

Symantec Compliance Accelerator™

Installation Guide

11.0



Symantec Compliance Accelerator: Installation Guide

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

Last updated: 2014-11-04.

Legal Notice

Copyright © 2014 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo, Enterprise Vault, Compliance Accelerator, and Discovery Accelerator are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the *Third Party Software* file accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Symantec as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street, Mountain View, CA 94043

<http://www.symantec.com>

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to help you resolve specific problems with a Symantec product. 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 software upgrades
- 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 website 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, DVDs, 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_apj@symantec.com

Europe, Middle-East, and Africa semea@symantec.com

North America and Latin America supportsolutions@symantec.com

Contents

Technical Support	3	
Chapter 1	Introducing Compliance Accelerator	8
	Key features of Compliance Accelerator	8
	About the Compliance Accelerator components	9
	Product documentation	9
	White papers on the Symantec Support website	10
	"How To" articles on the Symantec Support website	10
	Comment on the documentation	11
Chapter 2	Preparing to install Compliance Accelerator	12
	Configuration options for Compliance Accelerator	12
	Compliance Accelerator configuration for large installations	13
	Compliance Accelerator configuration for smaller installations	13
	Supported versions of Enterprise Vault in Compliance Accelerator environments	14
	Prerequisites for Compliance Accelerator	15
	Prerequisites for the SQL Server computer	15
	Prerequisites for the Compliance Accelerator server computer	15
	Prerequisites for Compliance Accelerator client computers	18
	Configuring Outlook to enable the processing of items with many attachments or many recipients	19
	Setting the Windows and ASP.NET Temp folder permissions	20
	Security requirements for temporary folders	21
	Granting additional users and groups access to the temporary folders	22
	Disabling networking facilities that can disrupt a Compliance Accelerator environment	22
	Disabling the Windows Search Service on the Compliance Accelerator server	23
	Configuring the SQL Server Agent service	23
	Assigning SQL Server roles to the Vault Service account	24
	Verifying that Enterprise Vault expands distribution lists	26

Chapter 3	Installing Compliance Accelerator	28
	Installing the Compliance Accelerator server software	28
	Allowing Enterprise Vault to communicate with Compliance Accelerator through the Windows firewall	29
	Creating the configuration database and customer databases	30
	Uploading the Compliance Accelerator report templates	36
	Installing Compliance Accelerator in a clustered environment	39
	Maximizing security in your Compliance Accelerator databases	40
	Installing the Compliance Accelerator client software	40
	Modifying the configuration file for the Compliance Accelerator client	40
	Using the MSI installer package to install the Compliance Accelerator client	41
	Uninstalling Compliance Accelerator	42
Appendix A	Ports that Compliance Accelerator uses	43
	Default ports for Compliance Accelerator	43
	Changing the ports that Compliance Accelerator uses	44
Appendix B	Troubleshooting	46
	Enterprise Vault Accelerator Manager service not created	46
	Enterprise Vault Accelerator Manager service does not start	47
	Home page of Compliance Accelerator website not found	47
	Cannot create or upgrade Compliance Accelerator customer databases when Symantec Endpoint Protection is running	49
	Permissions error when uninstalling the Compliance Accelerator client from a UAC-enabled computer	49
	Uninstalling the Compliance Accelerator client from a shared location may prevent other users from starting the client	50
Index		51

Introducing Compliance Accelerator

This chapter includes the following topics:

- [Key features of Compliance Accelerator](#)
- [About the Compliance Accelerator components](#)
- [Product documentation](#)

Key features of Compliance Accelerator

Compliance Accelerator lets organizations perform cost-effective supervisory review of their employees' communications to ensure compliance with regulatory bodies.

Among the key features of Compliance Accelerator are the following:

- A system for defining the employees that are to be monitored and grouping them in an organizational structure that reflects the departments within the company. The messages of selected *exception* employees can be kept separate and reviewed by specially assigned reviewers.
- The facility to capture a random sample of the items that have been sent to the Enterprise Vault archive of a journal mailbox.
- A client application that lets administrators configure Compliance Accelerator and designated reviewers read and mark the captured items.
- A secure SQL database that keeps information on all the monitored employees, captured items, and the review process that you have applied to the items.

About the Compliance Accelerator components

[Table 1-1](#) lists the primary Compliance Accelerator components.

Table 1-1 The Compliance Accelerator components

Component	Notes
Compliance Accelerator client	The client is used by Compliance Accelerator administrators to set up and manage the system and by reviewers to access the items that they are to mark.
Accelerator Manager website	This website lets you set up multiple Compliance Accelerator databases in which to store your data.
Enterprise Vault Accelerator Manager service	This service handles the requests from the Compliance Accelerator client and works with the Enterprise Vault components to access archives, perform searches, and so on.
Customer database	The customer database is a SQL database in which Compliance Accelerator stores details of departments, user roles, search results, and more. You can set up multiple customer databases.
Configuration database	The configuration database is a SQL database that specifies the location of the customer databases and stores details of the SQL Server, database files, and log files to use.
Compliance Accelerator website	This website provides functionality for some of the Compliance Accelerator reports.

Compliance Accelerator 11.0.1 does not include the Journaling Connector component that came with earlier versions of Compliance Accelerator. In version 11.0.1, all the functions of the Journaling Connector have been incorporated into Enterprise Vault itself.

Product documentation

[Table 1-2](#) lists the documentation that is available for Compliance Accelerator.

Table 1-2 The Compliance Accelerator documentation set

Document	Comments
Installation Guide	Outlines how to perform a first-time installation of the Compliance Accelerator server and client software.
Upgrade Instructions	Explains how to upgrade an existing installation of Compliance Accelerator to version 11.0.
Administrator's Guide	Provides information for Compliance Accelerator administrators on how to set up and assign roles, search for items to include in the review set, export items for offline review, create reports, and more.
Reviewer's Guide	Describes the features of the Compliance Accelerator client that are available to reviewers.
Online Help	Accompanies all the Compliance Accelerator applications and provides extensive information on how to use their facilities.
Release Notes	Provides late-breaking information that you may need to be aware of before you install and use Compliance Accelerator.

White papers on the Symantec Support website

For more information on the deduplication features in Compliance Accelerator, see the *Accelerator Deduplication* white paper. This is available from the following page of the Symantec Support website:

<http://www.symantec.com/docs/DOC3621>

"How To" articles on the Symantec Support website

Most of the information in the Compliance Accelerator manuals is also available online as "How To" articles on the Symantec Support website. You can access these articles by searching the Internet with any popular search engine, such as Google, or by following the procedure below.

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

- 1 Type the following in the address bar of your web browser, and then press **Enter**:
http://www.symantec.com/business/support/all_products.jsp
- 2 In the **Supported Products A-Z** page, choose **Enterprise Vault Compliance Accelerator**.

- 3 In the **Product Support** box at the right, click **How To**.
- 4 Search for a word or phrase by using the Knowledge Base Search feature, or browse the list of most popular subjects.

Comment on the documentation

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

Please include the following information with your comment:

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

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

We appreciate your feedback.

Preparing to install Compliance Accelerator

This chapter includes the following topics:

- [Configuration options for Compliance Accelerator](#)
- [Supported versions of Enterprise Vault in Compliance Accelerator environments](#)
- [Prerequisites for Compliance Accelerator](#)
- [Configuring Outlook to enable the processing of items with many attachments or many recipients](#)
- [Setting the Windows and ASP.NET Temp folder permissions](#)
- [Security requirements for temporary folders](#)
- [Disabling networking facilities that can disrupt a Compliance Accelerator environment](#)
- [Disabling the Windows Search Service on the Compliance Accelerator server](#)
- [Configuring the SQL Server Agent service](#)
- [Assigning SQL Server roles to the Vault Service account](#)
- [Verifying that Enterprise Vault expands distribution lists](#)

Configuration options for Compliance Accelerator

Compliance Accelerator is a client/server application. The client software runs on a Windows workstation, and the server software runs on a Windows server. For optimum performance, we strongly recommend that you install the server software

on a dedicated computer rather than your normal Enterprise Vault server. A SQL Server computer stores all the configuration and customer information.

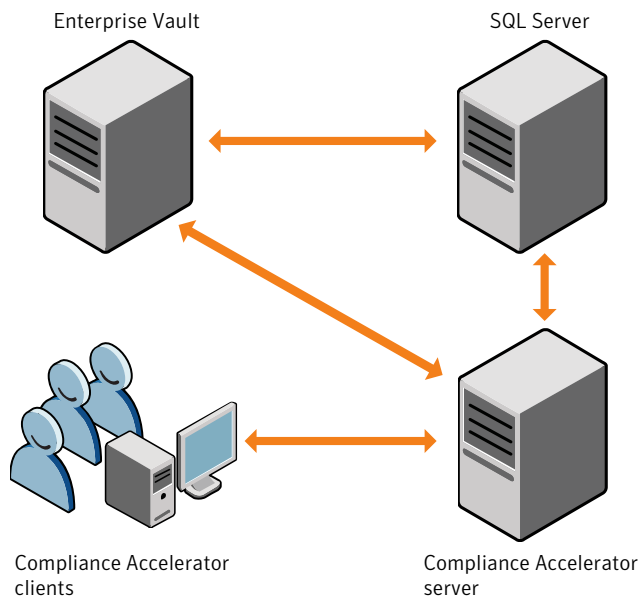
You can choose from several configuration options. If your planned configuration is different and you are unsure of what to configure on the Compliance Accelerator computer, contact Symantec for advice.

