

Symantec Compliance Accelerator™

Administrator's Guide

10.0

Symantec Compliance Accelerator: Administrator's 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: 2012-08-22.

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:

<http://support.symantec.com>

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:

<http://support.symantec.com>

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:

<http://support.symantec.com>

Customer service

Customer service information is available at the following URL:

<http://support.symantec.com>

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 Compliance Accelerator 13
	Key features of Compliance Accelerator 13
	About the Compliance Accelerator components 14
	The Compliance Accelerator process 15
	About the deduplication feature in Compliance Accelerator 17
	Product documentation 17
	White papers on the Symantec Enterprise Support site 18
	"How To" articles on the Symantec Enterprise Support site 18
	Comment on the documentation 18
Chapter 2	Introducing the Compliance Accelerator client 21
	About the Compliance Accelerator client 21
	Opening and closing the Compliance Accelerator client 21
	Finding your way around the Compliance Accelerator client 23
Chapter 3	Setting up employees and employee groups 27
	About employees and employee groups 27
	Creating employee profiles 28
	Mapping employee properties to Active Directory or Domino directory attributes 30
	Editing the details of employees 32
	Creating employee groups 32
	Assigning roles to employees 36
	About the predefined Compliance Accelerator roles 36
	About the Compliance Accelerator permissions 40
	Creating Compliance Accelerator roles 44
	Assigning Compliance Accelerator roles to employees or groups 46
Chapter 4	Working with departments 49
	About departments 49
	Creating departments 50

Adding monitored employees and groups to departments	55
Editing the monitoring policy for employees and groups	56
Moving employees or groups between departments	58
Moving departments	58
Assigning department reviewers, compliance supervisors, and delegates	59
Implementing Chinese Walls security	61
Enabling Chinese Walls	62
Managing Department Users	62
Managing exception employees	63
Designating employees as exceptions	64
Assigning further exception reviewers to an exception	64
Moving an exception employee to another department	65
Removing exception status	66
Removing exception reviewers	67
Grouping departments into partitions	67
Creating department partitions	67
Using attributes to classify departments	68
Setting up department attributes	69
Assigning attributes to departments	70

Chapter 5

Searching for items	73
About searching with Compliance Accelerator	73
Creating and running Compliance Accelerator searches	74
About the search criteria options	76
Guidelines on conducting effective searches	85
Pausing and resuming Compliance Accelerator searches	86
About the Monitor Searches tab	86
Searching the items of exception employees	88
Selecting the archives in which to search	89
Building Compliance Accelerator search schedules	91
Setting up new search schedules	92
Examples of recurring search schedules	93
Defining hotwords to search for	94
Adding hotwords	94
Editing existing hotwords	96
Deleting hotwords	97
Adding hotword sets	97
Editing existing hotword sets	98
Deleting hotword sets	99
Importing the predefined hotwords	99

	Configuring how Compliance Accelerator handles email addresses	100
Chapter 6	Manually reviewing items	103
	About reviewing with Compliance Accelerator	103
	About the Review pane	104
	Filtering the items in the Review pane	108
	Assigning review marks to items	112
	Adding comments to items	113
	Viewing the history of items	113
	Displaying printable versions of items	114
	Downloading the original versions of items	114
	Copying the item list to the Clipboard	115
	Changing how the Review pane looks	115
	Setting your Review pane preferences	116
	Escalating items	118
	Assigning escalated items to other escalation reviewers	119
	Closing escalated items	119
	Storing reviewing comments for reuse	120
Chapter 7	Working with research folders	123
	About research folders	123
	Creating research folders	124
	Copying items to research folders	125
	Reviewing the items in research folders	125
	Exporting items from research folders	126
	Giving other users access to your research folders	127
	Committing research folder items to the department review set	127
Chapter 8	Exporting items	129
	About exporting items	129
	Performing an export run	129
	About the limits on the number of simultaneous export runs	133
	How to optimize export runs	133
	Exporting items from the review set of an exception employee	134
	Making the export IDs visible in Microsoft Outlook	134
Chapter 9	Creating and viewing reports	137
	About the Compliance Accelerator reports	137
	Creating Compliance Accelerator reports	137
	Available Compliance Accelerator reports	138

- Compliance Supervisor Responsibility report 140
- Department Roles Detail report 140
- Department Roles Summary report 141
- Differential Sampling Summary by Department report 142
- Effective Roles by User report 143
- Evidence of *message type* Review by Department/Employee reports 143
- Item Aging by Department report 144
- Message Stats Summary report 144
- Message Summary report 145
- Monitored IDs by Department report 145
- Questioned Items by Department report 146
- Responsibility by Department report 146
- Responsibility by Reviewer report 147
- Review Activity Summary by Department report 147
- Reviewer Activity by Department report 148
- Reviewer Activity Detail report 148
- Reviewer Mapping report 149
- Unreviewed Departments report 150
- Unsupervised Departments report 150
- Viewing existing reports 151
- Deleting reports 151
- Viewing legacy reports in Crystal Reports format 152

- Appendix A Customizing Compliance Accelerator 153
 - Specifying the Windows domains with which to synchronize employee details 153
 - Customizing the reviewing action statuses 155
 - Setting Compliance Accelerator system configuration options 156
 - Ad Hoc Searches configuration options 158
 - Diagnostics configuration options 159
 - Document Conversion configuration options 160
 - Export/production configuration options 160
 - General configuration options 164
 - Home Page configuration options 166
 - Item Prefetch Cache configuration options 167
 - Item Prefetch Cache (Advanced) configuration options 170
 - Policy Integration configuration options 172
 - Profile Synchronization configuration options 175
 - Random Capture configuration options 176
 - Reviewing configuration options 179
 - Search configuration options 182

	Security configuration options	187
	System configuration options	188
	Vault Directory Synchronization configuration options	189
	Customizing the columns in the Review pane	191
Appendix B	Importing configuration data from an XML file	195
	About importing configuration data	195
	Sample XML files	195
	Format of the Dataload.xml file	196
	Importing the configuration data	197
	About the ImportExport command	198
	ImportExport syntax	199
	Examples of ImportExport commands	200
Appendix C	Troubleshooting	203
	Vault stores not displayed	203
	Incorrect results when searching by message type and direction in archives that Enterprise Vault 4.0 or earlier has indexed	204
	Search returns unexpected results	204
	Errors when exporting items	205
	Synchronization errors after you rename the SQL Server computer	207
	Performance counter errors when the Accelerator Manager service starts	207
	Journaling Connector problems when you do not specify the vault IDs for multiple customers	208
	Enterprise Vault deduplication process does not work as expected in Exchange 2007 environments	208
	SQL Service Broker warning when restoring a customer database to a different server	209
	Issues with reports	209
	Compliance Accelerator reports may not work correctly until you install the Support for Crystal Reports Web site	209
	You receive the message "An error occurred creating the report" when you try to generate reports	210
	Prompt to install SQL Server when printing a report for the first time	210
	Scripts errors when printing reports from the Compliance Accelerator client in SQL Server 2005 SP2 environments	211
	Reports that you export as CSV may not open properly in Microsoft Excel	211

Garbled Japanese characters when exporting reports in Acrobat format	212
Index	213

Introducing Compliance Accelerator

This chapter includes the following topics:

- [Key features of Compliance Accelerator](#)
- [About the Compliance Accelerator components](#)
- [The Compliance Accelerator process](#)
- [About the deduplication feature in Compliance Accelerator](#)
- [Product documentation](#)

Key features of Compliance Accelerator

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

Among the key features of Compliance Accelerator are the following:

- A system for defining the employees that are to be monitored and grouping them in an organizational structure that reflects the departments within the company. The messages of selected *exception* employees can be kept separate and reviewed by specially assigned reviewers.
- An optional Journaling Connector component that takes a random sample of the items that have been sent to the Enterprise Vault archive of a journal mailbox.
- A client application that lets administrators configure Compliance Accelerator and designated reviewers read and mark the captured items.

- A secure SQL database that keeps information on all the monitored employees, captured items, and the review process that you have applied to the items.

About the Compliance Accelerator components

Table 1-1 lists the primary Compliance Accelerator components.

Table 1-1 The Compliance Accelerator components

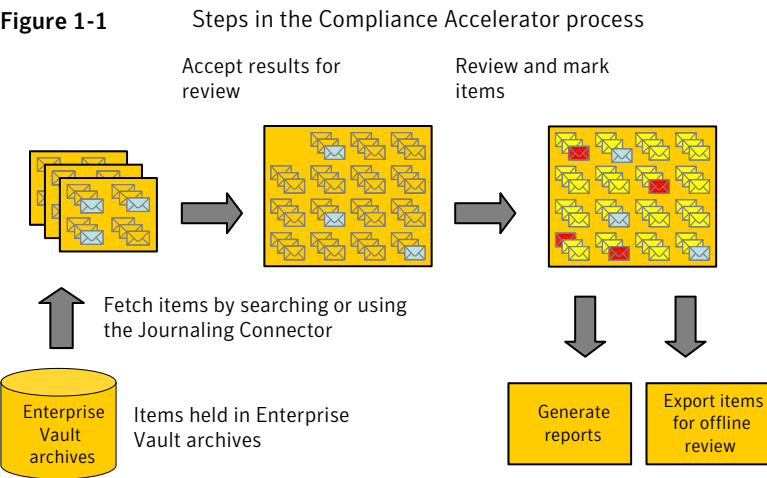
Component	Notes
Compliance Accelerator client	<p>The client is used by Compliance Accelerator administrators to set up and manage the system and by reviewers to access the items that they are to mark.</p> <p>See “About the Compliance Accelerator client” on page 21.</p>
Accelerator Manager Web site	<p>This Web site lets you set up multiple Compliance Accelerator databases in which to store your data.</p>
Enterprise Vault Accelerator Manager service	<p>This service handles the requests from the Compliance Accelerator client and works with the Enterprise Vault components to access archives, perform searches, and so on.</p>
Customer database	<p>The customer database is a SQL database in which Compliance Accelerator stores details of departments, user roles, search results, and more.</p> <p>You can set up multiple customer databases.</p>
Configuration database	<p>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.</p>
Support for Crystal Reports Web site (optional)	<p>This Web site lets you view any legacy reports in Crystal Reports (.rpt) format that you created with Compliance Accelerator 2007 or earlier. In version 10.0 of Compliance Accelerator, the reporting facilities employ Microsoft SQL Server Reporting Services rather than Crystal Reports.</p>

Table 1-1 The Compliance Accelerator components (continued)

Component	Notes
Journaling Connector (optional)	<p>The Journaling Connector collects a random sample of items that have been sent to the Enterprise Vault archive of a Microsoft Exchange or Lotus Domino journal mailbox. If you need to review a certain percentage of each employee’s communications every day, the Journaling Connector is the best way to fulfill the requirement. At a set time, Compliance Accelerator adds the items during the previous 24 hours to the items to be reviewed for a department. You can specify the percentage of each employee’s communications that you want to capture.</p> <p>Compliance Accelerator provides one Journaling Connector for Microsoft Exchange environments and another for Lotus Domino environments.</p> <p>Note: Compliance Accelerator does not deduplicate randomly-sampled items.</p>

The Compliance Accelerator process

Figure 1-1 provides an overview of the steps in the compliance process.



You typically perform the steps in the Compliance Accelerator process in the following order:

- Create an employee profile for every user who is to access Compliance Accelerator as an administrator, supervisor, or reviewer. You must also create a profile for every employee whose communications you want to monitor. You can enter a few employee details and then populate the rest by synchronizing with the corresponding Active Directory or Domino directory account.
- Assign roles to those users or groups of users who are to perform administrative tasks in Compliance Accelerator.

In a default Compliance Accelerator system, there are a number of predefined application and department roles. You can modify most of these as necessary, and you can create new roles. Each role has a number of permissions that are associated with it. Application roles let users perform system-wide tasks, whereas department roles let them perform certain tasks within a specific department only.
- Select the archives that you want to make available to all departments for searches. If necessary, department administrators can further customize this set of archives in their departments.
- Create one or more departments.
- In each department, do the following:
 - Assign roles to other users so that they can perform administrative, supervisor, and reviewer tasks in the department.
 - Add employees to the departments in which they are to be monitored.
 - If required, customize the archives that you want to include in your department searches.

Compliance Accelerator is now ready to monitor employees and add items to the department review sets for reviewers to work on.

- In each department review set, review each item and add a review status mark and comment, as appropriate.
- If you want to review items offline or send them to a third party, export them in a suitable format. The export formats include PST, Domino NSF database, HTML, and MSG.
- Use the reporting facilities to generate reports on various aspects of Compliance Accelerator, including the progress of reviewers and their roles and responsibilities.

About the deduplication feature in Compliance Accelerator

Compliance Accelerator provides a deduplication feature. The purpose of this feature is to identify and remove duplicate items from the results of a search, and so prevent them from appearing in the review set. To determine whether one item is a duplicate of another, Compliance Accelerator compares the metadata properties of the items, such as their author display names, subjects, and number of attachments. Note that the deduplication works within individual searches only; it does not span multiple searches, even when you run them within the same department.

For all types of searches (immediate, scheduled, and guaranteed sample), Compliance Accelerator deduplicates the items as part of the sampling process. For guaranteed sample searches, Compliance Accelerator adds randomly-sampled items to the review set to compensate for any shortfall that the deduplication process has caused.

Product documentation

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

Table 1-2 The Compliance Accelerator documentation set

Document	Comments
Installation Guide	Outlines how to perform a first-time installation of the Compliance Accelerator server and client software.
Upgrade Instructions	Explains how to upgrade an existing installation of Compliance Accelerator to version 10.0.
Administrator's Guide	Provides information for Compliance Accelerator administrators on how to set up and assign roles, search for items to include in the review set, export items for offline review, create reports, and more.
Reviewer's Guide	Describes the features of the Compliance Accelerator client that are available to reviewers.
Online Help	Accompanies all the Compliance Accelerator applications and provides extensive information on how to use their facilities.

Table 1-2 The Compliance Accelerator documentation set (*continued*)

Document	Comments
Release Notes	Provides late-breaking information that you may need to be aware of before you install and use Compliance Accelerator.

White papers on the Symantec Enterprise Support site

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

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

Although intended for Discovery Accelerator users, the *Effective Searching* white paper provides information that you may find useful when you conduct searches with Compliance Accelerator. This white paper is available from the following page of the Symantec Enterprise Support site:

<http://www.symantec.com/docs/HOWTO77131>

"How To" articles on the Symantec Enterprise Support site

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

Comment on the documentation

Let us know what you like and dislike about the documentation. Were you able to find the information you needed quickly? Was the information clearly presented?

Report errors and omissions, or tell us what you would find useful in future versions of our guides and online help.

Please include the following information with your comment:

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

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

We appreciate your feedback.

Introducing the Compliance Accelerator client

This chapter includes the following topics:

- [About the Compliance Accelerator client](#)
- [Opening and closing the Compliance Accelerator client](#)
- [Finding your way around the Compliance Accelerator client](#)

About the Compliance Accelerator client

The client is a feature-rich Windows application with which Compliance Accelerator users can add marks and comments to the items that they review. In addition, administrators can use the Compliance Accelerator client to administer and customize the application. The role to which a Compliance Accelerator user has been assigned determines the features of the client that each user can access.

You perform most of the activities that are described in this guide with the Compliance Accelerator client.

Opening and closing the Compliance Accelerator client

If you add a shortcut to the Compliance Accelerator client to the Windows desktop, you can open the client by double-clicking the shortcut. Alternatively, you can open the program by clicking the program name in the Windows **Start** menu.

To open the Compliance Accelerator client

- 1
- On the Windows **Start** menu, click the shortcut for the Compliance Accelerator client.

After a few moments, the **Select a Compliance Accelerator instance to connect to** dialog box appears.

- 2
- In the **Server** box, type the name or IP address of the computer on which the Compliance Accelerator server software is running.

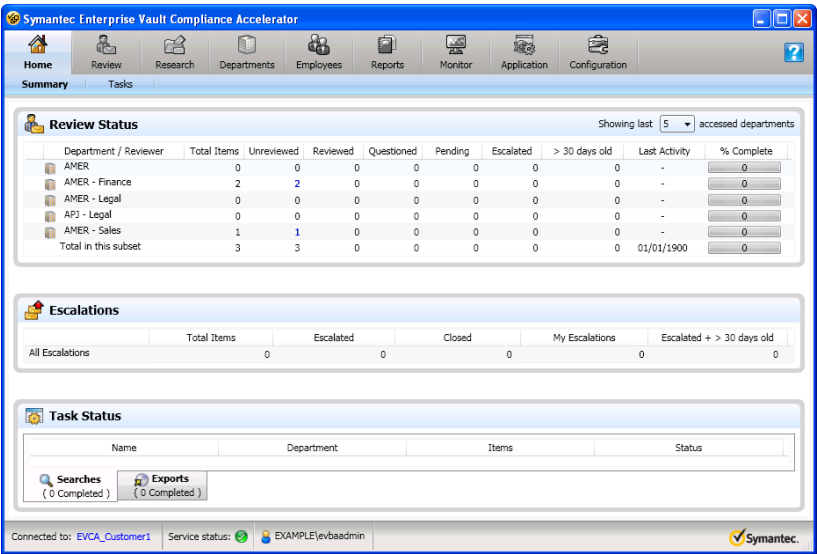
You can type the IP address in either IPv4 or IPv6 format.

- 3
- In the **Instance** box, select the Compliance Accelerator instance (customer database) that you want to access. Click the down arrow at the right of the box to list the available instances.

Each instance stores the details of a set of departments that you want to review. It also stores the associated user roles, search results, research folders, and more. Therefore, you may have multiple instances from which to choose.

- 4
- Uncheck **Ask every time the application is opened** if you always want to connect to the same instance without first displaying the **Select a Compliance Accelerator instance to connect to** dialog box.
- 5
- Click **Connect**.

After a few moments, the home page of Compliance Accelerator client appears.



To close the Compliance Accelerator client

- ◆ Click the close button in the upper-right corner of the window.

Finding your way around the Compliance Accelerator client

In the Compliance Accelerator client, the roles to which you have been assigned determine the features that you can access. [Table 2-1](#) describes the features that users with the most permissive roles can access. Compliance Accelerator administrators can assign multiple different roles to users and change the permissions that are associated with the roles.

Table 2-1 Primary tabs in the Compliance Accelerator client







Icon	Tab	Description
	Home	This tab provides a headline view of the status of the activities that you perform in Compliance Accelerator. It also gives you quick access to the activities that you are likely to perform frequently with Compliance Accelerator.
	Review	This tab lets you view the items in the review set and assign marks and comments to them.
	Research	This tab lets you set up research folders where you can work privately on the items that interest you without generating additional work for other Compliance Accelerator reviewers.
	Departments	This tab lets you manage your Compliance Accelerator departments, the employees who belong to them, and the supervisors and reviewers who are assigned to them.
	Employees	This tab lets you view and change the employee profiles in your Compliance Accelerator system, and enter the details of new ones. You must set up a profile for everyone who will run Compliance Accelerator—administrators and reviewers—and everyone whose communications will be monitored.
	Reports	This tab lets you generate reports on various aspects of Compliance Accelerator, including the progress of reviewers and their roles and responsibilities.

Table 2-1 Primary tabs in the Compliance Accelerator client *(continued)*




Icon	Tab	Description
	Monitor	This tab lets you monitor the status of all Compliance Accelerator searches and pause or resubmit them as necessary.
	Application	<p>This tab provides access to a range of commonly used administrative facilities. The options that are available when you click this tab may include the following:</p> <ul style="list-style-type: none">■ Searches. Create searches that run in multiple departments.■ Roles. Set up and amend the roles that you can assign to users to manage their access to Compliance Accelerator facilities.■ Role Assignment. Assign Compliance Accelerator roles to users.■ Reviewing Comments. Store the text of common comments that Compliance Accelerator reviewers can apply to the items on which they work.■ Hotwords. Set up lists of important words for which you may want to search with Compliance Accelerator.■ Archives. Customize the list of Enterprise Vault archives in which Compliance Accelerator searches for items.

Table 2-1 Primary tabs in the Compliance Accelerator client (*continued*)

Icon	Tab	Description
	Configuration	<p>This tab provides access to a range of configuration facilities that you are likely to use infrequently. The options that are available when you click this tab may include the following:</p> <ul style="list-style-type: none"> ■ Search schedules. Set up schedules with which you can run Compliance Accelerator searches repeatedly, at scheduled times. ■ Reviewing Statuses. Customize the status names with which Compliance Accelerator shows the status of items in the Review pane (Pending, Questioned, Reviewed, and so on). ■ Import Configuration. Import configuration data into Compliance Accelerator from an XML file. ■ Account Information. Specify multiple Windows domains with which Compliance Accelerator should synchronize the details of employees and employee groups. ■ Directory Mappings. Configure how Compliance Accelerator synchronizes employee properties with an external source like Active Directory. ■ Department Partitions. Group departments into partitions to restrict the scope of searches. ■ Department Attributes. Set up attributes with which you can categorize your departments. ■ Settings. Set hundreds of configuration options with which you can customize the appearance and performance of Compliance Accelerator.

Setting up employees and employee groups

This chapter includes the following topics:

- [About employees and employee groups](#)
- [Creating employee profiles](#)
- [Mapping employee properties to Active Directory or Domino directory attributes](#)
- [Editing the details of employees](#)
- [Creating employee groups](#)
- [Assigning roles to employees](#)

About employees and employee groups

Compliance Accelerator provides a system for defining the employees that you want to monitor and grouping them in a structure that reflects the departments in your company. All employees require a Compliance Accelerator profile. Each employee profile comprises a number of properties, some of which correspond to Active Directory or Domino directory attributes. When configuring an employee profile, you can choose whether Compliance Accelerator should automatically synchronize these properties with the corresponding directory account information.

The quickest way to add a large number of employee profiles to Compliance Accelerator is to create an employee group. Then you can synchronize this group with the user account information held in Active Directory or a Domino directory, or a Windows or Domino group.

The roles that you assign to employees determine what they can access and the tasks that they can perform in Compliance Accelerator.

The messages of certain employees such as senior managers can be kept separate and reviewed by specially assigned reviewers. In the terminology of Compliance Accelerator, such employees are *exception employees*.

Creating employee profiles

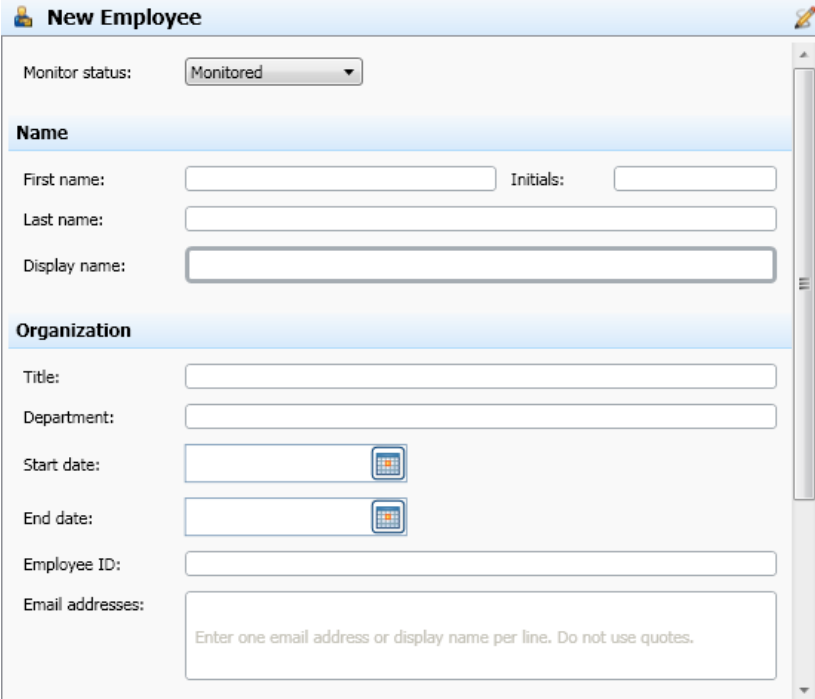
You must have the Manage Employees permission to set up an employee profile. By default, users with the application role of App User Admin have this permission.

See [“About the Compliance Accelerator permissions”](#) on page 40.

To create an employee profile

- 1 Click the **Employees** tab in the Compliance Accelerator client.
- 2 Click **New Employee** at the top of the window.

The New Employee pane appears.



New Employee

Monitor status: Monitored

Name

First name: Initials:


Last name:


Display name:

Organization

Title:

Department:

Start date: 

End date: 

Employee ID:

Email addresses:

Enter one email address or display name per line. Do not use quotes.

- 3 In the right pane, type the employee's first name, initials, and last name, and the display name with which the employee appears in Compliance Accelerator.
 Only the display name is mandatory. If the Windows account of the employee is held in Active Directory or a Domino LDAP directory, you can populate the other boxes by synchronizing Compliance Accelerator with it.
- 4 In the **Organization** section, type the company details for the employee. Complete the boxes as follows:

Title	Specifies the employee's job title.
Department	Identifies the employee's department within the organization. This department is not the Compliance Accelerator department to which the employee is to belong.
Start date	Your company policy should specify how this box is used. For example, the start date can indicate when the employee joined the company or when the employee was first monitored. By default, today's date appears in the box. To change this date, click the down arrow at the right of the box and then select the required date.
End date	As with the start date, your company policy should specify how this box is used. For example, the end date can indicate when the employee left the company. This date is important for preserving accurate system information.
Employee ID	<p>If your company's administration or finance department issues each employee with a unique company ID, you can enter it here. If you update employee data using an XML file, the Employee ID box must have a unique value. This value is used to identify the employee profile to update.</p> <p>See “About importing configuration data” on page 195.</p>
Email addresses	<p>Specifies the email addresses that belong to the employee. If the employee has multiple addresses, type each one on a line of its own.</p> <p>If you search for the items that were sent to or from this employee, Compliance Accelerator includes all the listed addresses in the search. To ensure that you capture all the relevant items, remember to add old email addresses.</p>

You can populate the **Title** and **Department** properties using synchronization if you hold user accounts in Active Directory or a Domino directory. You can also populate the **Start date**, **End date**, and **Employee ID** properties using

synchronization. However, you must first map these properties to suitable Active Directory or Domino directory attributes.

See “[Mapping employee properties to Active Directory or Domino directory attributes](#)” on page 30.

- 5
- In the **Windows Account** and **Domino Account** sections, enter the user name of the employee. Alternatively, click **Browse** to display a list of accounts, and then select the one for this employee.
- 6
- Check **Automatically synchronize** if you want Compliance Accelerator regularly to synchronize the employee profile properties with values in the associated Windows or Domino user account.

You must uncheck this option if you want to edit the profile manually after synchronization.

Note: If you want to conduct Compliance Accelerator searches for a synchronized Domino user, you must ensure that the user has an SMTP address defined in the Domino directory.

- 7
- Click **Save**.

Mapping employee properties to Active Directory or Domino directory attributes

Each employee profile in Compliance Accelerator comprises a number of properties, some of which correspond to Active Directory or Domino directory attributes.

[Table 3-1](#) lists the employee properties that Compliance Accelerator maps to the directory attributes by default.

Table 3-1

How employee properties map to Active Directory or Domino directory attributes

Employee property	Active Directory attribute	Domino directory attribute
Department	department	department
Display Name	displayName	cn
First Name	givenName	Givenname
Middle Name	initials	middleinitial

Table 3-1 How employee properties map to Active Directory or Domino directory attributes *(continued)*

Employee property	Active Directory attribute	Domino directory attribute
Surname	sn	sn
Title	title	Personaltitle

When configuring an employee profile, you can choose whether Compliance Accelerator should automatically synchronize these properties with the corresponding attributes.

You can also set up mappings for the following optional properties: Start Date, End Date, and Employee ID. The Employee ID property is mandatory if you want to import department and employee data by using XML files.

See [“About importing configuration data”](#) on page 195.

You must have the View System Configuration permission to view the existing mappings, and the Modify System Configuration permission to change them. By default, users with the role of Compliance System Admin have both permissions.

To view and modify an existing directory mapping

- 1 Click the **Configuration** tab in the Compliance Accelerator client, and then click the **Directory Mappings** tab.
- 2 In the left pane, click the employee property whose mapping you want to modify.
- 3 In the right pane, choose whether to synchronize the employee property with Active Directory, Domino directory, or both.

Active Directory Synchronisation

Synchronise from Active Directory ☒

Active Directory Attribute Name

Domino Synchronisation

Synchronise from Domino ☒

Domino Attribute Name

Preferred Source

Select the preferred source for this attribute if it is being synchronised from both Active Directory and Domino.

Preferred Source

- 4 Type the names of the Active Directory and Domino directory attributes with which to synchronize the employee property.
- 5 If you want to synchronize with both Active Directory and Domino directory, nominate one of them as the preferred source.
- 6 Click **Save**.
- 7 Restart the Enterprise Vault Accelerator Manager service on the Compliance Accelerator server to put the new mapping or changed mapping into effect.

Editing the details of employees

You can edit each employee's details to change the email addresses with which the employee is associated, amend the monitoring policy, and more.

You must have the Assign % Review permission to edit the monitoring policy for an employee. By default, users with the department role of Rule Admin have this permission.

To edit the details of an employee

- 1 Click the **Employees** tab in the Compliance Accelerator client.
- 2 In the left pane, click the name of the employee whose details you want to edit.

If Compliance Accelerator lists a lot of employees and groups, you can filter the list with the fields at the top of the pane. As well as filtering the employees and groups by name and type, you can filter them by their monitoring status and employment status.

- 3 In the right pane, change the details of the employee as necessary.
- 4 Click **Save**.

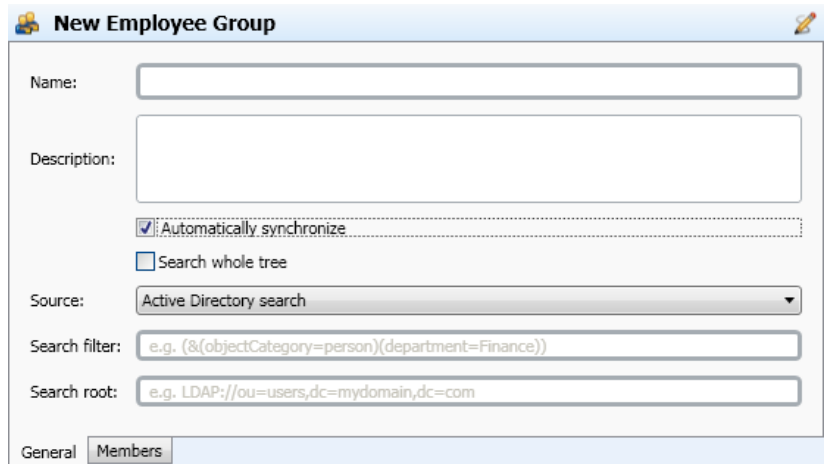
Creating employee groups

You must have the Manage Employees permission to set up an employee group. By default, users with the role of App User Admin have this permission.

To create an employee group

- 1 Click the **Employees** tab in the Compliance Accelerator client.
- 2 Click **New Employee Group** at the top of the window.

The New Employee Group pane appears.



New Employee Group

Name:

Description:

☒ Automatically synchronize

☐ Search whole tree

Source:

Search filter:

Search root:

General Members

- 3 Type the name of the group and a brief description.
- 4 If you want to synchronize the group with the user account information held in an external source like Active Directory, check **Automatically synchronize**. Then type the required details.

The options are as follows:

Active Directory search, or Domino
LDAP search

Lets you specify the appropriate search filter and search root. If the target employees are in various parts of your organization, their user accounts may be in different areas of the directory. By using a search with one or more search filters, you can find and automatically add these users.

An LDAP search filter can be based on any number of custom or standard attributes, but it must target user objects. You can combine multiple filters to find the members for a department. For example, you can enter the following to find all users whose department attribute is set to UK Equities:

(&(objectCategory=person)(department=UK Equities))

In the Search Root box, type the Distinguished Name for the search root. This name identifies where in the directory hierarchy to start the search. For example, if your directory spans multiple countries, you can set the root to the UK organizational unit by entering the following:

LDAP://OU=UK,DC=MyCompany,DC=com

Check **Search whole tree** to include the members of nested groups.

Active Directory container

Lets you type the name of the Active Directory container.

