Veritas Enterprise Vault™ Setting up IMAP

12.1

VERITAS™

Veritas Enterprise Vault: Setting up IMAP

Last updated: 2017-07-28.

Legal Notice

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:

http://www.veritas.com/docs/000095758

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:

http://www.veritas.com/docs/000001907

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:

http://www.veritas.com/community

Contents

About this guide

This chapter includes the following topics:

■ Where to get more information about Enterprise Vault

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
Veritas 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: ■ 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.

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

Document	Comments
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 the 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 SMTP Archiving	Describes how to archive SMTP messages from other messaging servers.
Setting up SharePoint Server Archiving	Describes how to archive content from Microsoft SharePoint servers.
Administrator's Guide	Describes how to perform day-to-day administration procedures.
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.
Classification	Describes how to assign classification values to the metadata properties of all new and existing archived items. Users of applications such as Enterprise Vault Search and Compliance Accelerator can then use the classification values to filter the items when they conduct searches or reviews.
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.

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

Document	Comments
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.veritas.com/docs/000097605

Enterprise Vault training modules

The Enterprise Vault and eDiscovery Tech Center (http://www.veritas.com/elibrary) is an eLibrary of self-paced learning modules developed around key features, best practices, and common technical support questions.

More advanced instructor-led training, virtual training, and on-demand classes are also available. For information about them, see http://www.veritas.com/education-services/training-courses.

Setting up IMAP

This chapter includes the following topics:

- About IMAP

- Configuring IMAP and enabling users for IMAP access

About IMAP

Enterprise Vault's IMAP feature provides IMAP client access to existing Exchange mailbox archives, and to new Internet mail archives for users of other mail services.

When you provision and enable users for IMAP access, Enterprise Vault sends these users a notification message which contains:

- Connection details for an IMAP server that is hosted by Enterprise Vault, which provides access to Exchange archives and Internet mail archives

- Connection details for an SMTP server in your environment, through which users can send outgoing mail from their clients and devices

When users have configured their devices to access their archives, they can access all the existing archived content, and archive new content both manually and automatically using their own client rules.

In the case of Exchange archives, the existing regime for archiving and retention remains in place. For new archives that are created for Internet mail users, retention is dictated by the IMAP policies you create and apply to the users when you provision and enable them for IMAP access.

The default IMAP archive

When a user is provisioned for a single IMAP archive, the user name for logging on to the archive comprises a domain name and a Windows user name that are separated by a backslash. For example:

`EMEA\JohnDoe`

When a user is provisioned for multiple IMAP archives, the user name for logging on to the default archive also comprises a domain name and Windows user name that are separated by a backslash. However, the user name for logging on to the remaining archives comprises a domain name, Windows user name, and identifier. For example:

`EMEA\JohnDoe\1962`

The identifier at the end of the user name is an internal identifier assigned to an archive automatically by Enterprise Vault.

When a user has been provisioned for multiple IMAP archives, a set of rules determines which is the default.

For newly provisioned archives:

- If a user is provisioned for multiple IMAP archives of the same type (Internet Mail or Exchange), then the default archive is the first archive that is provisioned.
- If a user is provisioned for both an Internet Mail archive and an Exchange archive, and then the client access provisioning task is run, the Internet Mail archive is the default archive.

If you have provisioned archives in an earlier version of Enterprise Vault and then upgraded to the current version, Enterprise Vault chooses the default archive from the following, which are in decreasing order of priority:

- The first provisioned Exchange archive that is active (not closed nor being deleted).
- The first provisioned Internet Mail archive that is active (not closed nor being deleted).

Note: If the default IMAP archive is deleted, no new default archive is selected. The user name for logging on to the remaining archives must include an identifier, even if only a single archive is available.

Configuring IMAP and enabling users for IMAP access

To configure Enterprise Vault IMAP access and enable users for IMAP, you must log in using the Vault Service account, or use an account that is assigned to the IMAP administrator role.

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

Table 2-1 introduces the tasks you must complete to configure IMAP, and to make Enterprise Vault IMAP access available to your users.

When you first configure IMAP, you should complete these tasks in order, and gain an understanding of each task. When you are familiar with the process, you can complete most of these tasks from within the provisioning group wizards. For example, when you run the **New Exchange Mailbox IMAP Provisioning Group** wizard, you are given the opportunity to create a policy, if a suitable one does not already exist.

Table 2-1   Configuring IMAP and enabling users for IMAP access

Step	Task	See this section for more details
Step 1	Obtain an SSL certificate for each IMAP endpoint that you intend to secure using SSL.	See "Obtaining SSL certificates" on page 12.
Step 2	Edit the notification message that is sent to IMAP users when they are enabled for IMAP.	See "Editing the IMAP notification message" on page 14.
Step 3	Define IMAP endpoints and SMTP endpoints. An IMAP endpoint defines the configuration of the IMAP server that runs on a single Enterprise Vault server. An SMTP endpoint contains the configuration of one of the existing SMTP servers in your environment, such as an Exchange SMTP server.	See "Defining IMAP and SMTP endpoints" on page 16.
Step 4	If you configure SMTP endpoints to accept credentials for the account that runs the client access provisioning task, you must grant the Vault Service account Send As permission on the mailbox from which IMAP notification messages are sent.	See "Granting the Vault Service account Send As permission" on page 19.
Step 5	Assign each IMAP endpoint to the Enterprise Vault server that you want to provide IMAP access.	See "Assigning IMAP endpoints to Enterprise Vault servers" on page 20.

