

Symantec Discovery Accelerator™

Installation Guide

10.0

Symantec Discovery 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: 2012-01-19.

Legal Notice

Copyright © 2012 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, Veritas, 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, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. 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 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 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 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

Contents

Technical Support	3
Chapter 1 Introducing Discovery Accelerator	9
Key features of Discovery Accelerator	9
About the Discovery Accelerator components	9
Product documentation	10
White papers on the Symantec Enterprise Support site	11
"How To" articles on the Symantec Enterprise Support site	11
Comment on the documentation	12
Chapter 2 Preparing to install Discovery Accelerator	13
Configuration options for Discovery Accelerator	13
Discovery Accelerator configuration for large installations	14
Discovery Accelerator configuration for smaller installations	15
Prerequisites for Discovery Accelerator	15
Prerequisites for the SQL Server computer	15
Prerequisites for the Discovery Accelerator server computer	16
Prerequisites for Discovery Accelerator client computers	19
Setting the Windows and ASP.NET Temp folder permissions	20
Disabling networking facilities that can disrupt a Discovery Accelerator environment	21
Configuring the SQL Server Agent service	21
Assigning permissions and roles in SQL databases	22
Assigning SQL Server roles to the Vault Service account	22
Assigning the permissions and roles required to create search schedules	24
Assigning the permissions required to enable cases for analytics	26
Verifying that Enterprise Vault expands distribution lists	26

Chapter 3	Installing Discovery Accelerator	29
	Installing the Discovery Accelerator server software	29
	Allowing Enterprise Vault to communicate with Discovery Accelerator through the firewall in Windows Server 2008 R2	30
	Creating the configuration database and customer databases	31
	Setting up a Custodian Manager Web site	38
	Uploading the Discovery Accelerator report templates	41
	Configuring Discovery Accelerator for use in a Network Load Balancing cluster	44
	Installing the Discovery Accelerator client software	45
	Modifying the configuration file for the Discovery Accelerator client	45
	Using the MSI installer package to install the Discovery Accelerator client	46
	Using ClickOnce to deploy the Discovery Accelerator client	47
Appendix A	Troubleshooting	55
	Enterprise Vault Accelerator Manager service not created	55
	Enterprise Vault Accelerator Manager service does not start	56
	Home page of Web site not found	56
	Cannot create or upgrade Discovery Accelerator customer databases when Symantec Endpoint Protection is running	58
	Other applications using the same TCP/IP ports as Discovery Accelerator	58
	Permissions error when uninstalling the Discovery Accelerator client from a UAC-enabled computer	60
	Users cannot start the Discovery Accelerator client when an invalid ClickOnce update is available for download	60
	Uninstalling the Discovery Accelerator client from a shared location may prevent other users from starting the client	61
Index	63

Introducing Discovery Accelerator

This chapter includes the following topics:

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

Key features of Discovery Accelerator

Discovery Accelerator is an electronic discovery and review system that integrates with Enterprise Vault services and archives. Discovery Accelerator lets authorized users search for, retrieve and preserve, analyze, review, mark, and export or produce emails, documents, and other electronic items for lead counsel examination or court-ready production—rapidly and in a cost-effective manner.

Using attorneys and external counsel to review large numbers of items is costly. With Discovery Accelerator, you can create a hierarchy of reviewers for a discovery action or case, with different levels of reviewers able to assign certain review marks. In this way, paralegal staff and non-legal staff can perform an initial review of search and collection results and leave only the privileged, relevant, or questionable items for counsel. Optionally, you can then produce the relevant items with an appropriate *Bates* number or else simply export them from Discovery Accelerator in various formats.

About the Discovery Accelerator components

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

Table 1-1 The Discovery Accelerator components

Component	Notes
Discovery Accelerator client	The client is used by Discovery Accelerator administrators to set up and manage the system and by reviewers to access the items that they are to mark.
Accelerator Manager Web site	This Web site lets you set up multiple Discovery Accelerator databases in which to store your data.
Enterprise Vault Accelerator Manager service	This service handles the requests from the Discovery Accelerator client and works with the Enterprise Vault components to access archives, perform searches, and so on.
Customer database	<p>The customer database is a SQL database in which Discovery Accelerator stores details of cases, user roles, search results, review marks and tags, and more.</p> <p>You can set up multiple customer databases.</p>
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.
Custodian Manager Web site (optional)	This Web site lets you store the details of the <i>custodians</i> (individual employees) and custodian groups for which you want to search with Discovery Accelerator. A custodian group is any collection of employees, such as Windows or Domino groups and distribution lists, Active Directory or Domino LDAP searches, and Active Directory containers.
Discovery Accelerator API Web site (optional)	<p>This Web site lets you use the Discovery Accelerator API to integrate third-party tools with the software, and thereby retrieve data from or export it to a Discovery Accelerator customer database.</p> <p>For more information on the Discovery Accelerator API, contact Symantec Support.</p>

Product documentation

Table 1-2 lists the documentation that is available for Discovery Accelerator.

Table 1-2 The Discovery Accelerator documentation set

Document	Comments
Installation Guide	Outlines how to perform a first-time installation of the Discovery Accelerator server and client software.
Upgrade Instructions	Explains how to upgrade an existing installation of Discovery Accelerator to version 10.0.
Administrator's Guide	Provides information for Discovery 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 Discovery Accelerator client that are available to reviewers.
Online Help	Accompanies all the Discovery 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 Discovery Accelerator.
Best Practices Guide	Provides extensive information on how best to plan for and implement Discovery Accelerator. To obtain this guide, go to the following page of the Symantec Enterprise Support site: http://www.symantec.com/docs/TECH159520

White papers on the Symantec Enterprise Support site

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

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

For extensive information on how to conduct searches with Discovery Accelerator, see the *Effective Searching* white paper. This is available from the following page of the Symantec Enterprise Support site:

<http://www.symantec.com/docs/TECH88031>

"How To" articles on the Symantec Enterprise Support site

Most of the information in the Discovery Accelerator manuals is also available online as "How To" articles on the Symantec Enterprise Support site. 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 Enterprise Support site

- 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 Discovery 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 Discovery Accelerator

This chapter includes the following topics:

- [Configuration options for Discovery Accelerator](#)
- [Prerequisites for Discovery Accelerator](#)
- [Setting the Windows and ASP.NET Temp folder permissions](#)
- [Disabling networking facilities that can disrupt a Discovery Accelerator environment](#)
- [Configuring the SQL Server Agent service](#)
- [Assigning permissions and roles in SQL databases](#)
- [Verifying that Enterprise Vault expands distribution lists](#)

Configuration options for Discovery Accelerator

Discovery 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, you typically install the server software on a dedicated server. A Microsoft SQL Server stores all the configuration and customer information.

Although you can install the Discovery Accelerator server software on the same computer as your normal Enterprise Vault installation, you may prefer to install it on a separate computer. You can choose from several configuration options. If your planned configuration is different and you are unsure of what to configure on the Discovery Accelerator computer, contact Symantec for advice.

The *Best Practices Guide* provides extensive information on how best to plan for and implement Discovery Accelerator.

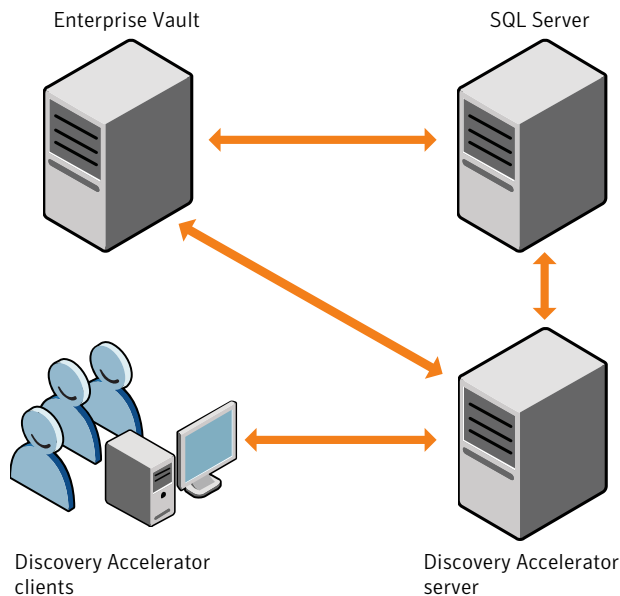
Do not install the Compliance Accelerator and Discovery Accelerator server software on the same computer.

