Symantec Enterprise Vault™
Installing and Configuring

Windows

6.0
Chapter 1  About this guide
   Prerequisite knowledge ................................................................. 17
   Formats available ............................................................................. 17
   Typographical conventions ............................................................. 18
   Related documentation ................................................................. 18

Section 1  Installing, configuring, and upgrading Enterprise Vault

Chapter 2  Upgrading to Enterprise Vault 6.0 SP4
   Introduction ...................................................................................... 23
   Upgrading to Enterprise Vault 6.0 SP4 .............................................. 24
      Removing services that are no longer required ............................. 24
      Preparing the Enterprise Vault servers ........................................ 25
   Installing Enterprise Vault 6.0 SP4 .................................................. 25
      Starting the Directory service .................................................... 26
   Running the Configuration Program ................................................. 27
      Upgrading from Enterprise Vault 5.0 .......................................... 27
      Upgrading from Enterprise Vault 6.0 .......................................... 29
      Postinstallation tasks ................................................................. 30
         Manually changing Enterprise Vault DCOM settings ............. 30
   Upgrading desktop clients ............................................................. 30
   Upgrading the Exchange Server forms ............................................ 30
      Upgrading forms ......................................................................... 31
   Upgrading desktop clients ............................................................. 32
   Upgrading the self-installing user extensions ................................. 32
      Copying the files ......................................................................... 33
      Editing the archived item form ................................................ 33
      Testing the edited form ............................................................ 34
      Publishing the edited form ....................................................... 34
      Publishing in Active Directory ................................................ 35
   Upgrading OWA 2000 extensions .................................................... 36
   Upgrading SharePoint Server ....................................................... 36
      Upgrading internet security settings for users ............................... 37
Chapter 3 Before installing

Operating system requirements ................................................................. 39
Basic hardware requirements .................................................................... 40
Storage requirements .................................................................................. 40
Disk space requirements ............................................................................ 40
Installation order ....................................................................................... 41
Notes on installation ................................................................................ 46
Installing MSMQ .................................................................................. 46
MSMQ when Enterprise Vault is on Active Directory controller . 47
.NET Framework and Active Server Pages on Windows 2003 ...... 48
Allowing HTML items larger than 4MB to be downloaded ........... 49
Installing Outlook on the Enterprise Vault computer ................. 49
Exchange System Manager on Enterprise Vault servers .......... 49
Configuring Application Pool accounts ................................................. 51
The Vault Service account ................................................................. 51
The Vault Site alias ............................................................................... 52
The service mailbox ................................................................................. 53
MSXML Requirement for Enterprise Vault servers ...................... 53
Requirements for users' computers ......................................................... 54
User Extensions for Outlook .................................................................. 55
What next? ............................................................................................ 55

Chapter 4 Preinstallation tasks

Creating the Vault Service account ....................................................... 57
Changing the Vault Service account .................................................. 58
Assigning Microsoft Exchange Server permissions ....................... 60
Creating a SQL login ............................................................................... 61
Creating the Vault Site alias ............................................................... 62
What next? ........................................................................................ 62

Chapter 5 Installing Enterprise Vault

Server installation ................................................................................ 63
What next? ........................................................................................ 65
Uninstalling Enterprise Vault .............................................................. 65

Chapter 6 Postinstallation tasks

Setting up security for the Web Access application ....................... 67
Effect on users .................................................................................... 67
Setting up the default authentication ................................................. 68
Customizing security for the Web Access application .................. 69
Using a default domain with basic authentication ....................... 69
Chapter 7 Running the Configuration Program

Introduction ................................................................. 79
Preparation ........................................................................ 80
Running the Configuration Program ..................................... 80
What next? ....................................................................... 83

Chapter 8 Running the Administration Console

Preparation ........................................................................ 85
Introduction ................................................................. 85
Starting the Administration Console .................................... 86
Permissions needed .......................................................... 86
Adding services .................................................................. 86
Creating Retention Categories ......................................... 87
Additional configuration tasks .......................................... 88
Reviewing site settings ...................................................... 88
Supporting secure web server connections .......................... 92
What next? ....................................................................... 92

Chapter 9 Setting up users’ desktops

Introduction ................................................................. 93
User Extension kits .......................................................... 94
User Extensions .............................................................. 94
Self-installing User Extensions ........................................ 94
Distributing the User Extensions ....................................... 95
Sending a shortcut .......................................................... 95
Performing a silent installation ........................................ 95
Distributing the User Extensions using SMS ...................... 96
Making the Self-Installing User Extensions available .......... 96
Copying the files ............................................................ 97
Editing the archived item form ................................................................. 98
Testing the edited form ............................................................................. 99
Publishing the edited form ...................................................................... 100
Publishing in Active Directory ................................................................. 100
Preparation ................................................................................................. 100
Publishing ................................................................................................... 101
Outlook 2003 ............................................................................................... 102
Getting users started .................................................................................. 102
Documentation ........................................................................................... 103
What next? .................................................................................................. 103

Chapter 10  Licenses and license keys
Overview ........................................................................................................ 105
Obtaining license keys .................................................................................. 106
What next? .................................................................................................. 106

Section 2  OWA and RPC over HTTP

Chapter 11  Configuring OWA access to Enterprise Vault
Enterprise Vault functionality in OWA clients ............................................ 109
About forms-based authentication in OWA 2003 clients ......................... 110
OWA configurations ..................................................................................... 111
Prerequisite software ................................................................................... 116
Configuring Enterprise Vault access for OWA 2003 users ....................... 118
  OWA 2003: Configuring Anonymous user on the Enterprise Vault server
  119
    What owau user.wsf configures ............................................................ 120
    Restarting the Admin service and synchronizing mailboxes ......... 121
    Installing OWA Extensions on a back-end Exchange Server 2003 ..... 122
    Configuring a back-end Exchange Server 2003 ............................. 123
    About Enterprise Vault forms registration ..................................... 125
    Installing OWA Extensions on a front-end Exchange Server 2003 .. 125
    Configuring a front-end Exchange Server 2003 .............................. 126
Configuring Enterprise Vault access for OWA 2000 users ...................... 127
  OWA 2000: Configuring Anonymous user on the Enterprise Vault server
  128
    What owau user.wsf configures ............................................................ 129
    Restarting the Admin service and synchronizing mailboxes ....... 130
    Installing OWA Extensions on a back-end Exchange Server 2000 .... 130
    Configuring a back-end Exchange Server 2000 ............................. 131
    About Enterprise Vault forms registration ..................................... 133
    Installing OWA Extensions on a front-end Exchange Server 2000 .... 133
Enabling Enterprise Vault access using OWA .............................................. 157
Configuring ISA Server 2004 for OWA Basic Authentication ............ 158
Configuring ISA Server 2004 for OWA forms-based authentication 161
How chained web listeners work ............................................................. 162
Steps to configure chained web listeners ............................................. 163
Exporting the Web site certificate form the OWA Web site .......... 163
Requesting a Web site certificate for the localhost listener .......... 164
Create a Web Publishing Rule that forwards incoming OWA requests to
the localhost Web listener ............................................................... 166
Create a Web Publishing Rule for the localhost listener that forwards
requests to the OWA Web site ...................................................... 169
Create a Web Publishing Rule that forwards requests for the
EnterpriseVaultProxy virtual directory to the internal network 173

Enabling Enterprise Vault access using RPC over HTTP .............. 175
Configuring an RPC firewall policy ..................................................... 175
Configuring an Enterprise Vault firewall policy ............................... 176

Chapter 14 How to uninstall Enterprise Vault OWA Extensions

OWA 2003: Removing OWA virtual directories, forms registration and Proxy
Bypass List .......................................................................................... 178
OWA 2003: Checking that components have been removed .......... 179
OWA 2003: Restoring OWA control files .......................................... 180
OWA 2003: Completing the removal of the OWA Extensions ........ 180
OWA 2000: Removing OWA virtual directories, forms registration and Proxy
Bypass List .......................................................................................... 180
OWA 2000: Checking that components have been removed .......... 181
OWA 2000: Completing the removal of the OWA Extensions ........ 182

Chapter 15 Configuring RPC over HTTP access to Enterprise Vault

About Enterprise Vault support for RPC over HTTP connections ........ 183
Summary of installation and configuration steps .............................. 185
Prerequisite tasks .................................................................................... 185
Installing OWA & RPC Extensions ..................................................... 188
Configuring an RPC proxy server (front-end Exchange Server) ......... 188
Configuring an RPC target server (back-end Exchange Server) ........ 189
Creating the EVServers.txt file ............................................................ 189
Configuration an RPC target Exchange Server ............................... 190
Configuring Enterprise Vault servers for RPC over HTTP ............ 191
ExchangeServers.txt file ................................................................. 191
Configuring an Anonymous user account for RPC over HTTP ....... 191
Configuring RPC over HTTP in Exchange Server mailbox policies ... 193
Section 3  Clustering Enterprise Vault

Chapter 16  Introducing clustering
Supported configurations and software ............................................................ 197
About the VCS GenericService agent ............................................................... 197
Typical Enterprise Vault configuration in a VCS cluster ............................ 198

Chapter 17  Installing and configuring VERITAS Storage Foundation HA
Installing and configuring VSFW HA ............................................................. 201
Managing disk groups and volumes ............................................................... 202

Chapter 18  Configuring the service group
Before you begin ............................................................................................. 205
Creating a service group ................................................................................ 206
Modifying an existing service group .............................................................. 213
Deleting a service group ................................................................................ 214

Chapter 19  Running the Enterprise Vault Configuration wizard
Before you begin ............................................................................................. 215
Setting up an active/passive configuration .................................................. 215
Adding cluster support in a first-time Enterprise Vault installation .......... 216
Upgrading an existing Enterprise Vault installation to a cluster ............... 219
Moving data to highly-available locations .................................................... 221
Setting up an N+1 configuration .................................................................... 224
N+1 configuration option 1 .......................................................................... 225
N+1 configuration option 2 .......................................................................... 226
Disallowing two Enterprise Vault servers on the same node ................... 227

Chapter 20  Implementing a VSFW HA-VVR disaster recovery solution
About the VSFW HA-VVR disaster recovery solution ................................. 229
Installing and configuring VSFW HA-VVR .................................................. 230
Setting up the cluster on the primary site .................................................... 230
Setting up the cluster on the secondary site ................................................. 231
Adding the VVR components for replication ............................................. 232
Adding the GCO components for wide-area recovery .............................. 232

Chapter 21  Troubleshooting clustering
VCS logging .................................................................................................... 235
Enterprise Vault Cluster Setup wizard error messages .............................. 236
Viewing the clustered message queues ......................................................... 236
Section 4 Setting up archiving

Chapter 22 Offline archives for offline users
- How the offline archive works .............................................................. 241
- Offline archive without Archive Explorer .......................................... 242
- Offline archive with Archive Explorer ............................................... 243
- Setting up offline archives ................................................................. 243
  - Configuring clients ......................................................................... 244

Chapter 23 Setting up archiving from mailboxes
- Creating a vault store and partition ..................................................... 245
- Adding an Exchange Organization ..................................................... 246
- Adding an Exchange Organizational Unit .......................................... 246
- Adding an Exchange Server ............................................................. 246
- Adding a Task Controller service ..................................................... 247
- Adding an archiving task .................................................................. 247
- Reviewing the Site archiving settings ................................................ 248
- Reviewing the mailbox policy settings .............................................. 248
  - Archiving Rules ............................................................................ 249
  - Archiving Actions ......................................................................... 249
  - Shortcut settings .......................................................................... 250
- Defining custom shortcut content ..................................................... 250
  - Layout of ShortcutText.txt .......................................................... 251
- Controlling the appearance of desktops ............................................ 253
- Creating Retention Categories ........................................................ 253
- Editing the Welcome message ........................................................ 254
- Editing the PST migration message .................................................. 254
- Editing Archive Usage Limit messages ............................................. 255
- Starting the Task Controller service and archiving task ................... 256
- Enabling mailboxes for archiving ..................................................... 256
- Installing the User Extensions on a server ...................................... 257
  - Users’ tasks .................................................................................. 257
- What next? ....................................................................................... 257

Chapter 24 Setting up archiving from public folders
- Creating a public folder archive ......................................................... 259
- Adding a Public Folder task .............................................................. 260
- Reviewing the public folder policy settings ...................................... 260
  - Archiving Rules ............................................................................ 260
  - Archiving Actions ......................................................................... 261
- Creating Retention Categories ........................................................ 261
Chapter 25  Setting up archiving of journaled messages

Preparation .........................................................................................................267
Creating a journal vault store ..........................................................................267
Creating a journal archive ................................................................................268
Adding permissions to the journal archive ....................................................268
Adding a Journaling task ..................................................................................269
Reviewing the journaling policy settings .......................................................269
Adding a journal mailbox as a target ..............................................................270
Starting the Journaling task .............................................................................270
What next? ..........................................................................................................271

Chapter 26  Setting up file system archiving

Introduction ........................................................................................................273
Installing the File Placeholder service ...........................................................273
Configuring the File Placeholder service .......................................................274
Setting file permissions ....................................................................................275
Editing the configuration file ...........................................................................275
What next? ..........................................................................................................275
Tips ...............................................................................................................276

Chapter 27  Configuring SharePoint archiving

Introduction ........................................................................................................277
Prerequisite software and settings ....................................................................278
SharePoint security certificates ........................................................................279
Obtaining and installing a SharePoint license ................................................279
Installing and configuring task order .............................................................279
Configuring the SharePoint server ................................................................280
Installing and configuring the Enterprise Vault components ......................280
Running the Configuration Program ...............................................................280
Installing the Archive Search Web Part ........................................................281
Installing Archive Search Web Part in a Web Server Farm .........................282
Configuring Enterprise Vault for SharePoint archiving ..............................284
Configuring the Internet Explorer security settings .....................................285
Creating a SharePoint task ..............................................................................285
Creating a SharePoint archiving policy .........................................................286
Assigning a vault store ................................................................. 288
Adding a SharePoint target virtual server ................................. 288
Creating target site collection objects ....................................... 290
Creating archiving target objects for subsites ...................... 292
Running the SharePoint archiving task ....................................... 293
Scheduling archive runs ................................................................. 294
Adding Web Parts and links to site pages ................................. 295
Adding the Archive Search Web Part to a site ...................... 295
Adding the archived version history link ................................. 295
Viewing and restoring archived documents ............................... 296
Using the version history page ..................................................... 296
Using the Archive Search Web Part ............................................. 297
Restoring a document using the Archive Search Web Part ...... 298
Using Archive Explorer ............................................................... 299
Internet Explorer settings for users ............................................. 299
Configuring “all-in-one” systems ................................................... 300

Chapter 28 Setting up Domino Journaling archiving
Preparation ...................................................................................... 301
Configuring Domino Journaling databases ............................ 302
Configuring access for Enterprise Vault ................................. 302
Adding a Domino domain ............................................................ 303
Adding a Domino server ............................................................... 304
Assigning a vault store ................................................................. 304
Creating a Domino Journal archive ........................................... 305
Adding permissions to the journal archive ............................... 305
Creating a Domino Journal policy .............................................. 306
Creating a Domino Journaling task ............................................. 306
Adding a Domino Journaling location ....................................... 306
Conflict with Microsoft Office 2003 ........................................... 307
Configuring clients ................................................................. 307

Chapter 29 Setting up SMTP archiving
Installing and configuring ............................................................. 310
Set up Microsoft SMTP Server .................................................. 311
Install the SMTP Archiving components ............................... 311
Create the holding area ............................................................... 312
Set up the SMTP Archiving configuration file ....................... 313
Example configuration file .......................................................... 317
Set up File System Archiving ..................................................... 318
Starting and stopping SMTP Archiving ................................. 318
Selecting the holding area folder to use ................................. 319
Section 5  Custom filtering and properties

Chapter 30  Introduction to filtering
Selecting Journaling .................................................................326
Group Journaling .................................................................327
Custom filtering .................................................................327
  Distributed Enterprise Vault environments .........................328
Custom properties ..............................................................328
Journal Filters with Envelope Journaling ...............................329

Chapter 31  Configuring filtering
Configuring selective journaling ........................................331
  Creating the selective journaling rules file ......................332
    Selective journaling filter rules ..................................332
  Adding selective journaling registry settings ..................333
    Managing invalid distribution lists ..............................334
Configuring group journaling .............................................335
  Creating the group journaling rules file ......................336
    Group journaling filter rules ...................................336
  Adding group journaling registry settings ...................337
    Testing group journaling settings ..............................337
Configuring custom filtering .............................................338
  Distributed Enterprise Vault environments ....................340
  Registry settings for Exchange Server journal filtering .......340
  Registry settings for Exchange Server user mailbox filtering ...342
  Registry settings for Exchange Server public folder filtering ...343
  Registry settings for Domino server journal filtering ..........344
About custom filtering ruleset files ...................................346
  Setting default filtering rules for all custom filtering ........347
  Setting filtering for individual Exchange Server mailboxes ...347
  Setting separate filtering rules for public folders ..........348
  Setting filtering for individual Domino journaling locations ..348
General format of ruleset files ........................................349
  Validating XML ruleset files ........................................351
Rule actions ...............................................................352
  Deleted Attachments.txt file .....................................354
  Assigning a retention category ..................................354
  Specifying a specific archive .....................................354
Message attribute filters ................................................355
  Filtering on message authors and recipients ..................355
Filtering on message direction ........................................................362
Filtering on message subject ............................................................364
Filtering on MAPI named properties ..............................................365
Attachment attribute filters ............................................................366
How message and attachment filters are applied ........................368
Example Ruleset File .........................................................................372

Chapter 32 Configuring custom properties
Controlling default settings .................................................................379
Setting IGNORENODEFAULT registry entry .................................379
Summary of default archiving actions ..............................................382
General format of custom properties.xml .........................................384
How to validate custom properties.xml ...........................................385
Defining additional properties to index ...........................................386
MAPI properties .............................................................................386
Domino properties .........................................................................388
Defining content categories .............................................................390
Assigning content categories in rules ...........................................392
Overriding default content category settings .....................................393
Defining how properties are presented in applications .......................393
Displaying custom properties in the browser search .......................396
Notes on displaying custom properties in browser search ..................398
Summary of Custom Property Elements and Attributes .................398

Section 6 Appendices
Appendix A Envelope Journaling
Format of Envelope Journaled messages .........................................405
Example 1: Message sent over SMTP .............................................406
Example 2: Message sent over an intranet .....................................407
Performance .......................................................................................409
Enterprise Vault and Envelope Journaling ........................................409
When recipients are stored as Undisclosed .......................................410

Appendix B Configuring NetBackup Server
Prerequisites .....................................................................................413
Setting client software path for NetBackup Server 6.0 .......................413
Creating a NetBackup Server Policy .................................................414
Preparation .........................................................................................414
Creating a new policy .......................................................................414
Policy properties — Attributes ..........................................................415
About this guide

This book describes how to install and configure a Symantec Enterprise Vault installation.

Prerequisite knowledge

To install and configure Enterprise Vault, you need a working knowledge of the following products:

- Windows® Server 2003 or Windows 2000® administrative tasks
- Microsoft SQL Server™
- Microsoft Message Queue Server
- Microsoft Outlook
- IIS (Internet Information Services)
- Your archive storage hardware and software

If you are going to be using Enterprise Vault with Domino server, Microsoft Exchange Server™ or Microsoft SharePoint™ Portal Server, you should also have a working knowledge of these products.

Formats available

This book is available as HTML Help and as an Adobe Acrobat (PDF) file on the Enterprise Vault CD-ROM. After installation, the documentation is also available in the Enterprise Vault program folder.

If you have yet to install the free Adobe Reader, you can download it from the Adobe Web site at http://www.adobe.com.
Typographical conventions

The following typographical conventions are used in this book:

Table 1-1  Typographical conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>This typeface</em></td>
<td>Is used when introducing a new term and for references to other books.</td>
</tr>
<tr>
<td><em>This typeface</em></td>
<td>Is used for dialog titles, labels and buttons.</td>
</tr>
<tr>
<td><em>This typeface</em></td>
<td>Is used for:</td>
</tr>
<tr>
<td></td>
<td>• File names and text file content</td>
</tr>
<tr>
<td></td>
<td>• Examples of what you type in</td>
</tr>
<tr>
<td></td>
<td>• Error text</td>
</tr>
</tbody>
</table>

Related documentation

The Enterprise Vault documentation is provided in the Documentation folder on the CD-ROM and, after installation, in the Administration Console help and in the Enterprise Vault installation folder. The table below lists the documentation that is supplied.

If required, you can install Adobe™ Acrobat Reader from the Redistributable Software folder on the Enterprise Vault CD-ROM.

The following guides, along with the online help, comprise the Enterprise Vault documentation set:

Table 1-2  Enterprise Vault documentation set

<table>
<thead>
<tr>
<th>Title</th>
<th>File name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction and Planning</td>
<td>Introduction_and_Planning.pdf</td>
</tr>
<tr>
<td></td>
<td>Introduction_and_Planning.chm</td>
</tr>
<tr>
<td>Installing and Configuring (this book)</td>
<td>Installing_and_Configuring.pdf</td>
</tr>
<tr>
<td></td>
<td>Installing_and_Configuring.chm</td>
</tr>
<tr>
<td></td>
<td>Administrators_Guide.chm</td>
</tr>
<tr>
<td>Utilities</td>
<td>Utilities.pdf</td>
</tr>
<tr>
<td></td>
<td>Utilities.chm</td>
</tr>
</tbody>
</table>
Table 1-2  Enterprise Vault documentation set (Continued)

<table>
<thead>
<tr>
<th>Title</th>
<th>File name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance Accelerator Installing and Configuring</td>
<td>CA_Installing_and_Configuring.pdf</td>
</tr>
<tr>
<td>Discovery Accelerator Installing and Configuring</td>
<td>DA_Installing_and_Configuring.pdf</td>
</tr>
<tr>
<td>Release Notes</td>
<td>ReadMeFirst.htm on the CD-ROM</td>
</tr>
</tbody>
</table>

For the latest information about Enterprise Vault, see the Enterprise Vault Web page at:
http://www.veritas.com/enterprisevault
Installing, configuring, and upgrading Enterprise Vault

The section includes the following chapters:

- Chapter 2, “Upgrading to Enterprise Vault 6.0 SP4” on page 23
- Chapter 3, “Before installing” on page 39
- Chapter 4, “Preinstallation tasks” on page 57
- Chapter 5, “Installing Enterprise Vault” on page 63
- Chapter 6, “Postinstallation tasks” on page 67
- Chapter 7, “Running the Configuration Program” on page 79
- Chapter 8, “Running the Administration Console” on page 85
- Chapter 9, “Setting up users’ desktops” on page 93
- Chapter 11, “Configuring OWA access to Enterprise Vault” on page 109
- Chapter 10, “Licenses and license keys” on page 105
Upgrading to Enterprise Vault 6.0 SP4

This chapter describes how to upgrade to Enterprise Vault 6.0 SP4. If you are performing a new Enterprise Vault installation, see the later chapters in this book for details of what to do.

Note: After you install Enterprise Vault 6.0 SP4 you must run the Configuration Program, even if you are upgrading from Enterprise Vault 6.0 or an Enterprise Vault 6.0 service pack.

Introduction

Servers must have Enterprise Vault 5.0 or Enterprise Vault 6.0 installed before you can upgrade to Enterprise Vault 6.0 SP4.

If you have a version of Enterprise Vault that is earlier than 5.0 then you must upgrade to Enterprise Vault 5.0 before you upgrade to 6.0 SP4.

You must upgrade the following to Enterprise Vault 6.0 SP4:

- All servers that are running Enterprise Vault services
- All computers that are running the Enterprise Vault Administration Console
- SharePoint servers

The User Extensions from Enterprise Vault 5.0 and later work with Enterprise Vault 6.0 SP4, so there is no technical reason requiring you to upgrade all client computers immediately. However, new client functionality will not be available until you do upgrade. You can upgrade Enterprise Vault clients to 6.0 SP4 from any earlier version of the software.
It is important that you do the correct preparation and follow the appropriate installation procedure:

- Upgrading Enterprise Vault servers: see “Upgrading to Enterprise Vault 6.0 SP4”
- Upgrade Enterprise Vault clients: see “Upgrading desktop clients”
- Upgrading SharePoint servers: see “Upgrading SharePoint Server”
- Upgrading OWA: see “Installing OWA Extensions on a back-end Exchange Server 2003” in Chapter 11, “Configuring OWA access to Enterprise Vault”.

**Upgrading to Enterprise Vault 6.0 SP4**

You can upgrade to Enterprise Vault 6.0 SP4 only from one of the following:

- Enterprise Vault 5.0. If you have an Enterprise Vault version earlier than Enterprise Vault 5.0 then you must upgrade to Enterprise Vault 5.0 before upgrading to Enterprise Vault 6.0 SP4.
  Note that, at the end of the upgrade from Enterprise Vault 5.0 all archiving tasks start automatically, even if the old archiving services were configured for manual start. If the new archiving tasks are within their scheduled periods, they begin archiving. When preparing for the upgrade, you may want to change the existing schedules so that tasks do not immediately start archiving when the upgrade is complete.

- Enterprise Vault 6.0.
- Enterprise Vault 6.0 SP1.
- Enterprise Vault 6.0 SP2.
- Enterprise Vault 6.0 SP3.

If you intend to upgrade an existing installation to a clustered environment you must first upgrade to Enterprise Vault 6.0 SP4 and then run the Convert to Cluster wizard as described in the chapter “Running the Enterprise Vault Configuration wizard”.

**Removing services that are no longer required**

During an upgrade from Enterprise Vault 5.0 to Enterprise Vault 6.0 SP4, existing Archiving, Journaling, and Public Folder services are converted to tasks and automatically started. Services that have been disabled are converted to tasks and then started.

If you have disabled services that you no longer need it is recommended that you remove them now, before upgrading.
See support article “273284, How to remove the Archiving, Retrieval, or Journaling service of VERITAS Enterprise Vault” for details of how to remove services that are no longer required.

Preparing the Enterprise Vault servers

Do the following on each computer that is running an Enterprise Vault service:

1. Check in MSMQ that there are no items on the Enterprise Vault Storage Archive queue. If there are items on this queue, wait for the Storage service to empty the queue before continuing.

2. Back up all Enterprise Vault databases in accordance with your normal backup procedures.

3. Log on as the Vault Service account.

4. Start the Windows Services manager.

5. Stop the Enterprise Vault Admin service. This stops the Admin service itself and also all other Enterprise Vault services, including the Enterprise Vault Directory service.

6. On any computer that runs a Shopping service, stop the IIS Admin service.

7. The installation procedure will overwrite the .MSG files in the language folders:
   - ApproachingArchiveQuotaLimit.msg
   - ArchiveQuotaLimitReached.msg
   - DisableMailboxMessage.msg
   - EnableMailboxMessage.msg
   - EnablePSTMigratedMessage.msg
   - PSTMigratedMessage.msg
   - Enterprise Vault\Languages\Mailbox Messages\<lang>

   where <lang> indicates the language used.
   - The installation does not modify the live versions of these files that you have in the Enterprise Vault program folder (normally C:\Program Files\Enterprise Vault). If you have made changes to the files in the <lang> folders that you want to keep, copy the files to another location.

Installing Enterprise Vault 6.0 SP4

You must be logged on as the Vault Service account in order to install Enterprise Vault 6.0 SP4.
The installation process does the following:

- Installs the Enterprise Vault 6.0 SP4 software.
- If you are upgrading from Enterprise Vault 5.0, backs up the Enterprise Vault registry entries to a file in the Enterprise Vault Reports folder (typically C:\Program Files\Enterprise Vault\Reports). The file name is:
  Upgrade50to60_RegistryBeforeMigration <date>.txt
  where <date> is the date and time that the log file was created.

To install the Enterprise Vault 6.0 SP4 software

1. Log on as the Vault Service account on the Directory Service computer.
2. Check in MSMQ that there are no items on the Enterprise Vault Storage Archive queue. If there are items on this queue, wait for the Storage service to empty the queue before continuing.
3. Insert the Enterprise Vault CD-ROM into the CD-ROM drive.
4. Double-click ReadMeFirst.htm in the top-level folder and read the contents before continuing.
5. Using Windows Explorer, open the folder \Enterprise Vault\Server.
6. Double-click the file Setup.exe to start the installation.
7. Work through the installation.
8. At the end of the installation, do not select the Run the Configuration option unless the Enterprise Vault 6.0 SP4 software has been installed on all the other servers in the site.
9. Install the Enterprise Vault software on the other computers in your Vault Site.
   The Enterprise Vault software upgrade is now complete, but you must obtain license keys for any additional services that you intend to run.
10. Work through the postinstallation section, “Postinstallation tasks”.

Starting the Directory service

After the upgrade installation on the Directory service computer you must start the Directory service.

To start the Directory service

1. Use Windows Services to start the Enterprise Vault Directory service.
2 When the Directory Service starts, it automatically upgrades the Directory Database schema. If you are upgrading from Enterprise Vault 5.0, the Directory Service also does the following during its start-up:

- Creates new default Exchange Server archiving policies
- Migrates existing Site Settings into the new default archiving policies.
- Leaves a log file in the Enterprise Vault Reports folder. The file name is:
  \(\text{Upgrade50to60\_SiteSettings} <\text{date}>.\text{txt}\)
  where \(<\text{date}>\) is the date and time the file was created.

3 Monitor the Enterprise Vault event log and wait for event 8576 to be logged:

   The Directory Service has completed the automatic upgrade of the EnterpriseVaultDirectory Database

4 Close the Windows Services applet.

   If you are upgrading from Enterprise Vault 5.0 and you fail to do this, any old Enterprise Vault services that have now been replaced by tasks may not be deleted until the computer is restarted.

---

### Running the Configuration Program

**Note:** Do not run the Configuration Program until you have installed the Enterprise Vault 6.0 SP4 software on all the Enterprise Vault servers in your Site.

After starting the Directory service on the Directory service computer you must run the Enterprise Vault Configuration program, also on the Directory service computer.

See the appropriate Configuration Program section, depending on the version of Enterprise Vault from which you are upgrading:

- Upgrading from Enterprise Vault 5.0
- Upgrading from Enterprise Vault 6.0

### Upgrading from Enterprise Vault 5.0

One of the Configuration Program’s jobs is to start the new Task Controller service, which then automatically does the following:

- Migrates settings from \(\text{DesktopSettings.txt}\) and the registry to the \(\text{Advanced}\) settings of the new default policies.
To run the configuration program:

1. Make sure that you have installed the Enterprise Vault 6.0 SP4 software on all Enterprise Vault servers in the Site and that the Enterprise Vault Admin service is running on each computer.

2. Check that:
   - The Directory service computer has network connectivity to all the servers in the Enterprise Vault site. For example, you could use the MS-DOS PING command to check that each server is available.
   - The Directory service has started on the Directory service computer and has completed its database upgrade, as described in “Starting the Directory service”.

3. Click Start > Programs > Enterprise Vault > Enterprise Vault Configuration to start the Configuration Program.

4. The only available option on the first screen of the Configuration Program is Upgrade this configuration. Click Next.

5. On the second screen, click Next to start the upgrade. There is a prompt for the Vault Service account password.

6. Enter the Vault Service account password and click OK. The Configuration Program shows a progress bar while it does the following:
   - Adds a Directory service to every Enterprise Vault server in the site.
   - Starts the new Task Controller service, which then automatically migrates settings as described above.
   - Converts existing services that archive from Exchange Server to tasks.
   - Changes the service names of Enterprise Vault services to be more readable to humans. This name is shown in the services’ property pages in the Windows Services applet.
   - The names of services that do not use the Vault Service account to log on are not changed.
   - Updates the Enterprise Vault DCOM settings on all servers in the Enterprise Vault Site.
   - Creates a log file of its actions in the Enterprise Vault Reports folder. The file name is: Upgrade50to60_ServicesToTasks <date>.txt
where \(<date>\) is the date and time the file was created.

7 At the end of the update, click **Finish** to close the Configuration Program.
Now go to “Upgrading the Exchange Server forms” on page 30 to continue with the upgrade tasks.

### Upgrading from Enterprise Vault 6.0

**To run the configuration program**

1 Make sure that you have installed the Enterprise Vault 6.0 SP4 software on all Enterprise Vault servers in the Site and that the Enterprise Vault Admin service is running on each computer.

2 Check that:
   - The Directory service computer has network connectivity to all the servers in the Enterprise Vault site. For example, you could use the MS-DOS PING command to check that each server is available.
   - The Directory service has started on the Directory service computer and has completed its database upgrade, as described in “Starting the Directory service”.

3 Once the Directory service has started, on the Directory service computer click **Start > Programs > Enterprise Vault > Enterprise Vault Configuration** to start the Configuration Program.

4 The only available option on the first screen of the Configuration Program is **Upgrade this configuration**. Click **Next**.

5 On the second screen, click **Next** to start the upgrade. There is a prompt for the Vault Service account password.

6 Enter the Vault Service account password and click **OK**.
   The Configuration Program shows a progress bar while it carries out the configuration, including:
   - Adding a Directory service to every Enterprise Vault server in the site.
   - Adding new policy settings.
   - Changing the service names of Enterprise Vault services to be more readable to humans. This name is shown in the services' property pages in the Windows **Services** applet.

7 At the end of the update, click **Finish** to close the Configuration Program.
Now go to “Upgrading the Exchange Server forms” on page 30 to continue with the upgrade tasks.
Postinstallation tasks

Manually changing Enterprise Vault DCOM settings
Work through this section if the Configuration Program warned you that there was an error updating the DCOM settings of Enterprise Vault servers. If there was no such warning you can ignore this section.

To update DCOM settings
1. Make sure that the Enterprise Vault Admin service is running on all Enterprise Vault servers in the Site.
2. Start the Enterprise Vault Administration Console
3. In the left pane of the Administration Console, right-click the Directory icon and then, on the shortcut menu, click Properties.
4. In the Directory Properties, click the Service Account tab.
5. Enter the password for the account and enter it again to confirm it.
6. Click OK.

Upgrading desktop clients
The User Extensions are not available as part of the server installation. There is a separate installation for the User Extensions.

Upgrading the Exchange Server forms
To install forms in the Organization Forms Library, you must use an account that has Owner permissions on the folder in which you are installing the forms. Do this on the computer where you have installed the Microsoft Exchange forms from the Enterprise Vault kit.
You can install the forms from Microsoft Outlook using a mailbox that has Owner permissions for the folder in the Organization Forms Library.
To install the forms, see the following section.

Note: If you ever need to reinstall the new forms, EVPendingArchive.fdm, EVShortcut.fdm, EVPendingDelete.fdm, and EVPendingRestore.fdm, uninstall the existing copies first, rather than installing the forms on top of the existing copies.
Upgrading forms

From Microsoft Outlook, do the following:

1. On the **Tools** menu, click **Options**.
2. Click the **Other** tab.
3. Click **Advanced Options**.
4. Click **Custom Forms**.
5. Click **Manage Forms**.
6. On the right-hand side of the dialog box, click the **Set** button.
7. Click **Forms Library** and select the folder where you want to install the forms. Click **OK**.
8. Click the **Install** button.
9. Select the **Forms** subfolder in the Enterprise Vault **Program** folder.
10. Select the language folder that is appropriate to the language of the forms you want to install.
11. Change the **Files to type filter** to **Form Message (*.fdm)**.
12. Double-click **EVPendingArchive.fdm** and review the displayed properties to check that this is the Enterprise Vault Item.
13. Click **OK**.
14. Click the **Install** button.
15. Change the **Files to type filter** to **Form Message (*.fdm)**.
16. Double-click **EVShortcut.fdm** and review the displayed properties to check that this is the Enterprise Vault Shortcut.
17. Click **OK**.
18. Click the **Install** button.
19. Change the **Files to type filter** to **Form Message (*.fdm)**.
20. Double-click **EVPendingRestore.fdm** and review the displayed properties to check that this is the Enterprise Vault Restore Pending Item.
21. Click **OK**.
22. Click the **Install** button.
23. Change the **Files to type filter** to **Form Message (*.fdm)**.
24. Double-click **EVPendingDelete.fdm** and review the displayed properties to check that this is the Enterprise Vault Delete Pending Item.
25 Click **OK**.

### Upgrading desktop clients

The User Extensions are not available as part of the server installation. There is a separate installation for the User Extensions.

### Upgrading the self-installing user extensions

If you have users of the self-installing User Extensions follow the instructions in this section to make the new version available to users. They will be automatically given the option to install new version when they click Enterprise Vault shortcuts.

The self-installing version of the User Extensions is an ActiveX control that enables users to use shortcuts and to search archived items. The normal User Extensions currently has more functionality than the self-installing User Extensions.

The self-installing User Extensions enables users to open Enterprise Vault shortcuts, search for archived items, and read the archived items.

There is no other functionality available in Outlook itself, so users cannot make changes to any Enterprise Vault folder properties and no Enterprise Vault buttons or menu options are available.

Users can, of course, use the Enterprise Vault Web Access application to restore archive items to their mailboxes and, if allowed, delete archived items from their archives.

For details of how to make the self-installing User Extensions available to your users, see “Making the Self-Installing User Extensions available” on page 96.

To upgrade the self-installing User Extensions you must do the following:

- Copy the files into an IIS Virtual Directory; see “Copying the files” on page 33.
- Edit the Enterprise Vault Archived Item form to enable the automatic installation of the self-installing User Extensions; see “Editing the archived item form” on page 33.
- Test that the edited form works correctly; see “Testing the edited form” on page 34.
- If necessary, publish the self-installing User Extensions in Active Directory®; see “Publishing in Active Directory” on page 35.
Copying the files

When you install the Enterprise Vault services or the Administration Console the Self-Installing User Extensions files are copied to the Enterprise Vault languages folder on your computer. This folder is normally:

C:\Program Files\Enterprise Vault\Languages\Self-Installing User Extensions\<language>

where <language> indicates the language used in the files.

Copy the complete language folder to the IIS Virtual Directory from which users download the current Self-Installing User Extensions.

Editing the archived item form

You must edit the Archived Item form so that it includes a pointer to the IIS Virtual Directory that contains the language folder with the downloadable files. Once you have edited the form you need to install it in the Organization Forms Library, so you must use an account that has Owner permissions on the Organization Forms folder.

You can install the form from Microsoft Outlook using a mailbox that has Owner permissions for the folder in the Organization Forms Library.

To edit the form

1. From Outlook, do the following:
   a. On the Tools menu, click Options.
   b. Click the Other tab.
   c. Click Advanced Options.
   d. Click Custom Forms.
   e. Click Manage Forms.
2. On the left-hand side of the dialog box, click the Set button.
3. Click Forms Library and select Organization Forms.
4. On the right-hand side of the dialog box, click the Set button.
5. Click Forms Library and select Personal Forms.
6. In the list of Organization Forms, select Enterprise Vault – Archived Item.
7. Click Copy.
   The Archived Item form is copied to your Personal Forms library.
8 Click **Close** and then exit from all the dialog boxes.

9 On the Outlook Tools menu, click **Forms** and then **Design a Form**.

10 Next to **Look In**, select **Personal Forms Library**.

11 Click **Enterprise Vault – Archived Item**.

12 Hold down the **Shift** key and click **Open**.
   
   The form opens, ready for you to make changes.

13 On the **Form** menu click **View Code**.

14 Scroll down the form to the Enterprise Vault Administrator section.

15 Find the following line:
   
   ```
   Const USE_SELF_INSTALLING_USER_EXTENSIONS=False
   ```

16 On this line, change **False** to **True**:
   
   ```
   Const USE_SELF_INSTALLING_USER_EXTENSIONS=True
   ```

17 Find the following line:
   
   ```
   Const DOWNLOAD_URL = "http://yourdomainhere"
   ```

18 On this line, change the URL so that it points to the IIS Virtual Directory that contains the language folder with the downloadable files.

19 On the form toolbar, click the **Publish Form** icon:
   
   The form is saved in your Personal Forms Library.

---

**Testing the edited form**

In order to test the form, you need a shortcut to an archived item and a computer that does not have the User Extensions installed.

1 If the computer has been used to open shortcuts before it will have a cached version of the Archived Item form. If this is the case, do the following:

   a Close Outlook.

   b Delete the Outlook, FRMCACHE.DAT. This is normally in C:\WINNT\forms\ 

   c Start Outlook.

2 Double-click a shortcut to an archived item. A message gives you the option of downloading the self-installing User Extensions. Click **Yes** to download and install the software.

---

**Publishing the edited form**

1 From Outlook, do the following:
Upgrading to Enterprise Vault 6.0 SP4
Upgrading the self-installing user extensions

a  On the Tools menu, click Options.
b  Click the Other tab.
c  Click Advanced Options.
d  Click Custom Forms.
e  Click Manage Forms.
2  On the left-hand side of the dialog box, click the Set button.
3  Click Forms Library and select Personal Forms.
4  On the right-hand side of the dialog box, click the Set button.
5  Click Forms Library and select Organization Forms.
6  In the list of Personal Forms, select Enterprise Vault - Archived Item.
7  Click Copy.
   The Archived Item form is copied to the Organization Forms library.

Publishing in Active Directory

1  Click Start, Programs, Administrative Tools, Active Directory Users and Computers.
2  In the left panel, navigate to the Organization Unit to which you want to make the self-installing User Extensions available.
3  Right-click the Organization Unit and, on the shortcut menu, click Properties.
4  Click the Group Policy tab.
5  Click New.
6  Enter a name for the new package, for example, "EV Desktop Rollout".
7  Click Edit.
8  On the left, under User Configuration Software Settings, click Software Installation.
9  Click the Action menu and then New, and then Package.
10 Select the MSI file and click Open.
11 The Deploy Software window opens.
12 Select Published and click OK.
   The new package appears in the list of software installations.
**Upgrading OWA 2000 extensions**

The OWA computer (back end) requires either Windows 2000 SP3 or a Microsoft hotfix because of a problem with IIS 5.0. The problem is described in Microsoft support article 294833.

Prior to the release of Windows 2000 SP3 there was a Microsoft hotfix to correct this problem. If you do not want to install Windows 2000 SP3 you may be able to obtain a copy of the hotfix.

---

**Upgrading SharePoint Server**

To upgrade SharePoint Server

1. Stop the Enterprise Vault Admin Service.
2. Restart IIS.
3. Run the Enterprise Vault setup program:
   a. Load the Enterprise Vault CD-ROM on your SharePoint server computer.
   b. Open the Enterprise Vault folder.
   c. Open the Server folder.
   d. Double-click SETUP.EXE to start the installation.
   e. Select Microsoft SharePoint Components. If you are installing only the Enterprise Vault SharePoint components on this computer, clear the check boxes for other Enterprise Vault components.
   f. Click Next.
   g. Work through the remainder of the setup wizard.
4. Restart IIS again.
5. Reinstall the archived version history link:
   a. In a browser, enter the URL:
      
      ```
      http://spcomputername/_layouts/1033/versionsadmin.asp
      ```
      
      where spcomputername is the name of your SharePoint server computer.
      
      This displays the page Enterprise Vault Archived Version History Administration.
   b. Click Remove the archived version history link.
c Click **Install the archived version history link**.
   A progress window is displayed briefly while the link is being installed.
   No confirmation message is displayed when installation is complete.
   Note that you need to perform this task only once for all of the SharePoint servers.

6 Start the Enterprise Vault Admin Service.

**Upgrading internet security settings for users**

You may need to modify the Internet Explorer security settings of your users.
See “**Internet Explorer settings for users**” on page 299 for details of the required settings.
Upgrading to Enterprise Vault 6.0 SP4

Upgrading SharePoint Server
Before installing

Read this chapter to find out:

■ The prerequisites needed before you can install Enterprise Vault:
  ■ Operating system requirements
  ■ Requirements for users’ computers
  ■ Disk space requirements
■ The order in which to install prerequisite software before installing Enterprise Vault

For full details of all the supported versions of prerequisite software, see the Enterprise Vault Certification Tables.

Operating system requirements

Not all the components of Enterprise Vault can be installed on all types of operating system, as follows:

■ You can install all the components of Enterprise Vault on:
  ■ Windows Server 2003 Enterprise Edition
  ■ Windows 2000 Server
  ■ Windows 2000 Advanced Server
  ■ Windows 2000 Datacenter Server
■ On Windows XP Professional or Windows 2000 Professional you can install:
  ■ Administration Console
  ■ User Extensions
  ■ Microsoft Exchange Forms

Note that Enterprise Vault Archive Explorer feature requires that the Enterprise Vault server is running Windows 2000 or later.
Basic hardware requirements

To install Enterprise Vault, a computer with TCP/IP installed and configured is required. The computer must have a registered IP address with DNS (Domain Name System) properties for the TCP/IP protocol set up.

The minimum physical memory required for Enterprise Vault servers running a production system is 1 GB. For best performance, a minimum of 4 GB is recommended.

If performance is not an issue, it is possible to run demonstrations using less than 1 GB, but the computer must be configured to have at least 1 GB of page file space.

Enterprise Vault requires access to SQL Server and, for mailbox archiving, Exchange Server. In most configurations, Enterprise Vault, SQL server and Exchange server will each be installed on separate computers. However, for pilot or demonstration configurations, some or all of the servers can be installed on the same computer.

Storage requirements

You are not restricted to any particular storage product for use with Enterprise Vault.

Enterprise Vault is designed to operate with various types of storage solution provided by third party software and hardware products. Archived data can be directed to:

- An NTFS volume
- A Network Share that appears on the network as an NTFS volume
- An EMC Centera™ device
- A SnapLock™ (WORM) device

Data may in turn be migrated to secondary and tertiary storage systems that are managed by third party hierarchical storage management (HSM) software, for example.

Disk space requirements

During installation you will require 70MB of disk space to install all the Enterprise Vault components.

After installation you will need disk space to accommodate the following data:

- The Vault Directory Database.
Before installing

The Vault Directory database requires 10MB for the data device and 25MB for the Transaction log device, making a total disk space requirement of 35MB.

This space is required on the Vault Directory computer.

■ The vault store databases.
Each vault store database has an initial storage requirement of 100MB for the data device and 80MB for the transaction log device, making a total initial disk space requirement of 180MB for each vault store database.

This space is required on the Microsoft SQL Server. Ensure that there is adequate space for database devices to grow as data is added. Transaction logs should be limited to an appropriate size for your back-up and maintenance plan.

A basic sizing guide for each vault store database is 300 bytes for each item archived plus 5 GB for static data, transaction logs and temporary data fluctuations.

■ The vault stores.
This space is required on the Storage service computer.

■ The indexes.
This space is required on the Indexing service computer.

■ The shopping baskets.
This space is required on the Shopping service computer.

Installation order

The order in which you install prerequisite software sometimes causes problems. The general rule is that it is best to install products in the order in which they were released.

The following tables show examples of the installation order when you are setting up different Enterprise Vault installations:


■ Typical installation order for a standalone Administration Console for administering Enterprise Vault on Windows 2000 or later.

■ Typical installation order for an Enterprise Vault server with Windows Server 2003 or Windows 2000 and communicating with Domino.

In the following tables, it is assumed that Enterprise Vault, SQL Server and Exchange Server are installed on separate computers. Notes are included to
cover pilot or demonstration configurations, where some or all of the servers are installed on the same computer.

**Table 3-1**  Typical installation order for an Enterprise Vault server system on Windows Server 2003 and Windows 2000 communicating with Exchange Server 2003 or Exchange 2000 Server

<table>
<thead>
<tr>
<th>Step</th>
<th>Software to install</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>See “Notes on installation” on page 46.</td>
</tr>
<tr>
<td>2</td>
<td>Outlook 2003</td>
<td>Also needs the CDO components if the computer will not have Exchange Server installed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Installing Outlook on the Enterprise Vault computer” on page 49</td>
</tr>
<tr>
<td>3</td>
<td>SQL Server 2000 or 2005 (SQL server will usually be installed on a separate computer)</td>
<td>Note if both Enterprise Vault and SQL Server are installed on the same Windows Server 2003 computer, you will need at least SQL Server 2000 with Service Pack 3.  Enterprise Vault works with Windows Authentication mode and with Mixed Mode Authentication.  This must be a case-insensitive SQL installation. Case-sensitive SQL installations are not supported.</td>
</tr>
<tr>
<td>4</td>
<td>On Windows 2000 only, install Service Pack 3</td>
<td></td>
</tr>
</tbody>
</table>
Before installing

Installation order

5 Server Manager for Exchange Server 2003 or Exchange 2000

Note that if both Enterprise Vault and Exchange server are to be on the same computer, you would also install Exchange Server 2003 or Exchange 2000 Server. The version you will require depends on the operating system running on the Enterprise Vault computer and the version of Exchange being managed. To find out the version you need to install, see “Exchange System Manager on Enterprise Vault servers” on page 49.


6 MSXML

Supplied in the Redistributable Software folder on the Enterprise Vault CD-ROM. Alternatively, install Internet Explorer 6, which includes MSXML.

“MSXML Requirement for Enterprise Vault servers” on page 53.

7 Microsoft Data Access Components (MDAC)

Use version 2.6 or later. Supplied in the Redistributable Software folder on the Enterprise Vault CD-ROM.

A suitable version is installed automatically with Windows Server 2003.

8 Microsoft .NET Framework v1.1 or later

Redistributable Software folder on the Enterprise Vault CD-ROM. To install, double-click dotnetredist.exe, which unpacks the file dotnetfx.exe. Then double-click dotnetfx.exe.


Table 3-1 Typical installation order for an Enterprise Vault server system on Windows Server 2003 and Windows 2000 communicating with Exchange Server 2003 or Exchange 2000 Server

<table>
<thead>
<tr>
<th>Step</th>
<th>Software to install</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Server Manager for Exchange Server 2003 or Exchange 2000</td>
<td>Note that if both Enterprise Vault and Exchange server are to be on the same computer, you would also install Exchange Server 2003 or Exchange 2000 Server. The version you will require depends on the operating system running on the Enterprise Vault computer and the version of Exchange being managed. To find out the version you need to install, see “Exchange System Manager on Enterprise Vault servers” on page 49. Note that you must install Exchange Server 2003 Server Manager on a Windows Server 2003 computer. Do not install Server Manager for Exchange 2000 on an Enterprise Vault server that is running Windows Server 2003.</td>
</tr>
<tr>
<td>6</td>
<td>MSXML</td>
<td>Supplied in the Redistributable Software folder on the Enterprise Vault CD-ROM. Alternatively, install Internet Explorer 6, which includes MSXML. “MSXML Requirement for Enterprise Vault servers” on page 53.</td>
</tr>
</tbody>
</table>
Before installing

### Installation order

a. If the Enterprise Vault Server and Exchange Server are on the same computer, the NNTP and SMTP services need to be installed.

<table>
<thead>
<tr>
<th>Step</th>
<th>Software to install</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 1    | Windows             | One of:  
  - Windows 2000 Professional  
  - Windows 2000 Server (with service pack 3)  
  - Windows XP Professional  
  - Windows Server 2003 |
| 4    | Server Manager for Exchange 2000 or Exchange Server 2003 | The version you will require depends on the operating system running on the Enterprise Vault computer and the version of Exchange being managed. To find out the version you need to install, see “Exchange System Manager on Enterprise Vault servers” on page 49. |
| 6    | Microsoft .NET Framework v1.1 or later | Redistributable Software folder on the Enterprise Vault CD-ROM. To install, double-click dotnetredist.exe, which unpacks the file dotnetfx.exe. Then double-click dotnetfx.exe. A suitable version is installed automatically with Windows Server 2003. Make sure ASP.NET is selected, as described in “Notes on installation” on page 46 |
### Table 3-3

Typical installation order for an Enterprise Vault server with Windows Server 2003 or Windows 2000 and communicating with Domino

<table>
<thead>
<tr>
<th>Step</th>
<th>Software to install</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 1    | Windows Server 2003 or Windows 2000 (with service pack 3) | Any suitable version:  
  - Windows 2000 Server  
  - Windows 2000 Advanced Server  
  - Windows 2000 DataCenter Server  
  - Windows Server 2003 Enterprise Edition  
  See “Notes on installation” on page 46. |
| 2    | SQL Server 2000 or 2005 (SQL server will usually be installed on a separate computer) | Note if both Enterprise Vault and SQL Server are installed on the same Windows Server 2003 computer, you will need at least SQL Server 2000 with Service Pack 3.  
  Enterprise Vault works with Windows Authentication mode and with Mixed Mode Authentication.  
  This must be a case-insensitive SQL installation.  
  Case-sensitive SQL installations are not supported. |
| 3    | On Windows 2000 only, install Service Pack 3 |  |
| 4    | MSXML | Supplied in the Redistributable Software folder on the Enterprise Vault CD-ROM.  
  Alternatively, install Internet Explorer 6, which includes MSXML.  
  See “MSXML Requirement for Enterprise Vault servers” on page 53. |
| 5    | Microsoft Data Access Components (MDAC) | Use version 2.6 or later. Available from the Redistributable Software folder on the Enterprise Vault CD-ROM.  
  A suitable version is installed automatically with Windows Server 2003 |
Before installing

Notes on installation

Install Windows with the following options:

- NTFS file system
- Message Queuing services. See “Installing MSMQ” on page 46 and “MSMQ when Enterprise Vault is on Active Directory controller” on page 47.
- .NET Framework
- IIS with Active Server Pages enabled.

On Windows Server 2003, additional steps are needed to enable ASP.NET and configure Active Server Pages. See “.NET Framework and Active Server Pages on Windows 2003” on page 48.

Installing MSMQ

If you want to install Enterprise Vault services on more than one computer in the network, you must set up MSMQ on each computer.

There can be more than one MSMQ site in an MSMQ organization. The Archiving, Public Folder, and Journaling tasks all use MSMQ to communicate with the Storage service. You can install these tasks all on the same computer or on separate computers.

The steps for installing MSMQ on Windows Server 2003 and Windows 2000 are different. Follow the instructions below for your operating system.

For more information about how to set up MSMQ, see the Windows Help.

### Table 3-3

<table>
<thead>
<tr>
<th>Step</th>
<th>Software to install</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Microsoft .NET Framework v1.1 or later</td>
<td>Available from the redistributable Software folder on the Enterprise Vault CD-ROM. To install, double-click dotnetredist.exe, which unpacks the file dotnetfx.exe. Then double-click dotnetfx.exe. A suitable version is installed automatically with Windows Server 2003. See “Notes on installation” on page 46.</td>
</tr>
<tr>
<td>7</td>
<td>Lotus Notes Client</td>
<td>Must be installed and run to complete its configuration wizard.</td>
</tr>
</tbody>
</table>
To install MSMQ on Windows Server 2003

1. In the Windows Control Panel, double-click Add/Remove Programs.
2. Select Application Server and then click Details to open the Application Server window.
4. Select Message Queuing checkbox, and then click Details to display the Message Queuing dialog box.
5. As installing MSMQ with Active Directory Integration affects the performance of Enterprise Vault, you are strongly recommended to clear the Active Directory Integration checkbox in the Message Queuing dialog box.
6. Click OK twice to return to the Windows Components wizard.
7. Follow the remaining instructions in the wizard.

To install MSMQ on Windows Server 2000

1. In the Windows Control Panel, double-click Add/Remove Programs.
2. Click Add/Remove Windows Components. The Windows Components wizard starts.
3. Click Next.
4. Select the Message Queuing Services checkbox, and then click Next. The Message Queuing Installation wizard starts.
5. In the Message Queuing Installation wizard, click Message Queuing server.
6. If the computer is an Active Directory controller, click Next to complete the installation.
   - If the computer is not an Active Directory controller, you get the following prompts:
     - Select the Manually select access mode to Active Directory checkbox and click Next.
     - Select Message Queuing will not access a directory service and click Next.
7. Follow the remaining instructions in the wizard.

MSMQ when Enterprise Vault is on Active Directory controller

Note: You do not need to perform these steps if Enterprise Vault is not installed on the Active Directory Controller.
If the Enterprise Vault server is to be installed on the Active Directory Controller, you must perform the following steps to configure Microsoft Message Queue Security to give permissions to the Administrators group. This enables the Vault Service account to access the queues that it needs. You need administration privileges in order to do this.

1. Click Start, Programs, Administrative Tools, Computer Management.
2. In the left-hand pane, double-click Computer Management, Services and Applications.
3. Right-click Message Queuing and, on the shortcut menu, click Properties. The Message Queuing Properties window appears.
4. Click Add. The Select Users, Computers, or Groups window appears.
5. Next to Look In, select Entire Directory.
6. In the list, click Administrators and then Add.
7. Click OK to go back to the Message Queuing Properties window.
8. Click Administrators.
9. Under Permissions, click the Allow checkbox next to Full Control.
10. Click OK.

.NET Framework and Active Server Pages on Windows 2003
On Windows 2000, when you install IIS and .NET Framework, Active Server Pages and ASP.NET are enabled by default. However, on Windows Server 2003, you need to enable these manually.

To enable Active Server Pages and ASP.NET manually
1. Open Add/Remove Programs and select Add/Remove Windows Components.
2. Ensure Message Queuing Services and ASP.NET are selected.
3. To install required components and enable Active Server Pages, select Application Server and click Details.
4. Select Internet Information Services (IIS) and click Details.
5. Scroll down to World Wide Web Service. Click this and then Details.
6. Select Active Server Pages and click OK.
7. Click OK to close the dialog boxes until you get back to the Windows component list.
8 Click **Next** to install the additional components.
9 Click **Finish**.

**To check that Active Server Page scripts can run**
1 Start the IIS Manager by clicking **Start**, **Programs**, **Administrative Tools**, **IIS Manager**.
2 Click **Web Service Extensions**.
3 Check that **Active Server Pages** are **Allowed**.

**Allowing HTML items larger than 4MB to be downloaded**
By default, IIS 6 on Windows Server 2003 prevents any file larger than 4MB from being downloaded.
When users view archived items in their browser using OWA, Enterprise Vault web access application or customized shortcuts, an HTML version of the item is downloaded to their browser. This limit will prevent users from viewing any HTML items that exceed 4 MB.

**To view details on how to change this limit**
1 Open **Internet Information Services (IIS) Manager**.
2 Click Help.
3 Search for **AspBufferingLimit**.
4 You want the occurrence found in the Troubleshooting section.

**Installing Outlook on the Enterprise Vault computer**
When you install Outlook on the Enterprise Vault server, you must create a profile and connect to an Exchange server mailbox before you install Enterprise Vault.
Outlook may display an error message about a conflicting program. If Outlook offers to fix the problem, click **Yes** and then follow the instructions given.
See the *Administrator's Guide* for information on MAPISVC.INF problems.

**Exchange System Manager on Enterprise Vault servers**
Enterprise Vault servers with an Archiving task, Journaling task, or Storage service must have the Exchange System Manager tools and fixes shown below. This ensures that the Enterprise Vault server has more resilient MAPI software than is supplied by default. The software you need to install is shown in "**Required Exchange System Manager versions**" on page 50. Please check the
ReadMeFirst file on your Enterprise Vault release CD-ROM for any late updates to this information.

Note: You cannot use Exchange System Manager on an Enterprise Vault server to manage Exchange Server. The version of mapi32.dll used by Enterprise Vault is not compatible with that required by Exchange System Manager.

Table 3-4 Required Exchange System Manager versions

<table>
<thead>
<tr>
<th>Operating system on Enterprise Vault server</th>
<th>Exchange Server version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2000 Server</td>
<td>5.5</td>
</tr>
<tr>
<td></td>
<td>Exchange Server 2000</td>
</tr>
<tr>
<td></td>
<td>Exchange System Manager.</td>
</tr>
<tr>
<td></td>
<td>If archiving from</td>
</tr>
<tr>
<td></td>
<td>a computer that is</td>
</tr>
<tr>
<td></td>
<td>running Exchange Server 5.5, include support for Exchange Server 5.5</td>
</tr>
<tr>
<td></td>
<td>Exchange 2000</td>
</tr>
<tr>
<td></td>
<td>Server Service Pack 3</td>
</tr>
<tr>
<td></td>
<td>Exchange 2000</td>
</tr>
<tr>
<td></td>
<td>Post-Service Pack 3 (SP3)</td>
</tr>
<tr>
<td></td>
<td>Rollup Patch 6487.1</td>
</tr>
<tr>
<td></td>
<td>Exchange 2000</td>
</tr>
<tr>
<td></td>
<td>Server Service Pack 3</td>
</tr>
<tr>
<td></td>
<td>Exchange 2000</td>
</tr>
<tr>
<td></td>
<td>Post-Service Pack 3 (SP3)</td>
</tr>
<tr>
<td></td>
<td>Rollup Patch 6487.1</td>
</tr>
</tbody>
</table>

|                                          | 2000                     |
|                                          | Exchange Server 2000     |
|                                          | Exchange System Manager. |
|                                          | Exchange 2000 Service    |
|                                          | Pack 3                   |
|                                          | Exchange 2000 Service     |
|                                          | Pack 3 (SP3)             |
|                                          | Rollup Patch 6487.1      |

|                                          | 2003                     |
|                                          | Exchange Server 2000     |
|                                          | Exchange System Manager. |
|                                          | Exchange 2000 Service     |
|                                          | Pack 3                   |
|                                          | Exchange 2000 Post-Service |
|                                          | Pack 3 (SP3)             |
|                                          | Rollup Patch 6487.1      |
Before installing

The Vault Service account

Configuring Application Pool accounts

In IIS, you can configure the level of isolation for particular web applications. For shopping baskets in the Enterprise Vault web access application to be created correctly, the application needs to run under the predefined Local System account.

The configuration program will automatically set the correct isolation and account settings. You do not need to configure this.

If you have IIS 6.0 installed, the configuration program will create a new Application Pool, EnterpriseVaultAppPool, for the web access application and assign the Local System account to that pool.

The Vault Service account

The Vault Service account is used by Enterprise Vault processes to access the Windows server operating system. The Enterprise Vault services, which are Windows services, run under this account.

The Vault Service account is shared by all the Enterprise Vault computers in the Enterprise Vault directory. If you are managing multiple Enterprise Vault sites, you can use the same Vault Service account for more than one Enterprise Vault site.

If you are using Exchange Server 2003 or Exchange 2000 Server, the Vault Service account must be a member of the Active Directory domain.

---

Table 3-4  Required Exchange System Manager versions

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2003</td>
<td>Enterprise System Manager or Exchange Server 2003</td>
<td>Enterprise System Manager or Exchange Server 2003</td>
<td>Enterprise System Manager or Exchange Server 2003</td>
</tr>
<tr>
<td></td>
<td>Exchange System Manager or Exchange Server 2003</td>
<td>Exchange System Manager or Exchange Server 2003</td>
<td>Exchange System Manager or Exchange Server 2003</td>
</tr>
<tr>
<td></td>
<td>Service Pack 1 (SP1)</td>
<td>Service Pack 1 (SP1)</td>
<td>Service Pack 1 (SP1)</td>
</tr>
</tbody>
</table>
“Creating the Vault Service account” on page 57 for details on how to set up this account.

You are recommended to be logged in to the Vault Service account when you install and administer Enterprise Vault.

The Vault Service account must be a domain-based Windows security account that belongs to the local Administrators group on all computers in the directory. The account password must not be blank.

We recommend that you do not make this account a Domain Administrator. It is better to assign Exchange Server permissions explicitly, as described in “Assigning Microsoft Exchange Server permissions” on page 60.

The account does not need a mailbox, but you may want to create one and use it for the service mailbox, described in “The service mailbox” on page 53.

If possible, create the account so that it is in the same domain as the Enterprise Vault computers. If it is necessary for the Vault Service account and the Enterprise Vault computers to be in different domains, create the account so that it is in a domain that is trusted by the Enterprise Vault computers’ domain.

During configuration, you are asked to provide the name and password of the Vault Service account. Enterprise Vault automatically grants the Vault Service account the following advanced user rights:

- Log On As a Service
- Act As Part Of The Operating System
- Debug programs
- Replace a process-level token

The Vault Site alias

The Vault Site alias is a DNS entry for an Enterprise Vault site. Each Enterprise Vault site should have a Vault Site alias, which is used by the Enterprise Vault software to refer to the Enterprise Vault site by name. The DNS entry is an alias whose value is the name of the computer that runs the Vault Directory Service for the site.

“Creating the Vault Site alias” on page 62 for more information on how to set up this alias.

Using a DNS alias serves two purposes:

- If the Vault Directory is shared between more than one Enterprise Vault site, it allows the configuration information for each of the Enterprise Vault sites to be distinguished.
Before installing The service mailbox

- It allows future flexibility if you change the computer that is running the Vault Directory service.

If you are setting up Enterprise Vault as a pilot system, to avoid the need of creating a temporary DNS entry you can configure Enterprise Vault without a Vault Site alias. Instead, you must supply a full and valid DNS name of the Directory Service computer when prompted for the Vault Site alias. In all other situations use a Vault Site alias for the site.

To use a DNS alias, you must set it up before starting the configuration. If you do not have access to the DNS Server in your organization you may need to request a DNS alias from your network manager.

The service mailbox

The service mailbox is a mailbox that is used by the Archiving, Journaling, and Public Folder tasks.

The tasks require exclusive use of this mailbox, so it must not be used for any other purpose.

