages to Enterprise Vault

As an alternative to Enterprise Vault Exchange Journal Archiving, you can use Enterprise Vault SMTP Archiving to store journaled messages from an Exchange Server. If you plan to use SMTP Archiving to fulfil this function, 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 messages 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.

With SMTP Journaling the archive is determined by the target routing address. If you want more than one target archive, then you need multiple routing addresses. Configure a different archive for each target routing address. To optimize

performance, the archives should be on different Enterprise Vault storage servers. You can use Exchange Transport Rule Journaling rules to send messages to the appropriate target routing address.

Chapter 3

Installing SMTP Archiving

This chapter includes the following topics:

About installing Enterprise Vault SMTP Archiving components

See *Installing and Configuring* for the required software and settings for Enterprise Vault SMTP servers.

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 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 manual.

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 “Creating archives for SMTP messages” on page 26.

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.

Reporting

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

If you want to generate more detailed usage reports for SMTP Archiving, you will 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 data archived using the 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.

Chapter 4

Configuring SMTP Archiving

This chapter includes the following topics:

Steps to configure SMTP Archiving

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 outlines the tasks required to configure SMTP Archiving. Detailed instructions are given in the sections indicated.

You can perform all of the steps manually, or perform Steps 1 and 2, and then use a configuration wizard to guide you through Steps 3 to 5.

To start the SMTP Archiving configuration wizard

1. Perform Step 1 and 2 as listed in Table 4-1.
2. In the Administration Console, right-click the **SMTP** container under **Targets**, and select **New** > **Target Email Address**.

   The configuration wizard starts and guides you through Steps 3, 4, and 5.

   When configuring SMTP target addresses, you are asked to select an archive, retention category, and policy that you configured in Steps 1 and 2.

Table 4-1 Steps to configure SMTP Archiving

Step	Task	Description
Step 1	Create archives.	See "Creating archives for SMTP messages" on page 26.
Step 2	Set up suitable SMTP Archiving policies and retention categories.	See "Configuring retention categories and SMTP policies" on page 26.
Step 3	Configure the SMTP server settings for all Enterprise Vault SMTP servers in the site.	See "Configuring the Enterprise Vault SMTP Servers in the site" on page 31. You can perform Steps 3 to 5 manually, as described in the sections that are referenced. Alternatively, you can use the configuration wizard. See "To start the SMTP Archiving configuration wizard" on page 25.
Step 4	Adding SMTP target addresses.	See "Adding SMTP target addresses" on page 37.
Step 5	Create the SMTP Archiving task, and configure the SMTP holding folder.	See "Adding an SMTP Archiving task" on page 38.

This section describes how to perform these steps using the Enterprise Vault Administration Console. Alternatively, you can perform the configuration tasks using the Enterprise Vault PowerShell cmdlets for SMTP Archiving. The cmdlets are particularly useful for tasks such as adding a large number of SMTP target addresses.

See "About the PowerShell cmdlets for SMTP Archiving" on page 43.

Whether you are using the Administration Console or Enterprise Vault PowerShell cmdlets, you should perform the configuration steps in the order shown.

Creating 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 of any type. Alternatively you may want to create new archives to hold the items that are stored using SMTP Archiving. The archive types that are typically used for journal archiving are SMTP, Shared, Exchange Journal, or Domino Journal archives. Before adding SMTP target addresses, you have to create any new archives that are required for SMTP Archiving. Enterprise Vault does not create these automatically.

With Selective SMTP 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.

The default behavior of the SMTP Archiving task is to store messages in the Inbox of the archive.

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.

Configuring retention categories and SMTP policies

Before adding SMTP target addresses, check that suitable retention categories and SMTP policies exist for the SMTP messages that you want to archive. If necessary create new retention categories or policies for these items.

About retention categories

In the Enterprise Vault Administration Console, retention categories are located in the **Retention Categories** container under **Policies**.

When the archiving task stores a message that contains the target address, 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 allow you to control visibility of the retention category to users, and deletion of the archived item by Enterprise Vault or users. To change these settings, open the properties of the retention category in the Enterprise Vault Administration Console. The settings are not options in the New Retention Category wizard.

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**.
3. Right-click **Retention Categories** and, 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.

For more information, see "Creating a new retention category" in the *Administrator's Guide*.

About SMTP policies

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

Table 4-2 lists the settings available in the policy properties.

Table 4-2 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. There are also special Enterprise Vault X-Headers that can be used 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 28.

Table 4-2 SMTP policy properties *(continued)*

Property	Description
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 2013 or Exchange Server 2010, 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. ■ 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 *Administrator's Guide*. See the section, Journal Reports settings, under "Advanced SMTP policy settings".
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, 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. 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. 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.

A message can contain several instances of the same X-Header. Enterprise Vault indexes the first value only.

If you want to add multiple properties to messages for Enterprise Vault to index, then it may be more efficient to use the special Enterprise Vault X-Header, X-Kvs-IndexData.

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.

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

X-Kvs-IndexData can be used to provide one or more properties for Enterprise Vault to index. Using standard X-Headers, you can only add one property per X-Header. The X-Kvs-IndexData header allows you to add several properties in the one X-Header. The header contents are specified using XML.

The following example adds two properties for Enterprise Vault to index:

```
X-Kvs-IndexData: <ARCHIVED_ITEM version="1.0"><PROPSET
NAME="EVXHDR"><PROP NAME="App" type="string" RESULTS="true"
SEARCH="true">ChatApp1</PROP></PROPSET><PROPSET NAME="EVXHDR"><PROP
NAME="Dept" type="integer" RESULTS="true"
SEARCH="true">5</PROP></PROPSET></ARCHIVED_ITEM>
```

The first property, EVXHDR.App has the value ChatApp1. The property is searchable and retrievable.

