Enterprise Vault™ PST Migration

15.0

VERITAS™

Enterprise Vault™: PST Migration

Last updated: 2024-03-04.

Legal Notice

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

https://www.veritas.com

Technical Support

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

https://www.veritas.com/support

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

https://my.veritas.com

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

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

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

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

Documentation

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

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

Documentation feedback

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

evdocs@veritas.com

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

https://www.veritas.com/community

Contents

Chapter 1 About this guide 7

Introducing this guide 7
Where to get more information about Enterprise Vault 7
Enterprise Vault training modules 10

Chapter 2 Introduction to PST migration 11

Introducing PST file migration 11
Tools for migrating PST files 12
Feature comparison of PST migration tools 12
About the Exchange PST Migration policy 13
Improving performance when archiving PST file contents 14
Migrating PST files in hosted environments 15
About the Personal Store Management node 16
Creating filters 17

Chapter 3 PST file ownership 19

About PST file ownership 19
PST file marking to determine PST file ownership 20
PST message sampling to determine PST file ownership 20
Configuring message sampling to determine PST file ownership 22
Results of message sampling 24

Chapter 4 PST migration: scripted 26

Overview of the scripting mechanism for PST migration 26
Undertaking the PST migration process using Policy Manager 27
Preparation for PST scripted migration 28
Output from PST migration 30
[PSTcheckpoint] section PST scripted migration 30
Enterprise Vault event log for PST scripted migration 32
Example initialization file for PST scripted migration 33

Chapter 5 PST migration: wizard-assisted 35

About the PST Migrator wizard 35
Outline of the wizard-assisted PST migration process 36
Preparation for the wizard-assisted PST migration process 38
Migration tips for the wizard-assisted PST migration process 39
How the wizard-assisted PST migration process affects users 41
Starting the wizard-assisted PST migration process 42

Chapter 6 PST migration: Locate and Migrate 43

About Locate and Migrate 43
Setting up PST Locate and Migrate 44
Administrator roles required to manage PST Locate and Migrate 44
Configuring the holding folder for PST Locate and Migrate 45
Creating and configuring the PST Locator, PST Collector, and PST Migrator tasks 47
Migrating PST files using PST Locate and Migrate 52
Running the PST Locator task to find domains and computers 54
Selecting computers for PST searching 59
Configuring paths to include or exclude for PST searching 60
Running the PST Locator task to find PST files 61
Running the PST Collector task 65
Running the PST Migrator task 65
PowerShell cmdlets for PST migration 66
Excluding network shares from PST migration using the PstLocatorTask.exe.config file 69
Troubleshooting PST migration 69

Chapter 7 PST migration: client-driven migration 71

About client-driven PST migration 71
Options to configure client-driven PST migration 72
Preparation for client-driven PST migration 73
Editing the PST migration messages for client-driven PST migration 74
Configuring the PST holding folder for PST client-driven migration 75
Creating a PST Migrator task for PST client-driven migration 76
Enabling mailboxes for PST client-driven migration 77
Enabling mailboxes for PST file submission 78

Permissions required for migrating PST files stored on network drives 79

Chapter 1

About this guide

This chapter includes the following topics:

- Introducing this guide
- Where to get more information about Enterprise Vault

Introducing this guide

This guide describes how to migrate and archive the contents of PST files to Enterprise Vault. Administrators can configure Enterprise Vault to migrate PST files automatically or let end users choose whether to migrate PST files to Enterprise Vault.

Where to get more information about Enterprise Vault

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

Table 1-1 Enterprise Vault documentation set

Document	Comments
Veritas Enterprise Vault Documentation Library	Includes all the following documents in Windows Help (`.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`*`\Administration Guides` 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 Domino Server Archiving	Describes how to archive items from Domino mail files and journal databases.
Setting up Exchange Server Archiving	Describes how to archive items from Microsoft Exchange user mailboxes, journal mailboxes, and public folders.
Setting up File System Archiving	Describes how to archive files that are held on network file servers.
Setting up IMAP	Describes how to configure IMAP client access to Exchange archives and Internet Mail archives.
Setting up SharePoint Server Archiving	Describes how to archive documents from Microsoft SharePoint servers.
Setting up Skype for Business Archiving	Describes how to archive Skype for Business sessions.
Setting up SMTP Archiving	Describes how to archive SMTP messages from other messaging servers.
Setting up Microsoft Teams Archiving	Describes how to archive Microsoft Teams data.

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

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

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

Enterprise Vault training modules

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

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

Chapter 2

Introduction to PST migration

This chapter includes the following topics:

- Introducing PST file migration
- Tools for migrating PST files
- Feature comparison of PST migration tools
- About the Exchange PST Migration policy
- Improving performance when archiving PST file contents
- Migrating PST files in hosted environments
- About the Personal Store Management node

Introducing PST file migration

Enterprise Vault can archive information that is held in PST files on users' computers. Administrators can enable mailboxes for PST file migration. Administrators can also let end users choose whether to migrate PST files to Enterprise Vault. To carry out the PST migration, Enterprise Vault finds the computers that contain PST files, locates the files, determines ownership, and migrates the files to the appropriate archives. To determine ownership of PST files, administrators can use PST file marking or PST message sampling. You can choose to migrate PST files to Exchange Mailbox archives or Internet Mail archives.

Enterprise Vault provides the following tools for migrating PST files to archives:

- Locate and Migrate
- Client-driven PST migration

- Scripted migration using Policy Manager
- PST Migrator wizard-assisted migration

Tools for migrating PST files

Enterprise Vault provides the following tools for migrating the contents of PST files to archives:

- Scripted migration using Policy Manager. This tool is useful for performing bulk migrations of PST files, but you need to collect the PST files in a central location.
  See "Overview of the scripting mechanism for PST migration" on page 26.
- PST Migrator wizard-assisted migration. If you have a small number of PST files, this tool provides a quick way to migrate them to Enterprise Vault.
  See "About the PST Migrator wizard" on page 35.
- Locate and Migrate. This tool locates PST files on users' computers, copies them to a central location, and then migrates them. You can configure specific paths to include or exclude during PST searching. Unless you have only a few PST files to migrate, Locate and Migrate is likely to require least effort on your part.
  See "About Locate and Migrate" on page 43.
- Client-driven PST migration. This tool lets you configure users' computers to locate PST files automatically and copy them to a central PST holding folder. Enterprise Vault then migrates the PST file contents from the holding folder to Enterprise Vault archives.
  You can also decide whether you want to give users control over migrating their PST files.

  Client-driven PST migration is useful in the following situations:

  - Users' computers are available on the network only occasionally.
  - You do not have permission to access PST files on the users' computers.
  - Users need continual access to their PST files.

  See "About client-driven PST migration" on page 71.

Feature comparison of PST migration tools

Table 2-1 shows a feature comparison of the PST migration tools.

Table 2-1 Feature comparison of PST migration tools

Feature	Scripted using Policy Manager	PST Migrator wizard	Locate and Migrate	Client-driven migration
Simple to use for a few PST files	No	Yes	No	No
Locate PST files on users' computers	No	No	Yes	Yes
Allow users to decide whether or not to migrate the PST files that are found on their computers	No	No	No	Yes
Allow users to manually submit PST files for migration	No	No	No	Yes
Collect users' PST files in central location	No	No	Yes	Yes
Suitable for migrating large numbers of PST files	Yes	No	Yes	Yes
Can use supplied password to open PST file	No	No	Yes	Yes
Can adjust Exchange Server quotas	No	No	Yes	Yes
Use marking in PST to determine archive	Yes	Yes	Yes	No
Use mail profile entry to determine archive	No	No	Yes	Yes
Use name of host computer to determine archive	No	No	Yes	No
Migrate files to Internet Mail archives	Yes	Yes	Yes	No

About the Exchange PST Migration policy

To customize the way that PST files are migrated for a group of users, you can edit the settings in the Exchange PST Migration policy that is associated with the

provisioning group to which the users' mailboxes belong. Exchange PST Migration policies are listed under **Policies** > **Exchange** in the Administration Console.

The Exchange PST Migration policy properties include settings to define the following:

- Whether to create shortcuts for migrated items, and where to create them.
- Custom shortcuts.
- Whether to adjust Exchange Server quotas to accommodate the additional shortcuts in mailboxes.
- The default retention category.
- The migration priority that the PST Collector and PST Migrator should use to collect and migrate PST files.
- The classes of items to migrate.
- Whether to allow users to submit PST files for migration and change the retention category of files that they choose to migrate.
- The paths that the Enterprise Vault Outlook Add-In should specifically look in or ignore when it searches for PST files on users' computers.
- Whether to migrate the Deleted Items folder and unexpired calendar items.
- The folder structure to create for shortcuts in users' mailboxes.
- The Windows code page to use if the PST Migrator creates folders in users' mailboxes.
- How to process PST files after successful migration.
- The notification emails that you want Enterprise Vault to send for various PST migration events.

When items have been migrated, the original items in the PST files are not deleted. If you want to delete the PST files after successful migration, choose to do so on the **Post Migration** tab of the PST Migration policy.

Improving performance when archiving PST file contents

When Enterprise Vault archives items, it converts the contents to HTML and indexes them. The default conversion timeout for this process is 30 minutes. Enterprise Vault makes three attempts to convert an item, and so can take up to 90 minutes before it fails an item and moves to the next one.

If there are very large or complex items in a PST file, it can take a long time to migrate them all. If you do not need the content of the items to be indexed, you can improve performance by lowering the conversion timeout to a few minutes.

To change the conversion timeout

1. On the Storage service computer, set the string registry value ConversionTimeout to the required timeout in minutes. The entry must be under the following registry key:

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

2. Restart the Storage service.

Note: This change to the conversion timeout also affects normal archiving, so remember to return it to the original value when you have migrated the PSTs.

You can also improve performance by making Enterprise Vault create text versions rather than HTML versions of certain document types. See the *Administrator's Guide* for instructions on how to control content conversion.

Migrating PST files in hosted environments

For each mail item that Enterprise Vault archives, it creates an XML document that contains the item's sender information and recipient information. This document is archived with the item, and Enterprise Vault subsequently uses the XML data during indexing.

Enterprise Vault builds the XML data it requires from the sender information and recipient information in each item as it is archived. However, if any of the information is not present in the item, Enterprise Vault attempts to establish a connection to the relevant Exchange server's domain controller to gather the information. This process requires that at least one Exchange server is targeted in your site.

If you migrate PST files in environments where no suitable Exchange server is available to provide the information that Enterprise Vault requires, migration performance can be degraded. For example, this situation can arise in the following circumstances:

- You migrate legacy data from the PST files that were created in an old Exchange environment, whose Exchange servers no longer exist.

- You migrate data from PST files in a hosted environment that has no Exchange server.

In cases like these, you should set a registry value to bypass the lookup of addresses during archiving.

To bypass Active Directory address lookups

1. On every Enterprise Vault Storage service computer, create a new DWORD registry value that is called BypassAddressLookups under the following registry key:

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

2. Set BypassAddressLookups to 1.
3. Restart the Storage service.

This setting allows PST migrations to use only the sender information and recipient information that it finds in each mail item that it archives. Enterprise Vault does not attempt to establish an Active Directory connection to resolve addresses.

About the Personal Store Management node

All the computers, mailboxes, and PST files that are found on the network are listed in various nodes under the Personal Store Management node.

When you click **Personal Store Management**, the page that opens displays a summary view of all the computers, mailboxes, and PST files that Enterprise Vault manages.

The Personal Store Management node has the following nodes:

- **Files.** This node contains information of the PST files that are being migrated or have been migrated to Enterprise Vault. You can use various options to change the migration status, priority, mailbox, archive, and retention category of the listed files.
- **Computers.** This node contains information of all the computers that have been found on the network. You can enable or disable PST file searching on the listed computers.

- **Mailboxes.** This node contains information of the list of mailboxes that are enabled for archiving. You can enable or disable the listed mailboxes for client-driven migration.

You can sort and filter the displayed information, and also saved a collection of items for future reference. You can also add, remove, or move columns to further customize the display. You can save the customization you make to the display.

You can export the displayed items to a CSV file or an HTML file. Note that when you export the details, Enterprise Vault exports the information in all the columns irrespective of the customization made.

Note: This node includes only those PST files that are searched and migrated to Enterprise Vault by the Locate and Migrate method or obtained by client-driven migration. This node does not include the files that have been migrated to Enterprise Vault using the wizard-assisted migration or the scripted migration.

For more information about each node, see the Administration Console help.

If the Personal Store Management is taking a long time to load, it could be because your Enterprise Vault server does not have a connection to the Internet.

For a possible workaround, see the section called "Performance issues when an Enterprise Vault server has no Internet connection " in the *Installing and Configuring* guide.

Creating filters

The parent nodes - **Files**, **Computers**, and **Mailboxes** - each have a **Filters** node. The **Filters** node includes the predefined filters and the filter criteria that you have created and saved for future reference. When you click a filter node, the filter is run and the display is updated dynamically.