Discovery Accelerator configuration for large installations

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

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

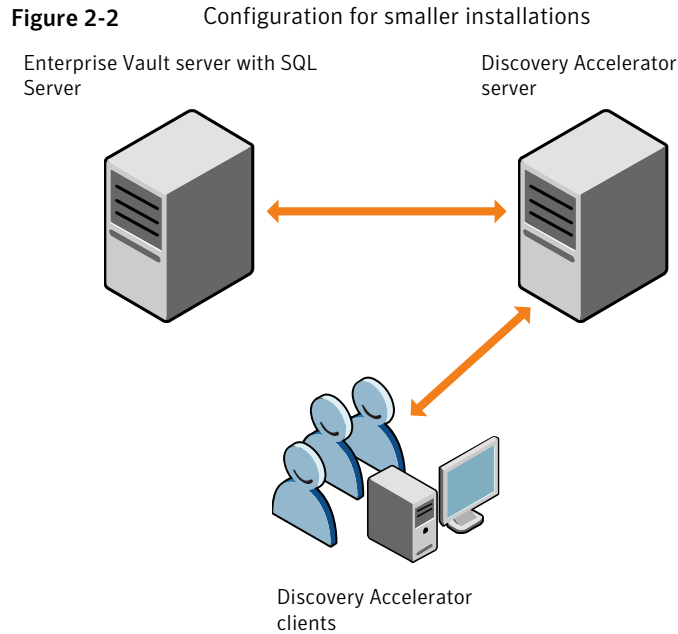
Figure 2-1 Configuration for large installations



Note: For information on the effect that using SQL Server 2008 can have on the analytics facilities in Discovery Accelerator, see the *Administrator's Guide*.

Discovery 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 Discovery Accelerator, SQL Server, and Enterprise Vault on the same computer.

Prerequisites for Discovery Accelerator

The computers on which you install SQL Server, the Discovery Accelerator server software, and the Discovery Accelerator client software each have different requirements.

Prerequisites for the SQL Server computer

The SQL Server computer must be running SQL Server 2005 SP2 or later.

Prerequisites for the Discovery Accelerator server computer

Table 2-1 lists the software items that you must install and configure on the computer that is to run the Discovery Accelerator server software.

Table 2-1 Prerequisite software for Discovery Accelerator server installation

Item	Notes
Windows	You require Windows Server 2008 R2 x64 Edition, original release or SP1.
Internet Information Services (IIS)	You require IIS 7.5 with ASP.NET, IIS 6.0 Management Compatibility, and Windows Authentication.
Internet Explorer	<p>You require Internet Explorer 7.0 or later to run the Accelerator Manager Web site and Custodian Manager Web site.</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>
Internet Explorer Web Controls	<p>The installation package for these controls is in the <code>Links To Related Software</code> folder on the distribution media.</p> <p>Some versions of Windows may display the message "This program has known compatibility issues" when you install the Internet Explorer Web Controls. You can ignore this message, as the Web Controls should still install without problem.</p>

Table 2-1 Prerequisite software for Discovery Accelerator server installation
(continued)

Item	Notes
Enterprise Vault	<p>If Discovery Accelerator is installed on a separate computer from Enterprise Vault, you must install the Enterprise Vault software on the Discovery Accelerator computer.</p> <p>As a minimum, you require a 9.0 or 10.0 version of one of the following:</p> <ul style="list-style-type: none"> ■ Enterprise Vault Services ■ Enterprise Vault API Runtime <p>Note the following important points about the version of Enterprise Vault that you install on the Discovery Accelerator server:</p> <ul style="list-style-type: none"> ■ All Enterprise Vault servers in all Enterprise Vault sites in a Discovery Accelerator environment must run the same version of Enterprise Vault. For example, when using Discovery Accelerator with two Enterprise Vault installations, you cannot have one site that runs Enterprise Vault 9.0 and another that runs Enterprise Vault 10.0. ■ The major version of Discovery Accelerator must be the same as, or one later than, the major version of Enterprise Vault. For example, you can run Discovery Accelerator 10.0 with Enterprise Vault 9.0 servers, but you cannot run Discovery Accelerator 9.0 with Enterprise Vault 10.0. ■ If the major version of Discovery Accelerator is the same as the major version of Enterprise Vault, the minor version (Service Pack) of Discovery Accelerator must be the same as, or later than, the minor version of Enterprise Vault For example, you can run Discovery Accelerator 10.0.1 with Enterprise Vault 10.0 servers, but you cannot run Discovery Accelerator 10.0 with Enterprise Vault 10.0.1. <p>See the Compatibility Charts for more information on supported versions of Enterprise Vault.</p> <p>To search on content in Discovery Accelerator, set indexing on the Enterprise Vault archives to full.</p>

Table 2-1

Prerequisite software for Discovery Accelerator server installation
(continued)

Item	Notes
Outlook	<p>You require one of the following to export Exchange Server items in PST format or download the original versions of the items:</p> <ul style="list-style-type: none">■ Outlook 2003 SP2 or SP3.■ Outlook 2007 SP2.
Windows Installer	<p>You require Windows Installer 3.1 or later. The installation package for version 3.1 is in the <code>Links To Related Software</code> folder on the distribution media.</p>
.NET Framework	<p>You require .NET Framework 3.5 SP1 or later.</p> <p>This is available as a separate download (see the <code>Links To Related Software</code> folder in the distribution media).</p> <p>We recommend that you do not configure the Discovery Accelerator server to download and install .NET Framework updates automatically from the Windows Update site. Contact Symantec Support before installing such updates.</p>
Lotus Notes client	<p>You require version 8.5.2 of the Lotus Notes client to export Lotus 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 <code>Links To Related Software</code> folder on the distribution media.</p>

For the best results, we recommend that you install the Discovery 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 Discovery Accelerator clients to the Enterprise Vault and Discovery 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 Discovery Accelerator searches and export runs. On both the Discovery 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.

The *Best Practices Guide* provides extensive information on the Discovery Accelerator server's hardware requirements. You can obtain this guide from the Symantec Enterprise Support site at <http://www.symantec.com/docs/TECH159520>.

Prerequisites for Discovery Accelerator client computers

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

Table 2-2 Prerequisite software for Discovery Accelerator client installation

Items	Notes
Windows	You require one of the following: <ul style="list-style-type: none">■ Windows XP SP2 or SP3.■ Windows Vista SP1 or SP2.■ Windows 7 original release or SP1.
.NET Framework	You require .NET Framework 3.5 SP1 or later. This is available as a separate download (see the Links To Related Software folder in the distribution media).
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 2003 SP1 or later.■ Outlook 2007.■ Outlook 2010.

Table 2-2 Prerequisite software for Discovery Accelerator client installation (continued)

Items	Notes
Lotus Notes client	You require version 7.0.3 or later of the Lotus Notes client to view Lotus 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 Lotus 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 Discovery Accelerator client is 1024×768 or higher. For the best results, ensure that your client computers have at least 2 GB of memory.

Setting the Windows and ASP.NET Temp folder permissions

To enable users to access any of the Discovery Accelerator Web sites, 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 Discovery 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, ensure that **Allow inheritable permissions from parent to propagate to this object** is checked.