Compliance Accelerator configuration for large installations

A self-contained installation of Compliance Accelerator with a separate SQL Server computer minimizes the effect that intensive Compliance Accelerator searches and export runs have on the Enterprise Vault installation. This configuration is likely to suit larger installations.

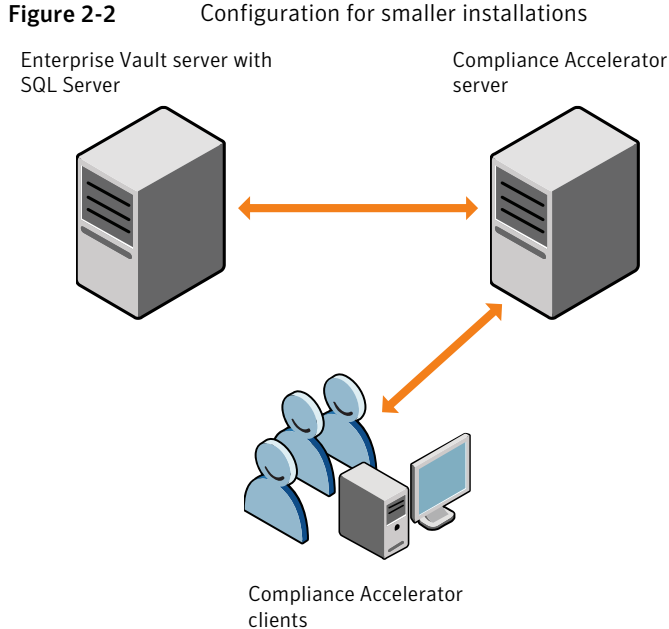
The Compliance Accelerator computer must be in the same domain as the Enterprise Vault server or in a trusted domain.

Figure 2-1 Configuration for large installations



Compliance Accelerator configuration for smaller installations

The only difference between the configuration for smaller installations and the configuration for large installations is that, in smaller installations, Enterprise Vault and SQL Server are on the same computer.



For test purposes, you can run Compliance Accelerator, SQL Server, and Enterprise Vault on the same computer.

Supported versions of Enterprise Vault in Compliance Accelerator environments

Note the following important points about the version of Enterprise Vault that you install in a Compliance Accelerator environment:

- All Enterprise Vault servers in all Enterprise Vault sites must run Enterprise Vault 11.0.1. Compliance Accelerator 11.0.1 does not work with earlier versions of Enterprise Vault.
- When upgrading both Compliance Accelerator and Enterprise Vault, you must first upgrade Enterprise Vault on the Enterprise Vault server, then Enterprise Vault on the Compliance Accelerator server, and finally Compliance Accelerator on the Compliance Accelerator server.

The order in which you perform these tasks differs from that in earlier versions of Compliance Accelerator, and is unique to Compliance Accelerator 11.0.1. Upgrades beyond 11.0.1 will resume the normal ordering of tasks.

See the [Compatibility Charts](#) for more information on supported versions of Enterprise Vault.

Prerequisites for Compliance Accelerator

The computers on which you install SQL Server, the Compliance Accelerator server software, and the Compliance Accelerator client software each have different requirements. The following sections describe these requirements.

For the latest information on supported devices and versions of software, see the Enterprise Vault *Compatibility Charts* (<http://www.symantec.com/docs/TECH38537>).

Prerequisites for the SQL Server computer

The SQL Server computer must be running one of the following versions:

- SQL Server 2008 R2 x64 Edition, original release or later
- SQL Server 2012 x64 Edition, original release or later

Prerequisites for the Compliance Accelerator server computer

[Table 2-1](#) lists the software items that you must install and configure on the computer that is to run the Compliance Accelerator server software.

Table 2-1 Required software for Compliance Accelerator server installation

Item	Notes
Windows	<p>You require one of the following:</p> <ul style="list-style-type: none"> ■ Windows Server 2008 R2 x64 Edition, original release or SP1. ■ Windows Server 2012, Standard Edition or DataCenter Edition. <p>We recommend that you disable the Windows Search Service to stop it from interfering with the progress of Compliance Accelerator export runs.</p> <p>See “Disabling the Windows Search Service on the Compliance Accelerator server” on page 23.</p>
Internet Information Services (IIS)	<p>You require IIS 7.5 or later with ASP.NET, IIS 6.0 Management Compatibility, and Windows Authentication.</p>

Table 2-1 Required software for Compliance Accelerator server installation
(continued)

Item	Notes
Internet Explorer	<p>You require Internet Explorer 7.0 through 11.0 to run the Accelerator Manager website. (Versions 10.0 and 11.0 are supported in Compatibility View only.)</p> <p>For optimum results, do the following:</p> <ul style="list-style-type: none"> ■ Configure the privacy settings in Internet Explorer to allow cookies. ■ Turn off any pop-up blockers. ■ Ensure that the advanced option Play animations in webpages is selected. <p>In Internet Explorer, click Internet Options on the Tools menu. Then, on the Advanced tab, locate the required option in the Multimedia category.</p>
Outlook	<p>You require Outlook 2007 SP2 or SP3 so that client users can export Exchange Server items in PST format and download the original versions of the items.</p> <p>Add the AttachmentMax and RecipientMax values to the registry on the Compliance Accelerator server to avoid problems when processing items that have many attachments or many recipients.</p> <p>See “Configuring Outlook to enable the processing of items with many attachments or many recipients” on page 19.</p>

Table 2-1 Required software for Compliance Accelerator server installation
(continued)

Item	Notes
Enterprise Vault	<p>If Compliance Accelerator is installed on a separate computer from Enterprise Vault, you must install the Enterprise Vault software on the Compliance Accelerator computer.</p> <p>As a minimum, you require an 11.0.1 version of one of the following:</p> <ul style="list-style-type: none"> ■ Enterprise Vault Services ■ Enterprise Vault API Runtime <p>See “Supported versions of Enterprise Vault in Compliance Accelerator environments” on page 14.</p> <p>There is no need to configure Enterprise Vault after you have installed it on your Compliance Accelerator server computer; do not run the Enterprise Vault configuration wizard. In addition, if the Enterprise Vault Admin service is running on your Compliance Accelerator server computer, we recommend that you stop it and set its startup type to Disabled.</p> <p>To search on content with Compliance Accelerator, set indexing on the Enterprise Vault archives to full.</p>
Windows Installer	<p>You require Windows Installer 3.1 or later. The installation package for version 3.1 is in the Links To Related Software folder on the distribution media.</p>
.NET Framework	<p>You require .NET Framework 3.5 SP1.</p> <p>This is available as a separate download (see the Links To Related Software folder in the distribution media).</p> <p>We recommend that you do not configure the Compliance Accelerator server to download and install .NET Framework updates automatically from the Windows Update site. Contact Symantec Support before installing such updates.</p>
Notes client	<p>You require version 8.5.2 or later of the Notes client so that client users can export Domino items.</p> <p>Install the client in single-user mode, using the account under which the Accelerator Manager service runs.</p>
Visual C++ 2008 SP1 Redistributable Package (x86)	<p>Enterprise Vault installs a suitable version of this package. The installation files for the package are also in the Links To Related Software folder on the distribution media.</p>

For the best results, we recommend that you install the Compliance Accelerator server software on a computer that has the following:

- 64-bit architecture.
- At least 4 GB of memory.
- Sufficient hard drive space to accommodate the searches and export runs that you expect to undertake.

All transaction requests from Compliance Accelerator clients to the Enterprise Vault and Compliance Accelerator servers use the Temp folder of the Vault Service account for temporary storage. Therefore, you must ensure that this folder has sufficient free space to handle large Compliance Accelerator searches and export runs. On both the Compliance Accelerator and Enterprise Vault servers, the Vault Service account's Temp folder must be on a drive that has a minimum of 40 GB of free space. However, 80 GB of free space is preferable. Exclude the Vault Service account's Temp folders from antivirus scanning.

- Multiple hard drives. For example, you might use drive C for the operating system, drive D for the CD or DVD drive, drive E for the Temp folder of the Vault Service account, and drive F for the export output folder. You might split the Windows paging file across drives E and F.