Note the following:

- You can create up to 100 filters within each **Filters** node. You can configure this number by creating a new DWORD registry value that is called MaxFilterCount under the following registry key:

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

Note: We recommend that you limit the filter count to 100. Exceeding this value may affect the performance of Enterprise Vault.

- The **Filters** node of each parent node includes predefined filters that you can use.
- You can rename or delete any of the filters created, including the predefined filters.
- To filter the list on the basis of multiple keywords, use commas to separate the keywords.

To create and save filters

1. Select the filter criteria you want to use to refine the list. You may select multiple criteria by clicking the + button. Use the - button to remove filter criteria.

   For example, to filter the list to see only those files that have failed to migrate, do the following:

   - In the first drop-down menu, select **Migration Status**.
   - In the second drop-down menu, select **contains any of**.
   - In the third drop-down menu, select **Failed to migrate**.

2. Click **Apply**. The display changes according to the filter criteria applied, and the **Apply** button changes to **Save**.
3. Click **Save**.
4. In the **Save** dialog box, do one of the following:

   - Click **Save filter** and enter a name and description for the filter.
   - Click **Save results** and enter a name and description for the saved results folder. Alternatively, you may choose to add the displayed items to an existing saved results folder.

5. Click **Save**. Saved filters are listed as separate nodes within the **Filters** node. When you click the saved filter, the filter is run and the display is dynamically updated. Saved results are listed as separate nodes within the **Saved Results** node, and displays static data.

Chapter 3

PST file ownership

This chapter includes the following topics:

- About PST file ownership
- PST file marking to determine PST file ownership
- PST message sampling to determine PST file ownership

About PST file ownership

Establishing the ownership of a PST file is important for storing its contents into the appropriate user's archive. Enterprise Vault determines the ownership using several methods.

If the PST file is found in a user's Outlook profile, then that user is considered to be the owner of the PST file. For all other PST files that are found on the network, Enterprise Vault tries to determine ownership in the following ways:

- PST file marking. You can configure the Enterprise Vault Outlook Add-In so that, when a user starts Outlook, the Enterprise Vault Outlook Add-In writes a marker into each PST file that is listed in the mail profile. The marker indicates the Enterprise Vault site, the associated archive, and the associated retention category. If PST Migrator finds one of these marked PST files, it can read this information and determine the mailbox that owns the default archive.
  See " PST file marking to determine PST file ownership" on page 20.
- PST message sampling. If you have chosen to use message sampling to identify the owner, and a possible owner is found, then that user's mailbox is used.
  See "PST message sampling to determine PST file ownership" on page 20.

You can use message sampling as the initial method to identify PST file owners or you may allow Enterprise Vault to use this method only if PST file marking fails. You can configure this by editing the Personal Store Management properties.

If Enterprise Vault cannot determine the ownership of the PST file, the associated mailbox, and its corresponding archive, then the PST file status is displayed as **Not ready**. You need to edit the properties of the PST file to provide the required information, and change the status to **Ready to copy**. You can also select a default archive to store the PST files that have no owners identified.

PST file marking to determine PST file ownership

Depending on configuration, when a user starts Outlook, the Enterprise Vault Outlook Add-In writes a marker into each PST file that is listed in the mail profile. The marker indicates the Enterprise Vault site, the associated archive, and the associated retention category. All the PST migration tools can use the marker to determine the owning mailbox and then migrate the file contents to that mailbox's default archive. Marking PST files can be enabled or disabled in Exchange Desktop policies using the setting, **Mark PST files**, in the list of advanced Outlook settings.

If marking is switched on, the Outlook Add-In does the following when Outlook starts:

- Tries to open every PST that is listed in the user's mail profile. The next time that the user starts Outlook, the Outlook Add-In prompts for passwords to password-protected PSTs, and displays error messages for any inaccessible PSTs.

  Note: To avoid migration failures due to incorrect passwords or missing passwords, edit the **General** tab of the Personal Store Management properties to allow Enterprise Vault to override passwords and migrate the files. This feature is not available for client-driven migration.

- Does not update the PST file marker again except if a different mail profile was used to access it. Enterprise Vault assumes that the owner of the PST file is the last profile that was used to access it.
- Marks any further PST files that are subsequently added to the mail profile. The marking happens when Outlook is started, so merely opening a PST file and then closing it again is not sufficient to mark that PST.

PST message sampling to determine PST file ownership

PST message sampling determines the owner of each PST file by sampling a configurable percentage of the messages in the file. Depending on how you have

configured message sampling, the feature then sets the migration status of files whose owners have been identified to **Ready to copy**.

See "Results of message sampling" on page 24.

You can use the **PST Ownership Identification** tab of the Personal Store Management properties to configure the following:

- Use message sampling as the initial method to identify PST file owners.
- Allow Enterprise Vault to use this method only if PST file marking fails.
- Configure the following criteria:
  - Sample size percentage: The percentage of messages within the PST file that you want Enterprise Vault to sample to look for possible owners.
  - Ownership percentage: The percentage of associated messages within the sample size that decides ownership.
  - Change migration state percentage: The percentage of messages that are associated with the assigned owner that decides whether the state of the PST file changes to **Ready to copy**.

  For example, for a PST file that has a 100 messages, when you set the sample size to 80%, Enterprise Vault scans 80 random messages to look for a possible owner. If you set the ownership percentage to 70%, Enterprise Vault assigns ownership to the user that has 56 or more associated messages in the PST file. If you set the change migration state percentage to 80%, Enterprise Vault checks whether the identified owner has 64 associated messages, and then changes the PST migration state to **Ready to copy**.
- Specify a default archive to store the PST files that do not have identified owners.

The Locate and Migrate tool and the options to add single and multiple PST files in the **Personal Store Management** > **Files** node in the Administration Console use these settings to identify PST file owners.

The ownership identification workflow depends on how you have configured message sampling.

Table 3-1 details the owner identification workflow with respect to message sampling.

Table 3-1 Owner identification workflow

Message sampling	Locate and Migrate	Add single or multiple PST files
Disabled	Enterprise Vault tries to identify the owner using the following methods in the listed order: ■ PST file marking ■ PST file permissions	Enterprise Vault tries to identify the owner using the following methods in the listed order: ■ PST file marking ■ PST file permissions ■ Directory permissions on the folder
Only if PST file marking fails or the files are unmarked	Enterprise Vault tries to identify the owner using the following methods in the listed order: ■ PST file marking ■ PST file permissions ■ Message sampling	Enterprise Vault tries to identify the owner using the following methods in the listed order: ■ PST file marking ■ PST file permissions ■ Directory permissions on the folder ■ Message sampling
Use message sampling first	Enterprise Vault tries to identify the owner using the following methods in the listed order: ■ Message sampling ■ PST file marking ■ PST file permissions	Enterprise Vault tries to identify the owner using the following methods in the listed order: ■ Message sampling ■ PST file marking ■ PST file permissions ■ Directory permissions on the folder

To optimize performance, make sure that you turn off message sampling and run the PST Locator task to look for PST files. After the PST Locator task completes, turn message sampling on and run the task again to identify possible owners.

Caution: The performance of message sampling depends on the number of items in the PST file.

Configuring message sampling to determine PST file ownership

You can use the Personal Store Management properties page to configure message sampling to determine the owners of PST files. Depending on how you configure

the message sampling settings Enterprise Vault changes the state of the PST file to **Ready to copy**, or stores the PST file in a default archive.

To optimize performance, make sure that you turn off message sampling and run the PST Locator task to look for PST files. After the PST Locator task completes, turn message sampling on and run the task again to identify possible owners.

Caution: The performance of message sampling depends on the number of items in the PST file.

To use message sampling to determine ownership of PST files

1. In the left pane of the Administration Console, expand the hierarchy until you see the **Personal Store Management** node.
2. Right-click **Personal Store Management**. Then click **Properties**. The Personal Store Management properties are displayed.
3. Click the **PST Ownership Identification** tab.
4. Click **Use message sampling** and do one of the following:
   - Select **Only if PST file marking fails, or the files are unmarked**. In this case, Enterprise Vault uses message sampling only if it finds unmarked PST files.
   - Select **Use message sampling first**. In this case, Enterprise Vault uses message sampling to look for possible owners.
5. In **PST file sample size**, specify the percentage of messages in the PST file you want Enterprise Vault to scan to look for possible owners.
6. Select **Assign ownership to users with this percentage of associated messages** and specify the percentage of messages that are associated with a certain user within the sample size to assign ownership. You can specify a value in the range 1% through 100%. We recommend that you specify a value between 51% and 100%.
7. In the **When no owner is identified** section, do one of the following:
   - Select **Leave as unassigned**. In this case, PST files for which no owner is found remain in the **Not ready** state.
   - Select **Assign to archive** and browse to select a default archive to store the PST files that have no owners identified. For such files, the state changes to **Do not migrate**.
8. Click the **Advanced** tab.

9 Click **Change migration state percentage**, and then click **Modify**. Enter a value between 80 - 100.

10 Click Message type exclude list, and then click **Modify**. Enter the message classes you want Enterprise Vault to ignore when it scans the sample size for possible owners.

11 Click **Apply**, and then click **OK** to save the settings.

Results of message sampling

Depending on how you have configured message sampling, you can get any of the following results.

Table 3-2 details the behavior of Enterprise Vault with respect to message sampling.

Table 3-2 Results of message sampling

Message sampling	Resulting action	PST migration status
Message sampling successfully identifies the owner.	Enterprise Vault matches the email address or display name with the available Exchange mailbox user, and assigns the archive of that user to the PST file so that items are migrated to that archive.	The PST file state changes to **Do not migrate**. If the percentage of associated messages matches the configured criteria for the change of migration state, the PST file state changes to **Ready to copy**.
Message sampling has identified a probable owner, but the number of associated messages does not meet the configured ownership criteria.	-	The PST file remains in the **Not Ready** state. If you have specified a default archive to store PST files that have no owners identified, the PST file is assigned to the default archive and the state changes to **Do not migrate**. If the PST file is in the **Not Ready** state, you can manually assign the correct archive and change the state.

Table 3-2 Results of message sampling *(continued)*

Message sampling	Resulting action	PST migration status
Message sampling has identified multiple possible owners. For example, the PST file has 2 owners with 50% associated messages each or 3 owners with 33.3% associated messages each.	Enterprise Vault displays this information in the **More details** section in the properties page of the PST file.	The PST file remains in the **Not Ready** state. If you have specified a default archive to store PST files that have no owners identified, the PST file is assigned to the default archive and the state changes to **Do not migrate**. If the PST file is in the **Not Ready** state, you can manually assign the correct archive and change the state.
Message sampling has identified the owner, but the associated archive is not found. This may happen in case the PST file is from outside the network or the user's mailbox is not enabled for archiving.	Enterprise Vault displays this information in the **More details** section in the properties page of the PST file.	The PST file remains in the **Not Ready** state. If you have specified a default archive to store PST files that have no owners identified, the PST file is assigned to the default archive and the state changes to **Do not migrate**. If the PST file is in the **Not Ready** state, you can manually assign the correct archive and change the state.

Chapter 4

PST migration: scripted

This chapter includes the following topics:

- Overview of the scripting mechanism for PST migration
- Undertaking the PST migration process using Policy Manager
- Preparation for PST scripted migration
- Output from PST migration
- Example initialization file for PST scripted migration

Overview of the scripting mechanism for PST migration

You can perform scripted migrations of the contents of PST files to Enterprise Vault using Policy Manager. For detailed information on Policy Manager, see the *Utilities* guide.

The scripting mechanism enables you to configure how each PST file is processed.

For example, for each PST file you can do the following:

- Specify the destination archive.
- Specify whether to create shortcuts to migrated items and, if so, whether to leave them in the PST file or to put them in a specific folder in the user's mailbox.
- Specify which retention category to use for migrated items.
- Control what happens to the PST file itself after the items in it have been migrated.

You write the Policy Manager initialization file, in which you list each of the files whose contents you want to migrate to Enterprise Vault. You can set up default

settings that apply to all PST files and you can override the default settings for individual PST files.

It is possible for you to make Enterprise Vault clients save details of the owner's default archive in each PST file (PST marking). Policy Manager can then use this information to determine the correct archive and mailbox to use for each PST file. If you prefer to not to use this mechanism, or to override it for some PST files, then for individual PST files you can override these values.

When you migrate PSTs using Policy Manager you can use report mode to check all the PST files listed in your initialization file. This mode generates a new copy of the initialization file, with lines that identify any problems. Entries for PST files that cannot be processed are marked so that PST migrator ignores these files.

