Symantec Enterprise Vault™ Adapter for Secure Messaging and Rights Management 9.0

Implementation Guide

10.0

Symantec

Symantec Enterprise Vault: Adapter for Secure Messaging and Rights Management Implementation Guide 9.0

Enterprise Vault 10.0

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043
http://www.symantec.com

www.symantec.com

Third-party legal notices

Third-party software may be recommended, distributed, embedded, or bundled with this Symantec product. Such third-party software is licensed separately by its copyright holder. All third-party copyrights associated with this product are listed in the accompanying release notes.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrades protection
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Managed Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Education Services	Education Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about enterprise services, please visit our web site at the following URL:

www.symantec.com/business/services/

Select your country or language from the site index.

Contents

Chapter 3 Prerequisites

Chapter 4 Installing and configuring

Chapter 5 Managing the Gateway Service

Chapter 1

About this guide

This book describes how to install and configure the Symantec Enterprise Vault Adapter for Secure Messaging and Rights Management™ 9.0 on Enterprise Vault 10.0. Note that the adapter is unchanged since Enterprise Vault 9.0. It includes the following chapters and appendixes:

Prerequisite knowledge

To install and configure the Symantec Enterprise Vault Adapter for Secure Messaging and Rights Management, you need to know how to administer the following products:

- Symantec Enterprise Vault™
- Microsoft® Windows® Server 2003, 2008, or 2008 R2 (x64)
- Microsoft® SQL™
- Microsoft® Active Directory®
- Microsoft® Exchange Server 2000, 2003, 2007, or 2010

In addition, to use the following security services, you need to know how to administer their products:

- Microsoft Windows® Rights Management Services (RMS) for Windows Server 2003 or Active Directory Rights Management Services (AD RMS) for Windows Server 2008.
  Note: Throughout this document, the term “RMS” is used to refer to both RMS and AD RMS, except where each product is specifically mentioned.
- Liquid Machines™ Document Control
- PGP:
  - PGP® Universal Server
  - PGP® Desktop

Formats available

This book is available as an Adobe Acrobat (PDF) file on the Symantec Enterprise Vault Adapter for Secure Messaging and Rights Management CD-ROM.

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

Related resources

There is an Enterprise Vault Web page at:
http://www.symantec.com/enterprisevault

Conventions

The following conventions apply throughout the documentation set.

Table 1-1 Typographical conventions

Convention	Description
GUI Font	Used to depict graphical user interface (GUI) objects, such as fields, list boxes, menu commands, and so on. For example: Enter your password in the **Password** field.
Italics	Used for placeholder text, book titles, new terms, or emphasis. Replace placeholder text with your specific text. For example: Replace *filename* with the name of your file.
`Code`	Used to show what commands you need to type, to identify paths where files are located, and to distinguish system or application text that is displayed to you or that is part of a code example.
Key+Key	Used to show that you must hold down the first key while pressing the second key. For example: Ctrl+S means hold down the Ctrl key while you press S.

Notes and warnings are used to emphasize information. The following samples describe how each is used.

Note: Used for important information that you should know, but that should not cause any damage to your data or your system if you choose to ignore it.

Warning: Used for information that will prevent a problem. Ignore a warning at your own risk.

Comment on the documentation

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

Please include the following information with your comment:

- The title and product version of the guide you are commenting on
- The topic (if relevant) you are commenting on
- Your name

Email your comment to evdocs@symantec.com. Please only use this address to comment on product documentation. See "Customer service" on page iv for guidelines on how to contact Technical Support about our software.

We appreciate your feedback.

Chapter 2

About the Symantec Enterprise Vault Adapter for Secure Messaging and Rights Management

This chapter includes the following topics:

Rights management: Controlling access to and use of data

Rights management is an important concept in protecting email and documents. *Rights management* means that access controls, along with rules about how data can be used, travel with copies of that data. Taking a copy out of a server and placing it onto a workstation or sending it out of a company's infrastructure and into the Internet does not remove the controls from the data. A *rights management service* determines who gets the rights to open each message or document. Rights-managed client applications allow recipients to view and manipulate the data and to send copies elsewhere, if the controls allow.

Control is accomplished through encryption. Documents and messages are protected by encrypting them, and access to them is controlled by permitting or denying access to the key that was used to encrypt them.

The Adapter works with any or all of the following security services:

- Microsoft Windows Rights Management Services
- Liquid Machines Document Control
- PGP

System architecture

The Symantec Enterprise Vault Adapter for Secure Messaging and Rights Management decrypts email messages and attachments, to ensure that journaled email messages are stored in Enterprise Vault in a way that is compliant with company policies, that is, in the clear.

The Adapter is installed on one or more computers, along with Enterprise Vault, specifically, ones that are running an Exchange Journaling task.

The Adapter acts as a gateway, changing the contents of mail messages as they cross the boundary from the main flow of mail messages into the archive. The gateway provides unprotected versions of the protected content of email messages or attachments, in supported formats, allowing that content to be stored and indexed in an unencrypted form. It also provides indexable metadata that describes the original protection of the message.

When an archived item is replied to, forwarded, or restored, the original protection is not reapplied, so you should limit access to the Exchange Journaling Mailbox, which is the only place where archived messages are available.

Several features of the Adapter can be enabled in the Configuration file, which you can access by using the Configuration Tool.

Protection systems

The Adapter can be configured to remove the protection from messages that have been protected and encrypted using any or all of the following systems:

- Microsoft Windows Rights Management Services (RMS)
- Liquid Machines Document Control
- PGP

Zip archives

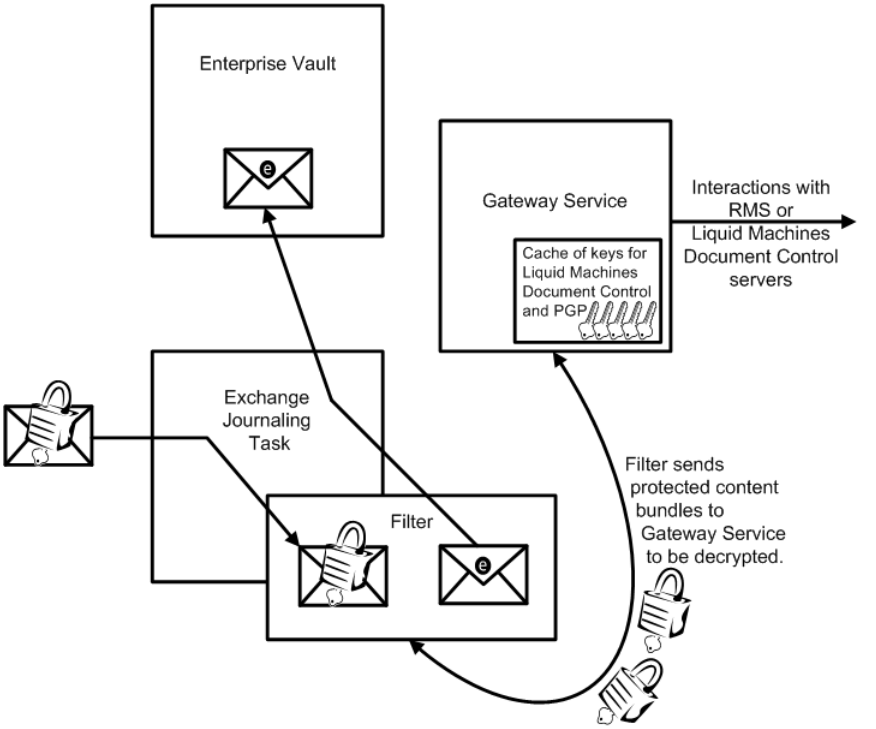
The Adapter can be configured to search the contents of Zip archives for protected data. Each file in a Zip archive can be examined and handled in the same way as a file attachment outside a Zip archive.

The examination of content in Zip archives can be limited to a fixed set of file extensions, or all files can be examined. The examination can include further recursion to any depth, in the case of a Zip archive within another Zip archive. The limitation is enabled by default, but if it is not enabled, then all elements of Zip archives are examined.

Any protected file found inside a Zip archive is decompressed and unprotected. The result is recompressed and reinserted into a reconstituted form of the Zip archive. The Zip archive's modification timestamp is preserved, so as not to affect the sorting order of items in Enterprise Vault. The Zip archive format stores each file separately in the Zip archive, so that it is possible to replace protected files without decompressing the remaining files.

Adapter components

When you install an Adapter, two distinct components are involved: the Filter and the Gateway Service.



Configuration Tool

The Configuration Tool, installed on the same computer as the Adapter, allows you to control the behavior of the Filter and the Gateway Service. You can use its graphical interface to change the Configuration file to specify which data formats the Adapter will process and to configure other parameters. See "Configuration Tool: Enabling features and configuring parameters" on page 38.

The Filter

The Filter is a custom filter registered with all Exchange Journaling tasks on an Enterprise Vault server computer. The Filter notices that a protected message is passing through the system. It gathers up the protected parts of the message, for example, the body, attached protected documents, or attached protected email messages, and passes them to the Gateway Service. The Gateway Service decrypts them and passes them back to the Filter, and the Filter then submits the new package of the email message and its decrypted contents back to the Exchange Journaling task. After that, the message is stored in Enterprise Vault.

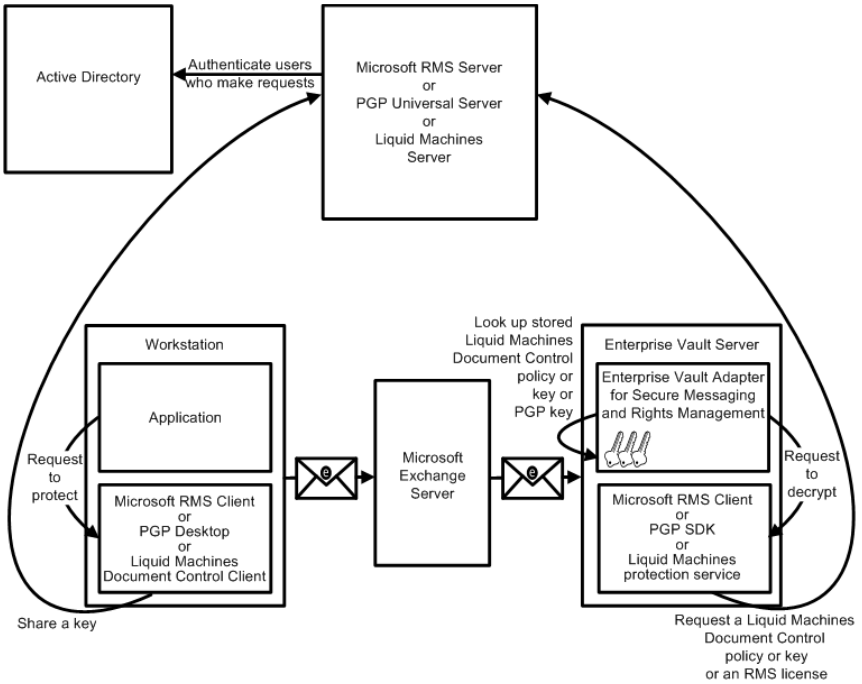
If you have multiple custom filters, you may need the Adapter to decrypt messages before they are submitted to other filters. Those other filters may only be able to properly process decrypted content. Determine the priority of the Adapter relative to other filters before you install it. For directions on controlling filter priority, see "Manually registering the filter" on page 36.

The Gateway Service

The Gateway Service is a process, or program, that you can see listed in the Windows Services console. It receives content from the Filter and decrypts it. When it is done, it sends the content back to the Filter.

The Gateway Service initiates communications with RMS or Liquid Machines Document Control servers based on its configuration. It handles caching of Liquid Machines policies and keys for offline operation and polling the servers for updated information. It also enforces Liquid Machines and RMS permissions, including Read and Remove permissions and expiration and offline access limits. The Gateway Service also holds the Additional Decryption Key (ADK) for decrypting PGP messages.

If you stop the Gateway Service, the Filter holds encrypted messages in a queue until the Gateway Service starts again and can process them. Unless specially configured otherwise, the Filter does not allow encrypted messages to enter the archive, should the Gateway Service be down.



The Key Upload utility

The Key Upload utility is a command-line tool that you can use to import one or more PGP decryption keys to the Gateway Service's Keyring. The Key Upload utility can add or update a key and validate that the key is suitable for decryption, For more information, see "The Key Upload utility" on page 48.

Security services

Microsoft Windows Rights Management Services (RMS)

The Microsoft RMS system provides infrastructure that enables messages and documents to be protected and controlled. Information Rights Management (IRM) enables users of Microsoft Office to restrict access to their documents.

Note: Office IRM (the Windows RMS feature) is supported in Office Professional 2003 or later.

RMS server: Issuing access licenses and authenticating users

The RMS Server provides the encryption keys, or, in Microsoft terminology, *licenses*, that are used to protect messages. Rights-managed applications, like Microsoft Office and the Enterprise Vault Adapter for Secure Messaging and Rights Management, need access to RMS Servers to get licenses to access protected content.

When a recipient requests access so that they can read a message or a document, the RMS Server also handles authenticating that user. That is, the RMS Server gathers the user's credentials, verifies them against Active Directory or another trusted RMS installation, and then checks to see if they are part of the access control list on the message.

RMS Client: Enabling applications to communicate with RMS server

Rights-managed applications, like Microsoft Office and the Adapter, decrypt protected messages and documents so that the appropriate recipients can read them. Desktop applications like Office may also preserve or carry forward protections when a recipient alters, replies, copies, or forwards a message or saves or alters an attachment.

To do all this, the applications must request access to licenses from the RMS Server on behalf of the user, submitting the user's credentials in the process. They may also need to generate new keys to encrypt materials and must share these with the RMS Server. This interaction with the RMS Server happens through the *RMS Client*. The RMS Client is a piece of middleware, standing between the Server and an RMS-enabled application; you can think of it as an API that applications like the Adapter use to access the Microsoft RMS system. The RMS Client must be installed on the same computer as the rights-managed applications, the workstations with Office, or the server with the Enterprise Vault Adapter for Secure Messaging and Rights Management.

The Adapter uses RMS Super User rights for decryption.

Liquid Machines Document Control

Liquid Machines Document Control provides encryption and rights-management of documents. In addition, it extends RMS protection to Microsoft Office XP and Office 2000, as well as to leading desktop and enterprise applications, such as Adobe Acrobat, Adobe Reader, Microsoft Visio, and Windows Notepad.

Liquid Machines Document Control Server: Providing policies, keys, and security

Liquid Machines Document Control provides enhanced enforcement options based on policies downloaded from a Liquid Machines Document Control server. The physical security (encryption) can be provided either by RMS or by a Liquid Machines Key Service (LMKS), which is part of the Liquid Machines Document Control Server. The combination of a Liquid Machines Document Control Server, various physical security services, and various clients is referred to as Universal Enforcement Services.

To be able to obtain policy information and cryptographic keys, the Adapter must communicate with one or more Liquid Machines Document Control Servers, version 6.1 or later.