Prerequisites for Compliance Accelerator client computers

Table 2-2 lists the software items that you must install and configure on the computers that are to run the Compliance Accelerator client software.

Table 2-2 Required software for Compliance Accelerator client installation

Items	Notes
Windows	<p>You require one of the following:</p> <ul style="list-style-type: none"> ■ Windows 7 original release or SP1. ■ Windows 8 or 8.1. For best results, run the client in Windows 7 compatibility mode.
.NET Framework	<p>You require .NET Framework 3.5 SP1.</p> <p>This is available as a separate download (see the Links To Related Software folder in the distribution media).</p>

Table 2-2 Required software for Compliance Accelerator client installation
(continued)

Items	Notes
Outlook	You require one of the following to view Exchange Server items in their original form rather than in an HTML representation of the items: <ul style="list-style-type: none"> ■ Outlook 2007. ■ Outlook 2010. ■ Outlook 2013.
Notes client	You require version 8.5.2 or later of the Notes client to view Domino items in their original form rather than in an HTML representation of the items. Install the client in single-user mode.
Visual C++ 2008 SP1 Redistributable Package (x86)	You require this package if you want to view Domino items in their original form rather than in an HTML representation of the items. The installation files for the package are in the Links To Related Software folder on the distribution media.

The recommended screen resolution for the Compliance Accelerator client is 1024x768 or higher. For the best results, ensure that your client computers have at least 2 GB of memory.

Configuring Outlook to enable the processing of items with many attachments or many recipients

You must install a supported version of Outlook on the Compliance Accelerator server so that client users can export Exchange Server items in PST format and download the original versions of the items.

See [“Prerequisites for the Compliance Accelerator server computer”](#) on page 15.

By default, Outlook does not allow any items that have more than 2048 attachments or 2048 recipients to be opened. To avoid problems when client users try to export or download any items that have a larger number of attachments or recipients, set the registry values AttachmentMax and RecipientMax on the Compliance Accelerator server.

To configure Outlook to enable the processing of items with many attachments or many recipients

- 1 On the Compliance Accelerator server, start the Registry Editor.
- 2 Do one of the following:

- If you do not use policies, locate and then click the following registry subkey:
`HKEY_CURRENT_USER\Software\Microsoft\Office\version\Outlook\Options\Mail`
- If you use policies, locate and then click the following registry subkey:
`HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\version\Outlook\Options\Mail`

where *version* is 12.0 for Outlook 2007 or 14.0 for Outlook 2010.

- 3 On the **Edit** menu, point to **New**, and then click **DWORD Value**.
- 4 Type **AttachmentMax**, and then press Enter.
- 5 Right-click **AttachmentMax**, and then click **Modify**.
- 6 In the **Value data** box, type the required value, and then click **OK**.
 The recommended value is `ffffff` in hexadecimal.
- 7 Repeat steps 3 through 6 to add the RecipientMax registry entry.
- 8 Exit the Registry Editor.

Setting the Windows and ASP.NET Temp folder permissions

To enable users to access any of the Compliance Accelerator websites, such as the Accelerator Manager site, you must ensure that the Authenticated Users group has Full Control permissions in the following folders:

- The Windows Temp folder on the Compliance Accelerator server. This folder is typically `%windir%\Temp`.
- The ASP.NET Temp folder on the IIS computer. This folder is typically:
`%windir%\Microsoft.NET\Framework\version\Temporary ASP.NET Files`
 64-bit versions of Windows also have the following ASP.NET Temp folder:
`%windir%\Microsoft.NET\Framework64\version\Temporary ASP.NET Files`

To set the Temp folder permissions

- 1 In Windows Explorer, right-click the folder whose permissions you want to change, and then click **Properties**.
- 2 Click the **Security** tab.
- 3 Add **Authenticated Users** and give them **Full Control**.
- 4 Click **Advanced**.
- 5 In the **Advanced Security Settings** dialog box, do one of the following:

- If you run Windows Server 2008 R2, check **Include inheritable permissions from this object's parent**.
- If you run Windows Server 2012, click **Enable inheritance**.

Security requirements for temporary folders

Note: The following article on the Symantec Support website provides comprehensive information on the security requirements:

<http://www.symantec.com/docs/TECH224726>

On both Compliance Accelerator server and client computers, Compliance Accelerator makes occasional use of various folders for temporary storage. To protect against unauthorized access to these folders, which can contain sensitive data, Compliance Accelerator checks access to them on startup and periodically thereafter. If the security check fails on the Compliance Accelerator server, the Enterprise Vault Accelerator Manager service stops and an error event is recorded in the Symantec Enterprise Vault event log. If the security check fails on a Compliance Accelerator client computer, the user must choose to rerun the check or close the client.

On server computers, Compliance Accelerator checks the security of these folders:

- The temporary folder of the user who is running the Enterprise Vault Accelerator Manager service.
- The folder that you specify as the "ECM Temporary Storage Area" through the Reviewing configuration options in the Compliance Accelerator client. By default, this folder is the Windows %TEMP% folder.

On client computers, Compliance Accelerator checks the security of the temporary folder that belongs to the user who is running the client.

In both cases, Compliance Accelerator considers the following to be authorized users:

- Members of the Built-in groups Administrators, Backup Operators, and System Operators
- The user to whom the temporary folder belongs
- The Local System account

Granting additional users and groups access to the temporary folders

On both Compliance Accelerator server and client computers, you can set registry entries to exempt selected users or groups from the security checks or turn the checks off altogether.

To use registry entries to configure the security checks

- 1 On the Compliance Accelerator server or client computer where you want to set the registry entries, open the Registry Editor.
- 2 Do one of the following:
 - On a server computer, browse to the following subkey:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KVS
 - On a client computer, browse to the following subkey:
HKEY_CURRENT_USER\Software\KVS

If this subkey does not exist, you must create it. This is typically the case if you have performed a per-machine installation of the Compliance Accelerator client, rather than a per-user installation.
- 3 Set one of the following registry entries:

TempFolderExceptions String. Specifies the names of one or more users or groups to exempt from the security check. Enter the credentials in the form *domain\user_name*, or *BUILTIN\user_name* for built-in users, and separate them with semicolons. For example:

OurDomain\Marie.Lopez;BUILTIN\Server Operators

SkipTempFolderCheck DWORD. Specifies whether to perform the security check (0, the default) or turn it off (1).

- 4 If you set the registry entry on a server computer, restart the Enterprise Vault Accelerator Manager service. If you set it on a client computer, restart the client.

Disabling networking facilities that can disrupt a Compliance Accelerator environment

The Windows networking subsystem provides a number of facilities that can cause issues in a Compliance Accelerator environment. We recommend that you disable these facilities.

To disable networking facilities that can disrupt a Compliance Accelerator environment

- 1 Disable the following features on your designated Compliance Accelerator server, Enterprise Vault servers, and all SQL Servers that host an Enterprise Vault database:
 - Receive-Side Scaling
 - TCP Chimney
 - TCP Segmentation Offloading
 - TCP/IP Offload Engine

The following article on the Symantec Support website provides instructions on how to disable these features:

<http://www.symantec.com/docs/TECH63230>

- 2 Disable any network interface card (NIC) Teaming that may be present on the Enterprise Vault and Compliance Accelerator servers.

For guidelines on how to disable NIC Teaming, consult the documentation that your hardware vendor provides.

Disabling the Windows Search Service on the Compliance Accelerator server

If the Windows Search Service is running on the Compliance Accelerator server, it can sometimes prevent Compliance Accelerator from exporting items for offline review. We therefore recommend that you disable the service, as described in the following article on the Symantec Support website:

<http://www.symantec.com/docs/TECH203434>

You can disable the service altogether or you can partially disable it by excluding selected folders from indexing, such as the Windows Temp and Compliance Accelerator export folders.

Configuring the SQL Server Agent service

Compliance Accelerator provides the facility to create schedules with which you can conduct recurrent or future searches for items. As these schedules are SQL Server Agent jobs, you must ensure that the SQL Server Agent service is running on your SQL Server computer.

We recommend that you configure the SQL Server Agent service to start automatically when the SQL Server computer starts.

To configure the SQL Server Agent service to start automatically

- 1 On your SQL Server computer, double-click the **Administrative Tools** applet in Control Panel.
- 2 Double-click **Services**.
- 3 Right-click **SQL Server Agent**, and then click **Properties**.
- 4 Change the startup type to **Automatic**, and then click **OK**.

Assigning SQL Server roles to the Vault Service account

The Vault Service account is the account that Enterprise Vault services and tasks use when accessing Enterprise Vault databases. You must assign a number of SQL Server roles to this account to perform various activities with Compliance Accelerator. The two required roles are as follows:

- **dbcreator** (database creator). The facility to create configuration and customer databases with Compliance Accelerator is dependent on the Vault Service account having this role.
- **sysadmin** (system administrator). Compliance Accelerator provides the facility to create schedules with which you can conduct searches repeatedly or at some future time. These schedules are SQL Server Agent jobs and, by default, Compliance Accelerator assumes that you want to make a user with the sysadmin role the creator and owner of them.