You can then do either of the following:

- Fix any problems and run the Policy Manager in report mode again to see whether there are any more problems. When the file is error free, you can run it in process mode to process all the files. You can run in report mode as many times as needed. Each time, Policy Manager creates a new initialization file that you can then run normally or use to fix problems.
- Run in process mode immediately. Files that could cause problems have been marked so that Policy Manager ignores them. You can then decide later what to do with these problem files.

Note the following:

- Policy Manager uses only message class and shortcut content settings from the Exchange PST Migration policy. The rest of the settings in the policy are ignored.
- Policy Manager can use the information written into the PST file by PST marking to identify the mailbox and archive associated with the PST file.
- Veritas recommend that you do not use Policy Manager to perform other tasks at the same time as performing PST migrations.
- If you have only a few PST files to migrate, you may find it easier to use the wizard-assisted PST migration tool instead.
  See “About the PST Migrator wizard” on page 35.

Undertaking the PST migration process using Policy Manager

In outline, you perform scripted migrations with Policy Manager as follows.

To undertake the migration process using Policy Manager

1. Decide whether to use markers within PST files to determine their ownership. By default, PST files are marked. You can turn off PST file marking in Exchange Desktop policies using the setting, **Mark PST files**, in the list of advanced Outlook settings.

   See " PST file marking to determine PST file ownership" on page 20.

2. Write the Policy Manager initialization file to specify which PST files you want to migrate to Enterprise Vault. In the file, specify that Policy Manager is to run in report mode. Remember to save the initialization file in Unicode format.

3. Run Policy Manager in report mode with the initialization file.

   Policy Manager does the following:

   - Checks that all the PST files listed are accessible.
   - Creates a new initialization file that shows any problems with the listed PST files, such as files that could not be accessed or are password-protected. The new initialization file has the same name as the original, with a number added to make it unique. For example, if the original script was called `PSTMigration.ini` then the new script would be called `PSTMigration_1.ini`.
   - Creates a log file with the same name as the original initialization file and a file type of `.log`. For example, if the original script was called `PSTMigration.ini` then the log would be called `PSTMigration.log`.

4. You can fix problems that are listed in the new initialization file, or you can leave them for later.

5. Run Policy Manager with the new initialization file. Policy Manager migrates the file contents and writes a log file with the same name as the initialization file and a file type of `.log`.

   If any PST files fail the migration process, Policy Manager automatically writes a new script that you can run to process just those failed files.

   If necessary, fix any problems and then run the new script to migrate the contents of just those PST files that were not processed before.

Preparation for PST scripted migration

- Policy Manager only uses a limited number of settings in Exchange PST Migration policies. Enterprise Vault archives items from the PST files according to the following settings in your Enterprise Vault installation:

  - Enterprise Vault archives only the classes of items that are defined as eligible for archiving on the **Message Classes** tab in Exchange PST Migration properties.
  - The migration obeys the registry settings that are set for the Storage service.
  - If you have configured customized shortcuts on the **Shortcut Content** tab of the Exchange PST Migration policy, then the PST Migrator uses these settings. Otherwise the shortcut content settings that are configured in the Exchange Mailbox policy are used.
- Items can be assigned a specific retention category during PST migration.

  Note: Some Enterprise Vault features, such as the retention folders and classification features, can override the specified retention category. For more information on retention, see the *Administrator's Guide*.

- The PST files must not be in use at the time of migration, so make sure that users do not have them open. You may find that it is better to move the PST files.
- The best procedure may be to gather all the PST files into the same place and then to migrate them from there. This makes it easier to generate the initialization file, assign permissions, and to manage files. Note though, that you may have some file name conflicts if there are PST files with the same name. Also, if any PST files are likely to be unmarked ensure that you know the owners because there may be no identifying information in the PST.
- The Vault Service account must have Full Control access to the PST file.
- The Storage service for the destination vault store must be running.
- PST files that are password-protected cannot be processed. You must remove such protection before migrating their contents.
  Alternatively, you may allow Enterprise Vault to override PST passwords during PST migration. To override passwords, enable **Override passwords for password-protected PST files** in the **General** tab of the **Personal Store Management** properties.
- If you intend to use the automatic PST compaction feature at the end of migrations, you may need some spare disk capacity for the compaction to take place. You can need as much as the size of the largest PST file, plus approximately 5% of its size. You may choose to ignore compaction if you plan to delete the PST files after migration.
- Policy Manager migration checks the mailbox storage limit when a mailbox has either Prohibit Send or Prohibit Send & Receive mailbox limits set. If both these

limits are set, Policy Manager does not move any item to the mailbox that exceeds the lower limit. If only one of the limits is set, then Policy Manager obeys that limit.

Note that, even if the storage limit prevents items from being moved to the mailbox, the items are still archived in the appropriate archive. In this case you can increase the mailbox quota and then migrate the PST file again to move the items to the mailbox.

Output from PST migration

When you run Policy Manager with an initialization file containing a [PSTdefaults] section, Policy Manager automatically writes a new initialization file that contains details of any problems that it found.

The new initialization file has the following features:

- There is a [PSTcheckpoint] section at the top of the file, summarizing the results of the run.
- If you had been using process mode then the following apply:
  - All [PST] sections for files that were processed successfully are commented out.
  - There is a JobStatus entry in each [PST] section, indicating for that file, either success or the type of error that occurred.

[PSTcheckpoint] section PST scripted migration

The contents of the [PSTcheckpoint] section vary according to whether you run the initialization file in report mode or process mode.

Report mode [PSTcheckpoint] section

The following [PSTcheckpoint] section results from running an initialization file in report mode. The Generation count of 1 shows that these results are from the first run of the file:

```
[PSTCHECKPOINT]
GENERATION = 1
CREATED = 02Oct2008 10:58:02 AM
SOURCE = E:\EV\pstmigration\pstlist.ini
PSTPROCESSEDCOUNT = 118
PSTNOTREADYCOUNT = 3
PSTWARNINGCOUNT = 2
```

The following entries are of interest:

- `PSTPROCESSEDCOUNT = 118` shows that the file contains references to 118 PST files.
- `PSTNOTREADYCOUNT = 3` shows that there are three files with problems. The `Report_Error` entries in the individual [PST] sections give you more information. Policy Manager automatically adds `DONOTPROCESS = TRUE` to each of these [PST] sections.
- `PSTWARNINGCOUNT = 2` shows that there are two files with warnings. In this case, these are both marked PST files whose markings are intentionally being overridden. The Report_Error entries in the individual [PST] sections gives more information.

Because Policy Manager has added the `DONOTPROCESS = TRUE` entries to each of the problem PST files, you could run this new initialization file in process mode immediately, leaving the problem PSTs to be addressed later. Alternatively, you could fix the problems, remove the `DONOTPROCESS = TRUE` entries, and then run the file again in either report mode or process mode.

Process mode [PSTcheckpoint] section

The following [PSTcheckpoint] section results from running an initialization file in process mode. The Generation count of 2 shows that these results are from the second run of the file:

```
[PSTCHECKPOINT]
GENERATION = 2
CREATED = 02Oct2008 10:59:36 AM
SOURCE = E:\EV\pstmigration\pstlist.ini
PSTPROCESSEDCOUNT = 115
PSTFAILEDCOUNT = 0
PSTUNPROCESSEDCOUNT = 3
PSTINCOMPLETECOUNT = 0
PSTPARTIALCOUNT = 0
```

The following entries are of interest:

- PSTPROCESSEDCOUNT = 115 shows that 115 PST files were processed. This is the same initialization file as shown above in the Report mode description. The three problem files have been left with DONOTPROCESS = TRUE entries, so Policy Manager has ignored them.
- PSTFAILEDCOUNT = 0 shows that there were no files for which processing could not be tried.

- PSTUNPROCESSEDCOUNT = 3 shows that three files were ignored. These are the three files with DONOTPROCESS = TRUE entries.
- PSTINCOMPLETECOUNT = 0 shows that no PST files were processed only partially. Policy Manager's processing was not interrupted.
- PSTPARTIALCOUNT = 0 shows that there were no PST files with individual items that could not be processed. If there had been such items, Policy Manager would have placed them in the Migration Failed Items folder in the PST files.

Enterprise Vault event log for PST scripted migration

When you run in process mode, the Enterprise Vault event log also contains one entry for each PST file processed. The entries appear in the Enterprise Vault event log with a source of Migrator Server. For example, the following log entry is for a PST file that contained 560 items and resulted in 560 shortcuts being placed in the mailbox:

```
PST Migration Report
Migration status: Completed
PST file: E:\Vault Test files\TestPSTs\um1.pst
Vault Name: Chris Waterlander
Vault Id:
14F921A913AB6D511AC9F0008C711C6F01110000server2.acme.com
RetentionCategory: Business
Exchange Server\Mailbox:
EV\/o=ACME/ou=DEVELOPER/cn=Recipients/cn=ChrisW
Number of folders processed: 43
Number of items archived to vault: 560
Total size of items archived: 137876 KB
Number of items unable to be archived: 0
Number of items moved to mailbox: 560
Elapsed Migration Time: 0:0:6 (hours:minutes:seconds)
```

There is a summary log entry for each PST file that is migrated. The entry lists the number of items that have been archived and also the number of items that have been moved to the mailbox.

Some items may not be eligible for archiving or moving to the mailbox. This is the case if they have a message class that you have specifically excluded from being archived (using the **Message Classes** tab of the Exchange PST Migration policy in the Administration Console), or if they were created on a computer that uses a language incompatible with that of the Storage service computer. For example, if a PST file contains a mixture of Japanese and English items, and the Storage Service computer uses Japanese, the English items are not eligible for archiving.

Example initialization file for PST scripted migration

The initialization file must be saved as a Unicode file.

Table 4-1 shows a sample initialization file that sets up migrations for five PST files.

Table 4-1 Sample initialization file

Initialization file section	Notes
[Directory] directorycomputername = server2 sitename = server2	■ The directory section is mandatory and must appear at the top of the file. ■ This section contains the name of the Enterprise Vault directory computer and the site name.
[PSTDefaults] ServerComputerName = server2 PSTLanguage = Western European MailboxFolder = EVPM PST Migrations MigrationMode = Report ShortcutMode = NoShortcuts IncludeDeletedItems = false SetPstHidden = false SetPstReadOnly = false CompactPst = true DeletePst = false CancelMbxAutoArchive = false	■ These default options apply to all PST migrations listed in the following [PST] sections unless overridden in those sections. ■ PST Language is mandatory. ■ There must only one [PSTDefaults] section and it must appear before the individual [PST] sections. ■ `MigrationMode=Report` specifies that this initialization file is to run in report mode. ■ `ShortcutMode=NoShortcuts` means that, by default, there will be no shortcuts to the migrated items. Items that cannot be migrated will be left in the PST files, not moved to the mailboxes. You can override this behavior for individual PST files.
[PST] Filename = E:\Migration\Missing.pst	■ The [PST] sections must appear after the [PSTDefaults] section ■ As a minimum each section must specify the PST filename. ■ If an option is unspecified then Policy Manager uses the value in the [PstDefaults] section. ■ This marked file is missing and will produce an error when Policy Manager runs.

Table 4-1 Sample initialization file *(continued)*

Initialization file section	Notes
[PST] Filename = \\server3\temp\marked1.pst	■ This file is on a remote computer. ■ This PST file has been marked by the Enterprise Vault client so that Policy Manager can automatically determine the target archive, the Exchange Server mailbox, and the retention category.
[PST] Filename = E:\Migration\marked2.pst MailboxDN = /o=ACME/ou=DEVELOPER/cn=Recipients/cn=JackH ShortcutMode = MailboxShortcuts	■ This PST file has been marked by the Enterprise Vault client so that Policy Manager can automatically determine the target archive, the Exchange Server mailbox, and the retention category. ■ The MailboxDN setting is overriding the PST marking. This will result in a warning when the initialization file is processed. The file will be processed correctly, using the specified enabled mailbox and that mailbox's default retention category and archive. ■ Policy Manager will create shortcuts to archived items and place them, together with any items that remain in the PST at the end of the migration, into the mailbox.
[PST] Filename = E:\Migration\marked3.pst ArchiveName = Jack Henry2	■ This PST file has been marked by the Enterprise Vault client. ■ The ArchiveName setting is overriding the owner entry that the client made. This will result in a warning when the initialization file is processed. The PST file will be processed correctly, using the specified archive and the default retention category from the owning mailbox.
[PST] ArchiveName = SharedArchive1 Filename = E:\Migration\unmarked.pst RetentionCategory = Business	■ This file has not been marked by an Enterprise Vault client. ■ You must specify the ArchiveName, PST filename, and RetentionCategory.

Chapter 5

PST migration: wizard-assisted

This chapter includes the following topics:

- About the PST Migrator wizard
- Outline of the wizard-assisted PST migration process
- Preparation for the wizard-assisted PST migration process
- Migration tips for the wizard-assisted PST migration process
- How the wizard-assisted PST migration process affects users
- Starting the wizard-assisted PST migration process

About the PST Migrator wizard

PST Migrator is a wizard that lets you store the contents of PST files in Enterprise Vault.