The mailbox must not be hidden from address lists and, on Windows Server 2003 and Windows 2000, the account must not be disabled.

If you have the privileges to create new mailboxes, then the Enterprise Vault configuration program can create the mailbox automatically when you are running the configuration program.

If you do not want the configuration program to create the mailbox, you can create the mailbox before running the configuration program and then, when prompted for a mailbox, select the mailbox you created.

MSXML Requirement for Enterprise Vault servers

All Enterprise Vault server computers require MSXML, which you can obtain by installing one of the following:

- Internet Explorer 6
  You need only Internet Explorer 6 web browser. This comes as the default with Windows Server 2003. On Windows 2000 you can select it from a Customized installation.

- MSXML version 3.0 SP2
  This is available as file msxml3sp2Setup.exe in the Redistributable Software folder on the Enterprise Vault CD-ROM.
Requirements for users’ computers

To be able to archive items from a mailbox, users must have either Outlook and User Extensions installed on their computers or use Outlook Web Access (OWA). However, users can view and restore various types of archived items (messages, documents, files) using the following methods:


■ Using Outlook Web Access (OWA). With OWA, users can archive mailbox items, search an archive, view and restore mailbox and public folder items. Outlook and Enterprise Vault User Extensions do not need to be installed on user desktops, but Enterprise Vault OWA Extensions must be installed and configured on front-end and back-end OWA Exchange servers. See “Configuring OWA access to Enterprise Vault” on page 109 for details.

■ Using Outlook or some other email client without Enterprise Vault User Extensions. This uses Enterprise Vault customized shortcuts. The shortcut in an archived message opens a browser window, which enables the user to access the original message, search archive(s), download items to their computer or restore items to an Exchange server mailbox. To support these customized shortcuts, users need a PC or Mac computer with Internet Explorer 5.5 or later installed and Java scripting enabled. The email client used to access Exchange mailbox can be any locally installed POP or IMAP client or a web email client.

■ Using the Enterprise Vault web access application. This enables users to search multiple archives using advanced filtering and restore multiple items. The web access application gives users access to different types of archived items (messages, documents, files). To support the Enterprise Vault web access application, users need a PC with Internet Explorer 5.5 or later installed and Java scripting enabled.

■ Using the Enterprise Vault Archive Explorer feature. This gives users a tree-view of the folders and items in their archives. Archived folders can be navigated in the same way as Outlook or file system folders. Archive Explorer gives users access to different types of archived items (messages, documents, files). To support Archive Explorer, users must have Internet Explorer 5.5 or later installed and Java scripting enabled.
User Extensions for Outlook

Before users can send items to an archive from within their Outlook client, the User Extensions or Self-Installing User Extensions must be installed on their computers.

For the normal User Extensions, the computers must be running the following:

- Operating system – one of the following:
  - Windows XP Professional or Windows 2000 Professional.
- Mail Client – one of the following:
  - Microsoft Outlook 2003
  - Microsoft Outlook 2002 (XP)
  - Microsoft Outlook 2000
  Note that Internet Explorer must be installed before the mail client is installed.
- Web browser – one of the following. Java scripting must be enabled:
  - Internet Explorer 5.5 SP2 or later. This must be installed, even if it is not used. If you intend to make the Self-Installing User Extensions available to users, Internet Explorer must allow them to download signed ActiveX controls.
  - TCP/IP protocol

What next?

Go to:

- “Preinstallation tasks” on page 57
Before installing

What next?
Preinstallation tasks

Read this chapter to find out what you must do before installing Enterprise Vault on Windows 2000 or Windows Server 2003.

You are recommended to back up your system disk before installing Enterprise Vault.

Before installing Enterprise Vault you must:

■ Create the Vault Service account for the Enterprise Vault site and give it permissions on each Microsoft Exchange Server computer. See “Creating the Vault Service account”.

■ You must also create a SQL login for the Vault Service account. See “Creating a SQL login” on page 61.

■ Create the Vault Site alias, as described in “Creating the Vault Site alias” on page 62.

Creating the Vault Service account

Note that, on Windows Server 2003 and Windows 2000, it may take some time for the Vault Service account to be registered in the Active Directory for the computer that is going to run Enterprise Vault. The account cannot be used until the registration is complete. The length of the delay depends on how Exchange is set up to replicate recipient information.

To create the Vault Service account

1. On the domain controller, click Start, Programs, Administrative Tools, Active Directory Users and Computers.

2. In the left-hand pane of Active Directory Users and Computers, double-click the Domain container.

3. Double-click the Users container.
Creating the Vault Service account

4. On the Action menu, click New and then User. The New Object — User screen is displayed.

5. Complete the New Object — User screen and click Next. The next screen asks for password details.

6. Enter a password and confirm it. You must set a password; the Vault Service account password cannot be blank.

7. Select the Password never expires checkbox.

8. Leave the remaining checkboxes clear:
   - User must change password at logon
   - User cannot change password
   - Account is disabled

9. Click Next to move to the mailbox server screen.

10. Complete the details and click Next to move to the summary screen.

11. Click Finish to create the new user.

You now need to add the new Vault Service account to the local Administrators group on each Enterprise Vault server computer as follows:

1. Log on to the Enterprise Vault computer as Administrator.

2. In Control Panel, open Administrative Tools and start the Computer Management console.

3. Expand System Tools and then Local Users and Groups.

4. Select Groups, and then double-click the Administrators group in the right-hand pane.

5. Use Add to add the Vault Service account to this group.

6. Click OK.

Changing the Vault Service account

Before you proceed, ensure that:

- The new Vault Service account is part of the Administrators group, with permission Full Control (All), on each Enterprise Vault computer in the Enterprise Vault site.

- The Microsoft Message Queue security has been set up to grant the Administrators group access to the Enterprise Vault queues.
To change the account and set up Microsoft Exchange Server permissions

1. Using the Vault Administration Console, stop all the Enterprise Vault services on every computer in the Enterprise Vault site.

2. Using the Vault Administration Console, change the Vault Service account name and password.


4. Run Microsoft Exchange Administrator.


6. Click the Permissions tab.

7. Click Add. The Add Users and Groups dialog box is displayed.

8. In the List Names From box, click the Windows domain that contains the account you want to use as the new Vault Service account.

9. Click the Names arrow and click the new Vault Service account. Click Add.

10. Click OK.

11. Click the Roles arrow and click Service Account Admin.

12. Click OK.

13. Select the Microsoft Exchange Server site and then, on the File menu, click Properties. Repeat step 9 to step 12.

14. Select the Configuration Container in the Microsoft Exchange Server site, and then on the File menu, click Properties. Repeat step 6 to step 12.

15. Display the contents of the Exchange Site Recipients container.

16. Look for the Enterprise Vault mailboxes. The name is Enterprise Vault Mailbox for <name> where <name> is the name of the Exchange Server computer. Depending on your configuration, you may have one or many such mailboxes.

17. Select the first Enterprise Vault mailbox.

18. Select File and then Properties.

19. Click Primary Windows Account and then select the account that you want to be the new Vault Service account.

20. Repeat step 18 and step 19 for each of the other Enterprise Vault mailboxes.

21. Use the Windows Services manager to start the Enterprise Vault Directory Service.
22 Use the Enterprise Vault Administration Console to start the other Enterprise Vault services.

Assigning Microsoft Exchange Server permissions

The Vault Service account needs to be able to access mailboxes on the Exchange Servers that Enterprise Vault is to archive. You need to grant permissions explicitly on each Exchange Server, as described in this section. If you later add another Exchange Server, you need to repeat the procedure on the new server to enable mailbox access for the Vault Service account.

You must have Exchange administration permissions to do the following tasks.

On Microsoft Exchange Server 2003 and Microsoft Exchange 2000 Server

1 Click **Start**, **Programs**, **Microsoft Exchange**, **System Manager**.
2 Expand the **Servers** container.
3 Right-click your Exchange Server and, on the shortcut menu, click **Properties**.
4 Click the **Security** tab.
5 Click **Add**.
6 Double-click the Vault Service account to add it to the list.
7 Click **OK** to go back to the **Security** tab. The Vault Service account has been added to the **Name** list.
8 In the **Name** list, click the Vault Service account.
9 In the **Permissions** list, make sure that all checkboxes in the **Allow** column are selected. Select any checkboxes that are not already selected.
10 Click **OK**.

If required, you can add the permissions at the **Organization** or **Administrative Group** level in the Exchange hierarchy. This will enable the permissions to be propagated automatically to any new Exchange Servers added below the level at which the permissions are assigned.

To assign the permissions at **Organization** or **Administrative Group** level

1 Enable the display of the **Security** page by configuring the **ShowSecurityPage** registry setting (see Microsoft Knowledge Base Article 883381).
2 In the left-hand pane of **Microsoft Exchange**, **System Manager**, right-click your Exchange Organization or the administrative group that you want, and select **Properties**.
3 Select the Security tab and set the required permissions for the Vault Service account, as described in the steps for individual Exchange Servers.

On Microsoft Exchange Server 5.5
1 Run Microsoft Exchange Administrator.
2 Expand the Organization container and select the Microsoft Exchange Server Site container. On the File menu, click Properties.
3 Click the Permissions tab.
4 Click Add. The Add Users and Groups dialog box is displayed.
5 In the List Names From box, click the Windows domain in which you created the Vault Service account.
6 Click the Names arrow and click the Vault Service account. Click Add.
7 Click OK.
8 Click the Roles arrow and click Service Account Admin.
9 Click OK.
Select the Configuration Container in the Microsoft Exchange Server Site, and then on the File menu, click Properties. Repeat steps 3 to 9.

Creating a SQL login
You must use SQL Enterprise Manager to create a SQL login for the Vault Service account, as follows:
1 Click Start, Programs, Microsoft SQL Server, Enterprise Manager.
2 Expand the SQL Server container.
3 Click Security.
4 Right-click Logins and, on the shortcut menu, click New Login.
5 Enter or select the name of the Vault Service Account. For example, domain\vaultadministrator
6 Check that Windows Authentication is selected and that the correct Domain for the account has been selected.
7 Under Security Access check that Grant access is selected.
8 On the Server Roles tab, select Database Creators.
9 Click OK.
Creating the Vault Site alias

To create a DNS alias, you need administration privileges to run DNS manager on your Primary DNS server. You must then assign a DNS alias to the IP address of the Vault Directory computer you are using to configure the new Enterprise Vault site. Give the alias a meaningful name so that you know to which Enterprise Vault site it relates.

What next?

Go to “Installing Enterprise Vault” on page 63.
Installing Enterprise Vault

Read this chapter to find out:

■ How to perform a new installation of Enterprise Vault.
■ How to uninstall Enterprise Vault.

Before you install Enterprise Vault

■ Complete the preinstallation tasks as described in "Preinstallation tasks" on page 57.
■ If you intend to install the Enterprise Vault Services component, stop the IIS Admin Service to make sure that IIS is not running during the Enterprise Vault installation.

Log in to the Vault Service account to install Enterprise Vault. This ensures that you are a member of the Administrators group and have the required Microsoft Exchange Server permissions.

Server installation

Note: Before you install Enterprise Vault you must have started Outlook, created a profile, and connected to the mailbox on the Exchange Server.

To install Enterprise Vault

1 Load the Enterprise Vault CD-ROM into your CD-ROM drive.
2 Double-click Admin Documentation link in the top-level folder to display the Enterprise Vault administrator documentation.
3 Click the ReadMe link to display the ReadMe text and read it before continuing with the installation.
4 Open the Enterprise Vault folder.
5 Open the Server folder.
6 Double-click SETUP. EXE to start the installation.
7 Follow the installation instructions.

Install the required components on each computer where you want to run or use Enterprise Vault according to the decisions you made during the planning stage. As a reminder, the components are:

■ Enterprise Vault services.
  Installs all the Enterprise Vault services. After the installation, you must configure the services before using them. Configuration is covered in “Running the Configuration Program” on page 79.

■ Administration Console.
  Installs the Administration Console. This is a snap-in to the Microsoft Management Console (MMC) that enables you to manage Enterprise Vault. This component also installs the Configuration Program.
  PST Migrator is also installed when you choose to install the Administration Console.
  You can install the Administration Console component on a separate computer running either Windows Server 2003 or Windows 2000 Server or Professional.

■ Exchange OWA Extensions:
  ■ Exchange 2003 OWA Extensions (Back-end). This component may not be shown. Installs the back-end OWA extensions.
  ■ Exchange 2003 OWA Extensions (Front-end). This component may not be shown. Installs the front-end OWA extensions.
  ■ If you do not have a front-end/back-end OWA configuration, you do not need to install this component.
  ■ Exchange 2000 OWA Extensions (Back-end). This component may not be shown. Installs the back-end OWA extensions.
  ■ Exchange 2000 OWA Extensions (Front-end). This component may not be shown. Installs the front-end OWA extensions.
    If you do not have a front-end/back-end OWA configuration, you do not need to install this component.
  ■ Exchange Server 5.5 OWA Extensions. This component may not be shown. Installs the OWA extensions.

■ SharePoint Portal Server Web Parts.
  This component may not be shown and is not needed by Enterprise Vault for Microsoft Exchange Server.
Installing Enterprise Vault

Uninstalling Enterprise Vault

■ File Placeholder service.

You need this component if you want to run File System Archiving to archive from the current computer and leave placeholders in place of archived files. Selecting this option installs the File Placeholder service and the File System Archiving filter driver.

What next?

You must do the postinstallation tasks before you start Enterprise Vault.

At the end of installation, you may be instructed to restart your computer. If you do not need to restart your computer, you can choose to run the Configuration Program immediately after the installation. Go to “Running the Configuration Program” on page 79. Alternatively, you can exit from the installation and do the postinstallation tasks. You must do these postinstallation tasks before you start Enterprise Vault.

If you need to restart your computer, do so and then do the postinstallation tasks as described in the next section.

If the installation was unable to configure the security for the Web Access application, you must configure it manually, as described in “Setting up security for the Web Access application” on page 67.

If you have installed the File Placeholder service without Enterprise Vault services, go to “Setting up file system archiving” on page 273 to find out how to do the configuration.

Uninstalling Enterprise Vault

Note the following before you proceed:

■ You can uninstall Enterprise Vault and then reinstall it on the same system, provided that the computer on which you uninstall Enterprise Vault is not running the Enterprise Vault Directory Service.

■ If an Enterprise Vault service has data associated with it, you cannot use the Enterprise Vault Administration Console to remove that service.

To uninstall Enterprise Vault

1 From the Windows Control Panel, select Add/Remove Programs.

2 From the list of programs, select Enterprise Vault, and then click Add/Remove.

   You are asked to confirm that you want to remove Enterprise Vault from your system.

3 Click Yes.
The uninstaller stops Enterprise Vault services that are still running. It then removes all Enterprise Vault Services and Enterprise Vault software from your system. The uninstaller does not delete data.

4 If you want to reinstall Enterprise Vault on the computer, do the following:
   a Re-run the Setup program. You do not have to select the same installation folder for Enterprise Vault that you previously selected.
   b Run the Enterprise Vault Configuration Program. When this program prompts you for a Directory Computer, give the same name as for the previous installation. The Configuration Program automatically creates the same services as the computer had before.

If you do not want to reinstall Enterprise Vault, delete the Enterprise Vault data manually.
Postinstallation tasks

Read this chapter to find out:

- How to configure the default security for the Enterprise Vault Web access Application.
- How to customize the security for the Enterprise Vault Web Access application to match your needs.
- How to distribute the Microsoft Exchange Server Forms.
- How to set up the Administration Console so that it can display Japanese fonts.

Setting up security for the Web Access application

The Enterprise Vault installation automatically sets up Basic authentication and Integrated Windows authentication.

Effect on users

The security that is automatically set up affects users when they log in to the Web Access application, as follows:

- A user logging in with a browser that supports Integrated Windows Authentication, such as Internet Explorer, must supply domain name and username separately:
  
  **Username:** username
  **Password:** password
  **Domain:** domain

  This domain can never be defaulted.

  An Internet Explorer user with suitably-customized browser settings does not need to supply logon details manually because the logon is automatic; Internet Explorer automatically uses the details of the account to which the
Postinstallation tasks

Setting up security for the Web Access application

A user logging in to the Web Access application with a browser that does not support Integrated Windows Authentication, must supply both domain name and username in response to a single username prompt:

**Username:** domain\username
**Password:** password

It is possible for you to set up a default domain; see “Using a default domain with basic authentication” on page 69.

For other Web Access application security options, see “Enabling remote access to the Web Access Application computer” on page 73.

The next section, “Setting up the default authentication”, describes the procedures to set up Basic authentication and Integrated Windows Authentication yourself. You do not need to do this unless the installation procedure gives you a message saying that setup could not set alias security.

Setting up the default authentication

The installation automatically configures Basic authentication and Integrated Windows Authentication for the Enterprise Vault Web Access application. If, when you installed Enterprise Vault, there was no message saying that setup could not set alias security, then the authentication described in this section has already been applied to your system.

The Enterprise Vault Web Access application is always installed on the same computer as Internet Information Server (IIS).

To set up the default authentication, log in to the IIS computer as Administrator and do the following:

1. Click **Start**, **Programs**, **Administrative Tools**, **Internet Services Manager**.
2. Expand the container for the Enterprise Vault Web Access application computer.
3. Expand the **Default Web Site** container.
4. Right-click the **EnterpriseVault** folder and, on the shortcut menu, click **Properties**.
5. Click the **Directory Security** tab.
6. In the **Anonymous access and authentication control** section, click **Edit**.
7. Clear the **Anonymous access** checkbox.
8. Select **Basic authentication**. A security message appears, warning about transmitting passwords without encryption. Click **Yes** to continue.
Customizing security for the Web Access application

The standard security for the Web Access application means that users must provide domain name, user name, and password whenever they start the Web Access application.

This section describes various levels of automatic authentication that you can set up for the users. If none of these methods is acceptable to you, the default authentication enables users to log on by supplying domain, username, and password.

Using a default domain with basic authentication

With only Basic authentication configured, users must provide a domain name when logging on to the Web Access application. For example, a user in domain
**myDomain** with a username of **Rogers** must specify `myDomain\Rogers` when logging on to the Web Access application.

It is possible for IIS and Enterprise Vault to use a default domain for Basic authentication. In this case, users in the default domain do not need to specify a domain name when starting the Web Access application. Users in other domains must still specify a domain name.

### Setting up a default domain in IIS

Note that the default domain does not work unless you also define it for the Web Access application, as described in “Setting up a default domain in the Web Access application” on page 70.

To set up IIS so that it uses a default domain for Basic authentication

1. Click **Start**, **Programs**, **Administrative Tools**, **Internet Services Manager**.
2. Expand the container for the Enterprise Vault Web Access application computer.
3. Expand the **Default Web Site** container.
4. Right-click the **EnterpriseVault** folder and, on the shortcut menu, click **Properties**.
5. Click the **Directory Security** tab.
6. In the **Anonymous access and authentication control** section, click **Edit**.
7. Clear **Anonymous access** if it is selected.
8. If **Basic authentication** is not already selected, then select it.
10. Enter the name of the domain that contains the majority of the user accounts that will be using the Web Access application and click **OK**.
    If there is a prompt about Inheritance Overrides, click **Select All** and then **OK**.

### Setting up a default domain in the Web Access application

Note that the default domain does not work unless you also define it in IIS, as described in “Setting up a default domain in IIS” on page 70.

To set up the Web Access application so that it uses the same default authorization domain as you have set up in IIS:

1. Use a text editor to create an initialization file called **WebApp.ini**, containing the following line:
   ```ini
   Domain=<DomainName>
   ```
Customizing security for the Web Access application

where `<DomainName>` is the name of the domain that you have specified in IIS for Basic authentication. Note that entries in this file are case-sensitive. For example, to use a domain called myDomain, the line to use is:

```
Domain=myDomain
```

2 Save the file in the Enterprise Vault program folder, normally C:\Program Files\Enterprise Vault, on the computer that runs the Web Access application.

Customizing security on the client computers

You can configure Internet Explorer so that users are automatically logged on to the Web Access application, without receiving a logon prompt. Essentially, you must configure Internet Explorer so that it trusts the Web Access application computer.

For this to work, you must also be using the Integrated Windows Authentication, as described in “Setting up the default authentication” on page 68.

To make Internet Explorer log on automatically, you may need to modify the Internet Explorer Internet Options on each client computer. The settings are saved in the Windows registry, so you can save them for rollout to many client computers.

There are many possible ways for you to configure Internet Explorer security, some of which may not be acceptable to you. Two methods are described here:

- Using the proxy bypass list
- Explicitly naming the Web Access application computer

See the Internet Explorer help if you need more information on configuring browser security.

Using the proxy bypass list

Note that you must be using a proxy server before you can use the proxy bypass list.

To configure Internet Explorer to use the proxy bypass list

1 In Internet Explorer, click **Tools** and then **Internet Options**.
2 Click the **Security** tab and then click the **Local Intranet** zone.
3 Click **Sites** and then select **Include all sites that bypass the proxy server**.
4 Click **OK**.
5 Click **Custom Level**.
6 Under Logon, select **Automatic logon only in Intranet zone**.
7 Click **OK**.
8 Click the **Connections** tab, and click **LAN Settings**.
9 Check that a proxy server is being used.
10 If either of the **Automatic configuration** settings is selected, you must make sure that the Web Access application computer is in the automatic configuration exceptions list.
11 If neither of the **Automatic configuration** settings is selected, click **Advanced** and, if there is no existing entry that includes the Web Access application computer, specify the Web Access application computer in the **Exceptions** list.

**Explicitly naming the Web Access application computer**
This section describes how to add the Web Access application to computer to the Internet Explorer local intranet zone.

It is possible to configure users’ desktops so that they automatically add the Web Access application computer to the Internet Explorer local intranet zone. See the *Administrator's Guide* for more details.

**To configure Internet Explorer to trust the Web Access application computer**
1 In Internet Explorer, click **Tools** and then click **Internet Options**.
2 Click the **Security** tab and then click the **Local Intranet** zone.
3 Click **Custom Level**.
4 Under **Logon**, select **Automatic logon only in Intranet zone** and then click **OK**.
5 Click **Sites** and then **Advanced**.
6 In the **Add this Web site to the zone** box, enter the fully-qualified domain name of the Web Access application computer and then click **Add**. For example, vault.company.com
7 In the **Add this Web site to the zone** box, enter the computer name, without the DNS domain, of the Web Access application computer and then click **Add**.
8 Click **OK**.

Once you have set up the security, users will not need to log on to search archives or to view or restore archived items.
Enabling remote access to the Web Access Application computer

You may need to grant users of the Enterprise Vault Web Access application access to the IIS computer, using the local IIS computer accounts database, not the domain accounts database.

**Note:** If the IIS computer is a domain controller, there is no local accounts database, only a domain accounts database. If you continue with these instructions when the IIS computer is a domain controller, you will make changes to the security access of the domain accounts database. This will affect all computers within the domain, not just the IIS computer. If you do not want to affect the whole domain, you should ensure that you run IIS on a non-domain controller.

**To grant access**

1. Click **Start**, **Programs**, **Administrative Tools**, **Local Security Policy**. The **Local Security Settings** window appears.
2. Expand the **Local Policies** container.
3. Click **User Rights Assignment**.
4. Set up Basic authentication access:
   a. (On Windows 2003) In the right-hand pane, right-click **Allow log on locally** and, on the shortcut menu, click **Properties**. The **Local Security Policy Setting** window appears.
   (On Windows 2000) In the right-hand pane, right-click **Log on locally** and, on the shortcut menu, click **Security**. The **Local Security Policy Setting** window appears.
   b. Check that the **Users** group appears in the list.
   (On Windows 2000) Check that **Local Policy Setting** is selected. If **Local Policy Setting** is not selected, add it.
5. Set up Integrated Windows Authentication access:
   a. In the right-hand pane, right-click **Access this computer from the network** and, on the shortcut menu, click **Properties** (on Windows Server 2003) or **Security** (on Windows 2000). The **Local Security Policy Setting** window appears.
   b. Check that the **Users** group appears in the list.
   (On Windows 2000) Check that **Local Policy Setting** is selected. If **Local Policy Setting** is not selected, add it.
   If you do not want to add the **Users** group, see the other options below.
By default, the Users group includes Domain Users. If the Users group does not include Domain Users, or if some Web Access application users are in a different domain, you must do one of the following:

- Add the Web Access application users to the Users group
- Add the Web Access application users to some other group and then grant the access right to that group
- Grant the access right to each Web Access application user's account.

The Enterprise Vault Web Access application is now set up and ready to be used by users in the same domain as IIS.

**Distributing the Microsoft Exchange forms**

To distribute the Microsoft Exchange forms that you have installed from the Enterprise Vault kit around your Microsoft Exchange Server organization, you are recommended to put them in the Microsoft Exchange Organization Forms Library.

However, before you install the forms, you may need to create a folder in the Organization Forms Library to hold the forms from the Enterprise Vault kit. If you need to do this, go to “Creating a folder” on page 74. Otherwise, go to “Installing the forms” on page 76.

**Creating a folder**

You must create a folder in the Organizations Forms Library with access provided to all Microsoft Exchange users who are going to use Enterprise Vault.

**On Exchange Server 2003 or Exchange 2000 Server**

1. Click Start, Programs, Microsoft Exchange, System Manager.
2. Expand the Organization (Exchange) object.
3. Expand your Administrative Group.
   - If this is not available, right click your Organization and select Properties. Then check Display Administrative Groups and click OK.
4. Expand Folders.
5. Right-click Public folders and, on the shortcut menu, click View System folders. The right-hand pane displays the system folders.
6. In the right-hand pane, right-click EFORMS REGISTRY and, on the shortcut menu, click New, and then click Organizational Form. A Properties window appears.
7. Fill in the details on the Properties window.
8 Under **E-forms language**, select the language that is appropriate to the forms you are going to install and then click **OK** to return to the Exchange System Manager screen.

9 In the right-hand pane, double-click the **EFORMS REGISTRY** folder.

10 Right-click the folder you just created (Organizational Forms) and, on the shortcut menu, and click **Properties**.

11 On the properties screen, click the **Permissions** tab.

12 Click **Client Permissions**.

13 Click **Add**.

14 Click a user name for the account that will be the owner of the forms. This will usually be the Enterprise Vault Service account.

15 Click the **Roles** down arrow and, in the list, click **Owner**.

16 Click **OK** to return to the Properties screen.

17 Click **OK** to close the Properties screen.

18 Close **Exchange System Manager**.

**On Exchange Server 5.5**

1 Run **Microsoft Exchange Administrator**.

2 On the **Tools** menu, click **Forms Administrator**.

3 Click **New**.

4 In the **Library folder name** box, type the library name you want to appear in the Administrator window or accept the default, **Organization Forms**.

5 In the **Language** box, select a language.

6 You need to give a particular mailbox **Owner** access to the folder. Click **Permissions**, and do the following:
   a Click **Add**.
   b Select the mailbox that you want to use and click **Add**.
   c Click **OK**.
   d Select the mailbox that you have just added. Click the **Roles** arrow and select **Owner**.
   e Click **OK**.

You have now created a folder in the Organization Forms Library to hold the forms from the Enterprise Vault kit. Go to “**Installing the forms**” on page 76 to install the forms in the library.
Installing the forms

You can install the forms from Microsoft Outlook using a mailbox that has Owner permissions for the folder in the Organization Forms Library. Do this on the computer where you have installed the Microsoft Exchange forms from the Enterprise Vault kit.

Users can access the new forms when they have installed the Enterprise Vault User Extensions.

1. On the Outlook Tools menu, click Options.
2. Click the Other tab.
3. Click Advanced Options.
4. Click Custom Forms.
5. Click Manage Forms.
6. On the right-hand side of the dialog box, click the Set button.
7. Click Forms Library and select the name of your forms library. Click OK.
8. Click the Install button.
9. Select the Languages\Forms subfolder in the Enterprise Vault Program folder.
10. Select the language folder that is appropriate to the language of the forms you want to install.
11. Change the Files to type filter to Form Message (*.fdm)
12. Double-click EVPendingArchive.fdm and review the displayed properties to check that this is the Enterprise Vault Archive Pending Item.
13. Click OK.
14. Click the Install button.
15. Change the Files to type filter to Form Message (*.fdm).
16. Double-click EVShortcut.fdm and review the displayed properties to check that this is the Enterprise Vault Shortcut.
17. Click OK.
18. Click the Install button.
19. Change the Files to type filter to Form Message (*.fdm).
20. Double-click EVPendingRestore.fdm and review the displayed properties to check that this is the Enterprise Vault Restore Pending Item.
21. Click OK.
22 Click the **Install** button.

23 Change the **Files to type** filter to **Form Message (*.fdm)**.

24 Double-click **EVPendingDelete.fdm** and review the displayed properties to check that this is the Enterprise Vault Delete Pending Item.

25 Click **OK**.

---

**Customizing users’ desktop settings and security**

You can selectively remove Enterprise Vault functionality from users’ desktops. You can hide or show menu options, buttons, and property sheets for all the following:

- Search archives
- Manual archive
- Restore from archive using a shortcut
- Cancel archiving
- Delete from archive
- Enterprise Vault properties for folders
- Enterprise Vault properties for messages
- Enterprise Vault properties for mailboxes

Additionally, you can automatically add the Web Access application computer to the Internet Explorer intranet zone, thus enabling users to search their archives without providing logon details.

See the *Administrator’s Guide* for more details.

---

**Japanese fonts**

If your Enterprise Vault installation is going to have users who have a Japanese version of the Enterprise Vault User Extensions, you must set up the Administration Console so that it can display Japanese characters.

The Japanese characters are used when displaying:

- Mailbox names
- Archive names and descriptions
- The Web Access application System Message
- Retention Category names and descriptions
Do the following on each computer that is going to run the Administration Console:

1. Start the registry editor and navigate to the following key:
   
   HKEY_LOCAL_MACHINE
   SOFTWARE
   \KVS
   \Enterprise Vault
   \Admin

2. Add the following registry string values:

<table>
<thead>
<tr>
<th>Value</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecondaryFontCharSet</td>
<td>SHIFTJIS</td>
</tr>
<tr>
<td>SecondaryFontSize</td>
<td>12</td>
</tr>
<tr>
<td>SecondaryFontFace</td>
<td>MS UI Gothic</td>
</tr>
</tbody>
</table>

3. Check that the MS UI Gothic font is installed:
   
   On Windows 2000 Server:
   
   a. In the Windows Control Panel, double-click Regional Options.
   b. On the General tab, under Language settings for the system, select Japanese if it is not already selected.
   c. Click OK.

   On Windows 2003:
   
   a. In the Windows Control Panel, double-click Regional and Language Options.
   b. In Regional and Language Options, click the Languages tab.
   c. Under Supplemental language support, select Install files for East Asian languages. There is an information message that tells you the files will be installed after you click OK or Apply.
   d. Click OK.

The values given here work well but, if you want to experiment with other settings, you can change the fonts while the Administration Console is running.

What next?

You have now completed the postinstallation tasks. Go to “Running the Configuration Program” on page 79.
Running the Configuration Program

Read this chapter to find out how to configure Enterprise Vault. This process involves running the Enterprise Vault Configuration Program, as well as a number of additional configuration tasks. You must do these before you can use Enterprise Vault.

Note the following:

■ If you have installed the File Placeholder service without Enterprise Vault services, go to “Setting up file system archiving” on page 273 to find out how to do the configuration.
   If you have installed Enterprise Vault services, the File Placeholder service configuration is included in the Enterprise Vault services configuration and is described in this chapter.

■ If you run the Configuration Program immediately after the installation, remember that there are some additional tasks that you need to do before users can use Enterprise Vault. See “Postinstallation tasks” on page 67.

■ If you exit from the Configuration Program before configuration is complete, you can run the Configuration Program again and have the option to delete the Directory database. Once you have successfully completed the Configuration Program, you cannot run it again on the same computer.

Introduction

The Configuration Program sets up Enterprise Vault. It enables you to:

■ Select which SQL Server you want to use for the Vault Directory database
■ Create the Vault Directory Database
Running the Configuration Program

Preparation

■ Create an Enterprise Vault site
■ Add each computer to the site
■ Select the Enterprise Vault services you want to run on each computer
■ Choose the storage areas to use for Enterprise Vault data

The following tasks must be done using the Configuration Program:
■ Creating a new Vault Directory
■ Creating a new Enterprise Vault site
■ Adding a new computer

You can also use the Configuration Program to select which of the Enterprise Vault services you want to run on the computer and to assign storage areas for the data, although you can defer these tasks and do them from the Administration Console.

You must run the Configuration Program on every computer in the Enterprise Vault site.

After configuration, use the Administration Console to manage the sites, computers, and services.

Preparation

If you have installed the File Placeholder service, we recommend that you install the appropriate Enterprise Vault licenses, including a File System Archiving (FSA) license, before running the Configuration Program.

On systems that do not include File Placeholder service, you can install license keys before or after working through the Configuration Program.

To find out how to get your Enterprise Vault license keys and how to install them, see “Licenses and license keys” on page 105.

Running the Configuration Program

You may be starting the Configuration Program after restarting your computer or from the last screen of the Installation Program.

When you are using the Configuration Program to configure Enterprise Vault on subsequent computers, refer to the online Help if you are unsure about how to proceed.

To run the Configuration Program

1 Click Start > Programs > Enterprise Vault > Enterprise Vault Configuration.
Running the Configuration Program
Preparation

The Configuration Program wizard starts. The first screen asks whether you want to create a new Vault Directory on this computer.

2 Click Yes and then Next.
The wizard asks for details of an account for Enterprise Vault services to use. This is the Vault Service account that you created earlier; see “The Vault Service account” on page 51.

3 Enter the details of the Vault Service account.
You must use the format domain_name\username when you specify the account. Alternatively, use the ... button to browse for the Vault Service account.
Enter the password for the Vault Service account and confirm it.

4 Click Next.
A warning message is displayed if the account you are using does not have sufficient privileges to validate the password to the Vault Service account. Click Yes to continue.
A message tells you that the Vault Service account has been added to the local Administrators group. Click OK to close the message.
A second message notifies you that the account will be given the advanced user rights, Log On As a Service and Act as Part of the Operating System, Debug programs, and Replace a process-level token. Click OK to close the message.
The Configuration Program creates the Directory service and then the next screen asks for the location of the SQL Server that you want to use for the Directory database.

5 Enter the location of the SQL Server that you want to use. You can specify a SQL Server instance if required

6 Click Next.
The wizard shows the default locations for the Vault Directory database and transaction log.

7 Change the locations if necessary.
If you have specified that SQL Server is on a remote computer, the paths for the data file and transaction log file must be valid on that remote computer.

8 Click Next.
The wizard creates the Vault Directory Database. The next screen asks for details of the new Vault Site.

9 Enter a name and description for the new Enterprise Vault site.

10 Enter the Vault Site alias that you created earlier; see “The Vault Site alias” on page 52.
11 Click **Next**.
The next screen asks for a DNS alias for current computer.
You are recommended to enter a DNS alias but you can, if necessary, enter the computer’s fully-qualified DNS name.

12 Enter a DNS alias for the current computer and click **Next**.

13 Click **Next** to add the computer to the Enterprise Vault Site.
An information screen lists software that is installed on your computer.
Based on this list, the wizard automatically selects Enterprise Vault services to add to your computer.

14 Click **Next**. The list shows the services that will be added to your computer.

15 Check the list of services. If there are services in the that you do not need, you can remove them now.

16 To add additional services to this computer, click **Add** and select the service that you want to add.

17 Once you have the correct list of services, click **Properties** for each service and review the settings. Change the settings as necessary.

18 When you have finished reviewing the services' properties, click **Next**.
The default storage locations for the Shopping service and the Indexing service are displayed.

19 Check that the storage locations are suitable. Click **Back** if you want to change them.

---

**Note:** You must make sure that the default index storage location is on an accessible device and that the Vault Service account can write to it. When you enable mailboxes, Enterprise Vault adds information about the index storage location to the Vault Directory Database. You cannot easily change the index storage location for mailboxes after you have enabled them.

However, you can use the Administration Console to change the index storage location, or add further locations, before you enable any mailboxes.

---

20 If you do not want to change the default locations for the Indexing and Shopping services, click **Next**.
If you do want to change the locations, click **Back**, select the service that you want to modify and click **Properties** to change the location.
The next screen asks for details of the service mailbox.

21 An information page is displayed.
Click **Next** to continue and start the services.

22 The services that you have added are listed.
Click **Next** to start the Enterprise Vault services. If any of the service does not start immediately, continue to click **Next** until they have all started.

**Note:** The services will not start unless you have installed the appropriate license keys. See “Preparation” on page 80 for more information.

If you do not have the license keys yet, you can continue configuring Enterprise Vault using the Administration Console, but you cannot run the services until the license keys have been installed.

23 Click **Finish** to exit from the Configuration Program.

**What next?**

You can now continue with your configuration from the Enterprise Vault Administration Console.

You must also install all prerequisite software on the other computers that you want to add to the Vault Site and then run the Configuration Program on each computer to add it to the Vault Site.

Remember that you can run the Configuration Program only once successfully on a computer. If you exit the Configuration Program after successfully configuring Enterprise Vault, you cannot run the program again. To do any further setup or management of the Enterprise Vault components, you must use the Administration Console.

To find out how to start the Administration Console, see “Running the Administration Console” on page 85.

Remember that if you progressed directly to the Configuration Procedure from installation, you must still set up IIS and Microsoft Exchange Server. These tasks are described in “Postinstallation tasks” on page 67.

See “Distributing the User Extensions” on page 95 for details of how to distribute the Enterprise Vault User Extensions to your users.
Running the Configuration Program

What next?
Running the Administration Console

Read this chapter to find out:
■ How to add services to your Enterprise Vault installation
■ How to create new Retention Categories
■ How to review and modify the Site settings

Preparation

At the end of the Configuration Program you were asked to start the Enterprise Vault services. These services will not start until you have installed the appropriate license keys.

To find out how to get your Enterprise Vault license keys and how to install them, see “Licenses and license keys” on page 105.

Introduction

The Administration Console enables you to manage the sites, computers, and services. Don’t forget that the Administration Console includes the following wizards:
■ Enable Mailboxes
■ Disable Mailboxes
■ New Partition
■ New Vault Store
■ New Archive
Starting the Administration Console

Permissions needed
In order to use the Administration Console you need to be logged in as an account that is a member of the local Administrators group on every computer that runs an Enterprise Vault service. This provides sufficient permissions for everything you do in the Administration Console except for adding a Public Folder task.

In order to add a Public Folder task you must be logged in as an account that has appropriate Exchange Server permissions. The Vault Service account has the correct permissions. Alternatively, set up the account you want to use so that it has the correct permissions; see “Assigning Microsoft Exchange Server permissions” on page 60.

To start the Administration Console
1. Click Start > Programs > Enterprise Vault > Administration Console.
   The Administration Console starts.

Adding services
If you want to add more services, you can do so from the Administration Console.

To add an Indexing service
1. In the MMC scope pane (left pane), expand the Vault Site hierarchy until the Enterprise Vault Servers container is visible.
2. Expand the Enterprise Vault Servers container.
3. Right-click the name of the computer to which you want to add a service and, on the shortcut menu, click New and then Service.
   The Add Service dialog box appears, listing the services you can add.
4. Click Enterprise Vault Indexing Service.
5. Click Add.
6. Make sure that the index storage location is on an accessible device and that the Vault Service account can write to it.
   When you enable mailboxes, Enterprise Vault adds information about the index storage location to the Vault Directory Database. You cannot easily
Running the Administration Console

Creating Retention Categories

change the index storage location for mailboxes after you have enabled them.

To add a Storage service
1. In the MMC scope pane, expand the Vault Site hierarchy until the Enterprise Vault Servers container is visible.
2. Expand the Enterprise Vault Servers container.
3. Right-click the name of the computer to which you want to add a service and, on the shortcut menu, click New and then Service. The Add Service dialog box appears, listing the services you can add.
4. Click Enterprise Vault Storage Service.
5. Click Add.

To add a Shopping service
1. In the MMC scope pane, expand the Vault Site hierarchy until the Enterprise Vault Servers container is visible.
2. Expand the Enterprise Vault Servers container.
3. Right-click the name of the computer to which you want to add a service and, on the shortcut menu, click New and then Service. The Add Service dialog box appears, listing the services you can add.
4. Click Enterprise Vault Shopping Service.
5. Click Add.

Creating Retention Categories

You may have decided during planning that you wanted more Retention Categories than the ones predefined in Enterprise Vault. If this is the case, you must create your own Retention Categories. Alternatively, you can edit the predefined Retention Categories to suit your needs.

To create a new Retention Category
1. Expand the Vault Site hierarchy until Retention Categories is visible.
2. Right-click Retention Categories.
3. From the shortcut menu, select New Retention Category. The New Retention Category wizard starts.
4. Work through the wizard. Click Help on any of the wizard screens if you need more information.
Additional configuration tasks

Reviewing site settings

Check the site settings and modify them as necessary.

To display the site settings

1. In the Administration Console, expand the contents of the left pane until the Enterprise Vault site is visible.

2. Right-click the Enterprise Vault site and then, on the shortcut menu, click Properties. Alternatively, select the site and click the Review Site Settings button on the toolbar.

3. Click Help on any of the Site Properties screens for further information.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Tab</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>How to archive from mailboxes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Whether to archive unread items</td>
<td>Mailbox Actions</td>
<td>Unread items are not archived.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Setting is locked.</td>
</tr>
<tr>
<td>The archiving condition – that is, whether</td>
<td>Mailbox Rules</td>
<td>Archiving is based on the period of time since an item was modified.</td>
</tr>
<tr>
<td>to archive based on the period of time since</td>
<td></td>
<td>The time period is six months.</td>
</tr>
<tr>
<td>an item was modified or based on the</td>
<td></td>
<td>Setting is locked.</td>
</tr>
<tr>
<td>percentage of the mailbox storage limit that</td>
<td></td>
<td></td>
</tr>
<tr>
<td>is released</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The minimum age at which items can be</td>
<td>Mailbox Rules</td>
<td></td>
</tr>
<tr>
<td>archived</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Whether to archive larger items before</td>
<td>Mailbox Rules</td>
<td></td>
</tr>
<tr>
<td>smaller items and, if so, the minimum size</td>
<td></td>
<td></td>
</tr>
<tr>
<td>of the items that are given priority</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Whether to delete the original item</td>
<td>Mailbox Actions</td>
<td>Original item is deleted after archiving.</td>
</tr>
<tr>
<td>after archiving</td>
<td></td>
<td>Setting is locked.</td>
</tr>
<tr>
<td>Whether to create a shortcut after</td>
<td>Mailbox Actions</td>
<td>Shortcut is created after archiving.</td>
</tr>
<tr>
<td>archiving</td>
<td></td>
<td>Setting is locked.</td>
</tr>
</tbody>
</table>
### Running the Administration Console

#### Additional configuration tasks

<table>
<thead>
<tr>
<th>Setting</th>
<th>Tab</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Whether to enable new mailboxes automatically</td>
<td>Archiving Defaults</td>
<td>New mailboxes are not automatically enabled.</td>
</tr>
<tr>
<td>Whether to suspend archiving initially</td>
<td>Archiving Defaults</td>
<td>Archiving is not initially suspended.</td>
</tr>
<tr>
<td>Which vault store to use for automatically-enabled mailboxes</td>
<td>Archiving Defaults</td>
<td>None.</td>
</tr>
<tr>
<td>Which Retention Category to use</td>
<td>Archiving Defaults</td>
<td>Miscellaneous, which has a default retention period of one year.</td>
</tr>
<tr>
<td>Which Indexing service to use</td>
<td>Indexing Defaults</td>
<td></td>
</tr>
<tr>
<td>Which indexing level to use</td>
<td>Indexing Defaults</td>
<td>Brief.</td>
</tr>
<tr>
<td>Whether to delete shortcuts automatically after a period of time</td>
<td>Shortcut Deletion</td>
<td>Shortcut deletion is enabled and the time period is set to 6 months.</td>
</tr>
</tbody>
</table>

#### How to archive from public folders

<table>
<thead>
<tr>
<th>Setting</th>
<th>Tab</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age limit on archiving: the minimum age at which items can be archived</td>
<td>Public Folder Rules</td>
<td></td>
</tr>
<tr>
<td>Whether to archive larger items before smaller items and, if so, the minimum size of the items that are given priority</td>
<td>Public Folder Rules</td>
<td></td>
</tr>
<tr>
<td>Whether to delete the original item after archiving</td>
<td>Public Folder Actions</td>
<td>Original item is deleted after archiving. Setting is locked.</td>
</tr>
</tbody>
</table>
### Additional configuration tasks

#### Setting a shortcut after archiving

- **Setting:** Whether to create a shortcut after archiving
- **Tab:** Public Folder Actions
- **Default Value:** Shortcut is created after archiving.
  Setting is locked.
  **Note:** In Enterprise Vault 3.5 you cannot search public folder archives. So, if you delete shortcuts to archived items, you cannot easily retrieve those items.

#### Archiving condition

- **Setting:** The archiving condition – that is, the amount of time since an item was modified before it can be archived
- **Tab:** Public Folder Rules
- **Default Value:** Archiving is based on the period of time since an item was modified. The time period is six months. Setting is locked.

#### Shortcut deletion

- **Setting:** Whether to delete shortcuts automatically after a period of time
- **Tab:** Shortcut Deletion
- **Default Value:** Shortcut deletion is enabled and the time period is set to 6 months. The same setting is used for mailbox archiving.

### When to archive from mailboxes and public folders

- **Setting:** The times at which the Archiving and Public Folder tasks process the Microsoft Exchange Server computers
- **Tab:** Site Schedule
- **Default Value:** Archiving and Public Folder tasks process Microsoft Exchange Server computers at the selected time of 6pm to 6am. You can override the schedule for individual services by editing their properties.

### Shortcut behavior

- **Setting:** What happens when a user double-clicks a shortcut
- **Tab:** General
- **Default Value:** The original item’s contents are shown, using the associated application.

- **Setting:** The level of detail that is kept in a shortcut
- **Tab:** General
- **Default Value:** Shortcuts always contain only the From and Subject information.
### Setting | Tab | Default Value
--- | --- | ---
Whether to store recipient information (To: and Cc: details) in shortcuts. | General | Shortcuts do not show recipient information.

Whether to store message bodies in shortcuts | Shortcuts do not show recipient information. Select **Message Body** to make shortcuts contain message text, but no attachments. The full messages, with attachments, are still stored in the archive.

Whether double-clicking a shortcut displays its properties or its contents | General | View contents.

### When to delete archived items

| Setting | Tab | Default Value |
--- | --- | ---
Whether to delete shortcuts automatically after a period of time. | Shortcut Deletion | Shortcut Deletion is disabled.

Whether users can delete items from their archives | General | Users cannot delete items from their archives.

Whether to run Storage Expiry to delete items from archives when their retention periods expire. This also deletes corresponding shortcuts in users mailboxes. If you do run Storage Expiry, you must decide whether to base expiry on sent/received date or on archived date. | Storage Expiry | Storage Expiry is disabled

Maximum size of archives. You can set a maximum size for every archive in the Site. You can override this setting at the vault store level or the individual archive level. | Archive Usage Limits | There are no limits to archive sizes.

**Note:** Archive Usage Limits are not intended as a general quota mechanism. They are intended to curb a user who sees a archive as a repository for anything and everything.
Supporting secure web server connections

On the **General** page of **Site properties**, the URL for accessing the Enterprise Vault web access application is set up automatically as:

```
http://iis_computer/location
```

where `iis_computer` is the address of the computer that is running IIS and `location` is the name of the virtual directory for the web access application. For new installations this is always **EnterpriseVault**. For example:

```
http://our_iis_computer/EnterpriseVault
```

If your IIS computer requires secure connections, using HTTPS, then you would change the above URL to:

```
https://our_iis_computer/EnterpriseVault
```

If you want to access the web server using a port other than the default port, you can specify the port in the URL as follows:

```
https://iis_computer:port/location
```

For example, to access the web access application on the web server, `our_iis_computer`, using HTTPS and port 321, you would specify the URL as:

```
https://our_iis_computer:321/EnterpriseVault
```

What next?

See the appropriate chapter:

- “**Setting up archiving from mailboxes**” on page 245
- “**Setting up users’ desktops**” on page 93
- “**Setting up archiving from public folders**” on page 259
- “**Setting up archiving of journaled messages**” on page 267
Setting up users’ desktops

Read this chapter to find out:
■ What users need in order to access items in their archive
■ The differences between the various User Extensions installation kits
■ How to distribute the User Extensions
■ How to distribute the Self-Installing User Extensions

Introduction

There are several ways that users can access items in their archive(s):
■ Using Enterprise Vault User Extensions for Outlook. These are installed on each user's desktop and give the user access to the full functionality of Enterprise Vault from within Outlook. Users can archive items, navigate folders in an archive, perform searches on multiple archives, view, restore and delete items and set access permissions on archive folders. As administrator, you can restrict what your users can do and see.

■ From Enterprise Vault shortcuts in messages. Users do not need to have User Extensions or Outlook installed on their desktops. The shortcuts give users browser access to archives, enabling them to view, search, restore and delete items, but not manually archive items. As the standard Enterprise Vault shortcuts do not work well with some email clients, you should use custom shortcuts for this option. “Defining custom shortcut content” on page 250.

■ Using the Enterprise Vault web access application. This is an option if you do not want to use either Enterprise Vault User Extensions or shortcuts. Using a browser, users can view, search, restore and delete items in their archives. With this option, users cannot manually archive items.
User Extension kits

There are two different versions of the Enterprise Vault User Extensions:

- User Extensions
- Self-Installing User Extensions

We supply several different User Extensions kits so that you can choose the one that best fits your purpose.

Before users have access to the full range of Enterprise Vault features from within their Outlook, you must provide the User Extensions in one of these ways:

- Send users a shortcut to the User Extensions
- Perform a silent installation
- Make the Self-Installing User Extensions available so that they can be installed automatically

User Extensions

The User Extensions provide the maximum functionality. In addition to the basic functionality of archive, view, and restore, users can view the Enterprise Vault properties of mailbox folders. If you allow them to do so, they can also modify these Enterprise Vault properties.

The User Extensions are supplied as a Microsoft® Windows® Installer (MSI) kit, which contains `EVClient<nn>.msi`, where `<nn>` is a number indicating the User Extensions version. You can deploy the MSI package using an Active Directory Group Policy as described in “Publishing in Active Directory” on page 100.

Notes:

- The computer must have Windows Installer version 1.2 or 2.0 in order to install the User Extensions.
- You can install the User silently by using the following command line:
  ```
  msiexec /qn /i EVClient<nn>.msi
  ```
  where `<nn>` is a number indicating the User Extensions version.

Self-installing User Extensions

The Self-Installing User Extensions is an ActiveX control that can be installed when a user opens a shortcut. The Self-Installing User Extensions are downloaded from a web page and then install automatically.
The Self-Installing User Extensions enable users to open Enterprise Vault shortcuts, search for archived items and read the archived items. They can restore, and perform manual archives, but cannot modify the default archiving settings. Additionally, users cannot make changes to any Enterprise Vault folder properties.

We supply two versions of the Self-Installing User Extensions kit:

- **EVDesktop.cab**: This is the file that is downloaded and installed automatically when a user opens a shortcut.
- **EVDesktop.msi**: This file is provided so that you can deploy the MSI package using an Active Directory Group Policy, as described in “Publishing in Active Directory” on page 100.

**Notes:**
- The computer must have Windows Installer version 1.2 or 2.0 in order to install the MSI kit.
- This kit can be installed silently.

**Distributing the User Extensions**

**Sending a shortcut**

A common method of distributing the User Extensions is to place a shortcut to the User Extensions Setup file into the Welcome message that is automatically sent to each enabled mailbox. Users can then click the shortcut to install the User Extensions.

Instructions on how to insert the shortcut into the Welcome message are included in the Welcome message itself. See “Editing the Welcome message” on page 254.

**Note:** The installer must be a member of the computer’s local Administrators group or be logged in as the Administrator on the local computer.

**Performing a silent installation**

If you have Microsoft Systems Management Server (SMS) available, you can use the supplied Package Definition file to create the silent installation package. See “Distributing the User Extensions using SMS”.

Make sure your users’ computers have the correct requirements, see “Requirements for users’ computers” on page 54.
Distributing the User Extensions using SMS

The User Extensions kit is in:

`Enterprise Vault\User Extensions\<lang>`

where `<lang>` indicates the language used.

To create an SMS package

1. Copy the complete User Extensions folder, and any subfolders, from the Enterprise Vault CD-ROM to a suitable location.
2. On the SMS server, click Start, then Programs, then Systems Management Server, then SMS Administrator Console.
3. In the left pane, expand Site Database until you see the Packages container.
4. Right-click the Packages container and, on the shortcut menu, click New and then Package From Definition. The Create Package from Definition wizard starts.
5. Click Next.
6. Click Browse and navigate to the folder containing the kit that you have chosen.
7. Click the .PDF file that you want to use and then click Open. The Package Definition page of the wizard shows that the Publisher is "kVault Software Ltd" and that Package definition is "KVS Enterprise Vault User Extensions".
8. Click Next.
9. Select either Always obtain files from a source directory or Create a compressed version of the source.
10. Click Next.
11. Specify the location of the kit files
12. Click Finish.

The package is now complete. You can distribute the package as required. See the Systems Management Server documentation if you need information on how to distribute a package.

Making the Self-Installing User Extensions available

When you install the Enterprise Vault services or the Administration Console, the Self-Installing User Extensions files are placed in the Enterprise Vault languages folder on your computer. This folder is normally:
Setting up users' desktops

Making the Self-Installing User Extensions available

C:\Program Files\Enterprise Vault\Languages\Self-Installing User Extensions\<lang>

where <lang> indicates the language used in the files.

If you intend to distribute the Self-Installing User Extensions through a web page, note that users without local Administrator permissions cannot install them because they are not allowed to install ActiveX controls from a web page. In this case, you must publish the Self-Installing User Extensions in Active Directory, as described in “Publishing in Active Directory” on page 100.

The following sections describe how to distribute the Self-Installing User Extensions through a web page. In summary, the process is as follows:

- Place the language folder you want to use into an IIS Virtual Directory; see “Copying the files” on page 97.
- Edit the Enterprise Vault Archived Item form to enable the automatic installation of the Self-Installing User Extensions. By default, the Self-Installing User Extensions is not enabled; see “Editing the archived item form” on page 98.
- Edit the Enterprise Vault Archived Item form to add the URL of the Self-Installing User Extensions files; see “Editing the archived item form” on page 98.
- Check that the edited form works correctly; see “Testing the edited form” on page 99.
- If necessary, publish the Self-Installing User Extensions in Active Directory; see “Publishing the edited form” on page 100.

Copying the files

The Self-Installing User Extensions kit is on the Enterprise Vault CD-ROM in the following location:

Enterprise Vault\Server\languages\Self-Installing User Extensions\<lang>

where <lang> indicates the language used.

Copy *.cab and *.htm from the language folder to a suitable IIS Virtual Directory that users will be able to download from.

Alternatively, create a new IIS Virtual Directory that points to the folder above the language folder in the hierarchy. Do not create the Virtual Directory so that it points to the language folder itself.

For example, if the language folder is:

D:\Enterprise Vault\Forms\en

then make the Virtual Directory point to:
Making the Self-Installing User Extensions available

D:\Enterprise Vault\Forms
If you are implementing an Enterprise Vault building blocks solution, create the same Virtual Directory on each of the Enterprise Vault servers and copy the files to those Virtual Directories. This ensures that, in the event of a fail-over, the Self-Installing User Extensions will still be available for download.

Editing the archived item form
You must edit the Archived Item form so that it includes a pointer to the IIS Virtual Directory that contains the language folder with the downloadable files. Once you have edited the form you need to install it in the Organization Forms Library, so you must use an account that has Owner permissions on the Organization Forms folder.
You can install the form from Microsoft Outlook using a mailbox that has Owner permissions for the folder in the Organization Forms Library.

To edit the form
1 On the Tools menu, click Options.
2 Click the Other tab.
3 Click Advanced Options.
4 Click Custom Forms.
5 Click Manage Forms.
6 On the left-hand side of the dialog box, click the Set button.
7 Click Forms Library and select the Organization Form Library folder that you created earlier, in “Distributing the Microsoft Exchange forms” on page 74.
8 On the right-hand side of the dialog box, click the Set button.
9 Click Forms Library and select Personal Forms.
10 In the list of Organization Forms, select Enterprise Vault – Archived Item.
11 Click Copy.
   The Archived Item form is copied to your Personal Forms library.
12 Click Close and then exit from all the dialog boxes.
13 On the Outlook Tools menu, click Forms and then Design a Form.
14 Next to Look In, select Personal Forms Library.
15 Click Enterprise Vault – Archived Item.
16 Hold down the Shift key and click Open.
The form opens, ready for you to make changes.

17 On the Form menu click View Code.

18 Scroll down the form to the Enterprise Vault Administrator section.

19 Find the following line:
   Const USE_SELF_INSTALLING_USER_EXTENSIONS=False

20 On this line, change False to True:
   Const USE_SELF_INSTALLING_USER_EXTENSIONS=True

21 Find the following line:
   Const DOWNLOAD_URL = "http://yourdomainhere"

22 On this line, change the URL so that it points to the IIS Virtual Directory that contains the language folder with the downloadable files. For example, if the full URL of the folder that the files are in is:
   http://server.mydomain.com/EVextensions/en
   then you would shorten the URL to:
   http://server.mydomain.com/EVextensions
   See also the example below.

23 On the form toolbar, click the Publish Form icon.
   The form is saved in your Personal Forms Library.

   For example, if the downloadable files are in:
   D:\Enterprise Vault\Forms\en
   then you can create a new IIS Virtual Directory Downloadable that maps to:
   D:\Enterprise Vault\Forms

   When editing the form, DOWNLOAD_URL becomes:
   DOWNLOAD_URL="http://server.mydomain.com/Downloadable/"

**Testing the edited form**

In order to test the form, you need a shortcut to an archived item and a computer that does not have the User Extensions installed.

1 If the computer has been used to open shortcuts before it will have a cached version of the Archived Item form. If this is the case, do the following:

   a Close Outlook.

   b Delete the Outlook file FRMCACHE.DAT. This is normally in
   C:\WINNT\forms\.

   c Start Outlook.
2 Double-click a shortcut to an archived item. A message gives you the option of downloading the Self-Installing User Extensions. Click Yes to download and install the software.

### Publishing the edited form

1 On the **Tools** menu, click **Options**.
2 Click the **Other** tab.
3 Click **Advanced Options**.
4 Click **Custom Forms**.
5 Click **Manage Forms**.
6 On the left-hand side of the dialog box, click the **Set** button.
7 Click **Forms Library** and select **Personal Forms**.
8 On the right-hand side of the dialog box, click the **Set** button.
9 Click **Forms Library** and select **Organization Forms**.
10 In the list of **Personal Forms**, select **Enterprise Vault – Archived Item**.
11 Click **Copy**. The Archived Item form is copied to the Organization Forms library.

### Publishing in Active Directory

You can publish the User Extensions and the Self-Installing User Extensions in Active Directory.

### Preparation

If you intend to distribute the Self-Installing User Extensions (**EVDesktop.msi**) through a web page, Windows Server 2003 and Windows 2000 users without local Administrator permissions cannot install them because they are not allowed to install ActiveX controls from a web page.

See the following Microsoft support articles for more information on publishing ActiveX controls in Windows 2000:

- **How to Publish ActiveX Controls in Windows 2000 Using IntelliMirror** ([http://support.microsoft.com/?kbid=241163](http://support.microsoft.com/?kbid=241163))
- **HOWTO: Install ActiveX Controls in Internet Explorer Using the Active Directory** ([http://support.microsoft.com/?kbid=280579](http://support.microsoft.com/?kbid=280579))
Setting up users’ desktops

Publishing in Active Directory

Note that, to permit the installation of the Self-Installing User Extensions, each user’s Windows Server 2003 or Windows 2000 computer must have a registry value with a name of UseCoInstall under the following registry key:

\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\UseCoInstall

UseCoInstall can be any type of value and can contain any or no data.

Publishing

To publish in Active Directory

1. Copy the appropriate file from the Enterprise Vault CD-ROM to the network share from which you want it to be distributed:
   - The file for the Self-Installing User Extensions is called EVDesktop.msi and is in:
     \Enterprise Vault\Languages\Self-Installing User Extensions\<language>
     where <language> indicates the language used in the files.
   - The file for the User Extensions is called EVClientm<nn>.msi, where <nn> is a number indicating the User Extensions version. The file is in:
     \Enterprise Vault\User Extensions\<language>
     where <language> indicates the user interface language.

2. Click Start, Programs, Administrative Tools, Active Directory Users and Computers.

3. In the left panel, navigate to the Organization Unit to which you want to make the Self-Installing User Extensions available.

4. Right-click the Organization Unit and, on the shortcut menu, click Properties.

5. Click the Group Policy tab.

6. Click New.
Enter a name for the new Group Policy Object, for example, “EV Desktop Rollout”.

With the new Click Edit. The Group Policy window appears.

In the left pane, under Computer Configuration, expand Software Settings.

Right-click Software installation and, on the shortcut menu, click New and then Package.

Type in the UNC path of the MSI file that you copied in step 1, for example, \\mycomputer\distribute, and then click Open.

The Deploy Software window opens.

Select Assigned and click OK.

The new package appears in the list of software installations.

Close the Group Policy window.

The new package will be installed when each user’s computer is restarted.

Outlook 2003

If an Outlook 2003 user has enabled Use Cached Exchange Mode, then by default Outlook forms are not synchronized. This results in archived items not showing Enterprise Vault icons.

The solution is to make Outlook synchronize forms, as follows:

1. Start Outlook.
2. Click Tools, then Send/Receive, then Send/Receive Settings
3. Click Define Send/Receive Groups
4. Select All Accounts Online and Offline and click Edit
5. Select Synchronize Forms
6. Exit from Outlook and then restart it.
7. Open an archived item. This automatically installs the forms.

Getting users started

You should ensure that users know how to install the Enterprise Vault user extensions, if necessary, using one of the methods described in this chapter, and how to use Enterprise Vault.

Users’ browsers must have Java scripting enabled.

Also ensure that the Microsoft Exchange Forms for Enterprise Vault have been installed on all Microsoft Exchange Server computers that are being processed.
by Enterprise Vault; see “Distributing the Microsoft Exchange forms” on page 74.

Documentation

The following documentation is available to users:
■ Online Help when using Outlook.
■ Online Help in the web browser when using the Web Access application.

What next?

You should now have a fully functioning Enterprise Vault system. You may find over time that you need to change some of the properties of Enterprise Vault to suit your requirements. For details about these and any other features of Enterprise Vault, refer to the online Help.
Setting up users’ desktops

What next?
Licenses and license keys

Read this chapter to:
- Learn about Demonstration, Evaluation, and Production modes
- Find out how to obtain Enterprise Vault license keys
- Find out how to install the license keys

Overview

You must install suitable licenses in order to run Enterprise Vault services. Enterprise Vault runs in one of three modes:

- **Production mode.** In this mode, a production license key is installed and the functionality of Enterprise Vault depends on the licenses that you have purchased.

- **Evaluation mode.** In this mode, an Evaluation license key is installed and the full functionality of Enterprise Vault is available, but the functionality is time-limited, as defined by the key. When the Evaluation license expires, the software continues to run in Demonstration mode.

- **Demonstration mode.** Enterprise Vault uses this mode when a license key expires, or if no license key is installed. Users can restore items, but there is no archiving. Exchange Mailbox, Exchange Public Folder, and Exchange Journaling tasks will not start, and you cannot migrate the contents of personal folder (PST) files to Enterprise Vault.

You can get license keys from your Enterprise Vault supplier, as described below.
Obtaining license keys

When Enterprise Vault services are installed on a computer, a file of computer-specific system information is automatically created. You can obtain license keys in one of two ways:

- Your supplier may obtain the license keys for you. Once you have the keys, install them as described below.
- You can obtain the keys yourself, as described below.

If you are going to obtain the keys yourself, do the following:
1. Contact Symantec Corporation to obtain your license keys.
2. When you have obtained the license keys, install them as described in the instructions that are supplied with the keys.

What next?

You can change from one mode to another by obtaining appropriate licenses and keys from your supplier and then installing the new keys.

If you have obtained Evaluation mode licenses, the license keys will expire at the end of the license period and Enterprise Vault will revert to running in Demonstration mode. You can upgrade to Production mode by obtaining new license keys.
This section includes the following chapters:

- Chapter 11, “Configuring OWA access to Enterprise Vault” on page 109
- Chapter 12, “Configuring OWA and RPC Extensions in clustered configurations” on page 145
- Chapter 13, “Using Microsoft ISA Server with OWA and RPC Extensions” on page 157
- Chapter 14, “How to uninstall Enterprise Vault OWA Extensions” on page 177
- Chapter 15, “Configuring RPC over HTTP access to Enterprise Vault” on page 183
Configuring OWA access to Enterprise Vault

Read this chapter to find out:

- The Enterprise Vault functionality available with different OWA clients
- How Enterprise Vault is supported in different OWA configurations
- Prerequisite software
- How to configure Enterprise Vault access for OWA 2003 users
- How to configure Enterprise Vault access for OWA 2000 users
- How to configure Enterprise Vault access for OWA 5.5 users
- How to upgrade existing Enterprise Vault OWA Extensions
- How to configure a simple environment to demonstrate or pilot Enterprise Vault OWA functionality
- Advice on troubleshooting OWA Extensions

Enterprise Vault functionality in OWA clients

The Enterprise Vault functionality available to users depends on the version of OWA running on the Exchange servers.