In the ADsPath box, type the Distinguished Name of the Active Directory container that holds the users to add to the employee group. For example, suppose that the UK Equities department points to this organizational unit container:

CN=Equities, OU=UK, DC=MyCompany, DC=com

You can enter the following to add all the employees in the department to the group:

LDAP://CN=Equities, OU=UK, DC=MyCompany, DC=com

Check **Search nested containers** to include the members of nested containers.

Windows group or distribution list, or Domino group or distribution list

Lets you type the name of a group in the form *domain_name\group_name*. The group may or may not be held in your directory. If you do not use Active Directory or a Domino directory, you can only update the display name of employee profiles by synchronizing. You need to enter additional employee information manually.

If you want to synchronize the employee group with a Domino group or distribution list, you must enable the following Domino LDAP attributes for anonymous access in Lotus Domino Administrator:

- cn
- dominocertificate
- mail
- maildomain
- member
- objectclass

See the Lotus Domino documentation for instructions on how to do this.

By default, Compliance Accelerator synchronizes employees and groups every four hours and every time that the Enterprise Vault Accelerator Manager service starts. However, you can change this setting.

See [“Setting Compliance Accelerator system configuration options”](#) on page 156.

- 5 If you want to add employees to the group manually, click the **Members** tab and then click **Add**. Then select the employees from the list.

You can select multiple adjacent employees by holding down the Shift key while clicking the first and last employee in the range. To select multiple nonadjacent employees, hold down the Ctrl key while clicking the required employees. Click **OK** when you have finished.

- 6 Click **Save**.

Assigning roles to employees

You assign roles to employees or employee groups to determine what they can access and the tasks that they can perform in Compliance Accelerator. For example, you can assign the role of department reviewer to an employee who needs to review and mark items in a department. Some roles are effective at the application level, across the entire Compliance Accelerator system, whereas others apply at the department level or folder level only.

Compliance Accelerator also allows for another level of compliance administration: the Compliance Supervisor role. Users with this role can appraise the work of department reviewers and manage exception employees in the department.

A standard Compliance Accelerator system comes with a number of predefined roles, but, if none precisely meets your requirements, you can create your own. You can also delete some of the predefined roles if you have no use for them.

About the predefined Compliance Accelerator roles

The predefined Compliance Accelerator roles fall into the following categories:

- Application roles, which apply at the Compliance Accelerator system level.
- Department roles, which apply to a particular department only.
- Folder roles, which apply to a particular research folder only.

Table 3-2 Application roles

Role	Description	Default permissions
App Rule Admin	This role lets you set up search schedules, create searches across departments, and manage global hotwords and reviewing comments.	<ul style="list-style-type: none"> ■ Add Hotwords. ■ Application Search. ■ Manage Reviewing Comments. ■ Manage Schedules. ■ Modify & Delete Hotwords.
App User Admin	This role lets you add users to the Compliance Accelerator system, create and manage departments, assign application roles, and create delegate users.	<ul style="list-style-type: none"> ■ Create Departments. ■ Grant Users Access. ■ Manage Delegates. ■ Manage Department Partitions. ■ Manage Department Users. ■ Manage Employees. ■ Manage Roles.
Compliance System Admin	This role lets you import configuration data into Compliance Accelerator from an XML file. Also, you can view and modify Active Directory and Domino directory attribute mappings and monitor the progress of searches.	<ul style="list-style-type: none"> ■ Export Configuration Data. ■ Import Configuration Data. ■ Modify System Configuration. ■ Monitor Search. ■ View System Configuration.

Table 3-3 Department roles

Role	Description	Default permissions
Compliance Supervisor	This role lets you use the appraisal features to check the work of department reviewers and manage exception employees in the department. You can also store items in personal folders for further research.	<ul style="list-style-type: none"> ■ Add Own Review Comments. ■ Apply Appraisal Status. ■ Apply Bulk Review Action. ■ Apply Review Action. ■ Export Messages. ■ Manage Exceptions. ■ Perform Ad Hoc Searches. ■ Review Messages. ■ View Reports.

Table 3-3 Department roles (*continued*)

Role	Description	Default permissions
Department Reviewer	This role lets you review items and mark items within the department, export items, and generate and view reports. You can also store items in personal folders for further research.	<ul style="list-style-type: none"> ■ Add Own Review Comments. ■ Apply Bulk Review Action. ■ Apply Review Action. ■ Escalate Messages. ■ Export Messages. ■ Perform Ad Hoc Searches. ■ Review Messages. ■ View Reports.
Department User	In a Compliance Accelerator environment where you have implemented Chinese Walls security, this role permits the selected user to be assigned to other roles in the department or in the research folders that are associated with the department.	—
Escalation Reviewer	This role lets you receive the items that other reviewers in the department have escalated to a higher authority for further review. Departments lower in the hierarchy inherit this role, so an escalation reviewer automatically has access to nested departments.	<ul style="list-style-type: none"> ■ Apply Bulk Actions to Escalations. ■ Apply Comments to Escalations. ■ Apply Review Action to Escalations. ■ Change Escalation Status. ■ Export Escalations. ■ Review Escalations.
Exception Reviewer	This role lets you search the items of exception employees to whom you are assigned. You can also review and mark the items, export them, and generate and view reports. You can also store items in personal folders for further research.	<ul style="list-style-type: none"> ■ Add Own Review Comments. ■ Apply Bulk Review Action. ■ Apply Review Action. ■ Escalate Messages. ■ Export Messages. ■ Perform Ad Hoc Searches. ■ Review Messages. ■ Search Capture. ■ View Reports.

Table 3-3 Department roles (*continued*)

Role	Description	Default permissions
Passive Reviewer	This role let you view items and export items from the department. You can also generate and view reports, and use the appraisal features to check and mark the work of department reviewers. You cannot apply review status marks to items.	<ul style="list-style-type: none"> ■ Apply Appraisal Status. ■ Export Messages. ■ Review Messages. ■ View Reports
Rule Admin	This role lets you create searches within the department and manage department hotwords. You can also configure the monitoring policy that is assigned to employees and generate and view reports. In addition, you can assign exception reviewers to specific employees.	<ul style="list-style-type: none"> ■ Add Hotwords. ■ Assign % Review Requirement. ■ Manage Exceptions. ■ Modify & Delete Hotwords. ■ Search Capture. ■ View Reports.
User Admin	<p>This role lets you manage the properties of the department and of monitored employees. You can also assign department roles to users, generate and view reports on department details, and review progress.</p> <p>In addition, you can manage the personal folders in which users have stored items for further research.</p>	<ul style="list-style-type: none"> ■ Add Monitored Employees. ■ Configure Department Properties. ■ Grant Users Access. ■ Manage Exceptions. ■ View Reports.

Table 3-4 Folder roles

Role	Description	Default permissions
Capture Messages	This role lets you search for new items to add to a research folder.	<ul style="list-style-type: none"> ■ Search Capture.
Commit Messages	This role lets you commit items in a research folder to the department review set for all other department reviewers to see.	<ul style="list-style-type: none"> ■ Commit Appraised Folder Messages. ■ Commit Reviewed Folder Messages.

Table 3-4 Folder roles (continued)

Role	Description	Default permissions
Export	This role lets you export items from a research folder for offline review.	<ul style="list-style-type: none">■ Export Messages.
Full Control	<p>This role lets you search for new items to add to a research folder, and review and mark the items. You can also export the items for offline review and commit them to the department review set.</p> <p>You can also give other users access to your folder so that they can participate in the review process.</p>	<ul style="list-style-type: none">■ Add Own Review Comments.■ Apply Appraisal Status.■ Apply Bulk Review Action.■ Apply Review Action.■ Commit Appraised Folder Messages.■ Commit Reviewed Folder Messages.■ Configure Folder Properties.■ Delete Folder.■ Escalate Messages.■ Export Messages.■ Grant Users Access.■ Review Messages.■ Search Capture.■ View Reports.
Review	This role lets you review items and mark items in a folder.	<ul style="list-style-type: none">■ Add Own Review Comments.■ Apply Appraisal Status.■ Apply Bulk Review Action.■ Apply Review Action.■ Escalate Messages.■ Review Messages.

About the Compliance Accelerator permissions

The following tables provide more information on the permissions that you can associate with user roles.

Table 3-5 Application permissions

Permission	Description
Add Hotwords	Add hotwords to the global hotword list.
Application Search	Create application-wide searches to run in multiple departments.

Table 3-5 Application permissions (*continued*)

Permission	Description
Create Departments	Add new departments and assign an owner, and modify the properties of existing departments.
Delete Department	Delete the selected departments and all the objects that are associated with them (department-specific searches, user folders, hotwords, and so on).
Export Configuration Data	Use the ImportExport command-line utility to export configuration data from the Compliance Accelerator database to an XML file.
Grant Users Access	Assign application roles to employees.
Import Configuration Data	Import configuration data that is held in XML files, and view the import log.
Manage Delegates	Permit employees to act as proxies for department administrators, application administrators, or reviewers.
Manage Department Partitions	Add and remove partitions, and select the departments to include in each partition.
Manage Department Users	In a Compliance Accelerator environment where you have implemented Chinese Walls security, assign the Department User role to users. This role makes the users available for selection when you assign other departmental roles.
Manage Employees	Add new employee profiles, and populate and modify profiles. You can also add new employee groups, edit group membership and properties, and delete employee groups.
Manage Reviewing Comments	Add, modify, and delete the predefined comments that reviewers can choose to apply to items.
Manage Roles	Add and remove roles, and select the permissions to assign to each role.
Manage Schedules	Create and change schedules for searches.
Modify & Delete Hotwords	Change and remove global hotwords.

Table 3-5 Application permissions (*continued*)

Permission	Description
Modify System Configuration	Change the mapping between Active Directory or Domino directory attributes and Compliance Accelerator employee properties. You can also change the review status marks available to reviewers, and change the archives available to all departments.
Monitor Search	Monitor the status of searches across all departments and pause and resubmit searches, even if you do not normally have access to the associated departments. However, you cannot view the search criteria or the results of the searches unless you normally have access permission.
View System Configuration	View the mapping between Active Directory or Domino directory attributes and Compliance Accelerator employee properties. You can also view the review status marks available to reviewers, and view the archives available to all departments.

Table 3-6 Department permissions

Permission	Description
Add Hotwords	Add hotwords that are visible in the selected department only.
Add Monitored Employees	Assign existing employees to the department.
Add Own Review Comments	Apply comments to items by typing your own free-form comments.
Add Standard Review Comments	Apply comments to items by selecting from a predefined set of comments. This permission does not let you enter free-form comments.
Apply Appraisal Status	Use the appraisal features to check and mark the work of department reviewers.
Apply Bulk Review Action	Apply an action status mark to more than one item at a time.

Table 3-6 Department permissions (*continued*)

Permission	Description
Apply Bulk Actions To Escalations	Apply an action status mark to more than one escalated item at a time.
Apply Comments To Escalations	Apply a comment to an escalated item.
Apply Review Action	Apply an action status mark to the items in a review set.
Apply Review Action To Escalations	Apply an action status mark to an escalated item.
Assign % Review Requirement	Assign a monitoring policy sample size to a department and to specific groups and employees in the department.
Change Escalation Status	Close escalated items and re-assign them to other escalation reviewers.
Commit Appraised Folder Messages	Commit items to which you have applied appraisal status marks to the department review set.
Commit Reviewed Folder Messages	Add items from a research folder to the department review set. This permission requires the Perform Ad Hoc Searches permission.
Configure Department Properties	View and modify the properties of the department.
Delete Department	Delete the current department and all the objects that are associated with it (department-specific searches, user folders, hotwords, and so on).
Delete Folder	Delete the research folders in which users have stored items.
Escalate Messages	Escalate items to a higher authority for review.
Export Messages	Export items from the department review set.
Export Escalations	Export escalated items.
Grant Users Access	Assign roles to users in the department.
Manage Exceptions	Create exception employees and assign reviewers to them.
Modify & Delete Hotwords	Change and delete hotwords in the department hotword list.

Table 3-6 Department permissions (continued)

Permission	Description
Perform Ad Hoc Searches	Possess the full research permissions to create, delete, and modify research folders, search and review items, and so on.
Review Escalations	Review the items that other reviewers have escalated for further auditing.
Review Messages	View items, action status, and comment history.
Search Capture	Define custom searches to capture items in a specific department.
Show Reviewer Summaries On Home Page	View a summary of reviewer activity on the start page of the application.
View Reports	Create and view reports. As the scope of reports may be wider than the department, employees with this permission in a department can only view their own reports.

Creating Compliance Accelerator roles

If none of the predefined roles provides the exact set of permissions that you want to assign to users, you can create your own roles.

You must have the Manage Roles permission to create roles. By default, users with the application role of App User Admin have this permission.

To create a role

- 1 Click the **Application** tab in the Compliance Accelerator client, and then click the **Roles** tab.
- 2 Click **New** at the top of the window.

The Role Details pane appears.

Role Details

Name:

Description:

Scope:

Permissions

	Allow
Add Hotwords	<input type="checkbox"/>
Add Monitored Employees	<input type="checkbox"/>
Add Own Review Comments	<input type="checkbox"/>
Add Standard Review Comments	<input type="checkbox"/>
Apply Appraisal Status	<input type="checkbox"/>
Apply Bulk Actions To Escalations	<input type="checkbox"/>
Apply Bulk Review Action	<input type="checkbox"/>
Apply Comments To Escalations	<input type="checkbox"/>
Apply Review Action	<input type="checkbox"/>

Save Cancel

- 3 In the right pane, type a unique name and an optional description for the role.

The role name can contain up to 50 characters. The description can contain up to 250 characters.

- 4 In the **Scope** box, choose whether to make the permissions that are associated with the role effective throughout the application or at the department level only. You cannot create folder-level roles.

Users with application roles can only perform tasks in a specific department if they have been assigned the appropriate roles in that department. To perform tasks in more than one department, the users must be assigned the appropriate role in every department that they need to access.

The selection that you make determines the permissions that are available.

- 5 Choose the permissions to associate with the role.
See [“About the Compliance Accelerator permissions”](#) on page 40.
- 6 Click **Save**.

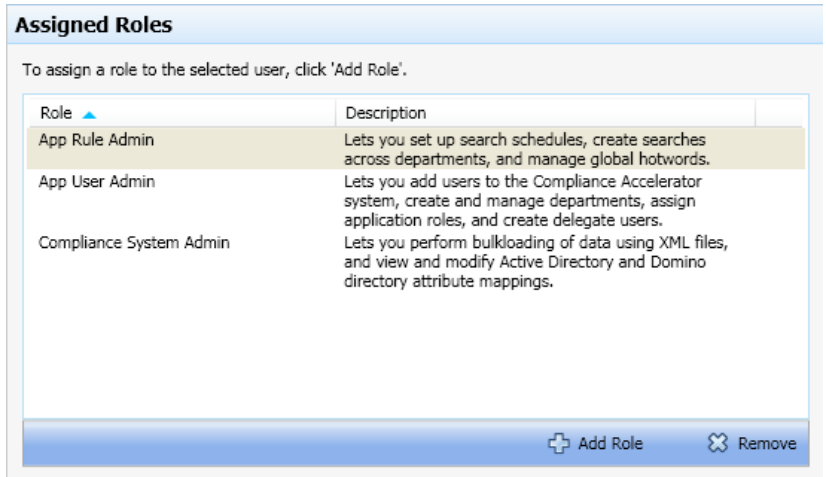
Assigning Compliance Accelerator roles to employees or groups

You must have the Grant Users Access permission to assign a role to an employee or group. By default, users with the application role of App User Admin have the first permission. Users with the department role of User Admin have the second.

As well as possessing the roles that you have explicitly assigned to them, employees can inherit roles from the groups to which they belong.

To assign a role to an employee or group

- 1 Do one of the following:
 - To assign an application role, click the **Application** tab in the Compliance Accelerator client, and then click the **Role Assignment** tab.
 - To assign a department role, click the **Departments** tab and then click the required department in the left pane. Then click the **Role Assignment** tab.
- 2 Click the name of the employee or group to whom you want to assign a role.
If the employee or group does not appear in the list, click **Add User** at the top of the pane. Then select the employee or group to add to the list.
- 3 In the right pane, do one of the following:
 - Click **Add Role** to assign a new role.
 - Click **Remove** to remove the selected role.



- 4 Click **Save**.
- 5 If you want to notify the selected user that he or she may now perform a ClickOnce installation of the Compliance Accelerator client, click **Send Email Invite**. Compliance Accelerator creates a new message that is ready to send to the user. Note that this facility is unavailable in Compliance Accelerator clients that you install with the MSI installer package.

To customize the subject line and body text of the notification message, follow these steps:

- Click the **Configuration** tab, and then click the **Settings** tab.
- Expand the **General** section to show the available options.
- Set the required values for the "CA Invitation Email Subject" and "CA Invitation Email Body" options.

Working with departments

This chapter includes the following topics:

- [About departments](#)
- [Creating departments](#)
- [Adding monitored employees and groups to departments](#)
- [Editing the monitoring policy for employees and groups](#)
- [Moving employees or groups between departments](#)
- [Moving departments](#)
- [Assigning department reviewers, compliance supervisors, and delegates](#)
- [Implementing Chinese Walls security](#)
- [Managing exception employees](#)
- [Grouping departments into partitions](#)
- [Using attributes to classify departments](#)

About departments

Compliance Accelerator lets you organize monitored employees into departments that reflect the structure of your company. For example, you can create departments that are called "Marketing", "Sales", and "Engineering". Then you can add the employees that you want to monitor to the appropriate departments.

After you have set up multiple departments, you can group them into partitions. This facility lets you restrict the scope of searches to items to and from monitored employees in departments in the same partition. If you do not define any partitions,

the searches that you initiate in one department can include the items of employees in other departments.

Creating departments

Within Compliance Accelerator, you can organize monitored employees into departments that reflect the structure of your company. You can add either a new top-level department or a nested department (a child department of an existing department).

The minimum information that is needed to create a department is its name and owner. The owner can be any employee that you have added to the system, but is typically the main system administrator for Compliance Accelerator.

You must have the Create Departments permission to add a new department. By default, users with the application role of App User Admin have this permission.

To create a department

- 1 Click the **Departments** tab in the Compliance Accelerator client.
 - 2 In the **Departments** pane at the left, do one of the following:
 - To create a top-level department, click **All Departments** and then click **New Department** at the top of the window.
 - To create a department that is the child of an existing department, click that department and then click the **Properties** tab. Then click **New Department Here** at the top of the window.
- If Compliance Accelerator lists a lot of departments, you can filter the list with the fields at the top of the pane. As well as filtering the departments by name, you can choose whether to list any exception employees, folders, and reviewers that are associated with them.

The Department pane appears.

Department

Name:

Status:

Owner:

Options

☒ Can contain departments

☐ Can contain monitored employees

Export details

Item ID padding:

Item ID prefix:

Output folder:

Search details

Default percentage sample for new searches: % ☐ Lock

Searchable Vault Stores:

- ☒ Demo Site
 - ☒ Domino Vault Store
 - ☒ Exchange Vault Store
 - ☒ File Vault Store
 - ☒ SharePoint Vault Store

General **Monitoring** History

- 3 In the **Name** box, type a unique name for the department.
The name can contain spaces and non-ASCII characters.
- 4 In the **Status** box, choose whether to make the department open or closed.
If you choose **Closed**, no monitoring of employees in the department occurs, and the department name does not appear in the start page of the application. However, employees who are also monitored in other departments continue to be monitored in those departments.
- 5 In the **Owner** box, select the display name and Windows user account of the principal administrator for the department.
Each department has an owner, who must have a Windows logon but does not need any special Windows or Compliance Accelerator privileges. By default, Compliance Accelerator grants the permissions that are associated with the User Admin role to department owners. These permissions are as follows:

- Grant Users Access
- Add Monitored Employees

- Configure Department Properties
- View Reports

- 6
- If you want to create a nested department that is a child of an existing one, ensure that the **Parent Department** box shows the correct department.
- 7
- If you have set up one or more department attributes, enter the required attribute values in the **Identity Attributes** area.

See [“Using attributes to classify departments”](#) on page 68.

- 8
- Check or uncheck the following options in the **Options** area:

Can contain departments	Specifies whether you can create nested departments under this department.
Can contain monitored employees	Specifies whether you can add monitored employees to this department. You may want to uncheck this option in cases where you need to set up a department hierarchy, where the top-level departments do not contain any monitored employees, but the nested departments do.

- 9
- In the **Export details** area, specify the default options to use when you export items for offline review. The options are as follows:

Item ID padding	Specifies the number of digits to use in the export number for each item. The default is 6.
Item ID prefix	Specifies the text to use as a prefix for the export number for each item. You may want to use letters to identify the export in accordance with legal or company naming convention.
Show Example	Displays a preview of the complete ID.
Output folder	<div>Specifies the folder on the Compliance Accelerator server in which to store the exported items.</div> <div>To export items to another computer, specify the UNC path to a share, as in <code>\\my_computer\exports</code>. However, if you want to export the items as a Personal Folder (<code>.pst</code>) file, we recommend that you specify the NTFS path; for example, <code>Z:\exports</code>. Windows does not support exporting to a <code>.pst</code> file through a UNC path.</div> <div>The folder path can contain up to 100 characters.</div>

10 In the **Search details** area, specify the policy that Compliance Accelerator must follow when it adds the results of a search to the department review set. The options are as follows:

Default percentage sample for new searches	Specifies the minimum percentage of the items that a search returns to add to the review set. When you create a search, you can qualify this option further by specifying the minimum number of items that are required per employee.
Lock	Stops the department administrators from changing the sample rate for new searches.
Searchable Vault Stores	Lets you select the vault stores whose archives are to be available for searching in the department. Department administrators with the appropriate permissions can customize the list of archives for searches in their departments.

11 If you have installed the Journaling Connector, click the **Monitoring** tab. Then set the general policy with which to capture the items of each employee and add them to the review set every day.

Monitoring policies

☐ Disable monitoring of employees in this department

☐ Cap the total number of messages in this department

☐ Cap total messages

☒ Cap by message type

*Guaranteed sampling does not support capping

Message Type:

Review Requirement:

Capping:

Microsoft Exchange Server

Internal:

2

%

External Inbound:

2

%

External Outbound:

2

%

Cap

Instant Messaging

Instant Messaging

2

%

Cap

Bloomberg

Bloomberg

2

%

Cap

Fax

Internal:

2

%

External Inbound:

2

%

External Outbound:

2

%

Cap

Lotus Domino

Internal:

2

%

External Inbound:

2

%

External Outbound:

2

%

Cap

General

Monitoring

History

Save

Cancel

The options are as follows:

Disable monitoring of all employees in this department

Specifies whether to stop monitoring of all employees in the department. Reviewers and department administrators can still access the department. Employees who are also monitored in other departments continue to be monitored in those departments.

If you select this option, you disable all the other options on the **Monitoring** tab.

Cap the total number of messages in this department

Lets you set a limit on the number of items that Compliance Accelerator captures and adds to the review set. If you are legally required to monitor a certain percentage of each employee's items, setting a limit may prevent you from meeting this requirement.

Capping applies only to the items that you capture with the Journaling Connector, and not to the items that you find when conducting searches. Nor does it apply to any items that policy management software has tagged for inclusion in the review set.

Message Type/Review Requirement/Capping

For each type of item, specifies as a percentage value the number of each employee's items to capture and add to the review set. Enter 0 for the item types that you do not use.

The types of Microsoft Exchange, fax, and Lotus Domino items are as follows:

- Internal. Selects the items where the author and all recipients are internal to your organization.
- External Inbound. Selects the items where the author is external to your organization and at least one recipient is internal.
- External Outbound. Selects the items where the author is internal to your organization and at least one recipient is external.

You can set monitoring policy at the employee level and group level as well as at the department level. Therefore, the values that are shown here may not apply to some employees. In that case, Compliance Accelerator honors the highest percentage for each item type. To set the values at the employee level or group level, use the Monitored Employees facility.

See [“Adding monitored employees and groups to departments”](#) on page 55.

12 Click **Save**.

Adding monitored employees and groups to departments

An important activity in Compliance Accelerator is to add employees and employee groups to the departments in which you want to monitor them. If you have not

already created the profiles for these employees and groups, you must do so before you can add them to a department.

See [“Creating employee profiles”](#) on page 28.

You must have the Add Monitored Employees and Grant Users Access permissions to add employees and groups to a department. By default, users with the department role of User Admin have these permissions.

To add monitored employees and groups to a department

- 1 Click the **Departments** tab in the Compliance Accelerator client.
- 2 In the **Departments** pane at the left, do one of the following:
 - Click the department to which you want to add some employees or groups, and then click the **Monitored Employees** tab. Then click **Add employees** at the top of the window.
 - Right-click the department to which you want to add some employees or groups, and then click **Add Monitored Employees**.
- 3 Select the employees and groups that you want to monitor.

You can select multiple adjacent names by holding down the Shift key and clicking the first and last names in the range. To select multiple, nonadjacent names, hold down the Ctrl key and click the required names.
- 4 Click **OK**.

Editing the monitoring policy for employees and groups

You can define the percentage of items that Compliance Accelerator should capture for each employee and add to the review set each day. If you monitor different types of items (Microsoft Exchange, Domino, instant message, Bloomberg, and fax), you can set a percentage for each type. For Exchange and Domino items, you can also set percentages on the items that travel in a particular direction (internal, external outbound, or external inbound).

If you use policy management software to classify items, the items that you capture through this method contribute to the monitoring policy quota that you define. When these items do not wholly satisfy the quota, Compliance Accelerator makes up the shortfall with the items that the Journaling Connector has sampled.

You must have the Assign % Review permission to edit the monitoring policy for an employee. By default, users with the department role of Rule Admin have this permission.

To edit the monitoring policy for an employee or group

- 1 Click the **Departments** tab in the Compliance Accelerator client.
- 2 In the **Departments** pane at the left, click the required department.
- 3 Click the **Monitored Employees** tab.

The Monitored Employees pane appears.

Monitored Employees		AMER Finance Group	
	Policy overridden	Exchange	Policy %
<input type="checkbox"/>	Monitored Employee	Internal	<input type="text"/>
<input type="checkbox"/>	AMER Finance Group	Inbound	<input type="text"/>
		Outbound	<input type="text"/>
		IM	<input type="text"/>
		Bloomberg	<input type="text"/>
		Fax	
		Internal	<input type="text"/>
		Inbound	<input type="text"/>
		Outbound	<input type="text"/>
		Domino	
		Internal	<input type="text"/>
		Inbound	<input type="text"/>
		Outbound	<input type="text"/>
		Ignore Department cap	<input type="checkbox"/>

- 4 Click the employee or group for which you want to amend the monitoring policy.
- 5 Enter the required details in the pane at the right.
For Microsoft Exchange, fax, and Lotus Domino items, the various types of items are as follows:
 - **Internal.** Selects the items where the author and all recipients are internal to your organization.
 - **Inbound.** Selects the items where the author is external to your organization and at least one recipient is internal.
 - **Outbound.** Selects the items where the author is internal to your organization and at least one recipient is external.
- 6 Check **Ignore Department cap** if you do not want the cap limit for the department to apply to the employee or group. The cap limit applies only to the items that you capture with the Journaling Connector. The items that you find when you conduct searches are unaffected.

Similarly, the limit does not apply to any items that policy management software has tagged for inclusion in the review set.

- 7 Click **Save**.

Moving employees or groups between departments

When an employee moves from one department to another, it is desirable to update Compliance Accelerator accordingly. The following conditions must apply before you can move monitored employees and employee groups from one department to another:

- You must have the Add Monitored Employees permission in both departments. By default, users with the department role of User Admin have this permission.
- In the properties for the target department, the option "Can contain monitored employees" must be checked.

When you move an employee or group to a new department, Compliance Accelerator applies the monitoring policy in that department to the employee or group. Similarly, the department reviewers in the new department rather than those in the old department are responsible for monitoring the employee or group. However, exception employees retain their old exception reviewers.

To move an employee or group between departments

- 1 Click the **Departments** tab in the Compliance Accelerator client.
- 2 In the **Departments** pane at the left, click the department that contains the employee or group that you want to move.
- 3 Click the **Monitored Employees** tab.
- 4 Drag the employee or group from the Monitored Employees list and drop it on the required department in the **Departments** pane.
- 5 Click **Move** to confirm that you want to move the employee or group.

Moving departments

When you move a department to a different place in the department hierarchy, any child departments move with it. The department's monitored employees, exceptions, reviewers, and supervisors also remain assigned to the department in its new position in the hierarchy.

You must have the Create Departments permission to move departments. By default, users with the role of App User Admin have this permission.

To move a department

- 1 Click the **Departments** tab in the Compliance Accelerator client.
- 2 In the **Departments** pane at the left, click the department that you want to move.

If Compliance Accelerator lists a lot of departments, you can filter the list with the fields at the top of the pane. As well as filtering the departments by name, you can choose whether to list any exception employees, folders, and reviewers that are associated with them.
- 3 Drag the department that you want to move and drop it on the new parent department.

You cannot drop a parent department on one of its children.
- 4 Click **Move** to confirm that you want to move the department.

The reviewers and supervisors of the parent department automatically have access to the moved department.

Assigning department reviewers, compliance supervisors, and delegates

Compliance Accelerator makes it easy to assign a number of key roles to the users of a department.

Department reviewers can review and mark the items in a department, export items for offline review, and generate and view reports. These users can also store items in research folders for further investigation.

Compliance supervisors can appraise the work of department reviewers and manage any exception employees in the department. Like department reviewers, compliance supervisors can also store items in personal folders for further research.

You can also assign an employee as a delegate for another reviewer or supervisor. The delegate automatically has reviewer access to the review sets of all the departments and exceptions for which the principal reviewer or supervisor is responsible. These departments and exceptions include those that are the result of inherited permissions or membership of a reviewer group or supervisor group. The only task that a delegate can perform on behalf of the principal reviewer is to review items. Delegate status does not bestow any other benefits.

Table 4-1 Permissions required to assign department reviewers, compliance supervisors, and delegates

Activity	Permission needed	Roles that provide this permission
Assign a department reviewer or compliance supervisor to a department.	Grant Users Access.	User Admin.
Assign a reviewer to an exception employee.	Manage Exceptions.	Compliance Supervisor, Rule Admin, or User Admin.
Make one user a delegate reviewer for another.	Manage Delegates.	App User Admin.

To assign a department reviewer, compliance supervisor, or delegate

- 1

Click the **Departments** tab in the Compliance Accelerator client.

2

In the **Users** pane at the left, click the name of the user to whom you want to assign a role.

3

Do one or more of the following:
- To make the user a department reviewer.

1

Click **Choose Action**, and then click **Assign Departments To Review**.

2

Select one or more departments in which to make the user a reviewer.

Compliance Accelerator lists the departments in which you have Grant Users Access permission and which you have yet to assign to this user.

3

Click **OK**.

To make the user a reviewer for an exception employee.

1

Click **Choose Action**, and then click **Assign Exceptions To Review**.

2

Select one or more exception employees to whom you want to assign the user.

Compliance Accelerator lists the available exception employees.

3

Click **OK**.

To make the user a compliance supervisor in a department.

- 1 Click **Choose Action**, and then click **Assign Departments To Supervise**.
- 2 Select one or more departments in which to make the user a compliance supervisor.

Compliance Accelerator lists the departments in which you have Grant Users Access permission and which you have yet to assign to this user.
- 3 Click **OK**.

To make the user a delegate for another reviewer.

- 1 Click **Choose Action**, and then click **Make The User A Delegate**.
- 2 Select one or more principal reviewers to whom you want to assign this user as a delegate.

You can assign several delegates to a reviewer or supervisor. However, you cannot assign groups as delegates.
- 3 Click **OK**.

To assign a delegate reviewer to the user.

- 1 Click **Choose Action**, and then click **Assign Delegate**.
- 2 Select one or more reviewers whom you want to assign to this user as a delegate.
- 3 Click **OK**.

Note: Another way to perform these actions is to drag users or departments from the left pane and drop them on the options at the right.

Implementing Chinese Walls security

Chinese Walls are the barriers between divisions of an institution that prevent communication between distinct business sections. For example, in investment banks, Chinese Walls are commonly employed to separate people who make investment decisions from people who are privy to undisclosed information that may influence those decisions.

You may want to erect similar barriers in Compliance Accelerator so that department reviewers can share the results of their searches with a specific subset

of department reviewers only, and not with all Compliance Accelerator reviewers. For example, consider a bank with an equity research department and an investment banking department. It would be appropriate for a Compliance Accelerator reviewer in the equity research department to share information with other reviewers and compliance supervisors in that department, but not with reviewers in the investment banking department. By implementing Chinese Walls, you can achieve this.