The main features of the wizard are as follows:

- You can migrate several PST files at the same time.
- You can either match PSTs to archives manually, or allow PST Migrator to do an automatic correlation based on the permissions set on the PST files. The automatic correlation can save you a lot of time, but it is important that you understand the process and make suitable preparations.
- PST Migrator processes PST files that are on a mapped network drive or in a shared network folder. You cannot use it to search across users' disks, migrating all the PST files that it finds.

- PST Migrator archives only those types of items for which you have enabled archiving. To view or modify the types of items that are archived, start the Administration Console and go to the **Message Classes** tab of the Exchange PST Migration policy properties.
- If you have configured customized shortcuts in the Exchange PST Migration policy, then the PST Migrator uses these settings. Otherwise the shortcut content settings configured in the Exchange Mailbox policy are used.
- You specify the required archiving settings as you work through the wizard.

PST migrator does not use any other settings from the Exchange PST Migration policy.

It is impossible to specify a migration process that suits everybody. For example, you may want to delete PST files after migrating them or you may want to continue using them. PST Migrator provides great flexibility, but you must think carefully about how you want to carry out the migration.

Outline of the wizard-assisted PST migration process

In outline, you perform wizard-assisted PST migrations as follows.

To undertake the migration process

1. Decide whether to use markers within PST files to determine their ownership. By default, PST files are marked. You can turn off PST file marking in Exchange Desktop policies using the setting, **Mark PST files**, in the list of advanced Outlook settings.

   See " PST file marking to determine PST file ownership" on page 20.

2. Decide on the retention categories to assign to the items in the PST files. If you want to assign retention categories that have a fixed expiry date rather than a specified retention period, ensure that they exist before you run the wizard below. The wizard lets you create retention categories that have a retention period, but it does not let you create those that have a fixed expiry date.
3. In the Administration Console, right-click the **Archives** container and, on the shortcut menu, click **Import PST**. The PST Migration wizard starts.
4. Select a vault store to use. You cannot select a vault store that is in backup mode.

5. Add to the list the PST files that you want to migrate to Enterprise Vault. You can select PST files from multiple mapped drives or network drives, but note that the Enterprise Vault Storage service must be able to access them.
6. Select how to match PST files with destination archives. You can choose either automatic correlation, or manual.
7. Specify the default retention category to use for items from PST files that do not have marking information, or if you have chosen not to use marking information.

   Note: Some Enterprise Vault features, such as the retention folders and classification features, can override the specified retention category. For more information on retention, see the *Administrator's Guide*.

8. Each PST file is listed together with the associated mailbox and destination archive, if known. It is important that you check the list of matches before beginning the migration. You can select or change the destination archive for a PST file, or remove PST files from the list, if necessary.
9. Each PST file is listed together with the retention category that will be applied to the items when they are archived. If required, you can change the retention category for individual PST files. You can choose an existing retention category or create a new one.

   Note again that some Enterprise Vault features, such as the retention folders and classification features, can override the specified retention category.
10. Specify whether PST Migrator is to create shortcuts for the items it archives.

    You can configure PST Migrator to do either of the following:

    - Archive the items and delete the original items from the PST without creating shortcuts.
    - Create shortcuts in the PST files and delete the original items after they have been archived. You might select this if users will still have access to the PST files at the end of the migration. The users must move the shortcuts to their mailboxes before they will work.
    - Create shortcuts in the associated mailboxes and delete the original items from the PST files after they have been archived.
11. Specify the required folder structure that the PST Migrator is to create in the mailbox for shortcuts to migrated items. You can specify a mailbox folder that is to correspond with the root folder in the PST file. Where there are several PST files to migrate, you can choose to merge the folder structures or keep them separate.

12 Select the language of the PST files to be migrated.

13 Specify whether PST Migrator is to migrate the **Deleted Items** folder in the PST files, or leave it in the PST file.

If calendar items are to be archived, specify whether PST Migrator is to migrate unexpired calendar items.

14 Specify what to do with each PST file after it has been processed. You can select the following:

- Leave the file as it is.
- Delete the file.

Note: Make sure that the PST files are backed up before you start the migration process.

- Compact the file to free up disk space.
- Set permission on the file to read-only to prevent users adding items to the file.
- Hide the file. If you are not migrating all the PST files at the same time, this can help you to see how many PST files are left to migrate. The next time you run PST Migrator the hidden PST files will not be visible, provided that you have set your desktop so that it does not show hidden files.

15 Specify whether PST Migrator is to create a report file for the migration. Report files are created in the `Reports` subfolder of the Enterprise Vault installation folder.

16 Start the migration.

During the migration, the PST Migrator writes two events to the Enterprise Vault event log for each PST file, one when it starts processing the file, and another when it has finished.

If an item cannot be migrated, it is moved to a folder called PST Migration Failed Items in the PST file.

Preparation for the wizard-assisted PST migration process

- The PST files must not be in use at the time of migration, so make sure that users do not have them open. You may choose to copy PST files so that users can continue using the original files while you migrate the contents of the copies.

- The Vault Service account must have Full Control access to the PST file. If you plan to perform PST migration using a different account, then both the account and the Vault Service account must have Full Control access to the PST file.
- The Storage service for the destination vault store must be running.
- PST Migrator's automatic correlation rejects any PST file that has more than one user account with write permission, leaving you to do the correlation manually. You may find it easier to set the permissions appropriately before running PST Migrator.
- PST Migrator does not migrate the PST files that are password-protected. You must remove such protection before running PST Migrator.
  Alternatively, you may allow Enterprise Vault to override PST passwords during PST migration. To override passwords, enable **Override passwords for password-protected PST files** in the **General** tab of the **Personal Store Management** properties.
- Items can be assigned a specific retention category during PST migration.
- If PST files are scattered in different locations on users' disks, you may find it easier to move them all to a central location before you run PST Migrator.
- If you have PST files that must be migrated to different vault stores, the quickest way to sort them is to use the automatic correlation within PST Migrator and remove those that do not correlate.
  See "Migration tips for the wizard-assisted PST migration process" on page 39.
- If you intend to use the automatic PST compaction feature at the end of migrations, you may need some spare disk capacity to provide room for the compaction to take place. You can need as much as the size of the largest PST file, plus approximately 5% of its size.
- PST Migrator checks the mailbox storage limit when a mailbox has either Prohibit Send or Prohibit Send & Receive mailbox limits set. If both these limits are set, PST Migrator does not migrate the items that exceed the lower limit. If only one of the limits is set, then PST Migrator obeys that limit.
  If a PST file fails migration because the mailbox is full, you can modify the appropriate mailbox storage limit and then migrate the PST file again.

Migration tips for the wizard-assisted PST migration process

- Migrate a few PST files and then, when you are familiar with the process, increase the numbers.

- Migration is much easier if you have PST files in just a few locations, rather than in many.
- Sort out the permissions on the PST files before running PST Migrator, otherwise they will just fail.
- There is a Windows server command-line utility, CACLS, which you can use to grant the Vault Service account Full Control access to the PST files.
- You can run more than one instance of PST Migrator. There is no point in running more instances than you have processors. For example, if you have two processors, then do not run more than two instances of PST Migrator. If the computer is also archiving at the same time, then reduce the number of PST Migrator instances.
- When Enterprise Vault archives items, it also converts the contents to HTML and indexes them. There is a default conversion timeout of 10 minutes for this process. Enterprise Vault makes three attempts to convert an item, so can take up to 30 minutes before failing an item and moving on to the next one.
  If there are very large, or very complex, items in a PST file, it can take a long time to migrate them all. If you do not need the content of the items to be indexed, then you can improve performance by lowering the conversion timeout to just a few minutes.
  This change to the conversion timeout also affects normal archiving, so remember to return it to the original value when you have migrated the PST files.

  To change the conversion timeout, perform the following steps in the order listed:

  - On the Storage service computer, set the following string registry value to the timeout, in minutes, that you want to use:

    ```
    HKEY_LOCAL_MACHINE
     \Software
      \Wow6432Node
       \KVS
        \Enterprise Vault
         \ConversionTimeout
    ```

  - Restart the Storage service.
- If you have PST files in the same location that you want to go to different vault stores, the quickest way to do this is as follows:
  - Run PST Migrator and select the first archive store that you want to use.
  - Select all the PST files, including those that should go to other vault stores.

- Select automatic correlation. PST Migrator will open the vault store and match PST files to archives within that vault store. All other PST files will not be matched.
- Click the **Archive** heading on the screen to sort by destination archive. This puts at the top of the list all the PSTs that could not be matched to archives.
- Drag-select all the PSTs that could not be matched to archives and then click **Remove**.
- On the PST Migrator screen that asks **What do you want to do with PSTs after all items are successfully migrated from each?**, select **Hide them**.
- At the end of the migration, PST Migrator hides the PST files that were migrated. The next time you run PST Migrator, these PST files will not appear in the list of PST files available for migration. The files appear hidden only if you have set your desktop so that it does not show hidden files.
- Repeat the process, running PST Migrator again, this time choosing a different vault store.
- When you have worked through all the vault stores, you may have some PST files left that failed to migrate. Run PST Migrator again and manually select the correct archive for each PST

- If you run PST Migrator on a computer that is not running the Storage service for the vault store, then you cannot choose PSTs on a local disk. However, you can choose PSTs from a mapped network drive or a shared network folder.

How the wizard-assisted PST migration process affects users

- You can migrate the contents of PST files, choosing to create shortcuts to migrated items, as follows:
  - If you create shortcuts in mailboxes, then PST Migrator duplicates the folder structure of the PST files under a new, top-level folder in the mailboxes.
  - If you create shortcuts in PST files to which users still have access, then the users must move the shortcuts to their mailboxes before the shortcuts will work.
- If users store new items in a PST file that has been migrated, you can run the migration again at any time, again creating shortcuts to migrated items. PST Migrator will migrate the new items.
- You can delete PST files at the end of the migration. If you do this then, obviously, the files are no longer available to users.

- If a user has configured Outlook to deliver new mail to a PST file rather than to the mailbox, there will be errors when Outlook next starts, as follows:
  - If the PST file no longer exists, there is an error as soon as Outlook starts and the user is then given the option to create a new PST file.
  - If the PST file still exists but is read-only, then there will be an error as soon as the user tries to access the PST or tries to create a mail message.

  The best solution is for users to make sure, before you perform the migration, that mail is not being delivered to PST files.

Starting the wizard-assisted PST migration process

When you have completed the preparatory steps, you are ready to start the PST migration.

To start the migration

1. In the left-hand pane of the Administration Console, expand the view until **Archives** is visible.
2. Right-click **Archives** and, on the shortcut menu, click **Import PST**. The PST Migration wizard starts.
3. Work through the wizard.

Chapter 6

PST migration: Locate and Migrate

This chapter includes the following topics:

- About Locate and Migrate
- Setting up PST Locate and Migrate
- Migrating PST files using PST Locate and Migrate
- Excluding network shares from PST migration using the PstLocatorTask.exe.config file
- Troubleshooting PST migration

About Locate and Migrate

Locate and Migrate partially automates the process of migrating the contents of PST files into Enterprise Vault. It can automatically search for PST files on users' computers and move them to a central holding area, from which they can be automatically migrated.

Depending on the configuration options that you select, there may be some manual intervention that is required to approve migration of PST files. Additionally, you may need to supply the passwords for password-protected PST files.

For password-protected PST files you may allow Enterprise Vault to override the passwords during PST migration. This setting is useful in cases the password is missing or is incorrectly provided. To override passwords, enable **Override passwords for password-protected PST files** in the **General** tab of the **Personal Store Management** properties.

Locate and Migrate comprises several Enterprise Vault task types:

- A PST Locator task. This task searches your network for computers and PST files. You can configure specific paths to include or exclude during PST searching. There can be only one PST Locator task in your Enterprise Vault site.
- A PST Collector task. This task moves the PST files that the PST Locator task has found to a central PST holding folder, ready for them to be migrated. This task uses the migration priority of the file when it collects files. There can be many PST Collector tasks in your Enterprise Vault site.
- A PST Migrator task. This task migrates the contents of PST files that are in the PST holding folder to Enterprise Vault archives. This task uses the migration priority of the file when it migrates files. There can be many PST Migrator tasks in your Enterprise Vault site.

Setting up PST Locate and Migrate

Table 6-1 outlines the preparations that you need to make to set up PST Locate and Migrate.

Table 6-1 Steps to configure PST Locate and Migrate

Step	Action	Description
Step 1	Decide whether to use PST marking.	See " PST file marking to determine PST file ownership" on page 20.
Step 2	Decide whether you want to use accounts other than the Vault Service account to manage PST migration objects in the Administration Console.	See "Administrator roles required to manage PST Locate and Migrate" on page 44.
Step 3	Create or edit Exchange PST Migration policies.	See "About the Exchange PST Migration policy" on page 13.
Step 4	Configure the network share that is to be used as the central PST holding folder.	See "Configuring the holding folder for PST Locate and Migrate" on page 45.
Step 5	Create and configure PST Locator, PST Collector, and PST Migrator tasks.	See "Creating and configuring the PST Locator, PST Collector, and PST Migrator tasks" on page 47.