See “Enterprise Vault features in OWA clients” on page 110.
With OWA 2003, OWA configuration options in the Enterprise Vault Administration Console (in the mailbox policy properties) enable you to
customize the Enterprise Vault options available in OWA 2003 Premium and Basic clients. See the Administrator’s Guide for more details.

### Table 11-1  Enterprise Vault features in OWA clients

<table>
<thead>
<tr>
<th>OWA version</th>
<th>Enterprise Vault functionality</th>
</tr>
</thead>
</table>
| OWA 2003    | - View items using standard OWA functionality  
- Reply to and forward shortcuts or original items (using standard OWA functionality)  
- Archive items and folders using Enterprise Vault buttons or menu options. Default archiving properties can be changed.  
- Restore items using Enterprise Vault buttons or menu options. Restore properties can be set.  
- Delete shortcuts and/or archived items using Enterprise Vault buttons or menu options or standard OWA functionality  
- Archive Explorer button.  
- Search Archives button.  
- View archived public folder items.  
- Administrator can configure Enterprise Vault functionality available in Premium and Basic clients. |
| OWA 2000    | - View items.  
- Reply to and forward shortcuts (using standard OWA functionality).  
- Delete shortcuts (using standard OWA functionality).  
- View archived public folder items. |
| OWA 5.5     | - View items.  
- Reply to and forward shortcuts (using standard OWA functionality). This requires additional configuration.  
- Delete shortcuts (using standard OWA functionality).  
- View archived public folder items. |

### About forms-based authentication in OWA 2003 clients

When using Enterprise Vault 5.0 OWA Extensions with forms-based authentication, OWA 2003 client users are prompted to re-authenticate when they first open an archived item or when they use archive search or archive explorer. This happens because the IIS virtual directory to which the user requests are directed is outside the Exchange virtual directory and uses different authentication. The authentication is valid for the session.

In Enterprise Vault 6.0, the OWA Extensions work differently. When using forms-based authentication, OWA 2003 client users are not prompted to re-enter login credentials when opening archived items. However, if the user
starts the archive search or Archive Explorer features in the OWA client, then they will be prompted for login credentials. As in Enterprise Vault 5.0, this is because the request accesses a different IIS virtual directory which uses different authentication.

With Enterprise Vault 6.0 OWA Extensions, behavior reverts to that of Enterprise Vault 5.0 in the following cases:

- If View mode is set to Enterprise Vault in the OWA 2003 settings on the Advanced page of the Exchange mailbox policy. This setting controls what happens when a user clicks Open the original item in the banner of a custom shortcut. If OWA is set, then the original item is rendered by OWA (and looks like an OWA message). If Enterprise Vault is set, then item is rendered by Enterprise Vault (and looks like a web browser page).

- If there is a problem viewing or restoring the item. In this situation, the OWA Extensions revert to using Enterprise Vault to render the items and the user is prompted for login details.

**OWA configurations**

The following figures give examples of some typical OWA configurations supported by Enterprise Vault. The types of authentication supported for each connection is also shown.
In “Front-end/back-end example configuration” there is one Exchange server configured as a front-end OWA server and two Exchange servers configured as back-end OWA servers. OWA client browser sessions connect to the front-end server.

Enterprise Vault OWA Extensions are installed on all front-end and back-end Exchange servers.

If the front-end OWA server is running Exchange Server 2003 and the back-end OWA server is running Exchange Server 2000, clients will only have the Enterprise Vault functionality available with OWA 2000 Extensions (see “Enterprise Vault features in OWA clients” on page 110).

Typically, users connect to the front-end server using basic authentication. Integrated Windows Authentication (IWA) is used for the connection between Exchange servers and anonymous authentication is used for the connection between the back-end Exchange server and the Enterprise Vault server.

On the Enterprise Vault servers, a special user is created and configured to manage the anonymous connections from OWA servers.
In “Back-end only example configuration” there are no front-end OWA servers. Instead, users connect to one of two Exchange servers configured as back-end OWA servers. This configuration can provide more security, as you can force users to use IWA authentication instead of basic authentication when connecting to the OWA servers. Anonymous authentication is used for the connection between the Exchange server and the Enterprise Vault server.
Figure 11-3  Clustered OWA servers example

“Clustered OWA servers example” gives an example of an active/passive cluster of OWA servers. In this configuration, Enterprise Vault OWA Extensions must be installed and configured on both Exchange servers in the cluster. Enterprise Vault automatically adds the necessary cluster addresses to its configuration files when you configure the OWA Extensions. There could also be a front-end OWA server, but this would not normally be included in a cluster configuration.

When one OWA server in the cluster fails over to the other, connections to the Enterprise Vault servers are established automatically, as shown in “Configuration after failover”; users can continue to access items in their Enterprise Vault archives.
If you have more than one virtual HTTP server on the front-end or back-end OWA server, for example to support connections from multiple domains, you must perform additional configuration steps to enable access to Enterprise Vault archives. This configuration is beyond the scope of this guide. For details of the steps required, contact Symantec Support.

To demonstrate the use of OWA with Enterprise Vault, you can set up all the required servers and OWA Extensions on one computer. See “Configuring a demonstration system” on page 142 for instructions on how to configure such configurations.

“Exchange 5.5 configuration example” shows a typical configuration example for OWA on Exchange Server 5.5. The OWA Extensions do not need to be configured and the Anonymous user is not required on the Enterprise Vault server. However, WinHTTP must be configured on the OWA 5.5 server with the correct proxy bypass list.
If you are setting up an Enterprise Vault environment to demonstrate or pilot OWA access to Enterprise Vault archives, the Enterprise Vault server and Exchange server can be installed on one computer.

See "Configuring a demonstration system" on page 142.

Prerequisite software

In addition to the prerequisite software for the Enterprise Vault server, there are the following software requirements for OWA Exchange Servers and OWA clients:

- Enterprise Vault OWA Extensions need to be installed on all front-end and back-end OWA Exchange servers. The table, “Enterprise Vault OWA Extensions to install”, shows which OWA Extensions you need to install on your Exchange servers.
  
The Enterprise Vault Extensions for OWA 2003 servers are named Exchange 2003 Front-end Ext. (OWA & RPC) and Exchange 2003 Back-end
Configuring OWA access to Enterprise Vault

Prerequisite software

Ext. (OWA & RPC), because they are also used for configuring RPC over HTTP connections.

Table 11-2  Enterprise Vault OWA Extensions to install

<table>
<thead>
<tr>
<th>If you have this</th>
<th>Install this</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Exchange 2003 Front-end Extensions (OWA &amp; RPC) or Exchange 2000 OWA Extensions (Front-end) on each front-end server.</td>
</tr>
<tr>
<td>Exchange Server 5.5</td>
<td>Exchange Server 5.5 OWA Extensions on your OWA server.</td>
</tr>
</tbody>
</table>

Note that the Enterprise Vault buttons are not available in OWA clients when using OWA 5.5 and OWA 2000, which means that you can only view archived items with these extensions. To be able to archive, restore and delete archived items from your OWA client and have integrated access to Archive Explorer and Search features, you need to use OWA 2003 on Exchange Server 2003.

- If you are running Microsoft Exchange Server 2003 on OWA servers, Microsoft Exchange Server 2003 Service Pack 1 or later is required.
- As Enterprise Vault OWA Extensions modify OWA control files on Exchange Server 2003, the version of these files must be one that is supported by Enterprise Vault.

At this release, the control file versions supported are

- 6.5.7226.0
- 6.5.7638.1
- 6.5.7651.9
- 6.5.7651.25

Exchange Server 2003 hotfixes may modify OWA control files. If you have installed an Exchange Server 2003 hotfix that has created an unsupported version of the OWA control files folder, or modified any files in the control
files folder, a “Save file error” will be reported when you attempt to install the Enterprise Vault OWA Extensions.

- If the back end OWA server computer is running Windows 2000, it requires either Windows 2000 SP3, or SP2 and a Microsoft hotfix, because of a problem with IIS 5.0. The problem is described in Microsoft support article 294833. If this is not installed, the OWA preview pane shows the following error instead of the shortcut content:
  Error type:
  Active Server Pages, ASP 0110 (0x80004005)
  Unable to Allocate required memory.
  \EVowa/preview.asp, line 2

- MSXML is required on Exchange OWA servers (with the exception of front-end OWA 2000 servers). This is installed automatically with Internet Explorer 6 web browser, which comes as the default with Windows Server 2003. On Windows 2000, you can select Internet Explorer 6 from a Customized installation.
  If you are using an earlier version of Internet Explorer, you may need to install MSXML version 3.0 SP2. This is available from the link, Download Microsoft XML Parser (MSXML) 3.0 Service Pack 5, in the Redistributable Software folder on the Enterprise Vault CD-ROM. Windows Installer is required in order to install MSXML version 3.0 SP2.

- On user desktops, Internet Explorer 5.5 SP2 or later is required to support the full functionality available with OWA 2003 clients.

Configuring Enterprise Vault access for OWA 2003 users

This section describes how to configure Enterprise Vault servers and Exchange Server 2003 computers to enable Enterprise Vault access for OWA 2003 users. The required steps can be summarized as follows:

- If your Exchange Servers are clustered, there is additional information that you need to read before proceeding.
  See “Supported cluster configurations” on page 146
  See “OWA: Configuring Enterprise Vault Extensions in active/passive Microsoft clusters” on page 148
  See “OWA: Configuring Enterprise Vault Extensions in an active/active Microsoft cluster” on page 151
  See “Configuring Enterprise Vault OWA and RPC Extensions on VCS” on page 155
On Enterprise Vault servers, configure the Anonymous user account to handle connections from back-end Exchange servers.


On back-end Exchange Server 2003 computers, run the Enterprise Vault configuration program for the Enterprise Vault OWA Extensions.

Use an OWA client browser session on each back-end Exchange Server to check the Enterprise Vault OWA configuration.


On front-end Exchange Server 2003 computers, run the Enterprise Vault configuration program for the Enterprise Vault OWA Extensions.

Use an OWA client browser session on each front-end Exchange Server to check the complete Enterprise Vault OWA configuration.

OWA 2003: Configuring Anonymous user on the Enterprise Vault server

On Enterprise Vault servers that support connections from OWA 2003 or OWA 2000 servers, follow the instructions in this section to configure a special user account for handling anonymous connections from OWA servers.

To configure OWA access on the Enterprise Vault server, you need to perform the following steps:

- Create the ExchangeServers.txt file on the Enterprise Vault server. This holds a list of the IP addresses for all the back-end OWA servers that will connect to the Enterprise Vault server.

- Create or select domain account to be used for Anonymous connections.

- Run the script, owauser.wsf, to configure the Anonymous user.

- Synchronize mailboxes and restart Enterprise Vault Admin service.

To create the ExchangeServers.txt file

1. Open Notepad.

2. Type the IP address of each back-end OWA server (that is, the Exchange Virtual Server IP address), one entry per line.
   If the OWA servers are clustered, enter the Virtual Server IP addresses first and then add the cluster IP address and the IP addresses of each node.
3 Save the file as `ExchangeServers.txt` in the Enterprise Vault installation folder (typically `C:\Program Files\Enterprise Vault`).

4 Close Notepad.

To configure the Anonymous user account for OWA

1 Create a domain user account to use as the Anonymous user account. This should be a basic domain account specifically created for the purpose; a local machine account cannot be used.
   If you are upgrading your OWA Extensions and the existing Anonymous user account is a domain account, then use this account. If your existing Anonymous user account is a local machine account, then you will need to create a new domain account for the Anonymous user.

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

3 Open a command prompt window and navigate to the Enterprise Vault installation folder.

4 Type and enter the command line:
   ```
cscript owauuser.wsf /domain:<domain> /user:<username> /password:<password> /exch2003
   ```
   The file `owauuser.wsf` is installed in the Enterprise Vault installation folder.
   For `<domain>`, give the domain of the Anonymous user account.
   For `<username>`, give the username of the Anonymous user account.
   For `<password>`, give the password of the Anonymous user account.
   To display help for the `cscript` command, type
   ```
cscript owauuser.wsf /?
   ```

5 The progress of the script execution is displayed in the command prompt window.
   See “What owauuser.wsf configures”.
   When the configuration script finishes, you are prompted to restart the Enterprise Vault Admin service and synchronize mailboxes.
   See “Restarting the Admin service and synchronizing mailboxes”.

6 Now you can install the OWA Extensions on back-end Exchange Server computers.

What owauuser.wsf configures

The `owauuser.wsf` script sets up the following on the Enterprise Vault server:
Assigns the following user rights to the Anonymous user:

- SeNetworkLogonRight
- SeInteractiveLogonRight
- SeBatchLogonRight
- SeChangeNotifyPrivilege

Creates (or updates) the new virtual directory, EVAnon, that points to the Enterprise Vault\WebApp folder and assigns anonymous access permissions to the OWA Anonymous user.

Access to EVAnon is also granted to the back-end OWA servers. You can check this by displaying the properties of the EVAnon virtual directory, selecting the Directory Security tab and clicking Edit in the IP address and domain name restrictions section.

Creating (or updates) the following two Registry values:

- HKEY_CURRENT_USER\Software\KVS\Enterprise Vault\AnonymousUser
  The value of this setting is the full name, including the domain, of the Anonymous user. For example, mydomain\EVOWAUSER

- HKEY_LOCAL_MACHINE\SOFTWARE\KVS\Enterprise Vault\Install\OwaWebAppAlias
  The value of this setting is the name of the virtual directory for anonymous connections, EVAnon.

Restarting the Admin service and synchronizing mailboxes

To complete the configuration, you need to restart the Enterprise Vault Admin service and synchronize mailboxes, as described in this section.

To restart the Admin service

1. Open Control Panel, select Administrative Tools and then select Services.
2. Right-click Enterprise Vault Admin Service and select Restart. Enterprise Vault services and tasks will restart.
3. Close the Services console.
To synchronize mailboxes

1. Click Start > Programs > Enterprise Vault Administration Console.
2. Expand the Enterprise Vault Directory container and then your site. Expand Computers and select the required Enterprise Vault server. Expand this container. Expand Tasks.
3. In the right hand pane, double click the Mailbox Archiving task for the Exchange server, to display the properties window for the task.
4. Select the Synchronization tab. Make sure All mailboxes and Mailbox properties and permissions are selected.
5. Click Synchronize.
6. Click OK to close the properties window.
7. Close the Enterprise Vault Administration Console.

Installing OWA Extensions on a back-end Exchange Server 2003

Follow the instructions in this section to install the Enterprise Vault OWA Extensions from the Enterprise Vault CD-ROM.

To install Enterprise Vault OWA Extensions

2. Open the Enterprise Vault folder. Check the ReadMeFirst.htm file in this folder for details of any last minute changes.
3. Open the Server folder.
4. Double-click SETUP.EXE to start the installation.
5. Follow the installation instructions and select the Exchange 2003 Back-end Ext. (OWA & RPC) component. See “Prerequisite software” on page 116.
   Exchange Server 2003 hotfixes may modify OWA control files. If you have installed an Exchange Server 2003 hotfix that has created an unsupported version of the OWA control files folder, or modified any files in the control files folder, a “Save file error” will be reported when you attempt to install the Enterprise Vault OWA Extensions.
6. On each back-end OWA 2003 server, you now need to configure the extensions.
Configuring a back-end Exchange Server 2003

After you have installed the OWA Extensions on back-end Exchange Server 2003 computers, configure the OWA Extensions, as described in this section. The Exchange back-end servers require direct access to the Enterprise Vault server, and must not go via a proxy. The configuration program creates WinHTTP proxy bypass entries for each Exchange server that will connect to the Enterprise Vault server.

To enable the configuration program to add the required entries to the proxy bypass list, create the EVServers.txt file as described in this section. You must create and populate the EVServers.txt file, even if you do not use a proxy server.

The steps to configure a back-end Exchange server are as follows:

- Create at least one public folder before you run the configuration program. As Microsoft Exchange installation automatically creates a public folder store, Enterprise Vault will attempt to register forms against public folders.
- Create the EVServers.txt file and add entries for the proxy bypass list.
- Run the OWA Extensions configuration program from the Start menu.

To create the EVServers.txt file

1. Open Notepad.
2. Type in, one entry per line, the Vault Site alias in both fully-qualified and LanMan forms. For example:
   ourvaultsitealias.domain.com
   ourvaultsitealias
   Also type in any aliases for each Enterprise Vault server computer in the Vault Site. Enter these one per line, in fully-qualified and LanMan forms. For example:
   vault1alias.domain.com
   vault1alias
3. Save the file as EVServers.txt in the OWA folder in your Enterprise Vault installation folder (typically, C:\Program Files\Enterprise Vault \OWA).

To run the OWA Extensions configuration program on a back-end Exchange server

1. Log on to the Exchange server computer using an account that has Exchange Full Administrator permission.
2 Ensure the Exchange server is running and that the web site associated with the Exchange server has an ExAdmin virtual directory created.

3 To start the configuration program, click Start > Programs, Enterprise Vault > Exchange 2003 Back-end Ext. Configuration (OWA & RPC).

4 A command prompt window opens and lists what the configuration program has done. The program configures the following for each Exchange virtual server it finds on the computer:
   - An EnterpriseVaultProxy virtual directory for each web server on the computer.
   - An EVOWA virtual directory for each web server on the computer.
   - A virtual directory called EnterpriseVaultname for each Exchange mailbox and public folder virtual directory. name is the name of the associated Exchange virtual directory.
     For example, if Exchange virtual directories are called Exchange and Public, virtual directories called EnterpriseVaultExchange and EnterpriseVaultPublic will be created.
   - Execution of scripts is enabled in the settings of the Exchange mailbox and public folder virtual directories.
   - Enterprise Vault forms are registered.
     See “About Enterprise Vault forms registration”.
   - Entries in the proxy bypass list from the EVServers.txt file.

5 When the configuration program has finished, you will see the following line in the command prompt window:
   Press ENTER to end

6 Details of the configuration process are sent to the log file:
   Enterprise Vault\OWA\BackEnd2003Setup.wsf.log
   Check the log file for any configuration errors.

7 From a browser, enter the URL for the back-end OWA server. Open an OWA client and check that you can view archived items. In OWA 2003 clients, you should also see the Enterprise Vault buttons. Archive Explorer and Search options should be displayed in the navigation pane.

8 Repeat the above steps to configure the OWA Extensions on each back-end Exchange server.

9 You can now install the OWA Extensions on front-end Exchange Server computers.
About Enterprise Vault forms registration
The back-end OWA 2003 Extensions register both Enterprise Vault mailbox and public folder forms in a new folder, KVS, under the schema-root.

To view this folder in a public folder store
1. Start Exchange System Manager.
2. Right-click Public Folders and select View system folders.
3. Expand schema-root. This displays a folder called KVS.
4. Expand the KVS folder. OWA 2000 forms and OWA 2003 forms are registered in separate folders called OWA2000Forms or OWA2003Forms respectively. If you have a mixed environment, the OWA Extensions automatically create both folders. However, on Exchange Server 2000, only the OWA2000Forms folder is populated and on Exchange Server 2003, only the OWA2003Forms folder is populated.

Installing OWA Extensions on a front-end Exchange Server 2003
Follow the instructions in this section to install the Enterprise Vault OWA Extensions from the Enterprise Vault CD-ROM.

To install Enterprise Vault OWA Extensions
2. Open the Enterprise Vault folder. Check the ReadMeFirst.htm file in this folder for details of any last minute changes.
3. Open the Server folder.
4. Double-click SETUP.EXE to start the installation.
5. Follow the installation instructions and select the Exchange 2003 Front-end Ext. (OWA & RPC) component. See “Prerequisite software” on page 116.
   Exchange Server 2003 hotfixes may modify OWA control files. If you have installed an Exchange Server 2003 hotfix that has created an unsupported version of the OWA control files folder, or modified any files in the control files folder, a “Save file error” will be reported when you attempt to install the Enterprise Vault OWA Extensions.
6. On each front-end OWA 2003 server, you now need to configure the extensions.
Configuring a front-end Exchange Server 2003

After you have installed the OWA Extensions on a front-end Exchange Server 2003 computer, you need to configure the extensions, as described in this section.

To run the OWA configuration program on a front-end Exchange Server 2003

1. Log on to the Exchange Server computer using an account that has Exchange Full Administrator Permission.
3. A command prompt window opens and lists what the configuration program has done.
   The program configures the following for each Exchange virtual server it finds on the computer:
   - An EnterpriseVaultProxy virtual directory for each web server on the computer.
   - Adds the names of back-end Exchange servers to the proxy bypass list.
4. When the configuration program has finished, you will see the following line in the command prompt window:
   Press ENTER to end
5. Details of the configuration process are sent to the log file:
   Enterprise Vault\OWA\FrontEnd2003Setup.wsf.log
   Check the log file for any configuration errors.
6. From a browser, enter the URL for the front-end OWA server. Open an OWA client and check that you can view archived items. In OWA 2003 clients, you should also see the Enterprise Vault buttons. Archive Explorer and Search options should be displayed in the navigation pane.
7. Repeat the above steps to configure the OWA Extensions on each front-end Exchange Server 2003.

This completes the basic configuration of your Enterprise Vault OWA environment.

If required, the functionality available to OWA 2003 users can be customized by administrators using the Enterprise Vault Administration Console; select OWA 2003 settings on the Advanced tab of the appropriate Exchange Server mailbox policy.

If your OWA environment includes a Microsoft ISA Server 2004 server, then you will also need to configure this to enable Enterprise Vault OWA users to access
Configuring OWA access to Enterprise Vault

Configuring Enterprise Vault access for OWA 2000 users

This section describes how to configure Enterprise Vault servers and Exchange Server 2000 computers to enable Enterprise Vault access for OWA 2000 users. The required steps can be summarized as follows:

- If your Exchange Servers are clustered, there is additional information that you need to read before proceeding.
  See “Supported cluster configurations” on page 146
  See “OWA: Configuring Enterprise Vault Extensions in active/passive Microsoft clusters” on page 148
  See “OWA: Configuring Enterprise Vault Extensions in an active/active Microsoft cluster” on page 151
  See “Configuring Enterprise Vault OWA and RPC Extensions on VCS” on page 155

- On Enterprise Vault servers, configure the Anonymous user account to handle connections from back-end Exchange Servers.

- On each back-end Exchange Server 2000, install the Enterprise Vault OWA Extensions.

- On back-end Exchange Server 2000 computers, run the Enterprise Vault configuration program for the Enterprise Vault OWA Extensions.

- Use an OWA client browser session on each back-end Exchange Server to check the Enterprise Vault OWA configuration.


- Use an OWA client browser session on each front-end Exchange Server to check the complete Enterprise Vault OWA configuration.
OWA 2000: Configuring Anonymous user on the Enterprise Vault server

On Enterprise Vault servers that support connections from OWA 2003 or OWA 2000 servers, follow the instructions in this section to configure a special user account for handling anonymous connections from OWA servers.

To configure OWA access on the Enterprise Vault server, you need to perform the following steps:

- Create the `ExchangeServers.txt` file on the Enterprise Vault server. This holds a list of the IP addresses for all the back-end OWA servers that will connect to the Enterprise Vault server.
- Create or select domain account to be used for Anonymous connections.
- Run the script, `owauser.wsf`, to configure the Anonymous user.
- Restart the Enterprise Vault Admin service and synchronize mailboxes.

To create the `ExchangeServers.txt` file

1. Open Notepad.
2. Type the IP address of each back-end OWA server (that is, the Exchange Virtual Server IP address), one entry per line.
   - If the OWA servers are clustered, enter the Virtual Server IP addresses first and then add the cluster IP address and the IP addresses of each node.
3. Save the file as `ExchangeServers.txt` in the Enterprise Vault installation folder (typically `C:\Program Files\Enterprise Vault`).

To configure the Anonymous user account for OWA

1. Create a domain user account to use as the Anonymous user account. This should be a basic domain account specifically created for the purpose; a local machine account cannot be used.
   - If you are upgrading your OWA Extensions and the existing Anonymous user account is a domain account, then use this account. If your existing Anonymous user account is a local machine account, then you will need to create a new domain account for the Anonymous user.
2. Log on to the Enterprise Vault server as the Vault Service account.
3. Open a command prompt window and navigate to the Enterprise Vault installation folder.
4. Type and enter the command line:
Configuring OWA access to Enterprise Vault

Configuring Enterprise Vault access for OWA 2000 users


The file owuser.wsf is installed in the Enterprise Vault installation folder.
For <domain>, give the domain of the Anonymous user account.
For <username>, give the username of the Anonymous user account.
For <password>, give the password of the Anonymous user account.
To display help for the cscript command, type
cscript owuser.wsf /?

5 The progress of the script execution is displayed in the command prompt window.
See “What owuser.wsf configures”.
When the configuration script finishes, you are prompted to synchronize mailboxes and restart the Enterprise Vault Admin service.
See “Restarting the Admin service and synchronizing mailboxes” on page 130.

6 Now you can install the OWA Extensions on each back-end Exchange Server computers.
See “Installing OWA Extensions on a back-end Exchange Server 2000” on page 130.

What owuser.wsf configures

The owuser.wsf script sets up the following on the Enterprise Vault server:

- Assigns the following user rights to the Anonymous user:
  - SeNetworkLogonRight
  - SeInteractiveLogonRight
  - SeBatchLogonRight
  - SeChangeNotifyPrivilege
- Updates the IIS settings for the OWARDR.asp file in the EnterpriseVault virtual directory, so that requests for OWARDR.asp are run under the context of the OWA Anonymous user.
Access to OWARDR.asp is only granted to the back-end OWA servers. You can check this by displaying the properties of the OWARDR.asp file, selecting the File Security tab and clicking Edit in the IP address and domain name restrictions section.
- Creates (or updates) the following Registry value:
  HKEY_CURRENT_USER
  \Software
Configuring OWA access to Enterprise Vault

Configuring Enterprise Vault access for OWA 2000 users

\KVS
\Enterprise Vault
\AnonymousUser

The value of this setting is the full name, including the domain, of the Anonymous user. For example, mydomain\EVOWAUSER

Restarting the Admin service and synchronizing mailboxes
To complete the configuration, you need to restart the Enterprise Vault Admin service and synchronize mailboxes, as described in this section.

To restart the Admin service
1 Open Control Panel, select Administrative Tools and then select Services.
2 Right-click Enterprise Vault Admin Service and select Restart. Enterprise Vault services and tasks will restart.
3 Close the Services console.

To synchronize mailboxes
1 Click Start > Programs > Enterprise Vault Administration Console.
2 Expand the Enterprise Vault Directory container and then your site. Expand Computers and select the required Enterprise Vault server. Expand this container. Expand Tasks.
3 In the right hand pane, double click the Mailbox Archiving task for the Exchange server, to display the properties window for the task.
4 Select the Synchronization tab. Make sure All mailboxes and Mailbox properties and permissions are selected.
5 Click Synchronize.
6 Click OK to close the properties window.
7 Close the Enterprise Vault Administration Console.

Installing OWA Extensions on a back-end Exchange Server 2000
Follow the instructions in this section to install the Enterprise Vault OWA Extensions from the Enterprise Vault CD-ROM.

To install Enterprise Vault OWA Extensions
1 On your Exchange server, load the Enterprise Vault CD-ROM into the CD-ROM drive.
2 Open the Enterprise Vault folder. Check the ReadMeFirst.htm file in this folder for details of any last minute changes.

3 Open the Server folder.

4 Double-click SETUP.EXE to start the installation.

5 Follow the installation instructions and select the correct OWA Extensions component for this Exchange server.

6 On each back-end OWA 2000 server, you now need to configure the extensions.

Configuring a back-end Exchange Server 2000

After you have installed the OWA Extensions on back-end Exchange Server 2000 computers, configure the OWA Extensions, as described in this section. Enterprise Vault requires direct access to the Exchange back-end server, and must not go via a proxy. The configuration program creates WinHTTP proxy bypass entries for each Exchange server that will connect to the Enterprise Vault server.

To enable the configuration program to add the required entries to the proxy bypass list, create the EVServers.txt file as described in this section. You must create and populate the EVServers.txt file, even if you do not use a proxy server.

The steps to configure a back-end Exchange server are as follows:

- Create at least one public folder before you run the configuration program. As Microsoft Exchange installation automatically creates a public folder store, Enterprise Vault will attempt to register forms against public folders.
- Create the EVServers.txt file and add entries for the proxy bypass list.
- Run the OWA Extensions configuration program from the Start menu.

To create the EVServers.txt file

1 Open Notepad.

2 Type in, one entry per line, the Vault Site alias in both fully-qualified and LanMan forms. For example:

ourvaultsitealias.domain.com
ourvaultsitealias

Also type in any aliases for each Enterprise Vault server computer in the Vault Site. Enter these one per line, in fully-qualified and LanMan forms. For example:

vaulttalias.domain.com
vaulttalias
3 Save the file as EVServers.txt in the OWA folder in your Enterprise Vault installation folder (typically, C:\Program Files\Enterprise Vault\OWA).

4 Close Notepad.

To run the OWA Extensions configuration program on a back-end Exchange server

1 Log on to the Exchange server computer using an account that has Exchange Full Administrator permission.

2 Ensure the Exchange server is running and that the web site associated with the Exchange server has an ExAdmin virtual directory created.

3 To start the configuration program, click Start > Programs, Enterprise Vault > Exchange 2000 OWA Extensions Configuration.

4 A command prompt window opens and lists what the configuration program has done. The program configures the following for each Exchange virtual server it finds on the computer:
   ■ An EVOWA virtual directory for each web server on the computer.
   ■ A virtual directory called EnterpriseVaultname for each Exchange mailbox and public folder virtual directory. name is the name of the associated Exchange virtual directory.
     For example, if Exchange virtual directories are called Exchange and Public, virtual directories called EnterpriseVaultExchange and EnterpriseVaultPublic will be created.
   ■ Execution of scripts is enabled in the settings of the Exchange mailbox and public folder virtual directories.
   ■ Enterprise Vault forms are registered.
     See “About Enterprise Vault forms registration”.
   ■ Entries in the proxy bypass list from the EVServers.txt file.

5 When the configuration program has finished, you will see the following line in the command prompt window:
   Press ENTER to end

6 Details of the configuration process are sent to the log file:
   Enterprise Vault\OWA\Backend2000Setup.wsf.log
   Check the log file for any configuration errors.
7. Now check the configuration on each back-end OWA server. From a browser, enter the URL for the back-end OWA server. Open an OWA client and check that you can view archived items.

8. Repeat the above steps to configure the OWA Extensions on each back-end Exchange Server.

9. You can now install the OWA Extensions on each front-end Exchange Server 2000 computer.

**About Enterprise Vault forms registration**

The back-end OWA 2000 Extensions register both Enterprise Vault mailbox and public folder forms in a new folder, **KVS**, under the schema-root.

To view this folder

1. Start Exchange System Manager.
2. Right-click **Public Folders** and select **View system folders**.
3. Expand schema-root. This displays a folder called **KVS**.
4. Expand the **KVS** folder. OWA 2000 forms and OWA 2003 forms are registered in separate folders called **OWA2000Forms** or **OWA2003Forms** respectively.
   
   If you have a mixed environment, the OWA Extensions automatically create both folders. However, on Exchange Server 2000, only the **OWA2000Forms** folder is populated and on Exchange Server 2003, only the **OWA2003Forms** folder is populated.

**Installs OWA Extensions on a front-end Exchange Server 2000**

Follow the instructions in this section to install the Enterprise Vault OWA Extensions from the Enterprise Vault CD-ROM.

To install Enterprise Vault OWA Extensions

2. Open the **Enterprise Vault** folder. Check the **ReadMeFirst.htm** file in this folder for details of any last minute changes.
3. Open the **Server** folder.
4. Double-click **SETUP.EXE** to start the installation.
5. Follow the installation instructions and select the correct OWA Extensions component for this Exchange server.
You do not need to configure front-end OWA 2000 Extensions.

6 From a browser, enter the URL for the front-end OWA server. Open an OWA client and check that you can view archived items.

7 Repeat the above steps to configure the OWA Extensions for each front-end Exchange Server 2000.

This completes the basic configuration of your Enterprise Vault OWA environment.

If your OWA environment includes a Microsoft ISA Server 2004 server, then you will also need to configure this to enable Enterprise Vault OWA users to access the archived items. The following sections describe how to configure the ISA Server for Basic or Forms-Based authentication:

- "Configuring ISA Server 2004 for OWA Basic Authentication" on page 158
- "Configuring ISA Server 2004 for OWA forms-based authentication" on page 161

### Configuring Enterprise Vault access for OWA 5.5 users

This section describes the steps required if your Exchange servers are running OWA 5.5. The steps can be summarized as follows:

- On your OWA 5.5 servers, install the Enterprise Vault OWA Extensions. On Exchange 5.5, you do not run a configuration program for the OWA Extensions.
- On your OWA 5.5 servers, configure WinHTTP to set up the proxy bypass list.

### Installing OWA Extensions on Exchange Server 5.5

Follow the instructions in this section to install the Enterprise Vault OWA Extensions from the Enterprise Vault CD-ROM.

To install Enterprise Vault OWA Extensions

1 On your Exchange server, load the Enterprise Vault CD-ROM into the CD-ROM drive.

2 Open the Enterprise Vault folder. Check the ReadMeFirst.htm file in this folder for details of any last minute changes.

3 Open the Server folder.

4 Double-click SETUP.EXE to start the installation.
5 Follow the installation instructions and select the correct OWA Extensions component for this Exchange server.
   You do not need to configure OWA 5.5 Extensions.

6 Repeat the above steps to install the OWA 5.5 Extensions on each Exchange Server.

7 On OWA 5.5 servers, you now configure WinHTTP.

Configuring WinHTTP for OWA 5.5

This section describes how to configure the WinHTTP proxy bypass list on OWA 5.5 servers. Repeat this on each OWA 5.5 server.

Use the WinHTTP Proxy Configuration Utility to configure WinHTTP. A version of this utility is available from a link in the Redistributable Software folder on the Enterprise Vault CD-ROM.

To unpack Proxycfg and configure WinHTTP

1 In Windows Explorer, double-click proxycfg.exe. You are prompted for a folder in which to place the unpacked files.

   Caution: One of the files you are about to unpack is also called proxycfg.exe, so specify a location other than the one containing proxycfg.exe.

Once you have unpacked Proxycfg the following files are in the folder you specified:

   ■ proxycfg.exe
   ■ ReadMe.txt

2 You may want to read the ReadMe.txt file that came with Proxycfg for details of the possible commands. In particular, if you are using an HTTP proxy server, you may want to specify a bypass list, specifying servers that can be accessed directly.

3 Start a command prompt window in the folder into which you unpacked Proxycfg

4 Configure WinHTTP so that the OWA server can access the Enterprise Vault Web Access application, as described in the following sections:

   ■ “Direct access, without a proxy HTTP server” on page 136
   ■ “Using a proxy HTTP server” on page 136

This completes the basic configuration of your Enterprise Vault OWA environment.
Direct access, without a proxy HTTP server

If you do not use a proxy HTTP server, enter the following command:

```
proxycfg -d -p "<local>" "<local>;<server_name>"
```

<server_name> must be the same as the computer name part of the URL for the web access application. For example, if your web access application has the following URL:

`http://myserver.example.com/EnterpriseVault`

where **myserver** is an alias for a computer called **server1**, then the `proxycfg` command to use could be:

```
proxycfg -d -p "<local>" "<local>;myserver;myserver.example.com; server1; server1.example.com"
```

To improve reliability, you can specify a semicolon-separated list of names that apply to the web access application server.

If there are several web access application servers, add them all to the list, separated by semicolons.

This command adds the servers to the proxy bypass list, which you must do because Integrated Windows Authentication occurs automatically only with hosts on the proxy bypass list.

If you are implementing an Enterprise Vault building blocks solution, make sure you include all the following in the proxy bypass list:

- The Vault Site alias, in both fully-qualified and LanMan forms. For example:
  - `ourvaultsitealias.example.com`
  - `ourvaultsitealias`

- The computer alias, in both fully-qualified and LanMan forms, of every Enterprise Vault server computer in the Vault Site. For example:
  - `vault1alias.example.com`
  - `vault1alias`

Using a proxy HTTP server

Enterprise Vault requires direct access, and must not go via a proxy.

Use `proxycfg` to see your current settings, and determine the name, if any, of the proxy server and current bypass list:

```
proxycfg
```

If you are using a proxy HTTP server, enter the following command to specify that the proxy server computer is to be used for all HTTP and HTTPS access:

```
proxycfg -d -p "<ExistingProxyServername>" *<local>;CurrentBypassList; <server_name>"
```
where:

- `<ExistingProxyServername> is the name of the proxy server computer. If there is no current proxy server, specify `<local>` for `<ExistingProxyServername>`.
- `CurrentBypassList` is the contents of the existing bypass list, if any, starting with `<local>` or the `<ExistingProxyServername>`.
- `<server_name>`, on back-end servers, is the computer name part of the URL for the web access application. If there are several servers, or the server has several names, this can be a semicolon-separated list of server names.

Depending on the network configuration you have, you may need to specify a bypass list; see the `ReadMe.txt` file that came with Proxycfg for more information.

If you are implementing an Enterprise Vault building blocks solution, make sure you include all the following in the proxy bypass list:

- The Vault Site alias, in both fully-qualified and LanMan forms. For example:
  - `ourvaultsitealias.example.com`
  - `ourvaultsitealias`
- The computer alias, in both fully-qualified and LanMan forms, of every Enterprise Vault server computer in the Vault Site. For example:
  - `vault1alias.example.com`
  - `vault1alias`

---

**Upgrading OWA Extensions to Enterprise Vault 6.0**

This section describes how you upgrade older versions of the Enterprise Vault OWA Extensions to Enterprise Vault 6.0.

It is important that you check the release notes in the `ReadMeFirst.htm` file on the Enterprise Vault CD-ROM for version-specific information on the Enterprise Vault OWA Extensions. For Enterprise Vault service packs, this file includes details of fixes to the OWA Extensions that are included in the service pack and any additional upgrade instructions.

**Upgrading OWA 2003 Extensions**

The Enterprise Vault 6.0 OWA Extensions provide the following new features for OWA 2003 users:
In a default installation of the Enterprise Vault 6.0 OWA 2003 Extensions, users can archive, restore and delete archived items and use Archive Explorer and Search in their Premium and Basic OWA clients.

The functionality available to OWA 2003 users can be customized by administrators in the Enterprise Vault Administration Console using the OWA 2003 settings on the Advanced tab of the Exchange Server mailbox policy.

Upgrade the Enterprise Vault OWA Extensions on each OWA 2003 server in your Enterprise Vault environment.

When you have upgraded the OWA Extensions, the new Enterprise Vault 6.0 OWA features are available automatically in OWA 2003 clients. If required, you can customize the functionality available to users and the behavior of the OWA Extensions using the OWA 2003 settings that are listed on the Advanced page of the Enterprise Vault mailbox policy.

For a description of these settings, see the Administrator's Guide.

---

**Note:** In previous releases, to display the Search Archives and Archive Explorer buttons in OWA 2003 clients you edited the OWA file, `vw-navbar.js`. From Enterprise Vault 6.0, Enterprise Vault buttons are configured using settings in the Administration Console. Do not edit the `vw-navbar.js` file.

---

**To upgrade Enterprise Vault OWA 2003 Extensions**

1. If your Exchange Servers are clustered, there is additional information that you need to read before proceeding.
   
   See “Supported cluster configurations” on page 146
   
   See “OWA: Configuring Enterprise Vault Extensions in active/passive Microsoft clusters” on page 148
   
   See “OWA: Configuring Enterprise Vault Extensions in an active/active Microsoft cluster” on page 151
   
   See “Configuring Enterprise Vault OWA and RPC Extensions on VCS” on page 155

2. On Enterprise Vault servers, you need to upgrade the configuration of the Anonymous user account, which handles connections from back-end Exchange Servers. You can use your existing Anonymous user account or create a new one.
   

3. On back-end Exchange Server 2003 computers, remove the existing Enterprise Vault OWA Extensions and restore the original OWA control files.
See “OWA 2003: Removing OWA virtual directories, forms registration and Proxy Bypass List” on page 178.

“OWA 2003: Restoring OWA control files” on page 180.
You do not need to completely remove the extensions using the Add/Remove Programs in the Control Panel.


5 On back-end Exchange Server 2003 computers, run the Enterprise Vault configuration program for the extensions.
This recreates the Enterprise Vault virtual directories.
“Configuring a back-end Exchange Server 2003” on page 123.

6 Use an OWA client browser session on each back-end Exchange Server to check the Enterprise Vault OWA configuration.

7 On front-end Exchange Server 2003 computers, remove the existing Enterprise Vault OWA Extensions and restore the original OWA control files.
See “OWA 2003: Removing OWA virtual directories, forms registration and Proxy Bypass List” on page 178.
“OWA 2003: Restoring OWA control files” on page 180.
You do not need to completely remove the extensions using the Add/Remove Programs in the Control Panel.


9 On front-end Exchange Server 2003 computers, run the Enterprise Vault configuration program for the extensions.
This recreates the Enterprise VaultProxy virtual directory.
“Configuring a front-end Exchange Server 2003” on page 126.

10 Use an OWA client browser session on each front-end Exchange Server to check the complete Enterprise Vault OWA configuration.

Upgrading OWA 2000 Extensions

Upgrade the Enterprise Vault OWA Extensions on each OWA 2000 server in your Enterprise Vault environment.
Note that the new OWA client functionality available in Enterprise Vault 6.0 OWA Extensions is only available when using OWA 2003 clients with Exchange Server 2003.

**To upgrade Enterprise Vault OWA 2000 Extensions**

1. If your Exchange Servers are clustered, there is additional information that you need to read before proceeding.
   
   See “Supported cluster configurations” on page 146
   
   See “OWA: Configuring Enterprise Vault Extensions in active/passive Microsoft clusters” on page 148
   
   See “OWA: Configuring Enterprise Vault Extensions in an active/active Microsoft cluster” on page 151
   
   See “Configuring Enterprise Vault OWA and RPC Extensions on VCS” on page 155

2. On Enterprise Vault servers, you need to upgrade the configuration of the Anonymous user account, which handles connections from back-end Exchange Servers. You can use your existing Anonymous user account or create a new one.
   

   
   See “OWA 2000: Removing OWA virtual directories, forms registration and Proxy Bypass List” on page 180.
   
   You do not need to completely remove the extensions using the **Add/Remove Programs** in the Control Panel.

   
   See "Installing OWA Extensions on a back-end Exchange Server 2000" on page 130.

   
   This recreates the Enterprise Vault virtual directories.
   
   “Configuring a back-end Exchange Server 2000” on page 131.

6. Use an OWA client browser session on each back-end Exchange Server to check the Enterprise Vault OWA configuration.

   
   “Installing OWA Extensions on a front-end Exchange Server 2000” on page 133.
8 Use an OWA client browser session on each front-end Exchange Server to check the complete Enterprise Vault OWA configuration.

Upgrading OWA 5.5 Extensions

Upgrade the Enterprise Vault OWA Extensions on each OWA 5.5 server in your Enterprise Vault environment.

Note that the new OWA client functionality available in Enterprise Vault 6.0 OWA Extensions is only available when using OWA 2003 clients with Exchange Server 2003.

To upgrade Enterprise Vault OWA 5.5 Extensions
1 On your Exchange server, load the Enterprise Vault CD-ROM into the CD-ROM drive.
2 Open the Enterprise Vault folder. Check the ReadMeFirst.htm file in this folder for details of any last minute changes.
3 Open the Server folder.
4 Double-click SETUP.EXE to start the installation.
5 Follow the installation instructions and select the correct OWA Extensions component for this Exchange server.
   You do not need to configure OWA 5.5 Extensions.
6 Repeat the above steps to install the OWA 5.5 Extensions on each Exchange Server 5.5.

Retaining customized shortcut behavior in OWA 5.5

In Enterprise Vault 5.0 it was possible for you to customize the file DesktopSettings.txt so that an OWA 5.5 user viewed the content of a shortcut when opening it, and then had to click a link to open the archived item. If you have customized your system in this manner, the upgrade to Enterprise Vault 6.0 OWA Extensions will change the behavior back to the default, in which opening the shortcut automatically opens the archived item.

To retain your customized behavior then, after the upgrade, do the following
1 Double-click the appropriate Exchange server mailbox policy to display its properties.
2 Click the Advanced tab.
3 Next to List settings from, select OWA 2003.
4 In the list, click OWA 5.5 Open Shortcut and then click Modify.
5 Select **Shortcut** and click **OK**.
Synchronize the mailboxes, using the **Synchronize** tab in the properties of the Exchange server mailbox task.

### Configuring a demonstration system

If you are setting up an Enterprise Vault environment to demonstrate or pilot Enterprise Vault OWA Extensions, the Enterprise Vault server and Exchange server are typically installed on one computer, as shown in the figure, “**Typical demonstration configuration**”. In this example, you would install and configure the Enterprise Vault OWA Extensions for a back-end Exchange server.

**Table 11-3**  
Typical demonstration configuration

To demonstrate the use of OWA with Enterprise Vault you can set up all the required servers on one computer. The OWA configuration can include a back-end Exchange Server only.

**To set up an OWA 2003 demonstration systems**

1. Configure the back-end server.
   - See “**Installing OWA Extensions on a back-end Exchange Server 2003**” on page 122.
   - See “**Configuring a back-end Exchange Server 2003**” on page 123.
2. From a browser, first try connecting to the back-end Exchange server and check that you can view archived items.

In this configuration, the Anonymous account is not required on the Enterprise Vault server.

### Troubleshooting

This section offers advice on troubleshooting Enterprise Vault OWA Extensions.
Save file error when installing OWA Extensions

Exchange Server 2003 hotfixes may modify OWA control files. If you have installed an Exchange Server 2003 hotfix that has created an unsupported version of the OWA control files folder, or modified any files in the control files folder, a “Save file error” will be reported when you attempt to install the Enterprise Vault OWA Extensions.

See “Prerequisite software” on page 116.

Errors when running the configuration program

The following error may be generated when configuring the OWA Extensions.

Registration failed

The following error may be generated when configuring the front-end or back-end OWA 2003 Extensions:

registration failed, error: -2147217895
Object or data matching the name, range, or selection criteria was not found within the scope of this operation.

You need to create at least one public folder before you run the configuration program. As Microsoft Exchange installation automatically creates a public folder store, Enterprise Vault will attempt to register forms against public folders. If no public folders exist, the error will be displayed.

ADO connection error

The following error may be generated when configuring the front-end or back-end OWA 2003 Extensions:

ADO connection error: -2147217895 Object or data matching the name, range, or selection criteria was not found within the scope of this operation.

This error occurs when the Simple Mail Transfer Protocol (SMTP) domain name of the Microsoft Exchange 2003 Mailbox Store System mailbox is different than that of the Microsoft Exchange 2003 server domain name.

For instructions on how to fix this, see the Enterprise Vault TechNote:
http://support.veritas.com/docs/280615

WinHTTP configuration problems

When you view the contents of an Enterprise Vault item, you may receive the following error message:

Failed to get the document from the Storage Service (E_ACCESS_DENIED)
Troubleshooting

This will occur if WinHTTP has not been configured correctly using Proxycfg. See the following articles for more information:

- **You may need to run the Proxycfg tool for ServerXMLHTTP to work** ([http://support.microsoft.com/?kbid=289481](http://support.microsoft.com/?kbid=289481))
- **Frequently asked questions about ServerXMLHTTP** ([http://support.microsoft.com/?kbid=290761](http://support.microsoft.com/?kbid=290761))

Enterprise Vault buttons not displayed in OWA 2003 client

If the Enterprise Vault buttons do not appear in OWA 2003 clients on a default installation, check the following:

- Clear client browser cache.
- Enterprise Vault forms are registered on the back-end OWA server. You can use Exchange Explorer in the Exchange Server SDK Development Tools to check form registrations.
  - If the forms are not registered, rerun the Enterprise Vault OWA Extensions configuration program.
- **EVOWA** Virtual Directory set to use the Exchange Application Pool.
- Any Exchange Server 2003 hotfixes applied are supported by Enterprise Vault. See "Prerequisite software" on page 116.
  - Enterprise Vault OWA configuration edits the OWA control files on the Exchange Server. If you have installed an Exchange Server 2003 hotfix, this may have modified OWA control files or changed the version of the control file folder.

**OWA 5.5 shortcut behavior changed after upgrade**

In Enterprise Vault 5.0 it was possible for you to customize the file DesktopSettings.txt so that an OWA 5.5 user viewed the content of a shortcut when opening it, and then had to click a link to open the archived item. If you have customized your system in this manner, the upgrade to Enterprise Vault 6.0 OWA Extensions will change the behavior back to the default, in which opening the shortcut automatically opens the archived item.

See "Retaining customized shortcut behavior in OWA 5.5" on page 141.
Enterprise Vault OWA Extensions for OWA 2000, and OWA and RPC Extensions for OWA 2003, are supported in configurations where the back-end Exchange Servers are configured in clusters that are managed by Microsoft Cluster Server or VERITAS Cluster Server (VCS). Front-end Exchange Servers typically use load balancing, not clustering.

This section provides additional information on installing the Enterprise Vault OWA and RPC Extensions on clustered Exchange Servers. We recommend that you read the information given here before installing and configuring the extensions on the individual Exchange Servers.

This chapter includes the following topics:

■ Supported cluster configurations
■ OWA: Configuring Enterprise Vault Extensions in active/passive Microsoft clusters
■ OWA: Configuring Enterprise Vault Extensions in an active/active Microsoft cluster
■ “RPC over HTTP: Configuring Enterprise Vault Extensions in active/passive Microsoft clusters”
■ “RPC over HTTP: Configuring Enterprise Vault Extensions in an active/active Microsoft cluster”
■ Configuring Enterprise Vault OWA and RPC Extensions on VCS
Supported cluster configurations

Exchange Servers in active/passive and N+1 configurations are supported. Active/active configurations are also possible, but not recommended by Microsoft.

**Figure 12-1**  Active/passive configuration

*Figure 12-1* illustrates an example basic active/passive Exchange Server cluster configuration. There is one Exchange Virtual Server, called EVS1, which can run on either node. As it is currently running on NODEA, this is the active node. If a problem occurs on this node, EVS1 will failover to NODEB, which then becomes the active node. Mailbox and public folder information stores and registered forms are held on the shared disks. The configuration information for the Exchange Virtual Server is held in Active Directory. In a basic active/passive configuration, there is one standby node for each active node.

N+1 clusters are similar to active/passive configurations in that there is a standby (passive) node to which applications on an active node can failover. However, in an N+1 configuration, the passive node is standby for multiple active nodes. *Figure 2* and *Figure 3* illustrate two different examples of N+1 Exchange Server cluster configurations.
Configuring OWA and RPC Extensions in clustered configurations

Supported cluster configurations

Figure 12-2  N+1 configuration

In Figure 12-2, NODEC is the standby node for NODEA and NODEB. The Exchange Virtual Server, EVS1, can run on either NODEA or NODEC. The Exchange Virtual Server, EVS2, can run on either NODEB or NODEC.

Figure 12-3  Alternative N+1 configuration

Figure 12-3 illustrates an alternative N+1 configuration, in which any of the nodes can act as standby for either of the Exchange Virtual Servers. Each of the Exchange Virtual Servers, EVS1 and EVS2, can run on NODEA, NODEB or NODEC.

Figure 12-4 illustrates an active/active configuration. Note that Microsoft does not recommend active/active configurations.

In these configurations there are no passive standby nodes; if the Exchange Virtual Server, EVS1, fails over, then both Exchange Virtual Servers will be running on NODEB, which could cause performance issues.
When configuring Enterprise Vault OWA and RPC Extensions for clustered environments, the extensions must be installed and configured on each node on which the Exchange Virtual Server can run.

Additional information on installing the extensions in active/passive and active/active clustered environments is given in the following sections.

**Figure 12-4**  
Active/active configuration

---

**OWA: Configuring Enterprise Vault Extensions in active/passive Microsoft clusters**

Enterprise Vault OWA Extensions are supported on clustered back-end, OWA 2000 or OWA 2003 Exchange Virtual Servers.

In active/passive Exchange Virtual Server cluster configurations, you must install the Enterprise Vault OWA 2000 or OWA 2003 Extensions on both active and passive nodes; you can install them on either an active or passive node first. Detailed instructions on how to install and configure the OWA Extensions are given in the following sections:

- “Configuring Enterprise Vault access for OWA 2003 users” on page 118.
- “Configuring Enterprise Vault access for OWA 2000 users” on page 127

**Figure 12-5** shows the location of the various virtual directories and configuration data used by the Enterprise Vault OWA 2003 and OWA 2000 Extensions.
Figure 12-5  Detail of OWA 2003 and OWA 2000 Extensions configuration

Configuring the OWA Extensions on the active node first

If you install and configure the OWA Extensions on the active node first, running the Enterprise Vault OWA configuration program will do the following:

- Register forms for the OWA Extensions against the Exchange Virtual Server mailbox and public information stores.
- Create in Active Directory the following Exchange Server virtual directories for the back-end Exchange Virtual Server:
  - EnterpriseVaultExchange
  - EnterpriseVaultPublic
- Create the following IIS virtual directories on the active node computer:
  - EnterpriseVaultProxy (on OWA 2003 only)
  - EVOWA
Populate the Proxy bypass list on the active node computer from the file, Enterprise Vault\OWA\EV Servers.txt.

If you examine the log file, Enterprise Vault\OWA\BackEnd200nSetup.wsf.log, after the configuration program has run, you will see the lines detailing the mailbox and public folder forms registration.

Configuring the OWA Extensions on the passive node first

If you install and configure the OWA Extensions on the passive node first, running the Enterprise Vault OWA configuration program will do the following:

- Create in Active Directory the following Exchange Server virtual directories for the back-end Exchange Virtual Server:
  - EnterpriseVaultExchange
  - EnterpriseVaultPublic

- Create the following IIS virtual directories on the passive node computer:
  - EnterpriseVaultProxy (on OWA 2003 only)
  - EVOWA

- Populate the Proxy bypass list on the passive node computer from the file, Enterprise Vault\OWA\EV Servers.txt.

Note that forms registration is only performed when you run the Enterprise Vault OWA configuration program on the active node. If you examine the log file, Enterprise Vault\OWA\BackEnd200nSetup.wsf.log, after the configuration program has run on the passive node, you will not see any forms registration lines.

Configuring the OWA Extensions on the associated active or passive node

When you install and configure the OWA Extensions on the active or passive node associated with the node that you have already configured, warning messages in the log file will indicate that the EnterpriseVaultPublic and EnterpriseVaultExchange virtual directories already exist. As these virtual directories were created when you configured the OWA Extensions on the first node, you can ignore these warning messages.

ExchangeServers.txt on the Enterprise Vault server

When you configure an Enterprise Vault server to support OWA access, you create the ExchangeServers.txt file, before you run the owau ser.wsf script to configure the Anonymous user account.
ExchangeServers.txt holds the IP addresses of all the back-end Exchange Servers that will contact the Enterprise Vault server. When configuring this file for clustered Exchange Virtual Server configurations, the file must include all the IP addresses of the Exchange Virtual Servers that will access the Enterprise Vault server, and all the IP addresses of the physical computers (nodes) on which the Exchange Virtual Servers can run.

**OWA: Configuring Enterprise Vault Extensions in an active/active Microsoft cluster**

Although Enterprise Vault OWA 2000 or OWA 2003 Extensions are supported in active/active clustered Exchange Virtual Server configurations, such configurations are not recommended by Microsoft and should be avoided, wherever possible.

In an active/active configuration, it does not matter which node you install the Enterprise Vault OWA Extensions on first.

Running the Enterprise Vault OWA configuration program on the first active node will perform the following tasks:

- Register the Enterprise Vault OWA forms against the mailbox and public stores in the Exchange Virtual Server.
- Create in Active Directory the following Exchange Server virtual directories for the back-end Exchange Virtual Server:
  - EnterpriseVaultExchange
  - EnterpriseVaultPublic
- Create the following IIS virtual directories on the active node computer:
  - EnterpriseVaultProxy (on OWA 2003 only)
  - EVOWA
- Populate the Proxy bypass list on the active node computer from the file, Enterprise Vault\OWA\EVServers.txt.

If you examine the log file, Enterprise Vault\OWA\BackEnd200nSetup.wsf.log, after the configuration program has run, you will see the lines detailing the mailbox and public folder forms registration.

When you then run the Enterprise Vault OWA configuration program on the other active node, it performs the following tasks for the Virtual Exchange Server associated with that node:

- Registers the Enterprise Vault OWA forms against the mailbox and public stores in the Exchange Virtual Server.
Create in Active Directory the following Exchange Server virtual directories for the back-end Exchange Virtual Server:
- EnterpriseVaultExchange
- EnterpriseVaultPublic

Create the following IIS virtual directories on the active node computer:
- EnterpriseVaultProxy (on OWA 2003 only)
- EVOWA

Populate the Proxy bypass list on the active node computer from the file, Enterprise Vault\OWA\EVServers.txt.

When you install and configure the OWA Extensions on the second active node in the cluster, warning messages in the log file will indicate that the EnterpriseVaultPublic and EnterpriseVaultExchange virtual directories already exist. As these virtual directories were created when you configured the OWA Extensions on the first node, you can ignore these warning messages.

RPC over HTTP: Configuring Enterprise Vault Extensions in active/passive Microsoft clusters

Enterprise Vault RPC Extensions are supported on clustered RPC target Exchange Virtual Servers (Exchange Server 2003).

In active/passive Exchange Virtual Server cluster configurations, you must install the Exchange 2003 Back-end Extensions (OWA & RPC) on both active and passive nodes; you can install them on either an active or passive node first. Detailed instructions on how to install and configure the extensions are given in the chapter on configuring RPC over HTTP access to Enterprise Vault. See "Configuring RPC over HTTP access to Enterprise Vault" on page 183.

Figure 12-6 shows the location of the various virtual directories and configuration data used by the extensions.
Configuring OWA and RPC Extensions in clustered configurations

RPC over HTTP: Configuring Enterprise Vault Extensions in active/passive Microsoft clusters

Figure 12-6  
RPC extensions configuration

If you install and configure the extensions on the active node first, running the Enterprise Vault RPC configuration program will do the following:

- Create the following IIS virtual directories on the active node computer:
  - EnterpriseVaultProxy
  - EVOWA
- Populate the Proxy bypass list on the active node computer from the file, Enterprise Vault\OWA\EVServers.txt.
Configuring RPC on the passive node first

If you install and configure the RPC Extensions on the passive node first, running the Enterprise Vault RPC configuration program will do the following:

- Create the following IIS virtual directories on the passive node computer:
  - EnterpriseVaultProxy
  - EVOWA
- Populate the Proxy bypass list on the passive node computer from the file, Enterprise Vault\OWA\EV Servers.txt.

Examine the log file, \OWA\FrontEnd2003Setup.wsf.log, for any errors.

ExchangeServers.txt on the Enterprise Vault server

When you configure an Enterprise Vault server to support RPC over HTTP access, you create the ExchangeServers.txt file, before you run the owau user.wsf script to configure the Anonymous user account.

ExchangeServers.txt holds the IP addresses of all the RPC target Exchange Servers that will contact the Enterprise Vault server. When configuring this file for clustered Exchange Virtual Server configurations, the file must include all the IP addresses of the Exchange Virtual Servers that will access the Enterprise Vault server, and all the IP addresses of the physical computers (nodes) on which the Exchange Virtual Servers can run.

RPC over HTTP: Configuring Enterprise Vault Extensions in an active/active Microsoft cluster

Although Enterprise Vault RPC Extensions are supported in active/active clustered Exchange Virtual Server configurations, such configurations are not recommended by Microsoft and should be avoided, wherever possible.

In an active/active configuration, it does not matter which node you install the Enterprise Vault Extensions on first.

Running the Enterprise Vault RPC configuration program on the first active node will perform the following tasks:

- Create the following IIS virtual directories on the active node computer:
  - EnterpriseVaultProxy
Configuring Enterprise Vault OWA and RPC Extensions on VCS

From Enterprise Vault 6.0 SP2, Symantec supports the installation of Enterprise Vault on VCS. It is also possible to install the Enterprise Vault OWA and RPC Extensions on a back-end Exchange Server that has been installed on VCS.

To install and configure the Enterprise Vault OWA and RPC Extensions

1. Install the appropriate Enterprise Vault OWA and RPC Extensions on all nodes that could host the Exchange Virtual Server.

2. Run the appropriate Enterprise Vault configuration program for the extensions on each Exchange Virtual Server node, while it is the active node. This means that you must run the configuration program on the active node, fail over the Exchange Virtual Server to the passive node, and then run the configuration program on that node. Repeat this process for all nodes that could host the Exchange Virtual Server.

3. On the Enterprise Vault server, the ExchangeServers.txt file must include all the IP addresses of the Exchange Virtual Servers that will access the Enterprise Vault server, and all the IP addresses of the physical computers (nodes) on which the Exchange Virtual Servers can run.
156 Configuring OWA and RPC Extensions in clustered configurations

Configuring Enterprise Vault OWA and RPC Extensions on VCS
This chapter describes the following tasks:

- How to configure Microsoft Internet Security and Acceleration (ISA) Server to enable OWA users to access Enterprise Vault archives.
- How to configure Microsoft Internet Security and Acceleration (ISA) Server to enable RPC over HTTP users to access Enterprise Vault archives.

**Enabling Enterprise Vault access using OWA**

*Figure 13-1  Overview*
Microsoft ISA Server can be used to secure access to OWA servers by using Web publishing rules (reverse proxy), to make front-end servers available on the Internet.

Instructions are given on how to configure ISA Server 2004 for the following configurations:

- Configuring ISA Server 2004 for OWA Basic Authentication
- Configuring ISA Server 2004 for OWA forms-based authentication

Configuring ISA Server 2004 for OWA Basic Authentication

Configuring ISA Server 2004 for basic authentication is relatively straightforward. The Mail Server Publishing Rule will reference the standard paths, which are the three virtual directories; Exchange, Public and Exchweb. For Enterprise Vault support, the extra path of EnterpriseVaultProxy needs to be added.

It is assumed that you have installed a suitable Certification Authority (CA) certificate on the front-end OWA server, and imported that certificate onto the ISA Server 2004.

To enable access to archived items for OWA users who use basic authentication

1. Logon to the ISA Server 2004 computer as a local administrator with permissions to configure the ISA Server.
2. Open the Microsoft Internet Security and Acceleration Server 2004 management console and expand the server name.
   a. Click the Firewall Policy node.
   b. In the right-hand task pane, click the Tasks tab and then click Publish a Mail Server.
3. On the Welcome to the New Mail Server Publishing Rule Wizard page, enter a name for the rule in the Mail Server Publishing Rule name box. For example, OWA Basic (External to Internal). Click Next.
5. On the Select Services page, select Outlook Web Access and click Next.
6 On the Bridging Mode page, select **Secure connection to clients and mail server**, and click **Next**.

7 On the Specify the Web Mail Server page, enter the name of the front-end OWA server (as identified to the internal network) in the **Web mail server** box. Alternatively, you can enter the common name of the CA certificate on the front-end OWA server. This is the **Issued to** name in the certificate. Click **Next**.

8 On the Public Name Details page, enter the name that external users will use to access the OWA site in the **Public name** box. This must match what is specified in the external DNS entry. Alternatively, select **Accept requests for any domain name** in the drop-down box. Click **Next**.

9 On the Select Web Listener page, click **New** to create a new Web listener. (This step assumes that no web listener exists yet).

10 On the Welcome to the New Web Listener Wizard page, enter a name for the listener in the **Web listener name** box. For example, **External443 (Basic)**. Click **Next**.

11 On the IP Addresses page, select the **External** checkbox. Click **Next**.

12 On the Port Specification page, clear the **Enable HTTP** checkbox.
   
   a Select **Enable SSL**.
   
   b Click **Select**. In the Select Certificate dialog box, click the Web site certificate (front-end OWA server), and click **OK**.
13. Click **Next** on the Port Specification page.

14. Click **Finish** on the Completing the New Web Listener Wizard page.

15. Click **Edit** on the Select Web Listener page.
   
   a. Select the **Preferences** tab. In the Web Listener dialog box, click **Authentication**.
   
   b. In the Authentication dialog box, clear the **Integrated** checkbox.
   
   c. Click **OK** in the prompt dialog.
   
   d. Select the **Basic** checkbox.
   
   e. Click **Yes** in the dialog box informing you that you should use SSL.
   
   f. Click **OK** in the Authentication dialog box.