Disabling networking facilities that can disrupt a Discovery Accelerator environment

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

To disable networking facilities that can disrupt a Discovery Accelerator environment

- 1 Disable the following features on your designated Discovery 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 Enterprise Support site 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 Discovery Accelerator servers.

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

Configuring the SQL Server Agent service

Discovery 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.

You must also ensure that the SQL Server Agent service is running if you want to use the analytics facilities in Discovery Accelerator to mark or tag items automatically. For more information on these facilities, see the *Administrator's Guide*.

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 permissions and roles in SQL databases

You must assign a number of SQL Server roles and permissions to the Vault Service account to perform various activities with Discovery Accelerator. The Vault Service account is the account that Enterprise Vault services and tasks use when accessing Enterprise Vault databases.

Assigning SQL Server roles to the Vault Service account

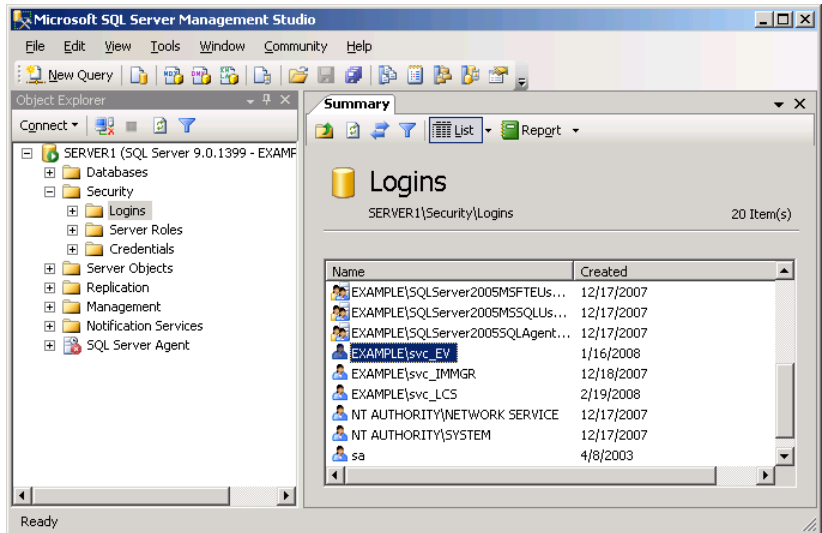
The facility to create configuration and customer databases with Discovery Accelerator is dependent on the Vault Service account having the SQL Server role of database creator (dbcreator).

You may also want to assign the system administrator (sysadmin) role to the Vault Service account.

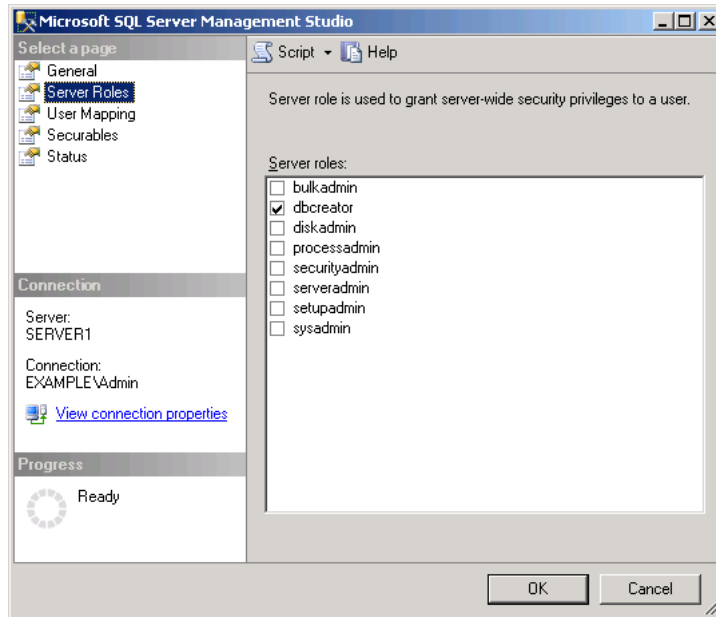
To assign SQL Server roles to the Vault Service account

- 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, 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 that **dbcreator** is checked.



Discovery 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, Discovery Accelerator assumes that you want to make a user with the SQL system administrator (sysadmin) role the creator and owner of them. Therefore, you can either grant the sysadmin role to the Vault Service account or take the following additional steps to assign the minimum permissions needed to the Vault Service account:

- Follow the instructions in the next section to grant permissions and roles in the msdb system database to the Vault Service account.
- After you have installed the Discovery Accelerator client, change the value of the security configuration option "Use SQL Server 2005 SystemAdmin Server Role for Schedules". For instructions on how to do this, see the *Administrator's Guide*.

Assigning the permissions and roles required to create search schedules

If you do not assign the SQL sysadmin role to the Vault Service account, you must grant sufficient permissions and roles to this account to make it the creator and owner of Discovery Accelerator search schedules. Briefly, you must do the following:

- Add the Vault Service account to the msdb system database.
- Grant permissions to the Vault Service account in various msdb tables and stored procedures.
- Assign the database role SQLAgentUserRole to the Vault Service account.

The following sections describe these activities in more detail.

To add the Vault Service account to the msdb system database

- 1 On the SQL Server computer, start SQL Server Management Studio.
- 2 Select the required SQL Server.
- 3 Browse to **Databases > System Databases > msdb > Security > Users**.
- 4 Right-click **Users**, and then click **New User**.
- 5 In the **User name** box, enter a new user name.
- 6 In the **Login name** box, enter the domain and user name of the Vault Service account in the form *domain\user_name*.
- 7 Click **OK**.

To grant permissions to the Vault Service account

- 1 Right-click the new user that you have just created, and then click **Properties**.
- 2 Select the **Securables** page.
- 3 Add the following msdb tables to the list of securables, and then grant the Select permission for them to the Vault Service account:
 - sysjobs
 - sysjobschedules
 - sysjobsteps
 - sysschedules
- 4 Add the stored procedure sp_add_category to the list of securables, and then grant the Execute permission for it to the Vault Service account.

To assign the database role SQLAgentUserRole to the Vault Service account

- 1 Browse to **Databases > System Databases > msdb > Security > Roles > Database Roles**.
- 2 Right-click **SQLAgentUserRole**, and then click **Properties**.
- 3 On the **General** page, click **Add**, and then select the Vault Service account that you have just created.

Assigning the permissions required to enable cases for analytics

To enable cases for analytics, the Vault Service account requires a number of permissions in various msdb tables and stored procedures. Without these permissions, errors occur when you try to enable a case for analytics.