Table 2-1   Configuring IMAP and enabling users for IMAP access *(continued)*

Step	Task	See this section for more details
Step 6	Define IMAP policies. These policies are applied to IMAP users by provisioning groups. Each IMAP policy determines which IMAP and SMTP endpoints are used by the users who are provisioned with the policy.	See "Defining IMAP policies" on page 21.
Step 7	Define Exchange and IMAP provisioning groups. Exchange IMAP and Internet mail IMAP provisioning groups determine the users and user groups that are to be enabled for IMAP access, and the IMAP policy that is applied to them. In the case of Internet mail IMAP provisioning groups, they also determine archiving defaults.	See "Defining IMAP provisioning groups" on page 21.
Step 8	Check the IMAP folder limit.	See "Checking the IMAP folder limit" on page 25.
Step 9	Run the client access provisioning task.	See "Running the client access provisioning task and the index administration task" on page 25.

Obtaining SSL certificates

If you intend to secure IMAP connections using SSL, you must obtain an SSL certificate to authenticate the Enterprise Vault servers that will operate as IMAP endpoints. You can use a single certificate that authenticates multiple servers, or use a separate certificate for each.

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.

Note the following requirements and recommendations:

■ Certificates must be in PEM format and Base64 encoded.

■ Your SSL certificate must include the fully qualified domain names of the endpoints that IMAP clients will connect to. For each endpoint, this is the **Alias** you assign when you create it.

■ A 2048-bit RSA key is recommended.

You can use the following OpenSSL syntax to create a certificate request, and a 2048-bit RSA key:

```
openssl req -new -newkey rsa:2048 -nodes -subj
"/C=country/ST=state/L=locality/O=org/OU=org_unit/CN=endpoint_alias"
-keyout key_file -out csr_file
```

where:

- *country* is the country in which your organization is based.

- *state* is the state in which your organization is based.

- *locality* is the town or city in which your organization is based.

- *org* is the name of your organization.

- *org_unit* is the requesting department in your organization.

- *endpoint_alias* is the fully qualified domain name of the alias for one of the endpoints to which users will make IMAP connections.

- *key_file* is the name of the file that will contain the certificate key.

- *csr_file* is the name of the file that will contain the certificate signing request (CSR).

For example:

```
openssl req -new -newkey rsa:2048 -nodes -subj
"/C=US/ST=California/L=Cupertino/O=Veritas Technologies LLC/OU=IT
Security/CN=imap.example.com" -keyout ev-imap-key.pem -out
ev-imap-csr.pem
```

In this example, two files are generated. You should send the CSR file to the CA, and retain the key file ready for subsequent configuration of the IMAP endpoints.

In a typical Enterprise Vault environment, which would use load balancing to distribute IMAP requests across multiple Enterprise Vault servers, you only need to request a certificate that authenticates the single fully qualified domain name assigned to the load balancer.

You can also use multiple endpoint aliases, for example to support geographical or organizational divisions in your organization. If you need to use multiple endpoint aliases, you can specify the additional aliases as Subject Alternate Names (SANs) when you make the request. The certificate you receive from the CA can then be used for all the endpoint aliases. Alternatively, you can request a separate certificate for each endpoint alias.

If you request a certificate from Veritas, 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.

When you receive the certificate from the CA, you must convert it to PEM format. For example, if you receive a p7b format file, you can use the following OpenSSL syntax to convert the certificate:

```
openssl pkcs7 -print_certs -in certificate.p7b -out certificate.pem
```

where:

- *certificate.p7b* is the p7b file you received from the CA.

- *certificate.pem* is the PEM format file you want to create.

For example:

```
openssl pkcs7 -print_certs -in cert.p7b -out ev-imap-cert.pem
```

When you configure IMAP endpoints, you can then use the certificate and key files you have created.

Note: When you create and configure each IMAP endpoint, you are prompted separately for a certificate file and an associated key file. If you have a single file that contains both the certificate and the key, you should specify the same file in each case.

Editing the IMAP notification message

When Enterprise Vault provisions and enables a user for IMAP, it automatically sends a notification email to the user's default email address. The message contains details of the IMAP server and SMTP server that the user can connect to, and the other configuration details that are needed to configure the IMAP client.

The message also contains a link to the following article on the Veritas Support website:

http://www.veritas.com/docs/000003777

This article contains links to further articles, which provide configuration instructions for popular IMAP clients and devices. If you want to, you can also edit the template message to add any other information you want your users to know about Enterprise Vault IMAP access.

During the installation, supported language versions of the IMAP notification template message are placed in folders beneath the Enterprise Vault program folder:

```
Enterprise Vault\Languages\Mailbox Messages\lang
```

where *lang* indicates the supported language.

For each supported language, the notification message is in a file called `IMAPEnabled.html`.