Administrator roles required to manage PST Locate and Migrate

If you want an account other than the Vault Service account to manage PST migration objects in the Administration Console, the account must have either the

PST Administrator role or the Power Administrator role. The Vault Service account has access to all objects and functions in the Administration Console.

The accounts under which the PST Locator, PST Collector, and PST Migrator tasks run must have appropriate access to the computers to be searched, and the PST files to be processed. The PST Migrator task requires access to the computers and original PST files for post-migration operations.

All the tasks also need appropriate access to the PST holding folder.

See "Configuring the holding folder for PST Locate and Migrate" on page 45.

The PST Migrator task account must have full access to its temporary files folder.

See "How to configure the PST Migrator task" on page 51.

Depending on the type of search that has been configured for the PST Locator task, the account must either be able to scan remotely the registry on each computer or have access to the drives on each computer.

To ensure that the tasks have adequate access to all the computers in the domain, you can run the tasks under the accounts that are members of the domain administrators' group. Use the settings on the **Log On** page of the task properties to specify the account.

For details of the permissions that the account needs, see the online Help for the **Log On** page. In addition, the account must have either the PST Administrator role or the Power Administrator role.

Note: It is not advisable to add the Vault Service account to the domain administrators' group.

Configuring the holding folder for PST Locate and Migrate

You configure the PST holding folder in Enterprise Vault site properties. The folder that you select must be a network share. The accounts that are used to configure the folder, or run the PST Locator, PST Collector, and PST Migrator tasks on all Enterprise Vault servers in the site must have access to the PST holding folder. The access permission that is required is shown in Table 6-2.

Table 6-2 Access required to the PST holding folder

Account	Access required
Account used to configure the PST holding folder	Read. Access can be removed after configuration, if required.

Table 6-2 Access required to the PST holding folder *(continued)*

Account	Access required
Logon account that the PST Locator task uses	Delete.
Logon account that the PST Collector task uses	Delete.
Logon account that the PST Migrator task uses	Delete.

To configure the holding folder for PST Locate and Migrate

1. In the left pane of the Administration Console, display the Enterprise Vault Site Properties.
2. On the **General** tab, click **Browse** next to **PST holding folder**.

   A prompt asks whether you want to browse Regular or Hidden shares.
3. Select the type of share that you intend to specify for the PST holding folder, and then click **OK**.
4. In the **Browse for Folder** dialog box, expand **Entire Network** > **Microsoft Windows Network**. Expand the required domain and then the server on which the share is located. The list of shares that are displayed contains shared folders to which the account has access.
5. Select the folder that you want to use for the PST holding folder and then click **OK**.
6. Click **OK** to close Site Properties.

Determining the size of the holding folder for PST Locate and Migrate

In Enterprise Vault site properties you can specify a maximum size in gigabytes for the PST holding folder. The size that is specified applies to each PST Collector task. For example, if you specify the maximum folder size as 5 GB, and there are two PST Collector tasks configured, then the total maximum size of the PST holding folder is 10 GB.

The PST Migrator task should empty the PST holding folder during its scheduled daily run. If PST files remain in the PST holding folder, they are not migrated until the next scheduled run starts. As PST files are set to read-only during migration, users cannot access these PST files for an extended period.

You can use one of the following techniques to ensure that the PST Migrator task empties the PST holding folder:

- Set a suitable maximum size for the PST holding folder that ensures the PST Migrator task can empty the folder during its scheduled daily run.
- Set a small maximum size for the PST holding folder, and then schedule the PST Collector task so that it keeps the folder full. Set the schedule for the PST Collector task so that it ends before the end of the PST Migrator task schedule. This approach ensures that the PST Migrator task has time to empty the folder during its scheduled run.
- When the PST Migrator task runs, it generates a report file. You can use the information in this report to determine the average number of PST files that the task can migrate during its scheduled run. In the properties of the PST Collector task, you can then specify the maximum number of PST files to store in the PST holding folder.

Creating and configuring the PST Locator, PST Collector, and PST Migrator tasks

To use the PST Locate and Migrate tool, you create and configure the following tasks:

- PST Locator task. This task searches your network for domains, computers, and PST files. You can configure specific paths to include or exclude during PST searching. There can be only one PST Locator task in each Enterprise Vault site. The PST Locator task is not required for client-driven PST migration.
- PST Collector task. This task moves the PST files that the PST Locator task has found to a central PST holding folder, ready for them to be migrated. This task uses the migration priority of the file when it collects files. There can be many PST Collector tasks in each Enterprise Vault site, but only one PST Collector task per Enterprise Vault server. You need to configure a PST Collector task on each Enterprise Vault server that hosts archives to which you intend to migrate PST files. The PST Collector task is not required for client-driven PST migration.
- PST Migrator task. This task migrates the contents of PST files that are in the PST holding folder to Enterprise Vault archives. This task uses the migration priority of the file when it migrates files. There can be many PST Migrator tasks in your Enterprise Vault site. You need to configure a PST Migrator task on each Enterprise Vault server that hosts archives to which you intend to migrate PST files.

The Locate and Migrate tasks run according to schedules that you define. However, there is also the Run Now option for each task so that you can run it immediately, if required.

To create a PST Locator task

1. In the Administration Console, expand your site until the **Enterprise Vault Servers** container is visible.
2. Expand **Enterprise Vault Servers** and then expand the server on which you want to add the PST Locator task.
3. Right-click **Tasks** and then, on the shortcut menu, click **New > PST Locator task**.

   The New PST Locator task wizard starts.
4. Work through the wizard to create the task.

To create a PST Collector task

1. In the Administration Console, expand your site until the **Enterprise Vault Servers** container is visible.
2. Expand **Enterprise Vault Servers** and then expand the server on which you want to add the PST Collector task.
3. Right-click **Tasks** and then, on the shortcut menu, click **New > PST Collector task**.

   The New PST Collector task wizard starts.
4. Work through the wizard.

To create a PST Migrator task

1. In the Administration Console, expand your site until the **Enterprise Vault Servers** container is visible.
2. Expand **Enterprise Vault Servers** and then expand the server on which you want to add the PST Migrator task.

3 Right-click **Tasks** and then, on the shortcut menu, click **New > PST Migrator task**.

The New PST Migrator task wizard starts.

4 Work through the wizard.

You need to supply the location of a folder that the task can use to hold temporary copies of the PST files during migration. This folder must be on a local drive. The account under which the PST Migrator task runs must have full access to the folder.

Note: Do not change the location of this folder while the PST Migrator task runs, or while Locate and Migrate processes PST files.

After you have created a PST Locator, PST Collector, or PST Migrator task, you can configure each task using the task properties. Double-click the task to display the task properties.

How to configure the PST Locator task

The PST Locator task properties include the following pages:

- **General**. Properties on this page let you configure how often the task should retry a failed operation, and the number of report files to keep.
- **Settings**. On this page you configure how the task is to search for domains, computers, and PST files.
  - Select whether the task is to use NetBIOS or Active Directory to find the domains and computers on which PST files reside.
  - You can configure the task to search computers for PST files using a registry or hard disk search. A registry search uses remote registry calls to search the Outlook profile for PST files. If a PST file is found in a profile, the Exchange mailbox in the profile is noted. If an Exchange mailbox is found, the task tries to determine the archive and the site that is associated with the primary mailbox referenced in the profile.

    A hard disk search scans all the local hard disks on the designated computer for files with an extension of `.pst`. It does not search the PST holding folder or the temporary migration folder on any computer running a PST Migrator task. On all computers, the Recycle Bin is not searched.

    As there can be very large numbers of PST files on computer hard disks, it is advisable to perform registry searches initially.

Note: On computers running Windows 7, you must enable the RemoteRegistry service to allow the PST Locator task to look for PST files using registry searches.

  - With the default settings, the task does not automatically search any computers for PST files; you need to select the computers to search. If you select the setting **By default search for PSTs on each computer**, the task automatically starts searching every computer it finds. As this process can take a very long time on a large network, use this setting with caution.

- **Search Paths**. Here you can specify the paths that you want the PST Locator to look in or ignore when looking for PST files.
- **Domains**. Domains that the task finds are listed on this page. Only the domains that are selected on this page are searched for computers and PST files.
- **Schedule**. It is advisable to schedule the PST Locator task to run during normal office hours, so that it finds the maximum possible number of computers and PST files when users' computers are switched on and connected to the internal network. If the site schedule is set to run tasks during non-office hours, you may want to override the site settings by specifying the schedule for this task.
- **Log On**. The account under which the PST Locator task runs must have appropriate access to the computers that it is to search for PST files. Depending on the type of search that is configured for the task, the account must either be able to scan remotely the registry on each computer or have access to the drives on each computer.

  To ensure that the task has adequate access to all the computers in the domain, you can run the task under an account that is a member of the domain administrators' group. Use the settings on the **Log On** page of the task properties to specify the account.

  See "Administrator roles required to manage PST Locate and Migrate" on page 44.

How to configure the PST Collector task

The PST Collector task properties include the following pages:

- **General**. Properties on this page let you configure how often the task should retry a failed operation, and the number of report files to keep.
- **Settings**. On this page you can configure what happens to the PST files after the task has copied them to the PST holding folder.
  - You can set the maximum number of PST files that this task is allowed to copy to the PST holding folder. This approach is one way of ensuring that

the PST Migrator task empties the PST holding folder during its daily scheduled run.
See "Determining the size of the holding folder for PST Locate and Migrate" on page 46.

- If you intend to back up the PST files before migrating them, select **Wait for PSTs to be backed up before migrating them** and then select the appropriate option, as follows:
  - **The migration status has changed to 'Ready to migrate'**. Select this option to make the PST Migrator task wait until PST files have a migration status of **Ready to migrate**. If you choose this option, you must set this status manually on each PST file.
  - **The file attribute 'Ready for archiving' has been reset**. Select this option to make the PST Migrator task wait until PST files have the Ready For Archiving attribute reset. Backup applications typically perform this action.

- **Schedule**. It is advisable to schedule the PST Collector task to run during normal office hours, so that it can access as many computers and PST files as possible when users' computers are switched on and connected to the internal network. If the site schedule is set to run tasks during non-office hours, you may want to override the site settings by specifying the schedule for this task.
- **Log On**. The account under which the PST Collector task runs must have appropriate access to the computers and PST files to be migrated. To ensure that the task has adequate access to all the computers in the domain, you can run the task under an account that is a member of the domain administrators' group. Use the settings on the **Log On** page of the task properties to specify the account.
  See "Administrator roles required to manage PST Locate and Migrate" on page 44.

How to configure the PST Migrator task

The PST Migrator task properties include the following pages:

- **General**. Properties on this page let you configure how often the task should retry a failed operation, and the number of report files to keep.
- **Settings**. This page contains the following configuration settings:
  - The location on a local drive of the temporary files folder that the PST Migrator task uses during the migration process. You specify the location of this folder when you create the PST Migrator task.
    If you have configured building blocks, you must create a temporary files folder with the same folder path on all the Enterprise Vault servers in your

building blocks environment. If the PST Migrator task fails over to a different server, it continues to use the same local path for the temporary files folder.

- The maximum number of PST files to migrate concurrently. Depending on your system configuration and workload, you may find that changing this number improves performance.

- **Schedule**. It is advisable to schedule the PST Migrator task to run during normal office hours, so that it can access as many computers and PST files as possible when users' computers are switched on and connected to the internal network. Access to the computers and original PST files is required for post-migration operations, such as unlocking the PST files, creating shortcuts or deleting the PST files. If the site schedule is set to run tasks during non-office hours, you may want to override the site settings by specifying the schedule for this task.
- **Log On**. The account under which the PST Migrator task runs must have appropriate access to the PST holding folder, temporary files folder, and computers and PST files to be migrated. Access to the computers and original PST files is required for post-migration operations. To ensure that the task has adequate access to all the computers in the domain, you can run the task under an account that is a member of the domain administrators' group. Use the settings on the **Log On** page of the task properties to specify the account.
  See "Administrator roles required to manage PST Locate and Migrate" on page 44.

Migrating PST files using PST Locate and Migrate

This section outlines how to use PST Locate and Migrate to search for PST files on users' computers and migrate the files to Enterprise Vault archives. The following sections describe the steps in more detail.

You can schedule and run the tasks in different ways depending on your workload, the time available, the number of PST files, and so on. This section assumes that you are interested in testing PST Locate and Migrate with relatively small numbers of PST files, possibly before starting a large-scale migration

Each time a task runs, it creates a report and places it in the `Reports` subfolder of the Enterprise Vault installation folder (for example, `C:\Program Files (x86)\Enterprise Vault\Reports`).