To assign the permissions required to enable cases for analytics

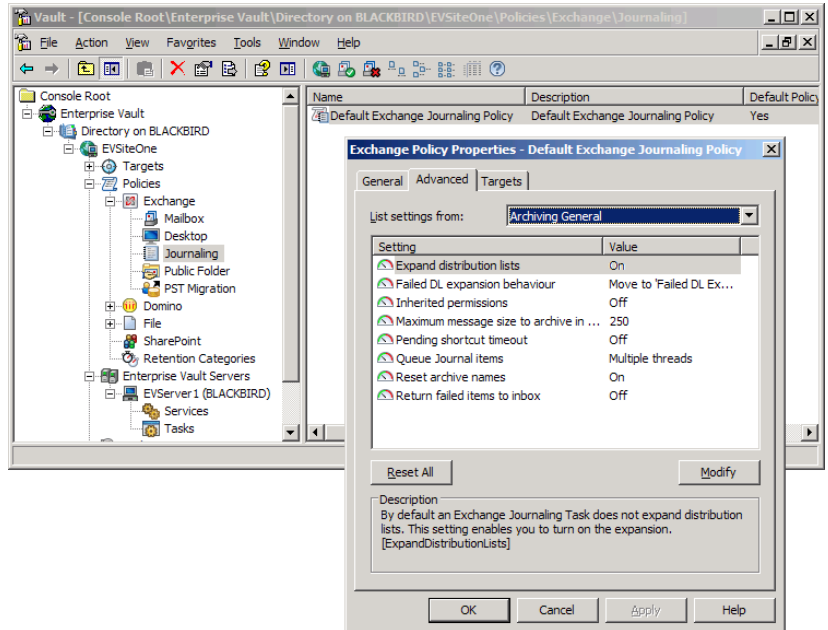
- 1 On the SQL Server computer, start SQL Server Management Studio.
- 2 Select the required SQL Server.
- 3 Browse to **Databases > System Databases > msdb > Security > Users**.
- 4 Right-click the Vault Service account, and then click **Properties**.
- 5 Select the **Securables** page.
- 6 Add the following msdb tables to the list of securables, and then grant the Select permission for them to the Vault Service account:
 - sysjobhistory
 - sysjobs
 - sysjobschedules
 - sysjobservers
 - sysjobsteps
 - sysschedules
- 7 Add the following stored procedures to the list of securables, and then grant the Execute permission for them to the Vault Service account:
 - sp_add_category
 - sp_add_job
 - sp_add_jobschedule
 - sp_add_jobserver
 - sp_add_jobstep

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 Discovery Accelerator

This chapter includes the following topics:

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

Installing the Discovery Accelerator server software

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

To install the Discovery Accelerator server software

- 1 Start the Discovery Accelerator installation program (`Symantec Enterprise Vault Discovery Accelerator Server_language.msi`).
- 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 but not the Custodian Manager Web site or Discovery Accelerator API Web site.

- 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 Web site. Then you can create the configuration database and customer databases.

The installation program automatically opens the Accelerator Manager Web site with administrator privileges if you have installed Discovery Accelerator on a server in which User Account Control (UAC) is enabled. (This is a requirement when accessing the Web site 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 Web site. 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 31.

- 4 If you want to use the Legal Hold facility to stop users from deleting items from their archives, you must install a Discovery Accelerator license on each storage server in your Enterprise Vault site. To install the license, find the Enterprise Vault license key file on each server, and open it in a text editor. Then paste into the file the Discovery Accelerator license key with which you have been provided.

The following is a typical example of a key:

```
<key>
  <name>EVDA</name>
  <version>1.0</version>
  <start_date>2009-05-28</start_date>
  <end_date>2010-12-31</end_date>
  <warn_policy>1,07</warn_policy>
</key>
```

Contact Symantec Corporation to obtain your license key, if you do not already have it.

Allowing Enterprise Vault to communicate with Discovery Accelerator through the firewall in Windows Server 2008 R2

If you have installed the Discovery Accelerator server software on a Windows 2008 R2 computer, you must configure the Windows firewall to permit Enterprise

Vault to communicate with Discovery Accelerator through it. Certain interactions between the Enterprise Vault server and the Discovery Accelerator server require unrestricted communication. You can allow Enterprise Vault to communicate with Discovery 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 Discovery Accelerator through the firewall in Windows Server 2008 R2

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

Creating the configuration database and customer databases

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

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 cases, user roles, search results, review marks and tags, 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 Discovery 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 Discovery Accelerator system. Setting up two customers lets both departments use Discovery Accelerator without needing access to the same Discovery Accelerator setup.

Before you proceed, note the following:

- If you have installed Discovery Accelerator on a server in which User Account Control (UAC) is enabled, you must open the Accelerator Manager Web site with administrator privileges. Right-click the **Internet Explorer** shortcut on the Windows **Start** menu and then click **Run As Administrator**.
- If Symantec Endpoint Protection is running on your Discovery Accelerator server, we recommend that you shut it down temporarily.
See [“Cannot create or upgrade Discovery Accelerator customer databases when Symantec Endpoint Protection is running”](#) on page 58.

To create the configuration database

- 1 If you have yet to display the Accelerator Manager Web site, 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 Discovery 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	<p>Specifies the name of the configuration database. The name cannot contain any of the following characters:</p> <p>\/:*?"<> '</p> <p>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.</p>
Use Existing Database	Instructs Discovery 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 E:\SQLData. 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 Discovery Accelerator prompts you to do so, restart the Enterprise Vault Accelerator Manager service by using the Services snap-in to Microsoft Management Console.
- 4 In the Accelerator Manager Web site, click **Upload License** to import your license key file into Discovery Accelerator.

To create the customer databases

- 1 In the left pane of the Accelerator Manager Web site, 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	Specifies whether this database is a customer database for Discovery Accelerator or Custodian Manager.
Name	Specifies a unique name for the customer. The name cannot contain any of the following characters: <code>\/:*?"<> '</code>
Directory DNS aliases	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. If you want to specify multiple Directory service computers, type the details of each one on a line of its own.

Administrator User or Group	<p>Optionally nominates an Active Directory user account or group account as an administrator for the Discovery 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 Discovery Accelerator client. If you uncheck this option, only automatic tasks like scheduled searches are permissible.</p>

IIS section

Virtual Directory	<p>Specifies the name of the IIS virtual directory for the Discovery API Web site. This site lets software developers integrate third-party tools with Discovery Accelerator, and thereby retrieve data from or export it to a Discovery Accelerator customer database.</p> <p>No two customers can share the same virtual directory name. The directory name must not include space characters or any of the following characters:</p> <p>* ? \ / % ' "</p> <p>Note that you cannot name the virtual directory for any Discovery Accelerator customer as "EVBAAdmin", because this name is reserved for the Accelerator Manager Web site.</p>
IIS Server	<p>Specifies the name or IP address of the IIS server that is to host the Discovery 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 ([]).</p> <p>The default entry for this field is the server on which you are running the Accelerator Manager Web site.</p>

Manage Virtual Directory	Lets you administer the virtual directory by using the Discovery 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. The default entry for this field is the server on which you are running the Accelerator Manager Web site.
------------	---

Database	Specifies the name of the customer database. The name cannot contain any of the following characters: \\/:*?"<> '
----------	--

Use Existing Database	Instructs Discovery 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 E:\SQLData.
------------------	--

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 F:\SQLLogs.
-----------------	--

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.

Database Locations For Analytics section

This area of the page lists existing database locations for analytics data, and lets you add new database locations. You must specify at least one database location for analytics. If you do not intend to use the analytics feature with this customer, use the default database location.

See [“Configuring analytics database locations”](#) on page 36.

- 3
- Wait for Discovery 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.

Configuring analytics database locations

When you enable a case for analytics, Discovery Accelerator must fetch all the case items from Enterprise Vault into the customer database, and index them. This requires a large amount of disk space. Discovery Accelerator lets you define locations to host the analytics table file groups and indexes. You can add more locations when you need more disk space.

The Customer page of the Accelerator Manager Web site lists existing analytics database locations, and lets you add more. Next to each location, check marks in

the **Table File Group** and **Full Text Indexes** columns show whether the location is used for table files, search indexes, or both.

When you plan and configure analytics database locations, consider the following:

- The volume of data. The collection and indexing of analytics data can generate very large databases and index files. As a rough guide, collecting one million items that are all 20 kilobytes in size can produce a database that is 40 gigabytes or more in size. However, this can vary from one environment to another. The *Best Practices Guide* for Discovery Accelerator provides extensive information on how to size your Discovery Accelerator databases appropriately. You can obtain this guide from the Symantec Enterprise Support site at <http://www.symantec.com/docs/TECH159520>.
- Performance. Host each database location on a physically separate disk. If you have more than one analytics database location, Discovery Accelerator uses them in rotation to spread the data and the disk access requirements. Each Discovery Accelerator case uses only one location for the search index and one location for the database.

The following examples show two valid configurations for analytics database locations.