16. Click **Apply** and then click **OK** in the Web Listener dialog box.

17. Click **Next** on the Select Web Listener page.

18. On the User Sets page, accept the default setting, **All Users**, and click **Next**.

19. Click **Finish** on the Completing the New Mail Server Publishing Rule Wizard page.

20. Right-click the newly created rule in the main Firewall Policy pane of the Microsoft Internet Security and Acceleration Server 2004 management console, and click **Properties**.

21. In the Properties dialog box, click the **Paths** tab.
   
   a. On the **Paths** tab, click the **Add** button.
   
   b. In the Path mapping dialog box, enter the value `/EnterpriseVaultProxy/*` in the box **Specify the folder on the Web site that you want to publish**. (If you want to publish the entire Web site, leave this box blank).
   
   c. Select **Same as published folder**.
   
   d. Click **OK**.

22. Click **Apply** and then click **OK** in the Properties dialog box.

23. Click on **Apply** to save the changes and update the firewall policy.

   This completes the set up steps to support users accessing OWA using basic authentication.
Enabling Enterprise Vault access using OWA

The configuration steps for forms-based authentication are more complex. This is because a web listener that is configured in ISA Server 2004 for forms-based authentication cannot support any other type of authentication. This is acceptable for standard OWA functionality, such as opening archived items. However, the EnterpriseVaultProxy virtual directory supports only basic authentication, so any functionality that requires this virtual directory (Archive Explorer and the Search application) will fail when published using an ISA Server 2004 that has been configured for forms-based authentication.

The solution is to chain web listeners together, so that requests for the Exchange, Public and Exchweb virtual directories can be authenticated using forms-based authentication, and calls to the EnterpriseVaultProxy virtual directory can be authenticated using basic authentication.

Figure 13-2  Mapped paths
How chained web listeners work

- The external host sends a request to http://webmail.ev.com/Exchange. The name webmail.ev.com resolves to the IP address on the external interface of the ISA Server 2004 firewall that the external Web listener is configured to use. This listener accepts the incoming request and does not prompt users for credentials, as it is configured for basic authentication.
- The ISA Server 2004 firewall allows you to configure the listener to forward the user credentials to the Web site. This prevents unauthenticated users from connecting to the Web site. SSL encryption on the connection encrypts the user credentials when they are sent by the client to the server.
- A Web Publishing Rule is created for the external listener that forwards incoming requests for the Exchange virtual directory to localhost.
- A second Web listener, created on the localhost network, is configured to use forms-based authentication. As the listener is configured to use forms-based authentication, it generates a form and sends this to the user.
- The user fills in the username and password information in the form and sends it to the ISA Server 2004 firewall.
- The firewall accepts the credentials on the external listener, and the Web Publishing Rule for the external listener forwards the credentials to the localhost listener.
- As the localhost listener uses forms-based authentication, it forwards the user credentials to the OWA Web site. When the user is authenticated, the connection request is forwarded to the OWA Web site on the internal network.
- User requests for Archive Explorer or the archive Search applications are directed to https://webmail.ev.com/EnterpriseVaultProxy, which
Enabling Enterprise Vault access using OWA requires basic authentication. These requests are serviced by the external listener, which is configured for basic authentication.

- As there is a change in authentication at this point (from forms-based to basic), the user is prompted for username and password information.
- The connection for **EnterpriseVaultProxy** is forwarded to the OWA server, based on a Web Publishing Rule that is configured to forward the connection to the **EnterpriseVaultProxy** virtual directory on the front-end OWA server on the internal network.

**Steps to configure chained web listeners**

- Exporting the Web site certificate from the OWA Web site and importing that certificate into the ISA Server 2004 firewall computer certificate store. This certificate will be used by the external listener. See “Exporting the Web site certificate form the OWA Web site” on page 163.
- Requesting a Web site certificate that has the name localhost and installing this certificate in the certificate store on the ISA Server 2004 firewall computer. This certificate is used by the localhost Web listener. See “Requesting a Web site certificate for the localhost listener” on page 164.
- Create the Web Publishing Rule that uses the external Web listener to accept the incoming requests for the OWA site and forwards these to the localhost Web listener. See “Create a Web Publishing Rule that forwards incoming OWA requests to the localhost Web listener” on page 166.
- Create the Web Publishing Rule that uses the localhost Web listener to accept the incoming requests from the external Web listener, and forwards these to the OWA Web site on the internal network. See “Create a Web Publishing Rule for the localhost listener that forwards requests to the OWA Web site” on page 169.
- Create the Web Publishing Rule that the external Web listener uses to forward requests for the /EnterpriseVaultProxy virtual directory directly to the internal network. See “Create a Web Publishing Rule that forwards requests for the EnterpriseVaultProxy virtual directory to the internal network” on page 173.

**Exporting the Web site certificate form the OWA Web site**

To secure communications from end to end, you need to install a Web site certificate on the OWA Web site on the internal network. There are several ways you can get the certificate:

- The Web enrollment site
- The Certificates MMC
An offline request.

After the Web site has a certificate, you can then export the certificate, along with its private key, to a file. You can then import that certificate into the ISA Server 2004 firewall computer’s Personal certificate store. In addition, the CA certificate of the CA that issued the certificate must be installed in the Trusted Root Certification Authorities certificate store on the ISA Server 2004 firewall computer.

Details of how to request a Web site certificate for the OWA Web site, how to export it to a file, and how to import that file into the firewall computer’s certificate store are beyond the scope of this technote. Instructions can be found at the following web site:


Requesting a Web site certificate for the localhost listener

This section describes how to:

- Obtain a certificate for the localhost Web listener. The easiest way to do this is to use the Web enrollment site for the Enterprise CA. In the example network used in this technote, the domain controller on the internal network is an Enterprise CA and the Web enrollment site is enabled.

- Install the certificate in the certificate store on the ISA Server 2004 firewall computer. You should not need to install the CA certificate in the Trusted Root Certification Authorities store, as this should have been done when the Web site certificate was installed on the firewall computer.

To obtain the Web site for the localhost listener

1. Logon to the ISA Server 2004 computer as a local administrator with permissions to configure the ISA Server.

2. Using the Microsoft Internet Security and Acceleration Server 2004 management console create an Access Rule that allows the firewall to connect to the CA Web enrollment site.

   Expand the server name and then click the Firewalls node. In the right-hand pane, click the Tasks tab and then click Create New Access Rule.

3. On the Welcome to the New Access Rule Wizard page, enter a name for the rule in the Access Rule name box. In this example, we will call the rule Firewall to CA. Click Next.

4. On the Rule Action page, select Allow and click Next.

5. On the Protocols page, select the Selected protocols option from This rule applies to list and click Add.
6 In the Add Protocols dialog box, click the **Common Protocols** folder and double click the **HTTP** protocol and then click **Close**.

7 Click **Next** on the Protocols page.

8 On the Access Rule Sources page, click **Add**.
   In the Add Network Entities dialog box, click the **Networks** folder and then double-click the **Local Host** network. Click **Close**.

9 Click **Next** on the Access Rule Sources page.

10 On the Access Rule Destinations page, click **Add**. If the domain controller is not in the **Computers** folder, click the **New** menu and then click **Computer**.

11 In the New Computer Rule Element dialog box, enter the name of your CA server computer in the **Name** box. In this example we will call it **CA**. Enter the IP address in the **Computer IP Address** box. In this example, the IP address is **10.0.0.2**, so we enter that into the box. Click **OK**.

12 In the Add Network Entities dialog box, click the **Computer** folder and double-click the **CA** entry. Click **Close**.

13 Click **Next** on the Access Rule Destinations page.

14 On the User Sets page, accept the default entry, **All Users**, and click **Next**.

15 Click **Finish** on the Completing the New Access Rule Wizard page.

16 Click **Apply** to save the changes and update the firewall policy.

17 Click **OK** in the Apply New Configuration dialog box.

---

**To request the certificate from the Enterprise CA on the internal network**

1 On the ISA Server 2004 computer, open Internet Explorer and enter the address of the CA into the **Address** bar. For example, **http://10.0.0.2/certsrv** and press Enter.

2 Enter a valid user name and password into the authentication dialog box and click **OK**.

3 On the Welcome page, click **Request a certificate**.

4 On the Request a Certificate page, click **Advanced certificate request**.

5 On the Advanced Certificate Request page, click **Create and submit a request to this CA**.

6 For an Enterprise CA, on the Advanced Certificate Request page, select the **Web Server** certificate from the Certificate Template list. In the **Name** box in the **Identifying Information for Offline Template** section, enter the common name that will be included in the certificate. In this example, we want the name to be localhost, so we enter **localhost** into the **Name** box.
Select **Store certificate** in the **local computer certificate store**. Click **Submit**.

For a stand-alone CA, on the Advanced Certificate Request page, enter details for **Identifying Information**. For example, if the name is to be localhost, enter **localhost** in the **Name** box. Change **Type of Certificate Needed** to **Server Authentication Certificate**. Select **Store certificate in the local computer certificate store**. Click **Submit**.

7 A Potential Scripting Violation dialog box informs you that the Web site is requesting a certificate on your behalf. Click **Yes**.

8 The ID of the requested certificate is then displayed on the Certificate Pending page.

The CA then issues the requested certificate.

**To install the certificate**

1 On the ISA Server 2004 computer open Internet Explorer and enter the address of the CA into the **Address** bar. For example, `http://10.0.0.2/certsrv` and press **Enter**.

2 On home page, click **View the status of a pending certificate request**.

3 Click the requested certificate.

4 On the Certificate Issued page, click **Install this certificate**.

5 Click **Yes** to the prompt that informs you that the Web site is adding one or more certificates to the computer.

6 Close the browser after you see the Certificate Installed page.

At this point the certificate will be available for binding to the localhost Web listener, as described in the following sections.

**Create a Web Publishing Rule that forwards incoming OWA requests to the localhost Web listener**

The first Web Publishing Rule to create is for the external Web listener. This rule will accept the incoming requests for the front-end OWA server and forward them to the localhost listener.
Enabling Enterprise Vault access using OWA

To create the Web Publishing Rule and associated Web listener

1. In the Microsoft Internet Security and Acceleration Server 2004 management console, expand the server name and click the Firewall Policy node. In the right-hand pane, click the Tasks tab and then click Publish a Mail Server.

2. On the Welcome to the New Mail Server Publishing Rule Wizard page, enter a name for the rule in the Mail Server Publishing Rule name box. In this example, we will call the rule OWA FBA (External to Localhost). Click Next.


5. On the Bridging Mode page, select Secure connection to clients and mail server and click Next.

6. On the Specify the Web Mail Server page, enter localhost in the Web mail server box. Click Next.

7. On the Public Name Details page, in the Public name box, enter the name that external users will use to connect to the OWA Web site. For example, owa.msfirewall.org. Alternatively, you can select Accept requests for any domain name. Click Next.


9. On the Welcome to the New Web Listener Wizard page, enter a name for the listener in the Web listener name box. In this example, we will call the listener External443 (basic) to indicate that the listener is listening on
the external interface of the ISA Server 2004 firewall, and that it is configured to use basic authentication. Click Next.

10 On the IP Addresses page, select the External checkbox. Click Next.

11 On the Port Specification page, clear the Enable HTTP checkbox and select Enable SSL. Click Select.

In the Select Certificate dialog box, click the Web site certificate for the OWA front-end server and click OK. Click Next on the Port Specification page.

12 Click Finish on the Completing the New Web Listener Wizard page.

13 Click Edit on the Select Web Listener page. On the External443 (basic) dialog box, select Preferences tab and click Authentication.

14 In the Authentication dialog box, clear the Integrated checkbox. Click OK in the prompt dialog.

Select the Basic checkbox. Click Yes in the prompt box that tells you to should use SSL. Click OK in the Authentication dialog.

15 Click Apply and then click OK in the External443 (basic) dialog.

16 Click Next on the Select Web Listener page.

17 On the User Sets page, accept the default setting, All Users, and click Next.

18 Click Finish on the Completing the New mail Server Publishing Rule Wizard page.
19 Right-click the **OWA FBA (External to Localhost)** rule in the Firewall Policy pane of the Microsoft Internet Security and Acceleration Server 2004 management console and click **Properties**.

20 In the OWA FBA (External to Localhost) Properties dialog box, click the **Paths** tab. Click **Add**.

21 In the Path mapping dialog, enter **/cookieauth.dll** in the box entitled **Specify the folder on the Web site that you want to publish**. (To publish the entire Web site, leave this box blank.) Select **Same as published folder**. Click **OK**.

22 Click **Apply** and then click **OK** in the OWA FBA (External to Localhost) Properties dialog.

23 Click **Apply** to save the changes and update the firewall policy.

24 Click **OK** in the Apply New Configuration dialog.

**Create a Web Publishing Rule for the localhost listener that forwards requests to the OWA Web site**

The next Web Publishing Rule to create is for the localhost Web listener. This rule will accept the incoming requests for the front-end OWA server and forward them to the front-end OWA server.
To create the Web Publishing Rule and associated Web listener

1 In the Microsoft Internet Security and Acceleration Server 2004 management console, expand the server name and click the Firewall Policy node. In the right-hand pane, click the Tasks tab and then click Publish a Mail Server.

2 On the Welcome to the New Mail Server Publishing Rule Wizard page, enter a name for the rule in the Mail Server Publishing Rule name box. In this example, we will call this rule OWA FBA (Localhost to Exchange). Click Next.


4 On the Select Services page, select Outlook Web Access and click Next.

5 On the Bridging Mode page, select Secure connection to clients and mail server and click Next.

6 On the Specify the Web Mail Server page, enter the name of the front-end OWA server in the Web mail server box. Alternatively, you can enter the common name of the CA certificate on the front-end OWA server. This is the Issued to name in the certificate. In this example we enter owa.msfirewall.org. Click Next.

7 On the Public Name Details page, in the Public name box, enter the name that external users will use to connect to the OWA Web site. For example, owa.msfirewall.org. Alternatively, you can select Any domain name in the Accept requests for list. Click Next.

8 Now you create the localhost Web listener. On the Select Web Listener page, click New to create a new Web listener.
9 On the Welcome to the New Web Listener Wizard page, enter a name for the listener in the **Web listener name** text box. In this example, we will call this listener **Localhost443 (FBA)** to indicate that the listener is listening on the external interface of the ISA Server 2004 firewall. Click **Next**.

10 On the IP Addresses page, select the **Local Host** checkbox. Click **Next**.

11 On the Port Specification page, clear the **Enable HTTP** checkbox. Select the **Enable SSL** checkbox. Click **Select**.

In the Select Certificate dialog box, click the **localhost** certificate and click **OK**. Click **Next** on the Port Specification page.

12 Click **Finish** on the Completing the New Web Listener Wizard page.

13 Now you configure forms-based authentication for the localhost listener. On the Select Web Listener page, click **Edit**. Select the **Preferences** tab.

Click **Authentication**. In the Authentication dialog, clear the **Integrated** checkbox. Click **OK** in the prompt dialog. Select the **OWA forms-based** checkbox. Click **OK**.

14 Click **Apply** and then click **OK** on the Localhost443 (FBA) dialog.

15 Click **Next** on the Select Web Listener page.

16 On the User Sets page, accept the default setting, **All Users**, and click **Next**.

17 Click **Finish** on the Completing the New mail Server Publishing Rule Wizard page.
18. On the main page, right-click the **OWA FBA (Localhost to Exchange)** rule in the Firewall Policy pane of the console and click **Properties**.

19. In the OWA FBA (Localhost to Exchange) Properties dialog, click the **Paths** tab.

20. Remove all the paths displayed; hold down the `Ctrl` key, click each of the paths in the path list, click **Remove**.

21. Click **Add**. In the Path mapping dialog box, enter the path `/*` in **Specify the folder on the Web site that you want to publish**. (To publish the entire Web site, leave this box blank.) Select **Same as published folder**. Click **OK**.

![OWA FBA (Localhost to Exchange) Properties](image)

22. Click **Apply** and then click **OK** in the OWA FBA (Localhost to Exchange) Properties dialog.

23. Click **Apply** to save the changes and update the firewall policy.

24. Click on **OK** in the Apply New Configuration dialog.

25. Now order the rules in the main Firewall Policy window. Select the **OWA FBA (External to Localhost)** rule in the Firewall Policy window and then click the move up arrow in the management console button bar to move the rule to the top of the list.
Using Microsoft ISA Server with OWA and RPC Extensions

Enabling Enterprise Vault access using OWA

Click the OWA FBA (Localhost to Exchange) rule and click the move up arrow until it is second on the list.

26 Click **Apply** to save the changes and update the firewall policy.

27 Click **OK** in the Apply New Configuration dialog box.

Create a Web Publishing Rule that forwards requests for the EnterpriseVaultProxy virtual directory to the internal network

The final Web Publishing Rule to create enables the external Web listener to forward incoming requests for the EnterpriseVaultProxy virtual directory on the front-end OWA server. This virtual directory uses basic authentication.

To configure the Web Publishing Rule for EnterpriseVaultProxy requests

1 In the Microsoft Internet Security and Acceleration Server 2004 management console, expand the server name and click the Firewall Policy node. In the right-hand pane, click the Tasks tab and then click Publish a Web Server.

2 On the Welcome to the New Web Publishing Rule Wizard page, enter a name for the rule in the Web Publishing Rule name box. In this example, we
will call the rule EnterpriseVaultProxy (EnterpriseVaultProxy to Internal). Click Next.

3 On the Select Rule Type page, select Allow as action to take when rule conditions are met. Click Next.

4 On the Define Website to Publish page, enter the Computer name or IP address of the front-end OWA server (as known on the internal network). Alternatively, you can enter the common name of the CA certificate for the front-end OWA server.
Select Forward the original host header instead of the actual one. Enter /EnterpriseVaultProxy/* in the Path text field and click Next.

5 On the Public Name Details page, enter the site name that external users will use to access the OWA Web site in the Site box. (This must match the value specified in the external DNS entry.) Alternatively, select Any domain name in the Accept requests for box and click Next.

6 Now associate this rule with the external Web listener. On the Select Web Listener page, in the Web listener box, select the External443 (basic) listener. Click Next.

7 On the User Sets page, accept the default value, All Users, and click Next.

8 Click Finish on the Completing the New Mail Server Publishing Rule Wizard page.

9 Click Apply to save the changes and update the firewall policy.

10 Click OK in the Apply New Configuration dialog box.
Enabling Enterprise Vault access using RPC over HTTP

Microsoft ISA Server can be used to secure access to RPC Exchange Servers by using Web publishing rules (reverse proxy), to make RPC proxy servers available on the Internet.

To configure the ISA Server, you need to perform the following tasks:

- Configure an RPC firewall policy that publishes the \rpc virtual directory on your RPC proxy server through ISA Server.
  See “Configuring an RPC firewall policy”.

- Configure an Enterprise Vault firewall policy that publishes the \EnterpriseVaultProxy virtual directory on your RPC proxy server through ISA Server.
  See “Configuring an Enterprise Vault firewall policy”.

Configuring an RPC firewall policy


In the walk-through procedures described in the article, follow the instructions in Procedure 8, Configure RPC over HTTP for Outlook 2003.

When you have completed the instructions given in the article, do the following to check that the correct port is specified in the RPC firewall policy for redirected requests:

- On the Firewall Policy page in the ISA Server Management console, right-click the RPC over HTTP rule that you have created and select Properties.
- Click the Bridging tab.
- Ensure that Redirect requests to SSL port : 443 is selected. Click Apply and the OK.
- Click Apply, to save the changes and update the firewall policy.
- Click OK in the Apply new configuration dialog.

Now configure a firewall policy for Enterprise Vault.
Configuring an Enterprise Vault firewall policy

On the ISA Server, create a web publishing rule that forwards requests from the \EnterpriseVaultProxy virtual directory to the internal network.

To create an EnterpriseVaultProxy Web Publishing Rule

1. In the ISA Server Management console, expand the server name and click the Firewall Policy node.
2. In the task pane, click the Tasks tab and then click Publish a Web Server.
3. On the Welcome to the New Web Publishing Rule Wizard page, enter a name for the rule in the Web Publishing Rule name text box. For example, EnterpriseVaultProxy. Click Next.
4. On the Select Rule Type page, select Allow as the action to take when rule conditions are met. Click Next.
5. On the Define Website to Publish page, enter the computer name or IP address of the RPC proxy Exchange Server.
6. Select Forward the original host header instead of the actual one.
7. Enter /EnterpriseVaultProxy/* in the Path box. Click Next.
8. On the Public Name Details page, enter the name that external users will use to access the RPC website in the Public name box. This must match what is specified in the external DNS entry. Alternatively, select Any domain name in the Accept requests for box and click Next.
9. On the Select Web Listener page, in the Web listener box, select the listener that you created earlier, when you configured the RPC firewall policy. Click Next.
10. On the User Sets page, accept the default value, All Users, and click Next.
12. Click Apply to save the changes and update the firewall policy.
13. In the Apply New Configuration dialog box, click OK.
How to uninstall Enterprise Vault OWA Extensions

This chapter describes how to remove Enterprise Vault OWA 2000 or OWA 2003 Extensions that have been installed and configured on front-end and back-end Exchange Servers.

Removing OWA 5.5 Extensions is more straightforward, and can be achieved using Add/Remove Programs in the Control Panel.

The instructions in this section are also valid if you are removing the OWA Extensions in a clustered environment. In environments where back-end OWA Servers are clustered, you need to perform the steps on each node on which the Exchange Virtual Servers can run.

The following steps summarize the process for OWA 2003:

- Run the Enterprise Vault OWA Extensions scripts, using the /remove switch, on front-end and back-end OWA 2003 Servers to remove virtual directories, forms registration and Proxy Bypass list configuration.

- See “OWA 2003: Removing OWA virtual directories, forms registration and Proxy Bypass List” on page 178.

- On front-end and back-end OWA 2003 Servers, restore the original OWA control files.

- See “OWA 2003: Restoring OWA control files” on page 180.

- On front-end and back-end OWA 2003 Servers, complete the removal of the Enterprise Vault OWA Extensions using Add/Remove Programs in the Control Panel and then manually remove configuration and log files.

The following steps summarize the process for OWA 2000:

- Run the Enterprise Vault OWA Extensions scripts, using the /remove switch, on back-end OWA 2000 Servers to remove virtual directories, forms registration and Proxy Bypass list configuration.
  See “OWA 2000: Removing OWA virtual directories, forms registration and Proxy Bypass List” on page 180.

- On front-end OWA 2000 Servers, the OWA Extensions are installed but not configured, so you run the removal script on back-end OWA 2000 Servers only.

- On front-end and back-end OWA 2000 Servers, complete the removal of the Enterprise Vault OWA Extensions using Add/Remove Programs in the Control Panel and then manually remove configuration and log files.
  See “OWA 2000: Completing the removal of the OWA Extensions” on page 182.

**OWA 2003: Removing OWA virtual directories, forms registration and Proxy Bypass List**

To remove the virtual directories, form registrations and Proxy Bypass List that are created by the Enterprise Vault OWA Extensions configuration program, you need to run the following Enterprise Vault scripts from the command line.

**On front-end OWA 2003 Servers:**

- Open a command prompt window.
- Enter the following command (on a single line):
  ```cmd
  C:\Program Files\Enterprise Vault\OWA>cscript FrontEnd2003Setup.wsf /remove
  ```
  This deletes the virtual directory, **EnterpriseVaultProxy**, and the Proxy Bypass List.

**On back-end OWA 2003 Servers,** run the following command. In an active/passive OWA 2003 cluster, run this command on the active node first, and then run it on the passive node.

- Open a command prompt window.
- Enter on a single line the appropriate command for the server:
  ```cmd
  C:\Program Files\Enterprise Vault\OWA>cscript Backend2003Setup.wsf /remove
  ```
  This deletes all the Enterprise Vault OWA virtual directories **(EnterpriseVaultProxy, EnterpriseVaultPublic, EnterpriseVaultExchange, EVOWA)**, forms registrations and Proxy Bypass List.
OWA 2003: Checking that components have been removed

This section describes how you can check that the various components configured for Enterprise Vault OWA Extensions have been removed.

To ensure the EnterpriseVaultPublic and EnterpriseVaultExchange virtual directories have been removed from Active Directory
1. On the domain controller, open Exchange System Manager and select the required Exchange Server.
2. Expand Protocols, HTTP folders.
3. Select the name of the required Exchange Virtual Server. EnterpriseVaultPublic and EnterpriseVaultExchange virtual directories should not be listed in the right-hand pane.

To ensure that the EnterpriseVaultProxy virtual directory has been removed from the front-end OWA 2003 Server
1. On the front-end OWA Server, open IIS Manager.
2. Expand the required web site and check that the EnterpriseVaultProxy virtual directory has been removed.

To ensure that EnterpriseVaultProxy and EVOWA virtual directories have been removed from the back-end OWA 2003 Server
1. On the back-end OWA Server, open IIS Manager.
2. Check that the EnterpriseVaultProxy and EVOWA virtual directories have been removed.

In a cluster environment, after running the removal script on the passive node, you may still see the EnterpriseVaultPublic and EnterpriseVaultExchange virtual directories in IIS. These will be removed when the Exchange Server synchronizes IIS and Active Directory configuration data.

To check that the Proxy Bypass List has been cleared, do the following on the front-end and back-end OWA 2003 Servers
1. Open a command prompt window.
2. Enter the command:
   \Proxycfg

The Enterprise Vault OWA entries should not be displayed. If these were the only entries, then nothing will be displayed.
How to uninstall Enterprise Vault OWA Extensions

OWA 2003: Restoring OWA control files

1. On front-end and back-end OWA 2003 Servers only, copy the OWA control files from the folder `C:\Program Files\Exchsrvr\exchweb\6.5.nnnn.n\Controls-originals` to their original location:
   `C:\Program Files\Exchsrvr\exchweb\6.5.nnnn.n\Controls`

2. You can then remove manually the Enterprise Vault controls folder:
   `C:\Program Files\Exchsrvr\exchweb\6.5.nnnn.n\Controls-originals copied by Enterprise Vault`

OWA 2003: Completing the removal of the OWA Extensions

1. When all the Enterprise Vault virtual directories, form registrations and Proxy Bypass List have been removed, select and remove the Enterprise Vault OWA Extensions in **Add/Remove Programs** in the Control Panel on front-end and back-end OWA 2003 Servers.

2. You can then remove manually the following files on front-end servers:
   - `C:\Program Files\Enterprise Vault\OWA\EVfrontend.ini`
   - `C:\Program Files\Enterprise Vault\OWA\Frontend2003setup.wsf.log`

3. You can also remove manually the following files on back-end servers:
   - `C:\Program Files\Enterprise Vault\OWA\EVbackend.ini`
   - `C:\Program Files\Enterprise Vault\OWA\Backend2003setup.wsf.log`
   - `C:\Program Files\Enterprise Vault\OWA\EVservers.txt`

OWA 2000: Removing OWA virtual directories, forms registration and Proxy Bypass List

To remove the virtual directories, form registrations and Proxy Bypass List that are created by the Enterprise Vault OWA Extensions configuration program, you need to run the following Enterprise Vault scripts from the command line.

On back-end OWA 2000 Servers, run the following command. In an active/passive OWA 2000 cluster, run this command on the active node first, and then run it on the passive node.

1. Open a command prompt window.

2. Enter on a single line the appropriate command for the server:
   ```c:\program files\enterprise vault\owa>cscript Backend2000Setup.wsf /remove```
181

How to uninstall Enterprise Vault OWA Extensions

**OWA 2000: Removing OWA virtual directories, forms registration and Proxy Bypass List**

This deletes all the Enterprise Vault OWA virtual directories (EnterpriseVaultPublic, EnterpriseVaultExchange, EVOWA), forms registrations and Proxy Bypass List).

As the OWA Extensions are installed but not configured on front-end OWA 2000 Servers, you do not need to run a removal script on these servers.

**OWA 2000: Checking that components have been removed**

To ensure the EnterpriseVaultPublic and EnterpriseVaultExchange virtual directories have been removed from Active Directory

1. On the domain controller, open Exchange System Manager and select the required Exchange Server.
2. Expand **Protocols, HTTP folders**.
3. Select the name of the required Exchange Virtual Server. **EnterpriseVaultPublic** and **EnterpriseVaultExchange** virtual directories should not be listed in the right-hand pane.
   In a cluster environment, after running the removal script on the passive node, you may still see the **EnterpriseVaultPublic** and **Enterprise VaultExchange** virtual directories in IIS. These will be removed when the Exchange Server synchronizes IIS and Active Directory configuration data.

To ensure that EVOWA virtual directory has been removed from the back-end OWA 2000 Server

1. On the back-end OWA Server, open IIS Manager.
2. Check that **EVOWA** virtual directory has been removed.
   In a cluster environment, after running the removal script on the passive node, you may still see the **EnterpriseVaultPublic** and **EnterpriseVaultExchange** virtual directories in IIS. These will be removed when the Exchange Server synchronizes IIS and Active Directory configuration data.

To check that the Proxy Bypass List has been cleared, do the following on back-end OWA 2000 Servers

1. Ensure that the **proxycfg** utility is on the C drive.
2. Open a command prompt window.
3. Enter the command:
   
   ```
   C:\Proxycfg
   ```
The Enterprise Vault OWA entries should not be displayed. If these were the only entries, then nothing will be displayed.

**OWA 2000: Completing the removal of the OWA Extensions**

1. When all the Enterprise Vault virtual directories, form registrations and Proxy Bypass List have been removed, select and remove the Enterprise Vault OWA Extensions in **Add/Remove Programs** in the Control Panel on front-end and back-end OWA 2000 Servers. On front-end servers this will remove the following folder and its contents:

   C:\Program Files\Enterprise Vault\OWA

2. On back-end servers, you can then remove manually the following files:

   C:\Program Files\Enterprise Vault\OWA\EVbackend.ini
   C:\Program Files\Enterprise Vault\OWA\Backend2000setup.wsf.log
   C:\Program Files\Enterprise Vault\OWA\EVservers.txt
Configuring RPC over HTTP access to Enterprise Vault

Read this chapter to find out:

- How to install and configure the Enterprise Vault OWA & RPC Extensions on RPC proxy Exchange Servers and RPC target Exchange Servers
- How to configure Enterprise Vault servers to support RPC over HTTP connections

If the Exchange Servers are in a clustered environment, ensure that you are familiar with the additional information in “Configuring OWA and RPC Extensions in clustered configurations” on page 145 before you install and configure the Enterprise Vault OWA & RPC Extensions.

If RPC over HTTP users access the Exchange Servers through an ISA Server, you will also need to configure the ISA Server, after you have installed and configured the Enterprise Vault OWA & RPC Extensions.

See “Enabling Enterprise Vault access using RPC over HTTP” on page 175.

About Enterprise Vault support for RPC over HTTP connections

Outlook 2003 users can access mailboxes on Exchange Server 2003 using Remote Procedure Call (RPC) over HTTP. With this protocol, MAPI protocol is used to tunnel Outlook RPC requests inside an HTTP session. This allows remote Outlook 2003 users to connect to their Exchange Server mailbox, without the requirement for Outlook Web Access (OWA) or a virtual private network (VPN) connection.
The HTTP session terminates at a server running Internet Information Services (IIS) that has the Microsoft Windows Server 2003 RPC over HTTP Proxy networking component installed. This server is called an RPC proxy server.

To support user access to Enterprise Vault archives using either OWA or RPC over HTTP, or both, you need to install and configure the Enterprise Vault component, **OWA & RPC Extensions**, on your Exchange Server computers and also configure your Enterprise Vault servers. The steps for configuring OWA access are different from the steps for configuring RPC over HTTP access. This chapter describes how to install and configure the Enterprise Vault Extensions for RPC over HTTP access only.

If you want to enable support for both OWA and RPC over HTTP connections, then follow the instructions for enabling OWA first. See "Configuring OWA access to Enterprise Vault" on page 109.

You can then work through this chapter to check that you have satisfied the prerequisites and configuration required for RPC over HTTP connections.

To allow Outlook 2003 users to access Enterprise Vault archives using RPC over HTTP, either the Enterprise Vault User Extensions or the Enterprise Vault Self-Installing User Extensions must be installed on the client desktop.

With the default configuration, RPC over HTTP users can perform the following actions:

- View archived items
- Archive items manually
- Restore archived items
- Delete archived items
- Search archives
- Use Archive Explorer
- Use Offline Vault
- Perform client-side PST migrations

**Note:** When using RPC over HTTP, the Enterprise Vault User Extensions will automatically behave like the Enterprise Vault Self-Installing User Extensions; that is, the end user will not have access to the Enterprise Vault Properties page, and will not be able to select a different archive or Retention Category for items that are to be archived.
Summary of installation and configuration steps

Installing and configuring the Enterprise Vault OWA & RPC Extensions for RPC over HTTP access involves the following steps:

- Check that prerequisite tasks on IIS and Exchange Servers are completed. See “Prerequisite tasks” on page 185.

- Install the appropriate Enterprise Vault OWA & RPC Extensions component on each RPC proxy (front-end Exchange Server) and each RPC target server (back-end Exchange Server). See “Installing OWA & RPC Extensions” on page 188.

- On each RPC proxy, configure the extensions by running the configuration program, Exchange 2003 Front-end Ext. Configuration (OWA & RPC). See “Configuring an RPC proxy server (front-end Exchange Server)” on page 188.

- On each RPC target Exchange Server, create the EVServers.txt file, and then configure the extensions by running the configuration program, Exchange 2003 Back-end Ext. Configuration (RPC only). See “Configuring an RPC target server (back-end Exchange Server)” on page 189.

- On the Enterprise Vault server, create the Exchange Servers.txt file, and an account to be used for Anonymous connections, and then run the script, owauser.wsf, to configure the Anonymous user account. See “Configuring Enterprise Vault servers for RPC over HTTP” on page 191.

- On the Advanced page of Enterprise Vault mailbox policies, configure RPC over HTTP desktop settings. In a default configuration, RPC over HTTP support is not enabled. See “Configuring RPC over HTTP in Exchange Server mailbox policies” on page 193.

Prerequisite tasks

The instructions for configuring RPC over HTTP access to Enterprise Vault assume that you have already completed the following tasks:

On the RPC proxy server, ensure that the RPC over HTTP settings in the properties pages are set as shown in the figure, “RPC proxy properties”.

On the RPC target server, ensure that the RPC over HTTP settings in the properties pages are set as shown in the figure, “RPC target properties”.
RPC target properties

- Obtained and installed a valid certificate on the RPC proxy server.
- Configured SSL on the RPC proxy server.
- Ensured that the operating system on client computers supports RPC over HTTP connections.
  All client computers that run Outlook 2003 must have either Windows Server 2003, Microsoft Windows XP SP2, or Microsoft Windows XP SP1 with the update described in the Microsoft Knowledge Base article, http://support.microsoft.com/?kbid=331320.
- On desktop computers, created an Outlook profile for using RPC over HTTP. See the Microsoft article, http://office.microsoft.com/en-ca/assistance/ha011402731033.aspx
- Configured your Enterprise Vault server to archive Exchange Server mailboxes or public folders or both.
  See “Setting up archiving from mailboxes” on page 245.
  See “Setting up archiving from public folders” on page 259.
- Installed Enterprise Vault User Extensions or Enterprise Vault Self-Installing User Extensions on the desktop computers.
  See “Setting up users’ desktops” on page 93.
Installing OWA & RPC Extensions

This section describes how to install the Enterprise Vault component, OWA & RPC Extensions, on your RPC over HTTP Exchange Servers. Repeat the installation instructions on each RPC proxy and RPC target Exchange Server.

To install the Enterprise Vault OWA & RPC Extensions component

2. Open the Enterprise Vault folder. Check the ReadMeFirst.htm file in this folder for details of any last minute changes.
3. Open the Server folder.
4. Double-click SETUP.EXE to start the installation.
5. On RPC proxy servers, select the Exchange 2003 Front-end Ext. (OWA & RPC) component.
   On RPC target servers, select the Exchange 2003 Back-end Ext. (OWA & RPC) component.
   Follow the installation instructions.
6. Now configure the extensions on each RPC proxy server.
   See “Configuring an RPC proxy server (front-end Exchange Server)”.

Configuring an RPC proxy server (front-end Exchange Server)

After you have installed the Enterprise Vault OWA & RPC Extensions on the RPC proxy servers, run the extensions configuration program, as described in this section, on each RPC proxy server.

To configure Enterprise Vault OWA & RPC Extensions on an RPC proxy server

1. Log on to the RPC proxy Exchange Server computer using an account that has Exchange Full Administrator permissions.
3. A command prompt window opens and lists what the configuration program has done.
   The configuration program sets up the following for each Exchange virtual server it finds on the computer:
Configuring an RPC target server (back-end Exchange Server)

After you have installed the Enterprise Vault OWA & RPC Extensions on an RPC target Exchange Server, you need to perform the following tasks on each RPC target Exchange Server:

- Create an EVServers.txt file.
  See “Creating the EVServers.txt file”.
- Run the extensions configuration program.
  See “Configuration an RPC target Exchange Server” on page 190.

Creating the EVServers.txt file

The EVServers.txt file enables the configuration program to set up WinHTTP with the correct proxy bypass list for the Enterprise Vault server. The entries you create in the EVServers.txt file will be appended to the proxy bypass list.

To create the EVServers.txt file:

1. Open Notepad.
2. Type in, one entry per line, the Vault Site alias in both fully-qualified and LanMan forms. For example:
   ourvaultsitealias.domain.com
   ourvaultsitealias
   Also type in any aliases for each Enterprise Vault server computer in the Vault Site. Enter these one per line, in fully-qualified and LanMan forms.
   For example:
Configuring an RPC target server (back-end Exchange Server)

To configure Enterprise Vault Extensions on an RPC target server

1. Log on to the Exchange Server computer using an account that has Exchange Full Administrator permissions.

2. Ensure the Exchange Server is running and that the web site associated with the Exchange Server has an ExAdmin virtual directory created.

3. To configure RPC over HTTP only (not OWA), then click Start > Programs, Enterprise Vault > Exchange Back-end Ext. Configuration (RPC Only)

4. A command prompt window opens and lists what the configuration program has done.
   If you run the RPC only configuration program, then the following is configured for each Exchange virtual server found on the computer:
   - An EnterpriseVaultProxy virtual directory for each web server on the computer.
   - Proxy bypass list.
   (If the OWA and RPC configuration program is run, then additional virtual directories are created).

5. When the configuration program has finished, you will see the following line in the command prompt window:
   Press ENTER to end

6. Details of the configuration process are sent to the log file:
   Enterprise Vault\OWA\BackEnd2003Setup.wsf.log
   Check the log file for any configuration errors.

7. Now configure the Enterprise Vault server as described in “Configuring Enterprise Vault servers for RPC over HTTP”.

3. Save the file as EVServers.txt in the OWA folder in your Enterprise Vault installation folder (typically, C:\Program Files\Enterprise Vault\OWA).


5. Now configure the extensions, as described in “Configuration an RPC target Exchange Server”.

Configuration an RPC target Exchange Server

This section describes how to configure the RPC target Exchange Servers.

To configure Enterprise Vault Extensions on an RPC target server

1. Log on to the Exchange Server computer using an account that has Exchange Full Administrator permissions.

2. Ensure the Exchange Server is running and that the web site associated with the Exchange Server has an ExAdmin virtual directory created.

3. To configure RPC over HTTP only (not OWA), then click Start > Programs, Enterprise Vault > Exchange Back-end Ext. Configuration (RPC Only)

4. A command prompt window opens and lists what the configuration program has done.
   If you run the RPC only configuration program, then the following is configured for each Exchange virtual server found on the computer:
   - An EnterpriseVaultProxy virtual directory for each web server on the computer.
   - Proxy bypass list.
   (If the OWA and RPC configuration program is run, then additional virtual directories are created).

5. When the configuration program has finished, you will see the following line in the command prompt window:
   Press ENTER to end

6. Details of the configuration process are sent to the log file:
   Enterprise Vault\OWA\BackEnd2003Setup.wsf.log
   Check the log file for any configuration errors.

7. Now configure the Enterprise Vault server as described in “Configuring Enterprise Vault servers for RPC over HTTP”.
Configuring Enterprise Vault servers for RPC over HTTP

Connections between RPC target Exchange Servers and Enterprise Vault servers use Anonymous authentication. To support these connections, you need to perform the following tasks to configure an Anonymous user account on the Enterprise Vault servers:

- Create the **ExchangeServers.txt** file. This file contains the IP addresses of all the RPC target Exchange Servers that will connect to the Enterprise Vault server. See “ExchangeServers.txt file” on page 191.
- Create and configure an account to be used for Anonymous connections. See “Configuring an Anonymous user account for RPC over HTTP” on page 191.
- Using the Enterprise Vault Administration Console, enable RPC over HTTP in Enterprise Vault mailbox policies. See “Configuring RPC over HTTP in Exchange Server mailbox policies” on page 193.

ExchangeServers.txt file

First, you need to create the **ExchangeServers.txt** file on the Enterprise Vault server. This holds a list of the IP addresses for all the RPC target Exchange Servers that will connect to the Enterprise Vault server.

**To create the ExchangeServers.txt file**

1. Open Notepad.
2. Type the IP address of each RPC target Exchange Server (that is, the Exchange virtual server IP address), one entry per line.
   If the RPC target Exchange Servers are clustered, enter the Virtual Server IP addresses first and then add the cluster IP address and the IP addresses of each node.
3. Save the file as **ExchangeServers.txt** in the Enterprise Vault installation folder (typically C:\Program Files\Enterprise Vault).

Configuring an Anonymous user account for RPC over HTTP

Now you can create and configure a user account for the Anonymous connections from servers listed in the **ExchangeServers.txt** file.
To configure an Anonymous user account

1. Create a domain user account to use as the Anonymous user account. This should be a basic domain account specifically created for the purpose; a local machine account cannot be used.
   If you have an existing Anonymous user account, and it is a domain account, then use this account. If your existing Anonymous user account is a local machine account, then you will need to create a new domain account for the Anonymous user.

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

3. Open a command prompt window and navigate to the Enterprise Vault installation folder.

4. Type and enter the command line:
   ```
cscript owauser.wsf /domain:<domain> /user:<username> /password:<password> /exch2003
   
   The file owauser.wsf is installed in the Enterprise Vault installation folder.
   For <domain>, give the domain of the Anonymous user account.
   For <username>, give the username of the Anonymous user account.
   For <password>, give the password of the Anonymous user account.
   To display help for the cscript command, type cscript owauser.wsf /?
   
   The progress of the script execution is displayed in the command prompt window.
   The owauser.wsf script sets up the following on the Enterprise Vault server:
   ■ Assigns the following user rights to the Anonymous user:
     ■ SeNetworkLogonRight
     ■ SeInteractiveLogonRight
     ■ SeBatchLogonRight
     ■ SeChangeNotifyPrivilege
   ■ Creates (or updates) the virtual directory, EVAnon, that points to the Enterprise Vault\WebApp folder and gives access permissions to the Anonymous user.
     Access to EVAnon is also granted to the RPC target servers. You can check this by displaying the properties of the EVAnon virtual directory, selecting the Directory Security tab and clicking Edit in the IP address and domain name restrictions section.
   ■ Creates (or updates) the following two Registry values:
Configuring Enterprise Vault servers for RPC over HTTP

HKEY_CURRENT_USER
\Software
\KVS
\Enterprise Vault
\AnonymousUser

The value of this setting is the full name, including the domain, of the Anonymous user. For example, mydomain\EVANONUSER

HKEY_LOCAL_MACHINE
\SOFTWARE
\KVS
\Enterprise Vault
\Install
\Owa\WebAppAlias

The value of this setting is the name of the virtual directory for anonymous connections, EVAnon.

To complete the configuration, you need to restart the Enterprise Vault Admin service and synchronize the mailboxes of RPC users.

Next, configure mailbox policies for RPC over HTTP, as described in “Configuring RPC over HTTP in Exchange Server mailbox policies”.

Configuring RPC over HTTP in Exchange Server mailbox policies

As RPC over HTTP connections are not enabled by default in Exchange Server mailbox policies, you must edit the mailbox policy settings. These settings also enable you to restrict the availability of RPC over HTTP to users.

To modify RPC over HTTP Exchange mailbox policy settings

1 In the left pane of the Administration Console, expand the hierarchy until Policies is visible.

2 Expand Policies.

3 Expand Exchange.

4 Click Mailbox.

5 In the right-hand pane, double-click the name of the policy you want to edit. The policy’s properties are displayed.

6 Click the Advanced tab.

7 Next to List settings from, select Desktop.

8 Edit the RPC over HTTP restrictions and RPC over HTTP Proxy URL settings as required.

   Double-click a setting to edit it, or click it once to select it and then click Modify.
The setting, **RPC over HTTP restrictions**, controls the behavior of the Enterprise Vault User Extensions when Outlook is configured to use RPC over HTTP. You can select one of the following values for this setting:

<table>
<thead>
<tr>
<th>Possible values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>All Enterprise Vault client functionality is available.</td>
</tr>
<tr>
<td>Disable User Extensions</td>
<td>RPC over HTTP working is not enabled in the Enterprise Vault client. This is the default value.</td>
</tr>
<tr>
<td>Disable Offline Vault only</td>
<td>Offline Vault is disabled.</td>
</tr>
<tr>
<td>Disable PST Import only</td>
<td>Client-side PST migration is disabled.</td>
</tr>
<tr>
<td>Disable Offline Vault and PST Import</td>
<td>Offline Vault and client-side PST migration are disabled.</td>
</tr>
</tbody>
</table>

The setting, **RPC over HTTP Proxy URL**, enables you to specify an alternative URL for the Enterprise Vault web server that clients can contact when Outlook is configured to use RPC over HTTP. By default, clients connect to the virtual directory, **EnterpriseVaultProxy**, on the RPC proxy server. If you change the name of this virtual directory, then you can use this setting to specify the alternative URL.

For example, if you change the virtual directory name to **EVProxy**, then you would use the **RPC over HTTP Proxy URL** setting to specify the URL: **HTTP://web_server/EVProxy**

where **web_server** is the name RPC proxy server.

9 The settings are applied to users’ mailboxes during the next synchronization run of the Exchange Mailbox task. If you want to apply the changes before the next synchronization, run **Synchronize**, which is on the **Synchronization** tab of the Exchange Mailbox task’s properties.

10 Remember that Outlook 2003 users will require a profile enabled for RPC over HTTP. See “Prerequisite tasks” on page 185.
Clustering Enterprise Vault

The section includes the following chapters:

- Chapter 16, “Introducing clustering” on page 197
- Chapter 17, “Installing and configuring VERITAS Storage Foundation HA” on page 201
- Chapter 18, “Configuring the service group” on page 205
- Chapter 19, “Running the Enterprise Vault Configuration wizard” on page 215
- Chapter 20, “Implementing a VSFW HA-VVR disaster recovery solution” on page 229
- Chapter 21, “Troubleshooting clustering” on page 235
Introducing clustering

You can integrate Enterprise Vault with VERITAS Cluster Server (VCS) to provide a highly-available solution for Enterprise Vault.

Supported configurations and software

Both active/passive and N+1 configurations are supported, but active/active configurations are not.

In an active/passive configuration, a dedicated spare server is available for each Enterprise Vault server, ready and waiting for the primary server to go down. In an N+1 configuration, there is a computer for each Enterprise Vault server and then one or more spare servers waiting for any of the active servers to fail over.

The following software must be installed:

- VERITAS Storage Foundation HA 4.3 MP1 for Windows
- Enterprise Vault
- Windows Server 2003

About the VCS GenericService agent

VCS uses the GenericService agent to monitor the Enterprise Vault services on different nodes based on the information in the Enterprise Vault Directory database. The agent brings online the following services, monitors their status, and takes them offline.

- Admin service
- Directory service
- Indexing service
- Shopping service
Introducing clustering

Typical Enterprise Vault configuration in a VCS cluster

- Storage service
- Task Controller service

See the VERITAS Cluster Server Bundled Agents Reference Guide for detailed information on the GenericService agent, including the resource type definitions, attribute definitions, and sample configurations.

The GenericService agent detects an application failure if a configured service is not running. When this happens, the Enterprise Vault service group is failed over to the next available system in the service group’s system list, and the services are started on the new system. This ensures continuous availability for the data that Enterprise Vault is managing and archiving.

Typical Enterprise Vault configuration in a VCS cluster

The following figure illustrates a typical configuration.

**Figure 16-1**  
Active/passive failover configuration

Here, the volumes for the Enterprise Vault services data are configured in a cluster disk group on shared storage. The Enterprise Vault virtual server is configured on the active node (System 1). If System 1 fails, System 2 becomes
the active node, and the Enterprise Vault virtual server comes online on System 2.
Introducing clustering

Typical Enterprise Vault configuration in a VCS cluster
Chapter 17

Installing and configuring VERITAS Storage Foundation HA

This chapter outlines the steps required to install and configure VERITAS Storage Foundation HA for Windows (VSFW HA) with Enterprise Vault.

If you want to implement a disaster recovery solution, see Chapter 20, “Implementing a VSFW HA-VVR disaster recovery solution” for instructions.

Installing and configuring VSFW HA

Except where noted, you can get detailed instructions on how to perform the steps outlined in this section from the chapter “Implementing a VSFW HA solution” in the VERITAS Storage Foundation and High Availability Solutions 4.3 Solutions Guide.

To install and configure VSFW HA

1. Install VSFW HA 4.3 on each node that is to be a part of the cluster. There are several stages to this process:
   a. Review the product installation requirements, disk space requirements, and requirements for VSFW HA.
   b. Configure the network and storage.
   c. Install VSFW HA.

2. Upgrade VSFW HA 4.3 to 4.3 MP1. For detailed instructions, see the VERITAS Storage Foundation and High Availability Solutions 4.3 Maintenance Pack (MP) 1 Release Notes.
3  Configure the cluster by running the VCS Configuration wizard.

4  Install Enterprise Vault on all systems in the cluster. For detailed instructions, see Section 1, “Installing, configuring, and upgrading Enterprise Vault”.

5  Configure the disk group and volumes from the first node. You must create shared volumes to store the following:
   ■ Indexing service data
   ■ Shopping service data
   ■ Vault store partitions
   ■ PST holding folders
   ■ EMC Centera staging areas
   We also recommend that you create separate volumes to store the MSMQ and registry replication data.

6  Mount the volumes on the system where you will configure the Enterprise Vault service group. For detailed instructions, see “Managing disk groups and volumes” on page 202.

7  Configure the Enterprise Vault service group. For detailed instructions, see Chapter 18, “Configuring the service group”.

8  Run the Enterprise Vault Configuration wizard to create the Enterprise Vault services and resources. For detailed instructions, see Chapter 19, “Running the Enterprise Vault Configuration wizard”.

9  Verify the cluster configuration and test the failover capability.

Managing disk groups and volumes

This section describes how to perform the following activities:
■ Importing a dynamic disk group
■ Mounting a shared volume
■ Unmounting a volume and deporting a disk group
While you set up a VSFW HA environment, keep the following points in mind:
■ You must mount the volumes on the system where you will configure the Enterprise Vault service group.
■ When a disk group is initially created, it is imported on the node where it is created.
■ A disk group can be imported on one node only at a time.
To move a disk group from one node to another, unmount the volumes in the group, deport the group from its current node, import it to a new node, and mount the volumes.

To import a dynamic disk group
1. On the Windows Start menu, click All Programs > VERITAS > VERITAS Enterprise Administrator to open the VERITAS Enterprise Administrator.
2. Right-click a disk name in the dynamic disk group or the dynamic disk group name in the tree view, and then click Import Dynamic Disk Group on the context menu.
3. Follow the on-screen instructions.

To mount a volume
1. If you have yet to do so, open the VERITAS Enterprise Administrator and import the dynamic disk group.
2. Right-click the volume, and then click File System > Change Drive Letter and Path.
3. In the Drive Letter and Paths dialog box, click Add.
4 Select one of the following options, depending on whether you want to assign a drive letter to the volume or mount it as a folder.

<table>
<thead>
<tr>
<th>To do this</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign a drive letter.</td>
<td>Click <strong>Assign a Drive Letter</strong>, and then choose the required letter.</td>
</tr>
<tr>
<td>Mount the volume as a folder</td>
<td>Click <strong>Mount as an empty NTFS folder</strong>, and then click <strong>Browse</strong> to locate an empty folder on the shared disk.</td>
</tr>
</tbody>
</table>

5 Click **OK**.

**To unmount a volume and deport the dynamic disk group**

1 In the VERITAS Enterprise Administrator, right-click the volume and then click **File System > Change Drive Letter and Path**.
2 In the Drive Letter and Paths dialog box, click **Remove**.
3 Click **OK**.
4 Right-click the disk, and then click **Deport Dynamic Group**.
5 Click **Yes** to confirm that you want to deport the disk group.
In VCS, a service group represents a virtual server. Each service group contains a set of resources, which you can bring online or offline when a group fails over to another node in the cluster. You can arrange a combination of these resources to make a complete Enterprise Vault server.

These resources include:

- IP address
- Computer name (Lanman resource)
- MSMQ
- Disk/storage (MountV and DiskGroup resources)
- Service resources

Before you can configure Enterprise Vault in a cluster, you must configure a service group to represent the Enterprise Vault server. VCS provides several ways to configure a service group, including the Enterprise Vault Cluster Setup wizard, Cluster Manager (both Java Console and Web Console), and the command line. This chapter describes how to configure a service group with the Enterprise Vault Cluster Setup wizard.

Before you begin

Before you configure an Enterprise Vault service group, do the following:

- Verify your DNS server settings. You must ensure that a static DNS entry maps the virtual IP address with the virtual server name. Refer to the appropriate DNS document for more information.
- Verify that the Command Server is running on all systems in the cluster.
Configuring the service group
Creating a service group

- Verify that the VERITAS High Availability Daemon (HAD) is running on the system from where you will run the Enterprise Vault Cluster Setup wizard.
- Ensure that you have Cluster Administrator privileges. You must also be a Local Administrator on the node where you run the wizard.
- Verify that MSMQ is installed locally on each node.
- Mount the shared volumes that you have created to store the following:
  - Indexing service data
  - Shopping service data
  - Vault store partitions
  - PST holding folders
  - EMC Centera staging areas
Unmount the volumes from other nodes in the cluster.

Creating a service group

Note that the Enterprise Vault Cluster Setup wizard is available from the Windows Start menu if you install Enterprise Vault after you install VCS. If you install Enterprise Vault first, you must separately install the wizard. To do this, locate and run the file Enterprise Vault Cluster Setup Wizard.msi.

To create the service group

1. On the Windows Start menu, click All Programs > VERITAS > VERITAS Cluster Server > Enterprise Vault Cluster Setup Wizard.
2 Review the information in the Welcome page, and then click **Next** to display the Wizard Options page.
3 Click **Create service group**, and then click **Next** to display the Service Group Configuration page.

4 In the **Service Group Name** box, type a name for the group, such as EVGRP1.

5 Move to the **Systems in Priority Order** box those systems on which you want to configure the service group.

   If you want to change the priority of the systems in the **Systems in Priority Order** box, click a system and then click the up-arrow or down-arrow button.
6 Click **Next** to validate the configuration and display the Virtual Server Configuration page.

7 Complete the fields as follows:

   a In the **Virtual Server Name** box, type the server name that you mapped to the virtual IP address when you set up the static DNS entry (see “Before you begin” on page 205).

   b In the **Virtual IP address** box, type the address that you mapped to the virtual server. This should be in the same subnet as the current computer, but it should not currently be in use on the network.

   c Enter the subnet mask to which the virtual server belongs.

   d For each system in the cluster, select the public network adapter name. The wizard lists all the TCP/IP-enabled adapters on the system, including the private network adapters if they are TCP/IP enabled. Be sure to select the adapters to assign to the **public** network, and not those assigned to the private network.

   e Click **Advanced** to specify details for the Lanman resource. You must select the distinguished name of the organizational unit for the virtual server. By default, the Lanman resource adds the virtual server to the default container Computers.
The user account for VCS Helper service must have adequate privileges on the specified container to create and update computer accounts.

8. In the Virtual Server Configuration page, click **Next** to display the MSMQ and RegRep Directory Details page.

This page enables you to virtualize the MSMQ resource so that it can be accessed using its virtual name. This resource also ensures that the queue state is maintained after failover.

9. Complete the fields as follows:

   a. In the **MSMQ Directory** field, enter the path to the required directory.

   b. In the **Replication Directory** field, enter the path to the registry replication directory. The replication data contains a list of the registry keys to replicate.

   We recommend that you configure the MSMQ and replication directories on different volumes.
10 Click **Next** to display the Storage Location Details page.

This page lets you select the volumes that you want to configure for Enterprise Vault services. A volume is available for selection only if you have configured it on the shared disk. The available volumes do not include those that you selected in the previous page of the wizard, when specifying the storage locations for MSMQ and registry replication.

11 In the **Available Volumes** box, select each volume on which you have configured the services and then click the right-arrow button to move it to the **Selected Volumes** box. You must select the volumes that you configured for each of the following:

- Indexing service data
- Shopping service data
- Vault store partitions
- PST holding folders
- EMC Centera staging areas
12 Click **Next** to display the Service Group Summary page.

13 Review your configuration. If you want to modify an attribute name for any reason, follow these steps:
   a. Click the resource, and then click the attribute that you want to modify.
   b. Click the **Edit** icon at the end of the table row.
   c. In the Edit Attribute dialog box, enter the attribute values.
   d. Click **OK**.
   e. Repeat the procedure for each resource and attribute.

14 Click **Next** to display the Completion page.

15 Click **Bring the service group online**, and then click **Finish**.
Modifying an existing service group

The following table lists the items that you can modify in a service group.

<table>
<thead>
<tr>
<th>Table 18-1</th>
<th>Modifiable service group items</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Item</strong></td>
<td><strong>Notes</strong></td>
</tr>
<tr>
<td>System list</td>
<td>You can add nodes to or remove them from the cluster. If you want to remove a node, make sure that it is not the active one.</td>
</tr>
<tr>
<td>Volumes</td>
<td>You can add or remove volumes. If you remove a volume on which an Enterprise Vault service is configured, the service ceases to be highly available and is not monitored.</td>
</tr>
<tr>
<td>Virtual IP</td>
<td>You can change the virtual IP address if the service group is offline. You cannot change the virtual server name, which is fixed when you create the service group.</td>
</tr>
</tbody>
</table>

You can modify an Enterprise Vault service group in several ways, including the Enterprise Vault Cluster Setup Wizard, Cluster Manager (both Java Console and Web Console), and the command line. The following steps describe how to modify the service group with the Enterprise Vault Cluster Setup Wizard.

Before you proceed, note the following:

- You must run the wizard from a node on which the service group is online. You can then use the wizard to add resources to or remove them from the configuration.
- You must take the service group partially offline to change the resource attributes. However, the MountV and VMDg resources for the service group should be online on the node where you run the wizard and offline on all other nodes. Mount all the volumes created to store Storage service data (vault stores), registry replication information, Shopping service data, Indexing data and MSMQ data.
- If you want to modify the system list or volumes, the service group must be online.

**To modify an existing service group**

1. On the Windows Start menu, click All Programs > VERITAS > VERITAS Cluster Server > Enterprise Vault Cluster Setup Wizard.
2. Review the information in the Welcome page, and then click Next to display the Wizard Options page.
3. Click Modify service group, and then click Next.
4. Follow the instructions to modify the service group.
Deleting a service group

Follow the steps below to delete a service group with the Enterprise Vault Cluster Setup wizard.

To delete an Enterprise Vault service group

1. On the Windows Start menu, click All Programs > VERITAS > VERITAS Cluster Server > Enterprise Vault Cluster Setup Wizard.
2. Review the information in the Welcome page, and then click Next to display the Wizard Options page.
3. Click Delete service group, and then click Next.
4. In the Service Group Summary page, click Next.
5. When the wizard prompts you to confirm that you want to delete the service group, click Yes.
6. Click Finish.
Chapter 19

Running the Enterprise Vault Configuration wizard

The Enterprise Vault Configuration wizard provides options for setting up Enterprise Vault in a cluster. This chapter describes the options that you must select to do this.

The chapter provides instructions on how to carry out the following tasks:

■ Setting up an active/passive configuration
■ Setting up an N+1 configuration

Before you begin

Before you run the Enterprise Vault Configuration wizard, ensure that:

■ The Enterprise Vault service group exists and is online on the node from which you want to run the wizard. For instructions on how to create or modify the service group, see Chapter 18, “Configuring the service group”.
■ You have installed VSFW HA 4.3 MP1 or later.

Setting up an active/passive configuration

As well as describing how to set up cluster support in a first-time installation of Enterprise Vault, this section describes how to upgrade an existing, standard installation of Enterprise Vault to a clustered environment.

For instructions on how to upgrade an existing installation, see “Upgrading an existing Enterprise Vault installation to a cluster” on page 219.
Adding cluster support in a first-time Enterprise Vault installation

You must run the Enterprise Vault Configuration wizard on each node of the cluster. On the first node, choose the option to **Create a new Enterprise Vault server with cluster support**. On each additional node, choose the option to **Add this node as a failover node for an existing clustered server**.

To create a new Enterprise Vault server with cluster support

1. On the Windows **Start** menu, click **All Programs > Enterprise Vault > Enterprise Vault Configuration**.
   
The first page of the wizard appears.

2. Click **Configure a new Enterprise Vault server with cluster group**, and then click **Next**.

3. Follow the on-screen instructions.
When the wizard prompts you for the DNS alias for the vault site, enter a DNS alias that points to the virtual server name.

In addition, take care to review the storage locations for the Indexing and Shopping services, when the wizard prompts you to do so.

4. In the Finish page, click **Bring all the resources online**, and then click **Finish**. After you have configured the server on the first node, run the wizard from each additional node that you want to configure as a failover node.
Caution: The path to the Enterprise Vault program folder must be the same on all nodes in the cluster. This is typically C:\Program Files\Enterprise Vault. If the path varies from one node to another, problems can occur during failover.

To add a failover node for an existing clustered server

1. On the Windows Start menu, click All Programs > Enterprise Vault > Enterprise Vault Configuration.
2. Click Add this node as a failover node for an existing clustered server, and then click Next.
3. Follow the on-screen instructions.
   When the wizard prompts you for the name of the service group to which you want to add the node, select the name of the service group that you chose for the first node.
4. In the summary page, review the information, and then click Next.
   The wizard informs you that it will create the Enterprise Vault service group on the new node.
5. In the Finish page, click Finish to exit the wizard.
6 Check that you can bring the resources online on the failover node. You can do this with Cluster Explorer, by clicking **Switch To** on the context menu.

---

**Upgrading an existing Enterprise Vault installation to a cluster**

There are two types of Enterprise Vault installation that you can upgrade to a cluster: a single, non-clustered Enterprise Vault server, and a building blocks configuration that contains multiple Enterprise Vault servers. To be eligible for upgrade to a cluster, the Enterprise Vault installation must have the following features:

- Enterprise Vault should already be configured in a non-clustered configuration, and it must not already be part of a cluster.
- Enterprise Vault must be configured using DNS aliases rather than fully qualified names.
- The Enterprise Vault server must have a full set of Indexing, Shopping, Task Controller and Storage services. However, it must not contain the SharePoint Portal Server 2001 service, as this is not supported in a cluster.
- In a building blocks environment, an Enterprise Vault server that is hosting services must not be running in failover mode.

**To upgrade an existing installation to a clustered Enterprise Vault environment**

1 Run the Enterprise Vault Cluster Setup wizard to create an Enterprise Vault cluster service group and add to the group the server that you are going to configure.

2 Ensure that the following items are all on highly-available shared storage devices.
   - Indexing service data
   - Shopping service data
   - Vault store partitions
Running the Enterprise Vault Configuration wizard

Setting up an active/passive configuration

- PST holding folders
- EMC Centera staging areas

If they are not, correct the locations in the Enterprise Vault Directory database and then move the associated data to the new locations. See “Moving data to highly-available locations” on page 221 for more information on how to move the data.

3 On the Windows **Start** menu, click **All Programs > Enterprise Vault > Convert to Cluster**.

4 Read the introductory information, and then click **Next**.

5 When the following page appears, check **All locations are highly available storage devices**, and then click **Next**.

6 If the wizard detects that there are messages in the Enterprise Vault MSMQ queues, choose whether to proceed with the conversion without migrating them to the clustered MSMQ queues.

**Tip:** Wait until the queues have cleared and then rerun the Convert to Cluster wizard. Any messages that are still in the queues are ignored in the new cluster. To accelerate the process of clearing the queues, stop the Task Controller service and ensure that File System Archiving is not performing an archiving run.
7 When the wizard prompts you to choose a service group in which to create the cluster resources for each Enterprise Vault service, select the group that you created earlier.

8 Click Next to create the cluster resources, and then review the list of actions that the wizard has carried out.

9 Click Finish to close the wizard.

10 Using the DNS snap-in to the Microsoft Management Console (MMC), change the site alias and computer name alias to point to the virtual server name rather than the local name.