To migrate PST files using PST Locate and Migrate

1. Use **Run now** or schedule a run of the PST Locator task to find available domains. On the **Domains** page in the task properties, you then select the domains in which the computers that you want to search for PST files are located

   See "Running the PST Locator task to find domains and computers" on page 54.

2. Use **Run now** or schedule another run of the PST Locator task to find the computers in the selected domains. All the computers that the task finds are listed in the Administration Console under **Personal Store Management** > **Computers**.

3. You can configure the PST Locator task so that it automatically searches for PST files on each computer that it finds. Alternatively, in the Administration Console, under **Personal Store Management** > **Computers**, you can select the computers that you want the task to search for PST files.

   See "Selecting computers for PST searching" on page 59.

   You can also use the **Add** option in the **Personal Store Management** > **Computers** context menu to add the computers that you want the task to look for PST files.

   See "Adding computers for PST searching" on page 56.

4. Use **Run now** or schedule another run of the PST Locator task, this time to search for PST files on the selected computers. All the PST files that the task finds are listed in the Administration Console, under **Personal Store Management** > **Files**.

   See "Running the PST Locator task to find PST files" on page 61.

   You can also use the **Add** option in the **Personal Store Management** > **Files** context menu to add PST files that you want to migrate to Enterprise Vault.

   See "Adding PST files for migration" on page 62.

5 In the Administration Console you can edit the properties of a PST file, provide passwords for password-protected PST files, change the migration priority, and change the migration status of a PST file, if required.

The PST Collector task copies PST files with a status of **Ready to copy** to the PST holding folder. Depending on the configuration options selected, some manual intervention may be required to approve PST files for migration. For example, migration may only be started once the PST files have been backed up, or the ownership of particular PST files may need to be verified. Additionally, you may need to provide passwords for password-protected PST files, or you may want to prevent the migration of particular PST files.

Note that for password-protected PST files you may allow Enterprise Vault to override the passwords during PST migration. This setting is useful in cases the password is missing or is incorrectly provided. To override passwords, enable **Override passwords for password-protected PST files** in the **General** tab of the **Personal Store Management** properties.

See "Editing PST file properties" on page 64.

6 Use **Run now** or schedule a run of the PST Collector task to copy the selected PST files to the central PST holding folder.

The PST Collector task considers the migration priority of the file when it copies files. The task copies the files that have a higher priority first.

See "Running the PST Collector task" on page 65.

7 Use **Run now** or schedule a run of the PST Migrator task to archive items from the PST files to the associated destination archive.

The PST Migrator task considers the migration priority of the file when it archives files. The task processes the files that have a higher priority first.

See "Running the PST Migrator task" on page 65.

Running the PST Locator task to find domains and computers

You can schedule the PST Locator task to run during normal office hours. This ensures that the task finds the maximum possible number of computers and PST files. When the PST Locator task has completed its search for PST files it does no more work, even if its schedule window is still open. It does not scan each computer again for a minimum of one day, although you can increase this period between scans.

When you first run the PST Locator task, it searches for available domains. You then select the domains to search and rerun the task to find the computers that you want to search for PST files.

When the PST Locator task finds a computer, it attempts to determine if the computer is a NetApp device. Performing this check can slow down the search for computers. You can switch off this check, and later identify the NetApp devices manually in the list of computers.

See "Switching off NetApp device identification checks by the PST Locator task" on page 58.

Before searching for PST files, you can edit the properties of the computers that have been found to include or exclude specific computers when searching for PST files. You can then run the task again to search for PST files on the selected computers.

You can also use the **Add** option in the **Personal Store Management** > **Computers** context menu to add the computers that you want the task to look for PST files in.

See "Adding computers for PST searching" on page 56.

To run the PST Locator task to find domains

1. In the **Tasks** listing of the Administration Console, right-click the PST Locator task and then click **Start**.
2. Do either of the following:
   - Right-click the task and then click **Run Now**.
   - Wait for the scheduled run time for the PST Locator task.

   The domains that have been found are then listed on the **Domains** page in the PST Locator task properties.
3. Open the PST Locator task properties and select the domains in which the computers that you want to search for PST files are located.
4. Click **OK** to close the task properties, and then restart the task to apply the changes.

To run the PST Locator task to find computers

1. Do either of the following:
   - Right-click the PST Locator task and then click **Run Now**. In the dialog box that is displayed, ensure that **Search for new computers** is selected.

- Wait for the scheduled run time for the PST Locator task.

2 The task searches for computers in the domains that you selected in the task properties. Computers that have been found on the network are listed under **Personal Store Management** > **Computers** in the Administration Console. You can run the task several times to build up a list of computers before beginning the search for PST files.

3 In the list of computers, select the computers that you want the task to search for PST files.

See "Selecting computers for PST searching" on page 59.

On a small network, if you want the task to automatically search every computer that it finds, select **By default search for PSTs on each computer** on the **Settings** page of the PST Locator task properties.

You can also specify paths to include or exclude for PST file searches.

See "Configuring paths to include or exclude for PST searching" on page 60.

Adding computers for PST searching

Computers that have been found on the network are listed under **Personal Store Management** > **Computers** in the Administration Console. You can also add the computers that you want to the PST Locator task to search for PST files in one of the following ways:

- Add a single computer.
- Add multiple computers using a CSV file.

To add a single computer to search for PST files

1 In the Administration Console, expand **Personal Store Management** > **Computers**.

2 Right-click and select **Add** > **Single** on the menu.

3 In the **Add computer to search for PST files** dialog box, browse to add the computer.

4 Next to **Associated mailbox**, click **Browse** to select the mailbox from a list of those available. You can leave **Associated mailbox** blank if required.

5 Select the **Search this computer when PST Locator task runs** check box to enable searches of the computer when the PST Locator task runs.

To add multiple computers to search for PST files

1 Specify details of the computers that you want to add in a CSV file, each on a separate line, in the following format:

Name,*Mailbox*,*EnableSearch*

Where:

- *Name* (mandatory) is the name of the computer that you want to add. You can specify the NetBIOS or the fully qualified domain name of the computer.
- *Mailbox* (optional) is the display name of the mailbox that you want the located PST files to be associated with in the archive.
- *EnableSearch* (optional) specifies whether the PST Locator task should look for PST files on this computer.
  0 - Do not search for PST files on this computer.
  1 - Search for PST files on this computer.

Note the following:

- The CSV file must be saved as a Unicode file. You can use Windows Notepad to create such files.
- If the first line of the CSV file fails to process, Enterprise Vault considers the line as the header row and ignores it during processing.
- If the value contains spaces or commas, enclose the value in quotation marks.
- List separators are required even when you do not specify optional parameters.

Example:

```
Name,Mailbox,EnableSearch,DirectoryName,SiteName

abc.xyz.com,"User 1",,,

pqr1.joe.com,,1,Directory1,Site1

xuv23j3.smith.com,,,,
```

2. In the Administration Console, expand **Personal Store Management** > **Computers**.
3. Right-click and select **Add** > **Multiple** on the menu.
4. In the **Add computer to search for PST files** dialog box, browse to select the CSV file that contains the details of the computers that you want to add.

The Enterprise Vault Management Shell also provides the `Add-EVPstComputer` cmdlet which lets you add single or multiple computers.

See "PowerShell cmdlets for PST migration" on page 66.

Switching off NetApp device identification checks by the PST Locator task

When the PST Locator task finds a computer, it attempts to determine if the computer is a NetApp device. Performing this check can slow down the search for computers. This section describes how to switch off the automatic identification of NetApp devices by the PST Locator task during the search for computers. Later you can identify NetApp devices manually by editing the computer properties in the Administration Console.

See "Selecting computers for PST searching" on page 59.

To switch off the automatic identification of NetApp devices you configure a setting in the file `PSTlocatorTask.exe.config`. This file and an example version of it are located in the Enterprise Vault program folder (for example `C:\Program Files (x86)\Enterprise Vault`). The example file contains examples of the settings that can be configured in `PstLocatorTask.exe.config`.

To switch off the automatic identification of NetApp devices

1. On the Enterprise Vault server that runs the PST Locator task, start Windows Explorer and navigate to the Enterprise Vault program folder (for example `C:\Program Files (x86)\Enterprise Vault`).
2. Copy the file, `PstLocatorTask.exe.config`, to a safe location.
3. If `PSTlocatorTask.exe.config` is the stub version of the file, then replace this file by copying and renaming the example file, `Example PstLocatorTask.exe.config`.
4. Open the `PstLocatorTask.exe.config` file in a text editor such as Windows Notepad.
5. Search for the following text:

   ```
   <PSTSettings>
   ```

6. Do one of the following:

   - If you have created the file by copying and renaming the example version, then the following lines exist in the entries under `<PSTSettings>`:

     ```
     <!--Determine whether computer is a NetApp Filer: Default: true-->
     <add key="LocateNetAppFilers" value = "true"/>
     ```

     Change the setting value to `"false"`.

   - If you created the file on a previous release, then add the following lines under `<PSTSettings>`:

```
<!--Determine whether computer is a NetApp Filer: Default: true-->
<add key="LocateNetAppFilers" value = "false"/>
```

7 Save and close the file.

8 In the Administration Console, restart the PST Locator task.

Selecting computers for PST searching

Computers that have been found on the network are listed under **Personal Store Management** > **Computers** in the Administration Console. You can select the computers that you want to search for PST files in one of the following ways:

- Select multiple computers at once.
- Edit the properties of individual computers.

You can edit the properties of the computer to specify paths you want the PST Locator task to look in or ignore when looking for PST files.

You can also use the **Add** option in the **Personal Store Management** > **Computers** context menu to add the computers that you want the task to look for PST files in.

See "Adding computers for PST searching" on page 56.

Note: The PST Locator task is unable to perform a hard disk search on a NetApp MultiStore (also known as "vFiler"). A NetApp Filer must be configured with a minimum ONTAPI Management API version of 1.4. The ONTAPI interface is the foundational API for NetApp products. Version 1.4 is provided with the Data ONTAP 7G software release, or later. For the latest information on supported devices and versions of software, see the Enterprise Vault Compatibility Charts.

To exclude a computer from PST searching, edit the properties of the computer.

To select multiple computers to search

1 In the Administration Console, expand **Personal Store Management** > **Computers** to display a list of the computers that have been found on the network.

2 Hold down Ctrl or Shift and highlight the computers that you want to search.

3 Right-click and select **Properties** on the menu.

4 A dialog box asks if you want the PST Locator task to search the selected computers. If the highlighted computers are the ones that you want to search, click **Yes**.

In the **Search** column, **Yes** is displayed for each computer that you selected.

To edit the properties of individual computers

1. In the Administration Console expand **Personal Store Management** > **Computers** to display a list of the computers that have been found on the network.
2. Double-click the name of the computer that you want to include when searching for PST files. The computer properties page is displayed.
3. To include the computer in PST searching, select **Search this computer when PST Locator task runs**.

   To exclude the computer from PST searching, clear the option check box.
4. If the computer is a NetApp Filer, click the **Settings** tab and check that **This computer is a NetApp Filer** is selected.

   This setting is selected automatically when the PST Locator task adds a NetApp Filer. However, if the computer was unavailable when found by the PST Locator task, it is not selected automatically.
5. Click the **Search Paths** tab to specify the paths that you want the PST Locator task to include or exclude when looking for PST files on this computer.
6. Click **OK** to close the properties.

Configuring paths to include or exclude for PST searching

You can edit the PST Locator task properties to configure the paths you want the PST Locator task to look for or ignore during the search for PST files. You can also edit the computer properties page to specify paths you want to include or exclude for PST searching.

You can also exclude specific network shares from PST searching using the `PstLocatorTask.exe.config` file.

See "Excluding network shares from PST migration using the PstLocatorTask.exe.config file" on page 69.

To configure paths for PST searching

1. Do either of the following:
   - In the **Tasks** listing of the Administration Console, right-click the PST Locator task and then, on the shortcut menu, click **Properties**.
   - In the Administration Console, expand **Personal Store Management** > **Computers** to display a list of the computers that have been found on the network. Select the name of the computer and, on the shortcut menu, click **Properties**.
2. Click the **Search Paths** tab.

3 In **Include in search**, do either of the following:

- Select **Search entire computer** to allow the PST Locator task to do a full computer search for PST files.
- Select **Search specific paths** and click **Add Paths** to add the paths that you want to include during PST searching.

4 To exclude paths from PST searching, in **Exclude from search**, click **Add Paths** to add the paths that you want to exclude.

Note: Paths you specify for exclusion should be subpaths of the paths that you have included for search.

Running the PST Locator task to find PST files

When you run the PST Locator task this time, it searches for PST files on the computers you selected to search. You can configure the task to search for PST files in the Outlook profiles on a computer (registry search) or on the computer's hard disks (hard disk search).