To locate and edit the IMAP notification message

1 Decide which language version of `IMAPEnabled.html` you want to use and locate the file.

2 Use a suitable editor to open `IMAPEnabled.html` for editing. For example, you could use `IMAPNotificationEmailViewer.exe`, which is installed in the Enterprise Vault program folder.

See "Using the IMAP notification message editor" on page 15.

3 Review the text and make any changes that you require.

4 Save the message.

5 Copy `IMAPEnabled.html` to the Enterprise Vault program folder (for example `C:\Program Files (x86)\Enterprise Vault`) on every Enterprise Vault server that runs a client access provisioning task.

Using the IMAP notification message editor

Enterprise Vault provides an editor to help you to display and to edit the IMAP notification message. The editor is a standalone executable file called `IMAPNotificationEmailViewer.exe`, which is installed in the Enterprise Vault program folder (for example `C:\Program Files (x86)\Enterprise Vault`).

The editor lets you:

■ Display a preview of the IMAP notification message.

■ Validate the contents of the email to ensure it meets the requirements of the client access provisioning task, which sends the IMAP notification messages to users.

■ Make basic changes to the message to suit your own requirements.

When you run the editor for the first time, if you have not already placed one of the language templates in the Enterprise Vault program folder, it prompts you to choose a template from one of the folders in `Enterprise Vault\Languages\Mailbox Messages`. Otherwise, the editor displays the copy of `IMAPEnabled.html` that you have already placed in the Enterprise Vault program folder.

The editor has two panes:

■ The editor pane, in which you can edit the notification message.

■ The preview pane, which immediately displays the results of any changes you make in the editor pane.
Note that the preview pane continues to display your changes as long as the message is valid. Otherwise, it displays any errors it encounters.

`IMAPEnabled.html` contains two types of special tag, which the editor displays in different colors to help you identify them:

- Conditional text tags, which the editor displays in red text.

- Placeholder tags, which the editor displays in blue text.

You can change the `value` attribute in the red conditional tasks. For example, the ID_SUBJECT tag contains the subject of the notification email:

```
<INPUT id="ID_SUBJECT" type="hidden" value="Your Enterprise Vault
archive is now accessible from any IMAP enabled device" />
```

If you wish, you can change "Your Enterprise Vault archive is now accessible from any IMAP enabled device" to a different value. However, you must not remove any of these tags.

Enterprise Vault uses the blue placeholder tags to insert into the IMAP notification message, values that are specific to each user. Although you must not change these blue tags, you may choose not to use them all in your IMAP notification message, so you may remove some of them if you wish.

If you do remove one or more of these placeholder tags, the editor warns that they are missing when you try to save the template. In this case, you should check that you have deliberately omitted the tags shown before you proceed and save the template.

The notification message shows the settings for the default IMAP archive, and for any other archives that the user can access. By default, the user name for the default IMAP archive comprises a domain name and a Windows user name that are separated by a backslash. For example:

```
EMEA\JohnDoe
```

The user names for the remaining archives consist of a domain name, a Windows user name and an identifier. For example:

```
EMEA\JohnDoe\1962
```

To show or hide the identifier in the user name for the default IMAP archive, click **Non Default UN** or **Default UN**. This is a preview feature, and does not actually change the format of the user name in the email received by an end user.

Defining IMAP and SMTP endpoints

To support IMAP connections from the users you enable for IMAP access, you must define IMAP endpoints and SMTP endpoints.

Note: IMAP endpoints determine the configuration of an IMAP server that is hosted on an Enterprise Vault server, to provide IMAP access to users' archives. SMTP endpoints contain the connection details that IMAP users require to connect to SMTP servers in your environment. Enterprise Vault does not provide an SMTP server for users of Enterprise Vault IMAP access.

An IMAP endpoint determines the configuration information for an IMAP server that runs on an Enterprise Vault server to accept connections from IMAP clients and devices. There must be one IMAP endpoint for each Enterprise Vault server you want to run an IMAP server.

Table 2-2 lists the items that you must configure for each IMAP endpoint.

Table 2-2   IMAP endpoint configuration items

Configuration item	Description
Endpoint name	A descriptive name that identifies the IMAP endpoint.
Alias name	The DNS alias, host name, or fully qualified domain name for an Enterprise Vault server. This should be the Enterprise Vault server with which you plan to associate the IMAP endpoint.
Port number	The port number on which the server will listen for IMAP requests. By default, this is port 993 (IMAPS). If you allow unencrypted connections to the IMAP server, consider that you might have to change the port number to 143 (IMAP).
Allow unencrypted connections option	By default, this option is selected so that the IMAP server requires encrypted connections. Clear this option if you want to allow unencrypted connections to the IMAP server. Note that unencrypted connections allow plain text passwords to be sent in IMAP requests. **Warning:** Do not allow unencrypted connections except in a secure network.
Certificate	If you do not choose to allow unencrypted connections, you must add SSL certificate and key files. See "Obtaining SSL certificates" on page 12.

An SMTP endpoint contains the configuration information that IMAP users require to connect to an existing SMTP server in your environment, such as an Exchange SMTP server. There must be one SMTP endpoint for each SMTP server on which you want to allow connections by your IMAP users.

Table 2-3 lists the items that you must configure for each SMTP endpoint.