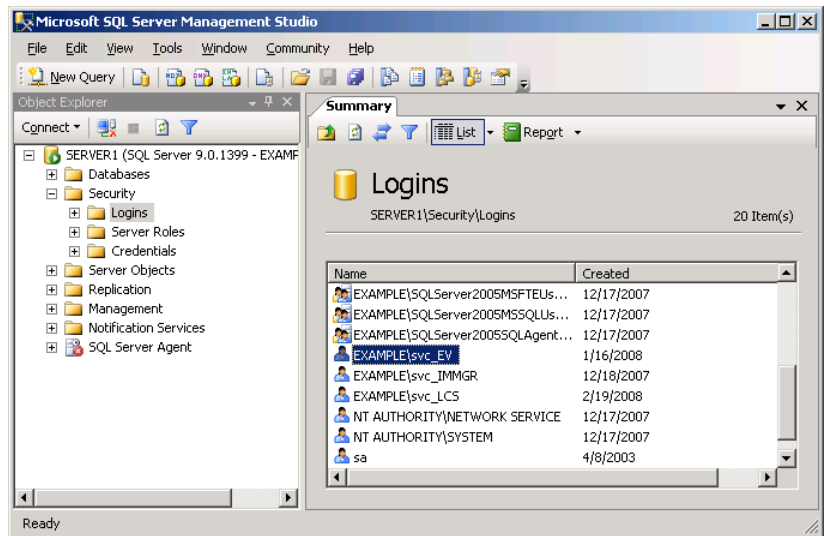
Note: The dbcreator and sysadmin roles are server-wide roles that may grant more security privileges to the Vault Service account than you are comfortable with. If this is the case, you can give the Vault Service account the minimum required permissions by following the instructions in this article on the Symantec Support website:

<http://www.symantec.com/docs/HOWTO80670>

Then, after you have installed the Compliance Accelerator client, you must change the value of the security configuration option "Use SQL Server SysAdmin Server Role for Schedules". For instructions on how to do this, see the *Administrator's Guide*.

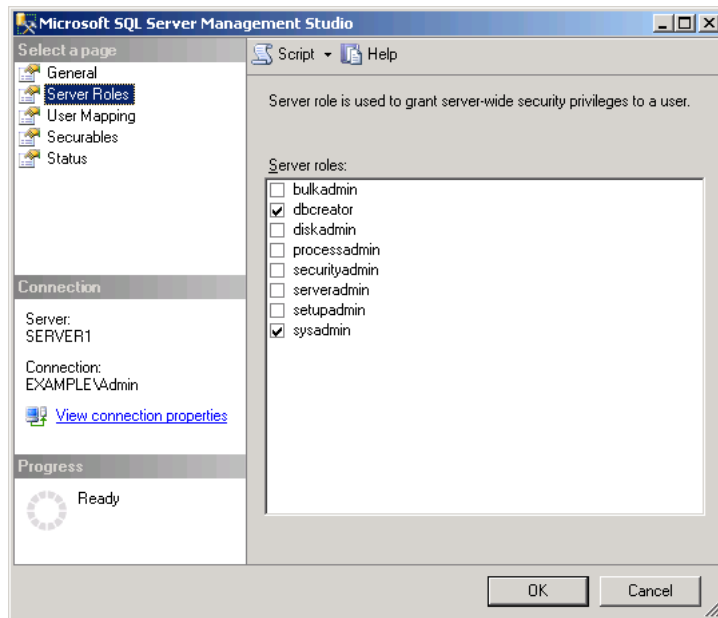
To assign SQL Server roles to the Vault Service account

- 1 On the SQL Server computer, start SQL Server Management Studio.
- 2 In the left pane of the SQL Server Management Studio window, expand the tree to display first the required SQL Server and then the **Security** folder.
- 3 Under the **Security** folder, double-click **Logins** to display the users in the right pane.



- 4 In the **Logins** list, right-click the Vault Service account, and then click **Properties**.
- 5 In the **Login Properties** dialog box, select the **Server Roles** page.

- 6 In the **Server roles** box, make sure that **dbcreator** and **sysadmin** are checked.



- 7 Click **OK**.

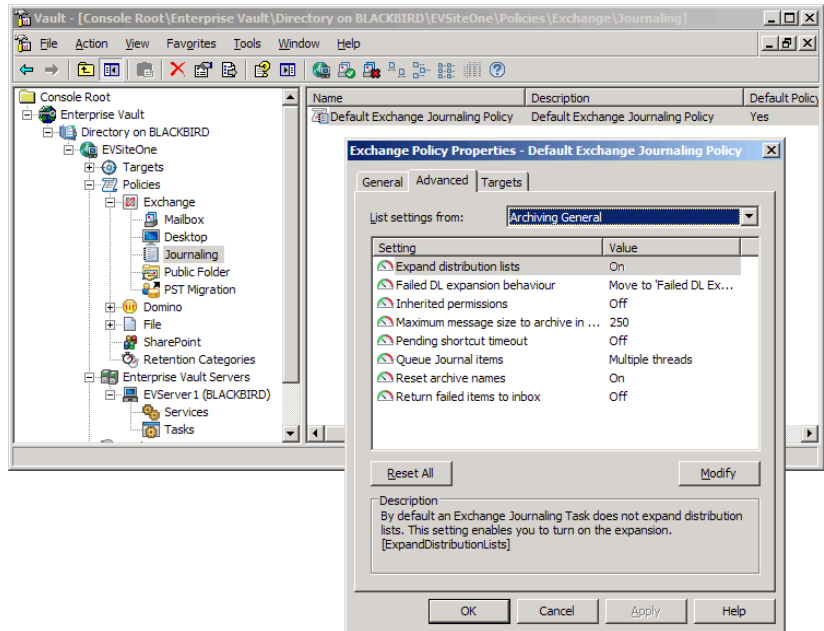
Verifying that Enterprise Vault expands distribution lists

In Microsoft Exchange environments, you must ensure that the Enterprise Vault Exchange Journaling Task expands distribution lists in the To, CC, and BCC fields of items.

To verify that Enterprise Vault expands distribution lists

- 1 Open the Enterprise Vault Administration Console.
- 2 Expand the contents of the left pane until the journaling policies are visible.

- 3 Right-click the required policy, and then click **Properties**. For example:



- 4 Click the **Advanced** tab, and then check the value for the **Expand distribution lists** setting.
- 5 If you need to change the value for the setting, do the following:
 - Click **Modify**.
 - Change the value to **On**.
 - Click **OK** in each dialog box to save the change that you have made.
 - Restart the Journaling task to put the change into effect.

Installing Compliance Accelerator

This chapter includes the following topics:

- [Installing the Compliance Accelerator server software](#)
- [Installing the Compliance Accelerator client software](#)
- [Uninstalling Compliance Accelerator](#)

Installing the Compliance Accelerator server software

Follow the instructions in this section to perform a first-time installation of the Compliance Accelerator server software. If you want to upgrade an existing Compliance Accelerator installation, see the `CAUpgradeInstructions` file.

Before you proceed, note the following:

- Installing this software on a computer on which you have also installed the Discovery Accelerator server software is not supported.
- You can configure Compliance Accelerator for use in a Network Load Balancing cluster. However, installing the software on the nodes in other types of clusters is not supported.
See [“Installing Compliance Accelerator in a clustered environment”](#) on page 39.

To install the Compliance Accelerator server software

- 1 Load the release media, and then do one of the following:
 - When the Install Launcher starts, follow the links to install the Compliance Accelerator server software.
 - In Windows Explorer, browse to the `Symantec Enterprise Vault Compliance Accelerator\Server` folder, and then run `setup.exe`.

The `setup.exe` program launches the Windows Installer (.msi) package that is in the same folder with elevated privileges. This is necessary to enable the installation to complete all of its processes.

- 2 Follow the on-screen instructions, which prompt you to submit information at several points.

- Choose between the following setup types:

Typical	Installs all the components. This option is recommended for most users.
---------	-------------------------------------------------------------------------

Custom	Lets you select the components to install. For example, you can choose to install the Enterprise Vault Accelerator Manager service only.
--------	------------------------------------------------------------------------------------------------------------------------------------------

Note: We recommend that you install the Compliance Accelerator website, as it provides functionality for some of the Compliance Accelerator reports.

- If you are prompted for details of the account under which to run the Enterprise Vault Accelerator Manager service, enter the details of the Vault Service account with which you manage your Enterprise Vault server.

- 3 If you have chosen to install the Accelerator Manager service then, when the installation program has finished, check the option to display the Enterprise Vault Accelerator Manager website. Then you can create the configuration database and customer databases.