There are two stages to implementing Chinese Walls security: you first enable Chinese Walls, and then assign the role of Department User to selected users in a department.

Enabling Chinese Walls

The Chinese Walls feature is an optional feature, which is disabled by default. You must have the Modify System Configuration permission to change the configuration settings. By default, only users with the role of Compliance System Admin have this permission.

To enable Chinese Walls

- 1 Click the **Configuration** tab in the Compliance Accelerator client, and then click the **Settings** tab.
- 2 Expand the **Security** section to show the available options.
- 3 In the **Enable Chinese Wall Department Users** row, check the option in the **Value** column.
- 4 Click **Save**.
- 5 Restart the Enterprise Vault Accelerator Manager service on the Compliance Accelerator server to put your changes into effect.

Managing Department Users

After you have enabled Chinese Walls, you must assign the role of Department User within a department to those users to whom you want to assign other roles in the department. Only those users to whom you assign the Department User role appear in the list of available users when you assign new department or folder roles. Department Users are defined on a per-department basis, and they are inherited in nested departments.

Consider the following table. This shows two top-level departments, Equity Research (EQ) and Investment Banking (IB), each of which has a nested department (EQ-EMEA and IB-EMEA). The EQ-EMEA department has a nested department of its own (EQ-EMEA-EUR).

Table 4-2 Sample Department User setup

Department	Department Users
Equity Research (EQ)	Adam Allen Alex Ash
Equity Research (EQ) > EQ-EMEA	Bert Bayer
Equity Research (EQ) > EQ-EMEA > EQ-EMEA-EUR	Chloe Chaplin Christina Cartman
Investment Banking (IB)	Edward Edwin
Investment Banking (IB) > IB-EMEA	Frieda Fawkes

In this example, the administrator of the department EQ-EMEA can select from the following users only when adding a new reviewer: Adam Allen, Alex Ash, and Bert Bayer. None of the other Department Users is available for selection when the administrator adds reviewers. If the administrator had not chosen to enable Chinese Walls, it would be possible to add all the users as reviewers—even if they worked in the Investment Banking department rather than the Equity Research department.

To manage Department Users

- 1 Click the **Departments** tab in the Compliance Accelerator client.
- 2 In the **Departments** pane at the left, click the required department.
- 3 Click the **Department Users** tab.
- 4 Click **Add Department Users**.
- 5 Click the names of the employees or groups to which you want to assign the Department User role.

You can select multiple adjacent names by holding down the Shift key and clicking the first and last names in the block. To select multiple, nonadjacent names, hold down the Ctrl key and click the required names.

- 6 Click **OK**.

Managing exception employees

An *exception* is a monitored employee who requires a different reviewer from the rest of the employees in the department. For example, the sensitive nature of a senior manager's communications may require a more senior person to review them. You can handle this situation by applying exception status to the manager

and then assigning a suitable reviewer. Compliance Accelerator treats each exception employee like a separate department within that employee's department. Special permissions are needed to create and manage exceptions and to review an exception's communications.

Designating employees as exceptions

You must have Manage Exceptions permission in the department to make an employee an exception. By default, users with the role of Compliance Supervisor, Rule Admin, or User Admin have this permission.

To designate an employee as an exception

- 1 Click the **Departments** tab in the Compliance Accelerator client.
- 2 In the **Departments** pane at the left, click the department in which you want to designate one or more employees as exceptions.
- 3 Click the **Monitored Employees** tab.
- 4 If the employee whom you want to designate as an exception does not appear in the Monitored Employees list, click **Add employees** and then select him or her from the list.
- 5 Click the required employee, and then click **Make an Exception**.
- 6 Select one or more exception reviewers to assign to the exception employee.
You can select multiple adjacent names by holding down the Shift key and clicking the first and last name in the range. To select multiple, nonadjacent names, hold down the Ctrl key and click the required names.
- 7 Click **OK**.

Assigning further exception reviewers to an exception

When you designate an employee as an exception, Compliance Accelerator prompts you to assign one or more reviewers for the exception. However, you can later assign further exception reviewers.

You must have the Manage Exceptions permission in the department to assign exception reviewers. By default, users with the role of Compliance Supervisor, Rule Admin, or User Admin have this permission.

To assign further exception reviewers to an exception

- 1 Click the **Departments** tab in the Compliance Accelerator client.
- 2 In the **Departments** pane at the left, click the department that contains the exception.

- 3 Click the **Monitored Employees** tab.
- 4 Do one of the following:
 - In the list of monitored employees, click the exception and then click **Add exception reviewers**. Select one or more exception reviewers from the list, and then click **OK**.

You can select multiple adjacent names by holding down the Shift key and clicking the first and last name in the range. To select multiple, nonadjacent names, hold down the Ctrl key and click the required names.
 - Drag the exception reviewer from the **Users** list at the left, and drop it on the exception in the list of monitored employees. Then click **Add**.

To assign an exception reviewer as the sole reviewer for the exception

- 1 Click the **Departments** tab in the Compliance Accelerator client, and then click the **Monitored Employees** tab.
- 2 In the **Departments** pane at the left, click the department that contains the exception employee.
- 3 Click the **Users** tab at the left to bring it to the front.
- 4 Drag the exception from the list of monitored employees and drop it on the required reviewer in the **Users** list.
- 5 Click **Make** to confirm that you want to make the reviewer or group the sole reviewer of the exception employee.

Compliance Accelerator removes any other reviewers whom you previously assigned to the exception.

Moving an exception employee to another department

You must have the following permissions in both departments to move an exception employee from one department to another:

- Add Monitored Employees
- Manage Exceptions
- Grant Users Access

By default, users with the department role of User Admin have these permissions.

To move an exception employee to another department

- 1 Click the **Departments** tab in the Compliance Accelerator client.
- 2 In the **Departments** pane at the left, click the department that contains the exception employee.

- 3 Click the **Monitored Employees** tab.
- 4 Drag the exception from the list of monitored employees and drop it on the target department in the **Departments** list at the left.
- 5 Choose whether to permit the reviewers in the exception's old department to access the review set in that department. You may want to permit the reviewers to access the review set if it still contains some unreviewed messages for the exception.

When there are messages to review, a separate review set link appears for the exception employee in the new department.

Removing exception status

When you have no further need to monitor employees as exceptions, you can remove their exception status. Then the employees become ordinary, monitored employees in their departments, and Compliance Accelerator captures their communications in the normal way. However, any items that Compliance Accelerator has captured while the employees had exception status remain in the exception review set.

You must have the Manage Exceptions permission in the department to remove exception status from an employee. By default, users with the role of Compliance Supervisor, Rule Admin, or User Admin have this permission.

Note: After you remove an employee's exception status, the items that the employee has sent or received while still an exception may appear in the results of a search. This may be the case if your search criteria specifies a date before you installed the Journaling Connector or during a period when you disabled it.

To remove exception status from an employee

- 1 Click the **Departments** tab in the Compliance Accelerator client.
- 2 In the **Departments** pane at the left, click the department that contains the exception employee.
- 3 Click the **Monitored Employees** tab.
- 4 Click the exception employee, and then click **Remove the exception status**.
- 5 Click **Remove** to confirm that you want to remove the employee's exception status and the designated exception reviewers.
- 6 If there are any unreviewed messages for the exception employee, choose whether to let reviewers continue working on the review set.

Removing exception reviewers

You can remove the role of exception reviewer from employees when they do not need to perform the role anymore. Note that if an exception has one reviewer only, you cannot remove the reviewer while the exception is still active. Remove the exception status from the employee before you remove the reviewer.

You must have the Manage Exceptions permission in the department to remove exception reviewers. By default, users with the role of Compliance Supervisor, Rule Admin role, or User Admin have this permission.

To remove an exception reviewer

- 1 Click the **Departments** tab in the Compliance Accelerator client.
- 2 In the **Departments** pane at the left, click the department that contains the exception.
- 3 Click the **Monitored Employees** tab.
- 4 Expand the list of exception reviewers under the exception.
- 5 Click the reviewer whom you want to remove, and then click **Remove**.
- 6 Click **Remove** to confirm that you want remove the exception reviewer.

Grouping departments into partitions

You can group departments into partitions to restrict the scope of searches. For example, you may find this facility useful if you want to restrict searching in some departments to items to and from certain other departments.

If you do not define any department partitions, the searches that you initiate in one department can include the items of employees in other departments. When you define partitions, searches are restricted to items to and from monitored employees in departments in the same partition.

You can also create department partitions by specifying the details in an XML configuration file. Then you can import this file into the Compliance Accelerator database.

See [“Importing the configuration data”](#) on page 197.

Creating department partitions

You must have the Manage Department Partitions permission to create a partition. By default, users with the application role of App User Admin have this permission.

To create a department partition

- 1 Click the **Configuration** tab in the Compliance Accelerator client, and then click the **Department Partitions** tab.
- 2 Click **New** at the top of the window.

The Partition Details pane appears.

Partition Details

Name:

Description:

Departments in this partition:

Departments

Add... Remove

- 3 Type a name and description for the partition.
- 4 Click **Add** to select the departments that you want to include in the partition.
- 5 Click **Save**.

Using attributes to classify departments

When you define the properties of your Compliance Accelerator departments, you can optionally assign additional, identifying attributes to them. For example, suppose that half of your departments are located in the United States and the other half are located in Europe. One of the supplied attributes, Country, lets you specify the country in which a department is located. By setting this attribute value when you define the properties of a department, you can provide context for the department and make its management a little easier.

You can also add department attributes and values by specifying the details in an XML configuration file. Then you can import this file into the Compliance Accelerator database.

Setting up department attributes

A standard Compliance Accelerator system comes with the following attributes that you can apply to your departments: Country, City, and Division. You can rename these attributes, supply values from which department administrators can choose when they assign the attributes to their departments, and more.

You must have the View System Configuration permission to view the properties of each attribute, and the Modify System Configuration permission to change them. By default, users with the application role of Compliance System Admin have these permissions.

To set up department attributes

- 1 Click the **Configuration** tab in the Compliance Accelerator client, and then click the **Department Attributes** tab.

The Department Attribute pane appears.

The screenshot shows the 'Department Attribute' configuration pane. It has a light blue header with the title 'Department Attribute'. Below the header, there are two text input fields: 'Name' with the value 'Country' and 'Description' with the value 'Country name'. Below these fields is a section titled 'Attribute Options In Department Properties' with a light blue header. This section contains three options: 'Visible' with a checked checkbox, 'Allow free text values to be entered' with a checked checkbox, and 'When this attribute is changed on a department' with three radio button options: 'Do nothing' (selected), 'Copy value to child departments if not set', and 'Overwrite value on all child departments'. Below this section is another section titled 'Attribute Values Available In Department Properties' with a light blue header. This section contains a 'Values' label and a table with columns 'Name' and 'Description'. The table is currently empty. At the bottom of the pane, there are 'Save' and 'Cancel' buttons.

Department Attribute			
Name	Country		
Description	Country name		
Attribute Options In Department Properties			
Visible	<input checked="" type="checkbox"/>		
Allow free text values to be entered	<input checked="" type="checkbox"/>		
When this attribute is changed on a department	<input checked="" type="radio"/> Do nothing <input type="radio"/> Copy value to child departments if not set <input type="radio"/> Overwrite value on all child departments		
Attribute Values Available In Department Properties			
Values	<div>New Edit Delete</div> <table><thead><tr><th>Name</th><th>Description</th></tr></thead><tbody></tbody></table>	Name	Description
Name	Description		
<div>Save Cancel</div>			

- 2 In the left pane, click the name of the attribute that you want to set up.

- 3 In the right pane, type the name and an optional description for the attribute.
The name cannot contain the following characters:
* ? < > |
- 4 If you want to make the attribute available for selection when you define the properties of a department, check **Visible**.
- 5 If you want to permit users to enter a free-text value for the attribute instead of choosing from a predefined list, check **Allow free text values to be entered**.
- 6 If you have nested departments, choose the required behavior in child departments when you change the attribute value assigned to a parent department. The options are as follows:

Do nothing	No change is made to the values that are assigned to associated child departments.
Copy value to child departments if not set	The same value is only set for the child departments that do not have a value set for this attribute.
Overwrite value on all child departments	The same value is set for all child departments, regardless of any value that is set for this attribute.

- 7 If you want to change the values from which users can choose when they set the attribute in department properties pages, do the following:
 - To add a new value, click **New** and then type the required name and description.
 - To edit an existing value, click it and then click **Edit**. Compliance Accelerator automatically updates the properties of any department to which you assigned the value.
 - To delete an existing value, click it and then click **Delete**. Compliance Accelerator automatically removes the value from the properties of any department to which you assigned it.
- 8 Click **Save**.

Assigning attributes to departments

As part of the process of configuring the properties of a department, you can assign up to three attributes to it.

You must have the Configure Department Properties permission to assign attributes to a department. By default, users with the department role of User Admin have this permission.

To assign attributes to a department

- 1** Click the **Departments** tab in the Compliance Accelerator client.
- 2** In the **Departments** pane at the left, click the department to which you want to assign one or more attributes.
- 3** Click the **Properties** tab.
- 4** On the **General** tab of the properties pane, enter the required values in the **Identity Attributes** section.
- 5** Click **Save**.

Searching for items

This chapter includes the following topics:

- [About searching with Compliance Accelerator](#)
- [Creating and running Compliance Accelerator searches](#)
- [About the search criteria options](#)
- [Guidelines on conducting effective searches](#)
- [Pausing and resuming Compliance Accelerator searches](#)
- [About the Monitor Searches tab](#)
- [Searching the items of exception employees](#)
- [Selecting the archives in which to search](#)
- [Building Compliance Accelerator search schedules](#)
- [Defining hotwords to search for](#)
- [Configuring how Compliance Accelerator handles email addresses](#)

About searching with Compliance Accelerator

As an alternative to using the Journaling Connector to capture items, you can search for the items that meet certain criteria and add them to the review set. Compliance Accelerator lets you create a search that runs in one department only, or you can create an application-wide search that runs in multiple departments. This process involves the following activities:

- Running one or more searches on the relevant vault stores for suitable information. Compliance Accelerator offers a wide range of search criteria

from which to choose: words and phrases to look for, date ranges, message size, author and recipient addresses, and more.

- Studying the search results to assess their suitability, and then either accepting or rejecting the results.
- Searching again, until you have amassed all the information that you need.

When you are happy with the search results, you then go on to review the items that you have found.

You can build search schedules if you want to run searches at set times or set up recurrent searches that run automatically. You can also customize the list of Enterprise Vault archives in which Compliance Accelerator searches for items.

If you want to search for instances of certain words in your employee's communications, you can store them as hotwords. When you next define the criteria for a search, you can select the hotwords from a list.

Creating and running Compliance Accelerator searches

You can create a search that runs in one department only, or you can create an application-level search that runs in multiple departments. If you want to run searches at set times or set up recurrent searches, you can create search schedules. Create the schedule before you create the search.

You must have the Search Capture permission to create a search that runs in one department only. You require the Application Search permission to create application-level searches. By default, users with the department role of Rule Admin or exception reviewer have the first permission. Users with the application role of App User Admin have the second permission.

To create and run a Compliance Accelerator search

1 Do one of the following:

- To create a search that runs in multiple departments, click the **Application** tab in the Compliance Accelerator client.
- To create a search that runs in one department only, click the **Departments** tab in the Compliance Accelerator client, and then click the required department in the left pane.
- To create a search that runs in a research folder, click the **Research** tab in the Compliance Accelerator client and then click the required folder in the left pane.

If Compliance Accelerator lists a lot of departments and folders, you can filter the list with the fields at the top of the pane.

- 2 Click the **Searches** tab.
- 3 Click **New Search**.

The search properties pane appears.

Search

Context: AMER - VIP

Name:

Based on Search: <No Template>

Search Type: Immediate

☐ Automatically accept search results

☐ Include items already in review

▶ **Sampling**

▲ **Date range**

Date range: Specific date range

From:

To:

▶ **Authors and recipients**

▶ **Search terms**

▶ **Attachments**

▶ **Miscellaneous**

Save Cancel

- 4 If you are creating a search that runs in a research folder, and you clicked **All Research** in the left pane, Compliance Accelerator prompts you to select a department with which to associate the search. Make your selection, and then click **Search**.
- 5 Enter the required search criteria.
See [“About the search criteria options”](#) on page 76.

- 6 Click **Save** to start an immediate search or queue a scheduled search to start automatically at the appointed time.

The **Search Details** pane provides the following information:

Archive	Shows the name of the archive that Compliance Accelerator has searched.
Volume	Provides the ID of the volume that holds the archive.
Vault Store	Indicates the type of vault store that contains the archive.
Status	Shows the current status of the search in each archive.
Duration	Shows the amount of time that Compliance Accelerator has taken to search each archive.
Hits	Shows the number of items in each archive that match the search criteria.
Information	Provides details of any errors that occurred.

You can filter the list of archives by selecting an option in the **Show** list. For example, you can filter the archives to show the top 2000 archives by hits, or all archives with a status of "Error". To download the search details as a comma-separated value (CSV) file, click **Download Search Details for All Archives**.

- 7 When the search has completed, choose whether to accept or reject the results. Note the following:
 - Compliance Accelerator does not add the captured items to the review set until you accept the search results. If you did not check **Automatically accept search results**, you must manually accept or reject the results.
 - If you reject the results of a search, Compliance Accelerator deletes the search and results from the database. However, it leaves the actual items in the archives.
 - It is important that search results make sense because, after you accept the search, you cannot undo it.

About the search criteria options

Compliance Accelerator groups the search criteria options into multiple sections, which are described below. Click the arrow icons at the right to expand or collapse the sections.

When you construct a search that contains multiple options, pay attention to how each option interacts with the others in the search properties pane. Compliance Accelerator links all the selected options together with Boolean AND operators rather than OR operators. For example, suppose that you construct a search whose criteria include the following:

- A data range in the **Date range** section
- A search term in the **Search terms** section
- A file extension in the **Attachments** section

The search results contain only those items that match all the search criteria. Compliance Accelerator ignores any items that match some of the search criteria options but not others.

Search section

The Search section identifies the search and specifies when it runs.

Context	Identifies the department or research folder in which the search will run. In the case of an application-wide search, this is <All Departments>.
Name	Specifies a name for the search, such as "Daily Message Capture (London)".
Based on Search	Lets you select an existing search as the basis on which to set the criteria for the new search.
Save results in	<p>If displayed, lets you select a location in which to save the results. Select New folder in <Context> in the drop-down list if you want to specify the details of a new folder in which to save the results.</p> <p>This option is available only when you create a search in a folder that is not linked to any department (you have selected "My Research" in the left pane).</p>

Search Type	<p>Specifies whether the search runs immediately or at a scheduled time. If you select Scheduled, you can specify a period during which the search is to run. You can also choose from one of a number of existing schedules.</p> <p>See “Building Compliance Accelerator search schedules” on page 91.</p> <p>You can also conduct <i>guaranteed sample searches</i>. Each guaranteed sample search runs at the selected sampling time, which is 1:00 A.M. by default. If the search returns fewer results than your monitoring policy demands, Compliance Accelerator adds randomly-sampled items to the review set to make up the shortfall. In effect, therefore, you can assemble more focused review sets that are weighted towards search-specific results instead of purely randomly-sampled items.</p>
Automatically accept search results	<p>Specifies whether to add the search results to the review set automatically. This option may be useful for any proven searches that you intend to run on a regular basis. If you check Automatically accept search results, you cannot reject the results and change the search criteria. We recommend that you uncheck Automatically accept search results until you have tested that the search returns the expected results.</p> <p>A search that returns an error from any archive is not automatically accepted, regardless of this setting.</p>
Include items already in review	<p>Specifies whether the search results can include the items that you have previously captured and added to the review set. For an immediate search or scheduled search, we recommend that you check this box to ensure that the results include the items that may already be in review from other searches.</p>

Sampling section

The Sampling section lets you sample the search results and add a random selection of items to the review set.

Compliance Accelerator does not deduplicate randomly-sampled items.

Sampling percentage	<p>Specifies the percentage of search results to include in the review set. You can specify fractions, as in 10.25.</p> <p>You may not be able to change the sampling percentage if the owner of department has locked this setting in the department properties.</p>
Minimum per author	<p>Specifies the minimum number of items per author to include in the review set. If there are no items for an author in the search results, none can be included in the sample. Note that as the authors can be from outside the selected department, you may return more search results than expected.</p>
Absolute limit	<p>Sets an upper limit on the total number of search results to add to the review set. This option takes precedence over any values that you set in the Percentage box and Minimum items per employee box.</p>

Date range section

The Date range section lets you search for items according to when they were sent or received.

Today / Yesterday / Last 7 days / Last 14 days / Last 28 days	<p>Limits the search to items that were sent or received during the selected period. The date ranges are relative to when the search runs, which is today in the case of an immediate search.</p> <p>You may find these options useful when creating a scheduled, recurrent search that runs once every day, week, two weeks, or four weeks. For example, if the search runs once a week, select Last 7 days to limit the range to the days since the search last ran.</p>
Specific date range	<p>Lets you search the items that were sent or received during a longer or more specific period than the other date range options permit. To enter a date, click the options at the right of the From and To boxes and then select the required date. Unlike the other date range boxes, a specific date range remains static and not relative to when the search runs.</p>

Since search last ran	<p>For a scheduled search only, lets you search the new items that have arrived since the last time you ran the search. This option is similar to options such as Today and Yesterday. However, it lets you set an explicit start date for the first run of the search.</p> <p>By default, this option searches from the date of the last run (or the start date for the first search) to the current day minus 1 (that is, up to yesterday).</p>
-----------------------	---

Authors and Recipients section

The Authors and Recipients section targets the departments for the search and the direction of the items to search. Any departments that you have organized into partitions can only search items to and from departments in the same partition.

Message Route	<p>Specifies the direction in which the items for which you want to search have traveled. You can search for the items that are to or from the selected departments, and for the items that have traveled between the selected departments and other departments.</p> <p>The available message route options can depend on the date range that you have specified and on how Compliance Accelerator has been configured.</p>
Any Of/All Of	<p>Specifies whether to apply the search to any of or all of the selected departments and employees.</p>
Use inheritance, automatically include new departments	<p>For application-wide searches only, lets you specify whether to apply the search to the subdepartments of the selected departments. By default, any new departments that are subdepartments of others automatically inherit any active, recurring searches that you have applied to those departments. This is also true of any existing departments that you move under departments that have recurring searches.</p>
Department tree	<p>Specifies the departments and employees that you want to include in the search. Click the arrows to the left of the department names to expand them and view the nested departments and exception employees.</p> <p>When you select a department, you do not automatically include any exception employees in the department. To search exception employees, you must select each one explicitly.</p>

Freeform email addresses / domains	<p>Lets you type one or more email addresses and domains. Type each address or domain on a line of its own to search for the items whose From, To, CC, or BCC field contains any of the addresses or domains. Type all the addresses and domains on a single line to search for items in which they are all present.</p> <p>Place the minus sign (-) in front of an address or domain to exclude it from the search. To exclude multiple addresses or domains, type them all on a single line.</p> <p>This field is not available for all possible message routes.</p>
------------------------------------	--

Search terms section

The Search terms section specifies the words or phrases for which Compliance Accelerator should search in the subject lines of items and their bodies. By default, when you search for words in both the subject of an item and its content, Compliance Accelerator finds those items that meet one or both criteria. However, it is possible to set up Compliance Accelerator so that only those items that meet both criteria are found.

Subject	Searches for those items that contain any or all of the specified words or phrases in their subject lines.
Content	Searches for those items that contain any or all of the specified words or phrases in their bodies and any searchable attachments.

The words or phrases that you specify here are highlighted in the **Review** pane when you review the items that this search has found.

Observe the following guidelines when you type the words and phrases:

- Compliance Accelerator searches are case-insensitive.
- If you type multiple words on the same line, Compliance Accelerator treats them as a phrase.
- Type each word on a line of its own if you want to use the **Any of** option or **All of** option to refine the search criteria.

In the following example, Compliance Accelerator joins together the three words with an OR operator ("server OR group OR cluster"). Any item that contains one or more of the words matches the search criteria.

```
Any Of: server
        group
        cluster
```

In the next example, Compliance Accelerator joins together the three words with an AND operator ("server AND group AND cluster"). Only those items that contain all three words match the search criteria.

```
All Of: server
        group
        cluster
```

In the following example, Compliance Accelerator joins together the phrase "server group" and the word "cluster" with an AND operator ("server group AND cluster"). Only those items that contain both the phrase "server group" and the word "cluster" match the search criteria.

```
All Of: server group
        cluster
```

- You must type at least the first three characters of the word or phrase.
- You can append a wildcard character to the end of the word or phrase to represent other characters. An asterisk (*) represents zero or more characters. A question mark (?) represents exactly one character.
- Place a minus sign (-) at the start of a line to indicate that you want to exclude from the search results any items that contain the following word or phrase. For example, the following search term finds the items that contain either of the words "server" and "group" but do not contain the word "cluster" ("server AND NOT cluster) OR (group AND NOT cluster)":

```
Any Of: server
        group
        -cluster
```

A search term cannot comprise an excluded word or phrase only. When you specify such words or phrases, you must also specify a positive word or phrase that you want to appear in the search results.

- Click **Hotwords** to choose from a list of hotwords and phrases, if you have previously created one.
See [“Defining hotwords to search for”](#) on page 94.
- Compliance Accelerator ignores any nonalphanumeric characters in the search term, except for those that have special significance, such as the plus sign, minus sign, and question mark.
For example, a search for the term **US@100** may find instances not only of **US@100** but also of **US100** and **US\$100**. Including nonalphanumeric characters in the search term may therefore return more results than you expect.

Attachments section

The Attachments section lets you search for items with a certain number or type of attachments.

Number Specifies the required number of attachments. The default option, "Does not matter", means that the item can have zero or more attachments. All the other options require you to type one or two values that specify the required number of attachments.

File extensions Specifies the file name extensions of particular types of attachments for which to search. Separate the extensions with space characters. For example, type the following to search for items with HTML or Microsoft Excel file attachments:

`.htm .xls`

This search option evaluates attachments by their file names only; it does not check their file type. For example, suppose that a user changes the file name extension of a `.zip` file to `.zap` and then sends the renamed file as an email attachment. A Compliance Accelerator search for items that have attachments with a `.zip` extension does not find the email with the renamed attachment.

The contents of some attachments may not be searchable because Enterprise Vault has not indexed them. In particular, file formats such as Fax and Voice do not have any indexable content.

Some Enterprise Vault registry entries prevent it from indexing the contents of selected file types. For example, this is the case with the `ExcludedFileTypesFromConversion` entry. For more information, see the Enterprise Vault *Registry Values* guide.

For more information on how Compliance Accelerator conducts searches in which you have specified file name extensions, see the following article on the Symantec Enterprise Support site:

<http://www.symantec.com/docs/TECH191321>

Miscellaneous section

The Miscellaneous section lets you search for items of a certain size and type or that have the specified retention category.

Message size	Specifies the size in kilobytes of each item for which to search, as reported by the message store (Microsoft Exchange, Lotus Domino, and so on). The item size includes the size of any attachments.
Message type	<div>Searches for items of the selected types. This option is only available if:</div> <div><div>■ Your Enterprise Vault server is running Enterprise Vault 5.0 or later.</div><div>■ You have specified a date range that does not include a date before you installed Enterprise Vault 5.0.</div></div>
Retention category	Searches for items to which Enterprise Vault has assigned the selected retention categories.

Policies section

The Policies section lets you search for items according to the tags with which any additional policy management software has classified them.

Policy

Lets you search for the items that match certain classification policies. There are several types of policies:

- **Inclusion.** Any item that your policy management software has classified for inclusion in the review set may be guilty of the most serious offenses, such as swearing, racism, or insider trading. You would normally want to ensure that the items exhibiting any of these features were included in your review set.
- **Exclusion.** Spam items and newsletters are typical examples of the items that your policy management software may classify for exclusion from the review set.
- **Category.** Your policy management software may categorize the items that exhibit certain characteristics, such as containing Spanish text. This type of policy provides no information on whether an item should be included in or excluded from the review set.

These policy types are not mutually exclusive. Your policy management software may apply multiple policies of different types to the same item.

Select the required policy type and then check the names of the policies for which you want to search. Alternatively, you can select **Custom** as the policy type and then type the names of one or more policies. Separate multiple policy names with commas, like this:

CustomPolicy1,CustomPolicy2

If you choose to search for multiple policies, the search results will contain items that match any one of the policies.

Filter policies by current department

Lets you omit from the list those policies that are not in use in the current department.

Guidelines on conducting effective searches

For the best results when conducting searches, follow these guidelines:

- **Make searches precise.** For example, include the author or recipient details, or specify date ranges.
- **In the properties of the department, limit the number of searchable vault stores.**
- **Only use wildcards when necessary, as they can severely affect performance.**
- **Avoid overusing search terms.** Thousands of terms can cause iterative searches.

- Ensure that scheduled searches do not run at the same time as system backups.
- Quickly accept or reject searches to avoid filling and slowing the database.
- Test new searches in research folders, and then delete the folders as necessary.

Although intended for Discovery Accelerator users, the *Effective Searching* white paper provides information that you may find useful when you conduct searches with Compliance Accelerator. This white paper is available from the following page of the Symantec Enterprise Support site:

<http://www.symantec.com/docs/HOWTO77131>

Pausing and resuming Compliance Accelerator searches

If you have the required permission level, you can monitor the status of all Compliance Accelerator searches and pause or resubmit them as necessary. This is true even if you do not normally have access to the departments with which the searches are associated. However, you cannot view the search criteria or the results of the searches unless you normally have access permission.

You must have the Monitor Search permission to pause and resume searches. By default, users with the role of Compliance System Admin have this permission.

To pause or resume a search

- 1 Click the **Monitor** tab in the Compliance Accelerator client.
- 2 Do one or more of the following:
 - To view detailed status information on a search, click its name.
 - To pause or resubmit one or more searches, select the required searches and then click **Pause** or **Resubmit**.

Note: If you pause a search that you are conducting over a wide date range or a large number of archives, Compliance Accelerator may take a little time to halt it.

About the Monitor Searches tab

The Monitor Searches tab lets you view the status of the searches that you have conducted. You can stop and pause searches that are still in progress, and resubmit failed searches. As [Table 5-1](#) shows, you can access the tab in several ways.

Table 5-1 How to access the Monitor Searches tab

To view the status of	Do this
Searches that are running in all departments.	Click the Monitor tab in the Compliance Accelerator client.
Searches that are running in one department only.	<ol style="list-style-type: none"> 1 Click the Departments tab in the Compliance Accelerator client. 2 Click the required department in the left pane. 3 Click Searches.
Searches that are running in one or more research folders.	<ol style="list-style-type: none"> 1 Click the Research tab in the Compliance Accelerator client. 2 In the left pane, click the required research folder, or click All Research to view the status of searches in all the folders. 3 Click Searches.

The Monitor Searches tab is divided into three panes:

- The filter pane at the top lets you filter the searches by name, status, date, and type. Select the required filter options and then click the **Apply filter** button at the right. Click the button again to clear the filter options.
- The center pane lists the searches that match the selected filter options. The information that this pane provides varies, depending on the context in which you display the Monitor Searches tab.

Name	Identifies the search.
Department or Folder	If displayed, identifies the department or folder in which the search has run.
Submitter	Identifies the person who submitted the search.
Run Date	Shows the date and time at which the search started.
Hits	Shows the number of items that match the search criteria.
Sampled	For guaranteed sample searches only, shows the number of randomly-sampled items that Compliance Accelerator has added to the search results to make up the shortfall. This is necessary when a search returns fewer results than your monitoring policy demands.

Duplicates	Shows the number of items that Compliance Accelerator has identified as duplicates.
Targeted Archives	Shows the number of archives that Compliance Accelerator has searched.
Status	Shows the status of the search.
Search Type	Indicates the type of search.
Enabled	If displayed, shows whether scheduled searches and guaranteed sample searches are currently enabled. When a search is not enabled, it does not run.

- When you click a search in the center pane, the bottom pane provides the following information:

Archive	Shows the name of the archive that Compliance Accelerator has searched.
Index Volume ID	Provides the ID of the volume that holds the archive.
Vault Store	Indicates the type of vault store that contains the archive.
Status	Shows the current status of the search in each archive.
Duration	Shows the amount of time that Compliance Accelerator has taken to search each archive.
Hits	Shows the number of items in each archive that match the search criteria.
Information	Provides details of any errors that occurred.