Table 2-3   SMTP endpoint configuration items

Configuration item	Description
Endpoint name	A descriptive name that identifies the SMTP endpoint.
SMTP server	The DNS alias, host name, or fully qualified domain name for the SMTP server.
Port number	The port number on which the SMTP server accepts connections.
Use encrypted connection (STARTTLS) option	By default, this option is selected so that communications with the SMTP server are encrypted using STARTTLS. Clear this option if you want to allow unencrypted communications. **Warning:** Do not allow unencrypted connections except in a secure network.
SMTP server requires authentication option	Select this option if the SMTP server requires client devices to authenticate.
Sender email address for notifications	The reply-to address that will be used in the notification messages that are sent when the client access provisioning task provisions users.

Table 2-3   SMTP endpoint configuration items *(continued)*

Configuration item	Description
SMTP server credentials	Select one of the following **SMTP server credentials** options: ■ **Connect anonymously**. Select this option if the SMTP server accepts anonymous connections. You can select this option only if you have cleared the **SMTP server requires authentication** option. ■ **Use the network credentials the client access provisioning task is running under**. If you select this option, remember to configure the SMTP server to accept the credentials. ■ **Use the following credentials**. Select this option to use any other credentials to connect to the SMTP server, then enter the appropriate user name and password.

To define IMAP and SMTP endpoints

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

2   Expand the **Client Access** container.

3   Right-click **IMAP**, and click **Properties**.

4   Use the **IMAP Properties** dialog box to create IMAP and SMTP endpoints, providing the information that is described in Table 2-2 and Table 2-3.

Granting the Vault Service account Send As permission

If you set an SMTP endpoint's **SMTP server credentials** option to **Use the network credentials the client access provisioning task is running under**, you must grant the Vault Service account Send As permission on the mailbox that is associated with the SMTP address you specified in the **Sender email address for notifications** option.

For example, if you set the notification sender address to IMAP-notifications@example.com, you must grant the Vault Service account Send As permission on the mailbox whose SMTP address is IMAP-notifications@example.com.

You can set this permission manually in Exchange or use the following procedure.

To grant the Vault Service account Send As permission

1 Log in to the Exchange Server using an account that is assigned the following management role:

- Active Directory Permissions

By default, members of the "Organization Management" role group are assigned this role.

2 Open the Exchange Management Shell.

3 Run the following command:

```
Add-ADPermission -Identity mailbox_name -User domain\user_name
-AccessRights ExtendedRight -ExtendedRights "send as"
```

where:

mailbox_name is the mailbox whose SMTP address you specified in the SMTP endpoint's **Sender email address for notifications** option. If *mailbox_name* contains spaces, enclose it in quotation marks.

domain is the Active Directory domain that the Vault Service account belongs to.

user_name is the Vault Service account. If *user_name* contains spaces, enclose it in quotation marks.

Assigning IMAP endpoints to Enterprise Vault servers

On each Enterprise Vault you want to provide an IMAP server, you must assign an IMAP endpoint, then enable IMAP on the server.

The IMAP endpoint that you assign to the server, defines the configuration of the IMAP server. When you assign an endpoint, you can also enable IMAP on the server. If you do this, Enterprise Vault starts the IMAP server which is immediately ready to accept IMAP connections.

Note: Each Enterprise Vault server can host only one IMAP endpoint. In a building blocks configuration, ensure that you do not failover an Enterprise Vault server that runs an IMAP server, to another Enterprise Vault server that already hosts its own IMAP server.

To assign an IMAP endpoint and enable IMAP

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

2 Expand the **Enterprise Vault Servers** container.

3 Right-click the Enterprise Vault server to which you want to assign an IMAP endpoint, and click **Properties**.

4 Click the **IMAP** tab.

5 From the **IMAP endpoint** list, select the endpoint you want to assign to this server. **IMAP endpoint details** shows the configuration information for the endpoint you select.

Note that you can also click **New** to create a new IMAP endpoint if there is no suitable endpoint in the list.

6 If you want to start the IMAP server straight away, select the **Enable IMAP** option. In this case, the Enterprise Vault Admin Service starts the IMAP server when you click **OK** or **Apply**.

Defining IMAP policies

When Enterprise Vault provisions users and enables them for IMAP, it applies the settings that are configured in an IMAP policy. Each IMAP policy determines which IMAP endpoint and SMTP endpoint users can connect to, and whether notifications are sent to users when they are enabled for IMAP.

To define an IMAP policy

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

2 Expand the **Policies** container.

3 Right-click **IMAP**, and click **New** > **Policy**.

4 Work through the wizard to create the new IMAP policy. The wizard prompts you to provide the following information:

- A name and description for the policy.

- The IMAP endpoint that is used by users who are provisioned with this IMAP policy.

- Whether or not a notification message is sent to users when they are enabled for IMAP.

- The SMTP endpoint that is used by users who are provisioned with this IMAP policy.

Defining IMAP provisioning groups

IMAP provisioning groups apply IMAP policies and other settings to the users you specify, and enable them for IMAP access to Enterprise Vault.

You can create Exchange IMAP provisioning groups, which give Exchange archiving users access to their existing archive through an IMAP connection. You can also create Internet mail IMAP provisioning groups to create new Internet mail archives for users of other Internet mail services.