The installation program automatically opens the Accelerator Manager website with administrator privileges if you have installed Compliance Accelerator on a server in which User Account Control (UAC) is enabled. (This is a requirement when accessing the website in such environments.) If UAC is not enabled, a Run As dialog box may prompt you for the name and password of the user account under which to access the website. Enter the details of the Vault Service account with which you manage your Enterprise Vault server.

See [“Creating the configuration database and customer databases”](#) on page 30.

Allowing Enterprise Vault to communicate with Compliance Accelerator through the Windows firewall

You must configure the Windows firewall on the Compliance Accelerator server to permit Enterprise Vault to communicate with Compliance Accelerator through it. Certain interactions between the Enterprise Vault server and the Compliance Accelerator server require unrestricted communication. You can allow Enterprise

Vault to communicate with Compliance Accelerator through the Windows firewall by adding the Accelerator service process to the exceptions list for the firewall.

You must be logged on to the computer as an administrator to complete this procedure.

To allow Enterprise Vault to communicate with Compliance Accelerator through the Windows firewall

- 1 In Control Panel, click **System and Security**, and then click **Windows Firewall**.
- 2 Click **Allow a program or feature through Windows Firewall**.
- 3 Click **Change settings**, and then click **Allow another program**.
- 4 Click **Browse**, and then browse to the Compliance Accelerator program folder (typically, `C:\Program Files (x86)\Enterprise Vault Business Accelerator`).
- 5 Click `AcceleratorService.exe`, and then click **Open**.
- 6 Click **Add**, and then click **OK**.

Creating the configuration database and customer databases

After you have installed the Compliance Accelerator server software, you must set up the required configuration and customer databases with the Accelerator Manager website.

The configuration database specifies the locations of the customer databases, and it stores details of the SQL Server, database files, and log files to use. Each customer database stores details of departments, user roles, search results, and more.

You can set up one configuration database only, but you can set up multiple customer databases. The configuration database can reside on one SQL Server, and the customer databases can reside on a different SQL Server. You may find it useful to set up multiple customer databases if, for example, you want to separate the groups who are to perform searches in Compliance Accelerator. Suppose that your legal department and human resources department both need to perform searches. These two departments may not be able to share roles in a Compliance Accelerator system. Setting up two customers lets both departments use Compliance Accelerator without needing access to the same Compliance Accelerator setup.

Before you proceed, note the following:

- If you have installed Compliance Accelerator on a server in which User Account Control (UAC) is enabled, you must open the Accelerator Manager website with administrator privileges.
- If Symantec Endpoint Protection is running on your Compliance Accelerator server, we recommend that you shut it down temporarily.

See [“Cannot create or upgrade Compliance Accelerator customer databases when Symantec Endpoint Protection is running”](#) on page 49.

To create the configuration database

- 1 If you have yet to display the Accelerator Manager website, start Internet Explorer and browse to the following location:

`http://server_name/EVBAAdmin`

where *server_name* is the name of the server on which you installed the Compliance Accelerator server software.

- 2 In the **Configuration Database Details** page, enter your preferred details, and then click **OK**.

SQL Server	Specifies the name or IP address of the SQL Server computer. You can specify the IP address in either IPv4 or IPv6 format. SQL instances are supported.
------------	---------------------------------------------------------------------------------------------------------------------------------------------------------

Database name	Specifies the name of the configuration database. The name cannot contain any of the following characters:
---------------	------------------------------------------------------------------------------------------------------------

`\ / : * ? " < > | '`

Note: Compliance Accelerator and Discovery Accelerator cannot share the same configuration database. So, if you previously created the configuration database for one application, you must create a new database with a different name when setting up the other application.

Use Existing Database	Instructs Compliance Accelerator to use the specified existing database instead of creating a new one. If you choose this option, the remaining boxes in the page are unavailable.
-----------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Data File Folder	Specifies a location for the configuration database file. This location should be a valid, existing path on the SQL Server computer, and it must be a local path (not a network share path). For example, you might specify the path as <code>E:\SQLData</code> . A minimum of 300 MB is required for the default configuration database.
------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Log File Folder	Specifies a location for the database log files. This location should be a valid, existing path on the SQL Server computer, and it must be a local path (not a network share path). For example, you might specify the path as <code>F:\SQLLogs</code> . A minimum of 300 MB is required for the database log files.
-----------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Initial Database Size	Sets the initial size in megabytes of the configuration database file. In the Growth % box, you can specify as a percentage of the file size the amount of space that is automatically added to the file each time more is needed.
Initial Log Size	Sets the initial size in megabytes of the database log files. In the Growth % box, you can specify as a percentage of the file size the amount of space that is automatically added to a file each time more is needed.

- 3 When Compliance Accelerator prompts you to do so, restart the Enterprise Vault Accelerator Manager service by using the Services snap-in to Microsoft Management Console.

Note: Restarting the service causes Compliance Accelerator to check the security of various temporary folders that the application uses. If this security check fails, an error event with an ID of 585 is recorded in the Symantec Enterprise Vault event log, and the service does not start.

See [“Security requirements for temporary folders”](#) on page 21.

- 4 In the Accelerator Manager website, click **Upload License** to import your license key file into Compliance Accelerator.

To create the customer databases

- 1 In the left pane of the Accelerator Manager website, right-click the server node, and then click **New Customer**.
- 2 Complete the details in the **Create Customer** page, and then click **OK**.

Customer Type	Indicates that this database is a customer database for Compliance Accelerator.
Name	Specifies a unique name for the customer. The name cannot contain any of the following characters: <code> \ / : * ? " < > ' </code>

VaultID(s)	<p>Identifies the journal mailbox archive that the customer uses. You can obtain the ID by looking at the archive's property page in the Vault Administration Console.</p> <p>One customer must have a blank VaultID(s) field to designate that it is the default customer. All other customers must have a unique entry in the field, such as the required ID or a statement such as "Do_Not_Use".</p>
Directory DNS aliases	<p>Specifies the DNS alias, server name, or IP address of the Enterprise Vault Directory service computer. You can specify IP addresses in either IPv4 or IPv6 format.</p> <p>Take care to specify the correct DNS alias information. If the information is wrong, no vault stores will be visible in any area of the Compliance Accelerator client.</p>
Administrator User or Group	<p>Optionally nominates an Active Directory user account or group account as an administrator for the Compliance Accelerator customer database. This user or group has full administrative permissions in the customer database and typically assigns application-wide roles to other users. Specify the account details in the form <i>domain\user_or_group_name</i>; for example, "OurDomain\Marie.Lopez".</p> <p>Note that the Vault Service account already has full administrative permissions in the customer database, so there is usually no need to nominate another user or group. However, you may want to do this if your company policy restricts the use of service accounts.</p>
Enable Customer's tasks	<p>Enables users to perform activities in the Compliance Accelerator client. If you uncheck this option, only automatic tasks like scheduled searches are permissible.</p>

IIS section

- Virtual Directory** Specifies the name of the IIS virtual directory that the Compliance Accelerator reporting functionality uses.
- No two customers can share the same virtual directory name. The directory name must not include space characters or any of the following characters:
- * ? \ / % ' "**
- Note that you cannot name the virtual directory for any Compliance Accelerator customer as "EVBAAdmin" because this name is reserved for the Accelerator Manager website.
- IIS Server** Specifies the name or IP address of the IIS server that is to host the Compliance Accelerator site. You can type the IP address in either IPv4 or IPv6 format. However, you cannot type an IPv6 address that includes colons (:) or is enclosed in square brackets ([]).
- The default entry for this field is the server on which you are running the Accelerator Manager website.
- Manage Virtual Directory** Lets you administer the virtual directory by using the Compliance Accelerator client. By default, the option is checked.

Database Details section

- SQL Server** Specifies the name or IP address of the SQL Server on which the customer database is to reside. You can specify the IP address in either IPv4 or IPv6 format. SQL instances are supported. The default entry for this field is the server on which you are running the Accelerator Manager website.
- Database** Specifies the name of the customer database. The name cannot contain any of the following characters:
- \ / : * ? " < > | ' "**
- Use Existing Database** Instructs Compliance Accelerator to use the specified existing database instead of creating a new one. If you check this option, many of the remaining boxes in the page become unavailable. By default, the option is not checked.