Table 3-1 Analytics database locations: example 1

Location	Table File Group	Full Text Indexes
C:\SQL\Data	Checked	Checked
D:\SQL\Data	Checked	Checked
E:\SQL\Data	Checked	Checked
F:\SQL\Data	Checked	Checked

Table 3-2 Analytics database locations: example 2

Location	Table File Group	Full Text Indexes
C:\SQL\Data	Unchecked	Checked
D:\SQL>Data	Unchecked	Checked
E:\SQL>Data	Checked	Unchecked
F:\SQL>Data	Checked	Unchecked

To add a database location for analytics

- 1 Browse to the Accelerator Manager Web site.
- 2 Right-click the appropriate customer, and then click **Properties**.
- 3 Under **Database Locations For Analytics**, click **New Location**.
- 4 Enter the path to the new database location. Note the following:
 - The database locations must reside on the SQL server, and you must use local paths to refer to them. For example, do not use UNC paths to refer to database locations.
 - The Accelerator Manager Web site does not verify that the specified locations exist. You must ensure that the paths are valid.
- 5 Check **Table File Group**, **Full Text Indexes**, or both.
- 6 Click **OK** next to the new location.
- 7 Repeat steps 3 through 6 if you want to add more database locations.

Setting up a Custodian Manager Web site

Custodian Manager is a browser-based application with which you can store the details of the custodians (individual employees) and custodian groups for which you want to search with Discovery Accelerator. A custodian group is any collection of employees, such as Windows or Domino groups and distribution lists, Active Directory or Domino LDAP searches, and Active Directory containers. After you have added the custodians and custodian groups to Custodian Manager, you can pick from them when you define the criteria for a Discovery Accelerator search.

Note: A Discovery Accelerator configuration database can have one Custodian Manager Web site only. All customers that share the configuration database share Custodian Manager.

To set up a Custodian Manager Web site

- 1 Open the Accelerator Manager Web site.

If you have installed Discovery Accelerator on a server in which User Account Control (UAC) is enabled, you must open the Accelerator Manager Web site with administrator privileges.
- 2 Right-click the server node in the left pane, and then click **New Customer**.
- 3 In the Create Customer page, set the customer type to **Custodian Manager**.
- 4 Enter your preferred IIS and SQL database details, and then click **OK**.

- 5 Browse to the Custodian Manager Web site that you have just created. The address of this Web site takes the following form:

`http://server_name/virtual_directory`

For example:

`http://server2/EVBACustodianManager`
- 6 Use the facilities in Custodian Manager to create and manage the custodians and custodian groups. For instructions on how to do this, see the *Administrator's Guide* and the online Help for Custodian Manager.

Assigning the required Active Directory permissions to the Custodian Manager synchronization account

By default, Custodian Manager uses the account under which the Accelerator Manager service is running when it synchronizes custodians and custodian groups with the corresponding Active Directory accounts. However, if you prefer, you can nominate a different account on a per-domain basis.

For instructions on how to specify a different user account for synchronization purposes, see the *Administrator's Guide*.

The nominated synchronization account must have certain delegated permissions to query the Active Directory domain.

To assign the required delegated permissions to the Custodian Manager synchronization account

- 1 Open Active Directory Users and Computers.
- 2 Right-click the domain object, and then select **Delegate Control**.
- 3 In the Delegation of Control Wizard, click **Next**, and then click **Add**.
- 4 In the Select Users, Computers, or Groups dialog box, enter the required account name, and then click **OK**, and then click **Next**.
- 5 In the Tasks to Delegate page, in **Delegate the following common tasks**, check the following tasks, and then click **Next**:
 - Read all user information
 - Read all inetOrgPerson information
- 6 Click **Finish**.

The Custodian Manager synchronization account must also have List Content and Read Property permissions on the Deleted Objects container in Active Directory. Without these permissions, it is not possible to deactivate any custodians

and custodian groups whose Active Directory details have been moved to the Deleted Objects container.

The following article on the Microsoft Web site provides detailed instructions on how to view and set permissions on the Deleted Objects container:

[http://technet.microsoft.com/en-us/library/cc816824\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc816824(WS.10).aspx)

In brief, the procedure is as described below.

To give the Custodian Manager synchronization account access to the Deleted Objects container in Active Directory

- 1 On the Windows **Start** menu, right-click **Command Prompt** and then click **Run as administrator**.
- 2 Take ownership of the Deleted Objects container by running the `dsaccls` command-line utility, as follows:

```
dsaccls deleted_objects_dn /takeownership
```

where the parameters are as follows:

<code>deleted_objects_dn</code>	The distinguished name of the Deleted Objects container.
<code>/takeownership</code>	Take ownership of the Deleted Objects container.

For example:

```
dsaccls "CN=Deleted Objects,DC=Contoso,DC=com" /takeownership
```

- 3 Grant the List Content and Read Property permissions to the user account under which Custodian Manager synchronizes custodians and custodian groups, as follows:

```
dsaccls deleted_objects_dn /G user_or_group:permissions
```

where the parameters are follows:

<code>deleted_objects_dn</code>	The distinguished name of the Deleted Objects container.
<code>user_or_group</code>	The user or group to whom the permissions apply.
<code>permissions</code>	The permissions to grant. For List Content and Read Property, specify the permissions as LCRP.

For example:


```
dsacIs "CN=Deleted Objects,DC=Contoso,DC=com" /G  
CONTOSO\VaultAdmin:LCRP
```

Uploading the Discovery Accelerator report templates

Using Microsoft SQL Server Reporting Services as the reporting mechanism, Discovery Accelerator provides extensive facilities for monitoring the details of a case and validating compliance with discovery requests. 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 Discovery 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.

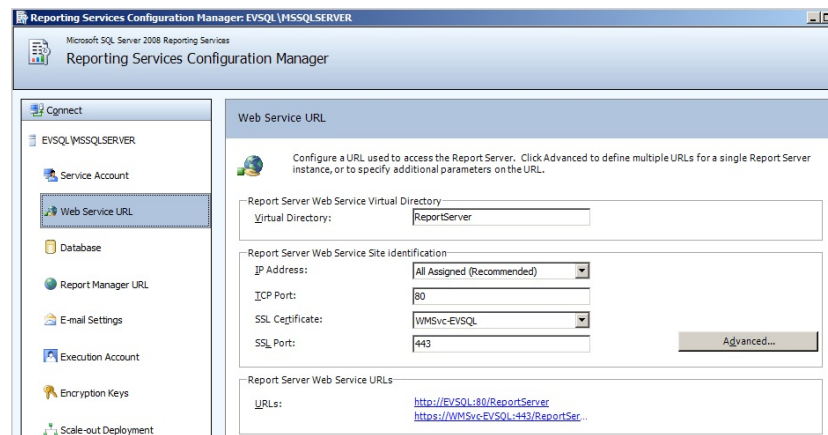
Note: Any reports that you used with Discovery Accelerator 2007 or earlier are not suitable for use with Discovery Accelerator 10.0.

To upload the Discovery 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:

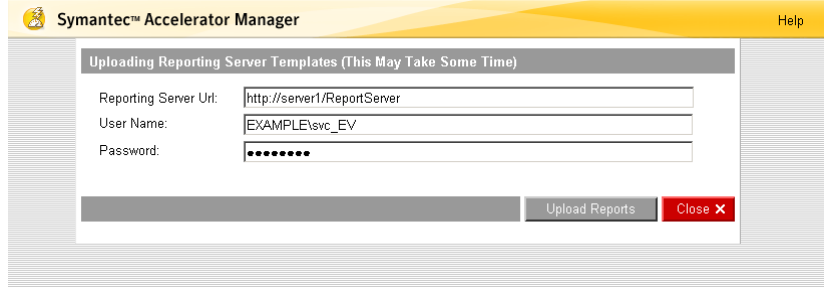
- The System Administrator role on the SQL reporting server.
You can assign this role by using the browser-based Report Manager tool that comes with SQL Server. First click **Site Settings** on the global toolbar in Report Manager and then click **Security**. Then click **New Role Assignment** and assign 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 Discovery Accelerator server, open the Accelerator Manager Web site.