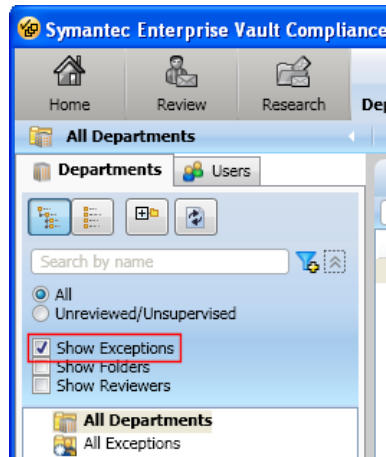
You can filter the list of archives by selecting an option in the **Show** list. For example, you can filter the archives to show the top 2000 archives by hits, or all archives with a status of "Error". To download the search details as a comma-separated value (CSV) file, click **Download Search Details for All Archives**.

Searching the items of exception employees

When you create an application search for multiple departments, Compliance Accelerator does not search the exception employees in those departments unless you explicitly instruct it to do so. For an alternative way to search an exception's items, follow the steps below.

To search the items of an exception employee

- 1 Click the **Departments** tab in the Compliance Accelerator client.
- 2 In the **Departments** pane at the left, check the filter option **Show Exceptions**.



- 3 Click the name of the exception employee whose items you want to search.
- 4 Click the **Searches** tab.
- 5 Create a new search and accept the results in the normal way.

Compliance Accelerator stores the accepted results in the review set for the exception. This review set is separate from the review set for the rest of the department employees. Only those exception reviewers who are assigned to the exception can access it.

Selecting the archives in which to search

You can customize the list of Enterprise Vault archives in which Compliance Accelerator searches for items. For example, there may be archives that you want to exclude from any searches because they contain irrelevant material.

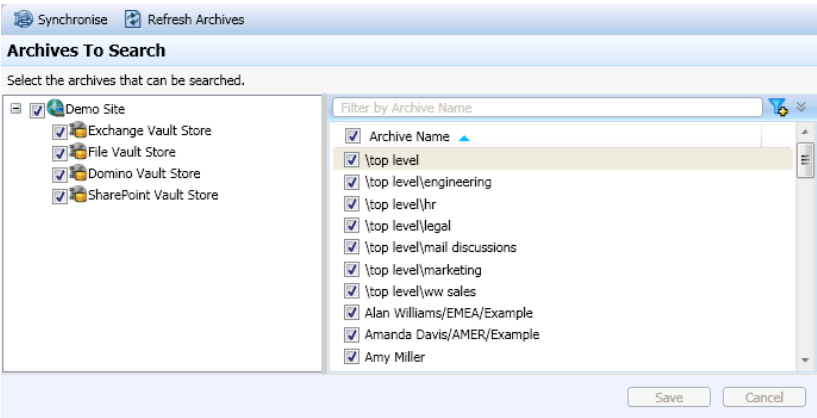
As well as setting the default, global list of archives, which are available to the searches you conduct in any department, you can customize the searchable archives for individual departments.

You must have the application permission **Modify System Configuration** to set the global list of archives, and the department permission **Configure Department Properties** to set a department-level archive list. By default, users with the

application role of Compliance System Admin have the first permission, whereas users with the department role of User Admin have the second.

To select the archives in which to search

- 1
- Do one of the following:
- To set the default list of archives that are available to all departments, click the **Application** tab in the Compliance Accelerator client, and then click the **Archives** tab.
- To set the list of archives in which to search for one department only, click the **Departments** tab and then click the required department in the left pane. Then click the **Archives** tab.
- If Compliance Accelerator lists a lot of departments, you can filter the list with the fields at the top of the pane. As well as filtering the departments by name, you can choose whether to list any research folders that are associated with them.
- 2
- Choose the archives in which to conduct searches.



Note: When many archives match the current selection and filter criteria, Compliance Accelerator may take some time to list them all. In these circumstances, Compliance Accelerator displays a prompt that advises you to change the criteria in order to reduce the number of listed archives. You can either do this or click **Show All Archives** to list all the archives. To stop the prompt from appearing each time you return to this pane during the current session, check **Don't show again in this session** before you click **Show All Archives**.

By default, Compliance Accelerator displays the prompt when more than 50,000 archives match the current criteria. To change this threshold, set the configuration option called "Display warning in Archives pane when number of archives to load exceeds this threshold".

See ["General configuration options"](#) on page 164.

Use the following techniques to include or exclude archives:

- If you want to set the list of archives in which to search for one department only, check **Customize searchable archives for this department**.
- Check or uncheck a vault store at the left to include its archives in searches or exclude them from searches.
- Click a vault store at the left to list the associated archives at the right. Then check or uncheck the archives to include or exclude them.
The **Status** column shows whether each archive has been copied, moved, or deleted as part of a Move Archive operation by the Enterprise Vault administrator.
If Compliance Accelerator lists a large number of archives, you can filter the list with the fields at the top of the right pane.
- Check or uncheck the **Archive Name** box at the top of the right pane to include or exclude all the available archives.

3 Click **Save**.

Building Compliance Accelerator search schedules

As well as running searches immediately, you can schedule them to run at a future time. This facility may be desirable if, for example, you want to run an extensive search during an off-peak period, or you need to run the same search repeatedly. To create a scheduled search, you first define a *search schedule* and then select it as one of the criteria of the search.

Note: The SQL Server Agent service is responsible for managing search schedules, so you must ensure that it is running. For instructions on how to configure the SQL Server Agent service, see the *Installation Guide*.

Setting up new search schedules

You must have the Manage Schedules permission to set up new search schedules. By default, users with the application role of App Rule Admin have this permission.

To set up a new search schedule

- 1 Click the **Configuration** tab in the Compliance Accelerator client, and then click the **Search Schedules** tab.
- 2 Click **New**.

The Schedule Details pane appears.

Schedule Details

Name: ☒ Enabled

Description:

Schedule Type

☐ Start when SQL server agent starts
☐ Start when CPU(s) are idle
☐ Once
☒ Recurring

Occurs every 1 day(s), at 01:00.

Recurring Schedule

Occurs:

Every day(s)

Daily frequency:

☒ Occurs once at: 01 h : 00 min (time)
☐ Occurs every:

Save Cancel

- 3 Type a name and an optional description for the schedule.
- 4 Check **Enabled** so that the schedule is available for selection when you define the criteria for a new search.
- 5 Select the required schedule type. The options are as follows:

Start when SQL server agent starts	Causes any searches that use this schedule to run immediately after the SQL Server Agent service has started.
Start when CPU(s) are idle	Causes any searches that use this schedule to run when the system is quiet. For more information on CPU idle schedules, see the information on scheduling jobs in the online Help for SQL Server Management Studio.
Once	Causes any searches that use this schedule to run only once, at the time that you set in the schedule. When you select this option, several additional boxes appear. Click the On date box to select the required date. Enter the time in the At time box in the format <i>hh:mm</i> , using the 24-hour clock.
Recurring	<p>Causes any searches that use this schedule to run automatically at the interval that you specify in the schedule.</p> <ul style="list-style-type: none"> ■ Occurs. Defines the interval in days, weeks, or months. ■ Daily frequency. Defines whether the schedule runs once a day or several times a day, within a given period. ■ Duration. Defines whether to restrict the schedule to a particular period within given dates.

In searches with a schedule type of **Once** or **Recurring**, the time that you specify is the time on the Compliance Accelerator server rather than that on your client computer.

6 Click **Save**.

Examples of recurring search schedules

Any searches that use the following schedules run automatically at the interval that you specify in the schedule.

To create a schedule that runs once every day at 2 A.M. from now on

- 1 Select **Daily**, and enter **1** in the **Every n day(s)** box.
- 2 Select **Occurs once at**, and enter **02:00** in the **(time)** box.
- 3 Select **No end date**.

To create a schedule that runs every 3 hours on Mondays, between 9 A.M. and 6 P.M., for the period between March 1 and August 2

- 1 Select **Weekly** and then check **Mon**.
- 2 Select **Occurs every**, and then enter **3** and select **Hour(s)**.
- 3 Enter **09:00** in the **Starting at** box and **18:00** in the **Ending at** box.
- 4 Select March 1 for the start date and August 2 for the end date.

To create a schedule that runs at 9 P.M. on the first day of alternate months from now on

- 1 Select **Monthly** and **Day**, and enter **1** in the day box and **2** in the **month(s)** box.
- 2 Select **Occurs once at**, and enter **21:00** in the **(time)** box.
- 3 Select **No end date**.

Defining hotwords to search for

Hotwords are predefined words or phrases that you can search for in employee items. When creating a search, you can select hotwords to search for in the subject lines of items, their content, or both.

To simplify the management of hotwords, you can group them into hotword sets. For example, you can use one set of hotwords to monitor items for unacceptable language and another to monitor them for unethical business practice. You can define hotwords and hotword sets at the global, application level, where they are applicable to all departments, and at the department level, where they are specific to that department.

Compliance Accelerator comes with several XML files that contain predefined hotwords and phrases. You can import these files into your system as global hotwords and phrases, and then modify them as necessary.

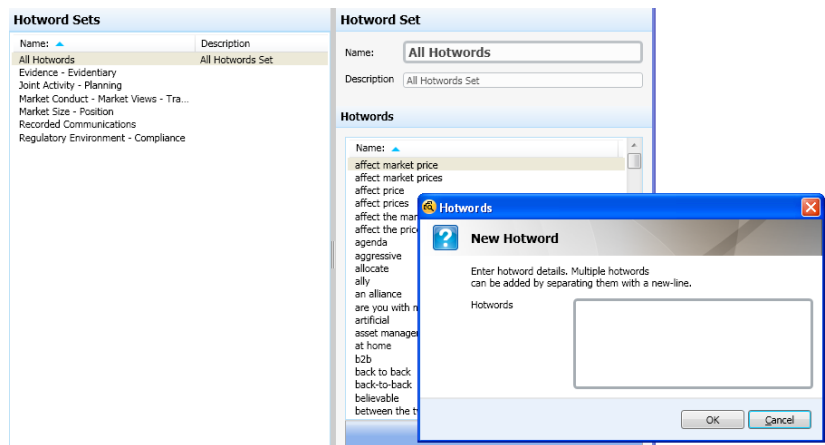
Adding hotwords

You must have the application permission Add Hotwords to add global hotwords, and the department permission Add Hotwords to add department-level hotwords. By default, users with the application role of App Rule Admin have the first permission, whereas users with the department role of Rule Admin have the second.

To add a hotword

- 1 Do one of the following:

- To add a global hotword, click the **Application** tab in the Compliance Accelerator client, and then click the **Hotwords** tab.
 - To add a department-level hotword, click the **Departments** tab and then click the required department in the left pane. Then click the **Hotwords** tab.
- 2 Select the hotword set to which you want to add the new hotword, or select **All Hotwords** to add a hotword that is not associated with any set.
 - 3 In the **Hotwords** box at the right, click **New**.



- 4 Type the hotwords and phrases. Observe the following guidelines as you do so:
 - Each word or phrase must be on a new line.
 - Enclose phrases in double quotation marks. If you copy and paste quoted phrases from programs such as Microsoft Word, take care to replace any curly quotation marks ("smart quotes") with straight ones. Compliance Accelerator does not recognize curly quotation marks as double quotation marks.
 - You can append a wildcard character to the end of the word or phrase to represent other characters. An asterisk (*) represents zero or more characters, and a question mark (?) represents exactly one character. For example, the hotword **commodit*** matches both "commodity" and "commodities".
- You must type at least the first three characters of the word or phrase to which you append the wildcard character.

Try not to over-use wildcard characters in the hotwords and phrases that you add to the criteria of a search. The greater the use of wildcard characters, the more complex the search becomes. This can lead to longer running searches and excessive memory usage.

- Compliance Accelerator ignores any punctuation symbols or other special characters, such as % or \$, that you include in a hotword or phrase. For example, **US@100** matches not only **US@100** but also **US 100** and **US\$100**.
- Place a minus sign (-) at the start of a hotword or phrase to indicate that you want to exclude from the search results any items that contain the word or phrase. For example, consider the following:
buy -commodit*
Only items that contain the word "buy" but do not contain the word "commodity" or "commodities" match this phrase.

Click **OK** when you have finished.

- 5 Click **Save**.

Editing existing hotwords

You can change an existing hotword or phrase as necessary. Note that if you previously included this hotword in an accepted search, the change is reflected when you view hotwords in the criteria for that search.

You must have the application permission Modify & Delete Hotwords to edit global hotwords, and the department permission Modify & Delete Hotwords to edit department-level hotwords. By default, users with the application role of App Rule Admin have the first permission, whereas users with the department role of Rule Admin have the second.

To edit an existing hotword

- 1 Do one of the following:
 - To edit a global hotword, click the **Application** tab in the Compliance Accelerator client, and then click the **Hotwords** tab.
 - To edit a department-level hotword, click the **Departments** tab and then click the required department in the left pane. Then click the **Hotwords** tab.
- 2 Click **All Hotwords**.
- 3 In the **Hotwords** box at the right, click the hotword and then click **Edit**.
- 4 Change the word or phrase as necessary, and then click **OK**.
- 5 Click **Save**.

Deleting hotwords

When you have no further use for a hotword, you can delete it. Deleting a hotword automatically removes it from all hotword sets to which it belongs.

You must have the application permission **Modify & Delete Hotwords** to delete global hotwords, and the department permission **Modify & Delete Hotwords** to delete department-level hotwords. By default, users with the application role of App Rule Admin have the first permission, whereas users with the department role of Rule Admin have the second.

To delete a hotword

- 1 Do one of the following:
 - To delete a global hotword, click the **Application** tab in the Compliance Accelerator client, and then click the **Hotwords** tab.
 - To delete a department-level hotword, click the **Departments** tab and then click the required department in the left pane. Then click the **Hotwords** tab.
- 2 Click **All Hotwords**.
- 3 In the Hotwords box, click the hotword that you want to delete.

You can select multiple adjacent hotwords by holding down the Shift key while clicking the first and last hotword in the range. To select multiple nonadjacent hotwords, hold down the Ctrl key while clicking the required hotwords.
- 4 Click **Delete**.
- 5 Click **Save**.

Adding hotword sets

As with hotwords, you can define hotword sets at the global, application level, where they are applicable to all departments, and at the department level, where they are specific to that department.

You must have the application permission **Add Hotwords** to add global hotword sets, and the department permission **Add Hotwords** to add department-level hotword sets. By default, users with the application role of App Rule Admin have the first permission, whereas users with the department role of Rule Admin have the second.

To add a hotword set

- 1 Do one of the following:

- To add a global hotword set, click the **Application** tab in the Compliance Accelerator client, and then click the **Hotwords** tab.
 - To add a department-level hotword set, click the **Departments** tab and then click the required department in the left pane. Then click the **Hotwords** tab.
- 2 Click **New** at the top left of the window.
 - 3 Type a name and optional description for the hotword set.
The name can contain space characters.
 - 4 Click **Add** at the bottom of the Hotwords box to select the hotwords to include in the set.

You can select multiple adjacent hotwords by holding down the Shift key while clicking the first and last hotword in the range. To select multiple nonadjacent hotwords, hold down the Ctrl key while clicking the required hotwords. Click **OK** when you have finished.
 - 5 Click **Save**.

Editing existing hotword sets

You can change the name and description of a hotword set, add words to it, and remove existing words.

You must have the application permission **Modify & Delete Hotwords** to edit global hotword sets, and the department permission **Modify & Delete Hotwords** to edit department-level hotword sets. By default, users with the application role of App Rule Admin have the first permission, whereas users with the department role of Rule Admin have the second.

To edit an existing hotword set

- 1 Do one of the following:
 - To edit a global hotword set, click the **Application** tab in the Compliance Accelerator client, and then click the **Hotwords** tab.
 - To edit a department-level hotword set, click the **Departments** tab and then click the required department in the left pane. Then click the **Hotwords** tab.
- 2 Click the hotword set that you want to edit.
- 3 Do one or more of the following:
 - To create one or more hotwords and add them to the hotword set, click **New** in the Hotwords box and then type each hotword on a line of its own.

- To add one or more existing hotwords to the hotword set, click **Add** in the Hotwords box and then select the required hotwords.
- To remove one or more hotwords from the set, select them in the Hotwords box and then click **Remove**.

4 Click **Save**.

Deleting hotword sets

When you have no further use for a hotword set, you can delete it. Note that deleting a hotword set does not remove the hotwords that it contains. If you delete a hotword set that you used in an accepted search, the hotword set is no longer displayed in the criteria for that search.

You must have the application permission **Modify & Delete Hotwords** to delete global hotword sets, and the department permission **Modify & Delete Hotwords** to delete department-level hotword sets. By default, users with the application role of **App Rule Admin** have the first permission, whereas users with the department role of **Rule Admin** have the second.

To delete a hotword set

- 1 Do one of the following:
 - To delete a global hotword set, click the **Application** tab in the Compliance Accelerator client, and then click the **Hotwords** tab.
 - To delete a department-level hotword set, click the **Departments** tab and then click the required department in the left pane. Then click the **Hotwords** tab.
- 2 Select the hotword set that you want to delete.
- 3 Click **Delete** at the top of the window.
- 4 Click **Delete** again to confirm that you want to proceed.

Importing the predefined hotwords

Compliance Accelerator comes with several XML files that contain predefined hotwords and phrases: `Hotwords (English).xml` and `Hotphrases (English).xml`. Once you have imported these files into Compliance Accelerator, you can edit or delete the hotwords and add new ones.

For optimum performance, shorten the hotword list so that it contains only those words that interest you. Searching for every word in the predefined list greatly reduces the speed with which Compliance Accelerator undertakes searches.

To import the predefined hotwords

- 1 Click the **Configuration** tab in the Compliance Accelerator client, and then click the **Import Configuration** tab.
- 2 In the **Configuration file** box, type the full path to the XML file that you want to import, or click **Browse** and then choose the file to import. The path can contain up to 250 characters.

Both the supplied files are typically in this folder on the Compliance Accelerator server:

```
C:\Program Files (x86)\Enterprise Vault Business  
Accelerator\AcceleratorAdminWeb\Installation
```

You can specify a UNC path or NTFS path to the file if it is stored on a remote computer. For example:

```
\\server2\EVBA\AcceleratorAdminWeb\Installation\Hotwords  
(English).xml
```

- 3 If you want to clear the import information from previous imports before you proceed, check **Clear log before import**.
- 4 Click **Import**.

Compliance Accelerator imports the contents of the files as global hotwords and phrases, and creates the global hotword sets Default Hotwords and Default Hotphrases.

Configuring how Compliance Accelerator handles email addresses

To determine whether addresses are internal or external addresses, Compliance Accelerator uses the SMTP address domains that are associated with the system mailbox under which the Enterprise Vault Journaling Task is running. For example, suppose that the Journaling Task runs under a Vault Service account that is called "vaultadmin", which has the SMTP address VaultAdmin@exampleinc.com. Compliance Accelerator recognizes as internal any address with one of the following formats:

- *@exampleinc.com
- *[*.]exampleinc.com

where [*.] means that the string can be repeated, as in john.doe@sales.emea.exampleinc.com. Any other addresses are treated as external.

Table 5-2 uses the example domain to show how Compliance Accelerator classes addresses:

Table 5-2 Compliance Accelerator classification of addresses

Address	Format matched	Result
miles@exampleinc.com	*@exampleinc.com	Internal
tony@example.com	No match	External
wayne@sales.exampleinc.com	*@[*.]exampleinc.com	Internal
herbie@salesexampleinc.com	No match	External

You can add domains in the following ways to ensure that Compliance Accelerator treats an address as internal:

- Add an additional SMTP alias address with the required domain to the Enterprise Vault Journaling Task user in Active Directory, Exchange Administrator, or the Lotus Domino LDAP directory. This is the recommended way to add internal domains.
- Use the InternalSMTPDomains registry value. You must set this value on each computer on which the Journaling Connector is installed. Setting this registry value is mandatory if you have installed the Domino Journaling Connector, but it is optional if you have installed the Exchange Journaling Connector.

To add internal domains using the InternalSMTPDomains registry value

- 1 Open the registry editor.
- 2 Create a string value that is called InternalSMTPDomains under the following key:

```
HKEY_LOCAL_MACHINE\Software\KVS\Enterprise Vault\Agents
```

- 3 Give InternalSMTPDomains a value that specifies the required domains as a semicolon-delimited string.

For example, you would set the value to the following to treat addresses like jld@eng.uk.eginc.com and kv@hq.eg.parentcorp.com as internal:

```
eginc.com;eg.parentcorp.com
```


Manually reviewing items

This chapter includes the following topics:

- [About reviewing with Compliance Accelerator](#)
- [About the Review pane](#)
- [Filtering the items in the Review pane](#)
- [Assigning review marks to items](#)
- [Adding comments to items](#)
- [Viewing the history of items](#)
- [Displaying printable versions of items](#)
- [Downloading the original versions of items](#)
- [Copying the item list to the Clipboard](#)
- [Changing how the Review pane looks](#)
- [Setting your Review pane preferences](#)
- [Escalating items](#)
- [Storing reviewing comments for reuse](#)

About reviewing with Compliance Accelerator

After you have performed a search and gathered together the potentially relevant items, selected individuals can review the search results. These reviewers read each item, select the appropriate status mark to assign to it, and add a comment as necessary. Items can be reviewed more than once, and other reviewers can add more comments or change the assigned mark.

If you assign supervisors to departments, they can assess the marks and comments that reviewers have applied and add appraisal marks and comments.

A standard Compliance Accelerator system comes with a number of predefined reviewing roles: department reviewer, escalation reviewer, exception reviewer, and passive reviewer. These roles have the following characteristics:

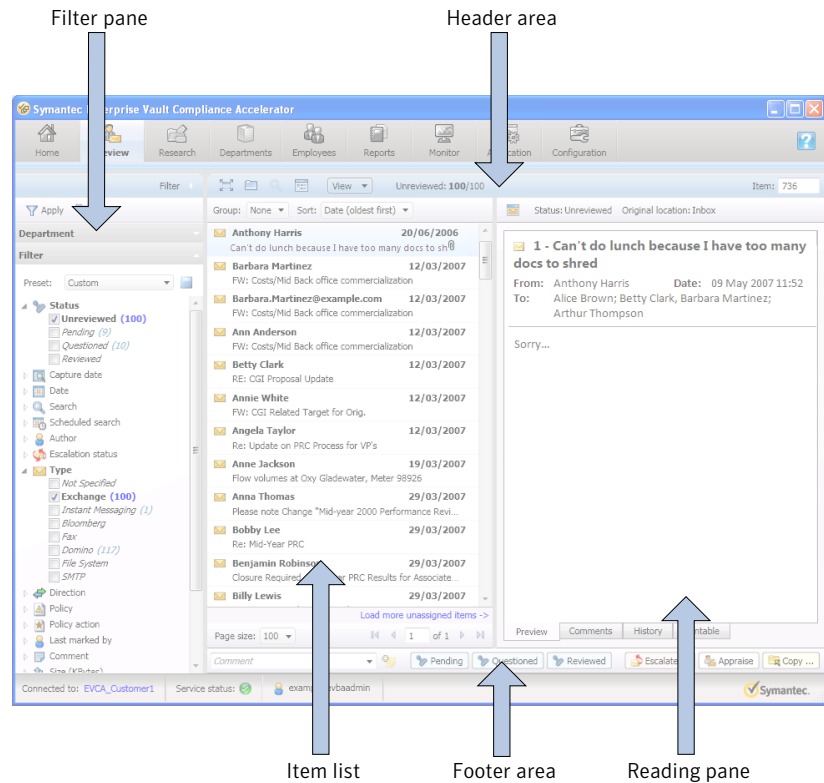
- All roles except the passive reviewer role permit a user to assign review marks to items.
- Passive reviewers can view items and review history, but they cannot assign or change review marks. However, passive reviewers can assign appraisal marks to the items that other users have reviewed.
- Exception reviewers can view the items of their assigned exception employees only.
- Escalation reviewers can receive items that other reviewers in the department have escalated to a higher authority for further review.

To access the Review pane

- ◆ Click the **Review** tab in the Compliance Accelerator client.

About the Review pane

The Review pane lets you review and mark the items in a review set. The pane is divided into the following areas:



Header area

The header area provides options for customizing the view and selecting different items to display.



Maximizes the Review pane by hiding the button bar across the top of the Compliance Accelerator window. Click the button again to restore the button bar.



Lets you view the items that you have copied to a research folder for further investigation.

See [“About research folders”](#) on page 123.





Lets you perform a search that is based on the currently selected item.



Sets your preferences for the Review pane.

See [“Setting your Review pane preferences”](#) on page 116.

View	Lets you hide or change the position of the Reading pane and set the size of the text to display in it.
Unreviewed	Shows the number of items in the list that you have yet to review.
Item	Shows the Compliance Accelerator ID of the highlighted item. If you know the ID of an item that you want to review, type it here and then press the Enter key to display the item.
Group	<p>Groups the items in the list by date, author, subject, or the policy action with which policy management software has tagged them.</p> <p>Display or hide the items in a group by clicking the down-arrow or up-arrow button at the left.</p>
Sort	In lists where you have chosen not to group the items, lets you sort the items by date, author, subject, or policy action.
	Downloads the current item in its original form and opens it in the appropriate application. You can also download an item by right-clicking the item and then clicking View original .
	Sends the current item for printing.
Mark	Shows the mark that is assigned to the current item.
Status	Shows the status of the current item.

Filter pane

The filter pane provides a large number of criteria by which you can filter the items in the list. The number next to each filter option shows the number of matching items that Compliance Accelerator will add to the item list when you apply the selected filters.

See [“Filtering the items in the Review pane”](#) on page 108.

Item list

The item list shows the items in the review set that match the filter options you have selected. Unreviewed items display in bold text.

Note: Compliance Accelerator stores the date and time values for items as Coordinated Universal Time (UTC). However, in the item list and right-hand Preview pane, it converts these values according to your computer's local time zone setting. As a result, two Compliance Accelerator reviewers in different time zones may see different dates and times for the same items.

This is the expected behavior, and it is identical to the way that applications like Microsoft Outlook show the dates and times of items.





Reading pane

The tabs at the bottom of the Reading pane have the following functions:

Preview	Displays an HTML preview of the current item.
Comments	Shows the comments that reviewers have assigned to the current item.
History	Displays the comment and audit history of the current item.
Printable	Displays a printable version of the current item.

Footer area

The footer area provides facilities for navigating from one item to another and applying marks and comments to those items.

	Displays the first page of items for review.
	Displays the previous page of items for review. Pressing the key sequence Alt+z performs the same function.
<i>n of m</i>	Shows the number of the currently displayed page and the total number of pages. To go to a particular page, type its number in the box and then press Enter.
	Displays the next page of items for review. Pressing the key sequence Alt+x performs the same function.
	Displays the last page of items for review.

Comment

Lets you type a comment to add to the selected items.

In the item list, the comment indicator symbol in the **Comment Present** column indicates that one or more comments have been added to the items.

Pending/Questioned/
Reviewed

Applies the required mark to the selected items.

You can mark several items at once if you have Apply Bulk Review Action permission.



If displayed, lets you assign the selected items to one or more escalation reviewers for further audit and review.



If displayed, lets a compliance supervisor mark an item as having being appraised.



If displayed, lets you delete one or more items from the review set.



If displayed, lets you commit to the review set either the selected items or all the items in the research folder for other reviewers to see.



If displayed, lets you assign an escalated item to another escalation reviewer.



If displayed, lets you close an escalated item once you have finished work on it. A closed item is still visible to other escalation reviewers, but they can only perform actions on it if a department reviewer re-escalates the item.



If displayed, lets you select a folder in which to copy either the selected items or all the items in the current review set.

Filtering the items in the Review pane

The options at the left of the Review pane provide a large number of criteria with which you can filter the items for review.

To filter the items in the Review pane

- 1 In the **Mode** drop-down list, choose whether to perform a standard review of the items in the review set or an escalation review.



Escalation Review mode is available to escalation reviewers only. It lets these reviewers view and mark the items that other reviewers have escalated to them for further attention.











- 2 In the **Department** drop-down list at the top of the filter pane, select the department or folder for which you want to display the items in the review set.
- 3 In the **Items** drop-down list, select a group of items that you want to review. The options are as follows:







Temporary Assignment	This option lets you reserve the specified number of items in the review set. Other reviewers cannot see these items until you have finished work on them.
All Items	<p>This option lets you view all the items in the review set, even if they have been assigned to other reviewers.</p> <p>You may duplicate the work of other reviewers if you use this option. Therefore, we recommend that you select this option only if there are no other reviewers working alongside you, or you want to browse the items without marking them.</p>

- 4 In the **Filter** section, select the *facets* (item classifications) that you want to apply. To show the available values, click the facet name or the arrow at the left of the name.

The following table lists all the available facets in alphabetical order.

 Author	Selects items by the name of the person who sent them.
 Capture date	Selects items that Compliance Accelerator has captured over the specified period.

	Capture method	<p>Selects items by the method that Compliance Accelerator has used to capture them and add them to the review set. The options are as follows:</p> <ul style="list-style-type: none"> ■ Search. Selects items that have been captured as a result of searches. ■ Random Sampling. Selects items that Compliance Accelerator has captured and added to the review set according to your designated monitoring policy. ■ Ad-hoc. Selects items that have been added to research folders. ■ Guaranteed Sample Search. Selects the results of guaranteed sample searches.
	Comment	Selects items to which reviewers have added comments.
	Date	Selects items by the date on which they were created.
	Direction	<p>Selects items that have traveled in the specified direction. The options are as follows:</p> <ul style="list-style-type: none"> ■ Internal. Selects items where the author and all recipients are internal to your organization. ■ External Inbound. Selects items where the author is external to your organization and at least one recipient is internal. ■ External Outbound. Selects items where the author is internal to your organization and at least one recipient is external.
	Escalated by	Selects items by the person who escalated them to an escalation reviewer for further attention.
	Escalation owner	Selects items by the escalation reviewer who has responsibility for them.
	Escalation status	Selects items by whether they have been escalated to an escalation reviewer or subsequently closed by that reviewer.
	Last marked by	Select items by the reviewer who last assigned a mark to them.
	Number of attachments	Selects items by the number of attachments that they have.
	Policy	Selects items by the policy with which your policy management software has tagged them.

	Policy action	<p>Selects items by the policy action with which your policy management software has tagged them. This action can be one of the following:</p> <ul style="list-style-type: none"> ■ Include (demands or suggests capture in the review set). ■ Exclude (precludes capture or advocates non-capture in the review set).
	Scheduled search	Selects items that one or more scheduled searches have captured.
	Search	Selects items that one or more searches have captured.
	Size (KBytes)	Selects items by their size in kilobytes.
	Status	Selects items by their status, such as Pending, Questioned, or Reviewed.
	Type	Selects items by their type.

Note the following:

- Each facet value is a hyperlink that, when clicked, selects that value and immediately filters the item list accordingly. Click the facet value again to remove it from the filter.
If you have already selected one or more values within the same facet, clicking another one deselects the others. However, it does not affect any values that you have selected within other facets.
- The numbers next to the facet values show the number of matching items. After you apply the filter, Compliance Accelerator updates these numbers to show how many of the items are now in the item list. For example, the values for the Author facet initially show the number of matching items in the entire review set. If you then set the value of the Status facet to Unreviewed and apply this filter, the Author values are updated to show only the number of unreviewed items for each author.
Facet values that are shown in an italicized font do not have any matching items in the current item list.
- When you select two or more values for a facet, Compliance Accelerator looks for items that match any of the values. For example, you can choose to view all the items that have a status of Pending or Questioned by selecting both values.
When you select values for two or more different facets, Compliance Accelerator looks for items that match all the facets. For example, selecting

the status value Pending and the type value Exchange matches only those items that have a status of Pending and a type of Exchange.

- When a facet has a large number of possible values, Compliance Accelerator displays an abbreviated list of the most relevant values. You can add more values to the list by clicking the blue hyperlinks at the end of the list.
- If you frequently use the same facet settings to filter the items in the Review pane, you can save them as a preset by clicking the **Save** button at the right of the **Preset** box. Then you can quickly apply the settings by selecting the preset from the drop-down list.
- You can apply marks to items by right-clicking the facet values. For example, to mark all the items by a particular author, right-click the author's name in the list and then click **Mark all items**.