Exchange IMAP users and Internet mail IMAP users can then access their archives from IMAP clients, and archive items both manually and using client rules.

Both Exchange IMAP provisioning groups and Internet mail IMAP provisioning groups determine the following settings for the users they provision:

■ Whether or not users are enabled for IMAP.

■ The IMAP policy that is applied to the users.

Internet mail IMAP provisioning groups also determine the following settings:

■ The level of indexing detail applied to new Internet mail archives that are created for users.

■ The retention category or retention plan that is applied to the items that users archive.

■ The vault store that is used for new Internet mail archives.

For both Exchange IMAP access and for Internet mail IMAP access, you can create multiple IMAP provisioning groups to apply different policies and settings to different groups of users. For example, you could create one provisioning group for sales users, and a different one for engineering users.

When you create multiple provisioning groups, you can set the order in which Enterprise Vault uses them. Note that users can be targeted by more than one provisioning group, but Enterprise Vault provisions users with only the first group that targets them. They are ignored by subsequent provisioning groups.

This feature is useful if you want to enable IMAP for all the 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 you do not want to enable, and configure the provisioning group so that it does not enable users for IMAP. If you give this provisioning group the highest priority, it prevents the targeted users from being enabled by any other provisioning group.

Note: If you remove a group of IMAP enabled users from a provisioning group, they lose IMAP access when the client access provisioning task runs. If these users are also targeted by a lower priority provisioning group, the next run of the client access provisioning task restores IMAP access to their archives.

Defining Exchange mailbox IMAP provisioning groups

Exchange IMAP provisioning groups let you provision users who are already enabled for Enterprise Vault Exchange archiving, to give them IMAP access to their Exchange archives.

When Exchange users have been enabled for IMAP access, they can access all the items in their Exchange archives from any IMAP client. Users can search their archives, and archive new items from any mail account that is configured on their IMAP client, either manually or using rules on the client. This includes items from their Exchange mailbox if it is accessible on the IMAP client.

To define an Exchange mailbox IMAP provisioning group

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

2   Expand the **Client Access** container, then the **IMAP** and **Provisioning Groups** containers.

3   Under **Provisioning Groups**, right-click **Exchange Mailbox**, and click **New** > **Provisioning Group**.

    The **New Exchange Mailbox IMAP Provisioning Group** wizard appears.

4   Work through the wizard to create the new provisioning group. The wizard prompts you to provide the following information:

    ■   A name for the provisioning group.

    ■   Whether or not the users who are provisioned by this group are enabled for IMAP, and the IMAP policy that is applied to them if they are enabled. Note that you can also create a new IMAP policy from within the wizard if a suitable policy does not exist already.

    ■   The individual users and user groups who will be provisioned by this group.

    ■   The Enterprise Vault server that will host the client access provisioning task for the domain whose users and groups you are provisioning. You need to do this only if a client access provisioning task does not already exist for the domain.

Defining Internet mail IMAP provisioning groups

Internet mail IMAP provisioning groups let you provision Internet mail users. Enterprise Vault creates new Internet mail archives, which users can then access from any IMAP client. Users can search their archives, and archive new items from any mail account that is configured on their IMAP client, either manually or using rules on the client.

To define an Internet mail IMAP provisioning group

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

2   Expand the **Client Access** container, then the **IMAP** and **Provisioning Groups** containers.

3   Under **Provisioning Groups**, right-click **Internet Mail**, and click **New** > **Provisioning Group**.

   The **New Internet Mail IMAP Provisioning Group** wizard appears.

4   Work through the wizard to create the new provisioning group. The wizard prompts you to provide the following information:

   ■   A name for the provisioning group.

   ■   Whether or not the users who are provisioned by this group are enabled for IMAP, and the IMAP policy that is applied to them if they are enabled. Note that you can also create a new IMAP policy from within the wizard if a suitable policy does not exist already.

   ■   The individual users and user groups who will be provisioned by this group.

   ■   The level of indexing detail applied to any new archives that are created for users who are provisioned by this group. You can use the Enterprise Vault site's setting, or make specific settings for this provisioning group.

   ■   The retention category or retention plan that is applied to any new archives that are created for users who are provisioned by this group.

   ■   Choose a vault store to host the new archives that are created for IMAP users.

   ■   The Enterprise Vault server that will host the client access provisioning task for the domain whose users and groups you are provisioning. You need to do this only if a client access provisioning task does not already exist for the domain.

Setting provisioning group priority

If you have created multiple provisioning groups, and some users are targeted by more than one group, you should set the order in which Enterprise Vault processes the groups. This is because Enterprise Vault provisions a user account the first time it encounters it in a provisioning group. Enterprise Vault ignores the user account if it is targeted by lower priority provisioning groups.

Enterprise Vault uses a separate list of provisioning groups to provision Exchange IMAP users and Internet mail IMAP users. You must set provisioning group priority

separately for Exchange IMAP provisioning groups and for Internet mail IMAP provisioning groups.

To change the order in which Enterprise Vault processes provisioning groups

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

2   Expand the **Client Access** container, then the **IMAP** and **Provisioning Groups** containers.

3   Right-click the **Exchange Mailbox** or **Internet Mail** container, and click **Properties**.

4   In the **Provisioning Groups** list, click a group, and click **Move Up** or **Move Down** to raise or lower its priority.