The Adapter caches policies and keys locally, which maximizes Adapter performance and allows offline operation. It contacts the servers on startup and polls them for policy changes periodically, based on a frequency specified by the Liquid Machines Document Control Server. The cache can also be updated dynamically if the Adapter encounters a document protected by a new policy that is not yet in the cache. The cache is stored in an encrypted form that is only accessible to the Gateway Service.

When policies and keys are available in the cache, the Adapter can unprotect documents that use LMKS Security without communicating with any server. Liquid Machines Document Control documents that use RMS Security still require communications in order to obtain a document-specific license.

Liquid Machines Document Control enforcement agents: Protecting documents

The Liquid Machines Document Control Client provides enforcement by integrating with applications on a user's workstation. Liquid Machines Document Control can protect documents using Ad-Hoc permissions, an RMS template, or a policy defined by Liquid Machines Document Control.

Ad-Hoc permissions and templates always make use of an RMS license and are always compatible with Microsoft Office IRM when used in IRM-supported applications (Word, Excel, and PowerPoint). Unprotection of such documents by the Adapter is based on RMS Super User capability.

The Liquid Machines Document Control Client can interact with both Liquid Machines Document Control Servers and RMS Servers. The Liquid Machines Document Control Server provides policy information to Liquid Machines Document Control Clients.

The Adapter interacts directly with Liquid Machines Document Control Servers to provide its unprotection services, so there is no prerequisite for installing any Liquid Machines Document Control software before installing the Adapter.

Liquid Machines Document Control policy permissions can be enforced using security from either RMS or LMKS. Unprotecting a document protected by any Liquid Machines policy requires that a user's identity be granted the right to Remove protection in the relevant policy.

PGP

PGP is a point-to-point technology that enables senders to encrypt data to send to specific recipients. It is not a rights management system and does not use permissions. PGP provides for data confidentiality and integrity using encryption and digital signatures. PGP decryption can be enabled in the Adapter configuration. The Adapter does not require the installation of any PGP Server or PGP Desktop component on the host where the Adapter is installed.

Additional Decryption Keys

The OpenPGP standard does not explicitly provide for the notion of a Super User or master key that would allow authorized parties to decrypt emails and attachments without being listed as a recipient. However, PGP Universal Server and PGP Desktop provide support for a special key known as an Additional Decryption Key (ADK) or Additional Recipient Request Key (ARRK). ADKs are keys that can be used by an authorized third party to decrypt PGP-encrypted content. When a recipient's key contains an ADK, PGP Desktop automatically encrypts a message to the ADK as well as to the recipient's key.

The Gateway Service can decrypt all PGP-encrypted content that was encrypted to one or more ADKs or to any user keys for which the Gateway Service can obtain the associated private key.

If a message or document is encrypted, but the ADK wasn't included as one of the decryption keys, that message or document is left unmodified by the Adapter, and an event is reported in the Event log.

Supported PGP message formats

The Adapter recognizes certain OpenPGP-based formats for encrypted and/or signed messages or attachments. It supports messages created by PGP Desktop and PGP Universal Server and properly recognizes messages created by other products that use the same format as messages created by supported products.

Specifically, the Adapter supports the PGP Partitioned message format, not the PGP/MIME or S/MIME formats that are also supported by PGP products. The Adapter will also recognize and decrypt PGP-Zip archives when attached to both encrypted and clear-text messages; however, it will not recursively decrypt independently protected documents inside a PGP-Zip archive.

If users are using a PGP Client other than PGP Desktop, messages can be scanned for encrypted content in the body, even when there is other content in the body. This scanning for inline PGP content applies only to plain-text messages and is only supported for messages using certain Windows code pages (character sets): single-byte code pages supported by the Operating System (see "Enabling support for international characters" on page 81). Any message that can only be represented in a multi-byte encoding (for example, most forms of Chinese) are not subject to inline scanning. PGP-encrypted messages in which the full contents are encrypted (not an inline case) are still handled regardless of their code page.

Unsupported messages and attachments are passed through unmodified.

More about protections

Protection systems

When enabled, the Enterprise Vault Adapter for Secure Messaging and Rights Management decrypts content that was protected using any or all of the following systems:

- Microsoft RMS
  Unprotection is based on RMS Super User capability.

  Note: Liquid Machines Document Control and RMS functionality can interact and cooperate to process documents, using RMS security with Liquid Machines policies.

- Liquid Machines Document Control
  The Adapter recognizes and unprotects files protected by any version through 7.3, or any later version that is compatible with 7.3. The appropriate permissions must have been granted, and the relevant policies and keys must be available, on an accessible Liquid Machines Document Control server.

- PGP
  The Adapter detects and attempts to remove protection from PGP messages. The appropriate decryption key must be available.

The Adapter does not decrypt content protected using other kinds of rights management or encryption systems.

File formats

In general, the Adapter can unprotect any protected file format produced by Office 2003, Office 2007, or Liquid Machines Document Control, version 7.3 or earlier, or PGP Desktop, version 10.0 or earlier. In addition, Zip archive contents can be examined, unprotected, and reinserted into a modified archive, if it is not encrypted with a password.

These functions can be used simultaneously on separate emails or combined on the same email where formats allow, for example, an RMS-protected attachment in a PGP-encrypted email.

The following occurrences are not decrypted:

- Emails or documents encrypted by a scheme other than RMS, Liquid Machines Document Control, or PGP, for example S/MIME.
- File attachments representing email messages. These could include .EML files, .MSG files, if not attached using Outlook, or any unknown format.
- PGP messages or documents of the following types:
  - Protected documents inside PGP-Zip archives.
  - Messages or documents protected by PGP keys that have not been uploaded to the Gateway Service.
- .RPMSG files. This kind of file is normally a hidden attachment to an RMS-protected email message. If a user manually detaches this hidden attachment from a protected email message and then reattaches it separately to any message, it will not be decrypted.
- Contents of other archive files; for example, .ARJ, .GZ, .RAR, and .TAR files are not examined and therefore are not decrypted.
- Any other document file that is not clearly identifiable as one of the file types listed above.

RMS installations and trusts

When you install the first RMS Server into an Active Directory domain and register the service connection point with Active Directory, it is called an *RMS installation* and it is associated, attached, installed into, or bound to the Active Directory forest in which the domain exists. You can install additional servers into this installation, for load-balancing or redundancy.

While it is possible to install RMS Servers into this same Active Directory in a way that is not associated with this installation, you cannot register the service connection point of these new servers with this Active Directory, and they are not the ones that rights-managed applications would typically use if they are members of this Active Directory. Getting applications to connect to such an unknown RMS installation requires special configuration of the Microsoft RMS Client that you must install on the Enterprise Vault server computer. If, for some reason, you are deploying this kind of infrastructure and are unfamiliar with how to manage the RMS Client in this situation, refer to the Microsoft RMS documentation.

An RMS installation can be configured to trust other RMS installations. For more information about RMS Trust Policies, refer to the Microsoft RMS documentation. An RMS installation can also be configured to trust the Microsoft Passport Service, which is available to individual consumers on the Internet. But if RMS Installation A trusts RMS Installation B, and Installation B trusts Installation C, it is not true that A trusts C. In other words, just because you trust a company does not mean you have to trust the other companies that they trust.

The Adapter will decrypt content from trusted installations if it has the appropriate privileges in the total RMS environment. For more information on how to verify such privileges, consult Microsoft RMS documentation.

More about unprotecting

Microsoft Windows Rights Management Services (RMS)

Processing with RMS if Liquid Machines Document Control is disabled

If RMS is enabled but Liquid Machines Document Control is disabled, the Adapter can unprotect all content from Microsoft Office IRM, as well as some documents produced by the Liquid Machines Document Control Client: those that can be unprotected without any need for a Liquid Machines policy. This includes documents from any application protected using Ad-Hoc permissions or an RMS Template. It also includes documents from some applications that use a Liquid Machines policy using RMS security in IRM-Compatible mode. The Adapter makes a best effort for such cases and unprotects only if it knows that the document can be unprotected without any auditing requirements. Because of details of the file formats used by the Liquid Machines Document Control Client, the Adapter can unprotect documents only from Word, Excel, PowerPoint, and sometimes Visio (based on the version of the Liquid Machines Document Control Client used).

Any Liquid Machines Document Control document that cannot be unprotected because of the limitations above is identified as a foreign document and passed through. To ensure unprotection of all Liquid Machines Document Control documents with proper auditing, we recommend that Liquid Machines Document Control functionality be enabled, and that the appropriate permissions be granted on the Liquid Machines Document Control server.

Foreign protection checking with RMS

If a document is in a format with a policy type that the Adapter expects to be able to unprotect, but the unprotect fails, the Adapter determines whether to treat the document as foreign content (expected error, passed through) or local content (unexpected error, possibly subject to retry). When Liquid Machines Document Control is disabled, or for any RMS document with no Liquid Machines policy, the method for doing this is based on the primary RMS Server and the configured server suffixes.

When an error occurs, one of the following happens:

- If the RMS installation mentioned in the email message is listed under **Local Server Domains** in the Configuration Advanced Options (see page 44), the Adapter assumes this is a real error and responds according to its configuration.
- If the installation is not listed, the message is stored in the archive in an encrypted state.

By default, the primary RMS server, the one you used to configure the RMS Client as part of the prerequisites, and the name of the DNS domain in which the primary RMS server resides, are always considered to be local. The primary RMS server is always included and need not be listed (and cannot be omitted). However, the DNS domain does need to be listed explicitly (and can be omitted), but is included in the default configuration.

The default value (using a special variable) always includes the domain of the Enterprise Vault server computer in the list of local servers. For example, if your RMS installation is called rms.symantec.com, both rms.symantec.com and *.symantec.com are automatically included. It is only in the case of unusual multi-domain scenarios that any change will be needed for this setting.

If you leave the Local Server Domains setting in the Configuration Tool blank (see "Advanced Options" on page 46), all RMS-protected documents will be considered local, even ones coming from foreign installations. When RMS-protected documents are considered local, they are not passed through to the archive, if an error occurs. This means that messages coming from truly foreign RMS servers will remain in the queue forever, since the error in this case, that the Adapter cannot obtain permission to decrypt the message from that foreign RMS server, can never be resolved.

Liquid Machines Document Control

Unprotection of Liquid Machines Document Control documents

The Configuration Tool can direct the Adapter to unprotect documents protected by Liquid Machines Document Control. (See “protection-config settings” on page 87.) A list of policy servers can be included by host name or URL.

If a configured server cannot be contacted when it is initially configured, the Event log shows an error, and Liquid Machines policy operations fail. Otherwise, the server is polled for policy updates on startup, shutdown, and periodically, based on the poll interval configured on the server.

The Adapter can also be configured to automatically contact additional servers when it encounters documents from those servers. In such cases, unprotection will succeed only if the Gateway Service user can properly authenticate to the appropriate server and obtain appropriate permissions. If a discovered server is contacted successfully, it will be kept active and polled for updates for a period specified in configuration, or until the Gateway Service is restarted. After that, it will become inactive and need to be discovered again.

When Liquid Machines Document Control is enabled, the Adapter can unprotect documents protected by the configured Liquid Machines Document Control Servers in exactly the same way as a Liquid Machines Document Control Client. The Gateway Service Account must have appropriate policy permissions, and the Liquid Machines policy permissions always take precedence over RMS Super User rights for documents protected by a Liquid Machines policy. For documents with non-Liquid Machines policies (RMS Ad Hoc or template), the RMS Super User rights are used as usual.

When Liquid Machines Document Control is enabled, and a document with a Liquid Machines policy is unprotected (or unprotecting is denied because of insufficient permissions), an audit message is generated, if required by the policy.

Liquid Machines Document Control Operation with RMS disabled

If Liquid Machines Document Control is enabled and RMS is disabled, the Adapter unprotects only Liquid Machines documents protected by LMKS. Any RMS-protected documents or emails are identified as foreign and passed through.

Foreign protection checking with Liquid Machines Document Control

For RMS documents with no Liquid Machines policy, even if Liquid Machines Document Control is enabled, foreign protection checking is the same as with RMS. If a document is in a format with a policy type that the Adapter expects to be able to unprotect, but the unprotect fails, the Adapter determines whether to treat the document as foreign content (expected error, passed through) or local content (unexpected error, possibly subject to retry). When Liquid Machines Document Control is disabled, the method for doing this is based on the primary RMS Server and the configured server suffixes. See **"Local Server Domains"** on page 45.

For documents with a Liquid Machines policy, the check is performed slightly differently. The document's protection information is compared against the list of manually configured Liquid Machines Document Control servers (not auto-discovered services), based on both the Service ID and the Service Locator stored in the document. Any match indicates content that should be unprotectable. Otherwise, the Liquid Machines Document Control server host name stored in the document is compared to the same configured set of server suffixes used in the RMS case. The identity of the RMS security service used for a document protected by a Liquid Machines policy is not used for this check. This may be important to the results if the RMS Server and the Liquid Machines Document Control Server are in different subdomains.

PGP

The Gateway Service cannot decrypt messages that were encrypted using externally managed keys or passphrases. Any unhandled content causes the logging of a distinguishable error message in the Event log. The Adapter handles this content in a manner similar to content protected by a foreign policy server using RMS or Liquid Machines Document Control.

Chapter 3

Prerequisites

This chapter includes the following topics:

Software

The Symantec Enterprise Vault Adapter for Secure Messaging and Rights Management requires:

- Symantec Enterprise Vault 10.0 installed on a computer that is running Microsoft Windows Server 2008 R2.
- An Enterprise Vault Exchange Journaling task configured to archive the target Exchange Server.
- If Microsoft Windows Rights Management Services (RMS) is enabled:
  - A fully functioning RMS SP2 or AD RMS installation in the Active Directory forest in which the Gateway Service account and the Enterprise Vault server computer will reside. The Gateway Service account is an Active Directory user account that you will create for exclusive use in configuring the Adapter. Before you proceed with installing the Adapter, ensure that your RMS installation is operating properly and that users can send and receive RMS-protected email messages.
  - Microsoft RMS Client (or AD RMS) installed on the Enterprise Vault server computer. You must properly configure the RMS Client SP2 to access the RMS installation noted above. (The AD RMS Client is included in a default installation of Windows Server 2008 or later.) The Adapter makes use of the RMS Client in the same way that workstations in your forest make use of it. Whatever you have done to properly configure the RMS Client on those workstations must also be

done on the Enterprise Vault server computer. Typically, this means that you have either registered the RMS Service Connection Point with Active Directory or enabled special Windows registry settings on the client computer. For more information, see Microsoft documentation. Because the Enterprise Vault server computer has Microsoft Outlook installed on it, you can log on to the Enterprise Vault server computer and use Outlook to prove that a user, notably the Gateway Service account you will create below, can send and receive RMS-protected messages. This is a good way to ensure that the RMS Client is properly configured on the computer.