5 Click **Apply** at the top of the filter pane.

Assigning review marks to items

As part of the review process, you assign a status mark to each message to indicate that you have reviewed it and have no concerns—or conversely, that you do have some concerns, and therefore want to question the message.

The permissions that are assigned to you determine whether you can assign a status mark to more than one message at a time. If you have the Apply Bulk Review Action permission, you can mark several messages at once, whereas the Apply Review Action permission limits you to marking the messages one at a time. By default, compliance supervisors, department reviewers, and exception reviewers have both permissions.

Tips:

- In the item list, the headers of unreviewed items display in bold text.
- You can quickly mark all the items that match a certain filter option by right-clicking that option in the left pane and then selecting the required mark.
- If you right-click an item in the list view, you can access additional commands for bulk-marking the items in the review set.

To assign a review mark to an item

- 1 In the Review pane, select the items that you want to mark.

To select multiple adjacent items, click the first item, and then hold down the Shift key and click the last item. To select nonadjacent items, click the first item, and then hold down the Ctrl key and click additional items. To select all the items, press Ctrl+A.
- 2 Click the required mark at the bottom right of the pane. After a few moments, Compliance Accelerator changes the status of the items accordingly.

Adding comments to items

As well as assigning a review mark to an item, you can add a comment to it.

The permissions that are assigned to you determine the types of comments that you can add. If you have the Add Own Review Comments permission, you can add comments in your own words. If you have the Add Standard Review Comments permission, you can select the comments to add from a predefined list. By default, users with the role of compliance supervisors, department reviewers, and exception reviewers have both permissions.

To add a comment to an item

- 1 In the Review pane, select one or more items to which you want to add a comment.
- 2 In the **Comment** box at the bottom of the pane, type a new comment or choose from a list of predefined comments, depending on your permission level.
- 3 Click the button at the right of the **Comment** box.

Compliance Accelerator displays a comment indicator in the **Comment present** column of the item list to show that you have added the comment.

Click the **Comments** tab at the bottom of the Reading pane to view the comments assigned to an item. You can also customize the item list columns to add a column that shows the comments on items.

Viewing the history of items

Compliance Accelerator provides ready access to historical information on a selected item, such as the dates and times at which the reviewers assigned marks and comments to it.

To view the history of an item

- 1 In the Review pane, select the item whose history you want to view.
- 2 Click the **History** tab at the bottom of the Reading pane.
Compliance Accelerator displays the following details:
 - The subject, date, and details of the sender and recipients.
 - The item type, such as Microsoft Exchange or Bloomberg, and its direction (Internal, ExternalInbound, or ExternalOutbound).
 - The department in which Compliance Accelerator captured the item.
 - When and how Compliance Accelerator captured the item.
 - The ID of the item within Compliance Accelerator.
 - The original location from which the item was archived.
 - The status history of the item, including the reviewers who marked the item and the date and time at which they did so.
 - If you have the appropriate permissions, additional information on when the item was appraised or escalated.
 - Any policy and policy action with which your policy management software has tagged the item.

Displaying printable versions of items

You can display the contents of items in a form that is suitable for printing.

To display a printable version of an item

- 1 In the Review pane, select the item that you want to print.
- 2 Click the **Printable** tab at the bottom of the Reading pane.
Compliance Accelerator displays a printable version of the item.
- 3 Click the **Print** button at the top of the Reading pane to send the item for printing.

Downloading the original versions of items

As well as viewing an HTML rendering of an item, you can download it in its original form to your computer. Note that downloaded items do not include any audit information, such as the comments that reviewers have assigned to them. If you want to obtain both an item and its audit information, you must export it from Compliance Accelerator.

You must have the Review Messages permission to download items. By default, all reviewers and supervisors have this permission.

To download the original version of an item

- ◆ In the Review pane, do one of the following:
 - Click the item that you want to download and then click the **View original item** button above the Reading pane.
 - Right-click the item and then click **View original**.

Compliance Accelerator downloads the item to your computer and displays it using the appropriate application.

Copying the item list to the Clipboard

You can copy one or all of the rows in the item list to the Windows Clipboard, and then paste them into a spreadsheet application like Microsoft Excel. The copied information includes additional information that Compliance Accelerator does not display in the list, such as the Enterprise Vault saveset identity of each item. Regardless of whether you have chosen to hide some of the columns in the item list, all the information is copied.

To copy the item list to the Clipboard

- 1 In the Review pane, do one of the following:
 - To copy a single row in the item list, right-click it and then click **Copy items details to clipboard**.
 - To copy all the rows, first press Ctrl+A to select them all. Then right-click and click **Copy items details to clipboard**.
- 2 Open the application in which you want to paste the information.
- 3 Paste the information in the normal way.

Changing how the Review pane looks

You can customize the appearance of the Review pane to suit the way you work and help you find items quickly.

Table 6-1 How to customize the Review pane

To do this	Do this
Expand the Review pane to occupy the available space	Click the Expand Reviewing Screen button above the item list.

Table 6-1 How to customize the Review pane *(continued)*

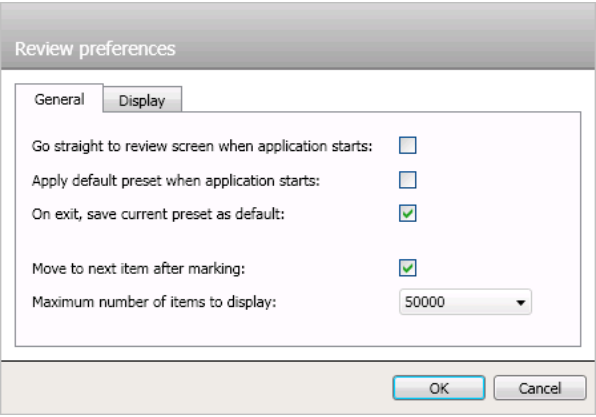
To do this	Do this
Change the position of the Reading pane.	<p>Click View above the item list, and then point to Reading Pane Layout and select the required position.</p> <p>You can position the Reading pane at the bottom or right of the main window, or detach it from the main window and display its contents in a new window.</p>
Change the size of the text in the Reading pane.	<p>Click View above the item list, and then point to Size of Reading Pane Text and select the required size.</p>
Hide or show columns in the item list.	<p>Right-click any column heading in the item list and then point to Select columns and select the columns to hide or show. Then click Apply changes.</p>
Sort the items in the item list.	<p>Click a column heading in the item list to sort the items by the entries in the column.</p> <p>The direction of the arrow in the column heading indicates whether the entries are sorted in ascending or descending order.</p>
Group the items by date, author, subject, or policy action.	<p>Select the required option in the Group box above the item list.</p> <p>Display or hide the items in a group by clicking the arrow at the left of the group.</p>
Specify the maximum number of items to display per page.	<p>In the Page Size box below the item list, select the required number of items.</p>

Setting your Review pane preferences

Compliance Accelerator provides extensive facilities with which you can customize the appearance and operation of the Review pane.

To set your Review pane preferences

- 1
- Click the **Review Preferences** button in the header area of the Review pane.
- The Review preferences dialog box appears.



2 Select your required options on the **General** tab. The options are as follows:

Go straight to review screen when application starts	When selected, lets you proceed directly to the Review pane when you start Compliance Accelerator.
Apply default preset when application starts	When selected, applies the default filter options to the items in the item list.
On exit, save current presets as default	When selected, saves the current filter options as the default options for the Review pane.
Move to next item after marking	When selected, causes Compliance Accelerator to display the next item in the list automatically when you mark an item.
Maximum number of items to display	Sets a limit on the number of items that you can display in the Review pane.

3 Select your required options on the **Display** tab. The options are as follows:

Font	Sets the font to use for all buttons and labels in the Review pane.
Item list font	Sets the font to use in the item list.
Reading pane font	Sets the font to use in the Reading pane.

Item list display type	<p>Specifies whether Compliance Accelerator displays the items in the list in a single-line layout or multiline layout. The multiline layout displays item information over two lines. The first line displays the sender, and the second line displays the text from the Subject box of the item header.</p> <p>If you select Automatic, Compliance Accelerator automatically switches to the multiline layout when there is insufficient screen space to display a header in a single line.</p>
Highlight search terms in reading pane	<p>Turns on or off highlighting for search terms.</p>
Use pop-up for text input	<p>Determines what happens when you type characters in the text input boxes in the Review pane, such as the Comment box. When this option is checked, Compliance Accelerator displays the characters in a separate pop-up window as you type them. This lets you view all the characters at once, instead of hiding older characters as you type new ones.</p>
Hide text on action buttons	<p>When selected, removes the text labels from the action buttons that are below the Preview pane.</p>
Show original location in reading pane	<p>When selected, provides additional information above the Preview pane on the location from which the current item was archived.</p>

4 Click **OK**.

Escalating items

Compliance Accelerator lets you escalate an item that you are reviewing to one or more higher authorities, called *escalation reviewers*, for further attention. After you have escalated an item, you can continue to perform the reviewing actions on it that your permissions allow. For example, if you have the required permissions, you can assign a review mark or add a comment to an escalated item. However, you cannot escalate the item again until an escalation reviewer chooses to close the escalation.

All escalated items are visible to all escalation reviewers.

You must have the Escalate Messages permission to escalate items. By default, department reviewers and exception reviewers have this permission.

To escalate an item

- 1 In the Review pane, select one or more items that you want to escalate.
- 2 Click the **Escalate** button at the bottom right of the pane.
- 3 Select one or more escalation reviewers to whom you want to assign the items. If you choose the **[Default]** option, Compliance Accelerator assigns the items to the default nominees for escalations within the department.
- 4 Click **OK**.

Assigning escalated items to other escalation reviewers

If you are an escalation reviewer, you can reassign an item that has been escalated to you so that another escalation reviewer has ownership of it. Note that having ownership of an escalated item does not prevent any other escalation reviewer from working on it. However, as Compliance Accelerator lets you filter the review set by escalation owner, you may find that reassigning ownership helps you to sift out the items that do not interest you.

To assign an escalated item to another escalation reviewer

- 1 In the **Mode** drop-down list at the left of the Review pane, ensure that **Escalation review** is selected.
- 2 Select one or more items that you want to assign to another reviewer.
- 3 Click the **Assign to another reviewer** button at the bottom right of the pane.
- 4 Select one or more escalation reviewers to whom you want to assign the items. If you choose the **[Default]** option, Compliance Accelerator assigns the items to the default nominees for escalations within the department.
- 5 Click **OK**.

Closing escalated items

If you are an escalation reviewer, you can close escalated items after you have finished work on them. A closed item is still visible to other escalation reviewers, but they can only perform actions on it after a department reviewer has reescalated it.

To close an escalated item

- 1 In the **Mode** drop-down list at the left of the Review pane, ensure that **Escalation review** is selected.
- 2 Select one or more items that you want to close.
- 3 Click the **Close** button at the bottom right of the pane.

Storing reviewing comments for reuse

When they work on a set of items, your reviewers may find it tedious to type the same comments over and over. You can speed up the reviewing process by storing the text of common comments, ready for your reviewers to apply to the items on which they work. Note that these reviewers must have the Add Standard Review Comments permission to apply the comments that you set up.

You must have the Manage Reviewing Comments permission to set up reviewing comments. By default, users with the application role of App Rule Admin have this permission.

To store a reviewing comment

- 1 Click the **Application** tab in the Compliance Accelerator client, and then click the **Reviewing Comments** tab.
- 2 Click **New Comment**.

The Reviewing Comment Details pane appears.



Reviewing Comment Details

Summary (optional). This is the wording the reviewer sees as the comment to apply. If not specified, the summary will be an abridged form of the complete comment:

The review comment; this is the actual wording applied as the comment:

Save Cancel

- 3 In the pane at the right, type an optional summary of the comment containing up to 100 characters.

This summary appears in the **Comment** box at the bottom of the Review pane. If you do not type a summary, Compliance Accelerator abridges the content of the comment and presents this as the summary.

- 4** In the review comment box, type the full text of the comment itself. This can contain up to 1024 characters.
- 5** Click **Save**.

Working with research folders

This chapter includes the following topics:

- [About research folders](#)
- [Creating research folders](#)
- [Copying items to research folders](#)
- [Reviewing the items in research folders](#)
- [Exporting items from research folders](#)
- [Giving other users access to your research folders](#)
- [Committing research folder items to the department review set](#)

About research folders

By creating one or more research folders, you can work privately on the items that interest you without generating additional work for other reviewers. For example, suppose that you are pursuing an alleged instance of insider trading. Rather than add a large number of search results to the review set, where they are visible to other reviewers, you can conduct the searches from a research folder and store the results there. Then you can review and mark the items in the normal way, or export them for offline review.

Finally, when you have finished with the items, you can commit them to the department review set for other reviewers to see.

Where necessary, you can give other users access to your research folders so that they can collaborate in the review process. The permissions that you grant these

users determine whether they can export items from the folder, search for more items to add to it, and review and mark the items.

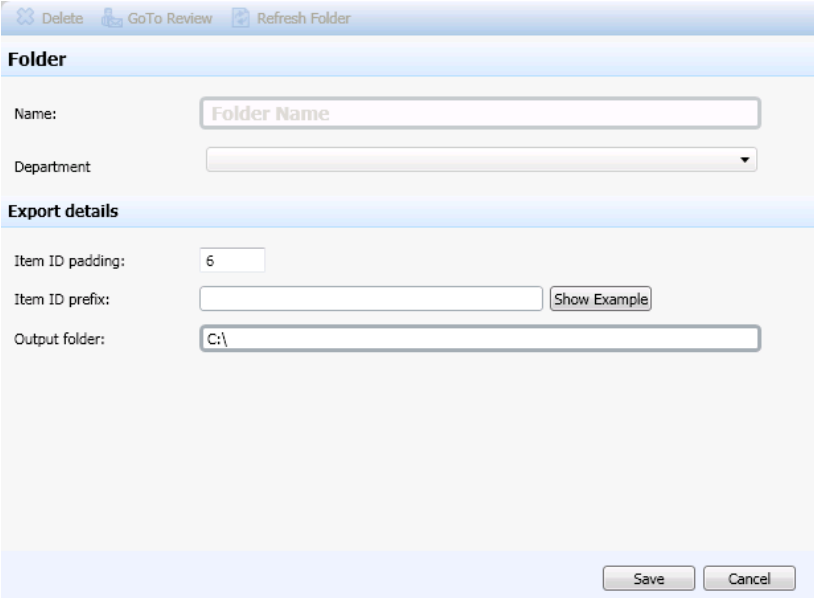
Creating research folders

Compliance Accelerator provides several methods for creating folders. In addition to the method described below, you can also create new folders when you define the criteria for searches, accept the search results, and review items.

To create a research folder

- 1 Click the **Research** tab in the Compliance Accelerator client.
- 2 In the left pane, click **All Research**.
- 3 Click **New** at the top of the window.

The folder properties pane appears.



The screenshot shows the 'Folder' properties pane in the Compliance Accelerator client. At the top, there are three buttons: 'Delete', 'GoTo Review', and 'Refresh Folder'. Below these is the 'Folder' section with a 'Name' field containing 'Folder Name' and a 'Department' dropdown menu. The 'Export details' section follows, with 'Item ID padding' set to '6', 'Item ID prefix' with a 'Show Example' button, and 'Output folder' set to 'C:\'. At the bottom right are 'Save' and 'Cancel' buttons.

- 4 In the **Name** box, type a name for the folder.
- 5 In the **Department** box, select the department with which to associate the folder. You must have the Perform Ad Hoc Searches permission in this department.

- 6 Specify a location in which you want to store any items that you export from the folder.
- 7 Click **Save**.

Copying items to research folders

You can copy items from the review set to a personal folder for further research. You can then review and mark the items, export them for offline review, search for more items that are related to the copied ones, and more.

You must have the Perform Ad Hoc Searches permission in the department to copy items from its review set to your folder. By default, compliance supervisors, department reviewers, and exception reviewers have this permission.

To copy an item to a research folder

- 1 In the Review pane, select one or more items that you want to copy to a folder.
To select multiple adjacent items, click the first item, and then hold down the Shift key and click the last item. To select nonadjacent items, click the first item, and then hold down the Ctrl key and click additional items. To select all the items, press Ctrl+A.
- 2 Click **Copy** below the preview pane.
- 3 Select the destination folder to which you want to copy the items.
- 4 Choose to copy the selected items only or all the items in the review set.
- 5 Click **Copy**.

Reviewing the items in research folders

You review the items in a folder in exactly the same way that you review the items in the review set.

In each case, you can apply review marks and comments to the items, and you can escalate them to an escalation reviewer for further consideration. However, you cannot mark the items in a folder as Appraised.

You must have the Review permission in the folder to review the items in it. By default, users with the Folder Full Control or Folder Review role have this permission.

To review the items in a research folder

- 1 Click the **Research** tab in the Compliance Accelerator client.
- 2 In the left pane, click the folder whose items you want to review.

- 3 Click the **Properties** tab.
- 4 Click **Go To Review**.
- 5 In the Review pane, review the items as you normally would do.
See [“About the Review pane”](#) on page 104.

Exporting items from research folders

If you want to review items offline or present them in evidence to a third party, you must export them. You can export the items in several different formats, including PST, Domino NSF database, HTML, and MSG. If you export to HTML, you can export review marking information along with each item.

Exporting does not affect the status of items, and you can continue to work on those that you have exported.

You must have the Export Messages permission in the folder to export items from it. By default, users with the Folder Full Control or Folder Export role have this permission.

To export the items from a research folder

- 1 Click the **Research** tab in the Compliance Accelerator client.
- 2 In the left pane, click the folder from which you want to export some items.
- 3 Click the **Export** tab.
- 4 Click **New**.
- 5 Enter the required run details and filter information.

Compliance Accelerator exports items to a folder on the Compliance Accelerator server rather than to a folder on the computer where you are running the client. If you use the same output folder and export run name for multiple runs, Compliance Accelerator overwrites the report summary each time. It is therefore advisable to give each run a different name.

The output folder path can contain up to 100 characters.

- 6 Click **Apply**.
- 7 Click **OK** to export the specified number of items.
- 8 Wait a few moments for processing to finish, and then browse to the output folder on the Compliance Accelerator server to retrieve the exported items.

Giving other users access to your research folders

You can give other users access to your folders by assigning roles to them. For example, anyone who wants to review and mark the items in a folder must have the Review role in that folder. Other roles permit users to export items from the folder and search for new items to add to it. The Full Control role combines all these permissions in one role.

You must have the Role Assignment permission in the folder to give other users access to it. By default, users with the Folder Full Control role have this permission.

To give another user access to a research folder

- 1 Click the **Research** tab in the Compliance Accelerator client.
- 2 In the left pane, click the folder to which you want to give access.
- 3 Click the **Role Assignment** tab.
- 4 Click the name of the user to whom you want to assign a role.
If the user does not appear in the list, click **Add** at the top of the pane and then select the user to add to it.
- 5 In the right pane, do one of the following:
 - Click **Add** to assign a new role.
 - Click **Remove** to remove the selected role.
- 6 Click **Save**.

Committing research folder items to the department review set

Having worked on the items in a research folder, you can commit them to the department review set for all other Department Reviewers to see. As well as the items themselves, Compliance Accelerator commits all the review marks, appraisal marks, and comments that you have applied to them. In fact, you can only commit items that you have marked in some way. Items with a status of Unreviewed are not yet ready to be committed.

You must have the Commit Appraised Folder Messages or Commit Reviewed Folder Messages permission in the folder, depending on the type of item you want to commit. By default, users with the Full Control or Commit Messages role have this permission.

To commit research folder items to the department review set

- 1** Click the **Research** tab in the Compliance Accelerator client.
- 2** In the left pane, click the folder whose items you want to commit.
- 3** Click the **Properties** tab.
- 4** Click **Go To Review**.
- 5** In the Review pane, select one or more items that you want to commit.

To select multiple adjacent items, hold down the Shift key and click the first and last item in the range. To select multiple, nonadjacent items, hold down the Ctrl key and click the required items.
- 6** Click the **Commit items from the folder to the department** button below the preview pane.
- 7** Choose whether to commit all the review marks, appraisal marks, and comments that you have applied to the items as well as the items themselves.

You can also choose whether to commit the selected items only or all the items in the department, and whether to remove the items from the folder after you have committed them to the department review set.
- 8** Click **Commit**.

Exporting items

This chapter includes the following topics:

- [About exporting items](#)
- [Performing an export run](#)
- [About the limits on the number of simultaneous export runs](#)
- [How to optimize export runs](#)
- [Exporting items from the review set of an exception employee](#)
- [Making the export IDs visible in Microsoft Outlook](#)

About exporting items

If you want to review items offline or present them in evidence to a third party then you must export them from Compliance Accelerator. Compliance Accelerator supports a number of file formats for exporting content. You can export all content in its native format or as an HTML rendering of the content. Export to HTML if you want to export review marking information and comments along with each item.

Performing an export run

If you want to review items offline or present them in evidence to a third party, you must export them from Compliance Accelerator. There are several output formats from which to choose, including PST, Domino NSF database, HTML, and MSG. Exporting the items as HTML lets you export review marking information along with each item.

As well as exporting the selected items, Compliance Accelerator also outputs some reports in HTML, plain-text, and XML formats. All three reports list the items that you have exported, and the HTML report provides hyperlinks to the items.

You must have the Export Messages permission to export items from a department. By default, all the reviewers and supervisors in the department have this permission. However, the option to export escalated items is available to those with the Export Escalations permission only. By default, only users with the role of escalation reviewer have this permission.

To perform an export run

- 1 Click the **Departments** tab in the Compliance Accelerator client.
- 2 In the left pane, click the department from which you want to export items.
If Compliance Accelerator lists a lot of departments, you can filter the list with the fields at the top of the pane. As well as filtering the departments by name, you can choose whether to list any research folders that are associated with them.
- 3 Click the **Export** tab.
- 4 Click **New** at the top of the window.

The Export Details pane appears.

Export Details

Name:

Output folder:

Items Selection

Item ID:	<input type="text" value=""/>
Message type:	<input checked="" type="checkbox"/> Microsoft Excha... <input checked="" type="checkbox"/> Instant Messagi... <input type="checkbox"/> SMTP <input type="checkbox"/> Domino <input type="checkbox"/> Bloomberg <input type="checkbox"/> Unspecified/Pre... <input type="checkbox"/> File system <input type="checkbox"/> Fax <input type="checkbox"/> Sharepoint
Message direction:	<input type="text" value="All"/>
Capture method:	<input type="text" value="All"/>
Policy Action:	<input checked="" type="checkbox"/> Include <input checked="" type="checkbox"/> Exclude <input checked="" type="checkbox"/> No Action <input checked="" type="checkbox"/> Not Specified
Date captured:	<input type="text" value="All"/>
Search:	<input type="text" value="All"/>
Current action status:	<input type="text" value="All"/>
Current action status author:	<input type="text" value="All"/>
Escalation Status:	<input type="text" value="All"/>
Escalation owner:	<input type="text" value="All"/>

- 5 In the **Name** box, type a name for the run.

The name that you specify here becomes the name of the subfolder in which Compliance Accelerator stores the output from the run.

- 6 In the **Output folder** box, type the path to the folder on the Compliance Accelerator server in which you want to store the output from the run.

The folder path can contain up to 100 characters.

Compliance Accelerator places the output from the run in a subfolder of the nominated folder.

- 7 In the **Items Selection** box, choose the items that you want to export.

The options are as follows:

Item ID	Specifies the ID of an individual item that you want to export. To determine the ID of an item, view the item in the Review pane.
Message type	Selects items by their type, such as Microsoft Exchange or Fax.
Message direction	Selects items that are traveling in a certain direction.
Capture method	Selects items that have either been captured and added to the review set using the monitoring policy (Randomly Sampled) or captured as a result of searches (Search).
Policy action	Selects items by the policy action with which your policy management software has tagged them. This action can be one of the following: Inclusion (demands or suggests capture), Exclusion (precludes capture or advocates non-capture), and No Action (the item is subject to normal random sampling).
Date captured	Selects items that Compliance Accelerator captured over the specified period.
Search	Selects items that the specified search has captured.
Current action status	Selects items by their action status, such as Unreviewed, Pending, Questioned, or Reviewed.
Current action status author	Selects items by the person who last assigned a review mark to them.

Escalation status	Selects items by whether they have been escalated to an escalation reviewer and subsequently closed by that reviewer.
Escalation owner	Selects items by the escalation reviewer who has responsibility for them.
Escalated by	Selects items by the person who escalated them to an escalation reviewer for further attention.
Current appraisal status	Selects items by whether a supervisor has appraised them. This option is only visible to supervisors with Apply Appraisal Status permission.
Current appraisal status author	Selects items by the supervisor who last assigned a mark to them. This option is only visible to supervisors with Apply Appraisal Status permission.
Policy	Selects items by the specific policy with which your policy management software has tagged them.

- 8 Check **Include journal recipients in reports** if you want the export reports to include recipient information from the journal envelope (P1) of Microsoft Exchange journal items. This lists all the recipients of each item, regardless of their placement in the To, CC and BCC fields.

Compliance Accelerator does not include recipient information from Lotus Domino journal items.

- 9 Choose whether to export the items in their original format or as HTML.

If you click **Original Type**, you can choose to output Microsoft Exchange items as individual MSG files or encapsulate them all in a single Personal Folders (.pst) file.

If you click **PST**, Compliance Accelerator displays some additional options with which you can set a password and a maximum size for the file. The password can contain alphanumeric characters only. The default size of the file is 600 MB, and it cannot exceed 1.5 GB.

If you click **HTML**, Compliance Accelerator displays some additional options with which you can choose to include comments and mark history, and the contents of attachments.

- 10 In the **Number of items to export** box, type the required number of items. Note that Compliance Accelerator exports the oldest items. For example, if you choose to export 100 items, Compliance Accelerator exports the 100 oldest items that match the selected options.

- 11 If you are exporting file system items or Lotus Domino items and want to make them read-only so that they cannot be changed or accidentally deleted, check **Read Only**.
- 12 Click **Apply**.
- 13 When the run has finished, open the output folder on the Compliance Accelerator server to retrieve the exported items. This folder also includes the reports that list the items that you have exported.

About the limits on the number of simultaneous export runs

By default, you can undertake up to four runs simultaneously. When you try to perform additional runs, Compliance Accelerator holds them in a queue until it has completed some of the active runs. Then it undertakes the additional runs in the order in which you initiated them. If you need to perform a high-priority run while the maximum number of runs is already in progress, you can ask a Compliance Accelerator administrator to stop one of those runs so that yours can start.

Compliance Accelerator administrators can change the maximum number of simultaneous runs that it is possible to undertake by setting the following **Export/production** configuration options:

- Number of production threads per production run
- Total number of production threads per customer

To access these configuration options, click the **Configuration** tab in the Compliance Accelerator client, and then click the **Settings** tab. The maximum number of simultaneous runs that you can undertake is the "Total number of production threads per customer" divided by the "Number of production threads per production run".

See ["Export/production configuration options"](#) on page 160.

How to optimize export runs

For the best results when exporting items, follow these guidelines:

- Export to a high-speed drive that is located on the Compliance Accelerator server.
- Avoid conducting multiple export runs at once. If this is unavoidable, store the output from each run on a different drive.

- Export email messages in their original format, if you can. This is much faster than encapsulating the messages in a single Personal Folders (.pst) file. Only export items in HTML format when this is essential.
- If an export fails for any reason, use the **Re-try** facility in preference to the **Re-Export** facility.

Exporting items from the review set of an exception employee

The procedure for exporting the items from the review set of an exception employee differs a little from the standard export procedure.

To export items from the review set of an exception employee

- 1 Click the **Departments** tab in the Compliance Accelerator client.
- 2 In the **Departments** pane at the left, check the filter option **Show Exceptions**.
- 3 Click the name of the exception employee whose items you want to export.
- 4 Click the **Export** tab.
- 5 Create a new export run in the normal way.
- 6 When the run has finished, browse to the output folder to retrieve the exported items.

Making the export IDs visible in Microsoft Outlook

When you view exported Personal Folders (.pst) files in Microsoft Outlook, you may find it helpful to see the export ID that Compliance Accelerator has assigned to each item. You can do this by adding a custom column to the view in Outlook.

The configuration option that is called "PST ExportID Column Name" lets you set the name of the custom column.

See ["Export/production configuration options"](#) on page 160.

To make the export IDs visible in Microsoft Outlook

- 1 Open the exported .pst file in Outlook.
- 2 Right-click the column headers in Outlook, and then click **Field Chooser**.
- 3 Click **New**.
- 4 In the **Name** box in the New Field dialog box, type **Export ID**, and then click **OK**.

- 5 Close the Field Chooser dialog box.
- 6 Right-click the column headers in Outlook, and then click **Customize Current View**.
- 7 Click **Fields** and then, in the **Select available fields from** list, select **User-defined fields**.
- 8 Add the **Export ID** field to the list of displayed fields, and then click **OK** twice to close the dialog boxes.

Creating and viewing reports

This chapter includes the following topics:

- [About the Compliance Accelerator reports](#)
- [Creating Compliance Accelerator reports](#)
- [Available Compliance Accelerator reports](#)
- [Viewing existing reports](#)
- [Deleting reports](#)
- [Viewing legacy reports in Crystal Reports format](#)

About the Compliance Accelerator reports

Compliance Accelerator provides extensive facilities for reporting on the roles and responsibilities of your Compliance Accelerator users and on the progress that reviewers and supervisors have made.

Besides printing the reports, you can export them in a number of formats, including XML, comma-separated values (CSV), Acrobat (PDF), Web archive (MHTML), Excel, and TIFF.

Creating Compliance Accelerator reports

You must have the View Reports permission to generate a new report. By default, most users with a department role have this permission.

To create a Compliance Accelerator report

- 1

Click the **Reports** tab in the Compliance Accelerator client.
- 2

Click **New** at the top left of the window.
- 3

In the **Type** box, select the type of report that you want to create.

See “[Available Compliance Accelerator reports](#)” on page 138.

In some instances, choosing a report type causes additional boxes to appear so that you can define the scope of the report.
- 4

In the **Name** box, type a unique name that contains up to 50 characters.
- 5

If required, type an optional description that contains up to 250 characters.
- 6

Set any remaining report parameters, and then click **Apply**.
- 7

When Compliance Accelerator has generated the report, double-click the report name in the left pane to view it.

Available Compliance Accelerator reports

[Table 9-1](#) describes the reports that accompany Compliance Accelerator.

Table 9-1 Available Compliance Accelerator reports

This report	Shows
Compliance Supervisor Responsibility report	The departments for which each compliance supervisor is responsible. For each of these departments, the reports also lists the reviewers in the department.
Department Roles Detail report	Information on the review settings and role assignments for each of the selected departments.
Department Roles Summary report	A summary of the review settings for each of the selected departments.
Differential Sampling Summary by Department report	For the selected sampling period, information on the sampling activity for the monitored employees in selected departments.
Effective Roles by User report	All the departments in which the selected user has a role, and what those roles are.

Table 9-1 Available Compliance Accelerator reports (*continued*)

This report	Shows
Evidence of <i>message type</i> Review by Department/Employee reports	For the selected department or employee, evidence that the required number and percentage of randomly sampled items have been captured and reviewed.
Item Aging by Department report	For the selected departments, the number of items that are either still unreviewed or pending review.
Message Stats Summary report	For each department and exception employee, the total number of sampled items and a breakdown by item type.
Message Summary report	The number of items that Compliance Accelerator has captured for review in each department, and a breakdown by type.
Monitored IDs by Department report	For each monitored employee, how many of that employee's items have been captured for review.
Questioned Items by Department report	For each department, a summary of the suspect items (those items that reviewers have marked as Questioned).
Responsibility by Department report	For each department, the owner, monitored employees, department reviewers, escalation reviewers, and compliance supervisors.
Responsibility by Reviewer report	For each reviewer, the departments in which he or she can review items, and the other reviewers in those departments.
Review Activity Summary by Department report	The total number of items of each type that Compliance Accelerator has captured in the selected reporting period
Reviewer Activity by Department report	For each department, the status of review set items, including how many items have been escalated, questioned, reviewed, and unreviewed.
Reviewer Activity Detail report	For each department, the status of the review set items for each reviewer.
Reviewer Mapping report	The review requirements and monitored employees in each department in which a reviewer operates.

Table 9-1 Available Compliance Accelerator reports (continued)

This report	Shows
Unreviewed Departments report	The departments to which no department reviewer is assigned.
Unsupervised Departments report	Departments to which no compliance supervisor is assigned.