- 4 Click **Reporting Server** at the bottom of the page.

The Uploading Reporting Server Templates page appears.



The screenshot shows the Symantec Accelerator Manager interface. At the top, there is a yellow header bar with the Symantec logo and the text 'Symantec™ Accelerator Manager'. On the right side of the header is a 'Help' link. Below the header, a dialog box titled 'Uploading Reporting Server Templates (This May Take Some Time)' is displayed. The dialog box contains three input fields: 'Reporting Server Url:' with the value 'http://server1/ReportServer', 'User Name:' with the value 'EXAMPLE\svc_EV', and 'Password:' with masked characters '*****'. At the bottom of the dialog box, there are two buttons: 'Upload Reports' and 'Close X'.

- 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 Discovery Accelerator server and SQL reporting server.

Caution: The Accelerator Manager Web site 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, Discovery 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.

Configuring Discovery 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.

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 Discovery Accelerator by distributing client requests across the nodes in the cluster; background Discovery 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 Discovery Accelerator client, your users must specify this virtual name or address as the server to which they want to connect.

For more information on load balancing, see the *Best Practices Guide*. This is available from the following page of the Symantec Enterprise Support site:

<http://www.symantec.com/docs/TECH159520>

To configure Discovery 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 Discovery Accelerator server software on each node in the cluster.
As a minimum, you must install the Enterprise Vault Accelerator Manager service on each node.

Installing the Discovery Accelerator client software

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

The Discovery Accelerator release media include two packages with which you can install the client software on your users' computers:

- An MSI installer package.
- A ClickOnce installation package. ClickOnce is a Microsoft technology that lets users install a Windows application by clicking a link in a Web page.

One advantage of using the MSI installer package is that it lets you install the client software on a per-user or per-machine basis, whereas ClickOnce installations are on a per-user basis only. On the other hand, ClickOnce provides the ease of deployment of Web applications and makes it simple to distribute updates to the Discovery Accelerator client.

Note: You cannot use both packages to install or upgrade the Discovery Accelerator client on the same computer.

Modifying the configuration file for the Discovery Accelerator client

Before you proceed, it is a good idea to modify the configuration file that accompanies your chosen installation package. One of the settings in this file is the name or address of the computer on which you have installed the Discovery 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 Discovery Accelerator client.

To modify the configuration file for the Discovery Accelerator client

- 1 Locate the configuration file `AcceleratorClient.Exe.Config` in the installation media for the Discovery 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 Discovery Accelerator server software. For example:

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

If you have configured Discovery 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 Discovery Accelerator client

Typically, you distribute the Discovery 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 Discovery 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 Discovery Accelerator client software

- 1 Ensure that the configuration file `AcceleratorClient.Exe.Config` file is in the installation folder for the Discovery Accelerator client software.
- 2 Do one of the following:
 - To perform a per-user installation, start the Discovery Accelerator installer package (Symantec Enterprise Vault Discovery 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 Discovery  
Accelerator Client.msi" TARGETDIR="install_path" ALLUSERS=1
```

Where:

<i>path_to</i>	Specifies the path to the .msi file.
<i>install_path</i>	Specifies the path to the folder in which to create an Enterprise Vault Discovery 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 Discovery Accelerator, you must type the following:

```
msiexec /I "D:\Symantec Enterprise Vault Discovery Accelerator  
Client.msi" TARGETDIR="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. Right-click the **Command Prompt** shortcut on the Windows **Start** menu and then click **Run as Administrator**.

- 3 Follow the on-screen instructions.

Using ClickOnce to deploy the Discovery Accelerator client

ClickOnce is a deployment technology that Microsoft has developed for the .NET Framework. It is designed to deploy applications from the Web, keep them up to date, and minimize the effect that those applications have on your users' computers.

In outline, the procedure for using ClickOnce to deploy the Discovery Accelerator client is as follows:

- Obtain a code-signing certificate with which to sign the ClickOnce package.
- Obtain the SHA-1 thumbprint of the code-signing certificate.
- Edit the supplied MSBuild file to suit your environment, and then build the final deployment package.
- Copy the deployment package to your IIS Server computer.

- Set up a Web site from which users can run the installation.

The following sections describe these steps in more detail.

Note: The Discovery Accelerator release media include a ready-made ClickOnce package with which you can review the contents of a deployment package without needing to obtain a certificate, edit the MSBuild file, or build the final package. However, this sample package is not intended for use in production environments.

Obtaining a code-signing certificate

One of the fundamentals of the ClickOnce design is that deployment packages must be secure and trusted. So, it is a requirement that all ClickOnce packages are signed using a suitable code-signing certificate. If you do not have one, you can make a self-signed certificate by running Microsoft's Certificate Creation Tool (`Makecert.exe`). This tool is available in recent versions of Visual Studio and the Windows SDK.

To make a self-signed certificate

- 1 Open a Command Prompt window.
- 2 Change to the folder in which you have installed `Makecert.exe`.
- 3 Type the following command:

```
makecert -a sha1 -b mm/dd/yyyy -e mm/dd/yyyy -eku oid -n
"CN=certificate_name" -pe -r -ss store
```

where the parameters are as follows:

- a Specifies that you want to use SHA-1 as the signature algorithm.
- b Specifies the date from which the certificate is valid.
- e Specifies the date on which the certificate expires.
- eku Inserts one or more key usage object identifiers (OIDs) into the certificate to denote that the certificate is intended for code signing.
- n Specifies the certificate name. This name must conform to the X.500 standard. The simplest method is to enclose the name in double quotation marks and precede it with CN=; for example, "CN=myName".
- pe Marks the generated private key as exportable so that you can include it in the certificate.
- r Creates a self-signed certificate.

-ss Identifies the certificate store in which to store the output certificate. Enter `My` to store the certificate in your personal store.

For more information on these options, see the following article on the Microsoft Web site:

[http://msdn.microsoft.com/en-us/library/bfskty3\(VS.80\).aspx](http://msdn.microsoft.com/en-us/library/bfskty3(VS.80).aspx)

For example, the following command creates a self-signed certificate that "YourCompany Inc" has issued and that is valid until January 2036. The command imports the certificate directly into your personal certificate store:

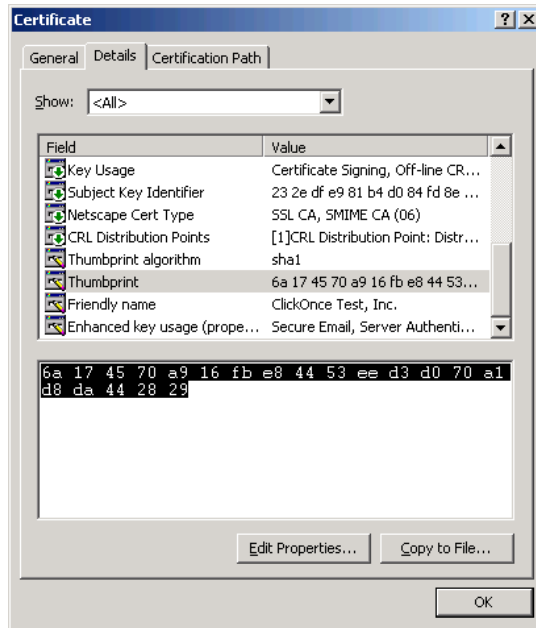
```
makecert -a sha1 -b 01/01/2000 -e 01/01/2036 -eku  
1.3.6.1.5.5.7.3.3 -n "CN=YourCompany Inc" -pe -r -ss My
```

Obtaining the SHA-1 thumbprint of the code-signing certificate

As part of the procedure for customizing the ClickOnce deployment package, you must supply the SHA-1 thumbprint of your code-signing certificate.