11 Use VERITAS Cluster Manager to bring the resources in the cluster online.

Moving data to highly-available locations

In outline, the procedure for moving the data to highly-available locations is as follows:

1 Stop the Indexing, Shopping, Storage, and Task Controller services.

2 Make a backup copy of the Enterprise Vault Directory database and data files.
Use the Vault Administration Console or SQL Query Analyzer against the Enterprise Vault directory to move the data, as described below.

<table>
<thead>
<tr>
<th>Item</th>
<th>What to do</th>
</tr>
</thead>
</table>
| IndexRootPathEntry [IndexRootPath] | 1 Move the contents of this location to a highly available location.  
2 Update the database using SQL to point at the new location.  
The SQL to view the current location is as follows:  
```
SELECT *
FROM IndexRootPathEntry
WHERE (IndexRootPathEntryId = '<ID FROM LOG FILE>')
```

The SQL to update the location is as follows:
```
UPDATE IndexRootPathEntry
SET IndexRootPath = '<THE NEW LOCATION>'
WHERE (IndexRootPathEntryId = '<ID FROM LOG FILE>')
```
| PartitionEntry [AccountName] | 1 Move the pool entry authorization (.pea) file to a highly available location.  
2 Use the Vault Administration Console to view the properties of the EMC Centera partition and then, on the Connection tab, edit the Pool Entry Authorization File Location box to point at the new location. |
| PartitionEntry [PartitionRootPath] | 1 Move the contents of this location to a highly available location.  
2 Update the database using SQL to point at the new location.  
The SQL to view the current location is as follows:  
```
SELECT *
FROM PartitionEntry
WHERE (PartitionEntryId = '<ID FROM LOG FILE>')
```

The SQL to update the location is as follows:
```
UPDATE PartitionEntry
SET PartitionRootPath = '<THE NEW LOCATION>'
WHERE (PartitionEntryId = '<ID FROM LOG FILE>')
```
## Setting up an active/passive configuration

<table>
<thead>
<tr>
<th>Item</th>
<th>What to do</th>
</tr>
</thead>
<tbody>
<tr>
<td>PartitionEntry/Locations</td>
<td>1   Move the secondary storage files to a highly available location.</td>
</tr>
<tr>
<td></td>
<td>2   Update the database using SQL to point at the new location.</td>
</tr>
<tr>
<td>[SecondaryLocation]</td>
<td>The SQL to view the current location is as follows:</td>
</tr>
<tr>
<td></td>
<td>```sql</td>
</tr>
</tbody>
</table>
|                             | SELECT *  
|                             | FROM PartitionEntry  
|                             | INNER JOIN Locations ON  
|                             | PartitionEntry.SecondaryLocation = Locations.LocationIdentity  
|                             | WHERE (PartitionEntry.PartitionEntryId = '<ID FROM LOG FILE>')            |
|                             | The SQL to update the location is as follows:                           |
|                             | ```sql                                                                   |
|                             | UPDATE Locations  
|                             | SET Location = '<NEW LOCATION>'  
|                             | WHERE LocationIdentity = (SELECT SecondaryLocation FROM  
|                             | PartitionEntry  
|                             | WHERE PartitionEntryId = '<ID FROM LOG FILE>')  
| PartitionEntry             | 1   Move the contents of this location to a highly available location.   |
| [StagingRootPath]           | 2   Update the database using SQL to point at the new location.          |
|                             | The SQL to view the current location is as follows:                      |
|                             | ```sql                                                                   |
|                             | SELECT *  
|                             | FROM PartitionEntry  
|                             | WHERE (PartitionEntryId = '<ID FROM LOG FILE>')                         |
|                             | The SQL to update the location is as follows:                           |
|                             | ```sql                                                                   |
|                             | UPDATE PartitionEntry  
|                             | SET StagingRootPath = '<THE NEW LOCATION>'  
|                             | WHERE (PartitionEntryId = '<ID FROM LOG FILE>')                         |
| PSTMigratorTask             | 1   Move the contents of the location to a highly available location.   |
| [MigrationDirectory]        | 2   Use the Vault Administration Console to view the properties of the PST Migrator Task and update the Temporary files folder. |
The previous sections describe how to set up an active/passive cluster, where each Enterprise Vault server has a dedicated spare node. In effect, therefore, each server requires at least two nodes. As a cheaper alternative, you can set up an N+1 configuration in which there is a single spare node for the cluster.

There are two basic types of N+1 configurations:

- The clustered Enterprise Vault servers run on two nodes, and there is a shared spare node.
- The two Enterprise Vault servers are configured to run on any of the three nodes in the cluster.

The following sections describe how to set up Enterprise Vault in these two configurations.

<table>
<thead>
<tr>
<th>Item</th>
<th>What to do</th>
</tr>
</thead>
<tbody>
<tr>
<td>ShoppingServiceEntry</td>
<td>1  Move the contents of this location to a highly available location.</td>
</tr>
<tr>
<td>[ShoppingRootPath]</td>
<td>2  Use the Vault Administration Console to edit the Shopping service location to the new highly available location.</td>
</tr>
<tr>
<td>SiteEntry</td>
<td>1  Move the contents of the location to a highly available location.</td>
</tr>
<tr>
<td>[PSTHoldingDirectory]</td>
<td>2  Use the Vault Administration Console to view the site properties and update the PST Holding Folder property to point at the new location.</td>
</tr>
</tbody>
</table>
N+1 configuration option 1

The figure below illustrates a configuration in which there is a spare node in addition to the two nodes on which the Enterprise Vault servers are running.

You configure the service group for EVSERVER1 to run on both NODEA and NODEC, and the service group for EVSERVER2 to run on both NODEB and NODEC. EVSERVER1 and EVSERVER2 are both virtual computer names from the service group.

To set up this N+1 configuration

1. Mount the volumes on the system where you will configure the Enterprise Vault service group. For detailed instructions, see “Managing disk groups and volumes” on page 202.

2. On either NODEA or NODEC, run the Enterprise Vault Cluster Setup wizard and create a service group called EVSERVER1 for these two nodes.

3. On either NODEB or NODEC, run the Enterprise Vault Cluster Setup wizard and create a service group called EVSERVER2 for these two nodes.

4. Take the following actions on NODEA and NODEB, depending on whether you are performing a first-time installation of Enterprise Vault or upgrading an existing installation:

<table>
<thead>
<tr>
<th>Node</th>
<th>New installation</th>
<th>Upgrade installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>NODEA</td>
<td>Run the Enterprise Vault Configuration wizard. Choose to configure a new Enterprise Vault server with cluster group for EVSERVER1.</td>
<td>Run the Convert to Cluster wizard. Choose to create the service resources in the EVSERVER1 service group.</td>
</tr>
</tbody>
</table>
On NODEC, run the Enterprise Vault Configuration wizard and choose to add this node as a failover node for an existing clustered server. Select either service group.

**Note:** When you bring the service groups online on NODEA and NODEB, Cluster Explorer may falsely indicate a problem with the GenericService resources (their icons in the left pane may have question marks). This is because VCS assumes that each resource is simultaneously online on two nodes. You can ignore this situation.

### N+1 configuration option 2

The second option involves configuring both EVSERVER1 and EVSERVER2 to run on any of three nodes. This has the advantage that if NODEB fails, the server moves to NODEC. NODEB can then be brought back online and act as a failover server for EVSERVER1 and EVSERVER2.
To set up this N+1 configuration

1. Mount the volumes on the system where you will configure the Enterprise Vault service group. For detailed instructions, see “Managing disk groups and volumes” on page 202.

2. With the Enterprise Vault Cluster Setup wizard, create a service group for EVSERVER1 that contains nodes NODEA, NODEB, and NODEC.

3. With the Enterprise Vault Cluster Setup wizard, create a service group for EVSERVER2 that contains nodes NODEA, NODEB, and NODEC.

4. Take the following actions on NODEA and NODEB, depending on whether you are performing a first-time installation of Enterprise Vault or upgrading an existing installation:

<table>
<thead>
<tr>
<th>Node</th>
<th>New installation</th>
<th>Upgrade installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>NODEA</td>
<td>Run the Enterprise Vault Configuration wizard. Choose to configure a new Enterprise Vault server with cluster group for EVSERVER1.</td>
<td>Run the Convert to Cluster wizard. Choose to create the service resources in the EVSERVER1 service group.</td>
</tr>
<tr>
<td>NODEB</td>
<td>Run the Enterprise Vault Configuration wizard. Choose to configure a new Enterprise Vault server with cluster group for EVSERVER2.</td>
<td>Run the Convert to Cluster wizard. Choose to create the service resources in the EVSERVER2 service group.</td>
</tr>
</tbody>
</table>

5. On NODEC, run the Enterprise Vault Configuration wizard and choose to add this node as a failover node for an existing clustered server. Select either service group.

Notice that the only difference in configuration between this option and option 1 is that, when you create the service groups, you must select all the nodes rather than a subset of the nodes.

You can take a similar approach if you require your system to have more than one spare server (N+2, N+3, N+4, and so on). In each case, you must configure a node for each Enterprise Vault server and then add the spare nodes as failover nodes.

Disallowing two Enterprise Vault servers on the same node

You cannot run multiple Enterprise Vault service groups on the same node in a cluster. When configuring the cluster in an N+x configuration, you can stop this from happening by setting the Limits and Prerequisites attributes for every node, as described below.
Running the Enterprise Vault Configuration wizard

Setting up an N+1 configuration

For more information on these steps, see the VERITAS Cluster Server Administrator’s Guide.

To prevent two Enterprise Vault servers from running on the same node

1. Use VERITAS Cluster Manager to log on to the cluster.
2. Click anywhere in the Cluster Monitor panel to open Cluster Explorer.
3. For each node in the cluster, perform the following steps:
   a. In the configuration tree at the left, click the node whose attributes you want to edit.
   b. In the View panel, click the Properties tab.
   c. Click Show all attributes to open the Attributes View dialog box.
   d. Find the Limits attribute.
   e. Click the icon at the right of the row.
   f. In the Edit Attribute dialog box, add a key called EnterpriseVault and give it a value of 1.
   g. Click OK to close the dialog box and return to the Attributes View dialog box.
   h. Repeat step e through step g for the Prerequisites attribute on each Enterprise Vault service group.

When both the Limits and Prerequisites attributes have a key called EnterpriseVault with a value of 1, two Enterprise Vault servers cannot run on the same node.
Implementing a VSFW HA-VVR disaster recovery solution

This chapter describes how to install and configure VSFW HA-VVR with Enterprise Vault. The steps are similar to those documented in the VERITAS Storage Foundation and High Availability Solutions 4.3 Solutions Guide.

About the VSFW HA-VVR disaster recovery solution

In this scenario, there is a source host on the primary site and a destination host on the secondary site. The application data is stored on the primary site and replicated to the secondary site by using the VERITAS Volume Replicator (VVR). The primary site provides data and services during normal operation. If a disaster occurs on the primary site and its data is destroyed, a secondary host can take over the role of the primary host to make the data accessible. The application can be restarted on that host.

The figure below shows a VSFW HA-VVR configuration. This example has one disk group on each site for the application. Note that a VVR replicator log is
Implementing a VSFW HA-VVR disaster recovery solution

About the VSFW HA-VVR disaster recovery solution

needed on each site. If there are multiple disk groups, an additional replicator log is required for each one.

Installing and configuring VSFW HA-VVR

To install and configure VSFW HA-VVR, complete the following tasks:

1. Set up the cluster on the primary site.
2. Set up the cluster on the secondary site.
3. Add the VVR components for replication.
4. Add the Global Cluster Option (GCO) components for wide-area recovery.

The following sections describe these tasks in detail.

Setting up the cluster on the primary site

Complete the following steps to set up the cluster on the primary site. Except where noted, you can obtain more information on how to perform these steps from the chapter “Implementing a VSFW HA-VVR Disaster Recovery Solution” in the VERITAS Storage Foundation and High Availability Solutions 4.3 Solutions Guide.

To set up the cluster on the primary site

1. Install VSFW HA 4.3 on each node that is to be a part of the cluster on the primary site. There are several stages to this process:
Implementing a VSFW HA-VVR disaster recovery solution

About the VSFW HA-VVR disaster recovery solution

Review the product installation requirements, disk space requirements, and requirements for VSFW HA.

Install Windows and configure the network settings.

Install VSFW HA on the primary site. Be sure to select the VVR and GCO options during the installation.

Using the VVR Security Service Configuration wizard, configure the VERITAS Volume Replicator Security Service (VxSAS).

Upgrade VSFW HA 4.3 to 4.3 MP1. For detailed instructions, see the VERITAS Storage Foundation and High Availability Solutions 4.3 Maintenance Pack (MP) 1 Release Notes.

Configure the cluster by running the VCS Configuration wizard.

Install Enterprise Vault as described in Section 1, “Installing, configuring, and upgrading Enterprise Vault”.

Configure the disk group and volumes. You must create shared volumes to store the following:

- Indexing service data
- Shopping service data
- Vault store partitions
- PST holding folders
- EMC Centera staging areas

We also recommend that you create separate volumes to store the MSMQ and registry replication data.

Configure the VCS service group at the primary site.

See Chapter 18, “Configuring the service group” and Chapter 19, “Running the Enterprise Vault Configuration wizard”.

Verify the cluster configuration, and test the failover capability.

Setting up the cluster on the secondary site

The process of setting up a cluster on the secondary site is similar to that on the primary site. Except where noted, you can obtain more information on how to perform these steps from the chapter “Implementing a VSFW HA-VVR Disaster Recovery Solution” in the VERITAS Storage Foundation and High Availability Solutions 4.3 Solutions Guide.

To set up the cluster on the secondary site

Create a parallel environment on the secondary site.
2 Upgrade VSFW HA 4.3 to VSFW HA 4.3 MP1. For detailed instructions, see the VERITAS Storage Foundation and High Availability Solutions 4.3 Maintains Pack (MP) 1 Release Notes.

3 Configure the cluster by running the VCS Configuration wizard.

4 Install Enterprise Vault as described in the Installing and Configuring Enterprise Vault manual.

5 Configure the disk groups and volumes on the secondary site. The disk group and volume setup on the secondary site must be identical to that on the primary site. The disks, disk groups, and volumes must be the same sizes, have the same names, and must be of the same type.

6 Configure the VCS service group at the secondary site, taking care to specify the same service group name that you specified on the primary site.

7 Verify the cluster configuration, and test the failover capability.

Adding the VVR components for replication

This section provides information on configuring the VVR components for replication. You can obtain more information on how to perform these steps from the chapter “Implementing a VSFW HA-VVR Disaster Recovery Solution” in the VERITAS Storage Foundation and High Availability Solutions 4.3 Solutions Guide.

To add the VVR components for replication

1 Create a replicator log volume at each site.

2 Set up the replicated data sets for VVR on the hosts for the primary and secondary sites. Note that the Setup Replicated Data Set wizard lets you configure replicated data sets for both sites.

3 Create the VVR RVG service group. You must run the Volume Replicator Agent Configuration wizard from the system that contains the application service group.

Adding the GCO components for wide-area recovery

You require the Global Cluster Option (GCO) components to manage global clustering for wide-area disaster recovery. For information on how to perform the steps below, see the chapter “Implementing a VSFW HA-VVR Disaster Recovery Solution” of the VERITAS Storage Foundation and High Availability Solutions 4.3 Solutions Guide.
To add the GCO components for wide-area recovery

1. Ensure that your environment meets the requirements for global cluster operations.
2. Link clusters by adding a remote cluster.
3. Convert the local service group to a global group.
4. Perform additional global cluster administration tasks.
Implementing a VSFW HA-VVR disaster recovery solution

About the VSFW HA-VVR disaster recovery solution
Troubleshooting clustering

This chapter lists the error messages and describes the problem associated with the agent.

VCS logging

VCS generates two error message logs: the engine logs and the agent logs. Log file names are appended by letters, where A indicates the first log file, B the second, C the third, and so on; for example, agent_A.txt.

The agent log is located at %VCS_HOME%\log (typically c:\Program Files\VERITAS\cluster server\log). The format of agent log messages is as follows:

<Timestamp> <Mnemonic> <Severity> <Message ID> <Message Text>

where:

Timestamp

Shows the date and time when the message was logged.

Mnemonic

Identifies the product (for example, VCS).

Severity

Indicates the severity of the error, which can be CRITICAL, ERROR, WARNING, NOTICE, or INFO. CRITICAL messages are the most severe, whereas INFO messages are the least severe.

Message ID

Is the unique numeric ID of the error message. The prefix V-16 denotes VCS.

Message Text

Is the message generated by VCS.

For example, a typical agent log message looks like this:
Enterprise Vault Cluster Setup wizard error messages

The table below describes some messages that you may see when you run the Enterprise Vault Cluster Setup wizard.

<table>
<thead>
<tr>
<th>Message</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Denied. You must have Administrator privileges to run the wizard.</td>
<td>Only users who are members of the local administrator's group can run this wizard.</td>
</tr>
<tr>
<td>VCS not running on the local machine. Either the service has not been started or it is in a stale state.</td>
<td>Verify that the VCS service has started and is running on the local machine.</td>
</tr>
<tr>
<td>MSMQ is not configured properly.</td>
<td>The wizard verifies that MSMQ is installed and configured on all the nodes. The error message is shown if MSMQ is not installed on one node or the configuration is different. To resolve the problem, verify that MSMQ has been installed and configured before proceeding with the Enterprise Vault Cluster Setup wizard.</td>
</tr>
<tr>
<td>The required resource type MSMQ is not installed on this system.</td>
<td>The wizard verifies that the MSMQ resource type is installed on the system. This resource type is installed with the 4.3 MP1.</td>
</tr>
</tbody>
</table>

Viewing the clustered message queues

You can view the clustered message queues with the Virtual MMC Viewer, which is supplied with VCS. Type the following command at a command prompt:

VCSVMCVIEW -target MSMQ
The Virtual MMC Viewer lists the clustered message queues like this:
Troubleshooting clustering

Viewing the clustered message queues
Setting up archiving

The section includes the following chapters:

- Chapter 22, “Offline archives for offline users” on page 241
- Chapter 23, “Setting up archiving from mailboxes” on page 245
- Chapter 24, “Setting up archiving from public folders” on page 259
- Chapter 25, “Setting up archiving of journaled messages” on page 267
- Chapter 26, “Setting up file system archiving” on page 273
- Chapter 27, “Configuring SharePoint archiving” on page 277
- Chapter 28, “Setting up Domino Journaling archiving” on page 301
- Chapter 29, “Setting up SMTP archiving” on page 309
Chapter 22

Offline archives for offline users

The Enterprise Vault client can maintain a personal, offline archive for offline workers. These are users with offline folder files (.ost files) on their local disks, who use Outlook to synchronize their online and offline folders.

The offline archive:

- Provides instant access to archived items, even when the user is not connected to your corporate network.
- Is in addition to, not instead of, the normal, online archive.
- Works with both mailbox folders and public folders.
- Is useful to mobile users who use laptop computers. Such users are often used to synchronizing their offline and online folders.
- May be useful in normal offices if you need to conserve bandwidth or improve performance, because the retrieval of an archived item all takes place on the local computer.

How the offline archive works

The offline archive works in one of two ways, depending on whether the user has access to Archive Explorer:

- If the user does not have access to Archive Explorer, the offline archive relies on the user having shortcuts to archived items. When the user opens a shortcut, the Enterprise Vault client opens the copy of the archived item that is in the offline archive, rather than attempting to open the version archived online in the user's archive. If the item is not available in the offline archive the client gives the user the choice of downloading the item immediately or later.
This mechanism means that the offline archive contains only items that were archived from one of the folders that the user synchronizes using Outlook synchronize; other folders are ignored.

- If the user has Archive Explorer, offline archive does not rely on shortcuts. Instead, the Enterprise Vault client downloads all items that are in the online archive.

This mechanism means that the offline archive contains a copy of everything that is in the online archive, regardless of which folder it was archived from.

**Offline archive without Archive Explorer**

When a user who does not have Archive Explorer starts Outlook in offline mode, the following happens:

1. A short while after Outlook starts, the Enterprise Vault client automatically begins checking through the offline folders, looking for:
   - Enterprise Vault shortcuts. If the corresponding items are not in the offline archive the client adds them to its download list.
   - Items that will be archived from the mailbox fairly soon. These items are copied into the offline archive so that they will already be there when the items become shortcuts in the user’s mailbox. These items have already been downloaded by the user as part of the Outlook synchronize, so the copy takes place on the users computer with no further download required.

2. When the Exchange mailbox items are archived and change to shortcuts, the next Outlook synchronize would delete the corresponding items from the local computer. Because the Enterprise Vault client has already taken copies, the items are available in the offline archive.

3. When the user opens a shortcut in an offline folder, the Enterprise Vault client automatically opens the copy that is in the offline archive. If the item is not in the offline archive, the user is given the option of downloading it immediately, or later. If the user chooses later, then item is added to the download list with a high priority.

4. At some time, a download is started to update the offline archive. This is something that can be done at a time to suit the user, such as immediately after the normal Outlook synchronize. The download to the offline archive can be automatic or can be started by the user.

If they want, users can change the order in which items are downloaded. They can also select individual items from the download list and download just those. The remaining items on the list will be downloaded when the user next does a full update of the offline archive.
Offline archive with Archive Explorer

When a user who does have access to Archive Explorer starts Outlook in offline mode, then a short while after Outlook starts, the Enterprise Vault client automatically:

1. Copies into the offline archive items that will soon be archived in the online archive. The copy takes place on the users computer with no further download required.

2. Obtains a list of all items that need to be downloaded in order to bring the offline archive up to date and downloads them. The download to the offline archive can be automatic or can be started by the user.

Users can, if they want, change the order in which items are downloaded. They can also select individual items from the download list and download just those. The remaining items on the list will be downloaded when the user next does a full update of the offline archive.

If a user has Outlook 2003 running in Exchange Cached Mode, items can be downloaded automatically at any time while there is a connection to Exchange Server. In order to do this, the user must have selected Download items automatically when online in Offline Vault Options.

Setting up offline archives

There are many settings that you can use to control the behavior of Enterprise Vault clients with offline archives. The Enterprise Vault clients automatically determine the site settings and work accordingly. However, if you need to modify any particular behavior, you can do so.

When you install Enterprise Vault, the default setting is that users can enable offline archives for themselves. If necessary, you can change this by setting a suitable value of the desktop setting OVEenabled. If you leave the setting as it is, users can create their own offline archives.

Note the following:

- Users who do not have access to Archive Explorer always have shortcuts created in their mailboxes, regardless of any other setting. Users who do have Archive Explorer do not rely on shortcuts for offline access, so are not forced to have shortcuts created in their mailboxes.

- If users do not have access to Archive Explorer then they have no means of searching the offline archive. Such users must rely on Enterprise Vault shortcuts in order to access the offline archive. In this case, be careful not to have settings that automatically delete shortcuts too soon. Check your
shortcut deletion settings, which are on the **Shortcut Deletion** tab of the Site Properties dialog box.

- When a user enables an offline archive, the offline archive is initially empty. The client scans the offline folders, copying some items into the offline archive and building a list of items to download. This can take some time if the user has a large OST file.
  
  If the scan is interrupted because the user exits from Outlook, the Enterprise Vault client continues the scan when Outlook is restarted.

- Because an offline archive is stored in a personal folder for each user, there is no problem with setting up offline archives for different people on the same computer.

### Configuring clients

You can use the settings on the **Advanced** tab of the Mailbox Policy Properties dialog box to control the appearance and behavior of the Enterprise Vault client when an offline archive has been enabled. You can control:

- The amount of feedback that the Enterprise Vault client gives to the user
- Which buttons and menu options are shown
- The behavior when archiving from synchronized mailbox folders
- The behavior when archiving from synchronized public folders

See the “Configuring Clients” chapter of the *Administrator’s Guide* for more information about the individual settings.
Setting up archiving from mailboxes

Read this chapter to find out how to set up archiving from mailboxes. In summary, the process to set up archiving from mailboxes is as follows:

- Create a vault store and vault store partition
- Add an Exchange Organization and Exchange Server
- Add a Task Controller service
- Add an archiving task
- Review the Site settings and archiving policy settings
- Customize the content of shortcuts
- Modify the appearance of users’ desktops
- Create additional Retention Categories
- Edit the Welcome message
- Enable mailboxes
- Install the user extensions

Creating a vault store and partition

You must create a vault store and a vault store partition before enabling mailboxes for archiving. Enabling mailboxes automatically creates archives so there must be an existing vault store and partition to create them in.

Each vault store can have multiple partitions, on different storage media, if required, but only one partition is active at a time. See the Administrator help for more information on partitions.
You start the **New Vault Store** wizard from the Administration Console. To do this from the Administration Console, right-click the **Vault Store** container and, on the shortcut menu, click **New** and then **Vault Store**. Alternatively, click the **Add new Vault Store** icon on the toolbar. Follow the instructions, and click **Help** on any of the wizard screens for further information.

The name you specify for the new vault store must contain any of only the following characters:

- The letters A through Z
- Numbers 0 through 9
- Spaces

When the vault store has been created, the wizard then takes you through creating a partition.

### Adding an Exchange Organization

1. In the left pane of the Administration Console, expand **Archiving Targets**.
2. Right-click **Exchange** and, on the shortcut menu, click **New** and then **Domain**.
   - The **New Domain** wizard starts
3. Work through the wizard.

### Adding an Exchange Organizational Unit

1. In the left pane of the Administration Console, expand **Archiving Targets**.
2. Expand **Exchange**.
3. Expand the domain to which you want add an Organizational Unit.
4. Right-click **Organizational Unit** and, on the shortcut menu, click **New** and then **Organizational Unit**.
   - The **New Organizational Unit** wizard starts
5. Work through the wizard.

### Adding an Exchange Server

1. In the left pane of the Administration Console, expand **Archiving Targets**.
2. Expand the Exchange domain that you added.
3 Right-click Exchange Server and, on the shortcut menu, click New and then Exchange Server. The New Exchange Server wizard starts.
4 Work through the wizard to add the Exchange Server.

Adding a Task Controller service
1 In the left pane of the Administration Console expand the hierarchy until the Enterprise Vault Servers container is visible.
2 Expand the Enterprise Vault Servers container.
3 Expand the name of the computer to which you want to add a Task Controller service.
4 Right-click Services and, on the shortcut menu, click New and then Service. In the Add Service dialog, in the list of services, click Enterprise Vault Task Controller Service and then click Add. There is a prompt for the password to the Vault Service account.
5 Enter the password for the Vault Service account and click OK.
6 The Task Controller service is added and appears in the list of services.

Adding an archiving task
To add an archiving task
1 In the left pane of the Administration Console, expand the Vault Site hierarchy until the Enterprise Vault Servers container is visible.
2 Expand Enterprise Vault Servers.
3 Expand the name of the computer to which you want to add an archiving task.
4 Right-click Tasks and, on the shortcut menu, click New and then Archiving Task. The New Archiving Task wizard starts.
5 Work through the wizard.
Reviewing the Site archiving settings

Check the Site Settings. The following tables list the settings, which tab they appear on in the Site Properties pages, and, if applicable, the default value for the setting.

**To review the site settings**
1. In the Administration Console, right-click your Enterprise Vault Site.
2. On the shortcut menu, click **Properties**.
3. Click **Help** on any of the Site Properties screens for further information.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Tab</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Whether users can delete items from their archives</td>
<td>General</td>
<td>Users cannot delete items from their archives.</td>
</tr>
<tr>
<td>Whether to delete mailbox shortcuts automatically after a period of time</td>
<td>Shortcut Deletion</td>
<td>Shortcut deletion is enabled and the time period is set to 6 months. The same setting is used for mailbox archiving.</td>
</tr>
<tr>
<td>Whether to delete shortcuts automatically after a period of time</td>
<td>Shortcut Deletion</td>
<td>Shortcut Deletion is disabled.</td>
</tr>
</tbody>
</table>

Reviewing the mailbox policy settings

Most of the settings that used during mailbox archiving come from the mailbox policy that is being used. There is a default mailbox policy, called **DefaultExchangeMailboxPolicy**, that you can edit as required. Alternatively, you can create further policies as necessary.

**To review the default mailbox policy settings**
1. In the left pane of the Administration Console, expand the **Policies** container.
2. Expand the **Exchange** container and click **Mailbox**.
3. In the right pane, double-click **DefaultExchangeMailboxPolicy**. The properties of the policy appear.
4. Check that the settings and change them as necessary. The settings are described below.
Archiving Rules

Use the settings on the Archiving Rules tab to control whether to use size-based archiving or quota-based archiving.

### Table 23-1 Mailbox policy archiving rules

<table>
<thead>
<tr>
<th>Setting</th>
<th>Tab</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>The archiving condition – that is, whether to archive based on the</td>
<td>Archiving Rules</td>
<td>Archiving is based on the period of time since an item was modified. The time period is six months. Setting is locked.</td>
</tr>
<tr>
<td>period of time since an item was modified or based on the percentage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>of the mailbox storage limit that is released</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Age limit on archiving: the absolute age at which items can be</td>
<td>Archiving Rules</td>
<td></td>
</tr>
<tr>
<td>archived</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Whether to archive larger items before smaller items and, if so, the</td>
<td>Archiving Rules</td>
<td></td>
</tr>
<tr>
<td>minimum size of the items that are given priority</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Archiving Actions

Use the settings on the Archiving Actions tab, listed in “Mailbox actions” on page 249, to control how Enterprise Vault behaves when it archives an item.

### Table 23-2 Mailbox actions

<table>
<thead>
<tr>
<th>Setting</th>
<th>Tab</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Whether to archive unread items</td>
<td>Archiving Actions</td>
<td>Unread items are not archived. Setting is locked.</td>
</tr>
<tr>
<td>Whether to create a shortcut after archiving</td>
<td>Archiving Actions</td>
<td>Shortcut is created after archiving. Setting is locked.</td>
</tr>
<tr>
<td>Whether to delete the original items after archiving</td>
<td>Archiving Actions</td>
<td>Original item is deleted after archiving.</td>
</tr>
</tbody>
</table>
Shortcut settings

Use the settings on the **Shortcuts** tab, listed in “Shortcut settings”, to control the behavior of Enterprise Vault shortcuts.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Tab</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>How much of the message bodies to store in shortcuts</td>
<td>Shortcuts</td>
<td>Shortcuts do not show recipient information. Select <strong>Message Body</strong> to make shortcuts contain message text, but no attachments. The full messages, with attachments, are still stored in the archive.</td>
</tr>
<tr>
<td>The level of detail that is kept in a shortcut</td>
<td>Shortcuts</td>
<td>Shortcuts always contain only the <strong>From</strong> and <strong>Subject</strong> information.</td>
</tr>
<tr>
<td>What happens when a user double-clicks a shortcut to open it</td>
<td>Shortcuts</td>
<td>The original item's contents are shown, using the associated application.</td>
</tr>
<tr>
<td>Whether double-clicking a shortcut displays its properties or its contents</td>
<td>Shortcuts</td>
<td>View contents.</td>
</tr>
<tr>
<td>Whether to store recipient information (To: and Cc: details) in shortcuts</td>
<td>Shortcuts</td>
<td>Shortcuts do not show recipient information.</td>
</tr>
</tbody>
</table>

The **ShortcutText.txt** file, described for customized shortcuts, may also be used to process standard shortcuts for untitled attachments. For this reason, you may want to make a copy of this file available, as described in “Defining custom shortcut content” on page 250, even if you are using standard shortcuts.

Defining custom shortcut content

The standard Enterprise Vault shortcuts do not work well with IMAP or POP3 clients. If you have users with such clients, you can choose to use custom shortcuts that can be viewed by any client that can render HTML content, such as Outlook Express.

In a new installation of Enterprise Vault, a default shortcut contains:

- From and Subject information.
Setting up archiving from mailboxes

Defining custom shortcut content

- Recipient information: To, CC, BCC.
- A banner containing a link to the complete archived item.
- No text from the message body.
- No list of attachments or links to attachments

You can change the settings so that shortcuts contain just as much information as you require. If you have users with IMAP or POP3 clients you probably want to customize shortcuts so that they contain links to archived attachments, because this enables those users to open those attachments.

Note that the changes you can make apply to shortcuts that are generated in the future, not to shortcuts that have already been created.

To define custom shortcut content

1. Locate the supplied ShortcutText.txt file, which is in the appropriate language folder beneath the ShortcutText folder in the Enterprise Vault program folder (normally C:\Program Files\Enterprise Vault\ShortcutText).
2. Open ShortcutText.txt with Windows Notepad.
   Make any required changes to the file. See “Layout of ShortcutText.txt” for a description of the file content.
3. Save the file.
4. Copy the file to the Enterprise Vault program folder (normally C:\Program Files\Enterprise Vault).
5. Copy the file to the Enterprise Vault program folder on all other servers in the Enterprise Vault site.
6. If the Archiving or Public Folder tasks are running, restart them to pick up the changes.

To apply the new content to new shortcuts

1. Start the Administration Console and go to the Shortcut Content tab in Site Properties.
2. Select Customize and then specify which options you want. Click Help on the tab for more information.

Layout of ShortcutText.txt

ShortcutText.txt is laid out using the standard Windows .ini file format:

[Section]
Item1='value1'
Item2='value2'
You can change any of the values within the file. Remember to enclose each value in quotes. For example:

```
"IPM.Task=This task has been archived."
```

The sections within `ShortcutText.txt` are as follows:

- **[Archived text]**. The entries in this section are displayed in the banner at the top of the shortcut.
  
  The entry used for the shortcut is the one that matches the archived item's message class. For example, shortcuts to items with message class IPM.Note contain the text 'This message has been archived'.
  
  Values in this section all have a space before the final quote — this separates the text from the link text.

- **[Link]**. The entry in this section specifies the text in the banner that is a link to the archived item.

- **[Attachment table]**. The `Title` entry in this section specifies the text immediately before the list of attachments.
  
  The `DefaultItemTitle` entry is used to label any attachments that have no title of their own.

The figure below shows how the definitions in these sections affect a shortcut.

**Figure 23-1** Structure of a shortcut
Controlling the appearance of desktops

You can selectively remove Enterprise Vault functionality from users' desktops. You can hide menu options, buttons, and property sheets for all the following:

- Search archives
- Manual archive
- Restore from archive using a shortcut
- Cancel archiving
- Delete from archive
- Enterprise Vault properties for Outlook folders
- Enterprise Vault properties for messages
- Enterprise Vault properties for mailboxes

Additionally, you can control the appearance of the client for those users who work with offline archives.

To modify the appearance of desktops, you create can edit the settings on the Advanced property tab of the appropriate Exchange Mailbox Policy. See the Administrator’s Guide for more details.

The changes are reversible at any time.

Creating Retention Categories

You may have decided during planning that you wanted more Retention Categories than the ones predefined in Enterprise Vault. If this is the case, you must create your own Retention Categories. Alternatively, you can edit the predefined Retention Categories to suit your needs.

To start the New Retention Category wizard from the Administration Console:

1. Expand the Vault Site hierarchy until Retention Categories is visible.
2. Right-click Retention Categories.
3. From the shortcut menu, select New Retention Category.

The New Retention Category wizard starts.

Follow the instructions, and click Help on any of the wizard screens for further information.
Setting up archiving from mailboxes

Editing the Welcome message

When Enterprise Vault enables a mailbox for archiving, it automatically sends a Welcome message to that mailbox. The Welcome message provides basic information for users on how to get help and what to expect. You must edit this message before it is sent to reflect how you have set up Enterprise Vault.

During the installation, the Welcome message is placed in a folder beneath the Enterprise Vault Program folder:

Enterprise Vault\Languages\Mailbox Messages\<lang>

where <lang> indicates the language used.

The Welcome message is in a file called EnableMailboxMessage.msg.

To set up the PST migration message:

1. Decide which language version of EnableMailboxMessage.msg you want to use and locate the file.

2. Using a computer that has Microsoft Outlook installed, double-click the file EnableMailboxMessage.msg in Windows Explorer to edit the message.

3. Review the text and make any changes that you require. If necessary, include instructions to users about how to install the Enterprise Vault user extensions on their computers.

4. Save the message.

5. Copy EnableMailboxMessage.msg to the Enterprise Vault program folder ( normally C:\Program Files\Enterprise Vault ) on every Enterprise Vault server in the site.

Editing the PST migration message

When a PST file is migrated (imported) to Enterprise Vault, an explanatory message is delivered to the user’s mailbox at the end of migration. You need to select the appropriate message file, edit it as necessary, and then make it available to all the Enterprise Vault servers in the site.

During the installation the PST migration message is placed in a folder beneath the Enterprise Vault Program folder:

Enterprise Vault\Languages\Mailbox Messages\<lang>

where <lang> indicates the language used.

The PST migration message is in a file called PSTMigratedMessage.msg.
Setting up archiving from mailboxes

To set up the PST migration message:
1. Decide which language version of PSTMigratedMessage.msg you want to use and locate the file.
2. Using a computer that has Microsoft Outlook installed, double-click the file PSTMigratedMessage.msg in Windows Explorer to edit the message.
3. Review the text and make any changes that you require.
4. Save the message.
5. Copy PSTMigratedMessage.msg to the Enterprise Vault program folder (normally C:\Program Files\Enterprise Vault) on every Enterprise Vault server in the site.

Editing Archive Usage Limit messages

You can set a maximum allowed size for users’ archives on the Archive Usage Limit page of Site Properties. On the same page, you can specify if you want messages sent to users who are approaching or have reached their archive limit. For those approaching their limit, you can also define the point at which you want the message sent.

If you have selected either of the User Notification check boxes, you need to make the appropriate messages available to all the Enterprise Vault servers in the site.

During the installation the archive limit warning messages are placed in a folder beneath the Enterprise Vault Program folder:
Enterprise Vault\Languages\Mailbox Messages\<lang>
where <lang> indicates the language used.

The message files are called ApproachingArchiveQuotaLimit.msg and ArchiveQuotaLimitReached.msg.

To set up the archive limit warning messages
1. Decide which language version of the messages you want to use and locate the files, ApproachingArchiveQuotaLimit.msg and ArchiveQuotaLimitReached.msg.
2. Using a computer that has Microsoft Outlook installed, double-click the files in Windows Explorer to open the messages.
3. Review the text and make any changes that you require.
4. Save the messages.
Copy the two message files to the Enterprise Vault program folder (normally C:\Program Files\Enterprise Vault) on every Enterprise Vault server in the site.

**Starting the Task Controller service and archiving task**

The Task Controller service and archiving task that you created have not yet been started. These must be started before you can enable mailboxes. The default is for archiving tasks to start automatically when the Task Controller service starts.

1. In the left pane of the Administration Console, expand the Enterprise Vault Servers container.
2. Expand the computer to which you added the Task Controller service and then click Services.
3. In the right pane, right-click Enterprise Vault Task Controller Service and, on the shortcut menu, click Start.

**Enabling mailboxes for archiving**

If during planning you decided not to use the option to enable new mailboxes automatically, you must enable them manually.

1. In the Administration Console, click Enable Mailbox on the Tools menu or click the Enable Mailboxes for Archiving icon on the toolbar. The Enable Mailbox wizard starts.
2. Follow the instructions, and click Help on any of the wizard screens for further information.

Note that newly-enabled mailboxes take longer to process than mailboxes that have been processed before. This applies both to normal archiving and Report Mode.
Installing the User Extensions on a server

There is no requirement for you to install the Enterprise Vault User Extensions on an Enterprise Vault Server, but you may want to do so to install a language variant of the client.

See “Setting up users’ desktops” on page 93 for details of how to install the User Extensions.

Users’ tasks

If you have changed the Site Settings so that archiving is initially suspended or the default Retention Category is None, users cannot immediately start archiving items. Depending on the settings you have selected, users must turn on automatic archiving for their mailboxes and/or select a Retention Category.

These tasks, together with any others that users must perform, are described in the Getting Started topic in the online Help in Outlook.

What next?

See “Setting up users’ desktops” on page 93 for details of how to distribute the Enterprise Vault User Extensions to your users.
Setting up archiving from mailboxes

What next?
Setting up archiving from public folders

Read this chapter to find out how to set up archiving from public folders. In summary, the process of setting up archiving from public folders is as follows:

■ Add the Exchange Server computer to your organization, create a vault store, and add a Task Controller service. You created these when setting up archiving from mailboxes. See “Setting up archiving from mailboxes” on page 245.
■ Create a public folder archive.
■ Add a Public Folder task.
■ Review the journaling policy settings.
■ Create new Retention Categories, if necessary.
■ Edit the message class list, if necessary, to specify which types of document Enterprise Vault archives.
■ Add public folder Archiving Targets.
■ Edit public folder properties as required.
■ Schedule the Public Folder task.

Creating a public folder archive

To create a public folder archive

1 In the left pane of the Administration Console, expand the Archives container.
Setting up archiving from public folders

Adding a Public Folder task

To add a Public Folder task

1. In the left pane of the Administration Console, expand the Site hierarchy until the Enterprise Vault Servers container is visible.
2. Expand the Enterprise Vault Servers container.
3. Expand the name of the computer to which you want to add the Public Folder task.
4. Right-click Tasks and, on the shortcut menu, click New and then Public Folder Task.
   The New Public Folder Task wizard starts.
5. Work through the wizard.

Adding a Public Folder task

To add a Public Folder task

1. Right-click Public Folder and, on the shortcut menu, click New and then Archive.
   The New Public Folder Archive wizard starts.
2. Work through the wizard.

Reviewing the public folder policy settings

The settings that are used during public folder archiving come from the public folder policy that is being used. There is a default public folder policy, called DefaultExchangePublicFolderPolicy that you can edit as required. Alternatively, you can create further policies as necessary.

Archiving Rules

Use the settings on the Archiving Rules tab to control which items Enterprise Vault selects as being eligible for archiving.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Tab</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age limit on archiving: the minimum age at which items can be archived</td>
<td>Archiving Rules</td>
<td>Items younger than two weeks are not archived.</td>
</tr>
</tbody>
</table>
Creating Retention Categories

You may have decided during planning that you wanted more Retention Categories than the ones predefined in Enterprise Vault. If this is the case, you must create your own Retention Categories. Alternatively, you can edit the predefined Retention Categories to suit your needs.

To create a new Retention Category:

1. In the left pane of the Administration Console, expand the Vault Site hierarchy until **Retention Categories** is visible.

2. Right-click **Retention Categories** and, on the shortcut menu, click **New Retention Category**.
The **New Retention Category** wizard starts.

3 Work through the wizard.

## Editing the message class list

A Public Folder task uses the message class when deciding which items to archive.

**To view or modify the message class list:**

1. In the left pane of the Administration Console, right-click **Directory** and, on the shortcut menu, click **Properties**. The Directory properties are shown.
2. Click the **Advanced** tab.
   - The list shows those message classes that are known to Enterprise Vault. Enterprise Vault archives messages from each class that has a check mark next to its description. If a class does not have a check mark next to its description, Enterprise Vault ignores messages from that class.
   - You can modify the message class list so that automatic archiving is turned on or off as required.
   - Note that Enterprise Vault archives items whose message classes match the text listed. You can use a trailing asterisk as a wildcard. For example, if you had a message class of 'IPM*' that would include 'IPM.Appointment', 'IPM.Contact', 'IPM.Document', and so on.

## Adding public folder archiving targets

There are two ways to add public folders: manually or automatically:

- Manual (standard) method. You select the public folder and the archive that is to be used for it. The same archive is used for the folder and its subfolders.
- Automatic method. You add an Enterprise Vault **auto-enabler** that then enables folders that are immediately beneath the folder you specify. These folders and their subfolders are all enabled for archiving.

  By default, a separate archive is automatically created for each folder at this level.

  For example, if you and an auto-enabler to `\myPublic Folder\`, then new archives will be created for `\myPublic Folder\Finance` and `\myPublic Folder\Property`. No archive will be created for `\myPublic Folder\Property\Commercial` because that folder will use the same archive as its parent `\myPublic Folder\Property`.  

Alternatively, you can select an existing archive to use. If new folders are added later, they are automatically archived too.

**Manual (Standard) method**

**To add a public folder archiving target**

1. In the left pane of the Administration Console, expand the hierarchy until `Archiving Targets` is visible.
2. Expand `Archiving Targets`.
4. Expand the domain that contains the Exchange Server that hosts the folder you want to add.
5. Expand `Exchange Server`.
6. Expand the Exchange Server that has the public folder you want to add.
7. Right-click `Public Folder` and, on the shortcut menu, click `New` and then `Public Folder`. The `New Public Folder` wizard starts.
8. Work through the wizard.

**Automatic method**

**To add a public folder auto-enabler**

1. In the left pane of the Administration Console, expand the hierarchy until `Archiving Targets` is visible.
2. Expand `Archiving Targets`.
4. Expand the domain that contains the Exchange Server that hosts the folder you want to add.
5. Expand `Exchange Server`.
6. Expand the Exchange Server that has the public folder you want to add.
7. Right-click `Public Folder` and, on the shortcut menu, click `New` and then `Public Folder Auto-Enabler`. The `New Public Folder Auto-Enabler` wizard starts.
8. Work through the wizard.
Applying archiving settings to public folders

The default public folder archiving settings are set on each public folder. These are the settings that you specified on the Public Folder Rules and Public Folder Actions pages of Site properties.

Using the Enterprise Vault user extensions for Outlook only users with Owner access to public folders can customize these settings.

To apply archiving settings to a public folder
1. View the public folder using an Outlook client that has the Enterprise Vault user extensions for Outlook installed.
2. Right-click the public folder and click Properties on the shortcut menu. The properties for the public folder are displayed.
3. Click the Enterprise Vault tab. The Enterprise Vault property page shows the folder currently has no settings.
4. Click Change. The Change Enterprise Vault Properties dialog box is displayed.
5. Select the settings you want to apply. Users will be able to apply custom settings to a public folder only if the settings on the Archiving Actions page of the public folder policy's properties are not locked.
6. Once you have finished applying settings, click OK.

Scheduling the Public Folder task

All Public Folder tasks run according to a schedule that you set. Each Public Folder task can be set to run according to:

- The Site Schedule, which is defined on the Site Schedule page of Site properties. By default all archiving tasks, including Public Folder tasks, run according to this schedule.
- Its own schedule, defined on the task's Schedule property page.

To modify the schedule for a single task
1. In the left pane of the Administration Console, expand the hierarchy until the Enterprise Vault Servers container is visible.
2. Expand the Enterprise Vault Servers container.
3 Expand the computer that is running the task whose schedule you want to modify.
4 Click Tasks.
5 In the right pane, double-click the task that you want to modify.
6 Click the Schedule tab.
7 Modify the schedule as required.

To modify the schedule for all archiving tasks
1 In the Administration Console, expand the contents of the scope (left) pane until the Vault Site is visible.
2 Right-click the Enterprise Vault Site and, on the shortcut menu, click Properties. The Site Properties appear.
3 Click the Site Schedule tab.
4 Modify the schedule as required.
Setting up archiving from public folders
Scheduling the Public Folder task
Setting up archiving of journaled messages

Read this chapter to find out how to set up archiving of journaled messages. In summary, the process of setting up archiving from a journal mailbox is as follows:

- Add the Exchange Server computer to your organization, create a vault store, and add a Task Controller service. You created these when setting up archiving from mailboxes; “Setting up archiving from mailboxes” on page 245.
- Create a journal vault store.
- Create a journal archive.
- Add permissions to the journal archive.
- Add a Journaling task.
- Review the journaling policy settings.
- Add a journal mailbox as a target.
- Start the journaling task.

Preparation

Before an Enterprise Vault Journaling task can be configured, you must have configured Exchange Server to direct all mail to one or many journal mailboxes.

Creating a journal vault store

All items from a journal mailbox need to be archived. It is good practice, for scalability reasons, to store items from journal mailboxes in a different vault.
Setting up archiving of journaled messages

Creating a journal archive

store from those used for mailbox and public folder archiving. If you have multiple journal mailboxes on an Exchange Server computer then, to gain the benefits shared storage, use the same vault store for all of them.

You must use the Administration Console to create a vault store for the Journaling task to use.

To create a journal vault store

1. In the left pane of the Administration Console, expand the hierarchy until **Vault Stores** is visible.
2. Right-click **Vault Stores** and, on the shortcut menu, click **New** and then **Vault Store**.
   The **New Vault Store** wizard starts.
3. Work through the wizard.

Creating a journal archive

To create a journal archive

1. In the left pane of the Administration Console, expand the hierarchy until **Archives** is visible.
2. Expand **Archives**.
3. Right-click **Journal** and, on the shortcut menu, click **New** and then **Archive**.
   The **New Journal Archive** wizard starts.
4. Work through the wizard. When prompted to select a vault store, choose the one that you just created.

Adding permissions to the journal archive

You must add permissions for those users who need to be allowed access to items that have been archived from the journal mailbox.

To add permissions to the journal archive

1. In the left pane of the Administration Console, expand the hierarchy until **Archives** is visible.
2. Expand **Archives**.
3. Click **Journal**.
4. In the right pane, double-click the archive whose permission list you want to modify.
Setting up archiving of journaled messages

Adding a Journaling task

The archives properties are shown.

5 Click the Permissions tab.

Users can have three different types of access to an archive:

- **Read.** Users can view and retrieve items from the archive. Those who need to search items archived from the journal mailbox, such as auditors, must have at least read access to the archive.

- **Write.** Users can archive items in the archive. The owner of the journal mailbox must have at least write access to the archive. This enables items to be archived from the journal mailbox.

- **Delete.** Users can delete items from the archive.
  
  Note that, even though you grant the delete permission here, a user cannot delete from the archive unless you also select Users can delete items from their archives on the General tab of Site Properties.

Adding a Journaling task

To add a Journaling task

1 In the left pane of the Administration Console, expand the Vault Site hierarchy until the Enterprise Vault Servers container is visible.

2 Expand the Enterprise Vault Servers container.

3 Expand the name of the computer to which you want to add a Journaling Task.

4 Right-click Tasks and, on the shortcut menu, click New and then Journaling Task.

   The New Journaling Task wizard starts.

5 Work through the wizard.

Reviewing the journaling policy settings

The settings that used during journal mailbox archiving come from the journaling policy that is being used. There is a default journaling policy, called DefaultExchangeJournalingPolicy, that you can edit as required. Alternatively, you can create further policies as necessary.

To review the default journaling policy settings

1 In the left pane of the Administration Console, expand the Policies container.
2. Expand the **Exchange** container and click **Mailbox**.

3. In the right pane, double-click **DefaultExchangeJournalingPolicy**. The properties of the policy appear.

4. Check the settings and change them as necessary. You can click each setting to see a description of what it controls.

### Adding a journal mailbox as a target

**To add a journal mailbox as a target**

1. In the left pane of the Administration Console, expand **Archiving Targets**.

2. Expand the domain that contains the Exchange Server with the journal mailbox you are adding.

3. Expand **Exchange**.

4. Expand the Exchange Server.

5. Right-click **Journal Mailbox** and, on the shortcut menu, click **New** and then **Journal Mailbox**. The **New Journal Mailbox** wizard starts.

6. Work through the wizard.

### Starting the Journaling task

**To start the Journaling task**

1. In the left pane of the Administration Console, expand the Vault Site hierarchy until the **Enterprise Vault Servers** container is visible.

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

3. Expand the name of the computer that has the Journaling task you want to start.

4. Click tasks.

5. In the right pane, right-click the task and, on the shortcut menu, click **Start**. You do not normally need to start the Journaling task in this manner: by default, the Journaling task starts automatically when the Task Controller service is started.
What next?

You can customize the journal mailbox so that items are archived to different archives and with different Retention Categories. See the Administrator’s Guide for details.
Setting up archiving of journaled messages

What next?
Setting up file system archiving

Read this chapter to find out:

■ How to install the File Placeholder service
■ How to configure the File Placeholder service

The File Placeholder service is part of File System Archiving — see the “File system archiving” chapter in the Introduction and Planning manual.

Introduction

When a file is archived, Enterprise Vault can, optionally, leave one of the following types of shortcut in its place:

■ An internet (URL) shortcut. This is a .url text file containing a hypertext link to the archived file.
■ A placeholder. This is a special file that appears exactly as the original file but, when opened, forces Enterprise Vault to fetch the archived file.

In order to create placeholder shortcuts on a particular file server you must install the File Placeholder service on that file server. Each disk on which placeholder shortcuts are created must be an NTFS device; it is not sufficient to use a non-NTFS device that appears on the network as an NTFS device.

Installing the File Placeholder service

You need to install the File Placeholder service component on each file server computer that you want Enterprise Vault to archive files from and leave placeholder shortcuts.
To install the File Placeholder service
1. Load the Enterprise Vault CD-ROM into your CD-ROM drive.
2. Open the Enterprise Vault folder.
3. Open the Server folder.
4. Double-click SETUP.EXE to start the installation.
5. Work through Setup to the Select Components to Install page
6. In the Components list select File Placeholder Service, which is at the bottom of the list.
7. Click Next to continue to the end of Setup.
8. At the end of Setup you are asked whether you want to restart your computer. Click Yes to restart your computer.

Configuring the File Placeholder service

This section describes how to configure the File Placeholder service.

If you installed the Enterprise Vault services component on the same computer as the File Placeholder service component, the File Placeholder service is automatically configured when you run the Enterprise Vault services configuration and you do not need to work through this section.

If you installed the File Placeholder service without installing the Enterprise Vault services component on the same computer then you must configure File Placeholder service as described in this section. This is typically the case when setting up archiving from file servers.

To configure File System Archiving
1. We recommend that you install a File System Archiving license, before running the Configuration Program.
2. If you did not restart the computer when prompted to do so after installing the File Placeholder service, restart it now.
3. Click Start> Programs > Enterprise Vault > File System Archiving Configuration.
   The Configuration Program wizard starts.
   The wizard asks for details of an account for Enterprise Vault services to use. This is the Vault Service account; see “The Vault Service account” on page 51.
5. Enter the details of the Vault Service account.
You must use the format `domain_name\username` when you specify the account. Alternatively, use the ... button to browse for the Vault Service account.

Enter the password for the Vault Service account and confirm it.

6 Click **Next**.

A warning message is displayed if the account you are using does not have sufficient privileges to validate the password to the Vault Service account. Click **Yes** to continue.

A message tells you that the Vault Service account has been added to the local Administrators group. Click **OK** to close the message.

A second message notifies you that the account will be given the advanced user rights, *Log On As a Service* and *Act as Part of the Operating System*, *Debug programs*, and *Replace a process-level token*. Click **OK** to close the message.

The configuration program will automatically add the Enterprise Vault Server to the list of trusted sites in Internet Explorer.

**Setting file permissions**

The Vault Service account must have Full Control access to the net shares and files that are archived. If necessary, modify the permissions appropriately.

**Editing the configuration file**

There is an optional configuration file that you can edit as necessary to tune File System Archiving. You can edit the configuration file to control the following:

- If you are archiving to an EMC Centera device, the number of threads available to process items. You are recommended to increase the default setting.
- Whether to archive from Recycle Bins.

See the *Administrator's Guide* for information on how to edit the configuration file.

**What next?**

The configuration of the computer on which you have installed File Placeholder service is complete. Using the Administration Console you must now do the following:
Setting up file system archiving

What next?

- Add the file server to the list of servers that are processed by File System Archiving.
- Create a volume policy.
- Add a new volume on the new file server. When you do this you must apply a volume policy.
- Create archive points as needed to control which folders are archived. See the administrator help for details of how to create archive points.

Tips

- Remember that a rule is applied to a file when all the criteria match. You may find that some files that you expect to be matched by a rule are not matched because, for example, the attributes are not matched exactly.
- Try not to apply too many rules in a policy. This makes it easier to apply the same policy to multiple volumes or folders. Also, by keeping it simple, you are less likely to get results you do not expect.
- When you have set up File System Archiving for a volume or folder, perform an archive run in Report Mode and then check the report to make sure that the rules are matching the files you expect.
Configuring SharePoint archiving

Read this chapter to find out:

■ How to configure your SharePoint servers for Enterprise Vault SharePoint archiving.
■ How to install the Enterprise Vault Archive Search Web Part on SharePoint servers.
■ How to configure the Enterprise Vault server for SharePoint archiving.
■ How to add the Archive Search Web Part to SharePoint pages.
■ How users can view and restore archived documents.
■ How users can view and restore archived versions of a document using the version history page.

Introduction

You can use Enterprise Vault to archive documents from servers running either Microsoft Windows SharePoint™ Services (WSS) or Microsoft SharePoint™ Portal Server 2003 (SPS 2003). At scheduled times, Enterprise Vault automatically copies documents from the SharePoint server and stores them in Enterprise Vault SharePoint archives.

Archived documents can be left on the SharePoint server or deleted, as required. Shortcuts can also be created on the SharePoint server. Deleting the original documents and creating shortcuts are configured using the SharePoint policy. If versioning is enabled for a document library, you can configure the number of versions of a document that are to be left on the SharePoint server after archiving. Users can restore older versions of a document from the archive.
An Archive Search Web Part enables users to explore the SharePoint archives that they have permission to access and search for archived documents. Once found, the documents can be viewed or restored to the SharePoint server.

**Figure 27-1** An example SharePoint archiving configuration

A single Enterprise Vault SharePoint archiving task can archive documents from multiple SharePoint virtual servers. For example, “An example SharePoint archiving configuration” shows an Enterprise Vault server archiving documents from a Windows SharePoint services server and a SharePoint Portal Server 2003.

**Prerequisite software and settings**

The instructions given in this guide apply to Windows SharePoint services on Windows Server 2003 and Microsoft SharePoint Portal Server 2003 with SQL document libraries.


The instructions in this document assume the following prerequisites are already set up:

- This software release requires the Enterprise Vault server to be running Enterprise Vault 6.0. Before installing the software for SharePoint archiving, the Enterprise Vault 6.0 server must be installed and configured, as described at the beginning of this guide.

- Your SharePoint server must be configured and running. SharePoint servers must be running Windows Server 2003 with Service Pack 1 or later. The version of Microsoft SharePoint™ Products must be at least either:
  - Microsoft Windows SharePoint services with Service Pack 1
Configuring SharePoint archiving

Installing and configuring task order

- Microsoft SharePoint Portal Server 2003 with Service Pack 1
- The SharePoint site collections and sites that you want to archive are configured in SharePoint. To be able to configure Enterprise Vault you will need to know the URLs of the SharePoint virtual servers.
- The Vault Service account must either be a member of the SharePoint administration group for the SharePoint virtual servers or have local administrator privileges on the SharePoint computer.

SharePoint security certificates

The certificate used by the SharePoint virtual server must have the same name as the virtual server. For example, if the SharePoint URL is https://sharepoint, then the name of the certificate used when issuing a certificate request must be sharepoint.

If the names do not match, Enterprise Vault will not be able to validate the SharePoint site when you try to configure it in the Administration Console.

Obtaining and installing a SharePoint license

In addition to the Enterprise Vault license, you must install a SharePoint license on each Enterprise Vault server that will be archiving SharePoint documents.

To purchase licenses, contact the following Regional Customer Care Centers at:

Americas – Amercustomercare@veritas.com
EMEA – internationallicense@veritas.com
APAC – apaccustomercare@veritas.com

Installing and configuring task order

To set up archiving of SharePoint virtual servers, perform the following tasks in the order shown:

1. Install and configure Enterprise Vault components on the SharePoint server, as described in “Configuring the SharePoint server” on page 280.
2. Install the Enterprise Vault Archive Search Web Part on the SharePoint server, as described in “Installing the Archive Search Web Part” on page 281.
3. Configure the Enterprise Vault server for SharePoint archiving, as described in “Configuring Enterprise Vault for SharePoint archiving” on page 284.
4. Next, to enable users to browse and search Enterprise Vault archives, you need to add the Archive Search Web Part to SharePoint pages. Adding the
Configuring the SharePoint server

This section describes the initial installation and configuration tasks that you need to perform on the SharePoint server computer. These must be done before you can configure SharePoint archiving on the Enterprise Vault server.

Installing and configuring the Enterprise Vault components

To install the Enterprise Vault components on your SharePoint server
1. Load the Enterprise Vault CD-ROM on your SharePoint server computer.
2. Open the Enterprise Vault folder.
3. Open the Server folder.
4. Double-click SETUP.EXE to start the installation.
5. Work through the installation wizard until you reach the Select Components to Install screen.
6. Select Microsoft SharePoint Components. If you are installing only the Enterprise Vault SharePoint components on this computer, clear the check boxes for other Enterprise Vault components.
7. Click Next.
8. Work through the remainder of the setup wizard.
9. Restart IIS.

At the end of the wizard, you are given the option of running the SharePoint configuration program immediately. Alternatively, you can run it later from Start > Programs > Enterprise Vault > SharePoint Configuration.

Running the Configuration Program

The SharePoint configuration program asks for details of the Vault Service account and configures the Enterprise Vault Admin service to log on using this account.
To configure Enterprise Vault components on the SharePoint server

1. If you did not choose to run the configuration program at the end of the installation, click **Start > Programs > Enterprise Vault > SharePoint Configuration** to start the configuration wizard.

2. Click **Next** to continue.

3. You are prompted for details of the account that Enterprise Vault services will use. Enter the details of the Vault Service account. You must use the format `domain_name\username` when you specify the account. Alternatively, use the ... button to browse for the account. Enter the password for the account and confirm it.

4. Click **Next**. A warning message is displayed if the account you are using does not have sufficient privileges to validate the password (see permissions required for this account in “Prerequisite software and settings” on page 278). Click **Yes** to continue.

5. On the last screen of the configuration wizard click **Finish** to exit the program.

Installing the Archive Search Web Part

Custom Web Parts are distributed as .cab files. You use the command line tool **Stsadm.exe** to add Web Parts from a .cab file to one or more virtual servers. For more information on adding custom Web Parts, see the following article on the Microsoft Web site:

http://www.microsoft.com/resources/documentation/wss/2/all/adminguide/en-us/stswp03.mspx

For instructions on installing the Web Part in medium or large Server Farm configurations, see “Installing Archive Search Web Part in a Web Server Farm” on page 282.

To install the Archive Search Web Part

1. On the SharePoint server open a Command Prompt window.

2. Use the **cd** command to go to the directory containing the **Stsadm.exe** tool and the Web Part CAB file; typically, `C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\60\BIN`. For example:

   cd "C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\60\BIN"

3. To install the Web Part on every virtual server on a SharePoint server, enter the following command (on one line):
Configuring the SharePoint server

stsadm.exe -o addwppack -globalinstall -force
-filename "EV_SharepointWebPartsCab.cab"

To install the Web Part on a particular virtual server, enter the command line:

stsadm.exe -o addwppack -globalinstall -url
<virt_svr_url>
-force -filename "EV_SharepointWebPartsCab.cab"

<virt_svr_url> is the URL of the SharePoint virtual server on which to install the Web Parts.

If you specify the URL of a single virtual server and the -globalinstall parameter, the Web Part will only appear in the Web Part Gallery of the virtual server that you specified. However, the assembly will be installed in the global assembly cache (GAC).

You should see the following installation message displayed

EV_sharepointwebpartscab.cab: Deploying to
http://<sharepoint_server_name>
Operation completed successfully

If an error occurs due to an obvious mistake, such as a typing error, rerun the above command; ensure that the -force switch is included in the command line. This forces the files to be installed over any existing files.

Installing Archive Search Web Part in a Web Server Farm

This section describes the Web Part installation steps if you have configured a medium or large Network Load Balancing Server Farm environment, as described in the Microsoft article in the resource kit:

http://www.microsoft.com/technet/prodtechnol/sppt/reskit/c1261881x.mspx

For the Archive Search Web Part to be installed correctly, SharePoint virtual servers must be configured to use host headers and not IP addresses.

To configure virtual servers to use host headers

In the instructions in this section, an example IP address of 172.15.10.200 is used for the SharePoint cluster. The example DNS record for the SharePoint cluster is sharepoint, which means that users enter the URL

http://sharepoint in their browsers. Replace these examples with the IP address and DNS value for your configuration.

On each Web Server in the cluster, the following steps must be repeated for each SharePoint virtual server (SharePoint web site in IIS):

1. On the Web Server computer, open Internet Information Services (IIS).
2. Open the properties dialog for the SharePoint web site and set the IP Address to All Unassigned.
3 Leave the TCP Port as configured.

4 Click Advanced and then Add.

5 In the TCP Port box, type in the required TCP Port.
   In the Host Header value box, type in a value that corresponds with the value in the DNS record for this SharePoint virtual server; this would be sharepoint in the given example.
   Leave the IP Address as All unassigned.
   Click OK.

6 In case users connect using the cluster IP address instead of the DNS name, it is advisable to repeat from step 4 and add a host header with the IP address as the host header value; 172.15.10.200 in the given example.

To install the Web Part and verify the installation
The following steps must be repeated on each Web Server in the cluster:

1 Open a Command Prompt window.

2 Use the cd command to go to the directory containing the Stsadm.exe tool and the Web Part CAB file; typically, C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\60\BIN. For example:
   cd "C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\60\BIN"

3 Enter the following command (on one line):
   stsadm.exe -o addwppack -url http://<sharepoint>
   -globalinstall -force -filename "ev_sharepointwebpartscab.cab"
   where <sharepoint> is the DNS record for the SharePoint virtual server.