Compliance Supervisor Responsibility report

The Compliance Supervisor Responsibility report lists the departments for which each compliance supervisor is responsible. For each of these departments, the report also lists the reviewers in the department.

This report provides the following information for each of the selected compliance supervisors.

Table 9-2 Fields in the Compliance Supervisor Responsibility report

This field	Shows
Department	The departments in which the user is a compliance supervisor.
Reviewer	The reviewers in each department.
On Behalf Of	If appropriate, the principal reviewers for whom each reviewer is a delegate.

Department Roles Detail report

For each of the selected departments, the Department Roles Detail report provides information on the review settings and role assignments.

This report provides the following information for each of the selected departments.

Table 9-3 Fields in the Department Roles Detail report

This field	Shows
Department Settings	

Table 9-3 Fields in the Department Roles Detail report (*continued*)

This field	Shows
Message Type	<p>The types of items that Compliance Accelerator may add to the department review set. For Microsoft Exchange, fax, and Lotus Domino, the report shows three item types:</p> <ul style="list-style-type: none"> ■ Internal: The items where the author and all recipients are internal to your organization. ■ External Inbound: The items where the author is external to your organization and at least one recipient is internal. ■ External Outbound: The items where the author is internal to your organization and at least one recipient is external.
Review Requirement	The percentage of each employee's items to capture and add to the review set.
Message Cap	Whether you have chosen to set a limit on the number of each employee's items to capture and add to the review set.
For All Message Types	Whether you have chosen to enable or disable monitoring of all employees in the department (Monitoring); whether you have chosen to set a limit on the total number of items in the review set (Capping); and, in cases where you have chosen to limit the number of items in the review set, what the limit is (Total Messages Cap).
Users and Groups with Roles in this Department	
User/Group	The users or groups that occupy roles in the department.
Role	The roles that the users or groups occupy.
Details of Role Assignment	How the user acquired the role: through explicit assignment, inheritance from a parent department, or membership of a group.

Department Roles Summary report

For each of the selected departments, the Department Roles Summary report provides a summary of the review settings.

This report contains the following fields.

Table 9-4 Fields in the Department Roles Summary report

This field	Shows
Message Type	<p>The types of items that Compliance Accelerator may add to the department review set. For Microsoft Exchange, fax, and Lotus Domino, the report shows three item types:</p> <ul style="list-style-type: none"> ■ Internal: The items where the author and all recipients are internal to your organization. ■ External Inbound: The items where the author is external to your organization and at least one recipient is internal. ■ External Outbound: The items where the author is internal to your organization and at least one recipient is external.
Review Requirement	The percentage of each employee's items to capture and add to the review set.
Message Cap	Whether you have chosen to set a limit on the number of each employee's items to capture and add to the review set.
For All Message Types	Whether you have chosen to enable or disable monitoring of all employees in the department (Monitoring); whether you have chosen to set a limit on the total number of items in the review set (Capping); and, in cases where you have chosen to limit the number of items in the review set, what the limit is (Total Messages Cap).

Differential Sampling Summary by Department report

For the selected sampling period, the Differential Sampling Summary by Department report summarizes the sampling activity for the monitored employees in selected departments.

This report contains the following fields.

Table 9-5 Fields in the Differential Sampling Summary by Department report

This field	Shows
Monitored Employee	The name of the monitored employee.
Total Messages	The total number of items that the monitored employee has sent and received.
Policy Sampled	The number and percentage of items that policy management software has tagged for inclusion in the review set.

Table 9-5 Fields in the Differential Sampling Summary by Department report
(continued)

This field	Shows
Search Sampled	The number and percentage of items that guaranteed sample searches have sampled.
Random Sampled	The number and percentage of items that Compliance Accelerator has randomly sampled.
Total Sampled	The total number and percentage of sampled items.

Effective Roles by User report

The Effective Roles by User report lists all the departments in which the selected user has a role, and shows what those roles are.

This report contains the following fields.

Table 9-6 Fields in the Effective Roles by User report

This field	Shows
Department	The name of the department in which the user has a role.
Role	The department roles that the user occupies.
Detail	How the user acquired the role: through explicit assignment, inheritance from a parent department, or membership of a group.

Evidence of *message type* Review by Department/Employee reports

For the selected department or employee, the Evidence of Review reports provide evidence that the required number and percentage of items of the selected type have been captured and reviewed. These reports include randomly sampled items only (those that the Journaling Connector has collected from the Enterprise Vault Journal mailbox archive).

This report contains the following fields.

Table 9-7 Fields in the Evidence of Review by Department/Employee reports

This field	Shows
Monitored Employee	The name of the monitored employee.

Table 9-7

Fields in the Evidence of Review by Department/Employee reports
(continued)

This field	Shows
Total Messages	The total number of items of the specified type that the monitored employee has sent and received.
Captured	The number and percentage of the employee's items that the Journaling Connector has collected.
Unreviewed	The number of unreviewed items.
Pending	The number of items that have a status of Pending.
Questioned	The number of items that have a status of Questioned.
Reviewed	The number of items that have a status of Reviewed.
% Reviewed	The percentage of items that have been reviewed.

Item Aging by Department report

For the selected departments, the Item Aging by Department report shows the number of items that are either still unreviewed or pending review. The report also gives an indication of how long each item has awaited review since it was first captured.

This report contains the following fields.

Table 9-8

Fields in the Item Aging report

This field	Shows
Total - <i>department_name</i>	The name of the department containing items that are either still unreviewed or pending review.
Number of messages within the capture age range	For each of the 30-day time periods, the number of items that are either still unreviewed or pending review from when they were first captured. The totals do not include any items that have been unreviewed or pending review for 90 days or more.

Message Stats Summary report

For each department and exception employee, the Message Stats Summary report shows the total number of sampled items and provides a breakdown by item type.

This report contains the following fields.

Table 9-9 Fields in the Message Stats Summary report

This field	Shows
<i>department_name</i>	The name of a Compliance Accelerator department. Click the department name to view a list of the sampled items in its review set.
<i>Message type</i> (Exchange Internal, and so on)	<p>The number of sampled items of the specified type. For Microsoft Exchange, fax, and Lotus Domino, the report shows three item types:</p> <ul style="list-style-type: none"> ■ Internal: The items where the author and all recipients are internal to your organization. ■ External Inbound: The items where the author is external to your organization and at least one recipient is internal. ■ External Outbound: The items where the author is internal to your organization and at least one recipient is external.
Total Sampled	The total number of sampled items of all types.

Message Summary report

The Message Summary report provides information on the number of items that Compliance Accelerator has captured for review in each department, and a breakdown by type.

This report contains the following fields.

Table 9-10 Fields in the Message Summary report

This field	Shows
Department: <i>name</i>	The name of the department for which to show the number of items. Click a department name to obtain more information on the items in the review set.
Message Type/Messages	The type and number of items that Compliance Accelerator has captured for review. Click the item type or number of items to see a list of these items.

Monitored IDs by Department report

For each monitored employee, the Monitored IDs by Department report shows how many of that employee's items have been captured for review.

This report contains the following fields.

Table 9-11 Fields in the Monitored IDs report

This field	Shows
Corp ID	The employee's company ID, if known.
Total	The total number of the employee's items that Compliance Accelerator has captured for review. The total includes randomly-sampled items, policy-captured items, and items that were captured through guaranteed sample searches.
Unreviewed	The number of the employee's items that are awaiting review.
Reviewed	The number of the employee's items that have been reviewed.

Questioned Items by Department report

For each department, the Questioned Items by Department report gives a summary of the suspect items (those items that reviewers have marked as Questioned).

This report contains the following fields.

Table 9-12 Fields in the Questioned Items report

This field	Shows
Item ID	The identifying number that Compliance Accelerator has assigned to the item.
Sent Date	The date and time at which the item was sent.
Comment	The last comment that the Compliance Accelerator reviewer has added to the item.
Sender	The person who sent the item.
Recipient(s)	The recipients of the item. Compliance Accelerator lists all the recipients, if possible, but it may truncate the list when there are a large number of recipients.

Responsibility by Department report

For each department, the Responsibility by Department report lists the owner, monitored employees, department reviewers, and more. Departments that have no reviewers are shown as (unreviewed). Delegate reviewers have the tag "On behalf of *reviewer_name*".

This report contains the following fields.

Table 9-13 Fields in the Responsibility By Department report

This field	Shows
Owner	The owner of the department (typically the main system administrator for Compliance Accelerator).
Monitored Employees	The departmental employees whom Compliance Accelerator is monitoring.
Departmental Reviewers	The Compliance Accelerator users who can review and mark the items in the department.
Escalation Reviewers	The Compliance Accelerator users to whom department reviewers can escalate items for further attention.
Compliance Supervisors	The Compliance Accelerator users who can appraise the work of department reviewers and manage any exception employees in the department.

Responsibility by Reviewer report

For each Compliance Accelerator reviewer, the Responsibility by Reviewer report lists the departments in which he or she can review items and identifies the other reviewers in those departments.

This report contains the following fields.

Table 9-14 Fields in the Responsibility by Reviewer report

This field	Shows
Department	The departments in which the user has a reviewer role.
Additional Reviewers	The names of other reviewers in the department.
On Behalf Of	If appropriate, the principal reviewer or supervisor for whom the user is acting as a delegate.

Review Activity Summary by Department report

The Review Activity Summary by Department report shows the total number of items of each type that Compliance Accelerator has captured in the selected reporting period. The report also shows the review status of these items.

This report contains the following fields.

Table 9-15 Fields in the Review Activity Summary report

This field	Shows
Total	The total number of items of the specified type that Compliance Accelerator has captured within the reporting period.
Unreviewed	The number of unreviewed items.
Reviewed	The number of items that reviewers have marked as Reviewed.
Pending	The number of items that reviewers have marked as Pending.
Questioned	The number of items that reviewers have marked as Questioned.

Reviewer Activity by Department report

For each department, the Reviewer Activity by Department report shows the status of review set items, including how many items have been escalated, questioned, reviewed, and unreviewed.

This report contains the following fields.

Table 9-16 Fields in the Reviewer Activity by Department report

This field	Shows
Review Status/Messages	The status and number of items that Compliance Accelerator has captured for review. Click the item status or number of items to see a list of these items.

Reviewer Activity Detail report

For each department, the Reviewer Activity Detail report shows the status of the review set items for each reviewer.

This report contains the following fields.

Table 9-17 Fields in the Reviewer Activity Detail report

This field	Shows
Reviewer	The name of the reviewer or, for the items that are awaiting review, "No reviewer".

Table 9-17 Fields in the Reviewer Activity Detail report (*continued*)

This field	Shows
Message Status	The marking status ("Questioned" or "Reviewed") and escalation status ("Escalated").
Messages	The number of items of the specified status, and the total number of items that this reviewer has either marked or escalated.
Delegation Details	If appropriate, the principal reviewer or supervisor for whom the user is acting as a delegate.
Marking activity total for <i>department_name</i>	The total number of items in the review set that all the department reviewers have marked.
Escalation activity total for <i>department_name</i>	The total number of items in the review set that all the department reviewers have escalated to a higher authority for further attention.

Reviewer Mapping report

The Reviewer Mapping report shows the review requirements and monitored employees in each department in which a reviewer operates.

This report contains the following fields.

Table 9-18 Fields in the Reviewer Mapping report

This field	Shows
Message Type	<p>The types of items that Compliance Accelerator may add to the department review set. For Microsoft Exchange, fax, and Lotus Domino, the report shows three item types:</p> <ul style="list-style-type: none"> ■ Internal: The items where the author and all recipients are internal to your organization. ■ External Inbound: The items where the author is external to your organization and at least one recipient is internal. ■ External Outbound: The items where the author is internal to your organization and at least one recipient is external.
Review Requirement	The percentage of each employee's items to capture and add to the review set.
Message Cap	Whether you have chosen to set a limit on the number of each employee's items to capture and add to the review set.

Table 9-18 Fields in the Reviewer Mapping report (continued)

This field	Shows
For All Message Types	Whether you have chosen to enable or disable monitoring of all employees in the department (Monitoring); whether you have chosen to set a limit on the total number of items in the review set (Capping); and, in cases where you have chosen to limit the number of items in the review set, what the limit is (Total Messages Cap).
Monitored Employees in <i>department_name</i>	For each monitored employee, the percentage of that employee's items to capture and add to the review set. This area of the report also shows the following: <ul style="list-style-type: none">■ The name of the exception reviewer whom you have assigned to the employee, if appropriate.■ Whether or not monitoring of the employee has been suspended.■ Whether or not the employee is exempt from any cap limit that you may have applied to the department that contains the employee.

Unreviewed Departments report

The Unreviewed Departments report lists the departments to which no department reviewer is assigned. Only the departments in which you have View Reports permission are listed.

This report contains the following fields.

Table 9-19 Fields in the Unreviewed Departments report

This field	Shows
<i>department_name</i>	The name of a Compliance Accelerator department. Click the department name to view a list of the sampled items in its review set.
Owner	The owner of the department (typically the main system administrator for Compliance Accelerator).

Unsupervised Departments report

The Unsupervised Departments report lists departments to which no compliance supervisor is assigned. Only the departments in which you have View Reports permission are listed.

Viewing existing reports

Compliance Accelerator makes it easy to view the contents of a report, print it, and export it in formats such as Excel, Acrobat (PDF), XML, and comma-separated values (CSV). Note that a report is a snapshot of data at the time that you created it. Viewing the report later does not refresh the data in it, so you must create a new report if you want to view the latest data.

You must have the View Reports permission to view an existing report. By default, most users with a department role have this permission.

To view an existing report

- 1 Click the **Reports** tab in the Compliance Accelerator client.
- 2 In the center pane, click the report that you want to view. Compliance Accelerator provides information on the selected report in the **Details** tab at the right.

You can filter the list of reports by checking the options in the left pane. Alternatively, in the **Search Reports** box at the top of the center pane, enter a keyword for which to search in the names and descriptions of the reports.

- 3 Click the **Preview** tab to display the contents of the report.
- 4 Do one or more of the following:
 - To page through the report, go to a specific page, find a specific word, or adjust the magnification level, click the navigation controls at the top of the preview pane.
 - To export the report, select the required format and then click **Export**. Compliance Accelerator prompts you to choose a location for the report file.
 - To update the report contents, click **Refresh**.
 - To print the report, click **Print** and then select the printing options that you want.

Deleting reports

When you have no further use for a report, you can delete it from Compliance Accelerator.

You must have the View Reports permission to delete a report. By default, most users with a department role have this permission.

Caution: You cannot recover reports that you accidentally delete.

To delete a report

- 1 Click the **Reports** tab in the Compliance Accelerator client.
- 2 In the left pane, click the report that you want to delete.
- 3 Click **Delete Report** at the top left of the window.
- 4 Click **Yes** to confirm that you want to delete the report.

Viewing legacy reports in Crystal Reports format

If you have any legacy reports in Crystal Reports (.rpt) format that you created with Compliance Accelerator 2007 or earlier, you can view them with the Support for Crystal Reports Web site. You have the option to install this Web site when you install the Compliance Accelerator server software.

To view legacy reports in Crystal Reports format

- 1 Start Internet Explorer.
- 2 Go to the home page of the Support for Crystal Reports Web site (typically, http://server_name/EVBACompliance).

Customizing Compliance Accelerator

This appendix includes the following topics:

- [Specifying the Windows domains with which to synchronize employee details](#)
- [Customizing the reviewing action statuses](#)
- [Setting Compliance Accelerator system configuration options](#)
- [Customizing the columns in the Review pane](#)

Specifying the Windows domains with which to synchronize employee details

You can specify multiple Windows domains with which Compliance Accelerator synchronizes the details of employees and employee groups. The domains also appear in the list from which you can choose when you add a new employee and browse for the corresponding Windows account.

You must have the Modify System Configuration permission to specify the Windows domains. By default, users with the application role of Compliance System Admin have this permission.

To specify the Windows domains with which to synchronize employee details

- 1 Click the **Configuration** tab in the Compliance Accelerator client, and then click the **Account Information** tab.
- 2 Click **New** at the top of the window.

The Domain Information pane appears.

The screenshot shows a window titled "Domain Information" with a light blue header. Below the header, there are three main sections: "Domain Information", "Account Information", and "Global Catalog Information".

- Domain Information:** Contains a text box labeled "Domain Name (NETBIOS)" and a larger text box below it labeled "Enter the fully qualified domain names (one per line) for this domain".
- Account Information:** Contains a checkbox labeled "Use specific account when connecting to the domain (The Service account will be used by default)". Below this are two text boxes: "Account Name (domain\user)" and "Account Password" (masked with asterisks).
- Global Catalog Information:** Contains a checkbox labeled "Use the following Global Catalog server" and a text box labeled "Global Catalog Server".

At the bottom right of the window, there are two buttons: "Save" and "Cancel".

- 3 In the **Domain Name (NETBIOS)** box, type the NetBIOS name of the Active Directory domain.
- 4 In the **Enter the fully qualified domain names** box, type any DNS fully qualified domain names that you want to map to the NetBIOS name.
- 5 If you want to use a specific account when you connect to the domain, type the name and password of the account in the **Account Information** area.

By default, when synchronizing with Active Directory, Compliance Accelerator uses the service account under which the Accelerator Manager service is running.

- 6 To force Compliance Accelerator to use a specific server instead of attempting to find the global catalog automatically, check **Use the following Global Catalog server** and then specify the required server.
- 7 Click **Save**.

Customizing the reviewing action statuses

You can customize the status names with which Compliance Accelerator shows the status of items in the Review pane.

Table A-1 Default status names and access keys

Action status	Appraisal status	Escalation status
Unreviewed	Not Appraised	Not Escalated
Pending (Alt+P)	Appraised (Alt+A)	Escalated (Alt+E)
Questioned (Alt+Q)		Closed (Alt+C)
Reviewed (Alt+R)		

You can rename these statuses, change their descriptions, and, in most cases, assign different access keys to them. When pressed in combination with the Alt key, an access key lets reviewers assign a specific status mark to an item in the Review pane. For example, the key combination Alt+R typically assigns the Reviewed mark to an item. You can also change the navigation keys with which reviewers can select the next or previous item in the pane.

You must have the Modify System Configuration permission to configure the reviewing statuses. By default, users with the role of Compliance System Admin have this permission.

To customize the reviewing action statuses

- 1 Click the **Configuration** tab in the Compliance Accelerator client, and then click the **Reviewing Statuses** tab.
- 2 In the left pane, click the name of the status mark or navigation key that you want to change.

It is not possible to mark a message as Unreviewed, Not Appraised, or Not Escalated, so none of these statuses has an access key or a button in the Review pane.

- 3
- Enter the new details.
- Note that the names appear on the status mark buttons in the Review pane. It is therefore advisable to keep them short so that they do not disturb the page display.
- 4
- Click **Save**.

Setting Compliance Accelerator system configuration options

Compliance Accelerator provides hundreds of configuration options with which you can customize the appearance and performance of the application. These configuration options are grouped into categories, as [Table A-2](#) explains.

Table A-2 Configuration settings by category

Category	Function
Ad Hoc Searches	Configure the searches that users can initiate from their research folders.
Diagnostics	Enable or disable the Compliance Accelerator troubleshooting facilities.
Document Conversion	Customize the error messages that Compliance Accelerator displays in the Review pane when it cannot open an item in the preview window of that pane.
Export/production	Configure the output when users export or produce items from Compliance Accelerator for offline review.
General	Configure general Compliance Accelerator options.
Home Page	Control the appearance of the Home page of Compliance Accelerator.
Item Prefetch Cache	Configure the primary settings for the Compliance Accelerator prefetch cache mechanism. This mechanism is designed to speed up the rendering of items in the Review pane.
Item Prefetch Cache (Advanced)	Configure advanced settings for the prefetch cache mechanism.
Policy Integration	Integrate Compliance Accelerator with your policy management software to better flag items for inclusion in or exclusion from the review set.
Profile Synchronization	Control how Compliance Accelerator synchronizes user profiles with the corresponding Active Directory or Domino directory accounts.

Table A-2 Configuration settings by category (*continued*)

Category	Function
Random Capture	Configure message sampling using the Journaling Connector.
Reviewing	Customize the appearance and functionality of the Review pane.
Search	Optimize the search features in Compliance Accelerator.
Security	Implement Chinese walls security restrictions on what users can access in Compliance Accelerator. You can also choose whether to make the SQL Server SystemAdmin logon the creator and owner of Compliance Accelerator search schedules.
System	Record the dates on which you installed Enterprise Vault and began to archive data, and more.
Vault Directory Synchronization	Configure when Compliance Accelerator synchronizes with the Enterprise Vault archives.

You must have the Modify System Configuration permission to change the configuration settings. By default, only users with the role of Compliance System Admin have this permission.

To set system configuration options

- 1 Click the **Configuration** tab in the Compliance Accelerator client, and then click the **Settings** tab.
- 2 Click the plus sign at the left of a section name to list the associated settings. Alternatively, type some characters in the filter box at the top of the window to search for the configuration options that contain those characters. For example, type **Color** to find all the options that contain this word in their names.
- 3 For each setting whose value you want to change, do the following in the order listed:
 - Click the value in the **Value** column.
 - Set the required value.
 - Click outside the **Value** column.
- 4 When you have set all the required options, click **Save**.
- 5 If you have changed any setting that has a tick in its **Restart Required** column, restart the Enterprise Vault Accelerator Manager service on the Compliance Accelerator server to put your changes into effect.

The following sections describe the available options.

Ad Hoc Searches configuration options

Use these settings to configure the searches that users can initiate from the research folders that they have created.

Ad-hoc search Pre-fix	Specifies the prefix to add to the names of ad-hoc searches that users save to the review set.
Allow hits to be deleted from an Ad-Hoc search result	Specifies whether users can delete the items from a folder search before they accept the search into the review set. By default, Compliance Accelerator lets users delete the items.
Allow users to commit items without committing audit history	Specifies whether reviewers can commit items from their research folders to the review set without also committing the associated review marks and comments. This option is only used if you select "Commit All Audit History When Committing An Item". By default, Compliance Accelerator expects users to commit the marks and comments when they commit items to the review set.
Commit All Audit History When Committing An Item	Specifies whether reviewers must commit the full audit history when committing items from their personal folders to the review set. By default, Compliance Accelerator lets users choose the elements that they want to commit.
Require Export permission in Department for Export permission in Folder	Specifies whether to limit the export facility in a folder to those users who have export permissions in the associated department. By default, Compliance Accelerator does not require users to have this permission.
Require Review permission in Department for Review permission in Folder	Specifies whether to limit the review facility in a folder to those users who have review permissions in the associated department. By default, Compliance Accelerator does not require users to have this permission.
Require Search permission in Department for Search permission in Folder	Specifies whether to limit the search facility in a folder to those users who have search permissions in the associated department. By default, Compliance Accelerator does not require users to have this permission.

Show shared folders to Delegates	Controls the extent to which delegates can access the folders to which their principal reviewers have access. By default, all folders that a principal owns are automatically available to delegates. However, any other folders to which the principal has access are not available. If you want delegates to have access to these shared folders, change this setting.
----------------------------------	--

Diagnostics configuration options

Use these settings to enable or disable the Compliance Accelerator troubleshooting facilities.

Enable performance monitor	Specifies whether to report Compliance Accelerator performance data, which you can view with the Windows Performance Monitor utility.
Enable tracing	Specifies whether to record every server action in the event log. Tracing to the event log applies to information events only, as Compliance Accelerator always records all error messages and warning messages in the log.
Save deduplication information	Specifies whether to generate deduplication information files in a <code>DeduplicationInfo</code> subfolder of your Compliance Accelerator program folder on the Compliance Accelerator server (typically, <code>C:\Program Files (x86)\Enterprise Vault Business Accelerator\DeduplicationInfo</code>). These deduplication information files, which are in plain text and XML format, may assist the Symantec Support team when dealing with deduplication-related problems. By default, this setting is unchecked; Compliance Accelerator does not create the files.

Save Search Criteria	Specifies whether to generate search criteria files in a <code>SearchCriteria</code> subfolder of your Compliance Accelerator program folder on the Compliance Accelerator server. These files, which are in plain text and XML format, may assist the Symantec Support team when dealing with search-related problems. By default, Compliance Accelerator does not create the files. See “Search returns unexpected results” on page 204.
Save XML Search Items To Commit	Specifies whether to save the XML files of the items to commit to the database under a subfolder of the server. By default, Compliance Accelerator does not save the XML files.
Save XML Search Results	Specifies whether to generate search results files (one for each Enterprise Vault archive that is searched) in a <code>SearchResults</code> subfolder of your Compliance Accelerator program folder on the Compliance Accelerator server. By default, Compliance Accelerator does not create the files.

Document Conversion configuration options

Use these settings to customize the error messages that the Review pane of the Compliance Accelerator client may display.

Conversion Errors	Specify the error messages to display if Compliance Accelerator cannot display an item in the preview window of the Review pane. Each message can contain up to 200 characters.
-------------------	---

Export/production configuration options

Use these settings to configure the output when users export items from Compliance Accelerator for offline review.

Add Bate identifier to File System exports	<p>Specifies whether to add an identifying Bates number to the file name of each exported item that Enterprise Vault has archived through File Systems Archiving.</p> <p>The options are as follows:</p> <ul style="list-style-type: none"> ■ 0. Omit the Bates number. ■ 1. Add the Bates number to the start of the file name. This option is the default option. ■ 2. Append the Bates number to the end of the file name.
Always date stamp exported File System items	<p>Specifies whether to append a last-modified date stamp to the file name of each exported item that Enterprise Vault has archived through File Systems Archiving. By default, Compliance Accelerator appends the date stamp.</p>
Automatic retry: Maximum retries	<p>Specifies the maximum number of attempts that Compliance Accelerator makes to repeat an export run that failed for any reason. Set the value to 0 to stop Compliance Accelerator from retrying the run.</p>
Automatic retry: Minimum time between retries (minutes)	<p>Specifies the minimum delay in minutes between automatic attempts to repeat a failed export or production run. By default, Compliance Accelerator waits five minutes between retries.</p> <p>Note that Compliance Accelerator multiplies this value by the number of retries. So, if this value is 5, the delay between retries starts at five minutes and increases to 10, 15, and so on with subsequent retries.</p>
Custom conversion extension	<p>Specifies the file name extension of the files to create when exporting items for viewing outside Compliance Accelerator. For example, you would specify <code>.xls</code> as the extension for export files in Microsoft Excel format.</p>
Custom conversion file	<p>Specifies the name of the template file to use when exporting files in their custom format. For example, if you have created a template file for exporting items in Microsoft Excel format, you can enter <code>ExcelReport.xslt</code> as the file name.</p>

Default export folder	<p>Specifies the default folder on the Compliance Accelerator server to use for exported items. If you do not specify a default export folder, Compliance Accelerator uses the folder <code>c:\Compliance Accelerator Export\customer_name</code>.</p> <p>The folder path can contain up to 100 characters.</p>
Default Production status	<p>Specifies the status that you want to set as the default current status when you perform an export run.</p> <p>Type one of the following values:</p> <ul style="list-style-type: none"> ■ 0. N/A ■ 1. Pending ■ 2. Reviewed ■ 3. Questioned
Default to Unicode for PST and MSG	<p>Specifies whether to export PST and MSG files in Unicode (Outlook 2003 and later) format or ANSI (Outlook 97 through 2002) format. By default, Compliance Accelerator exports the items in Unicode format.</p>
Domino Export Template	<p>Specifies the name of the file to use as a template when exporting files to a Lotus Notes Database Template (NTF) file. The default file name is <code>accelexp.ntf</code>.</p>
Domino ID File	<p>Specifies the name of the <code>.id</code> file that is used for local Domino authentication when exporting files to an NTF file. The default file name is <code>Accelerator.id</code>.</p>
Domino Password	<p>Specifies the password that is used for local Domino authentication when exporting files to an NTF file.</p>
Enable Production threads	<p>Specifies whether to enable or disable all exporting and production facilities. By default, Compliance Accelerator enables these facilities.</p>
HTML conversion file	<p>Lets you download, edit, and then upload an XSL style sheet. This style sheet serves as the template for all the export reports that Compliance Accelerator generates in HTML format.</p>

Maximum production retry for items stored on slow devices	Specifies the number of attempts that Compliance Accelerator makes to retrieve an item from an offline device, such as a tape drive, before giving up. Enter a value between 1 and 1000, where the default is 120.
Minimum number of minutes between retries for items stored on slow devices (min)	Specifies the number of minutes that Compliance Accelerator waits between retry attempts when trying to retrieve an item from an offline device. Enter a value between 1 and 300, where the default is 5.
Number of production report threads	Specifies the number of threads that Compliance Accelerator assigns to generating reports of export runs. The default is 5.
Number of production threads per production run	<p>Specifies the number of threads in the SQL connection pool that Compliance Accelerator assigns to each export or production run. Enter a value in the range 1 to 25, where the default is 25.</p> <p>See also the configuration setting "Total number of production threads per customer".</p> <p>To determine the maximum number of export or production runs that you can conduct simultaneously, divide the "Total number of production threads per customer" by the "Number of production threads per production run". For example, if you specify 100 for the first setting and 25 for the second setting, you can conduct up to four export or production runs simultaneously. If you try to conduct further export or production runs, Compliance Accelerator holds them in a queue until the required number of threads is available.</p>
Production order Search by RunDate	Sets the order in which Compliance Accelerator lists the searches when you set the criteria for an export run. You can choose to sort the searches by name or by run date. By default, Compliance Accelerator sorts the searches by name.

PST ExportID Column Name	<p>In Microsoft Outlook, specifies the label for the column in which to show Compliance Accelerator export IDs. When you export items from Compliance Accelerator as a Personal Folders (.pst) file, and then import this file into Outlook, the export IDs of the items appear in this column.</p> <p>See “Making the export IDs visible in Microsoft Outlook” on page 134.</p>
PST Folder Name	<p>Specifies the Outlook folder in which to place the items after you import a Personal Folders (.pst) file that you exported from Compliance Accelerator.</p>
Report chunk size	<p>Specifies the number of exported items to list in each report file. The default is 25000.</p>
Show PST version option on export run	<p>Specifies whether, when you undertake an export run, Compliance Accelerator prompts you to select a PST version: Outlook 97-2002 (ANSI) or Outlook 2003 (Unicode). By default, Compliance Accelerator does not display the prompt.</p>
TAB Conversion file	<p>Lets you download, edit, and then upload an XSL style sheet. This style sheet serves as the template for all the export reports that Compliance Accelerator generates in tab-separated format.</p>
Total number of production threads per customer	<p>Specifies the maximum number of threads per customer that Compliance Accelerator assigns when it conducts export or production runs. Enter a value between 50 and 1000, where the default is 100.</p> <p>See also the configuration setting "Number of production threads per production run".</p>

General configuration options

Use these settings to configure general Compliance Accelerator options.

Add User page refresh time	Specifies the frequency in seconds with which Compliance Accelerator refreshes the Select User dialog box. This dialog box lets you select a user account to add to Compliance Accelerator. It appears when you click Browse in the properties page for an employee. Specify a value between 1 and 300, where the default is 10.
Display warning in Archives pane when number of archives to load exceeds this threshold	Specifies a threshold count for the number of archives to load in the Archives To Search pane of the Compliance Accelerator client. If the number of archives that match the current selection and filter criteria exceeds this threshold, a warning message prompts you to change the criteria and reduce the number of archives. Specify a value in the range 50,000 to 200,000. The default is 50,000.
CA Invitation Email Subject	<p>Specifies the subject line of the message that Compliance Accelerator creates when you click Send Email Invite in the Role Assignment tab of the Compliance Accelerator client. When you assign roles to users, you can click Send Email Invite to notify them that they may perform a ClickOnce installation of the Compliance Accelerator client.</p> <p>Note that the Send Email Invite option is only available in those Compliance Accelerator clients that you install by using a ClickOnce deployment package. The option is unavailable in those clients that you install with the MSI installer package.</p> <p>See “Assigning Compliance Accelerator roles to employees or groups” on page 46.</p>
CA Invitation Email Body	<p>Specifies the body of the message that Compliance Accelerator creates when you click Send Email Invite in the Role Assignment tab of the Compliance Accelerator client. Compliance Accelerator automatically replaces the [url] placeholder with the Web site address of your ClickOnce deployment package.</p> <p>For more information, see the description of the "CA Invitation Email Subject" setting.</p>

Enable deduplication in search	Specifies whether to deduplicate the items in search results. By default, with this setting checked, Compliance Accelerator deduplicates the items. Note that Compliance Accelerator does not deduplicate randomly-sampled items.
Hide Active Directory accounts ending with '\$' in account selector	In areas of Compliance Accelerator where you select an Active Directory account, specifies whether to show any accounts whose names end with the character \$. By default, Compliance Accelerator shows these accounts.
List searches without sampled hits in filters	When you filter items by search, specifies whether to omit from the list those searches that failed to capture any items. By default, Compliance Accelerator shows these searches.
Show First Name followed by Last Name	Specifies the order in which to display the first and last names of employees. By default, the first name precedes the last name. You may want to uncheck this option when working in countries where the names are typically reversed, such as Japan.
Show search sample counts in filters	<p>In areas of Compliance Accelerator such as the Review pane, specifies whether to append the sample size to the name of each listed search. So, if a search has 200 hits, and your monitoring policy requires you to add 10% of captured items to the review set, Compliance Accelerator shows the search as "My Search [20]".</p> <p>By default, Compliance Accelerator shows the sample size.</p>

Home Page configuration options

Use these settings to control the appearance of the Home page of Compliance Accelerator.