To obtain the SHA-1 thumbprint of the code-signing certificate

- 1 On the Windows **Start** menu, click **Run**.
- 2 Type `MMC`, and then click **OK** to open the Microsoft Management Console.
- 3 On the **File** menu, click **Add/Remove Snap-in**.
- 4 In the Add/Remove Snap-in dialog box, click **Add**.
- 5 In the Add Standalone Snap-in dialog box, click **Certificates**, and then click **Add**.
- 6 In the Certificates snap-in dialog box, click **My user account**, and then click **Finish**.
- 7 Click **Close** to close the Add Standalone Snap-in dialog box.
- 8 Click **OK** to close the Add/Remove Snap-in dialog box.
- 9 In the console tree at the left, under **Certificates - Current User**, double-click **Personal** and then click **Certificates**.
- 10 Double-click the certificate that you want to use for code signing.
- 11 On the **Details** tab of the Certificate dialog box, click the **Thumbprint** field.



- 12 Select the value of the **Thumbprint** field, and then press Ctrl+C to copy it to the Clipboard.

Customizing and building the ClickOnce deployment package

The Discovery Accelerator ClickOnce package comes with a file called `GenerateClickOnce.msbuild`, which you can customize to suit your environment. For example, this file lets you specify the IIS Server address from which users can run the installation. You can also choose whether an installed Discovery Accelerator client should perform an update check at start-up.

After you have set your preferred configuration options in the file, use the MSBuild engine to build the final deployment package. This engine is included in .NET Framework 2.0 and later.

To customize and build the ClickOnce deployment package

- 1 Copy the files from the following folder in the release media to a new folder on your local drive:

```
..\Symantec Enterprise Vault Discovery Accelerator
version\Client\ClickOnce\ApplicationFiles
```

- 2 Browse to the new folder in Windows Explorer.

3 Open the `GenerateClickOnce.msbuild` file in a plain text editor such as Windows Notepad.

4 Modify the following properties at the start of the file:

Thumbprint	Specifies the SHA-1 thumbprint of the code-signing certificate. Remove the spaces from the string. This certificate must exist in your personal store. See “Obtaining the SHA-1 thumbprint of the code-signing certificate” on page 49.
OutputPath	Specifies the folder in which to output your ClickOnce deployment package.
DeploymentPath	Specifies the IIS Server address from which users can obtain the ClickOnce deployment package. See “Making the ClickOnce deployment package available for download” on page 52.
EnableAutoUpdates	Specifies whether an installed Discovery Accelerator client should automatically check your nominated deployment path for updates. Valid settings are "true" or "false".

For example, you can set the properties as follows:

```
<Thumbprint>df9634cc5e654f07521d11de8bc03d6ed789ef8e</Thumbprint>  
<OutputPath>\\Server1\WebServer</OutputPath>  
<DeploymentPath>http://server2/discovery</DeploymentPath>  
<EnableAutoUpdates>true</EnableAutoUpdates>
```

5 Save and close the file.

6 In Windows Explorer, search the folders under your .NET Framework installation for the file `MSBuild.exe`.

7 Open a Command Prompt window.

8 Change to the folder that contains the most recent version of `MSBuild.exe`. For example, you can type the following:

```
cd C:\WINDOWS\Microsoft.NET\Framework\v3.5
```

- 9 Type the following command:

```
MSBuild path_to\GenerateClickOnce.msbuild
```

where *path_to* specifies the absolute path to the `GenerateClickOnce.msbuild` file. For example, you can type the following:

```
MSBuild c:\ClickOnce\GenerateClickOnce.msbuild
```

MSBuild creates the final deployment package in the folder that you specified with the `OutputPath` property.

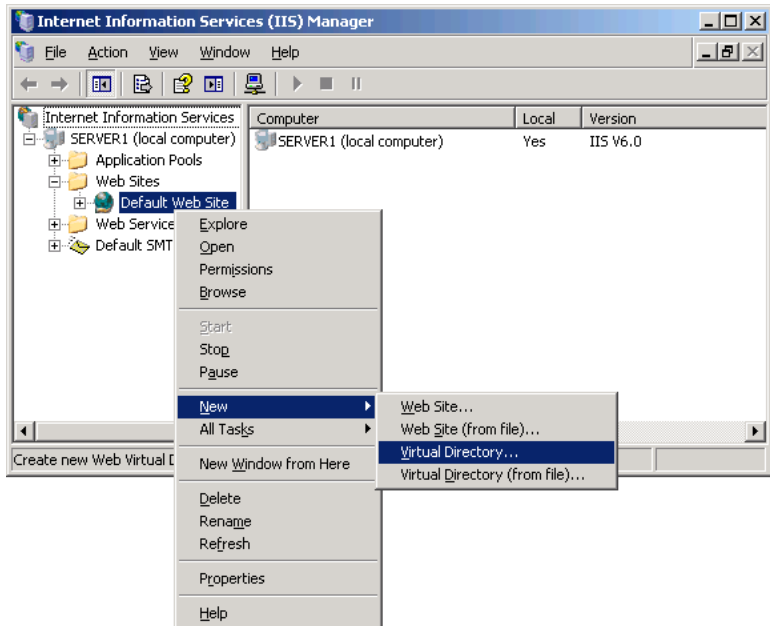
- 10 Copy the contents of the output folder to the required location on your IIS Server computer.

Making the ClickOnce deployment package available for download

After you have built the ClickOnce deployment package and copied it to a folder on your IIS Server computer, you must set up a Web site in IIS that points to this folder.

To make the ClickOnce deployment package available for download

- 1 Open IIS Manager on the server that is to host the Web site.
- 2 Right-click the container for your default Web site and then click **New > Virtual Directory**.



- 3 When the Virtual Directory Creation Wizard appears, click **Next**.
- 4 Set the virtual directory alias to match the value of the DeploymentPath property in your `GenerateClickOnce.msbuild` file.
For example, you would set the alias to `Discovery` if you set the DeploymentPath property to `http://server2/discovery`.
- 5 For the Web site home directory, enter the path to the folder that contains the ClickOnce deployment package, and then click **Next**.
- 6 When the wizard prompts you 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 to host the Web site.
- 2 Right-click the new virtual directory, and then click **Properties**.
- 3 On the **Directory Security** tab, click **Edit** under **Authentication and access control**.
- 4 Ensure that **Enable anonymous access** is checked.

- 5 On the **HTTP Headers** tab, click **MIME Types**.
- 6 In the MIME Types dialog box, register the following file extensions and their associated MIME types:
 - The file extension `.Deploy` and the MIME type `application/octet-stream`.
 - The file extension `.Manifest` and the MIME type `text/xml`.

Installing the Discovery Accelerator client from the IIS Server computer

Users can install the ClickOnce package after you have deployed it to your IIS Server computer.

Note: The Discovery Accelerator client provides a facility with which you can notify new users that the ClickOnce deployment package is available. When you assign a role to a user in the **Role Assignment** tab of the Discovery Accelerator client, you can click **Send Email Invite** to let the user know that he or she may now perform a ClickOnce installation of the client. For more information, see the *Administrator's Guide*.

To install the Discovery Accelerator client from the IIS Server computer

- 1 Open Internet Explorer.
- 2 Browse to the Web site from which you can obtain the ClickOnce deployment package.

For example, you can specify the Web site address as
`http://server2/discovery`.
- 3 Click **Install**.

Updating a ClickOnce installation

ClickOnce packages are designed to be easily updated. When a new version of the Discovery Accelerator client is available, you must rebuild the deployment package and copy it to your IIS Server computer. The update option that you have set in the `GenerateClickOnce.msbuild` file determines whether users download the updated version of the client software when they next start the client.