- If PGP is enabled:
  - In order to decrypt all messages, the Gateway Service must be given appropriate keys. Generally, this is an Additional Decryption Key (ADK), which must be created using PGP Desktop and associated with the internal users' policy on a PGP Universal Server. It is possible for small scenarios to instead load the private key of each user into the Gateway Service. See "Uploading an ADK" on page 47.
  - To be able to process plain-text messages encrypted by PGP that include international characters, you must enable support for all international characters on the server machine. You must enable this support in the OS, which requires installing some files from the Windows CD. See "Enabling support for international characters" on page 81.

    You may have already enabled support for international characters for use by Enterprise Vault.

Gateway Service account and permissions

You must create a service account in the Active Directory forest in which the Enterprise Vault server computer resides. This forest must also contain the RMS installation and Liquid Machines server if relevant. This account is referred to as the *Gateway Service account*. We recommend that you use the Vault Service account, because the decryption permissions given to it might extend security privileges beyond what is appropriate and secure.

The Gateway Service account must:

- Be an Active Directory domain account.
- [RMS Only] Be *mailbox enabled* within the Active Directory. This means that you must give it an Exchange Server mailbox and an SMTP email address. The email address is used as the primary identifier in RMS. However, no messages or data are stored by the Adapter in this mailbox, and therefore no storage space is consumed.
- Have the right to log on as a service to the Enterprise Vault server computer. The installer will grant this right automatically. However, you must ensure that no Active Directory group policy will override and remove this right.
- [RMS Only] Be configured as an RMS Super User. For instructions for enabling the RMS Super User functionality follow this list, see "Enabling RMS Super User functionality (RMS Only)" on page 24.
- [RMS Only] Be configured to run as an RMS service. This is an RMS-specific setting that is distinct from the Windows right to log on as a service. See "Configuring the Gateway Service account to run as an RMS service (RMS Only)" on page 26.
- [RMS Only] Have its profile initialized on the Enterprise Vault server computer. See "Initializing and configuring the Gateway Service account profile (RMS Only)" on page 27.
- [LMDC Only] Be included in a role in any relevant policies on the Liquid Machines Document Control Server to be able to unprotect Liquid Machines Document Control Documents, if Liquid Machines Document Control is enabled. See "Including the Gateway Server Account in policy roles (LMDC Only)" on page 27.
- [LMDC Only] Have access to appropriate root certificates. For more information, see "Configuring certificates for LMDC communications (LMDC only)" on page 28.

In addition for PGP, you must create and deploy one or more Additional Decryption Keys. See "Additional decryption keys (ADKs)" on page 46.

Enabling RMS Super User functionality (RMS Only)

If you already have an RMS Super Users group

Add the Gateway Service account you created as a member of this group.

You must now clear the Active Directory cache on the RMS installation. The cache does not refresh the membership of the Super Users group. See "Clearing the Active Directory cache from the RMS installation" on page 73.

If you do not have an RMS Super Users group

1. Create a security group or distribution list in your Active Directory (for example, RmsSuperUsers). It must be a Universal group. You may not use a Domain Local or Global group. You must make the group mail-enabled and specify its email address.
2. Add the Gateway Service account you created as a member of this group.
3. Grant Super User access to the group you created in Step 1 as follows:

If you are using RMS on Windows Server 2003, do the following:

a. Launch the RMS Cluster Administration console. For detailed instructions, refer to Microsoft documentation.
b. In the left pane, click **Security settings**.
c. On the Security settings page, under Super users, click **Enable**.
d. In the **Super Users Group Name** field, type the primary SMTP email address of the group you created, for example, **example.com**.
e. Click **Save**.

If you are using AD RMS on Windows Server 2008, do the following:

a. Launch the RMS Cluster Administration console. For detailed instructions, refer to the Microsoft documentation.
b. On the left pane, click **Security Policies** and then click **Super Users**.
c. On the right pane, click **Enable Super Users**.
d. On the center pane, click the link **Change super user group**. Enter the primary SMTP email address of the group you created, or click **Browse** to locate and select the RMS super user group.
e. Click **Apply** to save the changes, or click **OK** to save the changes and return to the Super Users dialog.

Because Microsoft Outlook is a prerequisite for Enterprise Vault, it will be installed on this computer. You can log on to the computer as the Gateway Service account and verify that it can send and receive RMS-protected messages. You can also forward a protected message to the Gateway Service account, one that the Gateway Service account should not be able to read under normal circumstances, and make sure that the new Super User status allows the Gateway Service account to open it. This is a good way to determine that the Super User privilege has been properly extended to the Gateway Service account.

Configuring the Gateway Service account to run as an RMS service (RMS Only)

On every RMS Server in your installation, you must make a change in file system permissions to a particular file and then restart IIS. Only when this task is completed on all RMS Servers is the configuration complete.

1. Log on to an RMS Server.
2. Launch Windows Explorer and navigate to the file system folder that is the root of the Web site on which RMS is installed. For example, when you install Windows, the Default Web Site places the root folder in the following folder:
   `C:\inetpub\wwwroot`
3. Within this folder, locate the following subfolder:
   `_wmcs/Certification/`
4. Right-click the following file:
   `ServerCertification.asmx`
   and then click **Properties**.
   (There is also a `Certification.asmx` file in this directory; but that is not the file you want.)
5. Click the **Security** tab.
6. Click **Add**.
7. Type the logon name of the Gateway Service account, and then click **OK**.
8. To extend this permission to the Gateway Service account, check the **Read & Execute** check box. The **Read** check box is also automatically checked.
9. Click **Add** again.
10. Click **Locations**.
11. Select the name of this RMS Server, and then click **OK**.
12. Type **RMS Service Group**, and then click **OK**.
13. To extend this permission to the RMS Service Group, check the **Read & Execute** check box. The **Read** check box is also automatically checked.
14. When you are done, click **OK**.
15. Restart IIS on the RMS Server.

Repeat this process for all RMS Servers in your installation.

Initializing and configuring the Gateway Service account profile (RMS Only)

To initialize the profile, you must log on interactively to the Enterprise Vault server computer as the Gateway Service account. This log on will create the profile.

The information included in this section is only required is RMS is to be enabled. Also, the Internet Explorer setup described below must be executed during the logon at the Gateway Service account.

If RMS is to be enabled, then during the logon to initialize the profile, we recommend using Outlook to verify that RMS can be used and that the Super User access has been successfully granted. For more information, see "Enabling RMS Super User functionality (RMS Only)" on page 24.

The host name of the RMS installation, as it appears in the RMS Licensing URL, must be included in the list of local intranet sites in Internet Explorer. This is only necessary if the URL contains a dot (.).

Example:

- For the following URL:
  `http://rms1.example.com/_wcms/licensing`
  you need to include the host name in the list of local intranet sites.
- For the following URL:
  `http://rms1/_wcms/licensing`
  you do not need to include the host name.

If your URL requires you to add RMS serves to the local intranet site, see Appendix B, "Adding RMS servers to the local intranet sites" on page 75.

Including the Gateway Server Account in policy roles (LMDC Only)

If Liquid Machines Document Control is enabled, in order to be able to unprotect Liquid Machines Document Control Documents, the Gateway Service Account must be included in a role in any relevant policies on the Liquid Machines Document Control Server. The Gateway Service Account should be included in a role with full permissions (including "remove policy protection"), no expiration, and unlimited offline access. It is possible to create a single role that appears in all policies. For more information, contact Liquid Machines Product Support.

Configuring certificates for LMDC communications (LMDC only)

In order to communicate securely with the LMDC Server, the Gateway Service must be able to validate that server's identity. This identity is checked when the SSL/TLS certificate is presented by the LMDC server at the time a connection is made. This certificate is checked in a way very similar to the checking performed by a browser when connecting to a secure Web site. If your organization already has appropriate certificate-management in place to allow desktop users to connect to the administrative console on your LMDC server, then you probably don't need any extra steps.

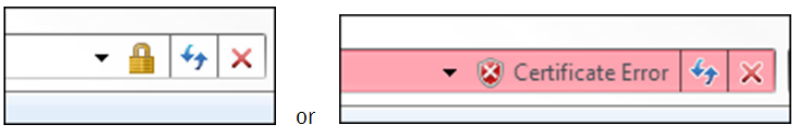
If you do not have certificate management set up, or if you see an error in the Event Log indicating "server identity could not be validated", you should ensure the correct root certificate is available locally by one of the two methods below. You can also disable certificate checking by using the <enable-peer-cert-checking> option in the configuration file, but this insecure option is best suited as a temporarily debugging step rather than a permanent configuration. The Gateway Service requires that the root certificate that issued the LMDC server's own certificate be present in the Trusted Root Certificate Authorities section of the Windows certificate store. It may be present in the store for the Gateway Service user, or in the local machine store. The certificate which is needed is the root of the certificate chain, and must come from a Certificate Authority. Self-signed server certificates are not supported.

Importing a certificate through Internet Explorer

Internet Explorer validates the same certificate as the Gateway Service, and provides a way to install that certificate if it is not present locally. To use this method you must log on as the Gateway Service account, launch Internet Explorer, and connect to the LMDC administrative console at following URL:

```
https://yourlmdcserver.domain.com/
   LiquidMachines-DocumentControl
```

If you receive a certificate warning from Internet Explorer, choose to continue. As soon as you see the logon page, do not log in, but look at the icon next to the address bar. It may be a lock icon (indicating that Internet Explorer accepted the certificate) or it may be a red button indicating a Certificate Error as shown below:



or

In either case, do the following:

1. Click the certificate icon (lock or error) and then **View Certificate**.
2. Select the **Certification path** tab.
3. Choose the topmost item in the Certification path box.
4. Click **View Certificate**.
5. If the certificate has not already been imported, you should see a button **Install Certificate**. Click that button.
6. Click **Next**.
7. Select **Place all certificates in the following store** and click **Browse**.
8. Choose **Trusted Root Certification Authorities** and click **OK**.
9. Click **Next**, and then **Finish** to complete the wizard.
10. If you see a Security Warning, click **Yes** to confirm the import of the certificate.

If you re-start Internet Explorer and re-connect, you should now see a lock icon indicating a valid certificate. These steps will install the necessary certificate only for use by the Gateway Service Account.

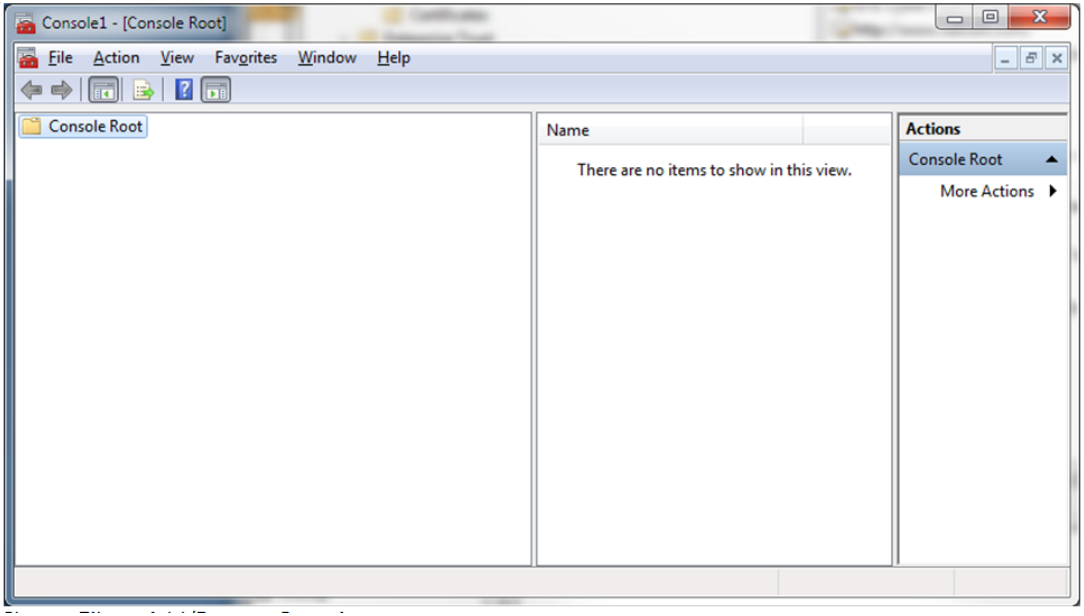
Importing a certificate from a file

This method can be used to import a certificate either for use of the logged on user (which should be the Gateway Service account) or all users on the local machine. To use this method you will need to obtain the necessary root certificate in a file (extension ".cer"). If you have already imported the certificate on a different machine, you can export it to a file from the same tool used here.

To launch the Certificate Management tool and import a certificate:

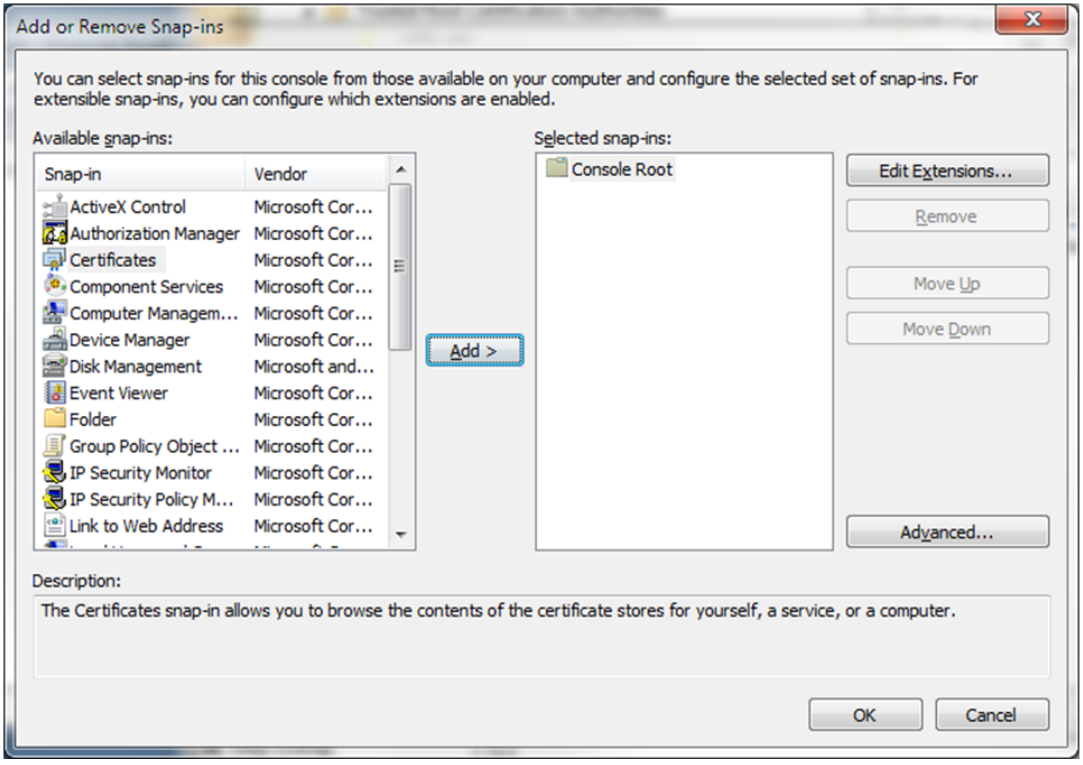
1 Open the **Start** menu and click **Run**.