The second property is EVXHDR.Dept, which has the value 5. This property is also searchable and retrievable.

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.

By default, the SMTP Archiving task archives all messages in the Inbox. As a result, searches of the archives that the archiving task uses find all items in the Inbox.

The X-Kvs-OriginalLocation header can be added to a message to specify the location of the message in the archive. If a message contains the example X-Header shown above, 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.

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.

Using Enterprise Vault Search or Discovery Accelerator to search messages for specific X-Header properties

You can search for X-Header properties using Discovery Accelerator and the Advanced Search facility in Enterprise Vault Search. In Enterprise Vault Search, you must 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.

Enterprise Vault adds X_Headers properties to the custom property set, EVXHDR. When you search for an X-Header property, specify the property set and the property 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 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 server, 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 is displayed.

   When you open the dialog 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.
Connection security	Specifies which of the following connections are permitted: ■ Only encrypted ■ Only unencrypted ■ Both encrypted and unencrypted By default only encrypted connections are allowed. 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 34. The wizard enables you to install the certificates.

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 33. 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*.

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.

If you request a certificate from VeriSign, you should specify “Microsoft” as the server platform. In this case, the certificate you receive 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, to specify all the SMTP servers in the site:

   ```
   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.

Adding SMTP target addresses

SMTP targets are the SMTP addresses that Enterprise Vault looks for in the SMTP messages that are sent to the Enterprise Vault SMTP server. The SMTP target addresses are added to the configuration of all Enterprise Vault SMTP servers in the site. In an environment that includes multiple Enterprise Vault SMTP servers, any of the SMTP servers can process messages that contain target email addresses.

To ensure that the SMTP server recognizes the messages for Enterprise Vault, add the SMTP routing addresses as targets. Routing addresses are the SMTP addresses that the MTAs use to route the messages to the Enterprise Vault SMTP servers. If you are implementing Selective SMTP Journaling, you also need to add as targets the other addresses that the archiving task uses to select the messages to archive.

By default, if a message contains the target SMTP address in the X-RCPT-TO field, then the SMTP archiving task archives the message according to the settings in the associated SMTP policy. If you are implementing Selective SMTP Journaling, then you need to perform some additional configuration of the target properties.

See "Additional configuration for Selective SMTP Journaling" on page 37.

To add an SMTP target address

1. In the navigation pane, navigate to **Targets** > **SMTP**.
2. Right-click the **SMTP** 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. Enter the SMTP policy and retention category to apply to messages that include the target address. Click **Next**.
5. Select the archive in which to store these messages. Click **Next**.
6. A summary of the target properties is displayed. Click **Finish**.
7. To start archiving messages that are sent to the new target address, 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.

Additional configuration for Selective SMTP Journaling

If you are implementing Selective SMTP Journaling, you will need to perform the following additional configuration:

- Add as targets both the routing addresses and the selected addresses.
  If you want to archive messages to and from a distribution list, remember to add the SMTP address of the distribution list as a target.
- Open Site properties, and select the **Advanced** tab.
  In the **List settings from** box, select **SMTP**.
  Ensure that the value of **Selective Journal Archiving** is **Yes**.
  If the value is **No**, select the setting and click **Modify**. Change the value of this setting to **Yes** and click **OK**. The archiving task may now search for the target addresses in all the following fields in messages: X-RCPT-TO, To, CC, BCC, From, and Sender.
  Apply the settings and close the Site properties dialog.
- Open the properties dialog for each of the SMTP target addresses, and set the check box, **Archive messages sent from or received by this SMTP address**, according to the archive or archives in which you want the archiving task to store messages that contain the target address. Use the following points to determine whether you select or clear the check box:
  - If the target is a selected address, select the check box. This ensures that the archiving task stores messages that contain this target address in the archive that is associated with the target.
  - If the target is a routing address, and you want the archiving task to store messages to this address in the associated journal archive, select the check box. If a message to this target address also includes a selected target address, then the task will store the message in the archive for the routing address and in the archive for the selected target address.
  - If the target is a routing address, and you want messages stored only in the archives that are associated with selected target addresses, clear the check box.

To apply these configuration changes you must 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 Archiving task

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.

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.

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 may happen in Selective SMTP Journaling, where the check box, **Archive messages sent from or received by this SMTP address**, is not selected for a target 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.

About the SMTP holding folder

Each SMTP Archiving task must have its own holding folder. The Enterprise Vault SMTP server 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.
- 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 should be excluded from virus scanning.

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 a message file, it moves the file to a folder named `Failed` in the holding folder. The `Failed` folder is a subfolder of the `minute` folder in which the message file is located.

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**. This folder is created as needed below the 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 off, the SMTP services and SMTP Archiving tasks on the other Enterprise Vault SMTP servers in the site receive and process new SMTP messages.

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

   When the SMTP Archiving task is finished processing the message 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.

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**.

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

   Note: If you do not stop the SMTP service then it will continue to accept 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.

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.

Chapter 5

PowerShell cmdlets

This chapter includes the following topics:

About the PowerShell cmdlets for SMTP Archiving

Table 5-1 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 5-1 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-EVSMTPHoldingFolder is provided by `Symantec.EnterpriseVault.PowerShell.Core.dll`, which is not imported automatically by the Enterprise Vault Management Shell. You must import this module.
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.
Get-EVSMTPTarget	Retrieves the properties of an existing SMTP target.
New-EVSMTPTarget	Adds a new SMTP target address.

Table 5-1 PowerShell cmdlets for SMTP Archiving *(continued)*

PowerShell cmdlet	Description
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`