5   Repeat step 4 until the provisioning groups are in the correct order of priority.

Checking the IMAP folder limit

Enterprise Vault limits the number of archived items that it returns to IMAP clients from each archive folder. Enterprise Vault returns the most recently archived items, up to the limit specified.

Note: If you change the folder limit setting from its default value, it can adversely affect the performance of IMAP clients on desktop and laptop clients.

You can check the current IMAP folder limit setting in your Enterprise Vault site properties.

To check the IMAP folder limit

1   In the left pane of the Administration Console, right-click your Enterprise Vault site, and click **Properties**.

2   Click the **Advanced** tab.

3   From the **List settings from** list, select **IMAP**.

4   Check the value assigned to the **Folder limit** setting.

Running the client access provisioning task and the index administration task

When you have finished the configuration of Exchange mailbox IMAP provisioning groups and Internet mail IMAP provisioning groups, you must run the client access provisioning task. You can wait for the task to run according to its schedule, or force the task to run immediately.

For Internet mail IMAP provisioning groups, Enterprise Vault creates an Internet mail archive for each user who does not already have one, then sends each user the IMAP notification message.

In the case of Exchange mailbox IMAP provisioning groups, each provisioned user's archive must be have a Metadata Store (MDS) before it is accessible using IMAP. Note that MDS also supports Enterprise Vault Search (EVS) so it is possible that some Exchange archives are already MDS-enabled.

The client access provisioning task checks each Exchange archive to see if it is MDS-enabled. If the archive is already MDS-enabled, the client access provisioning task enables the user for IMAP access and sends the notification message. If the archive is not MDS-enabled, the client access provisioning task creates an indexing subtask which MDS-enables the archive the next time the index administration task runs. In this case, a subsequent run of the client access provisioning task will enable the user for IMAP access to the Exchange archive.

Note: You can check the client access provisioning task report to find whether the task has created any MDS build tasks.

See "Reviewing the client access provisioning task report" on page 27.

Depending on the circumstances in your environment, you might have to complete all the following tasks before all provisioned users can access their archives using IMAP:

- Run the client access provisioning task.

- Run the index administration task. Note that you can monitor the index administration task's progress through MDS build tasks using the **Monitor Indexing Tasks** page.

- Run the client access provisioning task again.

To run the client access provisioning task

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

2   Under the **Enterprise Vault Servers** container, expand the server that hosts the client access provisioning task, and click **Tasks**.

3   In the right pane, check that the client access provisioning task is running.

   If the client access provisioning task is not running, right-click the task and click **Start**.

4 In the right pane, right-click the client access provisioning task, and click **Run Now**.

5 Select the **In normal mode** option, and click **OK**.

To run the index administration task

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

2 Under the **Enterprise Vault Servers** container, expand the server that hosts the index administration task, and click **Tasks**.

3 In the right pane, check that the index administration task is running.

If the index administration task is not running, right-click the task and click **Start**.

4 In the right pane, right-click the index administration task, and click **Run Now**.

To monitor MDS build tasks

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

2 Right-click the **Indexing** container, and click **Monitor Indexing Tasks**.

3 In the **Monitor Indexing Tasks** page, click a **Metadata Store Build** task to see the task's progress through the current MDS build subtasks.

Reviewing the client access provisioning task report

Each run of the client access provisioning task produces a report for each domain in which it provisions users for IMAP access. Each report includes summary information about the provisioned users.

The task creates reports in the `Reports\Client Access Provisioning` subfolder of the Enterprise Vault installation folder (for example `C:\Program Files (x86)\Enterprise Vault`).

If the client access provisioning task creates any Metadata Store (MDS) build tasks, this is stated in the report. This indicates that there are some Exchange archiving IMAP users who will not be able to access their archives using IMAP until their MDS build tasks have completed.

Note: If the error message `Error sending notification: The operation has timed out` is shown in the report, we recommend that you specify a new value for the `Send Email Timeout` setting in your Enterprise Vault site properties. For more information, see *Send Email Timeout (site properties IMAP setting)* in the *Administrator's Guide*.

Using the IMAP dashboard

This chapter includes the following topics:

- About the IMAP dashboard

- Using the Dashboard tab

- Using the Users tab

- Using the IMAP settings page

About the IMAP dashboard

The Administration Console provides an IMAP dashboard which shows details of the Enterprise Vault servers that are assigned an IMAP endpoint, and a list of IMAP sessions in which the IMAP server reported an error.

You can open the IMAP dashboard by clicking the **IMAP** node in the Administration Console and also from a web browser.

The IMAP dashboard has the following tabs:

- **Dashboard**. This shows the Enterprise Vault servers that are assigned an IMAP endpoint, and lists the most recent IMAP session in which an error occurred, for each user.

- **Users**. This shows connection details for specific users, who you can search for using their archive name or user name.

Using the Dashboard tab

You can open the IMAP **Dashboard** tab by clicking the **IMAP** node in the Administration Console, and this shows the dashboard in the right pane.