2 Type **mmc** and click **OK**. The Console Root screen appears:



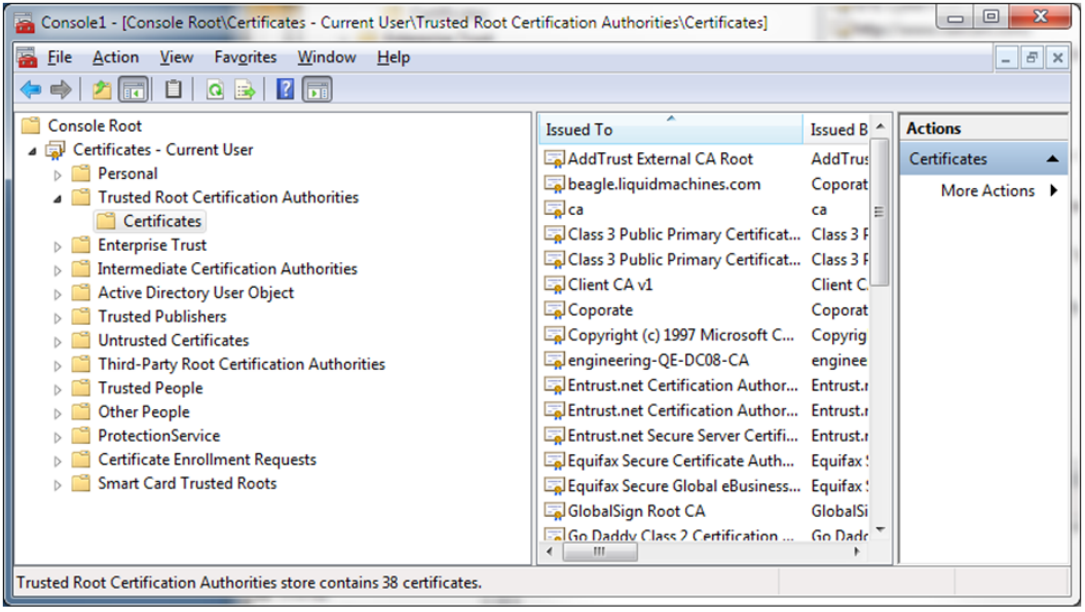
3 Choose **File > Add/Remove Snap-in**.

4 In the list of snap-ins choose **Certificates** then click **Add** as shown below:



5 Select **My user account** if you want to affect only the current user, or **Computer account** if you want to affect all users. Do not choose **Service account**.

6 Click **Finish**, and then **OK**. You should see the Certificates in the tree to the left. Expand that tree then expand **Trusted Root Certification Authorities** and click on **Certificates** as shown below.



7 Right-click **Certificates** and choose **All Tasks > Import**.

8 Click **Next**.

9 Click **Browse**, and then select the appropriate file, and click **Open**. Then click **Next**.

10 Select **Place all certificates in the following store** and click **Browse**.

11 Choose **Trusted Root Certification Authorities** and click **OK**.

12 Click **Next**, and then **Finish** to complete the wizard.

13 If you see a Security Warning, click **Yes** to confirm the import of the certificate.

Chapter 4

Installing and configuring

This chapter includes the following topics:

Upgrading from a previous version

The version of the Adapter for Secure Messaging and Rights Management supplied with Enterprise Vault 10.0 is the same as the one supplied with Enterprise Vault 9.0. If you are upgrading from Enterprise Vault 9.0, you do not need to update the adapter.

If you are upgrading from the previous version (Enterprise Vault 8.0), you should follow the installation steps below as normal. The installer will automatically uninstall the previous version before installing this version, and preserve the installation location and Gateway Service account name for you.

Note that the installation does not preserve configuration information. You will need to reconfigure the Adapter after the upgrade, using the Configuration Tool. You may wish to make a record your configuration by saving a screenshot of the Configuration Tool or by saving a copy of the configuration file before the upgrade.

Installation

This installation program restarts the Enterprise Vault Task Controller Service. This means that all tasks that the Task Controller Service manages will be restarted as well, if they were running. This ensures that Adapter files can be updated without a reboot. If a task is stopped but marked for automatic startup, it will be started as part of this process. If you do not want a stopped task to be started this way, then disable the task before performing the installation.

After installation, the Adapter is fully functional and running. However, it contains support for several security services that can be used independently, each with its own prerequisites, so none are enabled by default. Instead, after installation, you can use the Configuration Tool to enable and configure the appropriate protection types (RMS, Liquid Machines Document Control, and PGP), and to specify other relevant security settings.

1. Locate the installer file, **Symantec Enterprise Vault Adapter for Secure Messaging and Rights Management.msi**, on the distribution media and execute it.
2. To move past the **Welcome** page, click **Next**.
3. Read the license agreement. If you accept the license, select **I Agree,** and then click **Next**.
4. On the Customer Information screen, enter your name and organization name, and then click **Next**.
5. On the Destination Folder page, click **Change** if you wish to browse to a non-standard installation location, and then click **Next**.
6. On the **Enterprise Vault Gateway Service for Secure Messaging and Rights Management Credentials** page, enter the credentials of the Gateway Service account you created.
    a. In the **User** field, type the domain-qualified name of the Gateway Service account, for example, SYMANTEC\rmsgateway.
    b. In the **Password** field, type the Gateway Service account's password.
    c. Click **Next**.

7 To complete the installation, on the next page, click **Install**.

Note: If other custom filters are registered with Enterprise Vault, a message tells you that automatic registration is not possible and that you must register manually before the Adapter will be functional. See "Manually registering the filter" on page 36.

---

8 When it completes, click **Finish** to exit the installation wizard.

The software is installed and ready for operation. If the installation registered the Filter automatically, the Adapter is functioning. It will not decrypt any data, however, until one or more protection types are enabled using the Configuration Tool.

Manually registering the filter

If you have no other custom filters installed, the installer automatically registers the Filter with the Enterprise Vault Exchange Journaling task. However, if there are other custom filters, the installer will not automatically register the Filter. This allows you to manually specify the ordering of different custom filters. To do so:

1. Log on to the Enterprise Vault server computer as a user with local administrative privileges.
2. Start **regedit**.
3. Find or create the following key:
   `HKLM\SOFTWARE\Wow6432Node\KVS\Enterprise Vault\External Filtering\Journaling`
4. Inside the key are several string values. The actual values may vary, but the names will always be numbers, beginning with 1, continuing to 2, 3, and so on. Each value represents a custom filter, and the numbers represent the order in which those filters are invoked. Enterprise Vault requires that all registered filters be listed in a continuous set of values starting from 1. Any gaps in the numeric sequence indicate the end of the list of registered filters. Any filter that needs message content to be decrypted in order to process it must run later than the Adapter and thus have a higher number.
   You must reserve the correct value for use by the Enterprise Vault Adapter for Secure Messaging and Rights Management. For example, if all filters need content to be decrypted, reserve the value 1. This might require you to renumber the values, leaving them in the same order but increasing their number. For example, if there are six values, and you need 1, start by renaming 6 to 7, then 5 to 6, and so on, to ensure that 1 is not used. Inside the key, create the following string value:
   name: *`priority you reserved, for example 1`*
   value: `EVSMRMFilter.EVSMRMFilterImpl`
5. Restart the Exchange Journaling task.

Unregistering the Filter

The filter will be unregistered automatically when uninstalled. If you want to disable the Filter without completely uninstalling the product, you must manually unregister the Filter. You can do this whether you originally registered the Filter manually or the installer did it for you.

1. Open and edit the Windows Registry. For more information, see Microsoft documentation.
2. Find the following key:
   `HKLM\SOFTWARE\Wow6432Node\KVS\Enterprise Vault\External Filtering\Journaling`
3. Inside the key are several string values. The actual values may vary widely, but the names will always be numbers, beginning with 1, continuing to 2, 3, and so on.
4. Find the key whose actual value is `EVSMRMFilter.EVSMRMFilterImpl` and delete it.
5. Rename any other filters to fill the gap in numbering left by deleting this value. For example, if you deleted the value 3, you would have to rename 4 to 3, 5 to 4, and so on.
6. Restart the Exchange Journaling task.

To reregister the Filter, you must follow the instructions above for manual registration. If you have no other custom filters, set the priority to 1.

Uninstalling

Uninstalling reverses all the actions taken during installation. Installed files and shortcuts are deleted. The Gateway Service is unregistered. The Custom Filter is also unregistered from the Exchange Journaling task. Unregistration can proceed automatically even if registration had to be done manually.

The Adapter's data directory is deleted by an uninstall. It might contain useful diagnostic logs that should not be lost if the uninstall is for a problem that must be investigated. Be sure to copy those logs before uninstalling if you want to send them to Symantec support.

The Adapter's data directory includes a subdirectory called **SCache** that contains cached policies and keys, protected in a way that is only accessible to the Gateway Service Account. If the default location is used, the uninstall program removes it automatically, but if the Adapter's data directory has been moved to a different location, it must be removed manually. Failure to do so is a potential minor security risk (only the Gateway Service Account can access the data); it can also cause failures when a new version of the Adapter is installed that cannot read the data.

To uninstall the Adapter:

1. On the Windows taskbar, click **Start > Control Panel > Programs and Features**.
2. Scroll to **Symantec Enterprise Vault Adapter for Secure Messaging and Rights Management** and select **Symantec Enterprise Vault Adapter for Secure Messaging and Rights Management** and click **Uninstall.**

Configuration

Configuration Tool: Enabling features and configuring parameters

The Configuration Tool lets you change the behaviors of the Enterprise Vault Adapter for Secure Messaging and Rights Management using a graphical interface to change the Configuration file. See "Configuration file" on page 83.

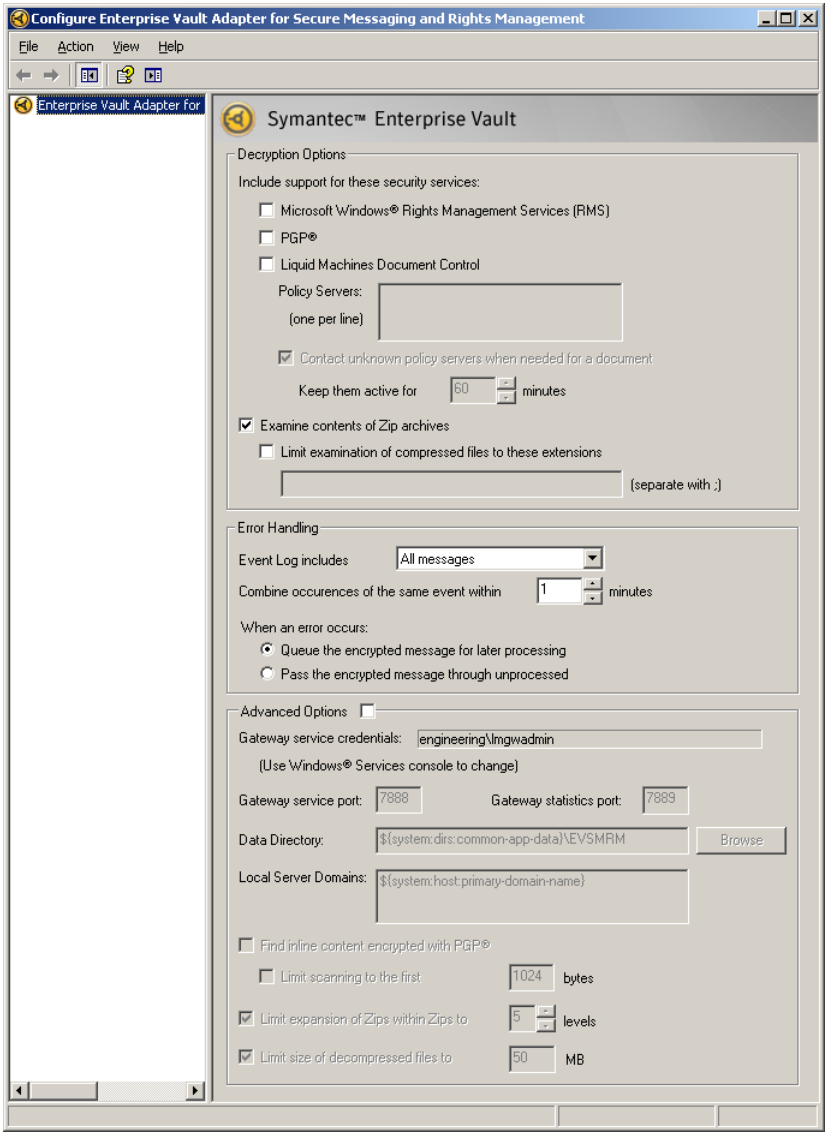
The default configuration disables all decryption ability in the Adapter, so you must use the Configuration Tool (or edit the Configuration file directly) to specify which data formats the Adapter will process (RMS, Liquid Machines Document Control, PGP, and Zip).

You can also use the Configuration Tool to view and/or configure parameters relating to Event logs, errors, service credentials, ports, the data directory, and local RMS domains. None of this configuration is required. All defaults should operate properly "out of the box." The Configuration Tool separates standard features (frequently changed) from advanced features (unlikely to need any adjustment).

To configure the Adapter:

1. Log on to the Enterprise Vault server computer as a user with local administrative privileges.
2. On the Windows taskbar, click **Start** > **Programs** > **Enterprise Vault** > **Configure Enterprise Vault Adapter for Secure Messaging and Rights Management**.

Note: This method launches only the Configuration Tool. You can build a single MMC tree that contains other tools as well. Run MMC manually (**Start > Run > mmc.exe**), then click **File > Add/Remove Snap-In** to add the Configuration Tool and other tools.


Configure Enterprise Vault Adapter for Secure Messaging and Rights Management
File
Action
View
Help
Enterprise Vault Adapter for
Symantec™ Enterprise Vault
Decryption Options
Include support for these security services:
Microsoft Windows® Rights Management Services (RMS)
PGP®
Liquid Machines Document Control
Policy Servers:
(one per line)
Contact unknown policy servers when needed for a document
Keep them active for
60
minutes
Examine contents of Zip archives
Limit examination of compressed files to these extensions
(separate with ;)
Error Handling
Event Log includes
All messages
Combine occurences of the same event within
1
minutes
When an error occurs:
Queue the encrypted message for later processing
Pass the encrypted message through unprocessed
Advanced Options
Gateway service credentials:
engineering\lmgwadmin
(Use Windows® Services console to change)
Gateway service port:
7888
Gateway statistics port:
7889
Data Directory:
${system:dirs:common-app-data}\EVSMRM
Browse
Local Server Domains:
${system:host:primary-domain-name}
Find inline content encrypted with PGP®
Limit scanning to the first
1024
bytes
Limit expansion of Zips within Zips to
5
levels
Limit size of decompressed files to
50
MB

3 In the settings dialog box, enter or select features and parameters, described below.

4 To save your changes, close the Configuration Tool.

Note: Alternatively, right-click the entry in the tree view to the left, and then click **Save Settings**.