List Exceptions On Home page	Specifies whether to hide or show the list of individual exceptions on the Compliance Accelerator home page. By default, Compliance Accelerator lists the exceptions.
------------------------------	---

Maximum number of exports to show on home page	Sets a limit on the number of export runs that Compliance Accelerator can list in the home page of the application. The default is 30.
Maximum number of searches to show on home page	Sets a limit on the number of searches that Compliance Accelerator can list in the home page of the application. The default is 30.
Maximum task age (days) to show on home page	Specifies the maximum age of the data that Compliance Accelerator can display for tasks in the home page of the application. The default is 30 days.
Show Department 'All Container' Review Link	Specifies whether to display an All Departments link at the top of the Review Messages column on the Compliance Accelerator home page. By default, Compliance Accelerator displays the link.
Show Escalation 'All Container' Review Link	Specifies whether to display an All Departments link at the top of the Escalated Messages column on the Compliance Accelerator home page. By default, Compliance Accelerator displays the link.
Show Folders on Home Page	Specifies whether to list individual research folders on the Compliance Accelerator home page. By default, Compliance Accelerator lists the folders.
Show Reviewers' statistics to reviewers	Specifies whether reviewers can see the statistics for other reviewers on the home page of the application. By default, all reviewers can see these statistics.

Item Prefetch Cache configuration options

Use these settings to configure the Compliance Accelerator prefetch cache mechanism. This mechanism retrieves and caches items from the vault store during a scheduled window every night, instead of retrieving each item when the user chooses to review it. The cache therefore helps to speed up the rendering of items in the Review pane. You can specify the size, location, and other characteristics of the cache.

To optimize performance in an environment where you review items very intensively, we recommend the following:

- Use the fastest storage available and set aside a full partition so that there is no competition for I/O.

- Set the maximum size within the cache to match the partition size.
- Set the cache to 365 days before expiry.
- Set the cache to retrieve the full items with HTML and MSG. If you do not need to export the items, you can choose to retrieve the items with HTML only.

The Item Prefetch Cache options are the more commonly used cache options. You can also set the Item Prefetch Cache (Advanced) options.

Cache enabled	Specifies whether to enable or disable the prefetch cache. By default, Compliance Accelerator disables the cache. Therefore, prefetching does not occur and the cache is not used for item retrieval, even if there are items in the cache. Only enable the cache for a Compliance Accelerator database in which you actively review items or where you connect to slow storage for export runs.
---------------	--

Note that the cache is either enabled or disabled for an entire database.

Cache location	Specifies the local path or network share path to the folder in which to store the cache. Within this folder, Compliance Accelerator stores the prefetched files in a subfolder that is called <code>AcceleratorPrefetch_CustomerId</code> .
----------------	--

Note the following:

- We recommend that you specify a local path, where possible. If you must specify a network share path, always use the UNC path rather than a mapped drive.
- The folder must already exist; Compliance Accelerator does not create it.
- In a hosting environment, multiple customers must not share the same folder.

Cache maximum item age (days)	<p>Specifies the number of days for which items can remain in the cache before Compliance Accelerator automatically deletes them. The item age is based on the creation time of the file in the cache, and not the time that Compliance Accelerator captured the item or the time that the item was originally sent. The default age is 5 days.</p> <p>Compliance Accelerator may remove an item from the cache earlier than the maximum item age if the cache becomes full.</p>
Cache maximum size (Mbytes)	<p>Specifies the maximum size of the cache in megabytes (MB). The default is 1000 MB. The larger the value of the "Cache maximum item age (days)" setting, the higher the cache maximum size must be to accommodate the items.</p>
End prefetching time of day (server local time)	<p>Specifies the time of day at which Compliance Accelerator stops prefetching items. The default is 05:00 A.M. Use this setting with "Start prefetching time of day" to determine the hours of the day that prefetching is active. Configuring a period during which caching does not occur lets you undertake other maintenance activities during this period, such as performing Enterprise Vault backups.</p> <p>To make prefetching active at all times, set this option and "Start prefetching time of day" to the same time.</p>
Start prefetching time of day (server local time)	<p>Specifies the time of day at which Compliance Accelerator starts to prefetch items. The default is 20:00 P.M. Use this setting with "End prefetching time of day" to determine the hours of the day that prefetching is active. Configuring a period during which caching does not occur lets you undertake other maintenance activities during this period, such as performing Enterprise Vault backups.</p> <p>To make prefetching active at all times, set this option and "End prefetching time of day" to the same time.</p>

Item Prefetch Cache (Advanced) configuration options

These settings provide additional, advanced options for configuring the Compliance Accelerator prefetch cache functionality. Use these settings with the Item Prefetch Cache options.

Cache encrypted	Specifies whether to encrypt files before they are stored in the cache. By default, Compliance Accelerator does not encrypt the cache.
Cache purge time of day (server local time)	Specifies the time of day at which Compliance Accelerator performs cache housekeeping (primarily removing old items). The default time is 19:00 PM.
Maximum capture age (days)	Excludes from the cache those captured items that are older than the specified number of days. The default is 3 days. This setting only has an effect when prefetching is first turned on, or if it has been disabled for some time and is then reenabled.
Maximum item fetch attempts	Specifies the maximum number of times that Compliance Accelerator tries to prefetch an item before giving up. The default is 10.
Maximum item size to store in cache (bytes)	Sets a limit on the size of items and parts of items that Compliance Accelerator can prefetch. If an item or part of an item exceeds this limit, it is ignored. The default is 10 MB. For example, Compliance Accelerator still prefetches an item that has multiple attachments, none of which is bigger than 10 MB, even though the combined size of the attachments may greatly exceed the 10 MB limit.
Minimum time between item fetch retries (minutes)	Specifies the number of minutes that Compliance Accelerator waits between attempts to prefetch items. The default is 30 minutes. Use this setting with "Maximum item fetch attempts" to configure retry behavior for failed fetches.
Prefetch attachments	Specifies whether to prefetch the attachments to items. By default, Compliance Accelerator prefetches attachments. Note that attachments of nested items are not prefetched.

Prefetch attachments as HTML	Specifies whether to render attachments as HTML when prefetching them. By default, Compliance Accelerator prefetches attachments as HTML.
Prefetch guaranteed sample search items	Specifies whether the results of guaranteed sample searches are eligible for prefetching. By default, they are.
Prefetch immediate search items	Specifies whether to prefetch the items that users have captured with an immediate, unscheduled search. By default, Compliance Accelerator does not prefetch these items.
Prefetch Native format	Specifies whether to prefetch items in their original, native format. By default, Compliance Accelerator does not prefetch the items in their native format. However, if your policy is to review items in their original format then you should enable this feature.
Prefetch Random Sampling items	Specifies whether the items that you have captured through random sampling are eligible for prefetching. By default, they are. For best results, ensure that prefetching is active for a suitable period after the nightly random sampling tasks are expected to complete.
Prefetch research items	Specifies whether to prefetch the items that users have placed in personal folders through ad-hoc searches. By default, Compliance Accelerator prefetches these items.
Prefetch scheduled search items	<p>Specifies whether to prefetch the items that users have captured with a scheduled search. By default, Compliance Accelerator prefetches the items.</p> <p>Note that items are only prefetched when the search is accepted, so this option works best when scheduled searches are set to auto-accept.</p>
Prefetch search items	Specifies whether to prefetch the items that users have captured with a search. You can further control this facility with the "Prefetch immediate search items" and "Prefetch scheduled search items" options. By default, Compliance Accelerator prefetches the items.

Prefetch XML structure	Specifies whether to prefetch the XML structure of an item. This structure defines the parts of the item and includes a list of attachments (but not the attachments themselves). The XML structure is used for the preview pane in the Review pane. An XSL transform is applied to the XML to convert it to HTML. By default, Compliance Accelerator prefetches the XML structure.
Render HTML for message review	<p>Specifies whether to prefetch the items for review in HTML format. By default, Compliance Accelerator prefetches the items in this format.</p> <p>Prefetching the items improves review performance because Compliance Accelerator does not need to perform the rendering from XML to HTML at review time. The benefits of this are most likely to be noticeable on a system where many reviewers work concurrently.</p>
Render printable HTML	Specifies whether to prefetch the printable versions of items in HTML format. By default, Compliance Accelerator does not prefetch the items in HTML format. However, it is advisable to change the setting if you expect to use the printable view functionality regularly.
Retry record retention period (days)	Specifies how long Compliance Accelerator keeps records of repeated, failed attempts to prefetch items. The default is 30 days.

Policy Integration configuration options

Use these settings to integrate Compliance Accelerator with your policy management software to better flag items for inclusion in or exclusion from the review set.

Always show policy display in review grid	When you preview an item that has no associated policies in the Review pane, specifies whether to show the Policy field above the item. By default, Compliance Accelerator hides this field when there are no associated policies.
---	--

Category policies message header	<p>Specifies the prefix to use for X-header lines that contain a semicolon-delimited list of category policies.</p> <p>Applying category policies to items does not affect their capture in any way; it provides a means to categorize the items. For example, you might use category policies to flag the items that are in Spanish or marked as Personal.</p>
Deduce overall policy action from policy types	<p>Determines how Compliance Accelerator proceeds when it encounters an item for which the policy management software has not specified an overall action in either an index property or item X-header. The overall action can be one of the following:</p> <ul style="list-style-type: none"> ■ Inclusion (demands or suggests capture). The Journaling Connector always samples the item, but you can choose to include or exclude the item when you conduct a search. ■ Exclusion (precludes capture or advocates non-capture). The Journaling Connector never samples the item, and you can choose to exclude it from searches. ■ No action. The item is subject to normal Compliance Accelerator random sampling by the Journaling Connector. <p>By default, when it encounters an item for which no overall policy action has been specified, Compliance Accelerator does the following:</p> <ul style="list-style-type: none"> ■ Includes the item if it has any associated inclusion policies. ■ Excludes the item if it has one or more associated exclusion policies but no inclusion policies. ■ Takes no action if the item has no associated inclusion or exclusion policies (but it may have some associated category policies). <p>If you disable this behavior, Compliance Accelerator assumes that it should take no action on items for which no overall policy action has been set.</p>

Exclusion policies message header	<p>Specifies the prefix to use for X-header lines that contain a semicolon-delimited list of exclusion policies.</p> <p>An exclusion policy either precludes capture or advocates the non-capture of items. For example, spam items or newsletters may fall into this category.</p>
Include policies take precedence over exclude policies	<p>Specifies whether to give higher priority to inclusion policies than to exclusion policies. By default, the Journaling Connector always samples an item that has at least one associated inclusion policy. This is the case even if the item also has one or more exclusion policies.</p>
Inclusion policies message header	<p>Specifies the prefix to use for X-header lines that contain a semicolon-delimited list of inclusion policies.</p> <p>An inclusion policy addresses the most serious issues, such as swearing, racism, and insider trading. You would normally want to ensure that items to which such policies were applied are always captured for review.</p>
Policy action message header	<p>Specifies the prefix to use for X-header lines that contain the prescribed overall policy action for an item (one of INCLUDE, EXCLUDE, or NOACTION).</p>
Sort Policies within type	<p>When you preview an item in the Review pane, specifies the order in which to list the associated policies in the banner above the item. Enter one of the following values:</p> <ul style="list-style-type: none"> ■ 0. The policies are not sorted. ■ 1 (default). Compliance Accelerator first groups the policies by policy type (inclusion, exclusion, and category) and then sorts them alphabetically within each type. ■ 2. The policies are sorted alphabetically, regardless of policy type. <p>Changing the sort order does not affect the items that are already in the Accelerator database; only newly-added items are affected.</p>

XML policy message header	<p>Specifies the prefix to use for X-header lines that define a policy action through a string of XML code. Each XML definition must be on a single X-header line, like the following:</p> <pre><POLICIES ACTION="INCLUDE"><INCLUSION> <POLICY>Profanity</POLICY></INCLUSION> </POLICIES></pre>
---------------------------	---

Profile Synchronization configuration options

Use these settings to control how Compliance Accelerator synchronizes employee profiles with the corresponding Active Directory or Domino directory accounts.

Automatically detect deleted profiles and mark them as deactivated	Specifies whether Compliance Accelerator should automatically deactivate those employee profiles for which it cannot find a corresponding Active Directory or Domino directory account.
Default Domino domain when creating profiles	Specifies a domain to add to a user name automatically when synchronizing employees with Domino accounts.
Default Domino server when browsing for users	Specifies the name of the default Domino LDAP server to use when you browse for new users to add to your Compliance Accelerator system.
Force users to use the default Domino server when browsing for users	Stops you from choosing any Domino LDAP server other than the default server when you browse for new users to your Compliance Accelerator system. By default, Compliance Accelerator lets you nominate any Domino server.
Minimum days to wait before profiles are deactivated	Specifies the number of days after which Compliance Accelerator should automatically deactivate those employee profiles for which it cannot find a matching Active Directory or Domino directory account.
Minimum number of failed synchronizations before deactivating profiles	Specifies the number of times that Compliance Accelerator should fail to synchronize an employee profile with the corresponding Active Directory or Domino directory account before it deactivates the profile.

Number of synchronization threads	Specifies the number of threads that Compliance Accelerator employs when it synchronizes employee profiles with the corresponding Active Directory or Domino directory accounts. Enter a value in the range 1 through 5, where the default is 1.
Remove addresses that do not exist in Domino or Active Directory	<p>Specifies whether Compliance Accelerator deletes the email addresses in an employee profile before it synchronizes the profile with Active Directory or a Domino directory. By default, Compliance Accelerator does not delete the addresses. This is because you may still want to perform searches that use old email addresses, or you may have entered some additional email addresses manually.</p> <p>Compliance Accelerator does not delete the email addresses in the profile if synchronization fails for any reason.</p>
Synchronization interval (hours)	Specifies the frequency in hours with which Compliance Accelerator synchronizes employee profiles with the corresponding Active Directory or Domino directory accounts. Enter a value in the range 1 through 24. The default is every eight hours and every time the Accelerator Manager service starts.
Synchronize profiles	Specifies whether Compliance Accelerator should attempt to synchronize employees and groups with the corresponding Active Directory or Domino directory accounts. The default is to do so.
When service starts wait before synchronizing (minutes)	Specifies the number of minutes to wait after the Accelerator Manager service starts before synchronizing employees and groups with Active Directory or a Domino directory. Enter a value in the range 0 through 720. By default, the service does not wait before synchronizing.

Random Capture configuration options

Use these settings to configure item sampling using the Journaling Connector.

Cache backup location	When cache safety mode is enabled, specifies a location for the cache folder. It is better to enter a local path for performance reasons, but you can also enter a network share path. The account that runs the Enterprise Vault Accelerator Manager service must have full access to this folder. If the folder does not exist and the service has the appropriate permissions, the folder is created.
Cache safety mode	Specifies whether to make a local copy of the items that the Journaling Connector has flagged for random capture, as an extra safeguard. By default, cache safety mode is not enabled. This setting is used with "Cache backup location". If you turn on this setting, you must also specify the cache backup location. Enabling safety mode has an effect on performance.
Enable background processing of captured items	Specifies whether Compliance Accelerator should process the items that the Journaling Connector has flagged for random capture. By default, background processing is enabled, but you may want to disable it if you want to delay adding items to the review set temporarily.
Exclude items with this text in subject	<p>Excludes from random sampling those items that contain the specified word or phrase in their subject lines. You can specify one exclusion term only, and you must enclose it in double quotation marks.</p> <p>You can use asterisks (*) as wildcard characters at the start, end, or both sides of the exclusion term. For example, the terms "*asset management", "asset management*", and "*asset management*" are all valid exclusion terms. If you do not use wildcards, the exclusion term must exactly match the entire subject line contents. So, the term "Read:" matches only those items whose subject lines contain nothing more than "Read:".</p> <p>For more information, see the following article on the Symantec Support site:</p> <p>http://www.symantec.com/docs/TECH186498</p>

First Pass Sampling time (local time)	Reduces the burden of resolving the transactions at the sample time by letting the server resolve some of the transactions before the main sampling time is reached. At this time, transactions of items that are captured are resolved. The default time is 20:00.
Maximum age of unresolved items (hours)	Specifies the number of hours after which Compliance Accelerator purges from temporary storage any sampled items that it has yet to move into the review set. Enter a value in the range 1 through 672, where the default is 96. This setting is used with "Maximum resolve attempts". Both conditions must be reached for the purging to take place.
Maximum resolve attempts	Specifies the maximum number of attempts that Compliance Accelerator should make to move an item into the review set before it purges the item. Enter a value in the range 1 through 500, where the default is 5. This setting is used with "Maximum age of unresolved items". Both conditions must be reached for the purging to take place.
Record extra statistics for evidence of review reports	Causes Compliance Accelerator to collect additional data for use in Evidence of Review reports. Compliance Accelerator holds the extra data in the tblMessageAddress database table, which can grow large as a result.

Sampling mode	<p>Specifies whether to use guaranteed sampling or statistical sampling of items.</p> <p>With guaranteed sampling (the default), Compliance Accelerator captures all items for every monitored employee throughout the day. After midnight, it picks a random sample from each employee's items and adds them to the review set. If you choose guaranteed sampling, you cannot cap the number of items that Compliance Accelerator adds to the department review set.</p> <p>With statistical sampling, Compliance Accelerator takes a random sample of the items that it has captured during the previous 24-hour period and adds them to the review set. This means that some employees may have fewer items captured than others with an identical monitoring percentage.</p>
Sampling time (local time)	<p>Specifies the time at which the Journaling Connector puts sampled items from the previous 24 hours in the review set. The default time is 01:00. This means that sampled items from the previous 24 hours become visible in the review set after 1 A.M. local time when the processing is complete.</p>
Stale config timeout (mins)	<p>Specifies the frequency in minutes with which the Journaling Connector synchronizes with the Compliance Accelerator database. Enter a value in the range 1 through 300, where the default is 60.</p>

Reviewing configuration options

Use these settings to configure the Review pane.

Default Page Size	<p>Specifies the default number of items to show in the Review pane. Enter a value in the range 1 through 1000, where the default is 100.</p>
-------------------	---

Display Marking List	Specifies how to show the available marks in the Review pane: as clickable options across the bottom of the page, or in a drop-down list. By default, Compliance Accelerator shows the marks as clickable options rather than as options in a drop-down list.
ECM Temporary Storage Area	<p>Specifies the path to the folder in which temporarily to store the items that you retrieve by using the Enterprise Vault Content Management API. By default, Compliance Accelerator uses the Windows %TEMP% folder.</p> <p>Note the following:</p> <ul style="list-style-type: none"> ■ We recommend that you specify a local path, where possible. If you must specify a network share path, always use the UNC path rather than a mapped drive. ■ The folder must already exist; Compliance Accelerator does not create it. ■ In a hosting environment, multiple customers must not share the same folder.
ECM Temporary Storage Area Cleanup Interval (Minutes)	Specifies the frequency in minutes with which to purge stale data from the temporary storage area. The default value is five minutes.
Facets To Hide	<p>Provides a comma-separated list of the filter options that are not available to users in the Review pane. The available options are as follows:</p> <p>appraisalid, appraiserid, author, capturedate, capturetype, commentid, direction, escalatedbyid, escalationid, escalationownerid, maildate, numattachments, policyaction, policyid, reviewerid, scheduledsearchid, searchid, size, type.</p>
Folder item color when it exists in the review set	Specifies the color with which to identify the items in a research folder that already exist in the associated review set. The default color is red.
Highlight Background Color	Specifies the background color with which to highlight instances of search terms in HTML renderings of items. You can enter a color name, such as "Yellow" (the default color), or a red-green-blue color value, such as "#FFFF00".

Highlight Foreground Color	Specifies the foreground color with which to highlight instances of search terms in HTML renderings of items. You can enter a color name, such as "Black" (the default color), or a red-green-blue color value, such as "#000000".
Hit Highlighting Type	Specifies whether to enable or disable search highlighting in HTML renderings of items. Set the value to 1 (the default) if you want to highlight instances of search terms in items, or to 0 to disable highlighting.
Item Unlocking Thread	Specifies whether to turn on or off the lock cleanup thread, which unlocks any items that have been accidentally left locked. For example, this may be the case if a reviewer's computer or Compliance Accelerator client stops working during a reviewing session. By default, the thread is turned on.
Label for messages without a subject	Specifies the subject line to assign to those items that do not have a subject line. The default is "No Title".
Maximum items user can temporarily self-assign	Sets a limit on the number of items that users can temporarily assign to themselves while they review. The default is 10000.
Maximum Page Size	Specifies the maximum number of items to list on a page within a review set. Enter a value between 1 and 300, where the default is 300.
Review Grid File	<p>Lets you download and upload an XML file with which to define the column layout in the Review pane for all users.</p> <p>See "Customizing the columns in the Review pane" on page 191.</p>
Review Set Expiry Time (Minutes)	Specifies the number of minutes of inactivity after which a user's review set expires. The default value is 120 minutes.
Sanitize HTML for review	Specifies whether to preprocess HTML items before review to remove any script that may cause navigation problems. By default, Compliance Accelerator preprocesses the items.

Show Appraisal UI	For users with the Apply Appraisal Status permission, specifies whether to hide or show the appraisal system features in the Review pane and Export pane.
Timeout for building or sorting review set (seconds)	Specifies the number of seconds within which Compliance Accelerator must build a review set or sort a review set before the process times out. The default is 300.

Search configuration options

Use these settings to optimize the search features in Compliance Accelerator.

Allow search and capture of existing items	Specifies whether, when you set the criteria for a new search, you can choose to include previously-captured items in the search results. By default, you have the option to do so.
Buffer Since Last Run	<p>When you select a schedule to use when you define the criteria for a new search, you can select Since last run in the Date range section. This option instructs Compliance Accelerator to search new items that have arrived since you last ran this scheduled search. In the Start box, you enter the date to be taken as a starting point for the first run of the search.</p> <p>By default, Since last run searches from the date of the last run (or the Start date for the first search) to the current day minus 1 (that is, up to yesterday). If required, you can change this interval to search to the current day minus <i>n</i> days. To use Since last run with any searches that run more than once a day, set the interval to 0.</p>
Combine subject and content fields with OR	When you search for words in both the subject of an item and its content, specifies whether to find only those items that meet one or both criteria. By default, Compliance Accelerator finds only those items that meet both criteria.
Disable Search against Other Departments	Specifies whether, when you define the criteria for a new search, the Other Depts option in the Author & Recipients area is available. By default, Compliance Accelerator does let you conduct searches against other departments.

Enable automatic synchronization of index volumes	Specifies whether Compliance Accelerator should automatically synchronize the index volumes for an archive when it encounters any unknown index volumes during a search. By default, Compliance Accelerator synchronizes the index volumes automatically.
Enable Search Threads	Specifies whether to enable or disable all search facilities. By default, Compliance Accelerator enables these facilities.
Error search if index is rebuilding or failed	Specifies whether the search of a particular archive returns an error if its index is offline, rebuilding, or failed. By default, Compliance Accelerator returns an error in these circumstances.
Error search if missing items or content	Specifies whether the search of a particular archive returns an error if its index has failed to index either an indexable archived item or the content of the item. The default setting is false (not enabled).
Error search if index requires width normalization	Specifies whether the search of a particular archive returns an error if its index must be rebuilt to handle full-width characters correctly. The default setting is Off.
Fail search of archive if archive has been copied or moved	Specifies whether to mark as failed a search of a moved or copied archive, if the destination archive is not included in the search. The default is False, which means that Compliance Accelerator produces a warning when searching such archives, but it does not mark them as failed.
Guaranteed Sample search timeout (mins)	Specifies the number of minutes for which guaranteed sample searches run before Compliance Accelerator automatically accepts them and uses the results for sampling. The default is 240 minutes.
Hotword Set Tag	Specifies the tag with which Compliance Accelerator prefixes hotword sets when you enter them in the criteria for a new search. The default is HWS.

Hotword Tag	Specifies the tag with which Compliance Accelerator prefixes hotwords when you enter them in the criteria for a new search. The default is HW.
Ignore non journal archives for Guaranteed Sample searches	Specifies whether to search non-Journal archives when conducting guaranteed sample searches. By default, Compliance Accelerator searches Journal archives only, as these archives are the only type to which the Journaling Connector writes.
Maximum number of searches listed in filters	For areas of Compliance Accelerator that list searches from which you can choose, specifies the maximum number of searches to include in the list. The default is 250.
Maximum Search Retries	Specifies the number of times that Compliance Accelerator tries to search an archive before giving up. Enter a value in the range 1 through 50, where the default is 5.
Number of acceptance search Threads	Specifies the number of threads that are assigned to accepting search result sets. For example, the default setting of 5 means that no more than five search results sets are accepted at a time. Enter a value in the range 1 through 10.
Number of delete search Threads	Specifies the number of threads that are assigned to deleting search result sets. For example, the default setting of 2 means that no more than two search results sets are deleted at a time. Enter a value in the range 1 through 10.
Number of sampling search Threads	Specifies the number of threads that are assigned to sampling search result sets. For example, the default setting of 5 means that no more than five search results sets are sampled at a time. Enter a value in the range 1 through 10.
Number of Vault search Threads	Specifies the number of threads that are assigned to searching archives per index server. For example, the default setting of 10 means that no more than 10 archives are searched per Enterprise Vault server at a time. Enter a value in the range 1 through 10.

Only allow 'Research this message' on the first selected message	Specifies whether, when you click multiple items in the Review pane and then click Search, Compliance Accelerator lets you specify the search criteria for each of the selected items or only for the first of the selected items.
Optimize search based on oldest and youngest items	<p>When set to True, improves performance by excluding from a search those archives that Compliance Accelerator has determined do not contain any items in the date range that you have specified in your search criteria. The default setting is False, which means that Compliance Accelerator searches all the available archives, regardless of whether their contents fall within your specified date range or not.</p> <p>Use this setting with "Synchronize thread checking period (sec)", which is one of the Vault Directory Synchronization configuration options. If you set "Optimize search based on oldest and youngest items" to True, you must lower the setting for "Synchronize thread checking period (sec)" to ensure that Compliance Accelerator does not run searches against out-of-date data. For example, you can lower the setting to 3600 seconds (one hour).</p>
Require 'Author' / 'Content' / 'From Date' / 'Recipients' / 'Subject' / 'To Date' to be specified	Specifies whether it is mandatory to enter the designated criteria before you can perform a search. By default, these criteria are optional. You may want to make them mandatory to prevent searches from returning an overwhelming number of results.
Retry time when index service is busy (min)	Specifies the frequency in minutes with which Compliance Accelerator tries to access an Enterprise Vault Indexing service that is too busy to perform a search. Enter a value in the range 1 through 300, where the default is 5.
Retry time when index service not running (min)	Specifies the frequency in minutes with which Compliance Accelerator tries to access an Enterprise Vault Indexing service that is unavailable. Enter a value in the range 1 through 300, where the default is 5.

Return only top messages in search results	Specifies whether searches return the top-level items only. Setting this option to Off means that all files attached to the top-level items are displayed in search results.
Save SMTP subject rather than filename	For items that were archived using File System Archiving (FSA), specifies whether to show the SMTP message subject rather than the FSA file name in the Review pane.
Search result page refresh time	Specifies the frequency in seconds with which Compliance Accelerator refreshes the results summary page during a running search. Enter a value in the range 1 through 300, where the default is 10.
Search timeout (hours)	Specifies the maximum time in hours that Compliance Accelerator allows for searches to complete. The default is four hours.
Searches page refresh time	Specifies the frequency in seconds with which Compliance Accelerator refreshes the Searches pane for a department. Enter a value in the range 1 through 300, where the default is 20.
Show Application Search Tree 'Constrain Tree Height' option	When you define the criteria for a new search, specifies whether a Constrain tree height option is available in the Authors & Recipients area. When checked, this option fixes the height of the department tree view in the Authors & Recipients area. By default, Compliance Accelerator hides the option.
Show Application Search Tree 'Expand All' option	When you define the criteria for a new search, specifies whether an Expand All link is available in the Authors & Recipients area. Clicking this link expands all the departments in the tree view. By default, Compliance Accelerator hides the link.
Show 'Guaranteed Sample' option for new searches	Specifies whether you can create Guaranteed Sample searches. By default, you can.
Show Search Result In Progress	Specifies whether users can access the Review pane while a search is in progress, so that they can immediately start to review the items that Compliance Accelerator has found. By default, Compliance Accelerator permits this.

Total number of search results worker threads	Specifies the maximum number of search results worker threads that are allowed to run on the system. These threads handle the processing of search results returned from the archive. The maximum value is 5, and the default is 2.
Total number of search threads	Specifies the maximum number of search threads that are allowed to run on the system across all index volumes. The maximum value is 500, and the default is 100.
Use sequence number for searches	Optimizes performance for searches that return more than 50,000 results. By default, this option is enabled.
When service starts, wait before synchronizing Index Services (minutes)	Specifies the number of minutes that Compliance Accelerator waits at startup before synchronizing with available index services. Enter a value in the range 0 through 300, where the default is 0.
When service starts, wait before starting Vault Searches (minutes)	Specifies the number of minutes that Compliance Accelerator waits at startup before searching the archives for items. Enter a value in the range 0 through 300, where the default is 0.

Security configuration options

Use these settings to implement *Chinese walls* security restrictions on what users can access in Compliance Accelerator.

A Chinese wall is a metaphor used to refer to the practice of ensuring that different parts of an organization are kept apart so that information does not circulate freely and to prevent conflicts of interest. By implementing Chinese walls, you can stop users in one part of your organization from giving access to departments and folders to users in another part of the organization.

Bypass Department Users Permissions check when removing all roles	Lets users who do not have the Manage Department User permission remove Department Users from departments.
Enable Chinese Wall Department Users	Prevents users from being assigned to roles in a department unless they have first been assigned to the Department User role in that department.

Use SQL Server 2005 SystemAdmin Server Role for Schedules	<p>When selected, makes the SystemAdmin logon the creator and owner of Compliance Accelerator search schedules.</p> <p>If you want to lock down your SQL Server instance, uncheck this setting and then do the following in the order listed:</p> <ul style="list-style-type: none">■ Add the Vault Service account to the msdb database.■ Give the Vault Service account Select permissions on the following msdb tables: sysjobs, sysjobschedules, sysjobsteps, and sysschedules.■ Give the Vault Service account Execute permissions on the msdb stored procedure sp_add_category.■ Assign the database role SQLAgentUserRole to the Vault Service account.
---	---

System configuration options

Use these options to record the dates on which you installed Enterprise Vault and began to archive data, configure the threads that Compliance Accelerator uses to pause searches, and more.