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 Web site not found](#)
- [Cannot create or upgrade Discovery Accelerator customer databases when Symantec Endpoint Protection is running](#)
- [Other applications using the same TCP/IP ports as Discovery Accelerator](#)
- [Permissions error when uninstalling the Discovery Accelerator client from a UAC-enabled computer](#)
- [Users cannot start the Discovery Accelerator client when an invalid ClickOnce update is available for download](#)
- [Uninstalling the Discovery 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 Discovery 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 Discovery 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 Web site not found

If you receive the message “Page Cannot Be Displayed” when you browse to the home page of the Accelerator Manager site, Custodian Manager site, or Discovery Accelerator API site, start IIS Manager and then check the following:

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

If the installation program failed to create the 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 Web site.
- 2 Right-click the container for your default Web site 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 For the Accelerator Manager Web site.

EVBACustodianManager For the Custodian Manager Web site.

EVBADiscovery For the Discovery Accelerator API Web site.

- 5 For the Web site home directory, enter the path to the appropriate subfolder of the Discovery Accelerator program folder (`AcceleratorAdminWeb` or `CustodianManagerWeb`), 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 Web site.
- 2 Right-click the `EVBAAdmin`, `EVBACustodianManager`, or `EVBADiscovery` 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 Web site is running.

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

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

When the Discovery Accelerator server is running in a centrally managed Symantec 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 Discovery Accelerator server, it saves you from having to shut down Symantec Endpoint Protection completely.

To disable Symantec Endpoint Protection's Intrusion Prevention check

- 1 Log on to the computer where the Symantec Endpoint Protection Manager Console is running.
- 2 Click **Start > Programs > Symantec Endpoint Protection Manager > Symantec 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 Symantec Endpoint Protection to roll out the policy to the servers in the group.

Other applications using the same TCP/IP ports as Discovery Accelerator

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

Table A-1 Default TCP/IP ports for Discovery Accelerator

Port	Used by
8085	The Discovery Accelerator Web sites (Accelerator Manager, Custodian Manager, and Discovery Accelerator API).
8086	Discovery Accelerator clients to communicate with the Discovery Accelerator server.

If another application needs to use these ports, you can set Discovery Accelerator to use different ones.

To change the port that the Discovery Accelerator Web sites use

- 1 On the Discovery Accelerator server, locate the copies of the `Web.config` file in the `AcceleratorAdminWeb` and `CustodianManagerWeb` subfolders of the Discovery Accelerator installation folder.
- 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 that a Discovery Accelerator client uses to communicate with the server

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

This folder is typically `%HOMEPATH%\Local Settings\Application Data\Enterprise Vault Discovery 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.

Permissions error when uninstalling the Discovery 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 Discovery 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 Discovery Accelerator Client.msi*. The issue does not arise when you choose to uninstall a per-user MSI installation or ClickOnce 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 Discovery Accelerator client in these circumstances

- 1 Right-click the **Command Prompt** shortcut on the Windows **Start** menu, and then click **Run as Administrator**.
- 2 Enter the credentials that you want to use, and then click **OK**.
- 3 Type the following command:

```
msiexec /x "path_to/Symantec Enterprise Vault Discovery  
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.

Users cannot start the Discovery Accelerator client when an invalid ClickOnce update is available for download

If you publish a corrupt or out-of-date ClickOnce update on your IIS Server computer, users may be unable to start the Discovery Accelerator client when they next try to do so. To resolve this issue, copy the previously working ClickOnce deployment package to your IIS Server computer.

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

If a user uninstalls the Discovery 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 Discovery Accelerator clients.

To perform a repair installation of the Discovery 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 Discovery 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.

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

Index

A

- Accelerator Manager service
 - creating manually 55
 - introduction to 10
 - troubleshooting 56
- Accelerator Manager Web site
 - introduction to 10
 - opening with administrator privileges 32
 - supported versions of Internet Explorer 16
- AcceleratorClient.Exe.Config file 46
- analytics
 - and SQL Server Agent service 21
 - assigning SQL permissions for 26
 - configuring database locations 36
- API Web site
 - installing 29
 - introduction to 10
- ASP.NET
 - supported versions of 16
 - Temp folder permissions 20
- Authenticated Users group 20

C

- C++ 2008 SP1 Redistributable Package 18, 20
- Certificate Creation Tool 48
- ClickOnce deployment package 50, 52, 60
- ClickOnce installation package 45, 47
- client software
 - installing 45
 - modifying the configuration file for 46
 - prerequisites for 19
 - uninstalling 61
- code-signing certificate
 - obtaining 48
 - obtaining the SHA-1 thumbprint of 49, 51
- configuration database
 - and required SQL Server roles 22
 - creating 31
 - introduction to 10
- configuration options 13

creating

- Accelerator Manager service manually 55–56
- configuration database 31
- customer databases 33
- IIS virtual directory 56
- Custodian Manager
 - installing 29
 - introduction to 10
 - setting up Web site 38
- customer databases
 - and required SQL Server roles 22
 - creating 31, 33
 - introduction to 10

D

- databases
 - and required SQL Server roles 22
 - creating 31
- dbcreator role in SQL Server 22
- Discovery Accelerator API Web site
 - installing 29
 - introduction to 10
- documentation 10
- Domino items
 - exporting 18
 - viewing 20

E

- Endpoint Protection, temporarily shutting down 32, 58
- Enterprise Vault
 - Exchange Journaling Task 26
 - expanding distribution lists 26
 - supported versions of 17
- Enterprise Vault Accelerator Manager service
 - creating manually 55
 - introduction to 10
 - troubleshooting 56

F

firewall, allowing communication through 31

G

GenerateClickOnce.msbuild 50

H

"How To" articles on Support site 12

I

installing

- client software 45
- server software 29

Internet Explorer

- supported versions of 16
- Web Controls 16

Internet Information Services (IIS)

- manually creating virtual directory 56
- permissions on Temp folders 20
- supported versions of 16

L

Legal Hold

- installing license for 30

license key file 30, 33

Links To Related Software folder 16, 20

load balancing 44, 46

Lotus Domino items

- exporting 18
- viewing 20

Lotus Notes client, supported versions of 18, 20

M

Makecert.exe 48

manuals and Help files 10

Microsoft Reporting Services 42

MSBuild engine 50

msdb system database 24–26

MSI installer package 45–46

N

.NET Framework, supported versions of 18–19

Network Load Balancing (NLB) 44, 46

NIC Teaming, disabling 21

O

Outlook, supported versions of 18–19

P

per-user and per-machine installations 46

permissions on Temp folders 20

prerequisites for Discovery Accelerator 15–16, 19

product documentation 10

R

Receive-Side Scaling, disabling 21

report templates, uploading 41

S

search schedules 24

and SQL Server Agent service 21

server software

- installing 29
- prerequisites for 16

SHA-1 thumbprint, obtaining 49, 51

SQL Server

- assigning permissions and roles 22, 25–26
- prerequisites for 15
- uploading report templates to 41

SQL Server Agent service, configuring 21

SQLAgentUserRole, assigning to Vault Service account 25

Symantec Endpoint Protection, temporarily shutting down 32, 58

sysadmin role in SQL Server 22

T

TCP Chimney, disabling 21

TCP Segmentation Offloading, disabling 21

TCP/IP Offload Engine, disabling 21

TCP/IP ports 58

Temp folder permissions 20

U

User Account Control (UAC)

and Accelerator Manager Web site 32

and Discovery Accelerator installation program 30

V

Vault Service account

- adding to msdb system database 25–26
- assigning roles to on SQL reporting server 42
- assigning SQLAgentUserRole to 25
- granting permissions to 25
- SQL Server roles required for 22

Visual C++ 2008 SP1 Redistributable Package 18, 20

W

white papers 11

Windows. *See* Temp folder permissions

- allowing communication through firewall 31
- supported versions of 19