Data File Folder	Specifies a location for the customer database file. This location should be a valid, existing path on the SQL Server computer, and it must be a local path (not a network share path). For example, you might specify the path as <code>E:\SQLData</code> .
Log File Folder	Specifies a location for the database log files. This location should be a valid, existing path on the SQL Server computer, and it must be a local path (not a network share path). For example, you might specify the path as <code>F:\SQLLogs</code> .
Initial Database Size	Sets the initial size in megabytes of the customer database file. In the Growth % box, you can specify as a percentage of the file size the amount of space that is automatically added to the file each time more is needed.
Initial Log Size	Sets the initial size in megabytes of the database log files. In the Growth % box, you can specify as a percentage of the file size the amount of space that is automatically added to a file each time more is needed.
Windows Authentication	Specifies whether to use a Microsoft Windows user account to connect to the customer database. If you uncheck this option, you must set the SQL logon name and password to use for the database connection.
Connection Time Out	Specifies the amount of time in seconds to wait for connections to the customer database to complete before terminating the attempt and generating an error.
Connection Life Time	Specifies the time in seconds that a connection to the customer database is considered valid. When the time has elapsed, the connection is disposed of.
Max Pool Size	Specifies the maximum number of database connections that can be simultaneously opened to the customer database.
DSN	Specifies the full connection string, or Data Source Name (DSN), to use when connecting to the customer database. The process of creating and connecting to the database automatically fills in this field. Do not modify the details unless Symantec Support advises you to do so.

- 3 Wait for Compliance Accelerator to create the customer database. This process can take several minutes to complete.
- 4 Repeat steps 1 through 3 for each customer database that you want to create.

Uploading the Compliance Accelerator report templates

Using Microsoft SQL Server Reporting Services as the reporting mechanism, Compliance Accelerator provides extensive facilities for reporting on the roles and responsibilities of your Compliance Accelerator users and on the progress that reviewers and supervisors have made. For information on the available reports and guidelines on how to use them, see the *Administrator's Guide*.

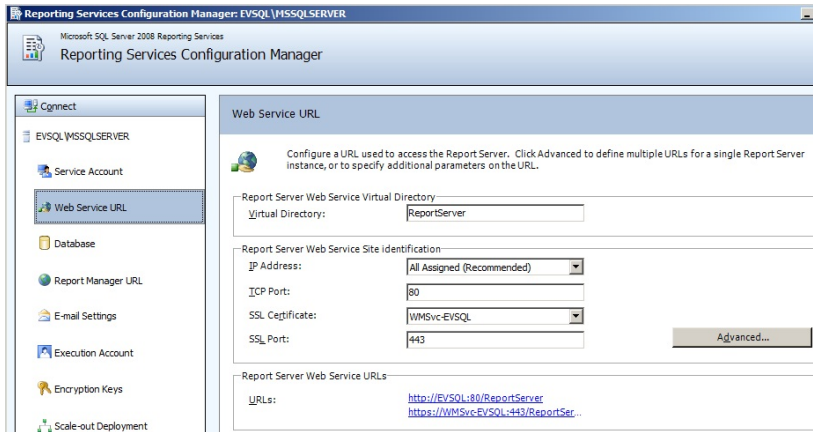
To make the reports available to users of the Compliance Accelerator client, you must upload the supplied template (.rdl) files to your SQL reporting server. The template files contain data retrieval and layout information for their respective reports in XML format.

To upload the Compliance Accelerator report templates

- 1 If you have not already done so, install and configure SQL Server Reporting Services on the selected reporting server.

You can check the configuration of SQL Server Reporting Services by using the Reporting Services Configuration Manager on the reporting server. Make a note of the virtual directory name on the Web Service URL page, as you need to specify this name later. The default name of the virtual directory is **ReportServer**.

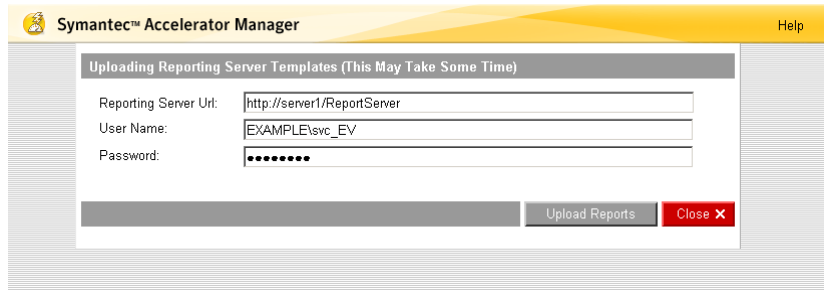
The following figure shows the typical settings in a Web Service URL page.



- 2 On the SQL reporting server, assign the following roles to the Vault Service account:
 - The System Administrator role on the SQL reporting server.
 You can assign this role by using the browser-based Report Manager tool that comes with SQL Server. First click **Site Settings** on the global toolbar in Report Manager and then click **Security**. Then click **New Role Assignment** and assign the System Administrator role to the Vault Service account.
 - The Content Manager role on the Home folder of the SQL reporting server.
 To assign this role in Report Manager, click **Security** on the **Properties** tab for the Home folder. Then click **New Role Assignment** and assign the Content Manager role to the Vault Service account.

See the Microsoft Reporting Services documentation for more information.

- 3 On the Compliance Accelerator server, open the Accelerator Manager website.
- 4 Click **Reporting Server** at the bottom of the page.
 The Uploading Reporting Server Templates page appears.



- 5 In the **Reporting Server URL** field, type the URL with which you access the SQL reporting server in the following form:

http://server_name/virtual_directory

where *server_name* is the host name, fully qualified domain name, or IPv4 or IPv6 address of the SQL reporting server, and *virtual_directory* is the name of the required virtual directory. For example:

http://EVSQL/ReportServer

Note the following:

- If you have multiple SQL Server instances, type the URL in the following form:
http://server_name/virtual_directory\$instance_name
 - If you have configured the SQL reporting server to listen for HTTP requests on a port other than the default, 80, type the URL in the following form:
http://server_name:port_number/virtual_directory
- 6 In the **User Name** field and **Password** field, type the credentials for the Vault Services account. By doing so, you identify the Vault Services account as the owner of all exchanges between the Compliance Accelerator server and SQL reporting server.

Caution: The Accelerator Manager website does not authenticate the logon credentials that you enter, so it is important to enter the correct ones. If you omit the credentials or enter the wrong ones, Compliance Accelerator client users receive the error message "An error occurred creating the report" when they try to generate reports.

- 7 Click **Upload Reports**.

Note that it can take several minutes to upload the report templates to the server. A confirmation message appears when the process has completed.

Installing Compliance Accelerator in a clustered environment

Symantec does not support installing the Compliance Accelerator server software on any node in a Windows Server failover cluster or Veritas Cluster Server (VCS) cluster. So, if you have configured Enterprise Vault for use in a cluster, you must not install the server software on one of the cluster nodes. However, an unclustered Compliance Accelerator installation can reference a clustered Enterprise Vault virtual server.

In addition, you can enhance the scalability, performance, and high availability of Compliance Accelerator by configuring it for use in a Network Load Balancing cluster.

Configuring Compliance Accelerator for use in a Network Load Balancing cluster

Network Load Balancing (NLB) is a clustering technology that Microsoft offers as part of Windows Server 2008 R2 and Windows Server 2012.

NLB balances the network traffic across all the nodes in a cluster, which work together to run a common set of applications and provide the image of a single system to client users. NLB helps to enhance the scalability and performance of Compliance Accelerator by distributing client requests across the nodes in the cluster; background Compliance Accelerator tasks are unaffected. It also provides high availability by detecting node failures and automatically redistributing traffic to operational nodes.

The process of setting up an NLB cluster requires you to specify a virtual name or IP address for the cluster. When they start the Compliance Accelerator client, your users must specify this virtual name or address as the server to which they want to connect.

To configure Compliance Accelerator for use in an NLB cluster

- 1 Ensure that each node that you want to include in the NLB cluster has a fixed IP address.

If you do not have these fixed addresses, you can obtain them from your network administrator.

- 2 Use the Network Load Balancing Manager that comes with Windows to set up and manage the cluster.

Consult the documentation that accompanies Network Load Balancing Manager for guidelines on how to do this.

- 3 Install the Compliance Accelerator server software on each node in the cluster.

As a minimum, you must install the Enterprise Vault Accelerator Manager service on each node.

Maximizing security in your Compliance Accelerator databases

By default, the Vault Service account owns all the Compliance Accelerator databases and can access all the objects in them. To maximize security in your SQL Server environment, you may want to change the ownership of each database and revoke many of the Vault Service account's access privileges. The following article on the Symantec Support website describes how to perform these activities:

<http://www.symantec.com/docs/HOWTO80670>

Installing the Compliance Accelerator client software

Caution: The version of the client software that you install on your users' computers must exactly match that of the Compliance Accelerator server software on the Compliance Accelerator server.

Modifying the configuration file for the Compliance Accelerator client

Before you proceed, it is a good idea to modify the configuration file that accompanies the installation package. One of the settings in this file is the name or address of the computer on which you have installed the Compliance Accelerator server software. By providing this information in the configuration file, you can save your users from having to supply the computer name or address when they first start the Compliance Accelerator client.