---

5 The Configuration Tool asks if you want to save changes and restart services. Click one of the following:

- **Yes**
  The Configuration Tool restarts both the Gateway Service and the Enterprise Vault Task Controller Service, as well as any tasks that the Controller manages that are running.
- **No**
  Your changes are lost and no services or tasks are restarted.

Note: If the restart fails, it may indicate that you have selected invalid configuration options. Check the Windows Application Event log for errors.

Features and parameters

You can view or configure the following features and parameters using the Configuration Tool.

Decryption options

- **Include support for these security services**
  Select the appropriate check boxes to include security services.
  See "Prerequisites" on page 21.
  - **Microsoft Windows Rights Management Services (RMS)**
  - **PGP**
  - **Liquid Machines Document Control**
    If you select this option, complete the following fields:
    Policy Servers
    Enter the Liquid Machines Document Control Servers with which the Adapter communicates, one per line. A trailing line break is optional. You can enter more servers than fit in the box; use the arrow keys to scroll.
    Contact unknown policy servers when needed for a document
    If you want unknown policy servers to be contacted when needed for a document, select this check box and complete the following field.
      Keep them active for
      Select the number of minutes to keep unknown policy servers active for use with other documents. They will be polled periodically, based on the period configured on the server, until that time elapses, after which they will need to be rediscovered.
- **Examine contents of Zip archives**
  If you want the contents of Zip archives to be examined, select this check box. If you select this option, you can complete the following field.
  - **Limit examination of compressed files to these extensions**
    If you want to limit the extensions to be examined in Zip archives (to limit the cost of decrypting other types of files), select this check box and enter file extensions, separated by semicolons. A trailing separator is optional; you can enter your extensions as in either of the following examples:
    - doc;xls;
    - doc;xls

You can also include an empty entry to indicate that files with no extension should be scanned, by including an extra semicolon. The empty entry can be included either between extensions or at the end of the list, as in the following examples:

- doc;;xls
- doc;xls;;

Error handling

- **Event Log includes**
  Select the level of log messages to include in the Windows Application Event log:
  - All Messages (default; includes Informational, Warning, Error, and Serious Error messages)
  - Warnings and Errors (includes Error and Serious Error messages)
  - Errors only (includes Serious Error messages)
  - Serious Errors Only
- **Combine occurrences of the same event within _ minutes**
  If the same event occurs repeatedly in a short period of time, you can specify that only one entry is written to the Event log within time interval you specify here.

  For example, if you set this to 5 minutes, and 20 errors of the same level occur over 10 minutes, only three mentions of the error are recorded to the log: one for the first event and one at the end of each 5-minute interval afterwards. The default is 1 minute.

- **When an error occurs:**
  You can configure what should happen when the Gateway Service or the Filter encounters an error that prevents it from decrypting a message.
  - **Queue the encrypted message for later processing** (the default) leaves the message in the Journal mailbox, where processing is tried again until the error is resolved.
    If you select this option, check the Event log for messages that indicate when such an error has occurred, so that the error can be resolved, to allow the message to be processed.
    If one item in a message causes a failure, and the failure triggers this behavior, then the message will be left in the queue after the first failure. If a later retry succeeds, the remaining items will be processed.
  - **Pass the encrypted message through unprocessed** allows the message to be stored in the archive in an encrypted state.
    If one item in a message causes a failure, and the failure triggers this behavior, then it is possible that later items will never be processed.

  A message can contain more than one protected item (several protected attachments, several protected files within a Zip archive, multiple nested messages, etc.), and the behavior applies to the entire message, regardless of the level at which the failure occurs or how many separate pieces of protected content the message may contain. For example, if a message contains two protected attachments, and there is a protection failure on the first, then the whole message will be queued or passed through without examining the second attachment. In the queue case, the second attachment is examined after the first one is successfully unprotected on a retry. In the passthrough case, the second attachment passes through unmodified.

Advanced options

To work with advanced options, select the Advanced Options check box. Use caution when changing any of these options.

- **Gateway Service credentials**
  The account credentials under which the Gateway Service runs appear here. You cannot change the credentials with the Configuration Tool. You must use the Windows Services console. See "Changing the Gateway Service account credentials" on page 51.
- **Gateway Service port**
  The Gateway Service listens on a TCP port for requests coming from the Filter. Set the port here; the default is 7888. You should not need to change this setting unless some other program is already using this port.

- **Gateway statistics port**

  The Gateway Service gathers performance statistics while it is running, for example, the number of messages processed. (See "Performance statistics" on page 53.) The statistics are available through a Web service, which listens on this TCP port. The default is 7889. You should not need to change this setting unless some other program is already using this port.

- **Data Directory**

  The Adapter stores log files, lock files, and other temporary data in this directory. If you change this directory, make sure you give Full Control file system permissions on the new directory to both the Gateway Service account and the Enterprise Vault Service account. The default is:

  ${system:dirs:common-app-data}\EVSMRM

  ${system:dirs:common-app-data} is a variable that expands to a value set by the Windows environment, typically:

  ```
  C:\ProgramData
  ```

  The size of the data directory is generally quite small--on the order of a few megabytes. If Liquid Machines Document Control is enabled, the data can scale with the number of policies and keys, but will still not be more than a few megabytes unless you have an unusually large policy set. Also, when Liquid Machines Document Control is enabled, the data directory holds audit messages until they can be delivered to the server. That data is also usually quite small, but if the rate of processing of protected data is particularly high, and/or the server is not contacted for a long time, those queues can grow. No maximum is applied to them, because the Adapter cannot allow audit data to be lost.

- **Local Server Domains**

  Enter the domain name suffixes of your known and trusted servers. You can enter more servers than fit in the box; use the arrow keys to scroll. For information on how this list is used, see "Foreign protection checking with RMS" on page 17 and "Foreign protection checking with Liquid Machines Document Control" on page 19.

- **Find inline content encrypted with PGP**
  If users are using a PGP Client other than PGP Desktop, and you want to find encrypted content in the body of a message even when there is other content in the body of the message, select this check box and complete the following field. Scanning for inline PGP content applies only to plain-text messages and is only supported for messages using certain Windows code pages, or character sets (see "Supported PGP message formats" on page 13).
  - **Limit scanning to the first _ bytes**
    If you want to limit scanning to the beginning of the message for performance reasons, select this check box and select the number of bytes you want scanned. If this check box is not selected, the full body of the message will be scanned.
- **Limit expansion of Zips within Zips to _ levels**
  If you want to limit the number of Zip files expanded, select this check box and select the number of levels of Zip files you want expanded, including the top level. Decompression uses CPU and memory resources, and it is possible to create hostile Zip files that are deeply recursive, so we do not recommend that you disable this limit.
- **Limit size of decompressed files to _ MB**
  If you want to limit the size of decompressed files, select this check box and select the maximum size of decompressed files. Decompression of large files uses CPU and memory resources, and it is possible to create hostile Zip files that decompress from a small size to a very large size, so we do not recommend that you disable this limit.

Additional decryption keys (ADKs)

To decrypt PGP messages, the Adapter needs the appropriate keys, generally in the form of an ADK. You can upload one or more ADKs or upload user private keys to support small installations without ADKs.

For more information, on deploying and uploading keys, see the PGP documentation.

Deploying an ADK

To deploy an ADK using the PGP Desktop and deploy the ADK to users:

- You can import the ADK to the Universal Server configuration. Each new user key created by the Server or PGP Desktop contains the ADK, but the ADK must be manually added to any user keys that existed previously.
- Users can add ADKs to their existing user keys from the PGP Desktop.

If the Universal Server is later configured to use a different ADK, new user keys contain the newer ADK. Existing user keys are not updated automatically, but can be manually updated from the PGP Desktop to use the newer ADK. Any user key that has been manually updated to use an ADK must also be republished to any public key servers and directories maintaining a copy of the key, as well as redistributed to senders to whom a user has sent their key.

Using an ADK

All messages sent between users whose email policy is managed by the Universal Server are encrypted to an ADK, provided that the recipient's key contains an ADK. The Gateway Service can decrypt these messages, as well as any attachments that were either encrypted as part of the message or encrypted separately using the same user key.

The Gateway Service can decrypt messages received from external users provided that the sender's PGP Client honors the additional recipient request, as indicated by the presence of an ADK on the recipient's public key.

Any user key retrieved from a public key server before the addition of an ADK is not encrypted to a known ADK. The Gateway Service cannot decrypt messages that have been encrypted to a stale user key.

Uploading an ADK

To upload an ADK to the Adapter, export the ADK with its private key from PGP Desktop and import it into the Gateway Service, using the Key Upload utility. Each imported ADK is protected by an internally generated passphrase and persisted to the Gateway Service's key store, known as a Keyring. The ADK passphrase is persisted in secure storage accessible only by the Gateway Service Account. The Keyring is stored in a subdirectory of the Gateway Service's data directory.

Keep a copy of each ADK imported to the Gateway Service in a safe, secure location in case the Adapter needs to be reinstalled and ADKs need to be reimported.

The Key Upload utility

You can use the Key Upload utility to upload an ADK to the Gateway Service. The utility supports command-line parameters that allow you to specify the name of the file containing the key to be imported and the key's passphrase. The file is expected to be of the same format as that created by PGP Desktop when exporting a key to a file. The file can contain multiple keys, as long as each key is secured by the same passphrase.

The keys you are uploading must include the private key. The utility verifies that each key to be imported contains a private key before adding the key to the Keyring protected by an internally generated passphrase.

Importing a key having the same key ID as an existing key effectively updates that key. Otherwise, the key is added to the Keyring with no impact to existing keys.

To run the Key Upload utility successfully, the Gateway Service must be started, and PGP must be enabled in the Configuration file. PGP must also initialize successfully; check the Event log for any failures.

Enter the following command on the command line:

```
evsmrm_uploadkey [options] --secret=passphrase
list-of-key-files1
```

Note: Unless the PATH has been updated to include the product installation directory for the Adapter, you will need to navigate to this directory in a command prompt to run the utility.

Command line options

`--help, -h`	Displays a help message, describing all options that are available, and exits.
`--verbosity=`*`value`* `(-V)`	Controls the verbosity of console output. Lower values produce less output. Minimum value: -1 Maximum value: 4 Default value: 0
`--gateway-addr=`*`ip-address`* `(-a)`	The IP address of the server machine. (This should not be a multicast address.) Usually the default (localhost) is acceptable, and this option can be omitted.
`--gateway-port=`*`port`* `(-p)`	The socket port on which the Gateway Service is listening for connections. Minimum value: 1024 Maximum value: 49151 Default value:7888 Usually the default is correct, and this option can be omitted.
`--secret=`*`passphrase`* `(-s)`	The secret passphrase required to retrieve private keys from the *`list-of-key-files`*. Default value: *`password`*
`list-of-key-files`	The names of one or more files containing private keys exported from PGP Desktop. Wild cards can be used.

The Gateway Service must be restarted for newly uploaded keys to take effect.

Chapter 5

Managing the Gateway Service

This chapter includes the following topics:

Changing the Gateway Service account credentials

The account credentials for the Gateway Service can only be changed in the Windows Services console.

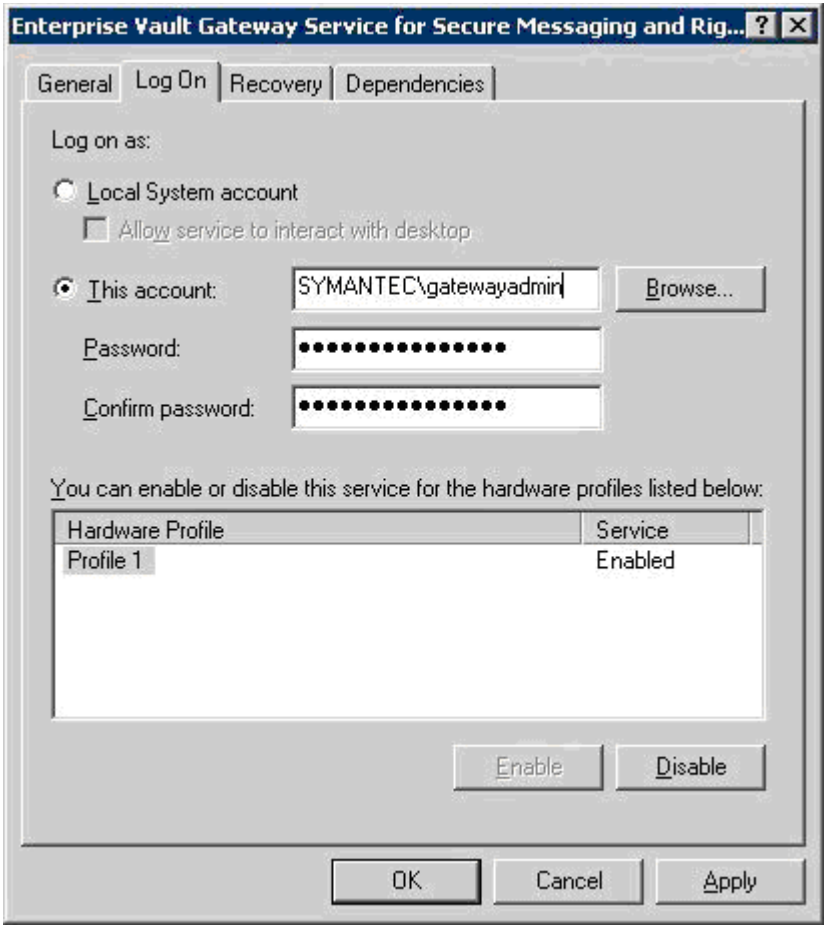
When you installed the Adapter, the installation granted the specified Gateway Service account full control on the data directory mentioned on page 45. If you change credentials, you must manually configure full control on this data directory for the new Gateway Service account.

The installation prerequisites instructed you to grant the Gateway Service account a number of special privileges, for example that of RMS Super User and that of being able to run as an RMS service. If you change credentials, you must complete all those same prerequisites for the new account.

To change the Gateway Service account credentials:

1. Open the Windows Services control panel.
2. Locate the Enterprise Vault Gateway Service.
3. Right-click the Gateway Service, and then click **Properties**.

4 On the **Log On** tab, be sure **This account** is selected. Then enter the domain-qualified user logon, for example, SYMANTEC\gatewayadmin, and the password.



5 Click **OK**.

6 The Gateway Service must be restarted for the change to take effect. To restart the Gateway Service, right-click it, and then click **Restart**.

Note: If you change the password on the existing Gateway Service account, repeat steps 1 to 3. On the **Log On** tab, type the new password, and then click **OK**. Again, you must restart the Gateway Service for the change to take effect.

Performance statistics

The Adapter keeps a number of performance counters that you can use to see how well it is running and gauge the amount of protected data present in your email infrastructure. Note that it is the Gateway Service, not the Filter, that keeps these statistics. When the Gateway Service is started, the statistics are cleared, that is, set back to zero.

You can use statistics to monitor and understand the operation of your Adapter. Consult with Symantec Technical Support on how best to do this for your configuration and environment. Below are some example approaches.