During a hard disk search, the task does not search either the PST holding folder or the temporary PST migration file folders on any computer running a PST Migrator task. On all computers, the Recycle Bin folder is not searched.

You can also use the **Add** option in the **Personal Store Management** > **Files** context menu to add PST files for migration.

See "Adding PST files for migration" on page 62.

To run the PST Locator task to find PST files

1 Do either of the following:

- Right-click the PST Locator task and, on the shortcut menu, click **Run Now**. In the dialog box that is displayed, select **Registry search** or **Hard disk search** as required.

Note: On computers running Windows 7, you must enable the RemoteRegistry service to allow the PST Locator task to look for PST files using registry searches.

- Wait for the scheduled run time for the PST Locator task.

2 The task searches for PST files on the computers that you selected. The PST files that have been found are listed under **Personal Store Management** > **Files** in the Administration Console. You can filter the PST files with a particular migration status, or for a certain user.

3 Before the PST Collector task runs to copy the PST files to the PST holding folder, you must edit the properties of the PST files to provide any missing information and change the status to "Ready to copy".

See "Editing PST file properties" on page 64.

Adding PST files for migration

PST files that have been found on the network are listed under **Personal Store Management** > **Files** in the Administration Console. You can also add the PST files that you want to migrate in one of the following ways:

- Add a single PST file.
- Add multiple PST files using a CSV file.

To add a single file for migration

1 In the Administration Console, expand **Personal Store Management** > **Files**.

2 Right-click and select **Add** > **Single** on the menu.

3 In the **Add PST files** dialog box, browse to add the PST file.

To add multiple PST files for migration

1 Specify the details of PST files that you want to add in a CSV file, each on a separate line, in the following format:

UNCPath,*Mailbox*,*Archive*,*ArchiveType*,*RetentionCategory*,*Priority*,*Language*

Where:

- *UNCPath* (mandatory) is the UNC path along with the file name of the PST file that you want to add.
- *Mailbox* (optional) is the display name of the mailbox that you want this PST file to be associated with in the archive.
- *Archive* (optional) is the name of the archive.
- *ArchiveType* (optional) is the type of archive. You can specify either "Exchange Mailbox" or "Internet Mail". If you specify a mailbox, the PST is migrated to the associated Exchange Mailbox archive. If you do not specify a mailbox, Enterprise Vault looks for the archive in both Exchange Mailbox archives and Internet Mail archives. If only one archive is found, Enterprise

Vault sets the archive type as that of the found archive and migrates the file to that archive. If multiple entries are found, then Enterprise Vault migrates the file to the Exchange Mailbox archive. Note that you cannot associate a mailbox with an Internet Mail archive.

- *RetentionCategory* (optional) is the retention category that should be applied to the contents of this PST file when it is archived.

  Note: Some Enterprise Vault features, such as the retention folders and classification features, can override the specified retention category. For more information on retention, see the *Administrator's Guide*.

- *Priority* (optional) is the priority in which the PST Migrator should start migrating the contents of this file.
  1 - Critical
  2 - Important
  3 - High
  4 - Medium
  5 - Low
  6 - lowest
- *Language* (optional) specifies the language that the PST Migrator is to use if it needs to create folder names in the mailbox. PST Migrator must use the same Windows code page that was used when the PST file was created.

Note the following:

- The CSV file must be saved as a Unicode file. You can use Windows Notepad to create such files.
- If the first line of the CSV file fails to process, Enterprise Vault considers the line to be the header row and ignores it during processing.
- If a value contains space characters or commas, enclose it in quotation marks.
- List separators are required even when you do not specify optional parameters.

The following is a sample CSV file:

```
UNCPath,Mailbox,Archive,ArchiveType,RetentionCategory,Priority,Language,DirectoryServer,
  SiteName

\\Server\E$\PSTBackup\Backup.pst,"Mailbox,Z",Archive,"Exchange Mailbox",Default,2,
  Western European,,
```

```
\\abc.xyz.com\c$\user1.pst,,"IMAP1","Internet Mail",RC1,1,Arabic,EVServer1,SiteA
\\Server1\D$\PSTs\HR.pst,,,,,,,,
```

2. In the Administration Console, expand **Personal Store Management** > **Files**.
3. Right-click and select **Add** > **Multiple** on the menu.
4. In the **Add multiple PST files** dialog box, browse to select the CSV file that contains the details of the files that you want to add.

The Enterprise Vault Management Shell also provides the `Add-EVPstFile` cmdlet, which lets you add single or multiple PST files for migration.

See "PowerShell cmdlets for PST migration" on page 66.

Editing PST file properties

The normal status of a PST file that has been found is "Do not migrate". When you are ready for the PST Collector task to copy the file to the PST holding folder, edit the PST file properties in the Administration Console and change the status to "Ready to copy".

If you have used message sampling to identify PST file owners, then depending on how you have configured ownership identification Enterprise Vault automatically changes the state to **Ready to copy**.

If the PST Locator task cannot determine the ownership of the PST file, the associated mailbox, and its corresponding archive, then the PST file status is displayed as "Not ready". You need to edit the properties of the PST file to provide the required information, and change the status to "Ready to copy".

If required, you can use the **Settings** tab in the PST file properties to specify the password for a password-protected file.

To edit the properties of a PST file

1. In the Administration Console listing, double-click the PST file name to display the PST file properties.
2. On the **General** page, do one of the following:
   - Next to **Mailbox**, click **Browse**, and then select the mailbox of the user who owns the PST file. The corresponding archive is automatically chosen.
   - Next to **Destination archive**, click **Browse**, and then select the mailbox archive of the user who owns the PST file. The corresponding mailbox is automatically chosen.
3. On the **Settings** page you can configure the following, if required:
   - Specify a retention category to be used for this PST file.

- Select the Windows code page to be used when creating folders for this PST file.
- Specify the migration priority as Critical, Important, High, Medium, Low, or Lowest. The default priority is Medium.
- Specify a password for PST file if it is password-protected.

4 When you have completed the required details, change the migration status on the **General** page to **Ready to copy**.

Running the PST Collector task

The PST Collector task copies PST files from users' computers to the PST holding folder. It copies only the PST files that have a status of "Ready to copy". It uses the migration priority of the file when it collects files. Files that have a higher priority are copied first.

You can restrict the number of files in the holding area so that the PST Migrator task can process all the files during its scheduled run. This ensures that the period for which items within PST files are unavailable is as short as possible.

The account under which the task runs must have Delete access to the original location of the PST file. The easiest way to ensure that the task has the correct access is to run it using an account in the domain administrators' group.

See "Administrator roles required to manage PST Locate and Migrate" on page 44.

To run the PST Collector task

1 In the **Tasks** listing of the Administration Console, right-click the PST Collector task and then, on the shortcut menu, click **Start**.

2 Do one of the following:

- Right-click the task and then, on the shortcut menu, click **Run Now**.
- Wait for the scheduled run time for the PST Collector task.

Running the PST Migrator task

The PST Migrator task archives the contents of PST files that are in the PST holding folder to Enterprise Vault archives. There can be many PST Migrator tasks in your Enterprise Vault site, but only one per Enterprise Vault server. You need to configure a PST Migrator task on each Enterprise Vault server that hosts archives to which you intend to migrate PST files. The task archives the contents of PST files that have a status of "Ready to migrate". It uses the migration priority of the file when it migrates files. Files that have a higher priority are processed first.

If you configured the PST migration to wait for the PST files to be backed up before the PST Migrator task archives the contents (in PST Collector task properties), then the PST file status may be displayed as "Ready to back up". The status changes automatically after the files have been backed up.

To run the PST Migrator task

1. In the **Tasks** listing of the Administration Console, right-click the PST Migrator task and, on the shortcut menu, click **Start**.
2. Do one of the following:
   - Right-click the task and then, on the shortcut menu, click **Run Now**.
   - Wait for the scheduled run time for the PST Migrator task.
3. When the file contents have been archived, the PST file status is displayed as "Ready for post-processing".

   When the PST Migrator task has successfully finished processing the PST file, the file status is displayed as "Complete". Depending on how you have set up email notifications, an email is sent to the end user's mailbox.

   If a problem prevents the task from completing an operation, details are displayed in the **More details** box of the PST file properties in the Administration Console. You can also check the report file that is generated during the run.

PowerShell cmdlets for PST migration

Enterprise Vault provides two PowerShell cmdlets which you can use to add computers as locate and migrate PST migration targets, and to add PST files whose contents you want to migrate to Enterprise Vault.

About the PST migration cmdlets

Table 6-3 describes the PST migration cmdlets that the Enterprise Vault Management Shell provides.

Table 6-3 PST migration cmdlets

Cmdlet	Description
`Add-EVPstComputer`	Adds a computer to the list of Locate and Migrate PST migration target computers. Depending on how you use `Add-EVPstComputer`, Enterprise Vault can search this computer for PST files. You can add computers that belong to individual users, and you can add file servers that host PST files that belong to many users.
`Add-EVPstFile`	Adds a PST file whose content you want to migrate to Enterprise Vault.

You can use these cmdlets on their own to add individual computers and files, or with PowerShell's `Import-Csv` cmdlet and CSV data, to add multiple computers or files in a single operation.

Running the PST migration cmdlets

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

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

```
Get-Help Add-EVPstComputer -detailed
```

Using Add-EVPstComputer

Use the following syntax when you run `Add-EVPstComputer`:

```
Add-EVPstComputer -Name <string> [-Mailbox <string>] [-EnableSearch]
[-SiteName <string>] [-DirectoryServer <string>]
```

For example:

```
C:\PS>Add-EVPstComputer -Name JohnDoeLaptop -Mailbox "John Doe"
-EnableSearch
```

This adds John Doe's laptop as a PST migration target, and also specifies John's mailbox, in which Enterprise Vault will place shortcuts for migrated items.

Using Add-EVPstFile

Use the following syntax when you run `Add-EVPstFile`:

```
Add-EVPstFile -UNCPath <string> [-Mailbox <string>] [-Archive
<string>] [-ArchiveType <string>] [-RetentionCategory <string>]
[-PasswordProtected] [-Language <string>] [-Priority <string>]
[-SiteName <string>] [-DirectoryServer <string>]
```

For example:

```
C:\PS>Add-EVPstFile -UNCPath
\\FileServer1\UserShares\VIPs\JohnDoe\PSTs\2012.pst
```

This adds the specified PST file for migration to Enterprise Vault.

Adding multiple computers or PST files

Enterprise Vault's PST migration cmdlets add individual computers as locate and migrate PST migration targets, or individual PST files for migration. To add multiple computers or PST files in a single operation, you can use the `Import-Csv` PowerShell cmdlet and CSV files that contain all the computers or files and their associated parameters.

To add multiple computers, construct CSV data in the same format as that used when you add multiple computers in the Administration Console.

See "Adding computers for PST searching" on page 56.

To add multiple PST files, construct CSV data in the same format as that used when you add multiple files in the Administration Console.

See "Adding PST files for migration" on page 62.

You can pipe the data that `Import-Csv` reads from a CSV file to the appropriate PST migration cmdlet. For example:

```
Import-Csv C:\files.csv | Add-EVPstFile
```

This reads data from `C:\files.csv` and pipes it to the `Add-EVPstFile` cmdlet.

By default, `Import-Csv` passes each value from the CSV data as a string. However, when you use the `Add-EVPstComputer` cmdlet, you must pass the `-EnableSearch` as a Boolean.

If you use `Add-EVPstComputer` with `Import-Csv`, you must convert the `-EnableSearch` value from the CSV data to a Boolean. For example:

```
Import-Csv c:\computers.csv | % { $_.EnableSearch =
[bool]([int]$_.EnableSearch ); $_ } | Add-EVPstComputer
```

For more information about the use of `Import-Csv`, type the following command in PowerShell:

```
Get-Help Import-Csv -detailed
```

Excluding network shares from PST migration using the PstLocatorTask.exe.config file

You can exclude specific network shares when searching for PST files by listing them in the configuration file `PstLocatorTask.exe.config`.