After installing the Web Part on each Web Server, you can validate the installation as follows:

1 On any of the Web Servers, open a Command Prompt window, go to the directory containing the Stsadm.exe tool and run the following command:
   stsadm.exe -o enumwppacks -farm

2 A list is displayed with details of each Web Server, for example:
   SPSWEB1, ev_sharepointwebpartscab.cab, http://sharepoint/
   SPSWEB2, ev_sharepointwebpartscab.cab, http://sharepoint/
Configuring Enterprise Vault for SharePoint archiving

After you have installed and configured the Enterprise Vault components on the SharePoint server, you can configure the Enterprise Vault server as described in this section.

To ensure that Enterprise Vault can access the SharePoint servers to be archived, you must first set up Internet Explorer security as described in “Configuring the Internet Explorer security settings” on page 285.

On the Enterprise Vault server start the Enterprise Vault Administration Console and create the following objects in the order shown below:

1. A SharePoint archiving task(s). This defines the main properties of the process that archives the SharePoint virtual server, such as the archiving schedule, account the process is to use and reports to generate. A single task can support several SharePoint virtual servers. See “Creating a SharePoint task” on page 285.

2. One or more SharePoint archiving policies. A policy defines what documents are to be archived and, if versioning is enabled on the SharePoint server, how many versions are to be left in SharePoint after archiving. See “Creating a SharePoint archiving policy” on page 286.

3. If required, a new vault store to use for the SharePoint archive(s). Alternatively, an existing vault store can be used. When the archiving task runs, an archive for each SharePoint site collection is created automatically. See “Assigning a vault store” on page 288.

4. A target SharePoint virtual server to be archived (SharePoint Archiving Target in the Administration Console). When you create a target SharePoint virtual server, you can auto-enable site collection archiving and assign default values for the archiving task, vault store, policy and retention category to be used. This means that site collection objects will be automatically created under the target virtual server when the archiving task runs. See “Adding a SharePoint target virtual server” on page 288. If automatic site collection archiving is not enabled, or you want to override the default settings, you can create site collection objects and subsite objects under the target virtual server. See “Creating target site collection objects” on page 290 and “Creating archival target objects for subsites” on page 292.
Configuring the Internet Explorer security settings

To ensure that Enterprise Vault can access the SharePoint servers, the following Internet Explorer security settings must be configured on all computers running Enterprise Vault tasks and services and also on any computers running a standalone Enterprise Vault Administration Console.

To configure the Internet Explorer security settings
1. Log in as the Vault Service account.
2. Open Internet Explorer and click Tools, Internet Options.
3. Click the Security tab on the Internet Options window.
4. Select Local intranet and click Sites.
5. Click Advanced in the Local intranet dialog box.
6. Add the URL of each SharePoint virtual server that you want to archive: http://<sharepoint_server_name>
7. Click OK twice to return to the Internet Options window.
8. Click Custom Level.
9. Scroll down to the User Authentication section, and select Automatic logon only in Intranet zone.
10. Click OK.
11. Click OK to close the Internet Options window.

Creating a SharePoint task

To create a new SharePoint task
1. In the explorer pane of the Enterprise Vault Administration Console, navigate to the Enterprise Vault computer that is to host the new SharePoint task. Click the computer name to display Services and Tasks.
2. Right click Tasks and select New, SharePoint Task. This will start the New SharePoint Task wizard.
3. Work through the windows. You will be prompted to give the task a name and description.
4. The final window displays a summary of the task settings.
To customize property settings for this task, such as the logon account that runs the task, right click the SharePoint task in the right hand pane and select Properties. The following properties are displayed:
Configuring SharePoint archiving

The **General** tab shows:
- The Enterprise Vault site and computer associated with this task.
- Whether the task is to run in report mode. Report mode only shows what is ready to be archived; it does not actually archive anything. Clearing the check box means that the task will run in normal mode and archive documents.

The **Log On** tab enables you to select the user that the task runs under.

The **Targets** tab lists the sites to be archived on the SharePoint server. Targets are assigned to tasks when you create archiving target objects (see “Creating target site collection objects” on page 290).

A SharePoint task can service several targets. Alternatively, you can create multiple SharePoint archiving tasks and assign targets to each task, as required.

Creating a SharePoint archiving policy

1. In the Enterprise Vault Administration Console tree, expand the Enterprise Vault site and then click **Policies**.
2. Under **Policies**, click **SharePoint**.
3. To create a new policy, right-click in the right-hand pane and select **New, Policy** (alternatively, right-click **SharePoint** under **Policies** in the tree). The **New SharePoint Policy** wizard starts.
4. In the first window, give the policy a name and description.
5. In the next window, select the action you want Enterprise Vault to take after archiving:
   - **Leave document in SharePoint** means that the document will not be deleted from SharePoint once it is archived; users will be able to access all versions of the document both on the server and in the archive.
   - **Delete document from SharePoint once archived** means that an archived document is deleted from SharePoint and only available in the archive.
Prune to \( n \) versions of the document enables you to set the number of versions \( (n) \) of an archived document that you want left in SharePoint after archiving. Earlier versions will be available in the archive only.

6. In the next window you can set your required policy for creating shortcuts on the SharePoint server.

7. You now create a rule to select the documents that you want to process with this policy. Click New to display the Rule window.

8. Enter a Name and Description for this rule.

9. In the Rule type section, select the action to be taken with files that match the rule. This can be one of Archive, Do not archive or Delete.

10. In the Filter files using the filename section specify the selection criteria. The first box lets you include or exclude the files specified in the second box.

    In the second box enter the files you want to target. You can include wildcards in the filenames. For example:
    - * on its own means all files.
    - *.doc means all files with the extension .doc.
    - Separate multiple filenames with a comma.

    In addition to selection by filename, you can select files by size using the Filter files using file size options.

12. When you click OK, the rule is added to the list of rules. One or more rules can be applied when selecting files to process with this policy. Click New to add further rules or Edit to change the highlighted rule.

    During processing, the rules are applied in order from the top of the list. The first rule that matches will be applied, so you need to ensure that the required default action is last. Use Move Up and Move Down to reorder rules.

    To disable a rule, clear the check box for that rule.

    Click Next.

13. The final screen shows a summary of what the policy will do.

14. Click Finish and then Close.

Existing SharePoint policies listed in the right-hand pane can be viewed, edited or copied:

- To view or edit the properties of an existing policy, right click it and select Properties.

- To copy an existing policy and give it a different name, right click the policy and select Copy Policy.
Assigning a vault store

SharePoint archives can be held in an existing vault store that is also used for other types of archive. Alternatively, you may want to create a new vault store for the archives. If you want to use a new vault store, create the vault store and partition before you create the SharePoint Archiving Target.

Each vault store can have multiple partitions, on different storage media, if required, but only one partition is active at a time. See the Administration Console help for more information on partitions.

You start the New Vault Store wizard from the Administration Console. To do this from the Administration Console right-click the Vault Store container and, on the shortcut menu, click New and then Vault Store. Alternatively, click the Create new Vault Store icon on the toolbar. Follow the instructions, and click Help on any of the wizard screens for further information.

The name you specify for the new vault store must contain any of only the following characters:

- The letters A through Z
- Numbers 0 through 9
- Spaces

When the vault store has been created, the wizard then takes you through creating a partition.

When the archiving task runs, archives are created automatically in the open vault store partition. An archive is created for each SharePoint site collection. In the Administration Console tree, you can see the archives under Archives, SharePoint. Note that documents in the top level site and all subsites of that site collection are stored in the same archive.

Access permissions on Enterprise Vault archives and archive folders are synchronized automatically with permissions on the corresponding SharePoint sites and document libraries.

You can view and customize the properties of vault stores, partitions and archives by right clicking the object in the Administration Console and selecting Properties. For information on the properties for each object, see the Administration Console online help.

Adding a SharePoint target virtual server

The SharePoint archiving target objects in the Enterprise Vault Administration Console tree (under Archiving Targets, click SharePoint) reflect the SharePoint structure: a virtual server object points to the SharePoint virtual server to be archived, site collection objects point to the top-level sites on the SharePoint
virtual server and site objects point to subsites. See “Archiving Targets” on page 291.

Note that, before you can configure the archiving target objects in Enterprise Vault, the virtual servers and site collections must exist in SharePoint and the Enterprise Vault components must be installed and configured on the SharePoint server. Internet Explorer security settings must also be set up as described in “Configuring the Internet Explorer security settings” on page 285.

To create a SharePoint Virtual Server object

1. Under Archiving Targets right click the SharePoint container and select New, SharePoint Virtual Server.
2. This starts a New SharePoint Virtual Server wizard. Click Next on the first screen.
3. Enter the URL for the virtual server on the SharePoint server. Click Next.
4. If you want Enterprise Vault to archive automatically all sites on this virtual server, select the Auto-enable Site Collections check box. The wizard will then take you through screens that enable you to select the task, policy, vault store and retention category to be used for all sites on this virtual server.
   - If auto-enable archiving is on, site collection objects will be added automatically under the target virtual server object the first time the archiving task runs. Subsites will also be archived using the default settings for the target site collection object, but target subsite objects will not be created automatically in the Administration Console.
   - The auto-enable option should only be used if the creation of new SharePoint site collections is controlled by an administrator.
   - If you do not want Enterprise Vault to archive some top-level sites on the virtual server, or you want to assign a different policy, retention category or task, clear the Auto-enable Site Collections check box. The wizard will then go directly to the final summary screen. You will need to create target site collection objects manually for any site collections that you do want archived. For instructions see “Creating target site collection objects” on page 290.
5. Before the virtual server is created, a summary of the object details is displayed. If they are correct, click Finish and then Close to exit the wizard.

To change default archiving settings for a virtual server

If you later decide to enable or disable automatic archiving or change default archiving settings, use the virtual server properties. To access these, right click the virtual server object in the Administration Console tree and select Properties.
To stop archiving sites on a virtual server
You can stop archiving all site collections on a virtual server by clearing the Archive this SharePoint Virtual Server check box on the virtual server properties page.

Creating target site collection objects
If Auto-enable Site Collections is selected on the target virtual server object, a target site collection object for each top level site will be created automatically when the archiving task runs.

“Archiving Targets” on page 291 illustrates the relationship between virtual servers and sites on the SharePoint virtual server (on the left) and associated Archiving Target objects in the Enterprise Vault Administration Console (on the right).

In the example shown, Site Collection C is not being archived, so only Site Collection D on SharePoint Virtual Server B has a target site collection object in Enterprise Vault.

In this example, automatic archiving of site collections is not enabled on the SharePoint Virtual Server B target object.
If you only want to archive some site collections, clear the **Auto-enable Site Collections** check box on the target virtual server object and create the required target site collection objects manually.

To create a target site collection object manually

1. Under **Archiving Targets, SharePoint**, right click the target virtual server object and select **New, SharePoint Site Collection**.
2. This starts a **New SharePoint Site Collection** wizard. Click **Next** on the first screen.
3. Enter the URL for the top level site in the site collection, for example: http://sps2003/sites/marketing
   Note that the default site collection in SharePoint may have the same URL as the virtual server.
4. Select the required scope of archiving for this site collection; the top level web site only, the subsites only, or both. Click **Next**.
5 Highlight the vault store to be used for the SharePoint archives. A separate archive will be created automatically in the vault store for each top-level site. Click Next.

6 Select the policy and archiving task to be used to archive the site collection. Click Next.

7 Select the retention category to be applied to any files that are archived. You can use New to create a new retention category, if required. Click Next.

8 The next screen shows a summary of the details for archiving the site collection. If this is correct, click Finish.

9 A prompt confirms that the object has been created. Click Close.

Creating archiving target objects for subsites

Target site objects are not added automatically for subsites in a SharePoint site collection, even if the subsites are being archived. If there is no target site object, the subsite is archived using the archiving settings of the top-level site in the site collection.

For example, in “Archiving Targets” on page 291, there is no target object in Enterprise Vault corresponding to the subsite under Site Collection A on the SharePoint server.

You only need to create a target site object manually if you want to override the default archiving settings or exclude the site (or its subsites) from archiving. Documents archived from all sites in a site collection will be stored in the same archive.

To create archiving target objects for subsites

1 Under Archiving Targets, SharePoint, expand the target virtual server object and find the target site collection object for the subsite you want to archive.

2 Right click the site collection object and select New, SharePoint Site. This starts a New SharePoint Site wizard. Click Next on the first screen.

3 The full path of the top-level site will be displayed below the box. Enter in the box the relative path for the subsite. For example, if the top-level site path is http://sps2003/sites/marketing and the full path for the subsite is http://sps2003/sites/marketing/presentations you would just enter presentations.
4 Select the required scope of archiving for this site; this site only, the subsites only, or both. Click Next.

5 Select the policy to be used to archive the site and subsites. Click Next.

6 Select the retention category to be applied to any files that are archived. You can use New to create a new retention category, if required. Click Next.

7 The next screen shows a summary of the archiving settings for the site. If this is correct, click Finish.

8 A prompt confirms that the object has been created. Click Close.

9 Target site objects for subsites are displayed in the right hand pane of the Administration Console when you click the site collection object in the tree. They are not shown in the tree.

Note that an archiving task can be assigned to a virtual server or top-level site, but not to a subsite.

Running the SharePoint archiving task

You can start an immediate archive run for all sites serviced by an archiving task, or for a particular site collection.

Alternatively, to archive regularly all the target sites associated with a task, you can use an Enterprise Vault site schedule or you can set a separate schedule for the SharePoint task. See “Scheduling archive runs” on page 294.

To archive immediately all target sites serviced by a SharePoint task

1 In the Enterprise Vault Administration Console tree, navigate to the Enterprise Vault computer that hosts the SharePoint task. Click the computer name to display Services and Tasks.

2 Click Tasks to display the SharePoint task in the right hand pane.

3 Right click the SharePoint task and select Run Now.

4 You then select how the task is to run. In report mode, nothing is actually archived, but a report is generated showing what documents are ready to be archived. In normal mode, the documents will actually be archived and a report may or may not be generated, depending on the task report properties.

   You can view the report in the Reports folder (typically C:\Program Files\Enterprise Vault\Reports).

5 Click OK to start the archive run. A prompt tells you that the task has started. Click OK to dismiss the prompt.
Running the SharePoint archiving task

To archive a particular target site collection only
1. In the Enterprise Vault Administration Console tree, expand the Archiving Targets container and under this, the SharePoint container.
2. Expand the virtual server object to display the site collection objects.
3. To archive all sites in a site collection, right click the site collection object and select Run Now.
   To archive a subsite only:
   a. Click the site collection object to display the site object for the subsite in the right hand pane.
   b. Right click the site object and select Run Now.
4. Select report or normal mode for the task and click OK to start the archive run.

Scheduling archive runs

To use the Enterprise Vault site schedule
1. First check that the site schedule is suitable. In the Administration Console tree, right click the Enterprise Vault site container and select Properties. Click the Site Schedule tab to see the default schedule set for all archiving tasks.
2. In the Administration Console tree, expand the Enterprise Vault Servers container under the Enterprise Vault site and then expand the Enterprise Vault server that is configured to archive the SharePoint server.
3. Click Tasks in the tree.
4. In the right hand pane, right click the required SharePoint task. (SharePoint will be displayed in the Type column), and select Properties.
5. Select the Schedule tab.
6. Select the Use site setting check box.
7. Click OK.

To create a separate schedule for the SharePoint task
1. In the Administration Console tree, expand the Enterprise Vault Servers container under the Enterprise Vault site and then expand the Enterprise Vault server that is configured to archive the SharePoint server.
2. Click Tasks in the tree.
3 In the right hand pane, right click the required SharePoint task. *(SharePoint will be displayed in the Type column)*, and select Properties.

4 Select the Schedule tab.

5 Clear the Use site setting check box.

6 Set the required schedule for this task.

7 Click OK.

### Adding Web Parts and links to site pages

After the Archive Search Web Part has been installed on the SharePoint server, and the archiving task has run, you can logon to the SharePoint sites and add the Web Part to the site page, as described in “Adding the Archive Search Web Part to a site”.

To enable users to see archived versions of a document on the version history page, you also need to add the archived version history link as described in “Adding the archived version history link”.

#### Adding the Archive Search Web Part to a site

To perform this task you will need permissions to modify the SharePoint site page and add Web Parts.

1 In Internet Explorer, open the home page for the SharePoint site where you want to add the Archive Search Web Part.

2 Click Modify Shared Page in the top right of the page, and select Add Web Parts, Browse.

3 Click Virtual Server Gallery. The Archive Search should be listed in the Web Part List.

4 Drag the Archive Search Web Part to where you want it placed on the page.

5 Close the Add Web Parts panel.

6 The Archive Search Web Part will now be displayed on the page.

#### Adding the archived version history link

1 In a browser, enter the URL:

   http://spcomputername/_layouts/1033/versionsadmin.aspx

   where *spcomputername* is the name of your SharePoint server computer.

   This displays the page Enterprise Vault Archived Version History Administration.
Configuring SharePoint archiving

Viewing and restoring archived documents

2 Click **Install the archived version history link**.
   If you later wanted to remove the link, go to this web page and click **Remove the archived version history link**.

3 A progress window is displayed briefly while the link is being installed. No confirmation message is displayed when installation is complete.
   Note that you only need to perform this task once for all of the SharePoint servers.
   The archived version history link does not appear on the version history page for a document until the library containing the document is archived.

Viewing and restoring archived documents

There are several ways of accessing documents in the Enterprise Vault SharePoint archives:

- Using the **Show archived versions for this document** link on the versions history page. From this page users can access versions of a document that are in the archive and also replace the current version of a document on the SharePoint server with a version in the archive. See “Using the version history page”.

- Using the Archive Search Web Part. The Archive Search Web Part enables users to search for archived documents in the archives. From the search results page, users can view documents and copy archived documents or document versions to the SharePoint server. See “Using the Archive Search Web Part” on page 297.

- Using Archive Explorer. Outside SharePoint, users can run Archive Explorer in a browser to navigate and search SharePoint archives that they have permission to access. Archived documents can be viewed but not restored using Archive Explorer. See “Using Archive Explorer” on page 299.

   In sites and document libraries, users will only be able to see documents that they have permission to access.

Using the version history page

If versioning is enabled in SharePoint for a document library, the versions history page displays the versions of a document on the SharePoint server. After the archiving task has run for the first time, a new link, **Show archived versions for this document**, is displayed under the SharePoint versions.

To access versions of the document stored in the archive, click **Show archived versions for this document**. You can **View** or **Restore** the document using the drop down menu from the document name:
- **View** enables you to open the archived document or save it on your computer.
- **Restore** enables you to restore the document to SharePoint as the latest version.

To display only the versions on SharePoint, click **Hide archived versions for this document**.

### Using the Archive Search Web Part

You use the Archive Search Web Part to find documents stored in the Enterprise Vault SharePoint archive. The search works in the same way as the SharePoint Portal Server search.

**To search for archived documents**

1. In the first box, select the scope for your search: **This Site** or **Site Collection**.
2. In the second box, enter words to search for in the document name, subject or content and press enter. For example, entering the following would return documents with any of the words **press**, **updated** or **v5** in the name, subject or content:
   
   **press updated v5**

   The wildcard character * can be used to denote one or more characters at the end of a word. At least three characters must precede the wildcard character. For example, **new* would find an archived document called December newsletter.doc and a document with the word newer in the content.**

   Note that to be able to search for phrases in the document content, indexing must be set to **Full** on the archive. To see the indexing level, right click the site collection archive in the Enterprise Vault Administration Console, select **Properties** and then click the **Advanced** tab on the properties window.

3. The results of the search will be displayed on the Archive Search Results page.

   Use the links on the left of the Archive Search Results page to group or sort the results by **Author**, **Date** etc. When you sort the results, an arrow will indicate the sort order; click the link a second time to reverse the order.

   The **Actions** section links enable you to hide or display the preview information for each item (**Show Less/Show More**), display just the group titles or the items in the groups (**Collapse Groups/Expand Groups**) and create a complex search filter or a simple search (**Advanced Search/Simple Search**). The links toggle between these actions, so when you select **Show Less**, for example, the link changes to **Show More**.
Using the advanced search

With the advanced search, you can search on a combination of the following criteria:

- Author
- Content
- Document type
- Document name
- Created or modified date

Contains means that in matching documents the selected property must contain the word or phrase as entered in the next box.

Is exactly means that in matching documents the selected property must contain exactly the word or phrase as entered in the next box.

For example, if the author of a document is John Peter Doe:

- Searching for Author Contains John Peter will result in a match.
- Searching for Author Contains John Doe or Doe John will not result in a match.
- Searching for Author Is exactly John Peter Doe will result in a match.
- Searching for Author Is exactly John Peter will not result in a match.

If you specify two properties, you can manage the way they are applied using the And/Or operator options. If three properties are specified, the second and third always use the And operator.

If you enter values for properties and select a Modified/Created date range, the search will look for documents that satisfy both the property criteria and the date criteria.

Restoring a document using the Archive Search Web Part

On the Archive Search Results page, a Restore link is displayed below each document listed.

To restore a copy of a search result document to the SharePoint server

1. Click the Restore link below the required document.
2. The Document Restored page is displayed, showing the name and location of the restored copy.
   - The restored copy is a new file with the name of the original document and a suffix \(^{(n)}\), for example:
     - my document\(^{(1)}\).doc
If you restore the original document again from the Archive Search Results page, another new document would be created with the name, my document(2).doc.

Restoring a document from the Archive Search Results page does not replace the latest version in the document library.

On the version history page for the new document, clicking **Show archived versions for this document** will display archived versions of the restored document, my document(1).doc in our example, and archived versions of the original document, my document.doc in our example.

### Using Archive Explorer

Outside SharePoint, you can navigate and search SharePoint archives that you have permission to access using Enterprise Vault Archive Explorer. The archives are displayed in a tree structure. All documents in a site collection are stored in the same archive. In the Archive Explorer tree, subsites and document libraries are displayed as child objects of the site collection archive.

**To access a SharePoint archive using Archive Explorer**

1. Open Internet Explorer.
2. Enter the address in the following form:
   
   `http://server_name/EnterpriseVault/archiveexplorerui.asp`
   
   where `server_name/EnterpriseVault` is the path to your Enterprise Vault Web application. `server_name` should be the name of your Enterprise Vault Web server.
3. Expand the required archive in the tree on the left. When you click the document library object in the tree, the documents archived from that library will be displayed on the right.

For more information on how to use Archive Explorer, see the online help on the Archive Explorer pages.

### Internet Explorer settings for users

To avoid users having to enter credentials every time they access the SharePoint server or Enterprise Vault SharePoint archive, the Enterprise Vault server and SharePoint server can be added to local intranet sites in Internet Explorer.

**To modify the setting for an individual user**

1. On each client computer, open Internet Explorer.
2. Go to **Tools, Internet Options** and click the **Security** tab.
3 Click Trusted sites and then Sites
4 Enter the URL for the SharePoint server and click Add. For example: http://my_sharepoint_server
5 Enter the Enterprise Vault Web Access application URL and click Add. For example: http://myEnterpriseVaultServer
6 Click OK to close the Trusted Sites window.
7 Close Internet Explorer.

If a pop-up blocker is being used, it should be configured so that it does not block the Web Access application URL.

If you are using Active Directory you can employ a group policy to apply the zone changes to all domain users running Windows 2000, Windows XP and Windows Server 2003, by editing the Internet Explorer Maintenance settings within the policy.

**Configuring “all-in-one” systems**

If you have installed the Enterprise Vault server and SharePoint server on the same computer, you need to exclude the Enterprise Vault URL as a managed path in the SharePoint server, in order to be able to access the Enterprise Vault browser search page and Archive Explorer.

To exclude the Enterprise Vault URL as a managed path
1 Click Start, Administrative Tools, SharePoint Central Administration.
2 If you are configuring a SharePoint Portal Server, scroll to the section Portal Site and Virtual Server Configuration and select Configure virtual server settings from the Virtual Server List page.
   If you are configuring Windows SharePoint services, in the Virtual Server Configuration section, select Configure virtual server settings.
3 From the Virtual Server List, select the name of the virtual server that the Enterprise Vault SharePoint components are installed on; this will typically be Default Web Site.
4 Select Define managed paths under Virtual Server Management.
5 In Add a new path, enter enterprisevault in the Path box and click Check URL. The Enterprise Vault web application page should be displayed. If it is not displayed, check that you have entered the correct URL.
6 Select Excluded Path and click OK.
Setting up Domino Journaling archiving

Read this chapter to find out how to set up archiving of Domino servers. In summary, the process of setting up archiving from a Domino server is as follows:

- Add a Domino domain to the Archiving Targets
- Add the Domino server to the Domino domain
- Create a Domino Journal archive
- Create a Domino Journal policy
- Create a Domino Journaling task
- Add a Domino Journaling location to the Domino server

Preparation

Do the following

1. Check the Enterprise Vault Certification Tables document to determine which version of the Lotus Notes client to install. You can obtain this document from the following address:

2. Install the Lotus Notes client on the Enterprise Vault server that will run the Domino Journaling task. During the client installation, select the single user option.

3. Configure the Lotus Notes client for a Domino server in your organization. Before installing, it is essential to
Configuring Domino Journaling databases

Enterprise Vault will archive from any subfolder of the server’s Data directory. Each subfolder, which must already exist, must be an immediate subfolder of the Data directory, and not lower down the folder structure. Otherwise, the Domino Journaling task fails to find any databases to archive.

Enterprise Vault will archive from all Domino Journaling databases that are in the subfolder.

The normal Enterprise Vault configuration is to retain the original item until the vault store that contains the archived item has been backed up. Enterprise Vault then deletes the original item. The Domino Database Management method must not interfere with this Enterprise Vault process, which means that the Purge and Compact method (specified in the Journaling section of the server configuration document) is unsuitable, because there is the potential to lose items that have, for some reason, not been archived.

Thus, the Domino Journaling database must have its Database Management method set to one of the following in the Journaling section of the server configuration document:

- **Periodic Rollover** or **Size Rollover**. Domino automatically places rolled-over databases in the server’s data folder. In order to ensure that all items are archived from the rolled-over databases, and to remove items when the archive has been backed up, Enterprise Vault automatically moves these rolled-over databases into the journal database folder.

- **None**. This method has the side-effect that the database will keep growing and will require manual maintenance.

Do the following

- Configure Domino Journaling so that the Journaling database is in a subfolder of the server’s Data directory. If Domino Journaling is already configured, you may need to move the Journaling database and update the server configuration document.

Configuring access for Enterprise Vault

When you configure Enterprise Vault to archive a Domino journaling location you must supply the location of at least one Lotus Notes user ID. Different user IDs can be specified for the three different Enterprise Vault Domino targets although for simplicity the same user ID can be used for each of the targets.

When you configure Enterprise Vault to archive a Domino Journaling location you must supply at least one Lotus Notes ID file. Enterprise Vault requires three levels of access, to domain, server, and journaling location. You can use a
different ID file for each level or, for simplicity, a single ID file. The access levels are as follows:

- Access to the Domino domain — This is provided by the ID file of a user who is enabled for Lotus Mail and whose account is in the same domain as the server. This account must have read access to the Domino Directory.

- Access to the Domino server — This is provided by the ID file of a user who has access to the Domino server and its directories. The account used at this level must have the following:
  - Read access to the server’s Notes Address Book (NAB)
  - If the server is configured for local journaling and database rollover, the ID file also needs Manager access to the rolled-over databases and must be at least Database Administrator on the server.

By default, Enterprise Vault will use the same ID file as is used to access the domain.

- Access to the Domino Journaling location — This is provided by the ID file of a user who has Editor, Designer, or Manager access to the journaling databases, and also has the Delete documents permission. If the database is encrypted, this ID file must be the one that was used to encrypt the database.

By default, Enterprise Vault will use the same ID file as is used to access the server. If you do not specify a file for server access, Enterprise Vault will use the same ID file as is used to access the domain.

Do the following

- Create suitable ID files and place them in the Lotus Notes data folder on the Enterprise Vault server that will run the Domino Journaling task; by default this is C:\Program Files\lotus\notes\data

### Adding a Domino domain

**To add a Domino domain**

1. In the left pane of the Administration Console, expand the Archiving Targets container.

2. Right-click Domino and, on the shortcut menu, click New and then Domino Domain.
   
   The New Domino Domain wizard starts.

3. Work through the wizard.
Adding a Domino server

To add a Domino server
1  In the left pane of the Administration Console, expand the Archiving Targets container.
2  Expand Domino.
3  Right-click the Domino domain to which you want to add a server and on the shortcut menu, click New and then Domino Server.
   The New Domino Server wizard starts.
4  Work through the wizard.

Assigning a vault store

Domino Journaling archives can be held in an existing vault store that is also used for other types of archive. Alternatively, you may want to create a new vault store for the archives. If you want to use a new vault store, create the vault store and partition before you add the Domino Journaling Location.

Each vault store can have multiple partitions, on different storage media, if required, but only one partition is active at a time. See the Administration Console help for more information on partitions.

You start the New Vault Store wizard from the Administration Console. To do this from the Administration Console right-click the Vault Store container and, on the shortcut menu, click New and then Vault Store. Alternatively, click the Create new Vault Store icon on the toolbar. Follow the instructions, and click Help on any of the wizard screens for further information.

The name you specify for the new vault store must contain any of only the following characters:

- The letters A through Z
- Numbers 0 through 9
- Spaces

When the vault store has been created, the wizard then takes you through creating a partition.

You can view and customize the properties of vault stores, partitions and archives by right clicking the object in the Administration Console and selecting Properties. For information on the properties for each object, see the Administration Console online help.
Creating a Domino Journal archive

To create a Domino Journal archive
1. In the left pane of the Administration Console, expand the Site hierarchy until the Archives container is visible.
2. Expand the Archives container.
3. Right-click Domino Journal and, on the shortcut menu, click New and then Archive.
   The New Domino Journal Archive wizard starts.
4. Work through the wizard.

Adding permissions to the journal archive

You must add permissions for those users who need to be allowed access to items that have been archived from the journal mailbox.

To add permissions to the journal archive
1. In the left pane of the Administration Console, expand the hierarchy until Archives is visible.
2. Expand Archives.
3. Click Domino Journal.
4. In the right pane, double-click the archive whose permission list you want to modify.
   The archives properties are shown.
5. Click the Permissions tab.

Users can have three different types of access to an archive:
- Read. Users can view and retrieve items from the archive. Those who need to search items archived from the journal mailbox, such as auditors, must have at least read access to the archive.
- Write. This is ignored for Domino Journal archives.
- Delete. Users can delete items from the archive.
  Note that, even though you grant the delete permission here, a user cannot delete from the archive unless you also select Users can delete items from their archives on the General tab of Site Properties.
Creating a Domino Journal policy

To create a Domino Journal policy
1. In the left pane of the Administration Console, expand the Site hierarchy until the Policies container is visible.
2. Expand the Policies container.
3. Right-click Domino Journaling and, on the shortcut menu, click New and then Policy.
   The New Domino Journaling Policy wizard starts.
4. Work through the wizard.

Creating a Domino Journaling task

To add a Domino Journaling task
1. In the left pane of the Administration Console, expand the Site hierarchy until the Enterprise Vault Servers container is visible.
2. Expand the Enterprise Vault Servers container.
3. Expand the name of the sever to which you want to add the Domino Journaling task.
4. Right-click Tasks and, on the shortcut menu, click New and then Domino Journaling Task.
   The New Domino Journaling Task wizard starts.
5. Work through the wizard.

Adding a Domino Journaling location

To add a Domino Journaling location
1. In the left pane of the Administration Console, expand the Archiving Targets container.
2. Expand Domino.
3. Expand the Domino domain that contains the server to which you want to add a location.
4. Expand the Domino server to which you want to add a location and, on the shortcut menu, click New and then Domino Journaling Location.
   The New Domino Journaling Location wizard starts.
5 Work through the wizard.

**Conflict with Microsoft Office 2003**

If you have a Domino Journaling task and Microsoft Office 2003 on the same server, a steady increase in handle usage can lead to out-of-memory errors. This is a known issue with Microsoft Office 2003, described in Microsoft support article 841532.

To apply the fix

1. Determine the location of the file `Msoxmlmf.dll`. The file is in the Office shared folder, the default location for which is:
   
   C:\Program Files\Common Files\Microsoft Shared\Office11

2. Click **Start**, click **Run**.

3. Type `regsvr32.exe /u` and then the path to `Msoxmlmf.dll`. For example, if the file is in the default location:

   `regsvr32.exe "c:\program files\common files\microsoft shared\office11\msoxmlmf.dll"`

4. Click **OK**.

See the Microsoft support article if you need more information about the issue.

**Configuring clients**

A web browser on a client computer can be used to search for archived items. An HTML preview of archived items is always available from within the search results. However, whether an alternate format of the item is available depends on the software that is installed on the user's computer.

Items are sent to the client computer in one of various formats. The particular format that is used depends on settings in the WebApp.ini initialization file that is used by the Web Access application. See "Postinstallation tasks" on page 67 for details of setting up the Web Access application.

"WebApp.ini settings for Domino" shows the requirements and corresponding WebApp.ini settings.

<table>
<thead>
<tr>
<th>Table 28-1 WebApp.ini settings for Domino</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Download format</strong></td>
</tr>
<tr>
<td>---------------------</td>
</tr>
<tr>
<td>As a .HTML file that is then opened by the web browser on the client computer.</td>
</tr>
</tbody>
</table>
### Table 28-1  WebApp.ini settings for Domino

<table>
<thead>
<tr>
<th>Download format</th>
<th>Requirements</th>
<th>WebApp.ini setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>As an Enterprise Vault saveset (.DVS file) that is then unpacked by the client to create a temporary .PST file containing the item.</td>
<td>Outlook and the Enterprise Vault User Extensions must be present on the user’s computer. If this prerequisite software is not present the Browser Search <strong>View Whole Item</strong> option in the search results produces an error message. It is not possible to hide the option</td>
<td>None required.</td>
</tr>
<tr>
<td>As an Outlook (.MSG) file that the client can open immediately without creating a temporary PST file.</td>
<td>Outlook must be installed on the Enterprise Vault Storage service server. If Outlook is not present on the server the user is presented with a login screen (three times) and then a blank web page is displayed. Outlook must also be present on the user’s computer.</td>
<td><strong>MsgNotDVS=1</strong></td>
</tr>
</tbody>
</table>
Setting up SMTP archiving

Read this chapter to find out:

- How to install and configure the required components for SMTP Archiving.
- How to start and stop the SMTP Archiving process.

“SMTP architecture” on page 310 illustrates the components used in SMTP Archiving. SMTP messages are sent to a third-party SMTP server. This server relays messages addressed to a particular domain to a Microsoft SMTP Server for archiving using Enterprise Vault SMTP Archiving. You can configure SMTP Archiving to handle messages for multiple domains, if needed.

SMTP Archiving processes the messages and stores them as EML files in folders in a holding area.

Enterprise Vault File System Archiving then retrieves the EML files from the holding area and stores them in archives.

See the Introduction and Planning manual for a fuller introduction to the Enterprise Vault SMTP Archiving solution.

Users can find and retrieve archived SMTP messages using Enterprise Vault Search or Archive Explorer, which they can run from a Web browser.
To set up SMTP Archiving

1. Install and configure the Microsoft SMTP virtual server, see “Set up Microsoft SMTP Server” on page 311.

2. Install and configure SMTP Archiving on the Microsoft SMTP Server computer, as described in “Install the SMTP Archiving components” on page 311.

3. Create the required domain root folders for the holding area, as described in “Create the holding area” on page 312. This is where the SMTP Archiving process puts the EML message files for File System Archiving to archive.
4 On the Microsoft SMTP Server computer, create a suitable SMTP Archiving configuration file, as described in “Set up the SMTP Archiving configuration file” on page 313.

5 On the Enterprise Vault server, configure File System Archiving to archive from the domain root folders. See “Set up File System Archiving” on page 318 for points to note when performing this step.

Set up Microsoft SMTP Server

As Microsoft SMTP Server is included in IIS, install IIS on the Microsoft SMTP Server computer, and configure an SMTP virtual server. The following software versions are required on the Microsoft SMTP Server computer:

- Windows Server 2000 or later
- IIS 5.0 or later

For instructions on how to configure Microsoft SMTP Server, see the Microsoft documentation.

As the Microsoft SMTP Server is the destination messaging server for any SMTP messages to be archived by Enterprise Vault, configure the required domain addresses in DNS.

All messages sent to SMTP Archiving are stored; it does not perform any filtering. For this reason, only SMTP messages should be sent to this server, and not Exchange MAPI messages. We recommend that you do not install SMTP Archiving on a server that is running Microsoft Exchange.

Although you can install the Microsoft SMTP Server on the same computer as Enterprise Vault, it is more common to install it on a separate computer. You must not configure this server to relay messages to other messaging servers; it should only receive messages for archiving.

Install the SMTP Archiving components

To install the SMTP Archiving components

1 On the Microsoft SMTP Server computer, log on as a user with local administrator privileges.

2 Put the Enterprise Vault CD-ROM in the drive.

3 Open the Enterprise Vault folder, and then open the Server folder.

4 Double-click Setup.exe to start the installation.

5 In the component selection window, select the SMTP Archiving components check box. This installs the SMTP Archiving process (EvSmtpArchiveConfig.exe) and a skeleton configuration file.
(EvSmtpArchiveConfig.exe.config) in the Enterprise Vault installation folder. This folder is typically C:\Program Files\Enterprise Vault.

6 Follow the on-screen instructions to complete the installation.

Create the holding area

Decide where you want to create the holding area for the EML files. We recommend that this should be on a drive that is local to the SMTP Archiving computer. The format of the target location can be FAT or NTFS.

If you do use a network drive or share for the holding area, ensure that SMTP Archiving can write to the share:

- When you start the SMTP archiving process, you can specify an account with write access to the share. This account will be granted the right “log on as a batch process” on the local system. (See “Starting and stopping SMTP Archiving” on page 318.)
- If you do not specify an account, the default behavior is to use the account used by IIS.

Note that using a network location for the holding area may affect performance.

The disk space required for the holding area will depend on the size of the messages and the speed at which Enterprise Vault archives the files.

To set up the holding area for the EML files, you need to create a root folder for each message recipient domain that will be archived. Both the account used by SMTP Archiving to write to the holding area and the account under which File System Archiving runs (typically, the Vault Service account), must also have read and write access to the holding area folders.

SMTP Archiving automatically creates the following subfolder structure under the domain root folder that you create:

<DomainRoot>\<MailboxName>\<Year>\<Month>\<Day>\<Hour>

The configuration file, described in “Set up the SMTP Archiving configuration file” on page 313, associates the <DomainRoot> folder name with the actual domain in messages.

<MailboxName> corresponds to the recipient name in the message address.

The archives created by File System Archiving depend on where the archive points are located in the holding area folder structure. In the SMTP Archiving configuration file you can configure SMTP Archiving to create archive points automatically, or you can create them manually. If they are created automatically, a separate archive is created for each mailbox.
Set up the SMTP Archiving configuration file

You configure the following information for SMTP Archiving in a configuration file:

- The Microsoft SMTP virtual server to which SMTP Archiving binds.
- The recipient address domains that SMTP Archiving is to process and the associated path to the domain root folder in the holding area, where SMTP Archiving is to put the EML files.
- The level of indexing to be applied.

The configuration file must be located in the Enterprise Vault installation folder, typically `C:\Program Files\Enterprise Vault`. A skeleton configuration file, `EvSmtpArchiveConfig.exe.config`, is installed when you install the SMTP Archiving components.

The file is in INI format, with several sections containing key=value entries:

```bash
[SectionName]
key1=value1
key2=value2
...
[SectionName]
key3=value3
key4=value4
...
```

Edit the skeleton configuration file, or create a new one, using a plain text editor such as Notepad, and save it as a Unicode file. Section and attribute names are not case-sensitive. White space and blank lines are ignored. Comment lines must have a semi-colon in the first non-white space.

You can specify local drives or UNC hidden or regular shares in the configuration file, but for security and performance reasons, we recommend that you use local paths where possible.

For an example of a configuration file, see “Example configuration file” on page 317.

<table>
<thead>
<tr>
<th>Section</th>
<th>Entry</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td></td>
<td></td>
<td>Specify one server section per file.</td>
</tr>
</tbody>
</table>
### Table 29-1 Configuration file entries

<table>
<thead>
<tr>
<th>Section</th>
<th>Entry</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name=&lt;servername&gt;</td>
<td>Yes</td>
<td>Specifies the name of the virtual server to which SMTP Archiving binds. This is the name assigned to the server in IIS Manager, where the default server has the name “Default SMTP Virtual Server”. In general, these names are not unique, but the name of the server to use for SMTP Archiving must be unique.</td>
</tr>
<tr>
<td></td>
<td>Priority=&lt;n&gt;</td>
<td>Optional</td>
<td>Determines when the SMTP Archiving process is started in relation to other processes registered against the server. The default is 32767 (the lowest priority), as no other processes are started after SMTP Archiving.</td>
</tr>
<tr>
<td></td>
<td>NonDeliveryFolder=&lt;folderpath&gt;</td>
<td>Optional</td>
<td>Identifies a folder in which to save messages for unrecognized domains (those not specified in this file). If you do not specify this folder, messages for unrecognised domains are lost.</td>
</tr>
<tr>
<td></td>
<td>DiskFullRetryLimit=&lt;n&gt;</td>
<td>Optional</td>
<td>Specifies the number of retry attempts for a message that was not saved because the disk was full. The default value is -1, which means that there is no upper limit.</td>
</tr>
<tr>
<td></td>
<td>DefaultIndexingLevel=Brief,Medium,Full or SiteDefault</td>
<td>Optional</td>
<td>Specifies the indexing level to set for archive points on auto-enabled mailbox folders. This value is effective for any domains for which an indexing level is not explicitly. SiteDefault takes the value from the Enterprise Vault Site Settings. The default is Full.</td>
</tr>
</tbody>
</table>
Setting up SMTP archiving
Installing and configuring

You can specify multiple domain sections in the file.

### Table 29-1 Configuration file entries

<table>
<thead>
<tr>
<th>Section</th>
<th>Entry</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td></td>
<td></td>
<td>You can specify multiple domain sections in the file.</td>
</tr>
<tr>
<td></td>
<td>Name=&lt;domainname&gt;</td>
<td>Yes</td>
<td>Specifies the name of the SMTP domain. Messages addressed to this domain are sent for archiving by SMTP Archiving.</td>
</tr>
<tr>
<td></td>
<td>Path=&lt;folderpath&gt;</td>
<td>Yes</td>
<td>Specifies the path to the domain folder in the holding area. SMTP Archiving automatically creates a folder structure under this folder, as described in “Create the holding area” on page 312.</td>
</tr>
</tbody>
</table>
Setting up SMTP archiving

Installing and configuring

AutoEnableMbxFolders= False or True

Optional If set to True, forces SMTP Archiving to create automatically the appropriate mailbox subfolder under the domain root. It also adds an archive point to the mailbox folder.

If set to False (the default), you must create the mailbox folders and archive points manually. When a mailbox folder does not exist, then messages are either saved in the non-delivery folder or, if you have not specified that folder, they are lost.

**Note:** If you choose to create the folders manually, ensure that their names contain characters that are acceptable in Windows folder names. In particular, the following characters are not permitted:

- / : * ? " < > | @
- ASCII codes 0 through 31 and 127

In general, SMTP Archiving cannot handle messages with recipient addresses that contain any of these characters.

<table>
<thead>
<tr>
<th>Section</th>
<th>Entry</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AutoEnableMbxFolders= True</td>
<td>Optional</td>
<td>If set to True, forces SMTP Archiving to create automatically the appropriate mailbox subfolder under the domain root. It also adds an archive point to the mailbox folder.</td>
</tr>
<tr>
<td></td>
<td>False</td>
<td>Optional</td>
<td>If set to False (the default), you must create the mailbox folders and archive points manually. When a mailbox folder does not exist, then messages are either saved in the non-delivery folder or, if you have not specified that folder, they are lost.</td>
</tr>
<tr>
<td></td>
<td>NonDeliveryFolder= &lt;folderpath&gt;</td>
<td>Optional</td>
<td>Specifies where to save messages in the following situations: Message could not be saved in the mailbox subfolder, because of a folder access error (such as disk full or access denied). The mailbox subfolder does not exist and AutoEnableMbxFolders is not set to True.</td>
</tr>
</tbody>
</table>
Installing and configuring

Example configuration file

Here is an example configuration file that archives messages for two domains, Domain1.Vault.Local and Domain2.Vault.Local:

[Server]
Name=Default SMTP Virtual Server
NonDeliveryFolder=d:\EvMailRoot\ServerNonDelivery
DiskFullRetryLimit=15
DefaultIndexingLevel=SiteDefault

[Domain]
Name=Domain1.Vault.Local
Path=D:\EvMailRoot\Domain1
NonDeliveryFolder=d:\EvMailRoot\Domain1\MailboxNonDelivery

[Domain]
Name=Domain2.Vault.Local
Path=D:\EvMailRoot\Domain2
AutoEnableMbxFolders=True
NonDeliveryFolder=d:\EvMailRoot\Domain2\MailboxNonDelivery
IndexingLevel=Brief

The holding area folders are on a local drive (D) on the SMTP Archiving computer.

The indexing level set in the Enterprise Vault Site Properties will be used for Domain1, but Brief indexing will be used for Domain2.

For Domain2 auto-enabling is set to True, which means that SMTP Archiving will create the mailbox folders for this domain in the holding area, and create an archive point for each mailbox folder.

For Domain1 mailbox folder creation is not auto-enabled, which means that the administrator must create the mailbox folders and suitable archive points.

<table>
<thead>
<tr>
<th>Section</th>
<th>Entry</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IndexingLevel=Brief, Medium, Full</td>
<td>Optional</td>
<td>Specifies the indexing level to set for archive points on auto-enabled mailbox folders for the domain. SiteDefault takes the value from the Enterprise Vault Site Settings. The default is Full.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Entry</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IndexingLevel=Brief, Medium, Full or SiteDefault</td>
<td>Optional</td>
<td>Specifies the indexing level to set for archive points on auto-enabled mailbox folders for the domain. SiteDefault takes the value from the Enterprise Vault Site Settings. The default is Full.</td>
</tr>
</tbody>
</table>
Set up File System Archiving

On the Enterprise Vault server, set up File System Archiving as described in “Setting up file system archiving” on page 273. Note the following before you proceed:

- Ensure that the Enterprise Vault server has Enterprise Vault 6.0 or later installed.
- Add the file server that holds the SMTP Archiving domain root folder to the list of servers that are processed by File System Archiving.
- Create a volume policy to apply Retention Categories and rules to all the archived items. We recommend that you do not replace the items with placeholder shortcuts, and therefore you do not need to install the File Placeholder service on the SMTP Archiving file server.
- You can manage any archive points that SMTP Archiving automatically creates in the same way as regular archive points (for example, by using the ArchivePoints command-line utility).
- We recommend that one archive is used for each recipient. This is the default if you configure SMTP Archiving to create Archive Points automatically.
- When setting an index level for the archives, choose Full if you want to be able to search for phrases in the message content. If no value is set for DefaultIndexingLevel in the configuration file, SMTP Archiving sets the indexing level to Full for archive points on auto-enabled mailbox folders. Note that custom SMTP headers (X-headers) are not indexed (with the exception of x-KVS-MessageType, which is used by Compliance Accelerator to enable searches on Instant, Bloomberg and Exchange messages).

Starting and stopping SMTP Archiving

To start the SMTP Archiving process and assign the required configuration file

1. Log on to the SMTP Archiving computer using the account configured for the SMTP Archiving process (typically the Vault Service account).
2. Open a Command Prompt window and change to the Enterprise Vault installation folder.
3. Enter the following command:
   
   EvSsmtpArchiveConfig <config_file>
   
   where <config_file> is the name of the required configuration file. The default file is EvSsmtpArchiveConfig.exe.config.
You can register one SMTP Archiving process per virtual server instance. If you run the above command multiple times against the same virtual server, the previous settings are overwritten.

You are prompted to specify an account to be used for writing to the holding area. You can use this option to specify an account with write permissions to the holding area if it is on a network share.

To use the IIS account (LocalSystem by default), press return without entering an account.

To specify an account, enter the domain and username in the form `<domain_name>\username`. This account will be granted the right “log on as a batch process” on the holding area system.

When you specify an account, it will be used until you stop and unregister the SMTP Archiving process (EvSmtpArchiveConfig.exe), or run the process again.

A message is sent to the Enterprise Vault event log when the SMTP Archiving process starts.

To stop and unregister the SMTP Archiving process, enter the following command:

`EvSmtpArchiveConfig <config_file> /U`

### Selecting the holding area folder to use

SMTP Archiving examines the recipient email address on each message to decide which folder in the holding area to use for that message.

“Example holding area folders used” on page 320 gives an example of the holding area folders that could exist for the configuration described in the example configuration file on “Example configuration file” on page 317.

SMTP Archiving examines the message recipient address and selects the target folder as follows:

1. It checks to see if a folder exists for the recipient domain.
2. If it does not exist, the message is sent to the ServerNonDelivery folder. If this folder does not exist, an error is written to the event log and the message discarded.
3. Under the appropriate domain folder, it checks for a mailbox folder for the recipient name.
4. If this is found, the message is stored as an EML file in that folder.
5. If the folder does not exist, and auto-enabling is on, a new folder is created for the recipient name.
6 If the folder does not exist, and auto-enabling is off, the message is sent to the MailboxNonDelivery folder. If this folder does not exist, an error is written to the event log and the message discarded.

Figure 29-2 Example holding area folders used

If SMTP Archiving encounters a Disk Full error for at least one of the folders, it waits for 60 seconds and then tries to store the message again. You can set a limit on the number of times that SMTP Archiving retries by specifying the DiskFullRetryLimit value in the configuration file (see “Set up the SMTP Archiving configuration file” on page 313).
If SMTP Archiving encounters an error, messages are sent to the Enterprise Vault event log. Critical messages are also sent to the Windows Application log and to Microsoft Operations Manager (MOM), if configured.

**Accessing archived messages**

Users can access archived SMTP messages using either Archive Explorer or the Enterprise Vault Browser Search.

To view messages in their original format, users must have Outlook Express installed.
Setting up SMTP archiving

Accessing archived messages
Custom filtering and properties

This section includes the following chapters:

- Chapter 30, “Introduction to filtering” on page 325
- Chapter 31, “Configuring filtering” on page 331
- Chapter 32, “Configuring custom properties” on page 377
Introduction to filtering

Read this chapter to find out:

■ The different filtering options available with Enterprise Vault
■ A summary of the steps required to configure filtering

Filtering provides more granular control over how Enterprise Vault archiving tasks process items during an archiving run.

Caution: Set up and test filtering on a development server before implementing it on your production servers.

Enterprise Vault provides the following filtering features:

■ Selective journaling. This feature provides simple filtering of Exchange Server journaled messages. You set up a filter for the Exchange Journaling task that selects, by address, the messages to archive. Other messages are deleted.

■ Group journaling. This feature enables the Exchange Journaling task to mark selected messages, in order to reduce the scope of subsequent searches. This can be particularly useful where there is a high volume of journaled email and you want to be able to identify messages sent between particular groups of users.

■ Custom filtering. This feature provides more sophisticated filtering for Exchange Server user and journal mailbox archiving, public folder archiving and Domino server journal archiving. You create rules that select messages by matching one or more attributes, such as email addresses, subject text, message direction or the value of certain message properties. The rules also include instructions on how selected messages are to be processed. This can include assigning a particular retention category, storing in a specified archive, deleting attachments of a specified type or size and deleting or marking the message.
The following functionality is not yet available when filtering Domino server messages:

- Messages cannot be selected based on the value of custom message properties
- Message attachments cannot be removed
- Selected messages can only be archived or marked and not archived; they cannot be deleted
- Custom properties. This feature is an extension of custom filtering. It enables you to configure Enterprise Vault to index additional properties on messages selected by the custom filters. These properties may be standard properties that a default Enterprise Vault system does not index or they may be properties added to messages by a proprietary, third party application.

Custom properties also introduces the concept of content categories for grouping the settings that are to be applied to messages that match a rule. These settings can include the retention category to assign, the archive to use and the additional properties to index.

**Selective Journaling**

For detailed setup instructions, see “Configuring selective journaling” on page 331.

**To set up Selective Journaling**

1. Set up Exchange Server Journal archiving.
2. Create a rules file called `SelectiveJournal_config.dat` and place it in your Enterprise Vault directory (normally `C:\Program Files\Enterprise Vault`). This file defines the attributes to match when selecting messages to archive. You can filter on any of the following:
   - Distinguished Name
   - Exact SMTP mail address
   - Character string in the address (starts with, ends with, or contains)
3. Configure the required registry setting to call the filter `SelectiveJournal.SJFilter`.
4. If required, set additional registry key to force a hard delete of items that are not archived.
5. Restart the Exchange Journaling task.
Group Journaling

For detailed setup instructions, see “Configuring group journaling” on page 335.

To set up Group Journaling
1 Set up Exchange Server Journal archiving.
2 Create a rules file called SJGroupFilter.dat and place it in your Enterprise Vault directory (normally C:\Program Files\Enterprise Vault). This file defines the distribution lists that contain the addresses to match, the Retention Category to assign and a sample rate, if required.
3 Create the Retention Category to be assigned to matched messages.
4 Create the distribution lists and populate them with the required user addresses.
5 Configure the required registry setting to call the filter SelectiveJournal.SJGroupFilter.
6 Restart the Enterprise Vault Journaling task.

Custom filtering

For detailed setup instructions, see “Configuring filtering” on page 331.

To set up custom filtering
1 Enable custom filtering by configuring the required registry settings for each type of archiving that you want to filter. Custom filtering can be applied to the following types of archiving:
   ■ Exchange Server user mailbox archiving
   ■ Exchange Server journal mailbox archiving
   ■ Exchange Server public folder archiving
   ■ Domino server journal archiving
2 Configure the required filter rules and actions in XML ruleset files in the Custom Filter Rules folder. You can have one default set of rules applied to all types of archiving enabled for filtering, or separate rules for different archiving locations, such as Exchange Server public folders, particular user or journal mailboxes or Domino server journal locations. In addition, for Exchange Server user mailbox archiving, you can set different filtering actions for specific users by creating a separate ruleset file for each of the targeted users. All other users would have the default ruleset file applied.
A ruleset file can include one or more rules. Each rule includes a set of one or more message attribute filters for evaluating items and an action to be applied to items that match the message attribute filters.

3 When the required XML files have been set up, restart the archiving tasks that have custom filtering applied.

To use custom filtering, Microsoft .NET Framework v1.1 or later must be installed on the Enterprise Vault server. A suitable version of .NET Framework is installed automatically with Windows Server 2003.

Distributed Enterprise Vault environments

In a distributed environment, with archiving tasks on more than one computer, the registry entries must be set up on each computer that hosts archiving tasks that are to be enabled for custom filters.

Similarly, the XML configuration files must be copied to all computers that host archiving tasks that are enabled for custom filters.

If you change the registry settings or XML files, remember to propagate the changes to each of the other computers.

Custom properties

As the custom properties feature provides extended functionality to custom filtering, it is enabled with custom filtering and shares custom filtering configuration.

For detailed set up instructions, see Chapter 32, “Configuring custom properties”.

To configure custom properties

1 Enable custom filtering by configuring the required registry settings for each type of archiving that you want to filter.

2 Define the required custom properties and content categories in an XML file called custom properties.xml in the Custom Filter Rules folder in the Enterprise Vault installation folder (typically C:\Program Files\Enterprise Vault).

This file contains the following information:

- The content categories available. A content category is a group of settings that are to be applied to an archived item. This can include a list of the additional properties that are to be indexed by Enterprise Vault.
Introduction to filtering

Journal Filters with Envelope Journaling

- The custom properties available. This is where the additional properties are defined for Enterprise Vault.
- The presentation fields available. These define how external applications, such as the Enterprise Vault browser search, can access content categories and custom properties.

3 To configure Enterprise Vault to index specific custom properties on all messages, without performing any filtering, create a custom properties.xml file but no ruleset file. The custom properties.xml file must include definitions of the custom properties and a default content category. The default content category will be applied to all messages and defines which properties Enterprise Vault is to index.

   To configure Enterprise Vault to filter messages and only assign content categories to specific messages that match filter rules, you create both a custom properties.xml file and also suitable ruleset files. The custom properties and content categories are defined in custom properties.xml and the filtering rules and actions are defined in the ruleset files.

4 When the required XML files have been created, restart the archiving tasks that have custom filtering applied.

   The presence of ruleset files and content categories (in custom properties.xml) enables you to control whether Enterprise Vault implements custom property indexing or custom filtering or both. See “Controlling default settings” on page 379 for more information on the actions taken with various configuration combinations.

Journal Filters with Envelope Journaling

All methods of filtering journal mailboxes support Microsoft Exchange Server Envelope Journaling. This feature ensures that target addresses in all BCC, Undisclosed and Alternate Recipient fields are captured. For more information on Envelope Journaling, see “Envelope Journaling” on page 405.

If you have journal filtering enabled and intend enabling Envelope Journaling, we recommend that you test your existing filters and check the results before enabling Envelope Journaling on your production Exchange Server. Filters that only identify sender and recipient addresses, but do not attempt to modify the message, should continue to work as before. Addresses will be identified, even if they are classed as undisclosed recipients. Filters that attempt to modify the message will fail, as the envelope message (with the original message attached) is passed to the filters, instead of just the original message.
Before enabling Envelope Journaling, you will need to make changes to any proprietary journal filters that modify the selected message, so that the envelope message or the original message are accessed, as required. See “Custom filtering” in the Application Programmer’s Guide for more information.
Configuring filtering

Read this chapter to find out detailed instructions on the following tasks:

- How to configure selective journaling
- How to configure group journaling
- How to configure custom filtering

See “Introduction to filtering” on page 325 for an overview of these different filtering features.

Custom filtering can be extended to use custom properties. Detailed instructions on how to configure custom properties is described in Chapter 32, “Configuring custom properties”.

Caution: It is important that you test your filtering configuration on a development server, using realistic data, before implementing it on your production servers.

Configuring selective journaling

You can configure an Exchange Journaling task to call the selective journaling external filter that decides whether to archive or delete an item. To select messages, you set up filtering rules to match the To, CC, and From fields. If a message matches any of these rules it is archived, otherwise it is deleted.

All the normal, site-defined Enterprise Vault filtering rules are obeyed first; if an item is not eligible for default archiving then the external filter is not called (in the case of journaling, all items are eligible for archiving, so the external filter will always be called).

If you enable selective journaling on an Enterprise Vault server, it will be enabled for all Exchange Journaling tasks that are hosted on that computer.
To configure selective journaling, do the following on each computer that hosts an Enterprise Vault Exchange Journaling task:

1. Set up Exchange Journal archiving, as described in “Setting up archiving of journaled messages” on page 267.

2. Create a filtering rules file, as described in “Creating the selective journaling rules file” on page 332. The same filtering rules file will be used by all Exchange Journaling tasks that are hosted on the computer.

3. Add the selective journaling registry settings for the Exchange Journaling task, as described in “Adding selective journaling registry settings” on page 333.

4. Restart the Exchange Journaling task.

Creating the selective journaling rules file

To set up the filtering rules file:

1. Log on to the Exchange Journaling task computer as the Vault Service account.

2. Use Notepad to create a file called `SelectiveJournal_config.dat` in the Enterprise Vault installation folder (normally `C:\Program Files\Enterprise Vault`).

3. In the file, specify the rules that you want the filter to use to select journaled messages for archiving. See “Selective journaling filter rules” for details and examples.

4. Save the file as a Unicode file.

Selective journaling filter rules

Each line of the rules file takes the following format:

```plaintext
<keyword>:<value>
```

The table below describes the keywords and values that you can enter in the file.

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
</table>
| cont    | Archive all items that have been sent to addresses that contain the specified text. | A text string. For example: cont:flashads
|         |             | The string can be part of an SMTP address. |
Configuring filtering

Configuring selective journaling

If you want to ensure that you archive all email to an internal email recipient, specify both the Distinguished Name and SMTP address of the recipient mailbox, for example,

```
recip:/o=symantec/ou=first administrative group/cn=recipients/cn=John Doe
exact:john_doe@example.com
```

Alternatively, specify a distribution list that the recipient is a member of. For example,

```
distlist:/o=symantec/ou=first administrative group/cn=recipients/cn=allfinance
```

Table 31-1

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>distlist</td>
<td>Archive all items that have been sent to anyone who is on the specified distribution list.</td>
<td>The Distinguished Name of the distribution list. For example: distlist:/o=acme/ou=finance/cn=recipients/cn=allfinance</td>
</tr>
<tr>
<td>ends</td>
<td>Archive all items that have been sent to addresses that end with the specified text.</td>
<td>A text string. For example: ends:example.com The string can be part of an SMTP address.</td>
</tr>
<tr>
<td>exact</td>
<td>Archive all items that have been sent to the specified email address.</td>
<td>The SMTP email address of the recipient. For example: <a href="mailto:smith@example.com">smith@example.com</a></td>
</tr>
<tr>
<td>recip</td>
<td>Archive all items that have been sent to the specified recipient. The recipient can be a user account or a distribution list.</td>
<td>The Distinguished Name of the recipient user account or distribution list. For example: recip:/o=acme/ou=developer/cn=recipients/cn=smith</td>
</tr>
<tr>
<td>starts</td>
<td>Archive all items that have been sent to addresses that start with the specified text.</td>
<td>A text string. For example: starts:john The string can be part of an SMTP address.</td>
</tr>
</tbody>
</table>

If you want to ensure that you archive all email to an internal email recipient, specify both the Distinguished Name and SMTP address of the recipient mailbox, for example,

```
recip:/o=symantec/ou=first administrative group/cn=recipients/cn=John Doe
exact:john_doe@example.com
```

Alternatively, specify a distribution list that the recipient is a member of. For example,

```
distlist:/o=symantec/ou=first administrative group/cn=recipients/cn=allfinance
```

Adding selective journaling registry settings

To add the selective journaling registry settings

1. Log on to the Journaling task computer as the Vault Service account.
Configuring selective journaling

2 Run regedit and navigate to the following location:

```
HKEY_LOCAL_MACHINE
\Software
\KVS
\Enterprise Vault
\External Filtering
\Journaling
```

Add the `External Filtering` and `Journaling` keys, if they do not exist.

3 Create a new STRING value with the name `1` and set its value to `SelectiveJournal.SJFilter`.

By default, items that are not archived are sent to the Deleted Items folder in the journal mailbox.

If you want items to be deleted immediately, without going to the Deleted Items folder, add the DWORD `
HardDeleteItems`, to the following location and give it a value of `1`:

```
HKEY_LOCAL_MACHINE
\Software
\KVS
\Agents
\SelectiveJournal
```

Add the `SelectiveJournal` key, if it does not exist.

4 To enable your changes, stop and restart all Journaling tasks on the server. You need to do this whenever you make a change to the rules file or if you modify the registry values.

Managing invalid distribution lists

You can set the following registry entry to control what the Exchange Journaling task does if a distribution list is invalid.

1 Log on to the Journaling task computer as the Vault Service account.

2 Run regedit and navigate to the following location:

```
HKEY_LOCAL_MACHINE
\Software
\KVS
\Enterprise Vault
\Agents
```
3 Create a new DWORD value with the name `ActionForInvalidDL` and set its value to one of the following:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>(Default) If a distribution list is invalid, continue to process the remainder of the recipient list.</td>
</tr>
<tr>
<td>1</td>
<td>If a distribution list is invalid, stop processing the recipient list.</td>
</tr>
<tr>
<td>2</td>
<td>If a distribution list is invalid, treat this as a match and archive message.</td>
</tr>
<tr>
<td>3</td>
<td>If a distribution list is invalid, leave the message in the journaling mailbox and log an error event in the Event Log.</td>
</tr>
</tbody>
</table>

**Configuring group journaling**

Group journaling stamps a message with a specific retention category if it was sent between two identified groups. The scope of subsequent searches can be substantially reduced by including the retention category in the search criteria. You can also specify that only a sample of messages with the retention category are to be archived. The percentage is specified in the configuration (minimum of 0.1%; 1 in every 1000).

If you enable group journaling on an Enterprise Vault server, it will be enabled for all Exchange Journaling tasks that are hosted on that computer.

**To set up group journaling**

1 Set up Exchange Server Journal archiving, as described in “Setting up archiving of journaled messages” on page 267.

2 Create a rules file, as described in “Creating the group journaling rules file” on page 336. This file specifies the addresses to match, the retention category to assign and the sample size. The same rules file will be used by all Exchange Journaling tasks that are hosted on the computer.

3 If it does not exist, create the retention category to be assigned to matched messages. See the *Administrator’s Guide* for instructions on how to do this.

4 In Exchange Server, ensure that the distribution lists exist and are populated with the required users.

5 On the Enterprise Vault Exchange Journaling task computer, add the group journaling registry settings, as described in “Adding group journaling registry settings” on page 337.
6 Restart all Exchange Journaling tasks on the computer and test your configuration, as described in “Testing group journaling settings” on page 337.