To modify the configuration file for the Compliance Accelerator client

- 1 Locate the configuration file `AcceleratorClient.Exe.Config` in the installation media for the Compliance Accelerator client software.
- 2 Open the configuration file in a plain text editor such as Windows Notepad.
- 3 Find the following configuration setting:

```
<add key="AcceleratorServer" value="localhost" />
```


- 4 Replace the value with the name, fully qualified domain name, or IPv4 or IPv6 address of the computer on which you installed the Compliance Accelerator server software. For example:

```
<add key="AcceleratorServer" value="server2" />
```

If you have configured Compliance Accelerator for use in a Network Load Balancing cluster, you must specify the virtual name or IP address of the cluster.

- 5 Save and close the file.

Using the MSI installer package to install the Compliance Accelerator client

Typically, you distribute the Compliance Accelerator client software by directing users to a central location from which they can run the MSI installer package. By default, the installer package for the Compliance Accelerator client software performs a per-user installation of the software. This type of installation does not permit other users of the computer to run the application. However, if you have administration privileges on the computer and want to permit all users to run the application, you can perform a per-machine installation.

To install the Compliance Accelerator client software

- 1 Ensure that the configuration file `AcceleratorClient.Exe.Config` file is in the installation folder for the Compliance Accelerator client software.
- 2 Do one of the following:
 - To perform a per-user installation, start the Compliance Accelerator installer package (Symantec Enterprise Vault Compliance Accelerator Client.msi).
 - To perform a per-machine installation, open a Command Prompt window and then type the following:

```
msiexec /I "path_to/Symantec Enterprise Vault Compliance Accelerator Client.msi" INSTALLDIR="install_path" ALLUSERS=1
```

Where:

path_to Specifies the path to the .msi file.

install_path Specifies the path to the folder in which to create an Enterprise Vault Compliance Accelerator subfolder for the client software.

For example, if the .msi file is located at the root of the D: drive, and you want to install the client software in the folder `C:\Program Files`

(x86)\Enterprise Vault Compliance Accelerator, you must type the following:

```
msiexec /I "D:\Symantec Enterprise Vault Compliance Accelerator Client.msi" INSTALLDIR="C:\Program Files (x86)" ALLUSERS=1
```

Caution: If User Account Control (UAC) is enabled on your computer, you must open the Command Prompt window with administrator privileges.

- 3 Follow the on-screen instructions.

Uninstalling Compliance Accelerator

If you remove a Compliance Accelerator server from an Enterprise Vault environment, you must manually remove the entry for the server from the AcceleratorConfigEntry table of the Enterprise Vault directory database. Otherwise, the Enterprise Vault Storage service may experience problems when any item is next sent for archiving.

In outline, the procedure for uninstalling Compliance Accelerator is as described below.

To uninstall Compliance Accelerator

- 1 Ask all users of the Compliance Accelerator client to uninstall it through Control Panel.
- 2 On the Compliance Accelerator server, uninstall the Compliance Accelerator server software and the Enterprise Vault software.
- 3 Delete the AcceleratorConfigEntry table from the Enterprise Vault Directory database. You can use the following script to do this:

```
DELETE FROM  
[EnterpriseVaultDirectory].[dbo].[AcceleratorConfigEntry]
```

Ports that Compliance Accelerator uses

This appendix includes the following topics:

- [Default ports for Compliance Accelerator](#)
- [Changing the ports that Compliance Accelerator uses](#)

Default ports for Compliance Accelerator

[Table A-1](#) lists the default ports that Compliance Accelerator uses.

Table A-1 Default ports for Compliance Accelerator

Port	Used for
80 for HTTP, or 443 for HTTPS	Communications between the SQL reporting server and the Compliance Accelerator clients and server.
1433	Communications between the Compliance Accelerator server and the SQL Server computer.
8085	Communications between the Compliance Accelerator server and the Accelerator Manager website.
8086	Communications between the Compliance Accelerator server and the Compliance Accelerator clients.

Compliance Accelerator uses standard DCOM ports to communicate with the Enterprise Vault server for searching, reviewing, and exporting. For information on the ports that Enterprise Vault uses, see the Enterprise Vault *Administrator's Guide*.

Changing the ports that Compliance Accelerator uses

You can set Compliance Accelerator to use different ports if another application requires the default ones.

To change the port used for communications with the SQL reporting server

- 1 On the Compliance Accelerator server, open the Accelerator Manager website.
- 2 Click **Reporting Server** at the bottom of the page.

The Uploading Reporting Server Templates page appears.

- 3 In the **Reporting Server URL** field, type the URL with which to access the SQL reporting server in the following form:

http://server_name:port_number/virtual_directory

To change the port used for communications with the SQL Server computer

- 1 If the Enterprise Vault Accelerator Manager service is running on the Compliance Accelerator server, stop it.
- 2 See the following article on the Symantec Support site for instructions on how to amend the configuration files on the Compliance Accelerator server:

<http://www.symantec.com/docs/TECH51129>

The name of the SQL Server computer appears in multiple configuration files. In each case, you must append the required port number to the SQL Server name, as in *server_name:port_number*.

- 3 Restart the Enterprise Vault Accelerator Manager service.
- 4 On the Compliance Accelerator server, open the Accelerator Manager website.
- 5 In the left pane, right-click the name of the SQL Server computer and then click **Properties**.
- 6 In the **Name** field, specify the required SQL Server computer as *server_name:port_number*.
- 7 Click **OK** to save the change that you have made.
- 8 For each customer database, do the following:
 - In the left pane, right-click the name of the database and then click **Properties**.
 - In the **SQL Server** field, specify the required SQL Server computer as *server_name:port_number*.
 - Click **OK** to save the change that you have made.

To change the port used for communications between the Compliance Accelerator server and the Compliance Accelerator websites

- 1 On the Compliance Accelerator server, locate the copies of the `Web.config` file in the `AcceleratorAdminWeb` and `ComplianceWebMin` subfolders of the Compliance Accelerator installation folder. (The `ComplianceWebMin` subfolder is only present if you have chosen to install the Compliance Accelerator website.)
- 2 Open each file in a text editor such as Windows Notepad.
- 3 Find the following line, and change the port number to a suitable alternative.

```
<add key="RemotePort" value="8085"/>
```

- 4 Save and close the files.
- 5 Restart the Enterprise Vault Accelerator Manager service.

To change the port used for communications between the Compliance Accelerator server and the Compliance Accelerator clients

- 1 On each Compliance Accelerator client computer, locate the `AcceleratorClient.Exe.Config` file in the installation folder.

This folder is typically `%HOMEPATH%\Local Settings\Application Data\Enterprise Vault Compliance Accelerator\Client`.
- 2 Open the file in a text editor such as Windows Notepad.
- 3 Find the following line, and change the port number to a suitable alternative.

```
<add key="AcceleratorServerPort" value="8086" />
```

- 4 Save and close the file.

Troubleshooting

This appendix includes the following topics:

- [Enterprise Vault Accelerator Manager service not created](#)
- [Enterprise Vault Accelerator Manager service does not start](#)
- [Home page of Compliance Accelerator website not found](#)
- [Cannot create or upgrade Compliance Accelerator customer databases when Symantec Endpoint Protection is running](#)
- [Permissions error when uninstalling the Compliance Accelerator client from a UAC-enabled computer](#)
- [Uninstalling the Compliance Accelerator client from a shared location may prevent other users from starting the client](#)

Enterprise Vault Accelerator Manager service not created

If the installation program is unable to create the Enterprise Vault Accelerator Manager service on the Compliance Accelerator server, you may need to create it manually.

To create the Enterprise Vault Accelerator Manager service manually

- 1 In Windows Explorer, search the folders under your .NET Framework installation for the file `InstallUtil.exe`.
- 2 Open a Command Prompt window.
- 3 Change to the folder that contains `InstallUtil.exe`.

- 4 Run the following command:

```
InstallUtil "InstallFolder\AcceleratorManager.exe"
```

where *InstallFolder* is the path to the folder in which you installed the Compliance Accelerator server software.

- 5 If the command fails, and you have more than one copy of `InstallUtil.exe`, try the same command with each of the other copies.
- 6 If service creation still fails, reinstall the .NET Framework and then type the command again using the newly installed copy of `InstallUtil.exe`.

Enterprise Vault Accelerator Manager service does not start

If you cannot start the Enterprise Vault Accelerator Manager service, check the status of the Windows Management Instrumentation (WMI) service. If the WMI service has stopped, start it and then start the Enterprise Vault Accelerator Manager service.

Home page of Compliance Accelerator website not found

If you receive the message "Page Cannot Be Displayed" when you browse to the home page of the Accelerator Manager website, start IIS Manager and then check the following:

- The virtual directories have been created.
- The websites are running.
- The virtual directories are configured to use ASP.NET 2.0 rather than an earlier version.

If the installation program failed to create a virtual directory as part of the installation process, you can create it manually.

To create the virtual directory manually

- 1 Open IIS Manager on the server that is hosting the website.
- 2 Right-click the container for your default website and then click **New > Virtual Directory**.
- 3 When the Virtual Directory Creation Wizard appears, click **Next**.