You can also access the IMAP **Dashboard** tab from a web browser at the following URL:

`http://`*`ev_server`*`/enterprisevault/MonitorIMAP.aspx`

where *ev_server* is an Enterprise Vault server.

The **Dashboard** tab contains the following lists:

- **IMAP servers with an assigned endpoint list**. Initially, this list contains an entry for each Enterprise Vault server that is assigned an IMAP endpoint. You can click any of the entries in the list to show information for just that server. To return to the information for all servers, click **Reset (Show data for all servers)**.

- **Showing user session information** lists user session details, initially for all the servers that appear in the **IMAP servers with an assigned endpoint list**. If you click one of the servers in the **IMAP servers with an assigned endpoint list**, this list shows session information for just that server.

By default, the **Showing user session information** list includes only the sessions during which the IMAP server reported an error. You can also show successful connections by clearing the **Only show errors** option.

You can also search for connection details for a specific user.

To search for connection details for a specific user

1   In the **Search** list, choose **Archive name** or **Username**.

2   Enter the archive name or user name of the user whose connection details you want to see.

3   Click **Search**.

Using the Users tab

You can open the IMAP **Users** tab by clicking the **IMAP** node in the Administration Console, then clicking the **Users** tab in the right pane.

You can also access the IMAP **Users** tab from a web browser at the following URL:

`http://`*`ev_server`*`/enterprisevault/SearchIMAP.aspx`

where *ev_server* is an Enterprise Vault server.

Use this tab to search for connection details of a specific IMAP user.

To search for connection details for a specific user

1   In the **Search** list, choose **Archive name** or **Username**.

2   Enter the archive name or user name of the user whose connection details you want to see.

3   Click **Search**.

4   In the list of results, click the user name or archive name to see connection details for the individual user.

Using the IMAP settings page

When you click the user name or archive name of a user in the **Users** tab of the IMAP dashboard, Enterprise Vault launches the **IMAP settings** page in your default browser.

The URL for the **IMAP settings** page is:

```
http://ev_server/enterprisevault/IMAP.aspx?sid=user_SID
```

where *ev_server* is an Enterprise Vault server, and *user_SID* is the security identifier (SID) of the user you clicked. If you know the SID for the user whose details you want to see, you can open the URL directly in your browser. End users who are logged in with a Windows account that is enabled for IMAP access, can also open the page without specifying the `sid` parameter.

The IMAP settings page lists all the IMAP settings the user requires to configure their IMAP client to access their archive.

The user name for the default IMAP archive consists of a domain name and a Windows user name. For example:

```
EMEA\JohnDoe
```

The user name for this archive can optionally include an identifier, as explained in the footnote below the settings. Other archives that the user can access require the user name to include the identifier. For example:

```
EMEA\JohnDoe\1962
```

Note: If you have already configured an IMAP client, such as Outlook, to access the default archive, and the user name includes an identifier, you do not need to change the configuration.

PowerShell cmdlets for IMAP

This chapter includes the following topics:

■ About the IMAP cmdlets

■ Running the IMAP cmdlets

■ Using Get-EVIMAPUsers

■ Using Get-EVIMAPUserSettings

■ Using Set-EVIMAPServerDisabled

■ Using Set-EVIMAPServerEnabled

About the IMAP cmdlets

Enterprise Vault provides PowerShell cmdlets which you can use to display IMAP users and their settings, and to enable and disable IMAP on configured IMAP servers.

Table 4-1 describes the IMAP cmdlets that the Enterprise Vault Management Shell provides.

Table 4-1   IMAP cmdlets

Cmdlet	Description
Get-EVIMAPUsers	Displays the details of users who are provisioned and enabled for IMAP.
Get-EVIMAPUserSettings	Displays the connection details for a specific IMAP user.

Table 4-1   IMAP cmdlets *(continued)*

Cmdlet	Description
`Set-EVIMAPServerDisabled`	Disables IMAP on a specific Enterprise Vault server.
`Set-EVIMAPServerEnabled`	Enables IMAP on a specific Enterprise Vault server.

Running the IMAP cmdlets

To run the IMAP cmdlets, first run the Enterprise Vault Management Shell. This loads the Enterprise Vault snap-in which makes the IMAP cmdlets available in the shell.

Help is available for the cmdlets. For example, the following command shows the detailed help for `Get-EVIMAPUsers`:

```
Get-Help Get-EVIMAPUsers -detailed
```

Using Get-EVIMAPUsers

`Get-EVIMAPUsers` lists the users who are provisioned and enabled for IMAP access. Use the following syntax when you run `Get-EVIMAPUsers`:

```
Get-EVIMAPUsers -ArchiveName -NTUserName [<CommonParameters>]
```

For example:

```
Get-EVIMAPUsers
```

This lists all the users in the Enterprise Vault site who are provisioned and enabled for IMAP access. You can also use `Get-EVIMAPUsers` to display details for an individual user, by specifying an archive name with the `-ArchiveName` parameter, or a Windows user with the `-NTUserName` parameter. For example:

```
Get-EVIMAPUsers -NTUserName JohnDoe
```

Here is an example of the output from `Get-EVIMAPUsers`:

```
MbxArchiveName : JohnDoe
MbxNTDomain   : EMEA
MbxNTUser     : JohnDoe
SID           : S-1-5-21-1295326745-1955594489-3830948510-1117
EnabledForIMAP : True
```

```
ReadyForIMAP   : True
Type           : Internet Mail
```

You can use the SID (security identifier) with `Get-EVIMAPUserSettings`, to display IMAP and SMTP connection settings for a user.