A large number of `client-requests-failed` or a high average `request-processing-time` (1000 milliseconds or more) may indicate a resource exhaustion problem on the Adapter computer or within your RMS or Active Directory infrastructure. Check your computer and operating system for other symptoms in the Event logs, such as out-of-memory errors, or timeout errors contacting RMS or Active Directory. You may want to restart the Gateway Service, and, if that does not work, then the Enterprise Vault Exchange Journaling task, in order to alleviate the exhaustion, until the problem can be better understood.

A steadily increasing number of `requests-in-progress` may indicate that a resource exhaustion problem is impending, or that mail transport queues are backing up. Check your Exchange server for steadily increasing message queue sizes or RAM consumption. You may want to restart the Gateway Service, and, if that does not work, then the Exchange Journaling task, in order to alleviate the exhaustion, until the problem can be better understood.

More counters appear in the display than are relevant to the Adapter. This is because the Statistics Service is common to other RMS adapter products. Only the statistics relevant to the Enterprise Vault Adapter for Secure Messaging and Rights Management are documented here.

The counters are available from a Web page. If you are logged onto the computer where the Adapter is installed, you can access it at the following URL: http://localhost:7889/status.

If you want to be able to access this URL from another computer, you can change the address and port on which the Adapter listens. For more information, see Appendix D, “Configuration file” on page 83.

.

Depending on your browser, you may be able to collapse and expand sections of the display. For example, in Internet Explorer:

- To collapse a section of the display, click its red minus sign (-). When you close a section, the minus turns to a plus (+).
- To expand a section of the display, click its red plus sign (+).

The display is written in eXtensible Markup Language (XML), so scripts or tools can process the output. The string at the top indicates this:

```
<?xml version="1.0" encoding="UTF-8" ?>
```

The next line shows the time and date the statistics were retrieved, called a *moment*:

```
<statistics moment="2005-06-17T17:09:46.125Z">
```

It shows the year, month, and day, and then the hour, minute, second, millisecond, and time zone.

`Z` indicates that the time is Coordinated Universal Time, not local time.

The remaining lines are grouped into sections: Counters, Levels, and Watches. Each section contains one or more items, and each item contains one or more values.

```
<section>
    <item one>
        <value one>0</value one>
        <value two>1</value two>
    </item one>
</section>
```

Counters

The first section contains counters. Counters keep track of how many times a particular event has happened since the Adapter was restarted. When the Adapter starts, the counter is set to zero (0), and each time a particular event happens, that event's counter increases by one.

Each counter has a name and a single, unlabeled value:

```
<counter-name>
    <value>#</value>
</counter-name>
```

The counters are:

- **client-connections-accepted**: How many times the Filter has initiated a network connection to the Gateway Service. This should be less than the number of requests, below, because the connections persist across requests. Regardless of message traffic, this number can become quite large, because of short-lived connections used by the Filter to monitor the health of the Gateway Service.
- **client-requests**: How many times the Filter has requested the Gateway Service to do something, such as process a message. Regardless of message traffic, this number can become quite large, because of requests used by the Filter to monitor the health of the Gateway Service.
- **client-requests-failed**: How many requests the Filter has made that have failed, because the Gateway Service refused them.
- **messages-unprotected**: How many messages were unprotected by the Adapter.
- **documents-unprotected**: How many documents were unprotected.

Levels

The second section contains levels. Levels measure how high some level has reached, or what its current setting is. For example, whereas a counter may say how many client connections have occurred, a level says how many are open right now. When the Adapter is restarted, all levels are reset to zero.

Each level has a name; a minimum and maximum value, which show the lowest and highest the counter has ever been; and a current value, which shows what the level was at the moment the results were retrieved.

```
<level-name>
    <current>#</current>
    <maximum>#</maximum>
    <minimum>#</maximum>
</level-name>
```

The levels are:

- **`open-client-connections`**: The number of open connections maintained from the Filter and the Configuration Tool to the Gateway Service. Generally this level will include one connection for each message processing thread in the Enterprise Vault Exchange Journaling task, plus a small number of additional connections for internal management tasks in the Adapter.
- **`requests-in-progress`**: The number of requests from the Filter that the Gateway Service is currently processing.

Watches

The last section contains watches. Watches measure the amount of time it takes to complete an action. For example, whereas a counter tells how many messages have been processed, a watch tells the longest time the Gateway Service ever took to process a message. That is, of all the messages the Adapter has processed, it has never taken more than N number of seconds to finish any one.

Each watch has a name, an average time, a maximum time, a minimum time, and a count of the events used to calculate the average. So, for example, it may have taken on average 300 milliseconds, never more than 1 second, and never less than 100 milliseconds to process a message, over the last 1000 messages processed.

```
<watch-name>
    <average-time-extent># ms</average-time-extent>
    <count>#</count>
    <maximum-time-extent># ms</maximum-time-extent>
    <minimum-time-extent># ms</minimum-time-extent>
</watch-name>
```

The watches are:

- **request-processing-time**: The amount of time it takes for the Gateway Service to return an answer to the Filter when it makes a request.
- **message-unprotecting-time**: The amount of time it takes for the Gateway Service to unprotect a message.
- **document-unprotecting-time**: The amount of time it takes for the Gateway Service to unprotect a document.

Diagnostic logging

The Adapter is also capable of generating diagnostic log file data suitable for analysis Symantec software engineers. Symantec Technical Support may require you to enable this logging as a part of a troubleshooting procedure. Support will provide instructions if necessary.

Indexing of RMS publishing license metadata

Microsoft RMS makes use of XrML within the publishing, or issuance, license of a protected email or document to describe a list of individuals given various rights or permissions on any piece of rights-protected content.

During archiving in Enterprise Vault, RMS-protected content is decrypted and reconstructed without its associated rights, then inserted into Enterprise Vault by the Adapter. As the content is being decrypted and reconstructed in plain text, the Adapter also adds the original metadata from the publishing license to the indexable item in Enterprise Vault. The metadata can be searched and retrieved during review.

This addition of index metadata only works for top-level items being archived into Enterprise Vault. In the case of email messages, different rights that might have existed on nested attachments—documents or email messages—do not have their metadata added to the index and are not searchable in this way.

The following table shows each display name for an RMS privilege, the corresponding Enterprise Vault index property name, and a description of the data.

Table 5-1 Metadata

Display Name	EV Index Property Name	Data
The following properties are set only for a top-level RMS-protected message unprotected by the Adapter; they are absent from any other messages.		
RMS Protected	RMSRights.PROTECTED	Set to **true** for any RMS-protected message unprotected by the Adapter. Absent for any other message. This allows an easy way to search for all messages that were unprotected.
Full Control	RMSRights.OWNER	Multiple values, each containing the email address of a user or group to whom this right is granted.
View Rights	RMSRights.VIEWRIGHTSDATA	Multiple values, each containing the email address of a user or group to whom this right is granted.
Export (Save As)	RMSRights.EXPORT	Multiple values, each containing the email address of a user or group to whom this right is granted.
Save	RMSRights.EDIT	Multiple values, each containing the email address of a user or group to whom this right is granted.
View	RMSRights.VIEW	Multiple values, each containing the email address of a user or group to whom this right is granted.
Print	RMSRights.PRINT	Multiple values, each containing the email address of a user or group to whom this right is granted.
Extract	RMSRights.EXTRACT	Multiple values, each containing the email address of a user or group to whom this right is granted.

Table 5-1 Metadata

Display Name	EV Index Property Name	Data
Edit	RMSRights.DOCEDIT	Multiple values, each containing the email address of a user or group to whom this right is granted.
Allow Macros	RMSRights.OBJMODEL	Multiple values, each containing the email address of a user or group to whom this right is granted.
Forward	RMSRights.FORWARD	Multiple values, each containing the email address of a user or group to whom this right is granted.
Reply	RMSRights.REPLY	Multiple values, each containing the email address of a user or group to whom this right is granted.
Reply All	RMSRights.REPLYALL	Multiple values, each containing the email address of a user or group to whom this right is granted.
License Acquisition URL	RMSRights.LICENSE_ACQUISITION_URL	Set to the licensing URL (for internal use) of the RMS server that controlled the protected data.
License Acquisition URL (for External access)	RMSRights.EXTRANET_LICENSE_ACQUISITION_URL	Set to the licensing URL (for external use) of the RMS server that controlled the protected data.
Owner	RMSRights.LICENSE_OWNER	Set to the single owner address included in the license, representing the original owner who always gets full rights. Distinct from the OWNER right, which can include multiple users. In normal usage, this field reflects the author of the content.

Table 5-1 Metadata

Display Name	EV Index Property Name	Data
Issuing Principal	RMSRights.LICENSE_ISSUER	Set to the principal that issued the license. For offline publishing, this will generally be the author. For online publishing, this will generally be the URL of the RMS server.
Require a connection to verify a user's permission	RMSRights.NOLICCACHE	Set to either **true** or **false**, based on whether the license inhibits license caching and thus requires a server connection on every use (meaning that offline access is not allowed).
Generated from an official template	RMSRights.OFFICIAL_TEMPLATE	Set to either **true** or **false**, based on whether the license came from an official (signed) template rather than a set of ad-hoc rights. This determines whether the server has validated the name and description fields below.
Name	RMSRights.NAME	Set to the name of the rights used (generally a template name) to protect the message. Absent if the name is empty or unavailable.
Description	RMSRights.DESCRIPTION	Set to the description of the rights used (generally a template description) used to protect the message. Absent if the description is empty or unavailable.

Indexing of PGP security properties

The following table shows each display name for a PGP security property, the corresponding Enterprise Vault Index property name, and a description of the data.

During archiving in Enterprise Vault, PGP-protected content is decrypted and reconstructed without its associated security properties, then inserted into Enterprise Vault by the Adapter. As the content is being decrypted and reconstructed in plain text, the Adapter also adds the original security properties to the indexable item in Enterprise Vault. The properties can be searched and retrieved during review.

This addition of index metadata only works for top-level items being archived into Enterprise Vault. In the case of email messages, different rights that might have existed on nested attachments—documents or email messages—do not have their metadata added to the index and are not searchable in this way.

A message can be protected with both RMS and PGP, in which case both sets of properties are saved.

Table 5-2 PGP Security Properties

Display Name	EV Index Property Name	Data
The following properties are set only for a top-level PGP-protected message unprotected by the Adapter; they are absent from any other messages.		
PGP-Encrypted	PGPSecurity.ENCRYPTED	Set to **true** on a previously encrypted message decrypted by the Adapter. Absent otherwise.
PGP-Encrypted and Signed	PGPSecurity.ENCRYPTED_AND_SIGNED	Set to **true** on a previously encrypted and signed message decrypted by the Adapter. Absent otherwise. Note that the property is not present on messages that are signed but not encrypted, since such messages are not modified by the Adapter.

Chapter 6

Troubleshooting

This chapter includes the following topic:

Common problems and how to fix them

The most common problem with the Adapter is a problem with the prerequisites or the Gateway Service account profile that results in a failure to connect.

RMS configuration problems

RMS configuration problems generate errors in the Application Event log, specifically ones that mention RMS. Typically, the event description also contains an RMS Client error string that begins with `DRM_`, for example `DRM_AUTHENTICATION_FAILED`.

To remedy this situation, check the following:

- Ensure that all the prerequisites were set up correctly. (See page 21.)
  - Ensure that the Gateway Service account was made an RMS Super User. (See page 24.)
  - Ensure that the Gateway Service account was configured to run as an RMS service. (See page 26.) If so, ensure that the procedure was executed on all RMS servers in your installation.
- Ensure that the RMS servers were added to the list of local intranet sites according to the instructions. (See page 75.)

Faulty prerequisites might have caused the RMS profile on the Enterprise Vault server computer to become corrupt. After you verify that all prerequisites are properly fulfilled, you might need to delete this RMS profile so that the Adapter can re-create it. The procedure to delete this RMS profile varies for Windows Server 2003 and Windows Server 2008.

To delete the RMS profile on Windows Server 2003:

1. Launch Windows Explorer and enter the following path in the address bar:
   `%ALLUSERSPROFILE%\Application Data\Microsoft\DRM\Server`
   Note: %ALLUSERSPROFILE% is an environment variable which is typically set to `C:\Documents and Settings\All Users`.
2. Delete all subdirectories listed in the directory.

To delete the RMS profile on Windows Server 2008:

1. Launch Windows Explorer and enter the following path in the address bar:
   `%ALLUSERSPROFILE%\Microsoft\DRM\Server`
   Note: %ALLUSERSPROFILE% is an environment variable which is typically set to `C:\programdata`.
2. Delete all subdirectories listed in the directory.

Note: You may need to enable **Show hidden files and folders** in Explorer to navigate to the files listed above.

Because Microsoft Outlook is installed on the computer, you can log on as the Gateway Service account, start Outlook, and test to see if you can send and receive protected messages. You can also test to see if you can open a protected message forwarded to the Gateway Service account, one that requires its Super User privilege to open.

PGP configuration problems

To remedy common PGP configuration problems, check the following:

- Ensure that the right ADK has been uploaded. (See page 47.)
- If you are not using ADKs, ensure that the appropriate user private keys were uploaded. (See page 46.)

Liquid Machines Document Control configuration problems

To remedy common Liquid Machines Document Control configuration problems, check the following:

- Ensure that the Liquid Machines Document Control Server was properly configured, and it can be contacted. (See page 12 and the *Liquid Machines Document Control Server Administration Guide*.)
- Ensure that the Gateway Service Account has appropriate policy permissions. (See page 27.)

Application Event logs

The Adapter logs important information about its operations to the Windows Application Event log on the Adapter computer. This section lists Errors, Warnings, and Informational messages you may receive. It tells what causes them and how to resolve the issues.

If you are unable to resolve problems using the procedures here, or if the problems recur frequently, contact Symantec Technical Support. Many events include diagnostic information, like stack traces of the code, which you may be asked to provide to Symantec Technical Support so that they can more closely analyze the problem.

Errors

- **A fatal error has occurred**: An error occurred that caused a process to terminate. The reason for the error is specified in the event description. This error may be logged either by the Filter or by the Gateway Service, depending on where it occurred. The error may terminate the Gateway Service or the Enterprise Vault Exchange Journaling task. In the former case, the Filter will automatically restart the Gateway Service. In the latter case, manual intervention will be necessary.

  Restart the Gateway Service, restart the Exchange Journaling task, and contact Symantec Technical Support.
- **A serious error has occurred**: An error has occurred, but the Adapter has recovered from it. The reason for the error is specified in the event description. This error may be logged either by the Filter or by the Gateway Service, depending on where it occurred.

  Contact Symantec Technical Support.

- **Enterprise Vault Adapter for Secure Messaging and Rights Management failed to restart Gateway Service**: The Filter needs to contact the Gateway Service in order to make a request. The Gateway Service is not running; the Filter has tried to start it but cannot.

  Check the Application Event log for any errors returned by the Gateway Service. Check to see if the Gateway Service is started in the Windows Services control panel.