Creating the group journaling rules file

To set up the filtering rules file

1 Log on to the Exchange Journaling task computer as the Vault Service account.

2 Use Notepad to create a file called $SJGroupFilter.dat in the Enterprise Vault installation folder (normally C:\Program Files\Enterprise Vault).

3 In the file, specify the rules that you want the filter to use to select journaled messages for archiving. See “Group journaling filter rules” for details and examples.

4 Save the file as a Unicode file.

Group journaling filter rules

Each line of the rules file takes the following format:

<keyword>:<value>

The table, “List of Group Journaling keywords for rules”, shows the keywords and values that you can enter in the file.

Table 31-2 List of Group Journaling keywords for rules

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>retcat</td>
<td>The retention category to assign to matching messages. The file must contain a retention category line and the retention category must exist</td>
<td>Retention category name. For example: retcat:Flagged</td>
</tr>
<tr>
<td>sample</td>
<td>The percentage sample rate of matching messages to be archived. If this line is missing, the sample rate defaults to 100%</td>
<td>Integer (without % sign). For example: sample:25</td>
</tr>
</tbody>
</table>
Table 31-2 List of Group Journaling keywords for rules

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>userset</td>
<td>Used to define the groups of user addresses to be matched. The rules file must contain two userset lines; one for each group. Each line defines a distribution list containing the addresses of group members. The specified distribution lists must not be empty.</td>
<td>Distinguished Name of the distribution list. For example: userset:/o=acme/ou=research/cn=recipients/cn=groupa userset:/o=acme/ou=research/cn=recipients/cn=groupb retcat:Flagged sample:25</td>
</tr>
</tbody>
</table>

Using the following example rules file, 25% of the messages sent by members of one distribution list to members of the other distribution list will be assigned the retention category, Flagged.

Adding group journaling registry settings

To add the group journaling registry settings

1. Log on to the Journaling task computer as the Vault Service account.
2. Run regedit and navigate to the following location:
   \HKEY_LOCAL_MACHINE\Software\KVS\Enterprise Vault\External Filtering\Journaling
   Add the External Filtering and Journaling keys, if they do not exist.
3. Create a new STRING value called \SelectiveJournal.SJGroupFilter.

Testing group journaling settings

To test the group journaling settings

1. Send a message from a user in one of the specified distribution lists to a user in the other distribution list.
2  Wait for Enterprise Vault to archive it and then search for it using the Retention Category field on the Advanced page of the Enterprise Vault browser search. (For the Advanced page, the URL should end with Search.asp?Advanced).
   The message should have the group journaling retention category assigned.

3  Now repeat the test only in reverse; send a message from a user in the second distribution list to a user in the first distribution list.
   Again, the message should have the group journaling retention category assigned.

4  Next, send a message from a user in the first distribution list to someone who is not in the second distribution list.
   The message should be archived with the retention category specified in the default Exchange journal mailbox policy.

5  Send a message from a user in the second distribution list to someone not in the first distribution list.
   Again, the message should be archived with the retention category specified in the default Exchange journal mailbox policy.

Configuring custom filtering

Selective and group journaling provide very limited filtering capabilities and are only available with Exchange Server journal mailbox archiving; the same filtering is applied to all journal mailboxes serviced by the Exchange Journaling tasks configured on the Enterprise Vault server computer. Custom filtering provides more sophisticated filtering for all types of Exchange Server archiving (user and journal mailbox and public folder) and can also be used with Domino server journal archiving. For example, you may want items with a particular subject, sender or recipients to be sent to a separate archive, or you may want messages sent within the company to be given a special retention category of Internal.

You can set up default filters that apply to all archiving tasks that are enabled for custom filtering. In addition, you can create separate custom filters for Exchange server public folder archiving, specific mailboxes (user or journal mailboxes) and specific Domino journaling locations.

If custom properties have been added to items, you may want these properties indexed for selected items. How to extend custom filtering to use the custom properties feature is described in Chapter 32, “Configuring custom properties”.
To implement custom filtering

1. Enable custom filtering for the required archiving tasks by configuring registry settings, as described in the following sections:
   - “Registry settings for Exchange Server journal filtering” on page 340
   - “Registry settings for Exchange Server user mailbox filtering” on page 342
   - “Registry settings for Exchange Server public folder filtering” on page 343
   - “ Registry settings for Domino server journal filtering” on page 344

2. Create filter rules and actions. These are held in one or more XML ruleset files, which must be placed in the folder, Enterprise Vault\Custom Filter Rules.
   The format of ruleset files and the rules and actions available are described in “General format of ruleset files” on page 349, “Rule actions” on page 352 and “Message attribute filters” on page 355.

3. Restart the archiving tasks that have custom filtering enabled.
   If custom filtering is enabled for Exchange server archiving tasks, the following message is sent to the Enterprise Vault event log when the archiving tasks start:
   ```
   EventID = 45329
   Description = External Filter 'EnterpriseVault.CustomFilter' initialising...
   ```
   The following message is sent to the Enterprise Vault event log when the Exchange server archiving tasks stop:
   ```
   EventID = 45330
   Description = External Filter 'EnterpriseVault.CustomFilter' stopped.
   ```
   If custom filtering is enabled for Domino server archiving tasks, the following message is sent to the Enterprise Vault event log when the archiving tasks start:
   ```
   EventID = 41086
   Description = External Filter 'KVS.EnterpriseVault.LotusDomino.CustomFilter' initialising...
   ```
   The following message is sent to the Enterprise Vault event log when the Domino server archiving tasks stop:
   ```
   EventID = 41087
   Description = External Filter 'KVS.EnterpriseVault.LotusDomino.CustomFilter' stopped.
   ```
Distributed Enterprise Vault environments

In a distributed environment, with archiving tasks on more than one computer, the registry entries must be set up on each computer that hosts archiving tasks that are to be enabled for custom filtering.

Similarly, the XML ruleset files must be copied to all computers that host archiving tasks that are enabled for custom filtering.

If you change the registry settings or XML files, remember to propagate the changes to each of the other computers.

Registry settings for Exchange Server journal filtering

Configuring the registry settings described in this section will enable custom filtering for all the Exchange Journaling tasks hosted on the server. By creating a named ruleset file, as described in “About custom filtering ruleset files” on page 346, you can limit filtering to particular journal mailboxes.

Caution: If the Compliance Accelerator Journaling Connector is being used to capture a required percentage of all journaled messages, do not configure a custom filter that deletes selected messages; this will compromise the accuracy of the Compliance Accelerator monitoring policy, because any deleted messages are not available for capture by the Journaling Connector.

To configure the registry settings to enable custom filtering for Exchange Journaling tasks

1. On the computer that hosts the Enterprise Vault Exchange Journaling task, log on as the Vault Service account.

2. Start Regedit.

3. Navigate to the following location: \HKEY_LOCAL_MACHINE\Software\KVS\Enterprise Vault\External Filtering\Journaling

If the External Filtering key does not exist, create it as follows:

a. Right click Enterprise Vault and select New > Key.

b. Name the key External Filtering.

Similarly, if the Journaling key does not exist, create it as follows:
Configuring filtering
Configuring custom filtering

a Right click External Filtering and select New > Key
b Name the key Journaling.

4 If the Journaling key does exist, any existing filters will be listed under it. Filter names will be an unbroken numbered sequence starting at 1.
If the Compliance Accelerator Journaling Connector is installed (KVS.Accelerator.PlugIn.Filter), it must be the last in the sequence, so you will need to rename it before creating the new custom filtering setting. For example, if the Journaling Connector is currently named 1, rename this setting as 2 and create the new custom filtering setting with the name 1.
To rename the Journaling Connector setting:
  a Right click the setting name and select Rename
  b Enter the new name, for example, 2

5 Create a new string value for the new custom filtering setting. The name of this setting must fit into the existing number sequence. If no other journaling filters exist, set the name to 1. Give it the value EnterpriseVault.CustomFilter.

6 If an entry called Override exists and has a non-zero value, set its value to 0.
If custom filtering is implemented and a rule action has marked messages as "Do not archive", setting Override to 0 (zero) prevents the Exchange Journaling task from re-examining the messages each time it processes the journal mailbox.
If you later change the rule action, you can temporarily set Override to 1 to force the Exchange Journaling task to reprocess any messages in the journal mailbox.

7 If it does not exist, create a DWORD value called MoveOnFilterFailure and set its value to 1.
This entry controls whether the Exchange Journaling task moves messages to the folder Failed External Filter when an unhandled error occurs in the external filter. This folder is automatically created when required in the journal mailbox.

8 Close Regedit.
After configuring the required XML filter rules, as described in “About custom filtering ruleset files” on page 346, you will need to restart the Journaling tasks.
Registry settings for Exchange Server user mailbox filtering

Configuring the registry settings described in this section will enable custom filtering for all the Exchange Mailbox tasks hosted on the server. By creating named ruleset files, “About custom filtering ruleset files” on page 346, you can limit filtering to particular mailboxes.

To configure the registry settings to enable custom filtering for Exchange Mailbox tasks

1. On the computer that hosts the Enterprise Vault Exchange Mailbox task, log on as the Vault Service account.
2. Start Regedit.
3. Navigate to the following location:
   ```plaintext
   HKEY_LOCAL_MACHINE\Software\KVS\Enterprise Vault\External Filtering
   ```
   If the `External Filtering` key does not exist, create it as follows:
   a. Right click `Enterprise Vault` and select `New > Key`.
   b. Name the key `External Filtering`.
4. Create a `Mailbox` key as follows:
   a. Right click `External Filtering` and select `New > Key`.
   b. Name the key `Mailbox`.
5. Create a new string value called 1 for the new custom filtering entry.
6. Right click the new entry and select `Modify`. Give it the value:
   ```plaintext
   EnterpriseVault.CustomFilter
   ```
7. Create a new DWORD called `Override` and set its value to 0 (zero).
   If custom filtering is implemented and a rule action has marked messages as "Do not archive", setting `Override` to 0 (zero) prevents the Exchange Mailbox task from re-examining the messages each time it processes the mailbox.
   If you later change the rule action, you can temporarily set the `Override` entry to 1 to force the Exchange Mailbox task to reprocess such messages.
8. If it does not exist, create a DWORD value called `MoveOnFilterFailure` and set its value to 1.
   This entry controls whether the Exchange Mailbox task moves messages to the folder `Failed External Filter` when an unhandled error occurs in
the external filter. This folder is automatically created when required in the user mailbox.

9 Close Regedit.

After configuring the required XML filter rules, as described in “About custom filtering ruleset files” on page 346, you will need to restart the Exchange Mailbox tasks.

Registry settings for Exchange Server public folder filtering

Configuring the registry settings described in this section will enable custom filtering for all the Exchange Public Folder tasks hosted on the server. You can create a public folder ruleset file to apply specific rules to public folder archiving, “About custom filtering ruleset files” on page 346. Unlike mailbox filtering, you cannot use named ruleset files to configure filtering for particular public folders.

To configure the registry settings to enable custom filtering for Exchange Public Folder tasks

1 On the computer that hosts the Enterprise Vault Exchange Public Folder task, log on as the Vault Service account.

2 Start Regedit.

3 Navigate to the following location:
   HKEY_LOCAL_MACHINE\Software\KVS\Enterprise Vault\External Filtering
   If the External Filtering key does not exist, create it as follows:
   a Right click Enterprise Vault and select New > Key.
   b Name the key External Filtering.

4 Create a PublicFolder key as follows:
   a Right click External Filtering and select New > Key.
   b Name the key PublicFolder.

5 Create a new string value called 1 for the new custom filtering entry.

6 Right click the new entry and select Modify. Give it the value:
   EnterpriseVault.CustomFilter

7 Create a new DWORD called Override and set its value to 0 (zero).
If custom filtering is implemented and a rule action has marked items as “Do not archive”, setting Override to 0 (zero) prevents the Exchange Public Folder task from re-examining the items each time it processes the public folder. If you later change the rule action, you can temporarily set the Override entry to 1 to force the Exchange Public Folder task to reprocess such items.

Close Regedit.

After configuring the required XML filter rules, as described in “About custom filtering ruleset files” on page 346, you will need to restart the Exchange Public Folder tasks.

Registry settings for Domino server journal filtering

How to configure Enterprise Vault to archive Domino journal databases is described in “Setting up Domino Journaling archiving” on page 301. Each Domino journal archiving target is configured in Enterprise Vault Administration Console as a Domino Journaling Location during the setup process. The following screen shot shows an example of a Domino journaling location configured in the Enterprise Vault Administration Console. In this example, the target Domino server is Server1 in the Domino organization, Org1, and the target journaling location, is the folder called Symantec in the Domino Data directory.

Figure 31-1 Domino journaling location in the Administration Console

Configuring the registry settings described in this section will enable custom filtering for all the Domino Journaling tasks hosted on the server. By creating a named ruleset file, as described in “About custom filtering ruleset files” on page 346, you can limit filtering to particular journaling locations.

**Note:** The Compliance Accelerator Journaling Connector does not currently support Domino server messages.
To configure the registry settings to enable custom filtering for Domino Journaling tasks

1. On the computer that hosts the Enterprise Vault Domino Journaling task, log on as the Vault Service account.

2. Start Regedit.

3. Navigate to the following location:
   HKEY_LOCAL_MACHINE \Software \KVS \Enterprise Vault \External Filtering \Lotus Journaling
   If the External Filtering key does not exist, create it as follows:
   a. Right click Enterprise Vault and select New > Key.
   b. Name the key External Filtering.
   Similarly, if the Lotus Journaling key does not exist, create it as follows:
   a. Right click External Filtering and select New > Key.
   b. Name the key Lotus Journaling.

4. If the Lotus Journaling key does exist, any existing filters will be listed under it. Filter names will be an unbroken numbered sequence starting at 1.

5. Create a new string value for the new custom filtering setting. The name of this setting must fit into the existing number sequence. If no other journaling filters exist, set the name to 1. Give it the following value

6. If an entry called Override exists and has a non-zero value, set its value to 0.
   If custom filtering is implemented and a rule action has marked messages as "Do not archive", setting Override to 0 (zero) prevents the Domino Journaling task from re-examining the messages each time it processes the Domino journaling location.
   If you later change the rule action, you can temporarily set Override to 1 to force the Domino Journaling task to reprocess any messages in the Domino journaling location.

7. Close Regedit.

After configuring the required XML filter rules, as described in "About custom filtering ruleset files", you will need to restart the Domino Journaling tasks.
About custom filtering ruleset files

You create filter rules and actions in XML ruleset files. A ruleset file can contain one or more rules for selecting items that the archiving task is processing. Each rule has an associated action, which the archiving task applies to any item that matches the rule.

All ruleset files must be available in the folder, Custom Filter Rules, in the main Enterprise Vault folder (typically C:\Program Files\Enterprise Vault) on the computer hosting the archiving tasks that are enabled for custom filtering.

After Enterprise Vault has been installed, this folder contains the following XML files:

- Example Filter Rules.xml — This provides examples of filter rules.
- ruleset schema.xdr — This contains the XML schema for validating the XML ruleset files.
- Example Custom Properties.xml — This provides example entries for the custom properties.xml file. This file is described in Chapter 32, “Configuring custom properties”.
- customproperties.xsd — This contains the XML schema for validating the custom properties XML file described in Chapter 32, “Configuring custom properties”.

When you modify a ruleset file, you must restart the associated archiving tasks to pick up the changes. In a distributed environment, you must copy the updated file to each computer with tasks enabled for custom filtering, and then restart the associated tasks on each computer.

**Caution:** It is important to set permissions on the ruleset files to prevent unauthorized editing. For increased security, you could also enable Windows file auditing on these files.

A ruleset file contains one or more rules. Each rule contains the following:

- A set of one or more attribute filters for evaluating messages or message attachments or both.

- An action to be applied to messages or attachments that match the attribute filters. Examples of actions are applying a particular retention category or storing the item in a specified archive. More than one action can be applied to matching items.
Configuring filtering

Configuring custom filtering

Setting default filtering rules for all custom filtering

If you create a ruleset file called Default Filter Rules.xml, this will be used as the default ruleset file for all custom filtering; both Exchange server and Domino server filtering.

To implement specific filtering for public folders, particular mailboxes or particular Domino journaling locations, you can create named ruleset files in addition to the default ruleset file. Each target location associated with a named ruleset file is processed according to the rules in its named ruleset file. All other custom filtering will use the rules in the default ruleset file.

If no custom filtering is to be applied other than those specified by named ruleset files, it is more efficient to omit the default ruleset file, Default Filter Rules.xml, and configure the IGNORENODEFAULT registry setting, as described in “Setting IGNORENODEFAULT registry entry” on page 379. In this way, custom filtering is only applied to target locations explicitly defined by named ruleset files.

If you want the same actions applied to all items that the archiving tasks process (that is, specific items are not selected for processing by matching attributes), you can omit ruleset files altogether and define a default content category in the file, custom properties.xml. For information on content categories and the custom properties.xml file, see Chapter 32, “Configuring custom properties”.

Setting filtering for individual Exchange Server mailboxes

To set up custom filtering for an individual Exchange Server user or journal mailbox, you need to create a separate ruleset file for each mailbox you want to filter. The name of each ruleset file must be:

mailbox_owner.xml

The mailbox owner will typically be the same as the account Display Name, but could be different if you have changed the mailbox owner name, for some reason.

For example, if you want to filter John Doe’s mailbox, and John Doe is the mailbox owner name, you would create a ruleset file called John Doe.xml. To apply filtering to a journal mailbox with the mailbox owner name Journal US1, you would create a ruleset file called Journal US1.xml. Any other mailboxes that do not have a named ruleset file and are serviced by the archiving tasks which have been enabled for custom filtering, are processed using the default ruleset file, Default Filter Rules.xml.

If archiving tasks are enabled for custom filtering, but neither the default ruleset file nor named ruleset files exist, the archiving tasks will attempt to use a default content category, as defined in custom properties.xml (these are
Configuring custom filtering

described in Chapter 32, “Configuring custom properties”). If none of the above exist, an error is logged and the archiving tasks stop.

You can configure archiving tasks to manage missing defaults gracefully using the IGNORENODEFAULT registry setting (see “Controlling default settings” on page 379 for details). This registry setting is particularly useful if you want to restrict filtering to named mailboxes only.

Tip: If custom filtering is enabled for all Exchange Server mailbox archiving and you want to apply different rules to Exchange Server user and journal mailboxes, you could create a named ruleset file for the Exchange Server journal mailbox and configure the default ruleset file for filtering all user mailboxes. This would avoid having to create a large number of named ruleset files.

Setting separate filtering rules for public folders

To set up specific filtering for Exchange Server public folders, you need to create a separate ruleset file called Public Folder Rules.xml. This will be used by all Exchange Public Folder tasks hosted on the Enterprise Vault server computer. If Public Folder Rules.xml does not exist, the default ruleset file, Default Filter Rules.xml, will be used. (If neither of these files exist, but a default content category is defined in custom properties.xml, items will be archived according to the settings in the default content category. Content categories and the file custom properties.xml are described in Chapter 32, “Configuring custom properties”).

If none of the above exist — Public Folder Rules.xml, Default Filter Rules.xml or a default content category — an error will be logged and the archiving tasks will stop, unless you have configured the IGNORENODEFAULT registry setting. See “Controlling default settings” on page 379 for details of this registry setting.

You can configure archiving tasks to manage missing defaults gracefully using the IGNORENODEFAULT registry setting.

Setting filtering for individual Domino journaling locations

To set up custom filtering for specific Domino journaling locations, you need to create a separate ruleset file for each journaling location that you want to filter. The name of each ruleset file must be:

journaling_location_name.xml

For example, if you want to filter the Domino journaling location that is shown as Symantec/* in the Administration Console, you would create a ruleset file called Symantec.xml. Any other journaling locations that are serviced by the
Configuring filtering

Configuring custom filtering

Domino archiving tasks and which have been enabled for custom filtering, are processed using the default ruleset file, Default Filter Rules.xml.

If archiving tasks are enabled for custom filtering, but neither the default ruleset file nor named ruleset files exist, the archiving tasks will attempt to use a default content category, as defined in custom properties.xml (these are described in Chapter 32, “Configuring custom properties”). If none of the above exist, an error is logged and the archiving tasks stop.

You can configure archiving tasks to manage missing defaults gracefully using the IGNOREDEFAULT registry setting (see “Controlling default settings” on page 379 for details). This registry setting is particularly useful if you want to restrict filtering to named mailboxes only.

General format of ruleset files

This section describes the required overall format of the XML ruleset files.

Ruleset files must be located in the Custom Filter Rules folder, in the main Enterprise Vault folder (typically C:\Program Files\Enterprise Vault) on the computer hosting the archiving tasks that are enabled for custom filtering.

Ruleset files have the following general format:

```xml
<?xml version='1.0' encoding='UTF-8'?>
<RULE_SET xmlns="x-schema:ruleset schema.xdr">
  <RULE [NAME='rule_name'] [ACTION='match_action']
    [ATTACHMENT_ACTION='match_action']
    [CONTENTCATEGORY='content_category']
    [RETENTION='retention_category']
    [ARCHIVEID='archiveid']>
    <message_attribute [attribute_value_operators]>
      <attribute_value>
      </attribute_value>
    </message_attribute>
    ... </message_attribute>
    ... </attachment_attributes>
  </RULE>
</RULE_SET>
```

```xml
<attachment_attributes>
  <attachment_attribute_values>
  </attachment_attribute_values>
</attachment_attributes>
```
The ruleset can contain one or more rules. Naming a rule (NAME="<rule_name>") is optional. It is advisable to include it for documentation purposes and to distinguish the rule in trace output.

Each rule contains one or more message attribute filters for evaluating messages. With Exchange server filtering, a rule may also contain attachment attribute filters for evaluating attachments to messages. Attachment filtering is not currently available with Domino server filtering.

You can use a combination of the following message attributes to select messages:

- Author
- Recipients
- Direction
- Subject text
- Named MAPI properties (Exchange server messages only)

You can use the following attachment attributes to select specific files attached to Exchange server messages:

- File name
- File size

How to write message attribute filters is described in "Message attribute filters" on page 355. How to write attachment attribute filters is described in "Attachment attribute filters" on page 366.

Matching against attribute values is case insensitive. All message attribute filters in a rule will be applied to a message, so the order of message attribute filters in a rule is not significant. A message matches a rule when it matches all the message attribute filters contained in that rule. When a message matches a rule, the action specified by ACTION= is applied to the message.

With Exchange server filtering, if the message attributes satisfy a rule, any attachments are then evaluated using attachment attributes. When an attachment matches a rule, the action specified by ATTACHMENT_ACTION= is applied to the attachment.

The order in which filters process messages and attachments is described in more detail in "How message and attachment filters are applied" on page 368.

Each rule has a message action associated with it. ACTION="<match_action>" defines the action to be applied to the message when it matches a rule. For example, an action could be to mark the item as evaluated but not archive it (ACTION="MARK_DO_NOT_ARCHIVE"). If the action is to archive the item, additional actions can be specified, such as assigning a specific retention
Configuring filtering
Configuring custom filtering

category (RETENTION="<retention_category>") or storing the item in a particular archive (ARCHIVEID="<archive_ID>"). Full details of the actions that can be applied are given in "Rule actions" on page 352. If no action is specified, it defaults to "ARCHIVE_ITEM".

The preferred way to specify how messages that match a rule are to be archived is to assign a content category. A content category is a group of settings that are to be applied to an archived item. This can include a retention category, an archive ID and a list of the additional properties that are to be indexed by Enterprise Vault. You define content categories in the file custom properties.xml. Content categories are described in “Defining content categories” on page 390.

If attachments to Exchange server messages are to be evaluated, a rule must have an attachment action associated with it; ATTACHMENT_ACTION="<match_action">". If an attachment action is specified, an attachment attribute element ( <FILES> element) must also be present in the rule. This defines the file names or file size (or both) to use when matching attachments. If attachments match the specified attachment filter, the attachment action is performed. Attachments to nested messages are also processed by the filter.

**Note:** For messages (and then attachments), each rule in the ruleset file will be evaluated in the order in which they appear in the file and only the first matching rule will be executed. For this reason, it is important to put the highest priority rules first. For more information on the order in which filters are applied, see “How message and attachment filters are applied” on page 368.

Validating XML ruleset files

Archiving tasks that are enabled for custom filtering validate ruleset XML against the schema, ruleset schema.xdr, when they start archiving items. If any of the XML is invalid, the tasks stop and you must correct any errors before restarting them.

To avoid disrupting tasks because of syntactic errors, it is a good idea to validate your XML file before it is accessed by the tasks. You could use a third party tool, such as xsdvalidator:


When using the tool, specify the namespace as:

x:schema:ruleset schema.xdr

The schema file, ruleset schema.xdr, is shipped in the Custom Filter Rules folder. The schema must be referenced at the start of any ruleset files as follows:
<xml version="1.0" encoding="UTF-8"/>
<RULE_SET xmlns="x-schema:ruleset schema.xdr">

If the file is to contain non-ANSI characters, ensure the correct encoding is set on the first line and save the file as a Unicode file.

Note: All the XML tags and predefined values shown in upper case in this document are case sensitive and must be entered as upper case in the ruleset file. Values entered should also be treated as case sensitive.

Rule actions

The following actions can be applied to messages that match a rule filter:

- **ACTION=*/"ARCHIVE_ITEM" — Archive the message. This is the default action if you do not include the ACTION= clause or a message does not match any of the rules.
  
  With this action you can have additional actions: assigning a retention category (RETENTION=*/"<retention_category>/") to the item, sending the item to a specific archive (ARCHIVEID=*/"<archive_ID>/") and assigning a particular content category. See “Assigning a retention category” on page 354, and “Specifying a specific archive” on page 354 for more information on how to set these additional actions.

- **ACTION=*/"MARK_DO_NOT_ARCHIVE" — Do not archive the message; leave it in the original location.

  Caution: Messages marked as MARK_DO_NOT_ARCHIVE remain in the original location. If you are applying filtering to the journal mailbox or Domino journaling location, this action should only be used for a small number of messages, as leaving lots of messages may affect journaling performance.

If you later change the rule action, you can temporarily set the Override registry key to 1 to force the task to reprocess marked items. The Override key is described in the sections describing how to configure custom filtering registry settings for archiving tasks:

- “Registry settings for Exchange Server journal filtering” on page 340
- “Registry settings for Exchange Server user mailbox filtering” on page 342
- “Registry settings for Exchange Server public folder filtering” on page 343
- “Registry settings for Domino server journal filtering” on page 344
Configuring filtering

Configuring custom filtering

- **ACTION**="MOVE_DELETED_ITEMS" – Do not archive the message; move it to the Deleted Items folder. This action is only supported for Exchange server filtering.
  
  This action cannot be used with public folder filtering; if this action is configured, an error will be logged and the tasks will stop.

- **ACTION**="HARD_DELETE" – Do not archive the message; delete it immediately without moving it to the Deleted Items folder. This action is only supported for Exchange server filtering, but is not recommended for Exchange server public folder filtering.

---

**Caution:** If the Compliance Accelerator Journaling Connector is being used to capture a required percentage of all Exchange server journaled messages, do not configure a custom journal filter that deletes selected messages; this will compromise the accuracy of the Compliance Accelerator monitoring policy, because any deleted messages are not available for capture by the Journaling Connector.

With Exchange server filtering, the following actions can be applied to message attachments that match an attachment filter:

- **ATTACHMENT_ACTION**="REMOVE" – If a file attached to a message matches the name or size specified in the attachment attribute filter, delete it.

- **ATTACHMENT_ACTION**="REPLACE" – If a file attached to a message matches the name or size specified in the attachment attribute filter, replace it with a file called Deleted Attachments.txt, which lists the attachments that have been deleted.

If the message has nested messages with attachments, the action will be applied to all nested message attachments.

If the action applied to a message is "HARD_DELETE", no attempt is made to evaluate any files attached to the message. For more information on how custom filters are applied to messages and attachments see “How message and attachment filters are applied” on page 368.

The extract below shows how a rule name, message action and attachment action might be specified in the ruleset file. In this example, any messages that satisfy the message attribute filters will be archived in the default archive. Also, any Exchange server messages attachments that match the attachment filter will be deleted and replaced with a file called Deleted Attachments.txt:

```xml
<RULE NAME="Archive Rule 1" ACTION="ARCHIVE_ITEM"
  ATTACHMENT_ACTION="REPLACE">
  <message attribute filters>
  <attachment attribute filter>
```
Deleted Attachments.txt file

If the attachment action is "REPLACE", users will see a file called Deleted Attachments.txt attached to messages that have had attachments deleted by the filter. When they open this file, it contains a list of the files that have been deleted.

The contents of this file are taken from the file, CF_Replace_Attachment.txt, in the Enterprise Vault directory (typically, C:\Program Files\Enterprise Vault). If required, you can modify the text of this file. For example, you may want to localize the descriptive text.

Assigning a retention category

The RETENTION="<retention_category>" option is only applicable if the rule action is ACTION="ARCHIVE_ITEM".

Retention_category is the name of an existing Retention Category defined in Enterprise Vault. A different Retention Category may be specified for different rules.

The extract below shows how the option might be specified in the ruleset file. In this example, any messages that satisfy the message attribute filters will be archived and given the Retention Category, Legal:

```
<RULE NAME="Example rule2" ACTION="ARCHIVE_ITEM"
   RETENTION="Legal">
   <message attribute filters>
</RULE>
```

Specifying a specific archive

The ARCHIVEID="<archive_ID>" option is only applicable if the rule action is ACTION="ARCHIVE_ITEM".

Archive_ID identifies an existing, enabled archive.

To find the ID of the required archive:

1. Right click on the archive in the Enterprise Vault Administration Console.
2. Select Properties. The Archive ID is displayed on the Advanced page of Properties.

You can define a different archive for different rules. If you do not specify an archive, the default archive for the mailbox or public folder is used.

The extract below shows how the option might be specified in the ruleset file. In this example, any messages that satisfy the message attribute filters will be stored in the archive specified:

```
<RULE NAME="Example rule" ACTION="ARCHIVE_ITEM"
   ARCHIVEID="Archive ID">
   <message attribute filters>
</RULE>
```
Message attribute filters

Each rule can contain one or more message attribute filters. Each message attribute filter defines an attribute in the message to evaluate. To match a rule, a message must satisfy all the message attribute filters included in the rule. That is to say, there is an implicit AND between all message attributes included in a rule. The order of the attributes within a rule is not significant.

Message attributes are defined in a rule using the following general format:

```xml
<RULE NAME="rule_name" ...>
  <message_attribute [attribute_value_operators]>
    <attribute_value>
    [<attribute_value>]
    </message_attribute>
  [<message_attribute>... </message_attribute>]
</RULE>
```

- `<message_attribute>` defines a message attribute to match. This can be AUTHOR, RECIPIENTS, DIRECTION or SUBJECTS.
- `<attribute_value>` defines the message attribute value(s) to match. For each attribute there may be one or more values.
- `<attribute_value_operators>` are special operator options that enable you to define how values for an attribute are to be applied. The operators INCLUDES= and ALLOWOTHERS= are particularly useful if you want to define negative and positive matches when filtering on AUTHOR, RECIPIENTS and SUBJECTS. This is discussed in more detail in "Using INCLUDES and ALLOWOTHERS operators" on page 359. Attribute value operators are not available when filtering on message DIRECTION.

How to define message attribute filters is described in the following sections:

- “Filtering on message authors and recipients” on page 355
- “Filtering on message direction” on page 362
- “Filtering on message subject” on page 364

Filtering on message authors and recipients

To match message sender (From address) and recipient addresses (To, cc, Bcc and Undisclosed addresses), you can use the message attributes <AUTHOR> </AUTHOR> and <RECIPIENTS></RECIPIENTS>; in the ruleset file outline, message attributes are shown as:
You can specify the actual addresses to match as SMTP email addresses, display names or SMTP domains using the following XML elements (these are represented by the `<attribute_value>` lines in the ruleset file outline):

- **<EA>name@domain</EA>**
  This form can be used to specify SMTP addresses. The value specified must be the complete SMTP email address; if the value specified here is only part of an address, the message will not match. Wildcard characters cannot be used.
  If the character ‘&’ is included in an SMTP address, the character must be replaced with `&amp;` as ‘&’ is a special character in XML. For example, the SMTP address `admin&finance@ourcompany.com` should be specified in the XML file as: `admin&amp;finance@ourcompany.com`

- **<DISPN>display name</DISPN>**
  This form can be used to specify display names. As with the SMTP address, the value must be the full display name, without wildcard characters. An example display name for Exchange server messages is `<DISPN>John Doe</DISPN>`
  For Domino server messages, the format of display names will depend on the Domino server configuration. To match all required messages, ensure that you include all possible variations for a display name. For example, display names could take one or more of the following forms:
  ```xml
  <DISPN>Kevin Smith@exampleorg@exampledomain</DISPN>
  <DISPN>CN=Kevin Smith/O=exampleorg@exampledomain</DISPN>
  <DISPN>Kevin Smith@exampleorg@exampledomain</DISPN>
  <DISPN>CN=Kevin Smith/OU=Sales/O=exampleorg@exampledomain</DISPN>
  ```
  If Organizational Units are included in display names, these must also be specified. For example,
  ```xml
  <DISPN>CN=Kevin Smith/OU=Sales/O=exampleorg@exampledomain</DISPN>
  ```

- **<DOMAIN>exampledomain.com</DOMAIN>**
  This form can be used to specify SMTP domains. The value specified can be the full domain or a subdomain. For example, if the following domain value is specified:
  ```xml
  <DOMAIN>ourcompany.com</DOMAIN>
  ```
  The following addresses will match:
  - john.doe@ourcompany.com
  - jack.doe@hq.ourcompany.com
  - jane.doe@uk.hq.ourcompany.com
  but the following address will not match:
Configuring filtering

Configuring custom filtering

- john.doe@hqourcompany.com

- `<DL>distribution list name</DL>`
  
  This option is only supported for Exchange server filtering. Use this form when you want to match messages that have been sent to any members of the specified distribution list. For example, if a rule contains the following line:

  `<DL>ALL SALES</DL>`

  Then messages sent to any member of the distribution list called ALL SALES will match, irrespective of whether the member’s name is shown as the Display Name or SMTP address on the message. See “Specifying distribution lists in attribute values” on page 358 for more information on matching distribution list names and members.

**Note**: Matching attribute values is case insensitive.

The following example shows how you can specify a simple rule to archive and set the Retention Category “Legal” on any messages sent from anyone in the domain, ourcompany.com, with legal@ourcompany.com or the Lotus Notes user, Greg Court, in the recipient list:

```
<RULE ... ACTION='ARCHIVE_ITEM' RETENTION='legal'>
  <AUTHOR>
    <DOMAIN>ourcompany.com</DOMAIN>
  </AUTHOR>
  <RECIPIENTS>
    <EA>legal@ourcompany.com</EA>
    <DISPN>Greg Court/ourorg@ourcompany.com</DISPN>
  </RECIPIENTS>
</RULE>
```

The attribute value operators, INCLUDES= and ALLOWOTHERS=, enable you to define complex filters. See “Using INCLUDES and ALLOWOTHERS operators” on page 359.

**Notes**

- There are situations where messages may not have an SMTP address; for example, messages imported into a mailbox from a PST file and Exchange Server addresses set up for internal messaging only. For this reason you may want to include both the display name and the email address in a rule (provided you are not using the INCLUDES=“ALL” operator).

- Be aware that display names do not have to be unique; an external sender, for example, could have the same display name as an internal sender.

- If changes to your Microsoft Exchange Server Global Address List (or Global Address Catalog in Active Directory) affect users or distribution lists
included in custom filters, you may have to update your custom filter rules accordingly. For example, if you are filtering on the display name of a distribution list and then change the display name, you will need to update the appropriate ruleset file entry.

- Changes made to the Microsoft Exchange Server Global Address List will not become effective until the next scheduled GAL update. If, for example, a user’s address has been changed to their married name, and you have set up a filter that includes the new address as AUTHOR, there may be a delay before messages are matched.

- To ensure that Bcc and Undisclosed recipients are available when filtering on the Exchange server journal mailbox, envelope journaling must be enabled on your Microsoft Exchange Server. For more information on this subject, see “Envelope Journaling” on page 405.

Specifying distribution lists in attribute values
If you want to match all messages sent to members of a particular Exchange server distribution list, then use the <DL> </DL> message attribute. For example,

```xml
<RECIPIENTS>
  <DL>ALL SALES</DL>
</RECIPIENTS>
```

would match any message sent to any member of the distribution list, ALL SALES.

For this matching to work, ensure that expansion of distribution lists is enabled in the Administration Console (in the Archiving General settings on the Advanced tab of the Exchange journal policy). Also, the distribution list must not be included in the “blacklisted” distribution list registry setting, BlacklistedDLs, which can be created in the following location:

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

For Domino server filtering (and also Exchange server filtering), you can specify distribution lists using the <EA>, <DISPN> and <DOMAIN> message attributes. However, only messages with the specified string will match; no attempt is made to compare message recipients with individual members in the specified distribution list. For example, the members of an Exchange server distribution list called ALL SALES are:

- john.doe@ourcompany.com
- ken.brookes@ourcompany.com
- len.scott@ourcompany.com
In the ruleset file, the following message attribute filter is specified in a rule:

```
<RECIPIENTS>
  <DISPN>ALL SALES</DISPN>
</RECIPIENTS>
```

If a message has the display name ALL SALES in the recipient list, the message will satisfy the attribute filter above. If the message does not have the display name ALL SALES in the recipient list, it will not match the attribute filter, even if the recipient list does include the email address of a member of the distribution list.

**Using INCLUDES and ALLOWOTHERS operators**

You can create more complex filters by specifying several values for AUTHOR or RECIPIENTS message attributes and using the operators, INCLUDES= and ALLOWOTHERS= to define how the attribute values are to be matched.

**INCLUDES=** can have the following values:

- INCLUDES="NONE" means match messages that do not include the values specified for the attribute
- INCLUDES="ANY" means match messages that include one or more of the values specified for the attribute
- INCLUDES="ALL" means match messages that include all of the values specified for the attribute

If the INCLUDES= operator is not specified, INCLUDES="ANY" is assumed.

**ALLOWOTHERS=** can have the following values:

- ALLOWOTHERS="N" means match messages that include only the values specified in the filter and no others
- ALLOWOTHERS="Y" means that matched messages can include attribute values other than those listed in the filter can be included

If the ALLOWOTHERS= operator is not specified, ALLOWOTHERS="Y" is assumed.

In the following example, messages will match the rule if they have all three of the listed email addresses (INCLUDES="ALL"), and only these addresses (ALLOWOTHERS="N"), in the recipient list:

```
<RULE ...>
  <RECIPIENTS INCLUDES="ALL" ALLOWOTHERS="N">
    <EA>john.doe@ourcompany.com</EA>
    <EA>ken.brookes@ourcompany.com</EA>
    <EA>len.scott@ourcompany.com</EA>
  </RECIPIENTS>
</RULE>
```

In the next example, messages will match the rule if they have any of the listed email addresses (INCLUDES="ANY") but nothing else (ALLOWOTHERS="N"): 
<RULE ...
 <RECIPIENTS INCLUDES="ANY" ALLOWOTHERS="N">
  <EA>john.doe@ourcompany.com</EA>
  <EA>ken.brookes@ourcompany.com</EA>
  <EA>len.scott@ourcompany.com</EA>
 </RECIPIENTS>
</RULE>

In the next example, messages will match the rule if they do not include any of the listed email addresses in the recipient list (INCLUDES="NONE"). Matched messages can have other addresses in the recipient list (ALLOWOTHERS="Y"):

<RULE ...
 <RECIPIENTS INCLUDES="NONE" ALLOWOTHERS="Y">
  <EA>john.doe@ourcompany.com</EA>
  <EA>ken.brookes@ourcompany.com</EA>
  <EA>len.scott@ourcompany.com</EA>
 </RECIPIENTS>
</RULE>

If you want to specify both positive and negative matches within a single rule, you can have multiple message attribute entries and use INCLUDES="NONE" or INCLUDES="ALL", as appropriate. For example:

<RULE ...
 <RECIPIENTS INCLUDES="NONE">
  <EA>john.doe@ourcompany.com</EA>
  <EA>len.scott@ourcompany.com</EA>
 </RECIPIENTS>
 <RECIPIENTS INCLUDES="ALL">
  <EA>Ken.Brookes@ourcompany.com</EA>
  <EA>robert.hill@ourcompany.com</EA>
 </RECIPIENTS>
</RULE>

In the above example, messages will match if they do not include john.doe@ourcompany.com or len.scott@ourcompany.com in the recipient list:

<RECIPIENTS INCLUDES="NONE" ...
</RECIPIENTS>

but do include both ken.brookes@ourcompany.com and robert.hill@ourcompany.com

<RECIPIENTS INCLUDES="ALL" ...
</RECIPIENTS>

By using different combinations of INCLUDES= and ALLOWOTHERS= values, you can set fairly complex filters. The table, “Effect of using different operator value combinations”, shows filter results for different messages when different combinations of values are set for the operators, INCLUDES= and ALLOWOTHERS=, in the following example filter:

<RULE ...
 ACTION="ARCHIVE_ITEM"
 <RECIPIENTS INCLUDES="NONE|ANY|ALL"
 ALLOWOTHERS="N|Y">
  <EA>Ann@example.com</EA>
  <EA>Bill@example.com</EA>
 </RECIPIENTS>
</RULE>
Ann@example.com and Bill@example.com are the recipient addresses to match. In the table, the main column headings show the recipients in five different test messages. (For brevity, the recipients are called Ann, Bill, and Colin in the column headings).

The first column shows different combinations of values set for the INCLUDES= and ALLOWOTHERS= operators.

"no match" means that, if the operator combination shown in the left column is set, a message sent to the recipients shown in the column heading would not satisfy the filter rule and would not be archived (that is, the rule action is not applied).

"match" means that, if the operator combination shown in the left column is set, a message sent to the recipients shown in the column heading would satisfy the filter rule and be archived.

The figures, “Msg 1 with INCLUDES="NONE" and "ALLOWOTHERS"=N" on page 362 and “Msg 1 with INCLUDES="ANY" and ALLOWOTHERS="Y"” on page 362, illustrate what happens in two of the scenarios in the table.

Table 31-3  Effect of using different operator value combinations

<table>
<thead>
<tr>
<th>Operator values set</th>
<th>Msg 1: recipient is Ann</th>
<th>Msg 2: recipients are Ann &amp; Bill</th>
<th>Msg 3: recipients are Ann, Bill &amp; Colin</th>
<th>Msg 4: recipients are Bill &amp; Colin</th>
<th>Msg 5: recipient is Colin</th>
</tr>
</thead>
<tbody>
<tr>
<td>INCLUDES=&quot;NONE&quot; + ALLOWOTHERS=&quot;Y&quot;</td>
<td>no match</td>
<td>no match</td>
<td>no match</td>
<td>no match</td>
<td>match</td>
</tr>
<tr>
<td>INCLUDES=&quot;NONE&quot; + ALLOWOTHERS=&quot;N&quot;</td>
<td>no match</td>
<td>no match</td>
<td>no match</td>
<td>no match</td>
<td>no match</td>
</tr>
<tr>
<td>INCLUDES=&quot;ANY&quot; + ALLOWOTHERS=&quot;Y&quot;</td>
<td>match</td>
<td>match</td>
<td>match</td>
<td>match</td>
<td>no match</td>
</tr>
<tr>
<td>INCLUDES=&quot;ANY&quot; + ALLOWOTHERS=&quot;N&quot;</td>
<td>match</td>
<td>match</td>
<td>no match</td>
<td>no match</td>
<td>no match</td>
</tr>
<tr>
<td>INCLUDES=&quot;ALL&quot; + ALLOWOTHERS=&quot;Y&quot;</td>
<td>no match</td>
<td>match</td>
<td>match</td>
<td>no match</td>
<td>no match</td>
</tr>
<tr>
<td>INCLUDES=&quot;ALL&quot; + ALLOWOTHERS=&quot;N&quot;</td>
<td>no match</td>
<td>match</td>
<td>no match</td>
<td>no match</td>
<td>no match</td>
</tr>
</tbody>
</table>
FIGURE 31-2  

Msg 1 with INCLUDES="NONE" and "ALLOWOTHERS"=N

Custom filtering enabled.
Rule filter configured:

```xml
<RULE ...ACTION="ARCHIVE_ITEM">
  <RECIPIENTS INCLUDES="NONE">
    ALLOWOTHERS="Y">
  
  <DISPN>Ann</DISPN>
  <DISPN>Bill</DISPN>
</RECIPIENTS>

</RULE>
```

FIGURE 31-3  

Msg 1 with INCLUDES="ANY" and ALLOWOTHERS="Y"

Custom filtering enabled.
Rule filter configured:

```xml
<RULE ...ACTION="ARCHIVE_ITEM">
  <RECIPIENTS INCLUDES="ANY">
    ALLOWOTHERS="Y">
  
  <DISPN>Ann</DISPN>
  <DISPN>Bill</DISPN>
</RECIPIENTS>

</RULE>
```

Filtering on message direction

The `<DIRECTION>` message attribute enables you to match messages based on the direction of the message, in relation to the organization.
without needing to specify the author or recipient details in the rule. Message
direction can be internal to the organization, outbound from the organization or
inbound to the organization. This option is available for both Exchange server
and Domino server filtering.

One or more of the following values can be specified in the
=DIRECTORY=</=DIRECTORY= message attribute:

■ INTERNAL="Y" means match the message if it is from an internal address
to an internal address. The message must not include any external
addresses in the recipient list.

■ OUTBOUND="Y" means match the message if it is from an internal address
to an external address. The message must include at least one external
address in the recipient list.

■ INBOUND="Y" means match the message if it is from an external address to
an internal address. The message must include at least one internal address
in the recipient list.

If the value is not specified, it defaults to "N". For any messages to match, at
least one value must be set to "Y".

The following example rule will archive and set the Retention Category
"Internal", on messages from one internal address to another internal address
only. Note that a message from one internal address to another internal address
that also has an external address in the recipient list will be treated as external:

<RULE NAME="Internal only" RETENTION="Internal" >
  <DIRECTION INTERNAL="Y" OUTBOUND="N" INBOUND="N" />
</RULE>

The following example rule will archive and set the Retention Category
"External", on messages sent to or received from addresses outside the
organization:

<RULE NAME="External" RETENTION="External" >
  <DIRECTION OUTBOUND="Y" INBOUND="Y" />
</RULE>

Defining which addresses are internal
Addresses are regarded as internal to the organization if they have the same
domain as one of the SMTP addresses assigned to the Enterprise Vault
Journaling task user (typically, the Vault Service account).

For example, if the journaling task runs under a Vault Service account called
vaultadmin, which has the SMTP addresses:

■ VaultAdmin@ourcompanyplc.com
■ VaultAdmin@ourcompanyinc.com

then any of these address will be recognized as internal:
Configuring custom filtering

- *@ourcompanyplc.com
- '@[*.]ourcompanyplc.com
- *@ourcompanyinc.com
- '@[*.]ourcompanyinc.com

where [*.] means the string can be repeated, as in john.doe@sales.emea.ourcompanyplc.com.

Any other addresses are treated as external.

With Exchange server filtering, addresses from local Microsoft Exchange Servers are also regarded as internal. (These addresses include the MAPI attribute, PR_SENDER_ADDRTYPE).

For Exchange server users, you can change the email addresses associated with a user in Active Directory (Exchange Server 2000 or later) or Exchange Administrator (Exchange Server 5.5).

Alternatively, you can specify additional internal domains using the InternalSMTPDomains registry key. Use this method to define internal addresses for Domino server filtering.

To add domains using the registry key, perform the following steps on each computer with an Enterprise Vault Exchange or Domino Journaling task:

1. Start Regedit and navigate to the following location:
   HKEY_LOCAL_MACHINE\Software\KVS\Enterprise Vault\Agents

2. Create a new String Value called InternalSMTPDomains.

3. Modify the key and in the Value Data field enter the required domains as a semicolon delimited string. For example, setting this string to "ourcompanyplc.com;ourcompanyinc.com;ourcompany.parentcorp.com" means that addresses such as jld@eng.uk.ourcompanyinc.com and kv@hq.ourcompany.parentcorp.com will also be treated as internal.

Filtering on message subject

The <SUBJECTS></SUBJECTS> message attribute enables you to match messages on the subject text of the message. Within a <SUBJECTS> attribute, values to match can be defined as follows:

- Match any message with a subject that is exactly the same as the specified string:
  <SUBJ MATCH="EXACT">string</SUBJ>
- Match any message with a subject that contains the specified string:
  `<SUBJ MATCH="CONTAINS">string</SUBJ>`
- Match any message with a subject that starts with the specified string:
  `<SUBJ MATCH="STARTS">string</SUBJ>`
- Match any message with a subject that ends with the specified string:
  `<SUBJ MATCH="ENDS">string</SUBJ>`

Matching against attribute values is case insensitive. Wildcards cannot be used.

In the following example, messages that have a subject of exactly Welcome New Employee or starts with Salary Summary for or ends with Message Notification will be moved to the wastebasket without being archived:

```xml
<RULE NAME="Delete" ACTION="MOVE_DELETED_ITEMS">
  <SUBJECTS>
    <SUBJ MATCH="EXACT">Welcome New Employee</SUBJ>
    <SUBJ MATCH="STARTS">Salary Summary for</SUBJ>
    <SUBJ MATCH="ENDS">Message Notification</SUBJ>
  </SUBJECTS>
</RULE>
```

The INCLUDES="NONE" operator can be used to match messages with a subject that does not include particular strings. For example, the following rule will match messages that do not have any of the specified values in the message subject:

```xml
<RULE ...
  <SUBJECTS INCLUDES="NONE">
    <SUBJ MATCH="EXACT">Welcome New Employee</SUBJ>
    <SUBJ MATCH="STARTS">Salary Summary for</SUBJ>
    <SUBJ MATCH="ENDS">Message Notification</SUBJ>
  </SUBJECTS>
</RULE>
```

**Filtering on MAPI named properties**

This option is only available with Exchange server filtering.

The `<NAMEDPROP>` message attribute enables you to select Exchange Server messages for processing depending on the value assigned to specific MAPI named properties. The custom properties feature is used to define the required properties, so that they are indexed by Enterprise Vault. Users can then search archived messages for those with a particular value set for the named property. To find out how to define named properties, see "Defining additional properties to index" on page 386.

Named properties can be single-valued or multi-valued. For example, Outlook categories are defined in MAPI as a named property that can have multiple values; that is, more than one category can be assigned to a message.

A named property filter takes the following general format:

```xml
<NAMEDPROP TAG="EV_tag_name" INCLUDES="operator_value"/>
```
Configuring custom filtering

The value of the TAG attribute is the name by which Enterprise Vault knows the property. This is the TAG value set in the custom properties.xml file (see “MAPI properties” on page 386).

The operator value can be "ANY", "NONE" or "ALL".

Each <PROP> line defines a specific value for the property that custom filtering is to use when evaluating messages.

The following example shows the filter that would match messages that had an Outlook category of either "Business" or "Innovation". Any messages that match are archived with the retention category, "Innovation". If a company policy states that certain Outlook categories must be assigned to messages that contain business critical information, a filter such as this can be configured to select messages with the specific Outlook categories set.

<!--Example: Archive items that have the Business and Innovation Outlook categories set -->

<RULE NAME="Business info rule" ACTION="ARCHIVE_ITEM"
RETENTION="Innovation">
  <NAMEDPROP TAG="Category" INCLUDES="ANY">
    <PROP VALUE="Business" />
    <PROP VALUE="Innovation" />
  </NAMEDPROP>
</RULE>

For more information on named properties, see the Microsoft article:


Attachment attribute filters

This option is only available with Exchange server filtering.

To enable you to delete certain attachments before archiving messages, a rule can contain attachment attribute filters which define which attachment files to select.

The following example XML shows how you can include one or more attachment attribute filters in a rule:

<RULE NAME="rule_name" ... ATTACHMENT_ACTION="<action>">
  [...message_attribute]...
  <FILES INCLUDES="ANY|ALL|NONE">
    <FILE FILENAME="<filename" SIZE_GREATER_THAN_KB="<integer>" />
    <FILE ... />
  </FILES>
  ...
</RULE>
Configuring filtering

Configuring custom filtering

The `<FILES>` tag defines an attachment filter.
If you specify an attachment action (ATTACHMENT_ACTION=), then you need to include at least one attachment filter (using the `<FILES>` tag). For an attachment to match a rule (and the attachment action applied), the attachment must satisfy all attachment filters specified in the rule. The order of attachment filters in a rule is not significant.

The INCLUDES= operator enables you to define how the following attribute lines are to be applied, when evaluating each attachment.

An attachment filter contains one or more `<FILE>` elements, that define the attributes to match. Each `<FILE>` element contains one or both of the following attributes:

- **FILENAME="<filename>"**
  <filename> is all or part of the file name to match. Wildcards can be included in the file name. You can use this attribute to filter files with specific text strings in the name or extension, for example, "*.AVI".
  When selecting files using the file extension, custom filtering only evaluates the file name, it does not check the type of the file contents; If files that would normally be deleted by a filter are given a different extension, they will not be deleted by the filter.
  Also, files contained in compressed files, such as .ZIP files, are not evaluated.

- **SIZE_GREATER_THAN_KB="<integer>"**
  This enables you to configure the filter to remove attachments over a certain size.

Where file name and size are specified in a `<FILE>` element, both must be satisfied for an attachment to match. For example, if an attachment is to match the following line, it must have an extension of .MP3 and be larger than 1 MB:

```
<FILE FILENAME="*.MP3" SIZE_GREATER_THAN_KB="1000" />
```

If you specify multiple `<FILE>` elements to use in evaluating attachment files, each one will be applied. For an attachment to match the rule, it must match each `<FILE>` element.

To define how the `<FILE>` lines are to be applied, when evaluating each attachment, use the INCLUDES= operator:
Configuring filtering

Configuring custom filtering

- INCLUDES="ANY" means that the attachment matches if it has the attributes specified in at least one of the <FILE> lines. This is the default action if the operator is not specified.
- INCLUDES="ALL" means that the attachment matches only if it has the attributes specified in all the <FILE> lines.
- INCLUDES="NONE" means that the attachment matches if it does not include any of the attributes specified in the <FILE> lines.

In the following example, an attachment will match the filter if all the following are true:

- The file is an MP3 file larger than 2MB
- The file name includes the text, "enlarge", and the file is larger than 1 MB
- The file has the extension, MPG
- The file is larger than 12 MB

```xml
<FILES INCLUDES="ANY">
  <FILE FILENAME="*.MP3" SIZE_GREATER_THAN_KB="2000" />
  <FILE FILENAME="*enlarge*." SIZE_GREATER_THAN_KB="1000" />
  <FILE FILENAME="*.MPG" />
  <FILE SIZE_GREATER_THAN_KB="12000" />
</FILES>
```

The following example shows how multiple attachment filters can be used to exclude certain attachments from deletion:

```xml
<RULE NAME="Filter attachments rule" ... ATTACHMENT_ACTION="REMOVE">
  <FILES INCLUDES="NONE">
    <FILE FILENAME="signature.jpg" />
  </FILES>
  <FILES INCLUDES="ANY">
    <FILE SIZE_GREATER_THAN_KB="5000" />
  </FILES>
</RULE>
```

With these attachment filters, attachments will be deleted if they do not have the filename, `signature.jpg`, and are larger than 5 MB.

How message and attachment filters are applied

This section describes the order in which message and attachment evaluation is applied when filtering Exchange server messages.
Note: With Domino server filtering, attachment evaluation is not available. This means that only message attribute filters are applied and attached messages are not evaluated.

When custom filters processes messages, the following general points are observed:

- Messages and attachments are evaluated separately. Messages are evaluated first against rules in the ruleset file, and then attachments are evaluated against any rules that contain an attachment action. If an attachment is a message, the message is evaluated using message filters in rules (with attachment action set) and then any attachments to the nested message are evaluated using attachment filters in rules.

- When evaluating a message, only the first rule in the ruleset file that matches the message is applied. Similarly, when evaluating attachments, only the first rule that matches is applied to the attachment. For this reason the order of rules in a ruleset file is significant.

- The rule action (and attachment action) are only applied to a message (or attachment) that satisfies all the filters in the rule.

- The default action for both messages and attachments is to archive the item. This means that messages and attachments that do not match any rules will be archived.

The figure, “Processing attachments,” shows how custom filtering processes a message with attachments. The message illustrated has a nested message attached and that message has a file attached. The simple ruleset file has two rules that contain message filters and one rule that contains attachment filters.
The top-level message is evaluated using the first message rule, rule1.

If that rule does match, then the rule ACTION is applied to the message. If the rule does not match, then rule2 is tried.

(If the message ACTION is HARD_DELETE, no further evaluation is done).

As there is a rule with ATTACHMENT_ACTION, and the message has an attachment, the message attachment is evaluated using the attachment filters in rule3.

Custom filters recognizes that the attachment is a message, so the message is evaluated against message filters in any rules with ATTACHMENT_ACTION set. In this example, only rule3 has ATTACHMENT_ACTION set and it does not have any message filters, so the message will not match the rule. Items that do not match filter rules are archived (the default action).

The attachment to the nested message is then evaluated using the attachment filters in rule3. If the attachment matches the attachment filters then the ATTACHMENT_ACTION is applied to the attachment.

Message filters and attachment filters can be combined in a single rule to select attachments to particular messages. How such filters are processed is illustrated in the next example.

The figure, “Example message with attachments,” shows an example message to the recipient, Karen Little, that has an MP3 file attached and also a message attached (a nested message). The message may also have attachments.
Configuring filtering

Configuring custom filtering

Figure 31-5 Example message with attachments

The following example ruleset file contains a single rule to be applied to this message. The overall effect of this rule is to delete certain attachments in Exchange server messages to recipients other than Gill Smith or John Doe. Attachments in messages to Gill Smith or John Doe are not deleted. Attachments with the following attributes will be deleted:

- MP3 attachments larger than 2 MB
- JPG attachments larger than 1 MB
- MPG files larger than 5 MB

```xml
<?xml version="1.0" encoding="UTF-8"?>
<RULE_SET xmlns="x-schema:ruleset schema.xdr">
  <!-- Disallowed attachment rule: This rule will delete the specified attachments for all recipients except Gill Smith and John Doe. -->
  <RULE NAME="Disallowed attachments (except directors)" ATTACHMENT_ACTION="REMOVE">
    <RECIPIENTS INCLUDES="NONE" ALLOWOTHERS="N">
      <EA>Gill.Smith@example.com</EA>
      <EA>John.Doe@example.com</EA>
    </RECIPIENTS>
    <FILES INCLUDES="ANY">
      <FILE FILENAME="*.MP3" SIZE_GREATER_THAN_KB="2000" />
      <FILE FILENAME="*.JPG" SIZE_GREATER_THAN_KB="1000" />
      <FILE FILENAME="*.MPG" SIZE_GREATER_THAN_KB="5000" />
    </FILES>
  </RULE>
</RULE_SET>
```

Assuming the appropriate archiving task has custom filtering enabled, the filters in this ruleset will be applied to the example message, as follows:

1. First apply the message attribute filter (the <RECIPIENTS> element) to the top-level message.
2. The recipient is not Gill Smith or John Doe, so the message attribute filter matches.
As the message matches the rule, it will be archived (ACTION=).

Is there a rule that contains ATTACHMENT_ACTION? Yes. This means that any attachments to the message must be evaluated using <FILES>attachment filters.

Does the attachment file name and file size match any of the <FILE>attribute lines in the rule? Yes, the attached file matches the first <FILE>line. This means that the attachment matches the rule, so delete the attachment, as specified in the ATTACHMENT_ACTION.

Does the message have another attachment? Yes, there is an attached message. Custom filtering recognizes that the attachment is a message and evaluates the message using the message attribute filter (the <RECIPIENTS> element).

As the nested message is to John Doe, the <RECIPIENTS> filter is not satisfied. The message is therefore archived together with its attachments.