- 4 For the virtual directory alias, type one of the following, and then click **Next**.

EVBAAdmin	Used by the Accelerator Manager website.
EVBACompliance	Used by the Compliance Accelerator reporting functionality.

- 5 For the website home directory, enter the path to the appropriate subfolder of the Compliance Accelerator program folder (`AcceleratorAdminWeb` or `ComplianceWebMin`), and then click **Next**.
- 6 When you are prompted to set the access permissions for the virtual directory, click **Next** without changing the default permissions.
- 7 Click **Finish** to close the wizard and create the virtual directory.

To configure the settings for the virtual directory

- 1 Open IIS Manager on the server that is hosting the website.
- 2 Right-click the `EVBAAdmin` or `EVBACompliance` virtual directory, and then click **Properties**.
- 3 On the **Virtual Directory** tab, do the following:
 - Make sure that **Read**, **Log visits**, and **Index this resource** are all checked.
 - Remove the entry in the **Application name** box.
 - Make sure that the application pool is set to **EVAcceleratorAppPool**.
- 4 On the **Documents** tab, remove all the entries in the **Enable default content page** box, and then add **Login.aspx**.
- 5 On the **Directory Security** tab, click **Edit** under **Authentication and access control**.
- 6 In the Authentication Methods dialog box, uncheck **Enable anonymous access** and check **Integrated Windows authentication**. (You can select **Basic authentication**, but it is less secure.)
- 7 Click **OK** to save the changes you have made to the Authentication Methods dialog box.
- 8 Click **OK** to close the properties dialog box.
- 9 Check that the website is running.

Cannot create or upgrade Compliance Accelerator customer databases when Symantec Endpoint Protection is running

If Symantec Endpoint Protection is running on your Compliance Accelerator server, you may be unable to create customer databases or upgrade existing ones. We recommend that you shut down Endpoint Protection while you perform these operations.

When the Compliance Accelerator server is running in a centrally managed Endpoint Protection environment, you need only disable the Intrusion Prevention check that is responsible for the issue. Although this disables the Intrusion Prevention check on all servers that are in the same group as the Compliance Accelerator server, it saves you from having to shut down Endpoint Protection completely.

To disable Endpoint Protection's Intrusion Prevention check

- 1 Log on to the computer where the Endpoint Protection Manager Console is running.
- 2 Open the Endpoint Protection Manager Console.
- 3 Click **Policies**.
- 4 Under **View Policies**, click **Intrusion Prevention**.
- 5 In the right pane, right-click your Intrusion Prevention policy, and then click **Edit**.
- 6 Click **Exceptions**.
- 7 Click **Add**.
- 8 Select the signature **ID 20079** in the list, and then click **Next**.
- 9 Set **Action** to **Allow** and **Log** to either option, and then click **OK**.
- 10 Click **OK**.
- 11 Wait a few moments for Endpoint Protection to roll out the policy to the servers in the group.

Permissions error when uninstalling the Compliance Accelerator client from a UAC-enabled computer

When both the following conditions apply, the message "You must be an Administrator to remove this application" appears when you try to uninstall the

Uninstalling the Compliance Accelerator client from a shared location may prevent other users from starting the client

Compliance Accelerator client from a computer in which User Account Control (UAC) is enabled:

- You performed a per-machine installation of the client by using the MSI installer package, `Symantec Enterprise Vault Compliance Accelerator Client.msi`. The issue does not arise when you choose to uninstall a per-user MSI installation.
- You tried to uninstall the client by right-clicking the MSI installer package and then clicking **Uninstall** on the context menu. The issue does not arise when you uninstall the client through the Add or Remove Programs applet in Control Panel.

To uninstall the Compliance Accelerator client in these circumstances

- 1 Open a Command Prompt window with administrator privileges.
- 2 Type the following command:

```
msiexec /x "path_to/Symantec Enterprise Vault Compliance  
Accelerator Client.msi" /qb!
```

Where the `/x` parameter specifies that you want to uninstall the client, and the `/qb!` parameter displays a basic user interface during the uninstallation process.

Uninstalling the Compliance Accelerator client from a shared location may prevent other users from starting the client

If a user uninstalls the Compliance Accelerator client from the same shared location to which other users have installed the client, these users may no longer be able to start the client. However, they can easily fix the problem by performing a repair installation of their Compliance Accelerator clients.

To perform a repair installation of the Compliance Accelerator client

- 1 On each computer where you want to perform the repair installation, start Control Panel.
- 2 Double-click the **Add or Remove Programs** applet.
- 3 Find and click **Symantec Enterprise Vault Compliance Accelerator Client** in the list of installed programs.
- 4 Click the **Click here for support information** hyperlink.
- 5 Click **Repair**, and then follow the on-screen instructions.

Index

A

- Accelerator Manager service
 - changing port used by 44
 - creating manually 46
 - installing 29
 - introduction to 9
 - troubleshooting 47
- Accelerator Manager website
 - changing port used by 44
 - introduction to 9
 - opening with administrator privileges 30
 - supported versions of Internet Explorer 16
- AcceleratorClient.Exe.Config file 40–41
- ASP.NET
 - supported versions of 15
 - Temp folder permissions 20
- AttachmentMax registry value 19
- Authenticated Users group 20

C

- C++ 2008 SP1 Redistributable Package 17, 19
- client software
 - installing 40
 - modifying the configuration file for 40
 - prerequisites for 18
 - uninstalling 50
- Clustered environments 39
- Compliance Accelerator website
 - installing 29
 - introduction to 9
- configuration database
 - and required SQL Server roles 24
 - creating 30
 - introduction to 9
- configuration options 13
- creating
 - Accelerator Manager service manually 46–47
 - configuration database 30
 - customer databases 32
 - IIS virtual directory 47

- customer databases
 - and required SQL Server roles 24
 - creating 30, 32
 - introduction to 9

D

- databases
 - and required SQL Server roles 24
 - creating 30
- dbcreator role in SQL Server 24
- documentation 9
- Domino items
 - exporting 17
 - viewing 19

E

- Endpoint Protection, temporarily shutting down 30, 49
- Enterprise Vault
 - Exchange Journaling Task 26
 - expanding distribution lists 26
 - supported versions of 14, 17
- Enterprise Vault Accelerator Manager service
 - changing port used by 44
 - creating manually 46
 - installing 29
 - introduction to 9
 - troubleshooting 47

F

- firewall, allowing communication through 30

H

- "How To" articles on Support site 10

I

- installing
 - client software 40
 - server software 28

- Internet Explorer
 - supported versions of 16
- Internet Information Services (IIS)
 - manually creating virtual directory 47
 - permissions on Temp folders 20
 - supported versions of 15
- L**
- license key file 32
- Links To Related Software folder 19
- load balancing 39, 41
- M**
- manuals and Help files 9
- Microsoft Reporting Services 37
- MSI installer package 41
- N**
- .NET Framework, supported versions of 17–18
- Network Load Balancing (NLB) 28, 39, 41
- NIC Teaming, disabling 22
- Notes client, supported versions of 17, 19
- O**
- Outlook
 - setting registry values for 19
 - supported versions of 16, 19
- Outlook, supported versions of 16, 19
- P**
- per-user and per-machine installations 41
- permissions on Temp folders 20
- prerequisites for Compliance Accelerator 15, 18
- product documentation 9
- R**
- Receive-Side Scaling, disabling 22
- RecipientMax registry value 19
- registry values for Outlook 19
- report templates, uploading 36
- Reviewing configuration settings 21
- S**
- search schedules
 - and SQL Server Agent service 23
- Search Service, disabling 23
- Server Manage, disabling Windows Search Service
 - in 23
- server software
 - installing 28
 - prerequisites for 15
- SQL reporting server
 - changing port used by 44
 - uploading report templates to 36
- SQL Server
 - assigning permissions and roles 24
 - assigning roles 24
 - changing port used by 44
 - prerequisites for 15
- SQL Server Agent service, configuring 23
- Symantec Endpoint Protection, temporarily shutting
 - down 30, 49
- sysadmin role in SQL Server 24
- T**
- TCP Chimney, disabling 22
- TCP Segmentation Offloading, disabling 22
- TCP/IP Offload Engine, disabling 22
- TCP/IP ports 43
- Temp folder permissions 20
- temporary folders, security checks on 21
- U**
- User Account Control (UAC)
 - and Accelerator Manager website 30
 - and Compliance Accelerator installation
 - program 29
- V**
- Vault Service account
 - assigning roles to on SQL reporting server 37
 - SQL Server roles required for 24
- Veritas Cluster Server 39
- Visual C++ 2008 SP1 Redistributable Package 17, 19
- W**
- white papers 10
- Windows. *See* Temp folder permissions
 - allowing communication through firewall 30
 - supported versions of 18
- Windows Search Service, disabling 23
- Windows Server Failover Clustering 39