Note also the `ReadyForIMAP` value. When you provision and enable an Exchange user for IMAP access, their existing Exchange archive must be MDS-enabled. Provisioning automatically creates an indexing subtask to enable the archive, and this subtask is processed the next time the index administration task runs. Until this subtask is processed, the `ReadyForIMAP` value that is listed by `Get-EVIMAPUsers` is `False`.

Internet mail archives are automatically MDS-enabled when they are created, and always have a `ReadyForIMAP` value of `True`.

Using Get-EVIMAPUserSettings

`Get-EVIMAPUserSettings` lists the IMAP and the SMTP connection settings for the Windows user whose SID (security identifier) you provide. Use the following syntax when you run `Get-EVIMAPUserSettings`:

```
Get-EVIMAPUserSettings -SID [-FullFormatUserName [<SwitchParameter>]]
[<CommonParameters>]
```

Example 1:

```
Get-EVIMAPUserSettings -SID
S-1-5-21-1295326745-1955594489-3830948510-1117
```

This lists the IMAP and the SMTP connection settings for the specified user, and details about the archive and its status.

```
Archivename              : JohnDoe
ArchiveOwner             : True
ArchiveType              : Internet Mail
IMAP_Connection_Security : SSL/TLS
IMAP_Password            : Use the password for account: EMEA\JohnDoe
IMAP_Port                : 993
IMAP_Server              : ev1.example.com
IMAP_UserName            : EMEA\JohnDoe
ReadyForIMAP             : True
SMTP_Connection_Security : None
SMTP_Password            : Not applicable
SMTP_Port                : 25
SMTP_Server              : smtp.example.com
```

```
SMTP_UserName           : Not applicable
WindowsUser             : EMEA\JohnDoe
```

Example 2:

```
Get-EVIMAPUserSettings -SID
S-1-5-21-1295326745-1955594489-3830948510-1117 -FullFormatUserName
```

This lists the IMAP and the SMTP connection settings for the specified user, and details about the archive and its status. The `-FullFormatUserName` parameter includes an identifier in `IMAP_UserName`. Here is an example of the output from `Get-EVIMAPUserSettings`:

```
Archivename             : JohnDoe
ArchiveOwner            : True
ArchiveType             : Internet Mail
IMAP_Connection_Security : SSL/TLS
IMAP_Password           : Use the password for account: EMEA\JohnDoe
IMAP_Port               : 993
IMAP_Server             : ev1.example.com
IMAP_UserName           : EMEA\JohnDoe\1962
ReadyForIMAP            : True
SMTP_Connection_Security : None
SMTP_Password           : Not applicable
SMTP_Port               : 25
SMTP_Server             : smtp.example.com
SMTP_UserName           : Not applicable
WindowsUser             : EMEA\JohnDoe
```

The `ArchiveOwner` value indicates whether or not the specified user is the owner of the archive that is listed. `True` means that the specified user owns the archive; `False` means that the specified user has delegate access to the archive.

Note also the `ReadyForIMAP` value. When you provision and enable an Exchange user for IMAP access, their existing Exchange archive must be MDS-enabled. Provisioning automatically creates an indexing subtask to enable the archive, and this subtask is processed the next time the index administration task runs. Until this subtask is processed, the `ReadyForIMAP` value that is listed by `Get-EVIMAPUserSettings` is `False`.

The `IMAP_UserName` value includes an identifier at the end for all the archives that the user can access. This identifier is included because the `-FullFormatUserName` parameter is specified. Without this parameter, the identifier would be omitted for the default archive. For more information, See

Using Set-EVIMAPServerDisabled

`Set-EVIMAPServerDisabled` stops the IMAP server and disables IMAP on an Enterprise Vault server. Use the following syntax when you run `Set-EVIMAPServerDisabled`:

`Set-EVIMAPServerDisabled -ComputerNameAlternate [<CommonParameters>]`

For example:

`Set-EVIMAPServerDisabled -ComputerNameAlternate ev1.example.com`

This stops the IMAP server that is running on ev1.example.com, and disables IMAP on the server.

Using Set-EVIMAPServerEnabled

`Set-EVIMAPServerEnabled` enables IMAP on an Enterprise Vault server that is configured for IMAP, and starts the IMAP server. Use the following syntax when you run `Set-EVIMAPServerEnabled`:

`Set-EVIMAPServerEnabled -ComputerNameAlternate [<CommonParameters>]`

For example:

`Set-EVIMAPServerEnabled -ComputerNameAlternate ev1.example.com`

This enables IMAP on ev1.example.com, and starts the IMAP server.

Index

R

Roles-based administration
    IMAP administrator role 10

S

SearchIMAP.aspx 30
Set-EVIMAPServerDisabled 36
Set-EVIMAPServerEnabled 36
SMTP endpoints
    defining 16
SSL certificates 12, 16
    converting 12
    format 12
    obtaining 12

V

Vault Service account
    requirement for Send As permission 19