Example Ruleset File

The following shows an example of the ruleset file, Default Filter Rules.xml (a renamed copy of Example Filter Rules.xml). If the registry keys have been set to enable custom filtering for Domino journaling locations and Exchange server user and journal mailboxes and public folders, this file will be used for filtering any archiving targets that do not have a named ruleset file.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<RULE_SET xmlns="x-schema:ruleset schema.xdr">
  <!-- Example Rule 1: This rule will exclude any email from archiving if it originates from someone in the Employee Benefits distribution list. -->
  <RULE NAME="Benefits correspondence" ACTION="MARK_DO_NOT_ARCHIVE">
    <AUTHOR>
      <DISPN>HR Employee Benefits</DISPN>
    </AUTHOR>
  </RULE>

  <!-- Example Rule 2: This rule will exclude any email from archiving if it is sent to someone in the Employee Benefits distribution list. -->
  <RULE NAME="Benefits correspondence" ACTION="MARK_DO_NOT_ARCHIVE">
    <RECIPIENTS>
      <DISPN>HR Employee Benefits</DISPN>
    </RECIPIENTS>
  </RULE>
</RULE_SET>
```
<!--Example Rule 3: This rule will move email to the wastebasket if it comes from any of the sources listed, and is about any of the subjects listed.-->

```xml
  <RULE NAME="Newsletters" ACTION="MOVE_DELETED_ITEMS">
    <AUTHOR INCLUDES="ANY">
      <EA>icweek@ucg.com</EA>
      <EA>WebDirect@ACLI.com</EA>
      <DOMAIN>limra.com</DOMAIN>
    </AUTHOR>
    <SUBJECTS INCLUDES="ANY">
      <SUBJ MATCH="STARTS">Society SmartBrief</SUBJ>
      <SUBJ MATCH="EXACT">TaxFacts ENews</SUBJ>
    </SUBJECTS>
  </RULE>
```

<!--Example Rule 4: Delete mail from known junk-mail sources, (and others), if it contains certain common spam subjects-->;

```xml
  <RULE NAME="Junk Mail" ACTION="HARD_DELETE">
    <AUTHOR INCLUDES="ANY" ALLOWOTHERS="Y">
      <DOMAIN>indiatimes.com</DOMAIN>
      <DOMAIN>websavings-usa.net</DOMAIN>
    </AUTHOR>
    <SUBJECTS INCLUDES="ANY">
      <SUBJ MATCH="CONTAINS">enlargement</SUBJ>
      <SUBJ MATCH="CONTAINS">weight loss</SUBJ>
    </SUBJECTS>
    <SUBJECTS INCLUDES="ALL">
      <SUBJ MATCH="CONTAINS">debt</SUBJ>
      <SUBJ MATCH="CONTAINS">consolidate</SUBJ>
      <SUBJ MATCH="CONTAINS">loan</SUBJ>
    </SUBJECTS>
  </RULE>
```

<!--Example 5: Take default action (ARCHIVE_ITEM) if the subject matches the composite rule: Must start with "MEMO", contain "INTERNAL" and end in "OurCompany" e.g. "MEMO : Contains information internal to OurCompany" would match, but "MEMO : do not distribute" would not match Also allocates the message to a content category "Memoranda"-->

```xml
  <RULE NAME="Internal Memo" CONTENTCATEGORY="Memoranda">
    <SUBJECTS INCLUDES="ALL">
      <SUBJ MATCH="STARTS">Memo</SUBJ>
      <SUBJ MATCH="CONTAINS">Internal</SUBJ>
      <SUBJ MATCH="ENDS">OurCompany</SUBJ>
    </SUBJECTS>
  </RULE>
```
Configuring filtering

Configuring custom filtering

<rule name="Management" contentcategory="ManagementMail" retention="Important">
  <author includes="any">
    <ea>mike.senior@management.com</ea>
    <ea>jon.little@management.com</ea>
    <ea>jill.taylor@management.com</ea>
  </author>
</rule>

<rule set/>

<rule name="Sent to Management ONLY" archiveid="16611b008a3f65749b4118182e0021461110000evsite.ourcompany.com">
  <recipients includes="any" allowothers="n">
    <ea>mike.senior@management.com</ea>
    <ea>jon.little@management.com</ea>
    <ea>jill.taylor@management.com</ea>
  </recipients>
</rule>

<rule name="External Recipient" action="mark_do_not_archive">
  <recipients includes="none">
    <domain>OurCompany.com</domain>
  </recipients>
</rule>

<rule name="Internal Recipient" action="archive_item" retention="Internal">
  <direction internal="y"/>
</rule>

<rule set/>

<rule name="Use a special retention category for mail addressed to any members of the specified DL -- This feature is not currently supported for Domino server filtering -->
<RULE NAME="On the VIP list" RETENTION="VeryImportant">
  <RECIPIENTS>
    <DL>TheVIPs</DL>
  </RECIPIENTS>
</RULE>

<!--Example 11: delete MP3 attachments before archiving - This feature is not currently supported for the Domino server filtering -->

<RULE NAME="DeleteMP3s" ATTACHMENT_ACTION="REMOVE">
  <FILES>
    <FILE FILENAME="*.MP3"/>
  </FILES>
</RULE>

<!--Example 12: match against named MAPI properties defined in Custom Properties.XML - This feature is not currently supported for the Domino server filtering -->

<RULE NAME="Category Match" ACTION="ARCHIVE_ITEM">
  <NAMEDPROP TAG="CaseAuthor" INCLUDES="ANY">
    <PROP VALUE="Engineering"/>
    <PROP VALUE="Support"/>
  </NAMEDPROP>
  <NAMEDPROP TAG="CaseStatus" INCLUDES="ANY">
    <PROP VALUE="Open"/>
    <PROP VALUE="Pending"/>
  </NAMEDPROP>
</RULE>
Configuring filtering

Configuring custom filtering
Configuring custom properties

Read this chapter to find out:

- How to include in Enterprise Vault indexes additional properties on an item, for example, properties that have been added to messages by third-party applications.
- How to configure the browser search to enable users to search on these indexed properties.
- How to configure content categories.

The custom properties feature is an extension to custom filtering that enables Enterprise Vault to access and index additional message properties when archiving items. Properties can be the following Exchange Server MAPI or Domino server properties that have been added to messages by a third-party application:

- Standard MAPI properties that are not currently indexed by Enterprise Vault
- Custom MAPI properties
- Named MAPI properties
- Domino server message properties

Content categories are groups of settings to be applied to messages as they are archived. Settings can include a retention category to be applied, an archive to be used and particular message properties to be indexed. You can configure Enterprise Vault to apply a content category on all messages archived by particular archiving tasks. Alternatively, by using custom filtering together with custom properties, you can configure Enterprise Vault to apply a content category on selected messages only.
Using named MAPI properties and custom filtering, you can also select messages to archive based on the value of specific named properties. You define custom properties and content categories in the XML file, custom properties.xml, which must be located in the folder Enterprise Vault\Custom Filter Rules. Additional entries in this file enable you to make the indexed properties available to the web browser search, or other third party applications, so that users can include the custom properties in archive search criteria. An example of this file is installed in Custom Filter Rules with the name Example Custom Properties.xml.

An API is available to enable third party applications to access the custom properties. For details of this API, see the Enterprise Vault Application Programmer’s Guide.

If you have special filtering requirements for your archiving system, Symantec Corporation can supply the appropriate custom filters. For details, go to http://support.veritas.com.

To configure custom properties or content categories

1. Ensure that the custom filtering registry settings for the required archiving tasks are configured. These need to be set, even if you want to implement custom properties or content categories, without filtering. The registry settings are described in the following sections:
   - “Registry settings for Exchange Server journal filtering” on page 340
   - “Registry settings for Exchange Server user mailbox filtering” on page 342
   - “Registry settings for Exchange Server public folder filtering” on page 343
   - “Registry settings for Domino server journal filtering” on page 344

2. Create the XML file, custom properties.xml. Place this file in the folder Enterprise Vault\Custom Filter Rules. The overall format of the file is described in “General format of custom properties.xml” on page 384.

The entries in this file enable you to do the following:

- Index custom properties on messages. Custom properties entries are described in “Defining additional properties to index” on page 386.
- Define required content categories. Content category entries are described in “Defining content categories” on page 390.
- Display custom properties and content categories in web search applications, so that users can include them in search criteria. Presentation entries are described in “Defining how properties are presented in applications” on page 393.
To configure Enterprise Vault to index specific custom properties on all messages, without performing any filtering, create a custom properties.xml file but no ruleset file. The custom properties.xml file must include definitions of the custom properties and a default content category. The default content category will be applied to all messages and defines which properties Enterprise Vault is to index. (This behavior can be altered using the IGNORENODEFAULT registry setting. See “Controlling default settings” on page 379 for details).

3 If you want to index the properties on selected messages or apply content categories to selected messages, create the required filter rules and actions in XML ruleset files. These are held in one or more XML ruleset files, which must also be placed in the folder, Enterprise Vault\Custom Filter Rules.

   The format of ruleset files and the rules and actions available are described in “Configuring custom filtering” on page 338.

4 Restart the archiving tasks that have custom properties and filters enabled.

### Controlling default settings

If Enterprise Vault archiving tasks are enabled for filtering, the action they take when archiving is determined by the existence of the various configuration entities:

- XML ruleset files in the folder, Enterprise Vault\Custom Filter Rules
- The XML ruleset file, Default Filter Rules.xml
- The XML custom properties file, custom properties.xml
- Content category entries in custom properties.xml

An additional configuration option, IGNORENODEFAULT registry entry, can be used to alter the archiving task behavior, if some of the configuration entities are not defined. How to set the IGNORENODEFAULT registry entry is described in “Setting IGNORENODEFAULT registry entry.”

Different configurations and the resulting actions of archiving tasks for each configuration are shown in the tables, “Example custom filter and custom property configurations” on page 382 and “Resulting actions for example configurations” on page 383.

### Setting IGNORENODEFAULT registry entry

If the appropriate registry keys are configured to enable custom filtering and properties for archiving tasks, then certain configuration entities are required
Configuring custom properties

Controlling default settings

to define the default actions of the archiving tasks. For example, if specific targets are to be archived using particular filter rules, then a named XML rule set file must exist for each of the archiving targets for custom filtering, and a Default Filter Rules.xml file must also exist to provide filtering rules for the other archiving targets serviced by the archiving tasks. If this file does not exist, then the archiving tasks will stop and an error reported in the event log.

Alternatively, if the Default Filter Rules.xml file does not exist, but you configure the IGNORENODEFAULT registry entry, the archiving tasks ignore the fact that the file is missing and use the default archiving task policy settings when archiving all targets that do not have a named rule set file.

The IGNORENODEFAULT registry entry also enables you to restrict custom filtering to target archiving targets with named rule set files only. (If the Default Filter Rules.xml file exists, it is used as the default by all archiving tasks enabled for custom filtering).

Similarly, to apply custom property indexing to specific target archiving locations, you would typically require the following configuration entities:

- A custom properties.xml file with entries defining the custom properties to index and an associated content category.
- A separate, named rule set file for each of the archiving targets requiring custom property indexing.
- In custom properties.xml, a default content category to use for all messages archived from other locations that are not covered by the named rule set files.

However, if you want to restrict custom filtering and custom property indexing to the named targets, it is more efficient to omit setting the default content category in custom properties.xml and set the IGNORENODEFAULT registry entry. In this way, custom property indexing is applied only to locations explicitly defined by named rule set files.

To set the IGNORENODEFAULT registry entry for Exchange server filtering

1. Log in as the Enterprise Vault Service account on the computer running the archiving tasks enabled for custom properties and filters.
2. Start Regedit.
3. Navigate to the following location:
   HKEY_LOCAL_MACHINE\Software\KVS\Enterprise Vault\External Filtering\Journaling\Mailbox|PublicFolder
4 Right click the required archiving key (Journaling, Mailbox or PublicFolder) and select New, Key.

5 Name the new key EnterpriseVault.CustomFilter.

6 Right click EnterpriseVault.CustomFilter and create a new DWORD called IGNORENODEFAULT.

7 Set the value to 1 to ignore missing default files or settings.  
   This key will apply to all tasks for the selected type of archiving.

8 Close Regedit.

9 Restart the associated archiving tasks.

In a distributed environment, where you have archiving tasks running on more than one computer, you will need to perform these steps on each computer running archiving tasks that have been enabled for custom filtering and properties.

To set the IGNORENODEFAULT registry entry for Domino server filtering

1 Log in as the Enterprise Vault Service account on the computer running the archiving tasks enabled for custom properties and filters.

2 Start Regedit.

3 Navigate to the following location:
   HKEY_LOCAL_MACHINE \Software \KVS \Enterprise Vault \External Filtering \Lotus Journaling

4 Right click the Lotus Journaling key and select New, Key.

5 Name the new key KVS.EnterpriseVault.LotusDomino.CustomFilter.

6 Right click KVS.EnterpriseVault.LotusDomino.CustomFilter and create a new DWORD called IGNORENODEFAULT.

7 Set the value to 1 to ignore missing default files or settings.  
   This key will apply to all Domino Journaling tasks on the computer.

8 Close Regedit.

9 Restart the associated archiving tasks.

In a distributed environment, where you have archiving tasks running on more than one computer, you will need to perform these steps on each computer.
running archiving tasks that have been enabled for custom filtering and properties.

Summary of default archiving actions

The table, “Example custom filter and custom property configurations” on page 382, shows ten different configurations for custom filtering and properties. The resulting actions taken by archiving tasks in each case are described in “Resulting actions for example configurations” on page 383. In all cases it is assumed that the appropriate registry settings have been configured to enable the archiving task for custom filtering. The following configuration entities are considered:

- Named XML ruleset files in the folder, Enterprise Vault\Custom Filter Rules. In the example cases shown, John Doe.xml and Sam Cole.xml are named ruleset files for the mailboxes John Doe and Sam Cole respectively. Remember that named ruleset files can also be created for Exchange server public folders, specific Exchange server journal mailboxes, or specific Domino server journaling locations (see “About custom filtering ruleset files” on page 346).

- The default ruleset file for all types of archiving, Enterprise Vault\Custom Filter Rules\Default Filter Rules.xml.

- The custom properties XML file, Enterprise Vault\Custom Filter Rules\custom properties.xml, with custom properties defined for indexing.

- Content category entries in the custom properties.xml file.

- The registry setting, IGNORENODEFAULT, with a value of 1.

<table>
<thead>
<tr>
<th>Table 32-1</th>
<th>Example custom filter and custom property configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case</td>
<td>Custom properties file exists</td>
</tr>
<tr>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>2</td>
<td>No</td>
</tr>
<tr>
<td>3</td>
<td>No</td>
</tr>
<tr>
<td>4</td>
<td>No</td>
</tr>
<tr>
<td>5</td>
<td>No</td>
</tr>
</tbody>
</table>
### Table 32-1  Example custom filter and custom property configurations

<table>
<thead>
<tr>
<th>Case</th>
<th>Custom properties file exists</th>
<th>Default content category defined</th>
<th>Named ruleset file exists: John Doe.xml</th>
<th>Named ruleset file exists: Sam Cole.xml</th>
<th>Default ruleset file exists</th>
<th>IGNORENODEFAULT set</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>7</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>8</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>9</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>10</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Table 32-2  Resulting actions for example configurations

<table>
<thead>
<tr>
<th>Case</th>
<th>Resulting action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>An error is written to the event log and the archiving task stops, because custom filtering is enabled but there is no ruleset file or custom property file.</td>
</tr>
<tr>
<td>2</td>
<td>Missing defaults are ignored and both mailboxes are archived according to the default Exchange mailbox policy.</td>
</tr>
<tr>
<td>3</td>
<td>An error is reported for Sam Cole's mailbox and the archiving task stops, because no default ruleset file or custom properties file exists.</td>
</tr>
<tr>
<td>4</td>
<td>John Doe's mailbox is archived according to rules in John Doe.xml and Sam Cole's mailbox is archived according to the default Exchange mailbox policy. Missing defaults are ignored.</td>
</tr>
<tr>
<td>5</td>
<td>John Doe's mailbox is archived according to rules in John Doe.xml and Sam Cole's mailbox is archived according to the rules in Default Filter Rules.xml. No custom properties are indexed. Content categories cannot be used.</td>
</tr>
<tr>
<td>6</td>
<td>As for case 5. The fact that IGNORENODEFAULT is set makes no difference.</td>
</tr>
<tr>
<td>7</td>
<td>An error is reported for John Doe's mailbox and the archiving task stops, because there is no applicable named ruleset file or default ruleset file or custom property file.</td>
</tr>
<tr>
<td>8</td>
<td>John Doe's mailbox is archived according to rules in the default Exchange mailbox policy. Sam Cole's mailbox is archived according to the rules in Sam Cole.xml.</td>
</tr>
<tr>
<td>9</td>
<td>All messages are archived from John Doe's mailbox and custom properties indexed. Messages are archived from Sam Cole's mailbox according to the rules in Sam Cole.xml.</td>
</tr>
<tr>
<td>10</td>
<td>As for case 9. The fact that IGNORENODEFAULT is set makes no difference.</td>
</tr>
</tbody>
</table>
General format of custom properties.xml

For Enterprise Vault to access and index additional custom or standard MAPI properties on Exchange Server messages or additional properties on Domino server messages, the properties must be defined in the file, custom properties.xml, which you create in the Enterprise Vault\Custom Filter Rules folder on the computer running the archiving tasks enabled for custom filtering. The installed file, Enterprise Vault\Custom Filter Rules\Example Custom Properties.xml provides an example of this file.

If this file is to contain non-ANSI characters, ensure the correct encoding is set on the first line and save the file as a Unicode file.

The file has three sections:

- `<CONTENTCATEGORIES></CONTENTCATEGORIES>` This section defines available content categories. A content category is a group of settings that will be applied to an item when it is archived. This can include custom properties to index. The entries are described in “Defining content categories” on page 390.

- `<CUSTOMPROPERTIES></CUSTOMPROPERTIES>` This section defines the additional message properties that are to be available to Enterprise Vault. The entries are described in “Defining additional properties to index” on page 386.

- `<PRESENTATION></PRESENTATION>` This section defines how the content categories and custom properties are displayed to users in external applications, such as the Enterprise Vault Web Access application browser search. The entries are described in “Defining how properties are presented in applications” on page 393.

**Note:** The order of these sections is significant.
The following outline shows the general format of the file:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<CUSTOMPROPERTYMETADATA
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="customproperties.xsd">

<!-- 1. DEFINITION OF CONTENT CATEGORIES AVAILABLE -->
<CONTENTCATEGORIES>
  <CONTENTCATEGORY> ... </CONTENTCATEGORY>
  [...CONTENTCATEGORY> ... </CONTENTCATEGORY>
</CONTENTCATEGORIES>

<!-- 2. DEFINITION OF CUSTOM PROPERTIES AVAILABLE -->
<CUSTOMPROPERTIES>
  <NAMESPACE> ... </NAMESPACE>
  [...NAMESPACE> ... </NAMESPACE>
</CUSTOMPROPERTIES>

<!-- 3. DEFINITION OF PRESENTATION PROPERTIES AVAILABLE -->
<PRESENTATION>
  <APPLICATION>
    <FIELDGROUPS>
      <FIELDGROUP> ... </FIELDGROUP>
      [...FIELDGROUP> ... </FIELDGROUP>
    </FIELDGROUPS>
    <AVAILABLECATEGORIES>
      <AVAILABLECATEGORY> ... </AVAILABLECATEGORY>
      [...AVAILABLECATEGORY> ... </AVAILABLECATEGORY>
    </AVAILABLECATEGORIES>
  </APPLICATION>
  [...APPLICATION> ... </APPLICATION>
</PRESENTATION>
```

The table “XML elements and attributes in the custom properties.xml file” on page 399 gives a summary description of all mandatory and optional elements and attributes in the file.

Whenever you modify the file, you must restart the associated archiving tasks. In a distributed environment, you must copy the updated file to each computer with tasks enabled for custom properties, and then restart the associated tasks on each computer.

If the browser search is being used to search for custom properties, then the Enterprise Vault Application Pool in IIS Manager must also be restarted.

How to validate custom properties.xml

When Enterprise Vault is installed, customproperties.xsd is placed in the Custom Filter Rules folder. This is the XML schema for validating custom properties.xml.
The schema file must be referenced in the CUSTOMPROPERTYMETADATA entry at the start of the custom properties.xml file, as follows:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<CUSTOMPROPERTYMETADATA
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="customproperties.xsd">
```

The XML is validated when the associated task starts processing messages. If anything is invalid, the task stops and you must correct any errors before restarting the task.

To avoid disrupting tasks because of syntactic errors, it is a good idea to validate your XML file before it is accessed by the tasks. You could use a third party tool, such as xsdvalidator:


When using the tool, specify the namespace as:

x-schema:customproperties.xsd

---

**Note:** All the XML tags and predefined values shown in upper case in this document are case sensitive and must be entered as upper case in the file. Values entered should also be treated as case sensitive.

---

### Defining additional properties to index

In the `<CUSTOMPROPERTIES>` section of custom properties.xml, you define the additional message properties that you want Enterprise Vault to evaluate or index. For Exchange Server messages, you define MAPI properties, as described in “MAPI properties”. You can also define additional Domino server properties, as described in “Domino properties” on page 388.

#### MAPI properties

Before MAPI properties can be defined in custom properties.xml, they must be defined in the MAPI subsystem. Currently, the Enterprise Vault custom properties feature supports only STRING and DOUBLE properties. Enterprise Vault supports single or multi-valued properties.

In MAPI, properties are grouped by NAMESPACE. Typically, properties accessed by a particular application are defined in the same namespace. Each namespace is identified by a GUID. Each property is defined by its STRING ID and namespace GUID.

For each property that you want to include, you will need the following details from the property definition in the MAPI subsystem:
Configuring custom properties
Defining additional properties to index

- If the property is a standard MAPI property, the Identifier part (bits 16 to 31) of the hexadecimal MAPI tag. For example, if the MAPI tag for the standard property is 0x0070001E, the Enterprise Vault NAME value would be 0x0070.

- If the property is a custom property, the GUID of the property's namespace.

- If the property is a custom property, the property's STRING ID. If the property is a named property, the ID will be a name. For example, the named MAPI property that holds Outlook categories is Keywords.

You can use third party MAPI tools, such as OutlookSpy, to view the MAPI properties associated with mailbox items. The following figure shows how MAPI properties on a message are displayed in OutlookSpy. The selected property is the named property, Keywords. This multi-valued property holds the Outlook categories assigned to the message. Details of the selected property are displayed on the right-hand side of the window.

Figure 32-1   Viewing MAPI properties

To make MAPI properties available to Enterprise Vault, you define them in the <CUSTOMPROPERTIES> section of custom properties.xml. The properties defined in this section can then be referenced in the content category and presentation sections.

Here is an example showing how properties can be defined:

```xml
<!-- 2. DEFINITION OF CUSTOM PROPERTIES AVAILABLE -->

<CUSTOMPROPERTIES>
  <NAMESPACE TYPE="MAPI"
    GUID="{DA6007CD-01AA-408f-B7D3-6DA958A09583}"
  >
    <PROPERTY NAME="Author1" TAG="CaseAuthor"/>
    <PROPERTY NAME="Status1" TAG="CaseStatus"/>
  </NAMESPACE>

  <NAMESPACE TYPE="MAPI"
    GUID="{EF1A0001-01AA-408f-B7D3-6DA958A09583}"
  >
    <PROPERTY NAME="Author2" TAG="Client"/>
  </NAMESPACE>
</CUSTOMPROPERTIES>
```
Configuring custom properties

Defining additional properties to index

In this example there are four NAMESPACES. The first three define custom MAPI properties, so the GUID of the NAMESPACE is required. As the properties defined in the fourth NAMESPACE are standard MAPI properties, no GUID is required.

The value of the TYPE attribute identifies the property type; in this example, the properties are MAPI properties.

Within each NAMESPACE the properties are defined in PROPERTY elements using NAME and TAG values.

- If the property is a custom MAPI property, NAME is the STRING ID defined in the MAPI subsystem. The value is case sensitive and must match exactly the value in the MAPI subsystem.
  
  If the property is a standard MAPI property, NAME is the Identifier part (bits 16 to 31) of the hexadecimal MAPI tag.

- TAG identifies the property within Enterprise Vault. It can contain only alphanumeric characters (A-Z, a-z, or 0-9); spaces and underscore characters are not permitted. The value assigned to the property TAG must be unique within the XML file; although you can cross refer to the property using the TAG value, the same value cannot be used to identify any other entities in the file.

  If you want to select messages by matching the values of specific properties, you need to create a <NAMEDPROP> filter in the appropriate XML ruleset file and specify the TAG value defined here. See “Filtering on MAPI named properties” on page 365.

Domino properties

To include custom Domino message properties in Enterprise Vault indexes, you define the required properties in custom properties.xml.
In the Lotus Notes client, you can view Domino properties on a message as shown in the figure, “Viewing Domino message properties”.

Figure 32-2 Viewing Domino message properties

To view Domino message properties

1. In the Lotus Notes client, right-click the message.
2. Select Document Properties in the menu.
3. Select the fields tab in the dialog that is displayed.

The property names are listed in the left-hand pane. When you select a property in the left-hand pane, details of that property are displayed in the right-hand pane.

To make Domino message properties available to Enterprise Vault, you define them in the <CUSTOMPROPERTIES> section of custom properties.xml. The properties defined in this section can then be referenced in the content category and presentation sections.

The properties are grouped using the <NAMESPACE> element. Typically, properties accessed by a particular application are defined in the same namespace.
This outline of the custom properties section shows how Domino properties are defined:

```xml
<CUSTOMPROPERTIES>
  <NAMESPACE TYPE="LOTUS">
    <PROPERTY NAME="Domino_prop_name" LOTUSTYPE="Domino_data_type"
      TAG="EV_prop_name"/>
  </NAMESPACE>
</CUSTOMPROPERTIES>
```

The `TYPE="LOTUS"` identifies the property as a Domino property. Within each `<NAMESPACE>` element, the properties are defined in `<PROPERTY>` elements using `NAME` and `TAG` attributes.

- In `NAME="Domino_prop_name"`, the value is the property name displayed in the Lotus Notes document properties. The value is case sensitive and must match exactly the value displayed in the Lotus Notes client.
- `LOTUSTYPE="Domino_data_type"` identifies the property data type. The following types are supported: "TEXT", "NUMBER", "TIME". Enterprise Vault indexes "NUMBER" properties as integers.
- `TAG` identifies the property within Enterprise Vault. It can contain only alphanumeric characters (A-Z a-z 0-9); spaces and underscore characters are not permitted. The value assigned to the property `TAG` must be unique within the XML file; although you can cross refer to the property using the `TAG` value, the same value cannot be used to identify any other entities in the file.

### Defining content categories

In the `<CONTENTCATEGORIES>` section of `custom_properties.xml`, you define the content categories that you want to apply to filtered messages.

A content category defines a group of settings that are to be applied to an item when it is archived. The settings can include the following information:

- The retention category to assign to the item
- The destination archive
- A list of the additional message properties that Enterprise Vault is to index

There can be more than one content category defined in the `<CONTENTCATEGORIES>` element.

In ruleset files, the actions associated with a rule can include assigning a particular content category to messages that satisfy the rule. The content
Configuring custom properties

Defining content categories

category definition in custom properties.xml provides the default settings for the content category. Some of these can be overridden for particular rules, as described in "Assigning content categories in rules" on page 392.

The following example shows entries for a content category called Litigation:

```xml
<!-- 1. DEFINITION OF CONTENT CATEGORIES AVAILABLE -->

<CONTENTCATEGORIES DEFAULT="Litigation">
  <CONTENTCATEGORY NAME="Litigation" RETENTIONCATEGORY="Litigation"
ARCHIVEID="15165263832890493848568161447.server1.local">
    <INDEXPROPERTIES RETRIEVE="Y">
      <PROPERTY TAG="CaseAuthor"/>
      <PROPERTY TAG="CaseStatus"/>
    </INDEXPROPERTIES>
  </CONTENTCATEGORY>
</CONTENTCATEGORIES>

■ <CONTENTCATEGORIES></CONTENTCATEGORIES> defines the content category section in the file.

■ The DEFAULT attribute specifies the content category to be used as the default. This default applies to all types of archiving enabled for custom filtering.

This attribute is optional, if custom filtering is used, but mandatory if there are no ruleset files (unless the registry setting IGNORENODEFAULT is configured).

If filters are configured in ruleset files and a default content category is specified, any item that does not match any rules will be archived according to the settings in the default content category. If no default content category is specified, then a content category will only be applied to an item if specified by a matching rule in a filter ruleset file.

If no applicable ruleset files exist, then you must specify a default content category using the DEFAULT attribute in the <CONTENTCATEGORIES> element in custom properties.xml. The settings in the content category are then applied to all messages archived (unless the registry setting IGNORENODEFAULT is configured).

The actions of archiving tasks are determined by combinations of ruleset files, custom properties, content categories and the registry setting IGNORENODEFAULT. For details of different configuration combinations and their effect, see "Controlling default settings" on page 379.

■ The <CONTENTCATEGORY> element defines a particular content category. There must be at least one content category defined.

■ The content category NAME is used to identify this content category in the presentation section of the file, rules in custom filter ruleset files and external subsystems, such as the Enterprise Vault Indexing service. The
name can include alphanumeric characters only (A-Z a-z 0-9); space and underscore characters are not permitted.
If the content category is included in the presentation section of the file, it will be possible to search on the content category name in order to find all items archived using this particular content category.

- RETENTIONCATEGORY is optional and enables you to assign a retention category to each item archived using this content category. The retention category must already exist in Enterprise Vault.
- ARCHIVEID is optional and enables you to specify a destination archive for the item. The archive must exist and be enabled. To find the ID of an archive, display the archive properties in the administration console and click the Advanced tab.
- The <INDEXEDPROPERTIES> element is mandatory and groups the additional properties that Enterprise Vault is to index.
- The RETRIEVE attribute (optional) determines whether or not the defined properties should be returned with archive search results. By default, the properties are not displayed with search results (RETRIEVE="N")
- A <PROPERTY> element is required for each additional property to be indexed.
- The TAG value must match the associated Enterprise Vault TAG value specified in the custom properties section, see “Defining additional properties to index” on page 386.

Assigning content categories in rules

The preferred way to specify the actions to be taken for messages that match a filter rule is to assign a content category in the rule, in the ruleset file. You define the default settings included in a content category in the content categories section of custom properties.xml.

In the ruleset file, you assign a content category as follows:

```
<RULE NAME="Example rule" ACTION="ARCHIVE_ITEM"
   CONTENTCATEGORY="content_category_name">
   <message attribute filters>
   </RULE>
```

The value of 'content_category_name' is the name of the required content category as specified in custom properties.xml.

In the ruleset file, content categories can only be assigned when ACTION="ARCHIVE_ITEM".
Overriding default content category settings

A rule can assign a content category and override some of the default content category settings. For example, if you have a content category that defines all the custom properties to index, a retention category and a destination archive, different rules can assign the content category but override values for the archive or retention category, as required.

For example, if a content category called Litigation is defined in custom properties.xml as follows:

```xml
<CONTENTCATEGORY NAME="Litigation" RETENTIONCATEGORY="Litigation" ARCHIVEID="15165263832890493848568161647.server1.local">
  <INDEXEDPROPERTIES RETRIEVE="Y">
    <PROPERTY TAG="AUTHOR01"/>
    <PROPERTY TAG="CASESTATUS"/>
  </INDEXEDPROPERTIES>
</CONTENTCATEGORY>
```

It can be referenced in a ruleset file as follows:

```xml
<RULE NAME="Example rule1" ACTION="ARCHIVE_ITEM" CONTENTCATEGORY="Litigation">
  <message attribute filters>
</RULE>
```

```xml
<RULE NAME="Example rule2" ACTION="ARCHIVE_ITEM" CONTENTCATEGORY="Litigation" ARCHIVEID="1516526383289049384890493848.server2.local">
  <message attribute filters>
</RULE>
```

Additional properties defined in the content category will be indexed with both rules. The second rule uses the same content category, but items that match this rule will be stored in a different archive.

---

**Caution:** Before you alter an existing configuration, make sure that you understand what default behavior has been configured for each type of archiving. Check the DEFAULT content category attribute in custom properties.xml and the IGNORENODEFAULT registry setting. For information on how default behavior is configured, see “Controlling default settings” on page 379.

---

Defining how properties are presented in applications

The presentation section of the file, `<PRESENTATION>`, defines how available content categories and custom properties are presented to external applications, such as an archive search engine.
Separating the presentation of properties from the underlying property definitions enables flexible mapping of custom property details onto a user interface. This also facilitates the support of multiple languages.

To access the custom property information in the `custom properties.xml` file, external applications must use the custom filter and property API. For details of this API, see the Enterprise Vault Application Programmer's Guide.

Entries in the presentation section define the following:

- Custom properties available for displaying by the named application
- How properties are to be grouped and displayed in the application
- Content categories available to the application
- How each content category should be displayed in the application

Presentation information can be defined for each application that will require access to custom properties in archived items.

Here is an example of a presentation section (partially completed) that shows how to define how custom properties are displayed in the Enterprise Vault browser search application:

```xml
<!-- 3. DEFINITION OF PRESENTATION PROPERTIES AVAILABLE -->

<PRESENTATION>
  <APPLICATION NAME="search.asp" LOCALE="1033">
    <FIELDGROUPS>
      <FIELDGROUP LABEL="Case Properties">
        <FIELD TAG="CaseAuthor" LABEL="Author" CATEGORY="Litigation"/>
        <FIELD TAG="CaseStatus" LABEL="Status" CATEGORY="Litigation"/>
      </FIELDGROUP>
      <FIELDGROUP LABEL="Client Properties">
        <FIELD TAG="Client" LABEL="Client Name" CATEGORY="ClientAction"/>
        <FIELD TAG="Topic" LABEL="Message Topic" CATEGORY="ClientAction"/>
      </FIELDGROUP>
    </FIELDGROUPS>
    <AVAILABLECATEGORIES>
      <AVAILABLECATEGORY CONTENTCATEGORY="Litigation" LABEL="Litigation"/>
      <AVAILABLECATEGORY CONTENTCATEGORY="ClientAction" LABEL="Client Action"/>
    </AVAILABLECATEGORIES>
  </APPLICATION>
</PRESENTATION>
```
The example shows entries for two applications — the US English (locale “1033”) version of the Enterprise Vault browser search and a Japanese (locale “1041”) version of a proprietary application. In this particular case, the same elements and attributes have been specified for both applications, but the LABEL values for the second application (omitted in the example) would be in Japanese.

- The properties available to each application are grouped using the `<APPLICATION>` element.
- The NAME attribute identifies the application.
- The value of the LOCALE attribute is defined by the calling application. The Enterprise Vault browser search uses the standard Microsoft Locale ID for the language that the application will use: 1033 represents US English. The second application in the example, mysearch.asp, also uses the Microsoft Locale ID; 1041 represents Japanese.

In the web search page, custom properties are displayed in groups defined by their content category; that is, when a particular content category is selected, the custom properties with that content category are displayed.

- The `<FIELDGROUPS>` element is used to define all the groups of custom properties to be displayed.
Each group is defined in a `<FIELDGROUP>` element. The `LABEL` attribute gives the title that will be displayed in the application for the group of properties. The value of the `LABEL` attribute must be unique in the application.

- `<FIELD>` elements define each property to be displayed in the group. The value of the `TAG` attribute identifies the property to be displayed. The value specified here must match the associated `TAG` value of the property in the `<CUSTOMPROPERTIES>` section of the file. The value of the `CATEGORY` attribute identifies the content category with which this property is to be associated. When the user selects this content category in the search criteria, a box for this property will be displayed. The value specified for `CATEGORY` must match the associated `NAME` for the content category in the content category section of the file. Also, `CATEGORY` must be one defined in the `<AVAILABLECATEGORIES>` element.
  
  - `TAG` must be unique in the `<FIELDGROUP>` and the `TAG/CATEGORY` combination must be unique within the `<APPLICATION>` element.
  - `LABEL` defines the name that you want displayed in the user interface for the custom property.

- `<AVAILABLECATEGORIES>` groups the content categories that are to be available for selection in the application. Each content category is defined using the `<AVAILABLECATEGORY>` element; the value of the `CONTENTCATEGORY` attribute must match the name of the content category specified in the content category section of the file. The `LABEL` attribute defines the name you want displayed for the content category in the user interface.

### Displaying custom properties in the browser search

The Enterprise Vault browser search application uses the custom filter and properties API to access custom properties defined in the `custom properties.xml` file. This section shows how the example presentation section entries in "Defining how properties are presented in applications" on page 393 would be displayed in the US English version of this application.

The figure, "Example presentation properties displayed in the browser search page", shows the Enterprise Vault browser search with the example custom properties and content categories displayed.
Configuring custom properties
Defining how properties are presented in applications

Figure 32-3  Example presentation properties displayed in the browser search page

![Search interface with custom properties]

The **Content Category** dropdown box shows the content categories available to be used in searches. These were defined using the `<AVAILABLECATEGORIES>` element. You can change the content categories listed in the dropdown box, but you cannot change or hide the label, **Content Category**.

Selecting a content category in the box and clicking **Search** will return all items that were archived with the selected content category.

The **Case Properties** and **Client Properties** sections display each group of custom properties (FIELDGROUP) associated with the selected content category. Entering a value for a custom property and clicking **Search** will search the custom property index entry of archived items.

To see the additional property details in the search results, **Details** must be set to **Full**.

If the user selects a different content category, the custom properties available will change.

As RETRIEVE="Y" was set in the definition of the **Litigation** content category (see “Defining content categories” on page 390), and **Details** was set to **Full** on the Search page, custom properties in search result items will be displayed at the end of the list of normal message attributes, as shown in the figure, “Custom properties displayed in search results”.
Configuring custom properties

Summary of Custom Property Elements and Attributes

Figure 32-4  Custom properties displayed in search results

Notes on displaying custom properties in browser search

- You must include the LOCALE attribute.
- If custom properties are to be used in the Enterprise Vault browser search, Internet Explorer security settings must allow cookies for the Enterprise Vault server site.
- When changes are made to the custom property configuration, you need to restart the Enterprise Vault Application Pool in IIS Manager.
- If the contents of the custom properties.xml file is changed, searches may return different results. For example, if an item is indexed using one content category and the properties included in the content category are changed, the custom properties returned by subsequent searches will be different. To ensure you can still search on the original properties, leave the original content category and create a new one.

Summary of Custom Property Elements and Attributes

The table “XML elements and attributes in the custom properties.xml file” summarizes all elements and attributes in custom properties.xml. The
value in the **Mandatory** column assumes that the IGNORENODEFAULT registry setting is not used.

### Table 32-3 XML elements and attributes in the custom properties.xml file

<table>
<thead>
<tr>
<th>Element</th>
<th>Attribute</th>
<th>Mandatory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONTENTCATEGORIES</td>
<td></td>
<td>Yes</td>
<td>Defines the content category section of the file.</td>
</tr>
<tr>
<td>DEFAULT=</td>
<td>No</td>
<td></td>
<td>Value is the name of the content category to be used as default. Required if custom properties in all items are to be indexed.</td>
</tr>
<tr>
<td>CONTENTCATEGORY</td>
<td>Yes</td>
<td></td>
<td>Defines a group of settings that are to be assigned to an archived item.</td>
</tr>
<tr>
<td>NAME=</td>
<td>Yes</td>
<td></td>
<td>Value is a unique name to identify category to ruleset and presentation interface.</td>
</tr>
<tr>
<td>RETENTIONCATEGORY=</td>
<td>No</td>
<td></td>
<td>Value is a Retention Category to be assigned to the archived item. Retention Category must exist in Enterprise Vault.</td>
</tr>
<tr>
<td>ARCHIVEID=</td>
<td>No</td>
<td></td>
<td>Value is the ID of the archive to store the item in. Value can be found in the properties of the archive in the Enterprise Vault Administration Console.</td>
</tr>
<tr>
<td>INDEXEDPROPERTIES</td>
<td>Yes</td>
<td></td>
<td>Defines a set of additional properties in the content category.</td>
</tr>
<tr>
<td>RETRIEVE=</td>
<td>No</td>
<td></td>
<td>Value is “Y” or “N”. Indicates whether or not properties in this set should appear in the search results. Default is “N”.</td>
</tr>
<tr>
<td>PROPERTY</td>
<td>Yes</td>
<td></td>
<td>Defines an additional property to index for items that are assigned this content category.</td>
</tr>
<tr>
<td>TAG=</td>
<td>Yes</td>
<td></td>
<td>Value is the Enterprise Vault TAG of the property.</td>
</tr>
<tr>
<td>CUSTOMPROPERTIES</td>
<td>Yes</td>
<td></td>
<td>Defines the custom property section of the file.</td>
</tr>
<tr>
<td>NAMESPACE</td>
<td>Yes</td>
<td></td>
<td>Defines a NAMESPACE that contains a group of custom properties.</td>
</tr>
<tr>
<td>TYPE=</td>
<td>Yes</td>
<td></td>
<td>Type of property. Value can be “MAPI” or “LOTUS”.</td>
</tr>
</tbody>
</table>
### Table 32-3

XML elements and attributes in the custom properties.xml file

<table>
<thead>
<tr>
<th>Element</th>
<th>Attribute</th>
<th>Mandatory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUID=</td>
<td>Yes</td>
<td>MAPI properties only. Value is identity of NAMESPACE to external applications.</td>
<td></td>
</tr>
<tr>
<td>PROPERTY</td>
<td>Yes</td>
<td>Defines a custom property.</td>
<td></td>
</tr>
<tr>
<td>NAME=</td>
<td>Yes</td>
<td>If the property is a custom MAPI property, value is the STRING ID defined in the MAPI subsystem. The value is case sensitive and must match exactly the value in the MAPI subsystem. If the property is a standard MAPI property, value is the Identifier part (bits 16 to 31) of the hexadecimal MAPI tag. If the property is a Domino property, value is the identity of the property as displayed in message properties in the Lotus Notes client. Value must be unique in NAMESPACE.</td>
<td></td>
</tr>
<tr>
<td>LOTUSTYPE=</td>
<td>Yes</td>
<td>Value is the Domino property data type: “TEXT”, “NUMBER” or “TIME”.</td>
<td></td>
</tr>
<tr>
<td>TAG=</td>
<td>Yes</td>
<td>TAG identifies the property within Enterprise Vault. It can contain only alphanumeric characters (A-Z a-z 0-9); spaces and underscore characters are not permitted. The value must be unique within the XML file. TAG value is the property name that will be stored in the index.</td>
<td></td>
</tr>
<tr>
<td>PRESENTATION</td>
<td>Yes</td>
<td>Defines the presentation property section of the file.</td>
<td></td>
</tr>
<tr>
<td>APPLICATION</td>
<td>Yes</td>
<td>Defines a group of fields for use by a named application.</td>
<td></td>
</tr>
<tr>
<td>NAME=</td>
<td>Yes</td>
<td>Value is the name of the application that will use the fields in this definition.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 32-3 XML elements and attributes in the custom properties.xml file

<table>
<thead>
<tr>
<th>Element</th>
<th>Attribute</th>
<th>Mandatory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOCALE=</td>
<td>Yes</td>
<td></td>
<td>The value depends on what the calling application requires to define the language. The Enterprise Vault browser search uses standard Microsoft Locale ID number that the application will run under. (Currently only “1033”, US English, is supported for displaying custom properties in the browser search.)</td>
</tr>
<tr>
<td>FIELDGROUPS</td>
<td>Yes</td>
<td></td>
<td>Define the field groups available to the application.</td>
</tr>
<tr>
<td>FIELDGROUP</td>
<td>Yes</td>
<td></td>
<td>A logical grouping of fields for the presentation interface.</td>
</tr>
<tr>
<td>LABEL=</td>
<td>No</td>
<td></td>
<td>Value will be presented to the application for this field group. The label must be unique within the application.</td>
</tr>
<tr>
<td>FIELD</td>
<td>Yes</td>
<td></td>
<td>Defines a field that will reference a custom property.</td>
</tr>
<tr>
<td>LABEL=</td>
<td>Yes</td>
<td></td>
<td>Value will be displayed on the application user interface to represent this custom property.</td>
</tr>
<tr>
<td>CATEGORY=</td>
<td>Yes</td>
<td></td>
<td>Value is the name of a content category listed in AVAILABLECATEGORIES for the application.</td>
</tr>
<tr>
<td>TAG=</td>
<td>Yes</td>
<td></td>
<td>Value is the TAG of a custom property. The tag must be unique in the FIELDGROUP.</td>
</tr>
<tr>
<td>AVAILABLECATEGORIES</td>
<td>Yes</td>
<td></td>
<td>Define which content categories are available to the application.</td>
</tr>
<tr>
<td>AVAILABLECATEGORY</td>
<td>Yes</td>
<td></td>
<td>Defines a content category.</td>
</tr>
<tr>
<td>LABEL=</td>
<td>Yes</td>
<td></td>
<td>Value defines how the content category is to appear in the user interface.</td>
</tr>
<tr>
<td>CONTENTCATEGORY=</td>
<td>Yes</td>
<td></td>
<td>Value is the NAME of the required content category as specified in the Content Category section of the file.</td>
</tr>
</tbody>
</table>
Configuring custom properties

Summary of Custom Property Elements and Attributes
Appendices

This section includes the following appendices:

- Appendix A, "Envelop Journaling" on page 405
- Appendix B, "Configuring NetBackup Server" on page 413
- Appendix C, "Integrating IBM Tivoli Storage Manager" on page 425
Envelope Journaling

Envelope Journaling is an optional feature for Exchange 2000 and Exchange Server 2003 that enables the capture of the complete recipient list. Prior to this, BCC recipients were captured, but alternate and undisclosed recipients were not. For Exchange Server 2003, Envelope Journaling is included in SP1.

An alternate recipient is a second mailbox to which all messages for a particular recipient are redirected.

An undisclosed recipient is usually a BCC recipient that has been sent over SMTP. The recipient address is not recorded on the final SMTP message, so it is not easy to tell the original, intended destination of the message when it arrives in the Journal mailbox.

For details of how to enable Envelope Journaling on Exchange 2000, see the Microsoft Knowledge Base Article 843105.

Envelope Journaling can later be disabled, if required, using a tool supplied by Microsoft. If you disable Envelope Journaling, the previous method of Journaling continues, unaffected, together with the option to preserve BCC information, which you can configure using a registry setting.

Format of Envelope Journaled messages

When Envelope Journaling is enabled, the original message is stored as an attachment to another message that shows the original message’s recipient information in its body. This information is a complete list of recipients and will include BCCs, Alternate Recipients, and Undisclosed Recipients.

The following sections illustrate the format of messages as they arrive in the Journal mailbox, when Envelope Journaling is enabled. In the first example, the message is sent over SMTP and in the second example, the message is sent over an Exchange Server intranet.
Example 1: Message sent over SMTP

The figure below shows the original message; the recipient list includes a distribution list and a BCC.

**Figure A-1** The original message

When this message is sent over SMTP, it arrives in the Journal mailbox in the form shown in the figure below.

**Figure A-2** The envelope message in the Journal mailbox

The top level message is actually the envelope message and the original message is attached. The contents of the envelope message include:
The sender

The message ID

All the message recipients, including any BCC, Alternate or Undisclosed Recipients

Note that the BCC field does not appear in the envelope message header and that the distribution list has been expanded and the list members included as recipients.

“The attached message” shows the attached message.

Example 2: Message sent over an intranet

In this example, a message with the same recipients as before is sent over an internal Exchange network. The figure below shows the original message.
When this message is sent, it arrives in the Journal mailbox in the form shown below.

The top level message is the envelope message and the original message is attached. The contents of the envelope message are the same as in the previous example:

- The sender
- The message ID
■ All the message recipients, including any BCC, Alternate or Undisclosed Recipients

Note that the BCC field does not appear in the envelope message header and that the distribution list has been expanded and the list members included as recipients.

The figure below shows the attached message on an Exchange 2000 system.

**Figure A-6** The attached message (Exchange 2000)

![Envelope Journaling Test](image)

Note that on Exchange Server 2000 the BCC entry is displayed correctly in the header of the attached message, as shown in "The attached message (Exchange 2000)". On Exchange 2003, BCC recipients become Undisclosed Recipients and are not displayed as BCC recipients in the header of the attached message.

**Performance**

The additional processing required for the envelope message means that the Envelope Journaling feature will impact journaling performance on the server.

**Enterprise Vault and Envelope Journaling**

Nothing needs to be enabled on the Enterprise Vault server; the Enterprise Vault Journaling task automatically recognizes an envelope message and processes it accordingly.

If Envelope Journaling has been enabled on the Exchange Server, but the Enterprise Vault system has not been upgraded to a version that supports the feature, the Enterprise Vault Journaling task will continue to archive messages when they appear in the journal mailbox, but note the following:
Only the recipient list in the header of the envelope message will be processed, so some information such as internal BCC recipients and Undisclosed recipients may be missed.

Information may not be indexed in the correct way (for example, the recipient list in the envelope message body). Instead, the contents of the envelope message will just be indexed in the normal way, which is meaningless in this case.

Selective or Group Journaling filters may not work as expected.

The following steps give an overview of how the Enterprise Vault Journaling task handles the envelope messages.

1. The complete list of recipients is extracted from the envelope message contents. This list is compared with recipients in the header of the attached message. Recipients found in the envelope message but not the attached message header will be classed as Undisclosed Recipients.

2. In most cases, Undisclosed Recipients will be indexed and stored under the new recipient category, Undisclosed. Exceptions to this are discussed in “When recipients are stored as Undisclosed” on page 410. You can search for Undisclosed Recipients using a new option box in the Recipient field of the advanced page of the Enterprise Vault browser search. Undisclosed recipients will also be recognized in Compliance and Discovery Accelerator searches.
   The search index property, RNDN, will be used for Undisclosed Recipients.

3. A copy of the envelope message, complete with original message attached, will be passed to any external filters (for selective journaling or the Compliance Accelerator Journaling Connector). See “Journal Filters with Envelope Journaling” on page 329 for more information on the support of external filters with Envelope Journaling.

4. If the message is to be archived, only the original message will be stored in the Journal archive, not the envelope message.

When recipients are stored as Undisclosed

As shown in “Format of Envelope Journaled messages” on page 405, when messages are addressed to Alternate Recipients and BCC recipients and sent over SMTP, these recipients will be included in the general recipient list in the envelope message content but not in the message headers of the original message. As there is no way of discovering the original category of such recipients, Enterprise Vault will store them as Undisclosed Recipients.
Note if messages sent over an Exchange Server 2000 intranet include BCC recipients, then Enterprise Vault can identify and store these recipients as BCC and not Undisclosed Recipients.

If a BCC recipient is also in the TO or CC fields and the message arrives over SMTP, then Enterprise Vault will store the recipient in the TO or CC field but not in the Undisclosed field.

When a message is redirected to an Alternate Recipient (that is, forwarded to the Alternate recipient without actually being delivered to the original recipient), then the message headers will show the originally intended recipient and not the final (Alternate) recipient. Both recipients will be indexed, even though the originally intended recipient never actually received the message. This is because it is not possible to determine from the journal message that the original recipient was skipped.

If an Alternate recipient also appears as an originally intended recipient (TO or CC), then the recipient will not be stored as an Undisclosed Recipient.
Envelop Journaling
Enterprise Vault and Envelope Journaling
Configuring NetBackup Server

This appendix describes how to configure Enterprise Vault and VERITAS NetBackup™ Server so that Collection files can be migrated to NetBackup Server. Enterprise Vault supports versions 5.1 and 6.0 of VERITAS NetBackup Server.

In summary, the procedure is:

■ Configure a NetBackup Server Policy for Enterprise Vault
■ Create a new Enterprise Vault vault store partition, or modify an existing NTFS partition, specifying NetBackup as the migrator software

Prerequisites

Before configuring Enterprise Vault to work with NetBackup Server you must have the following:

■ Enterprise Vault 6.0 or later installed and configured, with the OSL Collector Migrator component included in the Enterprise Vault license keys file.
■ NetBackup Server installed and configured, including devices, media, and storage units.
■ On the server that runs the Enterprise Vault Storage service, any version of NetBackup Client that is supported by NetBackup Server.

Setting client software path for NetBackup Server 6.0

If you are using NetBackup Server 6.0, you need to add the NetBackup client software path to the operating system path variable on the Enterprise Vault Server.
To add the client software path:

1. Open the Control Panel and then open System Properties.
2. Click the Advanced tab and then click Environment Variables.
3. In the System Variables box, click Path and then click Edit.
4. Add the path to the xbsa.dll file, which is the binary path for the NetBackup client. For example, "c:\Program Files\VERITAS\netbackup\bin"
5. Click OK three times.
6. Reboot the system.
7. Test the connection from the Enterprise Vault server.

Creating a NetBackup Server Policy

You must create a NetBackup Server policy for use with Enterprise Vault. The policy must have a schedule that makes NetBackup Server available all the time.

Preparation

Before you can configure NetBackup Server for use with Enterprise Vault you must do the following:

- Activate the NetBackup Server DataStore feature. If the feature is not present and active you must obtain and enter the key to enable it. If you do not already have the key, use the following: DRX6-3HWU-R3CT-9PCR-PPPP-JC6P-PPP6-PPPP-RP
  To check whether the DataStore feature is already active, click Help and then License Keys in the NetBackup Administration Console. When the license keys are shown, select Summary of active licensed features.

Creating a new policy

Create a new NetBackup Server policy with the following features:

- **Policy type**: set to DataStore.
- **Policy name**: Any valid policy name. Use this later, when you configure the Enterprise Vault partition. The default name used by Enterprise Vault is EV_Default_Policy.
  The following sections show the settings you must specify for the policy.
Policy properties — Attributes
On the Attributes tab, configure the following:

- **Policy type**: Select DataStore.
- **Active**: Select this to enable the policy and make sure that the time shown is either current or in the past.

You can modify other options on this tab as required.

Policy properties — Schedules

- The schedule name must reflect the policy name. For example, if the policy name is **EV_Default_Policy**, the schedule name must be **EV_Default_Schedule**.
- On the Schedule Attributes tab, set **Retention** to Infinity.
Configuring an Enterprise Vault vault store partition

- On the Schedule Start Window tab, set **Duration to 7 days**.

Policy properties — Clients
- **Client name**: Set this to be the name of the computer that runs the Enterprise Vault Storage service.

Configuring an Enterprise Vault vault store partition

This section describes how to create a new vault store partition and configure it so that NetBackup Server is used as the migrator software.

There are two ways to create a new partition:
- Create a new vault store: the **New Partition Wizard** starts automatically so that you can create the first partition in the new vault store; see “The New Partition wizard” on page 417.
Create a new partition in an existing vault store: to create a new vault store partition from the Administration Console, right-click the vault store and, on the shortcut menu, click **New** and then **Partition**. The **New Partition** wizard starts; see “The New Partition wizard” on page 417.

It is also possible to modify an existing partition so that collection files can be migrated to NetBackup Server.

To modify an existing partition

1. Double-click the partition to display its properties.
2. Under **File collection software**, click **Change**.
3. Select **Enterprise Vault**, and then click **OK**.
4. Click **OK** to close the partitions' properties.
5. Double-click the partition to display its properties again. There are now three extra property tabs that you can use to configure the partition so that NetBackup Server is used as the migrator software. The settings are the same as those you specify in the wizard when creating a new partition. For details, see the description of the wizard in “The New Partition wizard” on page 417.

The New Partition wizard

1. On the Welcome page, click **Next**.
2. Enter a **Name** and **Description** for the new partition, and then click **Next**.

3. Select a storage type for the new partition, and then click **Next**.

4. Specify the device for the new partition, and then click **Next**.
5 Specify whether to share archived items. Specify whether to create the vault store partition with security ACLs on the folders in the partition, and then click **Next**.

6 Select **Enterprise Vault** as the file collection software to use, and then click **Next**.

7 Specify a time for collections to take place.
Specify the maximum size for collection files, and then click **Next**.

8 Enter the age at which you want files to be collected. Select **Migrate collection files to secondary storage**, and then click **Next**.
9 Select VERITAS NetBackup as the file migrator software, and then click Next.

10 Specify the age at which you want collection files to be migrated by NetBackup.
Specify the age at which you want files to be deleted from the primary storage, and then click Next.
11 Click Finish.

12 Click Close.

The new partition has now been created. You must now modify the properties so that Collection files can be passed to NetBackup Server.

To modify the partition properties

1 In the right pane of the Administration Console, double-click the new partition to display its properties.

2 Click the Advanced tab.

3 In the list, double-click NBU_Policy and then enter the name of the NetBackup Server policy that is to be used with Enterprise Vault. This is the name of the policy that you created on NetBackup Server. Click OK.
4 In the list, double-click **NBU_Server** and then enter the name of the NetBackup Server computer. Click **OK**.

![Vault Store Partition Properties](image)

5 Click **Test** to check that the entries you have made are valid.

6 Click **OK** to close the vault store partition properties.

**Troubleshooting**

Failed to archive: Event 6954

NetBackup Client on the Enterprise Vault server is configured automatically by Enterprise Vault. However, if the configuration is not correct for some reason, errors such as the following are logged:

- **Event Type:** Error
- **Event Source:** Enterprise Vault
- **Event Category:** None
- **Event ID:** 6954
- **Date:** 01/07/2005
- **Time:** 15:59:36
- **User:** N/A
- **Computer:** DEMO

**Description:**
The 3rd party Migrator application 'NBU Migrator' has logged the following message:

Failed to retrieve file (error 00000003: System detected error, operation aborted.). Check the NBU Activity Monitor.
Note that the text of this event can vary, but the event ID is always 6954. Also, it is possible for there to be one item archived successfully and for the remainder to fail.

The most likely cause of this problem is that the NetBackup client does not have the same client name as that specified in the NetBackup Server policy.

To check the NetBackup client configuration

1. On the Enterprise Vault server, start NetBackup client (click Start, then All Programs, then VERITAS NetBackup, then Backup, Archive, and Restore).
3. On the General tab, check that Client name matches the name you entered in the NetBackup Server policy.

4. Try archiving again.

If the problem remains

1. On the Enterprise Vault server, start the registry editor, regedit.
2. Navigate to the following key:
   \HKEY_LOCAL_MACHINE\Software\VERITAS\NetBackup\CurrentVersion\Config
3. Check that the value of Client_Name is exactly the same as the value that is used in the NetBackup Server policy and the NetBackup client.
4. Try archiving again.
Integrating IBM Tivoli Storage Manager

This appendix describes how to configure Enterprise Vault and IBM Tivoli Storage Manager Server (TSM). This enables Enterprise Vault Collection files to be migrated to a storage device. In the instructions given in this appendix, collected files are migrated to an IBM TotalStorage DR550 Storage Device, but this could be some other device.

Prerequisites

- Enterprise Vault 6.0 or later, with the OSL Collector Migrator component included in the Enterprise Vault license keys file.
- IBM Tivoli Storage Manager Server Version 5.2.2 or later.
- IBM Tivoli Storage Manager Backup-Archive Client Version 5.2.2 or later, including the Client API Components. This TSM Client software must be installed on the same computer as the Enterprise Vault Storage service.

Configuring Tivoli Storage Manager Server

To set up Tivoli Storage Manager Server

1. Start the TSM Server management console.
2. Type the following Server Command to set up archive data retention protection:
426

Integrating IBM Tivoli Storage Manager
Configuring Tivoli Storage Manager Server

SET ARCHIVERETENTIONPROTECTION ON

3 Set the following values for the Archive Copy Group that is being used:
   ■ Retain Version = 0
   ■ Retain Minimum Days = 0
   ■ Retention Initiation = EVENT

4 On the TSM Server computer, edit the dsmserver.opt file to set the value of EXPInterval to 1.
   The dsmserver.opt file is in the following folder:
   $TSM_INSTALL_PATH\$SERVER_NAME\dmserv.opt
   For example:
   C:\Program Files\Tivoli\tsm\server2\dmserv.opt
Do the following on the TSM Client computer
1. Add the following to the dsm.opt file:
   ENABLEARCHIVERETENTIONPROTECTION YES
   The dsm.opt file is in the following folder:
   $TSM_INSTALL_PATH\baclient\dsm.opt
   For example:
   C:\Program Files\Tivoli\tsm\baclient\dsm.opt
2. Set the DSMI_CONFIG system environment variable to point to the dsm.opt file.

Configuring an Enterprise Vault vault store partition

This section describes how to create a new vault store partition and configure it so that the required migrator software is used. In the following instructions, IBM TotalStorage DR550 is used as the migrator software.

There are two ways to create a new partition:

- Create a new vault store: the New Partition Wizard starts automatically so that you can create the first partition in the new vault store; see “The New Partition wizard” on page 428.
- Create a new partition in an existing vault store: to create a new vault store partition from the Administration Console, right-click the vault store and, on the shortcut menu, click New and then Partition. The New Partition wizard starts; see “The New Partition wizard” on page 428.

It is also possible for you to modify an existing partition so that Collection files can be migrated to another storage device.

To modify an existing partition
1. Double-click the partition to display its properties.
2. Click Collections tab and select Use collection files.
3. In Collector box, select Enterprise Vault and click OK.
4. Click OK to close the partitions' properties.
5. Double-click the partition to display its properties again. The settings are the same as those you specify in the wizard when creating a new partition. For details, see the description of the wizard in “The New Partition wizard”.
6. Select Migration tab.
7. Select Migrate collection files check box.
8. In drop-down box, select the required migration software.
9 Enter age at which items are to be migrated and age to remove collection files from primary storage.

10 Click **Apply**.

11 Select **Advanced** tab and configure settings for the selected migration solution. An example of configuration settings for using IBM TotalStorage DR550 is given in the section, “To modify the partition properties” on page 433. (Note this step is not required if Enterprise Vault is used as the migration solution).

The New Partition wizard

1 On the Welcome page, click **Next**.

2 Enter a **Name** and **Description** for the new partition, and then click **Next**.
3 Select a storage type for the new partition, and then click **Next**.

![Storage Type Selection](image1)

4 Specify the device for the new partition, and then click **Next**.

![Device Selection](image2)

5 Specify whether to share archived items.
Specify whether to create the vault store partition with security ACLs on the folders in the partition, and then click Next.

6 Select Enterprise Vault as the file collection software to use, and then click Next.

7 Specify a time for collections to take place.
Specify the maximum size for collection files, and then click **Next**.

8 Enter the age at which you want files to be collected. Select **Migrate collection files to secondary storage**, and then click **Next**.
9 Select IBM TotalStorage DR550 as the file migrator software, and then click Next.

![New Partition Window](image1)

10 Specify the age at which you want collection files to be migrated by IBM TotalStorage DR550.
Specify the age at which you want files to be deleted from the primary storage, and then click Next.

![New Partition Window](image2)
11 Click **Finish**.

![New Partition dialog box](image)

12 Click **Close**.

![New Partition dialog box](image)

The new partition has now been created. You must now modify the properties so that Collection files can be passed to Tivoli Storage Manager (TSM).

**To modify the partition properties**

1. In the right pane of the Administration Console, double-click the new partition to display its properties.

2. Click the **Advanced** tab.

3. In the list, double-click **MANAGEMENT_CLASS** and then enter the name of the TSM management class. Click **OK**.

4. In the list, double-click **NODE_NAME** and then enter the name of the TSM Server computer. Click **OK**.

5. In the list, double-click **NODE_PASSWORD** and then enter the password for the TSM node. Click **OK**.
6 Double-click **USER_NAME** and then enter the TSM user name. Click **OK**.

7 Double-click **USER_PASSWORD** and then enter the password for the TSM user. Click **OK**.

8 Click **Test** to check that the entries you have made are valid.

9 Click **OK** to close the vault store partition properties.
Symbols

.NET Framework requirement 328

A
Active Directory
   Publishing the self-installing User Extensions 100
active/passive failover configuration 198
Administration Console
   Japanese fonts 77
   wizards 85
Administrator’s ReadMe 18
agent configuration, modifying 213
archiving
   initially suspended
   impact to users 257
AutoEnableMbxFolders 316

B
BlacklistedDLs 358

C
Chapter 21, 201, 328
Client computer
   customizing security 71
Collection files
   and NetBackup Server 413
   and Tivoli Server Manager 425
computer
   adding new 80
configuration
   modifying using wizard 213
   typical setup 198
Configuration Program 79, 85
   license keys 80
   running 80
configuration wizards
   Exchange Server Configuration 206
   configurations
   active/passive failover 198
Content categories
   introduction 326
Custom filtering
   assigning archive 354
   assigning retention category 354
   attachment filtering 353
   configuring 338
   default rules 347
   Domino registry settings 344
   events 339
   filtering attachments 366
   filtering messages 355
   filtering on DLs 357, 358
   filtering on message direction 362
   filtering on message subject 364
   format of ruleset files 349
   introduction 325
   named ruleset files 347, 348
   registry settings 339
   rule actions 352
   ruleset file example 372
   ruleset file schema 346
   ruleset file security 346
   ruleset files 346
Custom properties
   API 378
   introduction 326, 328
   supported properties 377
Custom properties.xml
   introduction 328
   schema 346
Customized filters 378

D
Default domain
   with basic authentication 69
Deleted Attachments.txt file 354
Demonstration mode
   defined 105
disk space requirements 40
DiskFullRetryLimit 314, 320
documentation 18

Domino Journaling
adding a domain 303
adding a location 306
adding a server 304
adding permissions to the journal archive 305
assigning a vault store 304
configuring access for Enterprise Vault 302
configuring the journaling databases 302
creating a task 306
creating a vault store 304
creating an archive 305
Database Management 302

Domino Journaling Archiving 301
set up 306
Domino Journaling archiving
preparation 301
Domino journaling location 344
Domino journaling locations
ruleset file name 348

E
EnableMailboxMessage.msg 254
enabling mailbox
manually 256
wizard 256
End user licence
agreement with Microsoft 18

Enterprise Vault
configuring 24, 79, 271
documentation 18
installing 63
software requirements 39
Enterprise Vault components
installing on SharePoint Portal Server 280
Enterprise Vault site
creating new 80
DNS entry for 52

Envelope Journaling 329
Evaluation mode
defined 105
Exchange
supported versions 197
Exchange agent
about 197
configuring using wizard 206
supported services 197
troubleshooting 235
typical setup 198
Exchange cluster
active/passive setup 198
Exchange cluster configuration
Active/Passive failover 198
Exchange Service agent 197
Exchange service group
modifying 213
External filters 326, 327, 341

F
Filtering
Custom filtering 325
Group journaling 325
Selective journaling 325
Fonts
in Administration Console 77

G
Group journaling
configuring 335
introduction 325
registry settings 337
rules file 336

H
HTTPS support 92

I
INCLUDES and ALLOWOTHERS operators 359
installation prerequisites
disk space 40
for users 54
operating system 39
Internal addresses
Defining 364
InternalSMTPDomains 364
Internet Explorer
for users 55

J
Japanese fonts
in Administration Console 77
L
license
  Microsoft end user agreement 18
License keys 105
  Configuration Program 80
  FSA 80
  obtaining 106
Licenses 105

M
Mail message
  archive limit messages 255
  at end of PST migration 254
mailbox
  enabling manually 256
MAPI named properties 365
MDAC version 43, 44, 45
Microsoft .NET Framework 43, 44, 46
Microsoft Exchange Forms
  distributing 74
Microsoft SQL Server
  setting up 54, 62
Microsoft Systems Management Server
  see SMS
MSMQ
  setting up 54, 62

N
New Retention Category wizard 87
  starting 253, 261
New Vault Store wizard
  starting 246, 288
NonDeliveryFolder for domains 314
NonDeliveryFolder for mailbox name 316

O
Operating 39
Organization Forms Library 74
Outlook 2003 Cached Exchange Mode 102
Outlook versions
  for users 55
Outlook Web Access Extensions
  installation option 64
OWA Extensions
  installing 109, 183, 273, 277

P
permissions
  for Vault Service account 60
Permissions, to install User Extensions 95
pilot system
  Vault Site alias in 53
Production mode
  defined 105
proxycfg 135
PST migration
  mail message to user 254
PST migration message 254
PSTMigratedMessage.msg 254

R
ReadMe files
  location of 18
Retention Category
  creating new 87, 253, 261
  None
  impact to users 257
Ruleset file schema 351
Ruleset files
  introduction 327

S
Searching for SMTP messages 321
Security
  on client computers 71
security
  for Web Access application 67
Selective journaling
  configuring 331
  introduction 325
  registry settings 333
  rules file 332
Self-Installing User Extensions
  requirements 55
Self-installing User Extensions
  Publishing in Active Directory 100
service group
  modifying 213
Services
  configuring 82
  starting during configuration 82
SharePoint archives
  contents 288
  permissions 288
Site Settings
  reviewing 248
SMTP Archiving
  command line 318
  domain to folder mapping 315
  format of holding area 312
  holding area 312
  holding folder permissions 312
  MAPI messages 311
  relaying 311
  unrecognized domains 314
  virtual SMTP server 314
  where to install SMTP server 311
SMTP configuration file 313
SMTP holding area folders 312
Software Product Description (see SPD)
SPD
  location of 18
SQL login
  for Vault Service account 61
  step 228
  supported services 197
  supported versions 197
T
TCP/IP
  required on client computers 55
Tivoli Server Manager 425
troubleshooting
  Exchange service agent 236
  troubleshooting information 235
  TSM 425
U
User Extensions
  distributing 94
  installing on a server 257
  self-installing
    computer requirements 55
  users
    online Help for 257
V
Vault Directory
  creating new 80
Vault Directory Database
  disk space requirements 40
Vault Directory Service
  and Vault Site alias 52
Vault Service account 51
  creating 57
  description 51
  permissions 60
  requirements 52
  SQL login 61
Vault Site alias 52
  configuring 81
  creating 62
  description 52
  in a pilot system 53
Vault Store
  creating 245
  name
    characters to include 246, 288
    valid characters 304
Vault Store Database
  disk space requirements 41
W
Web Access application
  application pool 51
  basic authentication 69
  https support 92
  setting up security 67
  specifying a port 92
Welcome Message
  editing 254
  location of 254
Windows Server
  for users 55
  wizards 85
    Enable Mailboxes for Archiving 256
    Exchange Server Configuration 206