  - If it is, consider restarting it.
  - If it is not, try to resolve any errors that might prevent it from starting. For example, maybe you need to type the correct password into the Gateway Service's start-up credentials or give the Gateway Service account the right to log in as a service on this computer.

- **Enterprise Vault Gateway Service for Secure Messaging and Rights Management rejected request**: The Filter or the Configuration Tool made a request to the Gateway Service that it cannot understand.

  Contact Symantec Technical Support.

- **Enterprise Vault Gateway Service for Secure Messaging and Rights Management failed to respond to request**: The Gateway Service was unable to properly complete a request, for an unknown reason.

  Contact Symantec Technical Support.

- **Failed to initialize Microsoft RMS**: The Adapter is unable to start up its profile for interacting with RMS.

  When this event occurs, any attempt the Adapter makes to unprotect messages will fail (and will log the **Failed to unprotect a message** event). You must remedy the situation and restart the Gateway Service to fully resolve this issue.

  Verify that your RMS infrastructure is working correctly. From an RMS and Office 2003 workstation, (ideally the Enterprise Vault server computer) log on as the Gateway Service account under which the Adapter runs and see if you can create and send a protected email. Verify that someone else can read it.

  You might need to reinitialize the Gateway Service account's machine-local profile data. To do this, stop the Adapter and delete the Gateway Service account's profile folder from the computer. This is typically located in the following directory:

  For Windows Server 2003:
  `C:\Documents and Settings\serviceaccountloginname`

  For Windows Server 2008:
  `C:\Users\serviceaccountloginname`

  Then log on to the Adapter computer as the Gateway Service account user under which the Adapter runs and restore any necessary settings (such as Local Intranet Sites entries for the RMS server), and start the Adapter.
- **Failed to unprotect a message**: The Adapter was unable to decrypt a message. Protection can fail for a variety of reasons. For example, a message may have been generated by a foreign RMS installation.

  You might want to follow the procedures for **Failed to initialize Microsoft RMS**, above.
- **Failed to unprotect a document**: A document unprotection failed.
- **Enterprise Vault Gateway Service for Secure Messaging and Rights Management initialization failed**: The Gateway Service has failed to start and will not process messages. Try restarting both the Gateway Service and the Exchange Journaling task and contact Symantec Technical Support.
- **Enterprise Vault Filter for Secure Messaging and Rights Management could not handle message format**: The Adapter has passed a message through because of an unhandled format or encoding.

- **Failed to initialize protection environment**: The generic protection features failed to initialize. Preceding events describe the status of each protection type.
- **Failed to initialize Liquid Machines Policies and Keys (Universal Enforcement Services)**: Liquid Machines Document Control was enabled and failed to initialize.
- **Failed to initialize PGP**: PGP was enabled and failed to initialize.

  When this event occurs, any attempt the Adapter makes to unprotect messages will fail (and will log the **Failed to unprotect a message** event). You must remedy the situation and restart the Gateway Service to fully resolve this issue.
- **Failed to update data for a Liquid Machines Policy Server**: A download or an upload failed for a server.

  When this event occurs, any attempt the Adapter makes to unprotect messages will fail (and will log the **Failed to unprotect a message** event). You must remedy the situation and restart the Gateway Service to fully resolve this issue.
- **Failed to process Zip archive**: Zip archive examination has been enabled, and the Adapter encountered a Zip archive that could not be processed at all (for example, an encrypted archive or a malformed archive).
- **Failed to process Zip archive entry**: Zip archive examination has been enabled, and the Adapter encountered an entry in a Zip archive that could not be processed at all (for example, one compressed using a nonstandard algorithm).
- **Enterprise Vault Gateway Service for Secure Messaging and Rights Management failed to upload decryption keys**: The Enterprise Vault Gateway Service for Secure Messaging and Rights Management failed to upload decryption keys.

Warnings

- **Enterprise Vault Filter for Secure Messaging and Rights Management state changed to PEND**: The Filter will hold messages in a queue, waiting to submit them to the Gateway Service for processing.

  Error handling in the Configuration Tool is set to "`Queue the encrypted message for later handling`" (or equivalently "`pend-message-on=error=true`" in the configuration file), and the Gateway Service has crashed, or is stopped but not set as disabled, and the Filter is attempting to restart it. If so, check the Application Event log for additional errors showing that the Filter failed to restart the Gateway Service. If you find these, troubleshoot what might be causing the restart failure.

  When the Filter leaves this state, it will log an Information entry to the Application Event log that the state has changed to `PROCESS`.

- **Enterprise Vault Filter for Secure Messaging and Rights Management state changed to PASSTHROUGH**: The Filter will not hold messages in a queue, but will instead pass them through without processing.

  Error handling in the Configuration Took is set to "`Pass the encrypted message through unprocessed`" (or equivalently "`pend-messages-on-error=False),` and the Gateway Service has crashed, is set as disabled, or has somehow been uninstalled, and the Filter is attempting to restart it. If so, check the Application Event log for additional errors showing that the Filter failed to restart the Gateway Service. If you find these, troubleshoot what might be causing the restart failure.

  When the Filter leaves this state, it will log an Information entry to the Application Event log that the state has changed to `PROCESS`.

- **Enterprise Vault Filter for Secure Messaging and Rights Management pended a message**: A message has been received by the Filter and has been queued, awaiting processing. This can occur when protected content is encountered in the PEND state, mentioned above, or when an internal error in the Filter occurs, if the `pend-messages-on-error` flag is set to `True`.

- **Enterprise Vault Filter for Secure Messaging and Rights Management passed a message through unprocessed**: A message has been received by the Filter and was passed through unprocessed. This can occur when protected content is encountered in the PEND state mentioned above, or when an internal error occurs in the Filter, if the `pend-messages-on-error` flag is set to `False`.
- **Zip archive exceeded recursion depth limit**: Zip archive examination has been enabled, and the Adapter encountered nested Zip archives in excess of the configured depth.
- **Zip archive entry exceeded decompressed size limit**: Zip archive examination has been enabled, and the Adapter encountered a single file larger than the configured size limit.

Informational messages

- **Enterprise Vault Filter for Secure Messaging and Rights Management has been initialized**: The Exchange Journaling task has loaded the Filter, and it is ready to handle messages.
- **Enterprise Vault Filter for Secure Messaging and Rights Management has been shut down**: The Exchange Journaling task has unloaded the Filter, and it is no longer handling messages.
- **Enterprise Vault Filter for Secure Messaging and Rights Management event processing started**: The Filter has detected its first event and is now actively processing messages.
- **Enterprise Vault Filter for Secure Messaging and Rights Management state changed to PROCESS**: The Filter has recovered from a PEND or PASS state, as documented in Warnings, above.
- **Enterprise Vault Filter for Secure Messaging and Rights Management restarted Gateway Service**: The Filter has successfully restarted the Gateway Service.
- **Enterprise Vault Gateway Service for Secure Messaging and Rights Management has been initialized**: The Gateway Service has started successfully.
- **Enterprise Vault Gateway Service for Secure Messaging and Rights Management has been shut down**: The Gateway Service has stopped gracefully.
- **Enterprise Vault Gateway Service for Secure Messaging and Rights Management uploaded decryption keys**: Keys were successfully uploaded using evsmrm_uploadkey.

- **Protection environment initialized**: All configured protection features have been initialized. Generic features were successful; preceding events describe the status of each protection type.
- **Microsoft RMS session initialized**: The Adapter has successfully initialized the profile it uses to connect with your RMS infrastructure.
- **Liquid Machines Policies and Keys (Universal Enforcement Services) initialized**: Liquid Machines Document Control was successfully enabled and initialized.
- **PGP initialized**: PGP was successfully enabled and initialized.
- **Successfully updated data for a Liquid Machines Policy Server**: A poll to a Liquid Machines Document Control server has completed successfully.
- **Failed to unprotect a message from external server**: A message unprotection failed on content that comes from a server that is not determined to be local.
- **Failed to unprotect a message without decryption key**: A message unprotection failed on content that could not be decrypted by any of the uploaded keys.
- **Failed to unprotect a document from external server**: A message unprotection failed on content that comes from a server that is not determined to be local.
- **Failed to unprotect a document without decryption key**: A document unprotection failed on content that could not be decrypted by any of the uploaded keys.

Appendix A

Clearing the Active Directory cache from the RMS installation

This appendix includes the following topic:

Clearing the Active Directory cache from the RMS installation

We recommend that you make a backup copy of the RMS databases before making these changes.

1. Log on to the Microsoft SQL Server computer that hosts the RMS Server databases as an account with SQL system administrator privileges.
2. Start SQL Enterprise Manager. On the Windows taskbar, click **Start > Programs > Microsoft SQL Server > Enterprise Manager**.
3. Navigate the tree of servers and databases to expand the DRMS_DirectoryServices database. The name of this database typically ends with the name of the server cluster and the TCP port on which it listens, for example, _rms_80.
4. To display the list of tables on the right, click **Tables**.
5. Right-click the first appropriate table, PrincipalAliases, and then click **Open Table > Return all rows**. A new console child window appears with the records in the table listed.

Clearing the Active Directory cache from the RMS installation

6. Click the gray box to the left of the first row. To select all records, hold **Shift** and click the gray box next to the last row.
7. Press **Delete**. A dialog box asks you to confirm that you want to delete all rows. Click **Yes** to continue.
8. Repeat step 5, step 6, and step 7 for the following tables:
   - PrincipalMembership
   - PrincipalIdentifiers
   - GroupAliases
   - GroupMembership
   - GroupIdentifiers

Appendix B

Adding RMS servers to the local intranet sites

This appendix includes the following topic:

For information, see "Initializing and configuring the Gateway Service account profile (RMS Only)" on page 27.

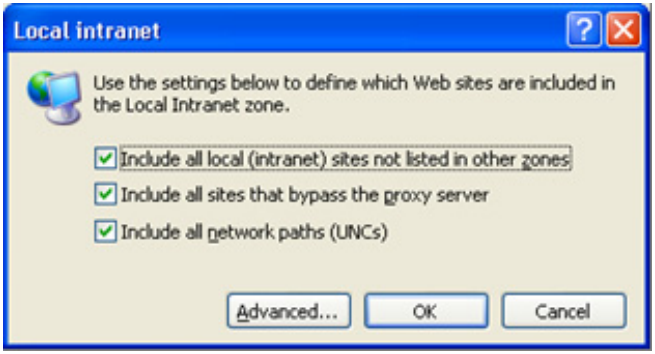
Adding RMS servers to the local intranet sites

1. Log on to the Enterprise Vault server computer as the Gateway Service account under which the Adapter will run.
2. In Internet Explorer, on the **Tools** menu, click **Internet Options**.

Adding RMS servers to the local intranet sites

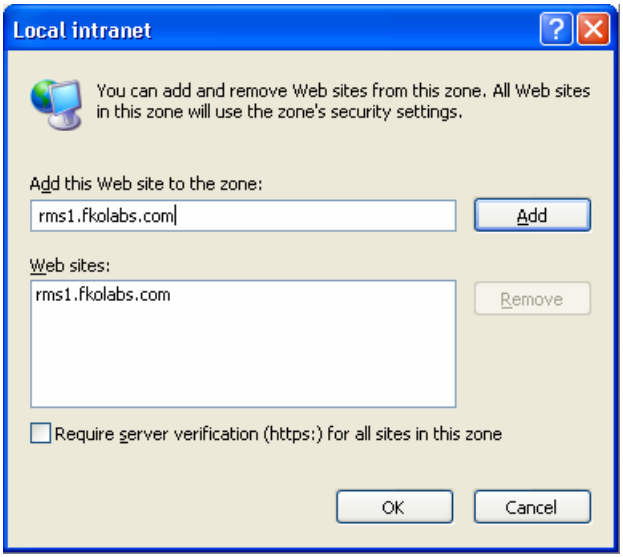
3 In the **Internet Options** dialog box, click the **Security** tab.

4 On the **Security** tab, click **Local intranet**, and then click **Sites**.



5 On the Local intranet dialog box, click **Advanced**.

6 In the **Add this web site to the zone** field, enter the common name of the RMS Server, for example, `rms1.fkolabs.com`. Then click **Add**.



7 Click **OK** to close all dialog boxes.

Adding RMS servers to the local intranet sites

Appendix C

Enabling support for international characters

This appendix includes the following topic:

- "Enabling support for international characters" on page 81

For information, see "Software" on page 21.

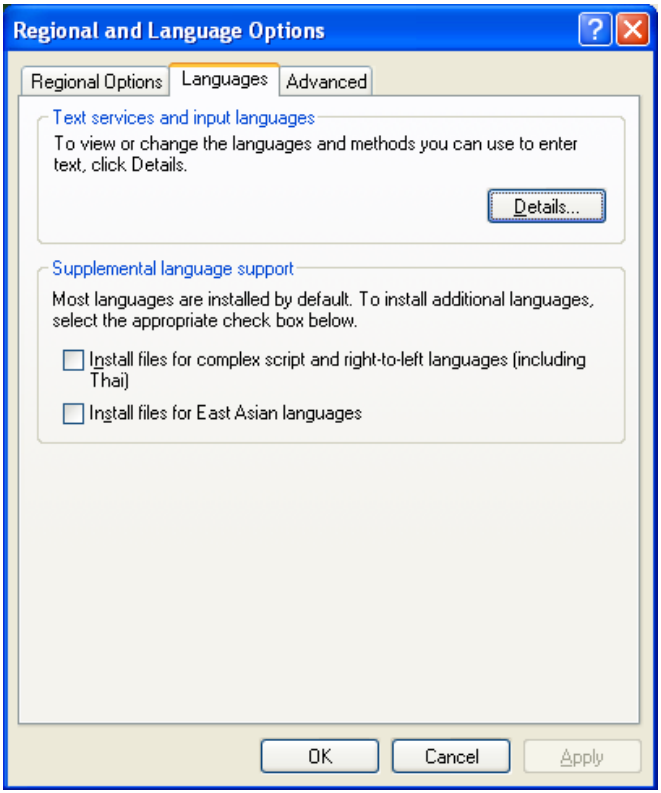
Enabling support for international characters

When using Windows Server 2003, in order for the Gateway Service to successfully decrypt plain-text PGP messages with international characters, you must install Windows support for all international character sets on the server machine. This requires installing some files from the Windows CD as described below.

When using Windows Server 2008, international character support is enabled during the default installation.

To enable support for international characters for Windows Server 2003:

1. On the Windows taskbar, click **Start > Control Panel > Regional and Language Options**.
2. In the **Regional and Language Options** dialog box, click the **Languages** tab.



3 Under **Supplemental language support**, select the **Install files for complex script and right-to-left languages (including Thai)** check box.

4 A message tells you that the files will require 10 MB or more of disk space and that they will be installed after you click **OK** or **Apply**. Click **OK** on the message.

5 Under **Supplemental language support**, select the **Install files for East Asian languages** check box.

6 A message tells you that the files will require 230 MB or more of disk space and that they will be installed after you click **OK** or **Apply**. Click **OK** on the message.