To exclude network shares from PST migration using the PstLocatorTask.exe.config file

1. On the Enterprise Vault server that runs the PST Locator task, start Windows Explorer and navigate to the Enterprise Vault program folder (for example, `C:\Program Files (x86)\Enterprise Vault`).
2. Do one of the following:
   - If the `PstLocatorTask.exe.config` file exists in the folder, copy it to a safe location.
   - If there is no `PstLocatorTask.exe.config` file, create it by copying and renaming the file `Example PstLocatorTask.exe.config`.
3. Open the `PstLocatorTask.exe.config` file in a text editor such as Windows Notepad.
4. Search for the following text:

   ```
   <PSTSettings>
   ```

5. Immediately below this heading, add a line to list the network shares that you do not want to search. The syntax is as follows:

   ```
   <add key="SharesToAvoid" value="share_1;share_2;share_3..."/>
   ```

   Where `share_1`, `share_2`, and so on, comprise a semicolon-separated list of the UNC paths of the network shares. For example, to exclude the shares `\\myComputer\C$` and `\\yourComputer\G$`, you would type the following:

   ```
   <add key="SharesToAvoid"
   value="\\myComputer\C$;\\yourComputer\G$"/>
   ```

6. Save and close the file.
7. In the Administration Console, restart the PST Locator task.

Troubleshooting PST migration

You can use the task report files to assist in troubleshooting PST migration failures. Each time a task runs, it creates a report and places it in the `Reports` folder, which is a subfolder of the Enterprise Vault program folder (for example `C:\Program`

`Files (x86)\Enterprise Vault\Reports`). The report file name takes the following form:

- PSTLocTask_*server_datetime*.txt
- PSTColTask_*server_datetime*.txt
- PSTMigTask_*server_datetime*.txt

If file sharing is not enabled on a user's computer, the PST Locator task is unable to search the registry or files on that computer. Note that Windows does not automatically enable file sharing. If the PST Locator task cannot search the registry or files, this results in errors such as the following in the report file:

```
** 18/07/2005 14:34:21 Hard disk search failure on DEMO : Failed to
read registry to get list of drives : The network path was not
found. **

** 18/07/2005 14:34:21 Registry search failure on DEMO : The network
path was not found. **
```

These errors are also reported if the Windows firewall is on. If the firewall is on, then you need to create an exception in Windows firewall for "File and Printer sharing", TCP port 139 and 445.

Chapter 7

PST migration: client-driven migration

This chapter includes the following topics:

- About client-driven PST migration
- Preparation for client-driven PST migration
- Editing the PST migration messages for client-driven PST migration
- Configuring the PST holding folder for PST client-driven migration
- Creating a PST Migrator task for PST client-driven migration
- Enabling mailboxes for PST client-driven migration
- Permissions required for migrating PST files stored on network drives

About client-driven PST migration

You can configure the Enterprise Vault Outlook Add-In so that it migrates PST files automatically to a central PST holding folder on the Enterprise Vault server. The PST Migrator task then processes the PST files and archives the contents.

You need to configure a PST Migrator task on every Enterprise Vault server that hosts a Storage service and manages the archives to which you intend to migrate PST files. When a PST file migrates, the migration process runs on the Enterprise Vault server that manages the destination archive.

Client-driven PST migration can be useful in the following cases:

- You do not have permission to access PST files on the user's computer.
- Users need continual access to their PST files.

- The user's computer is available on the network only occasionally—for example, a user with a laptop computer who visits the office on one day each week.
- You want to give users control over migrating their PST files.

In summary, the client-driven migration process is as follows:

- You enable mailboxes for client-driven PST migration.
  Depending on whether you want to give users more control over PST file migration, you may allow users to choose files for migration.
- An explanatory mail message is immediately sent to the newly enabled mailboxes.
- The next time a user starts Outlook, the computer is scanned for PST files.
- Starting with PST files in the user's profile, each PST file is sent as a series of approximately 10-MB chunks to the PST holding folder.
- The PST Migrator task migrates the chunks to the user's archive.
- When a PST file has been successfully migrated, checks are made to make sure that no more items have been added to it. Depending on how you have set the PST Migration policy, the PST file is removed from the user's profile after all the items are migrated.

Options to configure client-driven PST migration

Enterprise Vault provides various options to configure client-driven migration depending on the type of control you want users to have over the migration of their PST files.

Table 7-1 details various options to configure client-driven migration.

Table 7-1 Options to configure client-driven PST migration

To do this	Client-driven migration enabled	Search Paths	Allow PST submission
Allow the Enterprise Vault Outlook Add-In to migrate located PST files without user intervention.	Yes	Yes	No
Allow users to choose whether to migrate located PST files. Users can also submit PST files for migration.	Yes	Yes	Yes

Table 7-1 Options to configure client-driven PST migration *(continued)*

To do this	Client-driven migration enabled	Search Paths	Allow PST submission
Allow only the manual submission of PST files. You do not want the Outlook Add-In to look for PST files on the user's computer.	Yes	By default, the Outlook Add-In looks for PST files on the user's computer. However, you can stop it from searching for PST files by excluding all relevant local drives (C:, D:, E:, and so on).	Yes

Preparation for client-driven PST migration

Table 7-2 outlines the steps that are required to configure client-driven PST migration. Enterprise Vault provides other tools for migrating PST files to archives.

See "Tools for migrating PST files" on page 12.

Note: Client-driven PST migration does not work if the registry value PSTDisableGrow is enabled on users' computers. For information about how to override PSTDisableGrow, see the *Setting up Exchange Server Archiving* guide.

Table 7-2 Steps to configure client-driven PST migration

Step	Action	Description
Step 1	For migrating the PST files that are on network shares, the account that runs the Directory service requires a set of minimum permissions.	See "Permissions required for migrating PST files stored on network drives" on page 79.
Step 2	Configure the PST holding folder.	See "Configuring the PST holding folder for PST client-driven migration" on page 75.
Step 3	Set up the PST migration messages.	See "Editing the PST migration messages for client-driven PST migration" on page 74.
Step 4	Create a PST Migrator task, and configure temporary files folder.	See "Creating a PST Migrator task for PST client-driven migration" on page 76.

Editing the PST migration messages for client-driven PST migration

When you enable a mailbox for client-driven PST migration, Enterprise Vault automatically delivers messages to that mailbox for various PST migration events. The type of emails that Enterprise Vault sends to user mailboxes depends on how you have set up notifications in the Exchange PST Migration policy.

During the installation, the messages are placed in the following folder beneath the Enterprise Vault program folder (typically, `C:\Program Files (x86)\Enterprise Vault`):

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

Where *lang* indicates the language used.

Ensure that you have copied the messages into the Enterprise Vault program folder. Otherwise, the messages are not sent even if you have configured the Exchange PST Migration policy to send notifications.

Table 7-3 lists the messages and describes the circumstances under which each is sent.

Table 7-3 PST migration messages

Message	Subject and description
EnablePSTMigrationMessage	Enterprise Vault is ready to migrate your Outlook Personal Folders files (`.pst`) The PST migrator sends this message when you enable a user's mailbox for client-driven migration using the **Personal Store Management** > **Mailboxes** > **Enable Client-Driven Migrations** option.
EnabledForPSTImportMessage	Your mailbox is enabled for the submission of PST files to Enterprise Vault™ The PST migrator sends this message to users when you allow users to submit PST files for migration to Enterprise Vault. This happens when you select the **Allow PST submission** check box in the **Migration** tab of the Exchange PST Migration policy properties.

Table 7-3 PST migration messages *(continued)*

Message	Subject and description
PSTAwaitingAuthorizationMessage	ACTION REQUIRED: Enterprise Vault has located PST files on your computer that require your attention The PST migrator sends this message when Enterprise Vault finds PST files on the user's computer that need to be allowed for migration by the user.
PSTMigratedMessage	Your PST file *{0}* has been archived by Enterprise Vault The PST migrator sends this message to users when the PST file is successfully migrated to Enterprise Vault.

To edit a PST migration message for client-driven PST migration

1. Decide which language version of the message you want to use and locate the message file.
2. Using a computer that has Microsoft Outlook installed, double-click the message file in Windows Explorer to open it.
3. Review the text and make any changes that you require.
4. Save the message file.
5. Copy the edited message file to the Enterprise Vault program folder on every Enterprise Vault server in the site.

Configuring the PST holding folder for PST client-driven migration

The PST holding folder is used as a collecting area for the PST files that the PST Migrator task has archived. The folder must be a network share to which the logon account that the PST Migrator task uses has Delete access.

The account that you use to configure the PST holding area must have sufficient access to the folder to list it in a selection dialog box. Typically, the Vault Service account is used as the logon account by the tasks and when configuring the PST holding folder, but it is possible to specify different accounts.

To configure the PST holding folder

1. In the left pane of the Administration Console, display the Enterprise Vault Site Properties.
2. On the **General** tab, click **Browse** next to **PST holding folder**.

   A prompt asks whether you want to browse Regular or Hidden shares.
3. Select the type of share that you intend to specify for the PST holding folder, and then click **OK**.
4. In the **Browse for Folder** dialog box, expand **Entire Network** > **Microsoft Windows Network**. Expand the required domain and then the server on which the share is located. The list of shares that are displayed contains shared folders to which the account has access.
5. Select the folder you want to use for the PST holding folder and then click **OK**.
6. Click **OK** to close Site Properties.

Creating a PST Migrator task for PST client-driven migration

If you have configured Locate and Migrate, then you already have a PST Migrator task and can ignore this section. If you have not configured Locate and Migrate then you need to work through this section.

Note: You need to configure a PST Migrator task on every Enterprise Vault server that hosts a Storage service and manages the archives to which you intend to migrate PST files. When the migration process migrates a PST file, it runs on the Enterprise Vault server that manages the destination archive.

To create a PST Migrator task

1. In the Administration Console, expand your site until the **Enterprise Vault Servers** container is visible.
2. Expand **Enterprise Vault Servers** and then expand the server on which you want to add the PST Migrator task.

3 Right-click **Tasks** and then, on the shortcut menu, click **New > PST Migrator task**.

The New PST Migrator task wizard starts.

4 Work through the wizard.

You need to supply the location of a folder that the task can use to hold temporary copies of the PST files during migration. This folder must be on a local drive. The account under which the PST Migrator task runs must have full access to the folder.

Note: Do not change the location of this folder while the PST Migrator task runs, or while client-driven migration processes PST files.

Enabling mailboxes for PST client-driven migration

Enterprise Vault provides a wizard that lets you enable mailboxes for client-driven migration. You can enable a small number of mailboxes at a time so that at any one time there is a manageable number of PST files to process.

After you have enabled a mailbox for client-driven PST migration, the Enterprise Vault Outlook Add-In starts scanning for PST files when the corresponding user next starts Outlook.

The list of PST files that all client computers have found appears in the Administration Console, in the **Files** container under **Personal Store Management**.

The located PST files are also listed in the Enterprise Vault PST Migration page in the Enterprise Vault Outlook Add-In. Depending on how you have configured the Exchange PST Migration policy, users can see the migration status of the files and choose files for migration.

To enable mailboxes for client-driven PST migration

1 In the left pane of the Administration Console, expand **Personal Store Management**.

2 Right-click **Mailboxes** and click **Enable Client-Driven Migrations**.

The **Enable Mailbox for Client-Driven Migration** wizard starts.

3 Work through the wizard.

The wizard prompts you to do the following:

- Select the Microsoft Exchange Server computer that has the mailboxes you want to enable for client-driven PST migration.
- Select the mailboxes that you want to enable for client-driven PST migration.

4 Click **Finish** to enable the selected mailboxes for client-driven migration and exit from this wizard.

Enabling mailboxes for PST file submission

You can configure the Exchange PST Migration policy to give users more control over the migration of PST files that are located on their computers. Selecting the **Allow PST submission** option in the PST Migration policy properties page enables the following features in the Enterprise Vault Outlook Add-In.

- The **Manually add a PST file** button is displayed on the PST Migration page. This button allows users to browse for PST files on their computer and their network locations and submit them for migration to Enterprise Vault.
- All the PST files that Enterprise Vault finds are listed in the **Migrate PST Files** dialog box, which allows users to choose whether to migrate PST files to Enterprise Vault.

To enable mailboxes for PST file submission

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

2 Click **Policies** > **Exchange** > **PST Migration**.

3 Right-click the PST Migration Policy that you want to edit and then select **Properties**.

4 In the **Client-driven migration** section of the **Migration** tab, select **Allow PST submission**.

5 Select **Allow retention category override** if you want to allow users to change the retention category of the PST files that they choose to migrate.

Note: Some Enterprise Vault features, such as the retention folders and classification features, can override the specified retention category. For more information on retention, see the *Administrator's Guide*.

---

6 Click **Search Paths** to specify the paths that you want the Enterprise Vault Outlook-Add-In to include or exclude when searching for PST files.

7 Click **OK**.

Permissions required for migrating PST files stored on network drives

You can configure this facility to migrate the PST files that are stored on Windows-based shares, and on NetApp Filers.

To migrate PST files from a Windows share, the account that runs the Directory service must be a member of one of the following security groups on the file server:

- Administrators
- Server Operators
- Power Users

To migrate PST files from a NetApp Filer, the account that runs the Directory service must be a member of the Administrators group on the NetApp Filer.

If you use the NetApp Filer autohome feature, see the following technical note:

https://www.veritas.com/docs/100002054

You cannot migrate files that are hosted on the following:

- Non-Windows file servers, other than NetApp Filers
- NetApp vFiler devices running a version of Data ONTAP earlier than Data ONTAP 8.0
- Distributed File System (DFS) shares