7 On the **Languages** tab, click **OK** or **Apply**.

8 When the **Insert Disk** message appears, do one of the following:

- Insert the Windows CD into your CD-ROM drive and then click **OK**.
- Click **OK** and then select an alternate location from which to copy the files, such as a floppy disk or a network server.

If you want full support for the full range of code pages, after you complete the steps above, follow these additional steps on the Enterprise Vault server machine:

1 In the **Regional and Language Options** dialog box, click the **Advanced** tab.

2 Under Code page conversion tables, select all the check boxes, to install converters for all the code pages.

3 Click **OK**.

Appendix D

Configuration file

This appendix includes the following topics:

Overview

The operational behavior of the Enterprise Vault Adapter for Secure Messaging and Rights Management can be controlled with a Configuration file. Some of the options in the Configuration file can also be managed from the Configuration Tool. (See page 38.) Changes you make using the Configuration Tool are written to the Configuration file. Options that can also be changed from the Configuration Tool are **underlined** in this section.

The Configuration file is located in the folder in which the Adapter is installed. Typically it can be found at the following location:

```
C:\Program Files (x86)\Enterprise Vault\Adapter for
Secure Messaging and Rights Management\evsmrm-config.xml
```

The Configuration file is written in the XML language. You can use Notepad or another text editor to make changes to it. XML uses *elements*, delimited by angle brackets (<>). An element usually begins with a start-tag (`<pend-message-on-error>` in the first example below) and ends with an end-tag that begins with a slash (`</pend-message-on-error>`).

Note: If you use any international characters (non-ASCII characters), be sure to select the "Unicode" encoding option when saving the file.

In the Configuration file, the tags surround *settings* (like `false`). Elements can include other elements, as in the second example; we call the outer elements *sections*. Sections can be nested, in which case we call the inner sections *subsections*.

You can use *variables* in the file: type in a certain string, and, when the Gateway Service runs, it changes the string to a value particular to that computer. You can add *comments* to the file that the Gateway Service will ignore when processing the file, so you can include information about your company policies or your IT infrastructure. Enter a comment between `<!-- and -->`, like this: `<!-- comment -->`

***Example**:*

```
<pend-message-on-error>false</pend-message-on-error>
```

This setting controls how the Adapter handles messages. The `pend-message-on-error` setting is opened, the value `false` is put in, and then the setting is closed.

***Example**:*

```
<logging>
     <root-dir>${system:dirs:common-app-data}\EVSMRM </root-dir>
</logging>
```

This example shows the setting `root-dir`, with the following value: *`${system:dirs:common-app-data}`*`\EVSMRM`

It also shows the tab embedded within the logging setting, or section.

***Example**:*

```
<bind-addr>${system:host:ip-addr}</bind-addr>
```

This example shows the setting `bind-addr`. A variable is used for the value. When the Gateway Service starts, it changes the variable to the IPv4 address of the first Ethernet interface of this computer.

Extra whitespace can be included between elements and will be ignored. However, you should not include extra whitespace between the start and end tags that define a value (for example, a path).

To pick up changes you have made to the Configuration file, restart the Gateway Service. If the Gateway Service fails to start, check the Application Event log for an error indicating a problem with the Configuration file, such as an invalid value or improper syntax. Note that when the Gateway Service and the Configuration file are correctly configured, restarting the Gateway Service neither disrupts message flow nor affects the operation of other critical services.

Some settings affect the Filter and thus require that the Exchange Journaling task be restarted as well. After changing the Configuration file, restart the Gateway Service first, because it can validate all parameters and report any problems. Then restart the Exchange Journaling task.

Sections

These are currently the main sections in the Configuration file:

- **`logging`**: Parameters that control how and where the Adapter logs diagnostic information.
- **`gateway-service`**: Parameters that control the behavior of the Gateway Service.
- **`protection-config`**: Parameters that control how the Gateway Service unprotects content.
- **`zip-archives`**: Parameters that enable or disable examination of Zip files.
- **`reporting`**: Parameters that control the verbosity and other behaviors of application event logging.
- **`monitoring`**: Parameters that control the behavior of the Performance Statistics XML page.
- **`adapters`**: Parameters that control behaviors specific to the Filter component.

Settings

Settings are grouped by section. For most settings, default values are in parentheses.

Note: Some settings in the file are not documented here. These settings are clearly marked ***Do not change this without consulting Support***.

---

logging settings

- **root-dir**: The location where the Adapter stores log files when verbose diagnostic logging has been turned on. The default value is:
  `${system:dirs:common-app-data}\EVSMRM\logs`
  Note: If the data directory is changed in the Config UI, this value will also be changed to be a sub-directory of the new data directory.
- **max-backup-logfile-count**(2): The maximum number of old log files to keep around before deleting the oldest. The minimum value is 0; the maximum value is 100 (inclusive).
- **max-logfile-size**(10 MB): The maximum size any log file is allowed to reach before being rolled over to backup files. The minimum value is 100 KB; the maximum value is 1 TB (inclusive).
- **max-logfile-lifetime**(1 day): The maximum amount of time any log file is allowed to be used before being rolled over to backup files. The current remaining time extent is calculated from the previous midnight. The minimum value is 1 hr; the maximum value is infinite (inclusive).

gateway-service settings

- **data-dir**: The location where the Adapter stores bookkeeping data. The default value is:
  `${system:dirs:common-app-data}\EVSMRM`

networking subsettings

- **bind-addr**(127.0.0.1): The IP address on which the Gateway Service listens for network connections. For security reasons, this should generally not be changed.
- **bind-port**(7888): The TCP port on which the Gateway Service listens.

request-limits subsettings

Configures the limits on how requests will be accepted and processed by the Gateway Service. Since Enterprise Vault has its own limits, these settings usually do not need to be changed.

- **max-concurrent-requests** (50): The maximum number of requests which will be executed simultaneously. Further requests wait for processing until earlier requests are complete. The minimum value is 1 and the maximum value is 100.

- **max-request-wait-time** (infinite): The maximum amount of time any given request can wait for acceptance. Timeout will cause the request to fail. The minimum value is 0, meaning the requests always fail immediately when the concurrent limit is exceeded and the maximum value is infinite.
- **max-request-size** (250 MB): This value determines the largest request which will be accepted for processing. The minimum value is 1 KB and the maximum value is 1 GB.

protection-config settings

- **unprotectable-server-suffixes**: Content that has been protected by RMS or Liquid Machines Document Control contains the name of the server used to protect it. These names take the form of a host name like rms.symantec.com. See "Local Server Domains" on page 45. If one of these suffixes matches, then a failure to unprotect is considered an error, causing retry, queue, or passthrough as configured. If none of these suffixes match, then a failure to unprotect is not considered an error, but results in content remaining protected. Matching is not case-sensitive. An empty suffix, or no setting at all, matches anything.

ms-rms subsettings

- **enabled** (false): Enables or disables all RMS functionality.

lm-ues subsettings

Default values are in parentheses.

- **enabled** (false): Enables or disables all Universal Enforcement Services functionality.
- **policy-servers**: Policy Servers that should be contacted to obtain policy information, identified by host-name or by URL. Servers can be identified by host name or by URL, for example, <policy-server>server.mydomain.com</policy-server>.
- **allow-server-discovery** (true): Enables the ability to contact new LMDC servers based on document contents.
- **discovered-server-lifetime** (60 min): Configures the time for which discovered servers will be kept active (and polled) before they must be discovered again.
- **discovered-server-cleanup-period** (5 min): Indicates how often discovered servers should be checked and deactivated if they are past their maximum configured lifetime.

forward-proxy-specification subsettings

Allows configuration of a forward proxy if one is required in order to communicate with the LMDC Server.

- **proxy-type** (DIRECT): Indicates whether a proxy should never by used (DIRECT), always be used (TUNNEL), or whether the Gateway should attempt to detect proxy configuration from the network (AUTO-DETECT).
- **try-direct-first** (false): Controls whether the gateway should always try a direct connection to the server before using a proxy.

proxy-server subsettings

The Proxy Server to use when the proxy-type is TUNNEL.

- **proxy-server-addr** (proxy.example.com): The host name or IP address of the proxy server.
- **proxy-server-port** (80): The port number of the proxy server.

outbound-ssl subsettings

Configures settings for secure connections to the LMDC Server.

- **enable-peer-cert-checking** (true): Determines whether the server's SSL certificate will be checked by the Gateway. Disable this only if you are having trouble obtaining the correct root certificate, and are sure that the server is trustworthy.

pgp subsettings

- **enabled** (false): Enables or disables all PGP functionality.
- **scan-limit** (0): The number of bytes to scan at beginning of the message for a candidate PGP tag. 0 indicates no scanning (header must be in initial bytes); -1 indicates unlimited scanning.

zip-archives settings

- **enable-inspection** (true): Enables or disables inspection of Zip files.
- **inspect-zip-entry-filetypes**: Specifies the types of files within a zip archive that should be inspected. Each is represented by an entry like this: <zip-entry-filetype>doc</zip-entry-filetype>. Specifying no filetypes causes all files within a Zip archive to be examined. An empty filetype causes files with no extensions to be examined.
- **decompressed-size-limit** (50 MB): Limits the size of files to be decompressed for examination.
- **max-recursion-depth** (4): Specifies the depth of recursion into nested Zip archives. This value is one less than the corresponding value in the Configuration Tool. 0 indicates examination of a single-level Zip file with no recursion; -1 indicates unlimited recursion.

reporting settings

- **event-log-severity** (All): The minimum severity of events that are sent to an Application Event log. Values are fatal, error, warning, and info.
- **log-frequency-error** (1 minute): The maximum frequency at which the same type of error can be reported in the Event log before multiple occurrences are batched in a single entry, and how frequently such batches are reported. Setting **Combine occurrences** in the Configuration Tool changes this setting. (See page 43.)
- **log-frequency-warning** (1 minute): The maximum frequency at which the same type of warning can be reported in the Event log before multiple occurrences are batched in a single entry, and how frequently such batches are reported. Setting **Combine occurrences** in the Configuration Tool changes this setting. (See page 43.)
- **log-frequency-info** (1 minute): The maximum frequency at which the same type of Info message can be reported in the Event log before multiple occurrences are batched in a single entry, and how frequently such batches are reported. Setting **Combine occurrences** in the Configuration Tool changes this setting. (See page 43.)
- **batching-period** (1 minute): How often the Gateway Service and Filter examine any pending batches of log entries for reporting in the Event log. Batched log entries can be logged any time after the time defined by their frequency has passed but are not examined for possible logging unless another of the same event occurs or a batching period elapses.

monitoring settings

- **enabled** (`true`): Whether the Adapter collects performance statistics and displays them in a simple XML Web page. These are discussed in "Performance statistics" on page 53.

networking subsettings

`networking` subsettings control how the Performance Statistics Web Service connects to the network, such as the IP address and port.

Default values are in parentheses.

- **bind-addr** (`127.0.0.1`): The IP address on which the Performance Statistics Web Service listens for network connections. If you would like the status page to be accessible remotely, set this to the primary IP address of the host computer.
- **bind-port**(`7889`): The TCP port on which the Performance Statistics Web Service listens.

request-limits subsettings

Configures the limits on how requests will be accepted and processed by the Gateway Service.

- **max-concurrent-requests** `(5)`: The maximum number of requests which will be executed simultaneously. Further requests wait for processing until earlier requests are complete. The minimum value is 1 and the maximum value is 100.
- **max-request-wait-time** `(infinite)`: The maximum amount of time any given request can wait for acceptance. Timeout will cause the request to fail. The minimum value is 0, meaning the requests always fail immediately when the concurrent limit is exceeded and the maximum value is infinite.
- **max-request-size** `(1 KB)`: This value determines the largest request which will be accepted for processing. The minimum value is 1 KB and the maximum value is 1 GB.

adapters settings

- **pend-message-on-error** (`true`): How the Filter handles messages that cannot be processed successfully, after any rapid retries configured below are exhausted. If true, messages are held in a queue for processing later. If false, messages pass through unprocessed.
- **ping-gateway-service** (`5 seconds`): How often the Filter tests the Gateway Service to see if it is up and communicating, and to restart it if it has crashed. This value should be short enough that a ping will occur and the Gateway Service can be restarted, if necessary, before a message exhausts its retry-connection-delay intervals, described below.
- **retry-connection-delay**: How many times and at what intervals the Filter tries to connect to the Gateway Service before giving up. These rapid retries apply only to communications or decryption, including between the Filter and the Gateway Service, and problems communicating with a policy server.

  In the case of repeated failures, the Filter uses each of these intervals in order. If failures persist, the Filter either queues and retries messages or passes them through, based on its configuration. For example, if you use the defaults of 1 second, 2 seconds, 4 seconds, 8 seconds, and 16 seconds, the Filter retries after 1 second, then retries again after an additional 2 seconds, then again after an additional 4 seconds, 8 seconds, and 16 seconds. At that point, the message is either queued and retried again each time the Exchange Journaling task runs or passed through, according to the configuration.

evfilter subsettings

- **save-protection-info** (`true`): If true, information on the prior protection of content will be saved in index properties for later searching.
- **state-affects-all-messages** (`false`): If true, an Adapter state of PEND or PASSTHROUGH will affect all messages, rather than only protected messages.

Variables

The following variables can be used in some configuration settings. To use one, enclose it in braces { } and preface it with a dollar sign ($), like this: ${run:thread:id}

Place the variable in the Configuration file in the place where you want its value to be substituted.

- **env**: The value of any system environment variable; it is case insensitive on Windows. For example ${env:HOMEDRIVE} yields the value of HOMEDRIVE, typically C.
- **run:thread:id**: The ID of the current thread.
- **run:thread:name**: The descriptive name of the current thread (if any).
- **run:moment**: The current moment in time.
- **run:host:name**: The current fully-qualified DNS name of this host, for example, rms1.acme.lan, as it is set at runtime.
- **run:host:ip-addr**: The current IPv4 address of the first Ethernet adapter on this host, for example, 192.168.130.1, as it is set at runtime.
- **system:dirs:cwd**: The current working directory.
- **system:dirs:temp**: The current user's temp directory, typically: C:\Documents and Settings\currentuser\Local Settings\Temp
- **system:dirs:user**: The current user's home directory, typically: C:\Documents and Settings\currentuser
- **system:dirs:common-app-data**: The directory containing application data common to all users, typically: C:\Documents and Settings\All Users\Application Data
- **system:dirs:user-app-data**: The directory containing application data specific to the current user, typically: C:\Documents and Settings\currentuser\Application Data
- **system:host:name**: The fully-qualified DNS name of this host, as it is set at system start.
- **system:host:ip-addr**: The IPv4 address of the first Ethernet adapter of this host, as it is set at system start.

- **system:host:primary-domain-name**: The fully-qualified DNS name of the domain name of the first Ethernet adapter for this host, as it is set at runtime. For example, if this hostname is `ev1.example.com`, then the domain is `example.com`.
- **app:dirs:install**: The installation directory for the application, by default:
  `C:\Program Files\Enterprise Vault\Adapter for Secure Messaging and Rights Management`

Indexf

D

E

F

G

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z