Enterprise Vault Oldest Archived Item Date	<p>Specifies the date on which Enterprise Vault archived the oldest available data.</p> <p>If the oldest archived item date and "Enterprise Vault V5 Installation Date" are the same then, when entering the criteria for a search, you can specify the message type without also specifying a start date. (Compliance Accelerator does not return any pre-5.0 data.) However, if the oldest archived item date is earlier than the V5 installation date, you can only specify the message type if you specify a start date that is on or after the V5 installation date.</p>
Enterprise Vault V5 Installation Date	<p>Specifies the date on which you first installed or upgraded Enterprise Vault 5.0 or later.</p>

IIS Application Pool	Identifies the application pool in which the Accelerator Web applications are grouped. Application pools allow specific configuration settings to be applied to groups of applications and to the worker processes that service those applications. The default application pool is EVAcceleratorAppPool.
Initial Pausing Queue Size	Specifies the maximum number of searches that you can pause instantly. The default is 2.
Number Of Pause Search Threads	Specifies the number of threads that are assigned to pausing searches. Enter a value in the range 1 through 10, where 1 is the default value.
Pause queue threshold	Specifies the total number of pause search requests that can be queued at once. Enter a value in the range 10 through 100, where 10 is the default value.
Pause Threads Delay	Specifies the number of minutes that Compliance Accelerator waits at startup before it initializes the threads that are assigned to pausing searches. By default, Compliance Accelerator does not delay before it initializes the threads.
Search Pause Thread Checking Period (Sec)	Specifies the number of seconds to wait before starting pause threads. The default is 5.
Show Vault Management Option	Does not serve any function in the current version of Compliance Accelerator. The option will be removed from Compliance Accelerator in a later release.

Vault Directory Synchronization configuration options

Use these settings to configure when Compliance Accelerator synchronizes with the Enterprise Vault archives.

Archive registration/deregistration task period (minutes)	<p>Specifies the frequency in minutes with which to run the archive registration/deregistration task. The default is 60 minutes. To prevent the accidental deletion of Enterprise Vault archives whose contents appear in the Compliance Accelerator review set or search results, this task registers an interest in the archives. The task also discards existing archive registrations when they are no longer required.</p> <p>See also the options "Enable archive registration task" and "Discard existing archive registrations after you turn off 'Enable archive registration task'".</p>
Archive selection page size	<p>Specifies the maximum number of Enterprise Vault archives to display on a single page during archive selection. By default, Compliance Accelerator lists a maximum of 100 archives. If the number of available archives exceeds the value that you specify here, Compliance Accelerator displays some extra hyperlinks so that you can page through the archives.</p>
Automatically enable new Vault Stores in departments/cases	<p>Specifies whether, when a new vault store is created, Compliance Accelerator automatically includes it in searches.</p> <p>The options are as follows:</p> <ul style="list-style-type: none">■ 1. New vault stores are never automatically enabled.■ 2. New vault stores are always automatically enabled.■ 3 (default value). New vault stores are automatically enabled when all the other vault stores in the same site are already enabled.
Discard existing archive registrations after you turn off 'Enable archive registration task'	<p>Specifies whether to keep or discard any existing archive registrations if you choose to disable the archive registration task. By default, Enterprise Vault keeps the existing archive registrations after you disable the task.</p> <p>See also the options "Archive Registration task period (minutes)" and "Archive registration/deregistration task period (minutes)".</p>

Enable archive registration task	<p>Specifies whether to enable or disable the archive registration task. By default, the task is enabled. If you disable it, a message prompts you to choose the required setting for the option "Discard existing archive registrations after you turn off 'Enable archive registration task'".</p> <p>See also the option "Archive Registration task period (minutes)".</p>
Synchronize archives on search	<p>Specifies whether to synchronize all the archives when running a new search. By default, Compliance Accelerator does not synchronize all the archives.</p>
Synchronize Retention Categories on search	<p>Specifies whether to synchronize all the retention categories when running a new search. By default, Compliance Accelerator does not synchronize all the retention categories.</p>
Synchronize thread checking period (sec)	<p>Specifies the frequency in seconds with which Compliance Accelerator synchronizes with the Enterprise Vault archives. The default is 21600 (six hours). For best results, you may want to change the synchronization period to 3600 (one hour).</p> <p>The more frequently synchronization occurs, the greater the load on the Compliance Accelerator database. However, if the synchronization is not frequent enough, Compliance Accelerator may take a long time to recognize new archives, vault stores, and retention categories.</p>
Synchronize Vault Stores when viewing Department/Case properties	<p>Specifies whether to synchronize the vault stores when displaying the properties page for a department. By default, Compliance Accelerator does not synchronize the vault stores.</p>

Customizing the columns in the Review pane

Each reviewer can hide or show columns in the item list of the Review pane by right-clicking the column header and then clicking **Select Columns**. The reviewer can also change the column order by dragging and dropping the column headers. However, the changes that a reviewer makes in these ways are available to that reviewer only.

If you want to customize the column layout in the Review pane for all Compliance Accelerator users, you must set up an XML configuration file. Note that reviewers can still change their column layout on the Review pane by using the **Select columns** menu and drag and drop.

[Table A-3](#) lists the columns that you can display and the name to use when you refer to the column in the XML file.

Table A-3 How the column headers are identified in the XML file

Column header in Review pane	Name to use in XML file	Default visibility
Modified	NeedCommitting	True
Attachments	Attachments	True
Policy action	PolicyAction	False
Comment present	CommentPresent	True
Department	Department	False
From	From	True
All recipients	To	False
Subject / Filename	Subject	True
Date	Date	True
Action status	Status	True
Last reviewed by	ReviewerPrincipalName	False
Capture type	CaptureType	True
Message type	MessageType	True
Message direction	MessageDirection	False
Item ID	DiscoveredItemID	False
Comment	Comment	False
Last comment by	CommentPrincipalName	False
Appraisal status	AppraisalName	True
Last appraised by	AppraiserName	True
Escalation status	EscalationName	True

Table A-3 How the column headers are identified in the XML file (*continued*)

Column header in Review pane	Name to use in XML file	Default visibility
Escalation owner	EscalationOwner	True
Escalated by	EscalatedByName	True
Policy summary	PolicySummary	False
Archive	KVSVaultName	False
Original Location	ItemPath	False

To configure the default column layout in the Review pane

- 1 Click the **Configuration** tab in the Compliance Accelerator client, and then click the **Settings** tab.
- 2 Expand the **Reviewing** section to show the available options.
- 3 In the **Review Grid File** row, click **Save as**.
- 4 Select a location in which to store the review grid file.
- 5 Open the review grid file in a text editor such as Windows Notepad.
- 6 Edit the file as necessary, using the information at the start of the file to guide you.

Each column that you want to display must have the attribute `visible='true'`. This is either because you have specified the attribute in the configuration file or because the default setting for the column is `true`. The order of the configuration lines determines the left-to-right order of the columns in the Review pane.

The XML file must contain at least one configuration line between the `<reviewgrid>` and `</reviewgrid>` tags.

- 7 Save the file.
- 8 In the **Review Grid File** row on the System Configuration tab, click **Browse**.
- 9 Select the XML file that you want to import.
- 10 Click **Open** at the right of the row to save the changes that you have made.
- 11 Click **Save** at the bottom right of the window.
- 12 Start a new Compliance Accelerator session to see the column changes.

Importing configuration data from an XML file

This appendix includes the following topics:

- [About importing configuration data](#)
- [Sample XML files](#)
- [Format of the Dataload.xml file](#)
- [Importing the configuration data](#)
- [About the ImportExport command](#)

About importing configuration data

As part of the process of setting up Compliance Accelerator, you must enter configuration data on employees, departments, partitions, roles, and so on. If this data already exists outside Compliance Accelerator and is convertible to XML format, you can import it into Compliance Accelerator from an XML file. Then you can quickly load large amounts of configuration data that might otherwise be time-consuming to enter.

You can also use the import facility to load predefined hotwords and phrases from some XML files that come with Compliance Accelerator.

Sample XML files

The Compliance Accelerator server software comes with a number of sample XML files. These files are in the `AcceleratorAdminWeb\Installation` subfolder of the

Compliance Accelerator program folder (typically C:\Program Files (x86)\Enterprise Vault Business Accelerator).

Table B-1 describes the sample XML files.

Table B-1 Sample XML files

File	Function
Dataload.xml	Explains how to load department and employee data to create a flat department structure.
Dataload_tree.xml	Gives an example of how to load the data to create a structured organization with nested departments.
DataLoadCaptureExclusions.xml	Gives some examples of how to exclude certain file types from review sets.

Format of the Dataload.xml file

You can use the `Dataload.xml` file with both Compliance Accelerator and Discovery Accelerator, so it contains some information that applies to both applications. However, the file is well documented and shows which sections apply to which application.

Table B-2 Primary Compliance Accelerator sections in Dataload.xml file

Section	Defines
ApplicationVaultStore	Vault stores that the application uses. This section is mandatory.
CaptureExclusions	Types of items, such as non-delivery reports and out-of-office replies, that the Journaling Connector is not to capture and add to the review set.
Employee	<p>Employees to add to the system, their email addresses, and any application roles to assign to them.</p> <p>Employees are identified using the <code>EmployeeID</code> field, which equates to the Employee ID box in the employee properties page of the Compliance Accelerator client. If you create some profiles using the Compliance Accelerator client and later want to update them using an XML file, ensure that each employee has a unique ID.</p>

Table B-2 Primary Compliance Accelerator sections in Dataload.xml file
(continued)

Section	Defines
EmployeeGroup	Employee groups, their members, and any application roles that are assigned to each group.
HotWordCategory	Global hotwords sets.
Attribute_n_Definition	Identity attributes that, when used in combination with the filter options in the Departments pane, let you hide or show selected departments in that pane.
Department	Departments. This section includes definitions of the following: <ul style="list-style-type: none"> ■ Department members and exception employees ■ The required review percentage for the department, groups, and individuals ■ Department roles that are assigned to individuals or groups ■ Vault stores for the department ■ Department hotword sets
Partition	Partitions, and the departments in them.
Proxy	Delegates for reviewers and compliance supervisors.
StandardReviewComment	Common comments that reviewers can add to the items that they review.

The second part of the file describes each XML entry. The last part of the file provides sample entries for a Compliance Accelerator system.

If you use any non-ASCII characters in a dataload file, you must specify the appropriate encoding. For example, you can save a file that contains accented European characters in Unicode format or add the following at the start of the file:

```
<?xml version="1.0" encoding="iso-8859-1" ?>
```

Importing the configuration data

You must have the Import Configuration Data permission to import configuration data from an XML file. By default, users with the application role of Compliance System Admin have this permission.

To import configuration data from an XML file

- 1 Click the **Configuration** tab in the Compliance Accelerator client, and then click the **Import Configuration** tab.
- 2 In the **Configuration file** box, type the full path to the XML file that you want to import, or click **Browse** and then choose the file to import.

The path can contain up to 250 characters.

You can specify a UNC path or NTFS path to the file if it is stored on a remote computer. For example:

```
\\server2\EVBA\import.xml
```

- 3 If you want to clear the import information from previous imports before you proceed, check **Clear log before import**.
- 4 Click **Import**.

About the ImportExport command

The ImportExport command provides a command-line alternative to the Compliance Accelerator client for importing data into a customer database. It also lets you export the data from the database to an XML file.

The command is installed in the Compliance Accelerator program folder on the Compliance Accelerator server, together with a configuration file,

```
ImportExport.exe.config.
```

You must have the Import Configuration Data permission to import data with ImportExport, and the Export Configuration Data permission to export the data. By default, users with the application role of System Admin have these permissions.

All newly imported departments comply with the U.S. government's Federal Information Processing Standards (FIPS).

Note: For the best results when using ImportExport on a computer in which User Account Control (UAC) is enabled, run the command with administrator privileges. Right-click the **Command Prompt** shortcut on the Windows **Start** menu, select **Run as Administrator**, and then type the command to start ImportExport. Otherwise, you may find that you cannot perform some operations with ImportExport, such as exporting data from a customer database to an XML file.

ImportExport syntax

```
ImportExport.exe -F:FileName -C:CustomerID [-I] [-L:LogFile] [-O]
[-NoValidation] [-BypassService] [-LogToDB] [-LeaveDBLog]
[-ShowOnlyErrors] [-CommitOnceOnSuccess] [-?]
```

[Table B-3](#) describes the parameters that you can append to the command.

Table B-3 ImportExport command parameters

Parameter	Function
-F: <i>FileName</i>	Identifies the XML file from which to import data or to which the data is to be exported.
-C: <i>CustomerID</i>	Identifies the Compliance Accelerator customer for which to import or export data. If you run ImportExport without any parameters then, when prompted for a customer ID, you can type ? to list all the customer names and identifiers.
-I	Instructs the command to import configuration data into the customer database from the XML file that you specify with the -F parameter. Omit this parameter to export data to the specified XML file.
-L: <i>LogFile</i>	Specifies the name of the log file. If you omit the path to the file, the command creates it in the Compliance Accelerator program folder on the Compliance Accelerator server.
-O	Overwrites the output XML file and log file, if they exist. If you omit this parameter, and the output and log files exist, the command displays an error message and stops.
-NoValidation	Accelerates the process of importing data from an XML file by turning off XML validation. The command ignores this parameter if you export data to a file.

Table B-3 ImportExport command parameters (continued)

Parameter	Function
-BypassService	<p>Instructs the command to bypass the Enterprise Vault Accelerator Manager service and connect directly to the customer database. This may be necessary if you experience out-of-memory problems when you try to import data into or export data from a very large database.</p> <p>To use this facility, you must ensure that:</p> <ul style="list-style-type: none">■ You have access permissions to the customer database.■ The <code>ImportExport.exe.config</code> file specifies the SQL Server for the Compliance Accelerator database as the DSN key. Each time you start the Enterprise Vault Accelerator Manager service, it automatically updates the DSN key value in this file to match the value that is specified in the <code>AcceleratorManager.exe.config</code> and <code>AcceleratorService.exe.config</code> files. So, if you specify a different value in the <code>ImportExport.exe.config</code> file, Compliance Accelerator overwrites it when you next start the service.
-LogToDB	<p>Writes the log messages to both the log file and the customer database.</p>
-LeaveDBLog	<p>If you also specify the <code>-LogToDB</code> parameter, instructs the command to leave log information on previous imports and exports in the Compliance Accelerator database instead of overwriting it.</p>
-ShowOnlyErrors	<p>If you also specify the <code>-LogToDB</code> parameter, instructs the command to report error messages but not information messages.</p>
-CommitOnceOnSuccess	<p>Commits the data to the Compliance Accelerator database only if the command imported it without error.</p>
-?	<p>Displays the online Help information for the command.</p>

Examples of ImportExport commands

The following command imports unvalidated data from the file `data.xml`, which is in the folder `C:\temp`. The log file, `import.log`, contains error messages only,

and the command overwrites the previous contents of the log file as it imports the XML data.

```
ImportExport.exe -C:2 -I -F:C:\temp\data.xml -NoValidation -O  
-L:import.log -ShowOnlyErrors
```

The following command exports the data in the Compliance Accelerator database to the XML file `export.xml`, which is in your `%USERPROFILE%` folder on the Compliance Accelerator server (`C:\Documents and Settings\username`). The command also overwrites the error messages that it has previously logged in the database.

```
ImportExport.exe -C:2 -F:export.xml -LogToDB -LeaveDBLog  
-ShowOnlyErrors
```


Troubleshooting

This appendix includes the following topics:

- [Vault stores not displayed](#)
- [Incorrect results when searching by message type and direction in archives that Enterprise Vault 4.0 or earlier has indexed](#)
- [Search returns unexpected results](#)
- [Errors when exporting items](#)
- [Synchronization errors after you rename the SQL Server computer](#)
- [Performance counter errors when the Accelerator Manager service starts](#)
- [Journaling Connector problems when you do not specify the vault IDs for multiple customers](#)
- [Enterprise Vault deduplication process does not work as expected in Exchange 2007 environments](#)
- [SQL Service Broker warning when restoring a customer database to a different server](#)
- [Issues with reports](#)

Vault stores not displayed

In those areas of the Compliance Accelerator client where you can select the vault stores in which to conduct searches, the absence of vault stores may indicate that the Enterprise Vault Directory service is not running. If this is the case, try starting the service. Ensure also that the same version of Enterprise Vault is running on the Compliance Accelerator and Enterprise Vault servers.

Incorrect results when searching by message type and direction in archives that Enterprise Vault 4.0 or earlier has indexed

If some Enterprise Vault archives in your site contain messages that Enterprise Vault 4.0 or earlier has indexed, you may find that any searches by message type and direction that you conduct with Compliance Accelerator do not return the expected results. This issue arises because earlier versions of Enterprise Vault did not add information to messages about the message type and direction. The issue does not affect older archives whose indexes you have rebuilt with Enterprise Vault 5.0 or later.

You can resolve this issue by setting two configuration options in Compliance Accelerator. These options specify the date on which you first installed or upgraded to Enterprise Vault 5.0 or later, and the date on which Enterprise Vault archived the oldest available data.

To specify the installation and oldest archived item dates in the Compliance Accelerator database

- 1 Click the **Configuration** tab in the Compliance Accelerator client, and then click the **Settings** tab.
- 2 Expand the **System** section to show the available options.
- 3 In the **Enterprise Vault Oldest Archived Item Date** row, click the **Value** column.
- 4 Select the date on which Enterprise Vault archived the oldest available data.
- 5 In the **Enterprise Vault V5 Installation Date** row, click the **Value** column.
- 6 Select the date on which you first installed Enterprise Vault 5.0 or later.
- 7 Click **Save**.

If the oldest archived item date and V5 installation date are the same then, when you enter the criteria for a search, you can specify the message type and direction without also specifying a start date. However, if the oldest archived item date is earlier than the V5 installation date, you can only specify the message type and direction if you specify a start date that is on or after the V5 installation date.

Search returns unexpected results

Symantec Support may request a search criteria file if you report a problem with searches that return unexpected results.

To generate the search criteria file

- 1 Click the **Configuration** tab in the Compliance Accelerator client, and then click the **Settings** tab.
- 2 Expand the **Diagnostics** section to show the available options.
- 3 In the **Save Search Criteria** row, check the option in the **Value** column.
- 4 Click **Save**.
- 5 Restart the Enterprise Vault Accelerator Manager service on the Compliance Accelerator server.
- 6 Rerun the searches.

On the Compliance Accelerator server, Compliance Accelerator creates a file that is called `Criteria_SearchID.txt` in the `SearchCriteria` subfolder of the Compliance Accelerator program folder. If the folder contains several files, you can identify the associated searches by hovering the mouse pointer over the search names in the Compliance Accelerator client.

Errors when exporting items

If you receive the following error message when you export items, the version of the file `mapisvc.inf` on the Compliance Accelerator server may be incorrect.

```
Error      Failed to write the file:
The EVPSTAPI COM object has not been initialized
```

To fix MAPI problems

- 1 In Windows Explorer, browse to the `%windir%\system32` folder on the Compliance Accelerator server.
- 2 Double-click `fixmapi.exe` to run the MAPI repair tool. Note that this tool does not appear to do anything when you run it.
- 3 Restart the Compliance Accelerator server.
- 4 Test whether the problem has been fixed.

If you cannot fix the problem by running FIXMAPI.EXE

- 1
- In the %windir%\system32 folder on the Compliance Accelerator server, rename the existing mapisvc.inf file.
- 2
- Copy the version of mapisvc.inf that comes with Microsoft Outlook to the %windir%\system32 folder. This version is typically in the following folder:

C:\Program Files\Common Files\System\MSMAPI\locale_ID

where locale_ID is the numeric identifier for your locale. The following table lists some common locale identifiers.

Chinese Simplified	2052	Hebrew	1037
Chinese Traditional	1028	Italian	1040
Danish	1030	Japanese	1041
Dutch	1043	Portuguese	2070
English U.S.	1033	Spanish	3082
French	1036	Swedish	1053
German	1031		

- 3
- Restart the Compliance Accelerator server.

If you receive the following message when you export data from Compliance Accelerator, two or more employees may have the same EmployeeID.

Error: APP AT - Customer ID: 17 - An Error has occurred when exporting the data.
Description: System.Data.ConstraintException: Failed to enable constraints. One or more rows contain values violating non-null, unique, or foreign-key constraints.

You can fix this problem by deleting the mapping between the Compliance Accelerator EmployeeID property and the corresponding Active Directory attribute. Then, after you have performed the export run, you can restore the mapping between the EmployeeID property and Active Directory attribute.

To delete the Active Directory mapping

- 1
- Click the **Configuration** tab in the Compliance Accelerator client, and then click the **Directory Mappings** tab.
- 2
- Click the **EmployeeID** property name in the left column.
- 3
- Click **Delete**.

Synchronization errors after you rename the SQL Server computer

If you rename the SQL Server computer, the following message may appear in the event log of the Compliance Accelerator server when the Compliance Accelerator database synchronizes with SQL Server:

Cannot add, update, or delete a job (or its steps or schedules) that originated from an MSX server. The job was not saved.

For more information on this problem and guidelines on how to resolve it, see the following article in the Microsoft Knowledge Base:

<http://support.microsoft.com/?kbid=281642>

You may also be able to fix the problem by running a script on the SQL Server computer.

To fix synchronization errors by running a SQL script

- 1 Connect to your SQL Server with Query Analyzer.
- 2 Type the following command to access the msdb database:

```
USE msdb
```

- 3 Run the following script:

```
DECLARE @srv sysname SET @srv = CAST(SERVERPROPERTY('server_name')
AS sysname) UPDATE sysjobs SET originating_server = @srv
```

where you must replace *server_name* with the new name of your SQL Server computer.

Performance counter errors when the Accelerator Manager service starts

When the Enterprise Vault Accelerator Manager service starts, the following error messages may appear in the event log of the Compliance Accelerator server:

```
Event Type:      Error
Event Source:    Accelerator Manager
Event Category:  None
Event ID:        41978
Description:     APP ATM - Error: deleting Performance Counters
Description:     Input string was not in a correct format.
```

```
Event                Type:Error
Event                Source:Accelerator Manager
Event Category:      None
Event ID:             41980
Description:          APP ATM - Error: Creating Performance Counters
Description:          Input string was not in a correct format.
```

For more information on this problem and guidelines on how to resolve it, see the following article in the Microsoft Knowledge Base:

<http://support.microsoft.com/?kbid=300956>

Journaling Connector problems when you do not specify the vault IDs for multiple customers

When both the following conditions apply, you may see errors in the event log when the Journaling task starts. In addition, the Journaling Connector stops working.

- You have two or more Compliance Accelerator customers for which you did not specify a vault ID.
You have the option to specify a vault ID when you define the properties of a customer with the Accelerator Manager Web site. Each vault ID identifies a journal mailbox from which the customer may take a random sample of items.
- You use the default sampling method, guaranteed sampling, to capture items for inclusion in the review set.

To fix this problem, use the Accelerator Manager Web site to check the properties of each customer and ensure that you have specified a vault ID in each case. You can use the Vault Administration Console to obtain the required vault ID.

Enterprise Vault deduplication process does not work as expected in Exchange 2007 environments

In a Microsoft Exchange 2007 environment, the *deduplication* process with which Enterprise Vault minimizes the number of duplicate items that it archives does not work as expected. When Microsoft Exchange 2007 journals an item that has both individual recipients and one or more distribution lists, Enterprise Vault may archive it several times—and consequently the Journaling Connector may fail to capture it correctly.

This issue arises because of a change in the way that Microsoft Exchange 2007 deals with items that are addressed to both individual recipients and distribution

lists. For more information, see the following article on the Symantec Enterprise Support Web site:

<http://www.symantec.com/docs/TECH51325>

SQL Service Broker warning when restoring a customer database to a different server

SQL Server may record the following warning message in the event log if you restore a Compliance Accelerator customer database to a different server than that on which it originally resided:

```
Service Broker needs to access the master key in the database
'database_name'. Error code:25. The master key
has to exist and the service master key encryption is required.
```

You can suppress this warning message by using the following SQL Server command to create a master key for the database:

```
CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'password'
```

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

[http://msdn.microsoft.com/en-us/library/aa337551\(SQL.90\).aspx](http://msdn.microsoft.com/en-us/library/aa337551(SQL.90).aspx)

Issues with reports

A number of issues can arise when you generate, print, or export reports from the Compliance Accelerator client.

Compliance Accelerator reports may not work correctly until you install the Support for Crystal Reports Web site

If you do not choose to install the Support for Crystal Reports Web site when you install the Compliance Accelerator server software, some report features in Compliance Accelerator may not work. You may therefore need to install this Web site even if you do not have any legacy reports in Crystal Reports format. Follow the steps below to modify your existing Compliance Accelerator installation.

To install the Support for Crystal Reports Web site

- 1 Log on to the Compliance Accelerator server as the Vault Service account.
- 2 In Control Panel, select **Add or Remove Programs**.

- 3 In the Add or Remove Programs dialog box, click **Symantec Enterprise Vault Compliance Accelerator**.
- 4 Click **Change**.
- 5 On the first page of the setup wizard, click **Next**.
- 6 On the second page, click **Modify**.
- 7 On the Prerequisites page, check **I have read and met the above prerequisites** and then click **Next**.
- 8 On the Prerequisite Status page, click **Next**.
- 9 On the Custom Setup page, choose to install the Support for Crystal Reports Web site, and then click **Next**.
- 10 On the Ready to Install page, click **Install**.
- 11 Click **Finish** to exit from the Compliance Accelerator installation program.

You receive the message "An error occurred creating the report" when you try to generate reports

If you receive the following message when you try to generate a report, it is possible that the report templates were uploaded to the SQL reporting server with the wrong logon credentials:

```
An error occurred creating the report
```

```
An error has occurred during report processing ---> ...  
Cannot impersonate user for data source 'CustomerDatabase'. --->  
Logon failed. ---> Logon failure: unknown user name or bad password.  
(Exception from HRESULT: 0x8007052E)
```

The Accelerator Manager Web site does not authenticate the logon credentials that you enter when you upload the templates to the reporting server. Consequently, if you omit the credentials or enter the wrong ones, account validation issues occur when you subsequently generate a report.

For guidelines on how to upload the report templates to the SQL reporting server, see the *Installation Guide*.

Prompt to install SQL Server when printing a report for the first time

When you print a report for the first time from the Compliance Accelerator client, a Security Warning window prompts you to install Microsoft SQL Server. This is a known issue in Microsoft SQL Server Reporting Services, which requires you to download an ActiveX control for client-side printing of reports. To resolve this

issue, enable the setting **Download signed ActiveX controls** in Internet Explorer so that you can install the required control.

To change the security settings in Internet Explorer

- 1 In Microsoft Internet Explorer, click **Tools > Internet Options**.
- 2 Click the **Security** tab.
- 3 Select the **Trusted sites** zone, and then click **Sites**.
- 4 Type the URL of the SQL reporting server.
- 5 Click **Add**, and then click **Close**.
- 6 Click the **Custom level** button.
- 7 Scroll to the **ActiveX controls and plug-ins** node.
- 8 Click **Enable** for **Download signed ActiveX controls**, and then click **OK**.

Scripts errors when printing reports from the Compliance Accelerator client in SQL Server 2005 SP2 environments

In a Compliance Accelerator environment where you are running SQL Server 2005 SP2, the following error message may appear when you print reports from the Compliance Accelerator client:

```
An error has occurred in the script on this page.
...
Could not complete the operation due to error 8007f305.
```

You can resolve this issue by upgrading to SQL Server 2005 SP3.

Reports that you export as CSV may not open properly in Microsoft Excel

By default, SQL Reporting Services exports CSV files with Unicode encoding rather than ANSI encoding. The data in a Unicode-encoded CSV file does not tabulate properly when you open it in Microsoft Excel.

To work around this problem

- 1 Locate the file `rsreportserver.config` in the SQL Reporting Services installation folder.
- 2 Open the file in a text editor such as Windows Notepad.

- 3 Comment out the following text block by enclosing it in the marks `<!--` and `-->`:

```
<Extension Name="CSV" Type="Microsoft.ReportingServices.Rendering.CsvRenderer.CsvReport, Microsoft.ReportingServices.CsvRendering"/>
```

- 4 Add the following text block:

```
<Extension Name="CSV" Type="Microsoft.ReportingServices.Rendering.CsvRenderer.CsvReport, Microsoft.ReportingServices.CsvRendering">
<Configuration>
  <DeviceInfo>
    <Encoding>ASCII</Encoding>
  </DeviceInfo>
</Configuration>
</Extension>
```

- 5 Save and close the file.

After you have edited the configuration file, SQL Reporting Services ignores any Unicode characters that were stored in the initial report.

Garbled Japanese characters when exporting reports in Acrobat format

If the Japanese characters in a Compliance Accelerator report are garbled when you export the report in Acrobat (PDF) format, you may be able to resolve the problem by taking the following steps:

- Ensure that you have installed the supplemental files for East Asian languages on the SQL reporting server. To do this, open Regional and Language Options in Control Panel and then, on the Languages tab, check **Install files for East Asian languages**.
- Install version 5.00 or later of the Microsoft Gothic font on the SQL reporting server. This version is supplied with Windows Vista and Windows 7, but most other versions of Windows come with version 2.30. See this page for more information:
<http://www.microsoft.com/typography/fonts/font.aspx?FMID=1610>
- Upgrade to SQL Server Reporting Services 2008.

Index

A

- Accelerator Manager service
 - introduction to 14
 - performance counter errors at start-up 207
- Accelerator Manager Web site
 - introduction to 14
- action statuses, customizing 155
- Active Directory attributes
 - mapping to employee properties 30
- Ad Hoc Searches configuration settings 156, 158
- Add Hotwords permission 36, 40, 94, 97
- Add Monitored Employees permission 36, 40, 56, 58, 65
- Add Own Review Comments permission 40, 113
- Add Standard Review Comments permission 40, 113
- adding
 - department attributes 69
 - department partitions 67
 - departments 50
 - employee groups 32
 - employees and groups to departments 56
 - exception employees 64
 - folders 124
 - new directory mappings 30
 - roles 44
- Allow Archive Selection in Research Folders permission 40
- amending
 - directory mappings 30
 - employee details 32
 - hotword sets 98
 - hotwords 96
 - monitoring policy for employees and groups 56
- App Rule Admin role 36, 92, 94, 96–99, 120
- App User Admin role 32, 44, 46, 50, 58, 67, 74
- Application roles 36
- Application Search permission 36, 40, 74
- Apply Appraisal Status permission 36, 40
- Apply Bulk Actions to Escalations permission 36, 40
- Apply Bulk Review Action permission 40
- Apply Comments to Escalations permission 36, 40

- Apply Review Action permission 40
- Apply Review Action to Escalations permission 36, 40
- appraisal statuses, customizing 155
- archives, selecting the archives to search 89
- Assign % Review permission 32, 56
- Assign % Review Requirement permission 36, 40
- Assignment Bypass permission 36, 40

B

- Bloomberg messages 56

C

- Capture Messages role. 36
- Change Escalation Status permission 36, 40
- changing
 - directory mappings 30
 - employee details 32
 - hotword sets 98
 - hotwords 96
 - monitoring policy for employees and groups 56
- Chinese walls security restrictions 38, 41, 61, 157, 187
- comments
 - adding to review items 113
 - storing for reuse 120
- Commit Appraised Folder Messages permission 36, 40, 127
- Commit Messages role 36, 127
- Commit Research Items Marks and Comments permission 40
- Commit Reviewed Folder Messages permission 36, 40, 127
- committing folder items to review set 127
- Compliance Supervisor Responsibility report 138, 140
- Compliance Supervisor role 36, 64, 66–67, 113, 125
- Compliance System Admin role 30, 36, 69, 153, 155, 197
- configuration database
 - introduction to 14

configuration settings

- Ad Hoc Searches 156, 158
- Diagnostics 156, 159
- Document Conversion 156, 160
- Export/production 156, 160
- General 156, 164
- Home Page 156, 166
- Item Prefetch Cache 156, 167
- Item Prefetch Cache (Advanced) 156, 170
- Policy Integration 156, 172
- Profile Synchronization 156, 175
- Random Capture 157, 176
- Reviewing 157, 179
- Search 157, 182
- Security 157, 187
- System 157, 188, 204
- Vault Directory Synchronization 157, 189

Configure Department Properties permission 36, 40, 70

Copy Research Items permission 40

Create Departments permission 36, 40, 50, 58

creating

- department attributes 69
- department partitions 67
- departments 50
- employee groups 32
- exception employees 64
- folders 124
- hotword sets 97
- hotwords 94
- new directory mappings 30
- reports 137
- reviewing comments 120
- roles 44
- search schedules 92
- searches 74

Crystal Reports Web site

- introduction to 14
- viewing reports in 152

customer databases

- introduction to 14

D

Dataload.xml file 196

Dataload_tree.xml file 196

DataLoadCaptureExclusions.xml file 196

deduplication 17, 208

Delete Department permission 36, 40

Delete Folder permission 36, 40

deleting

- exception reviewers 67
- hotword sets 99
- hotwords 97
- reports 151

department attributes 49

- assigning to departments 70
- overview of 68
- setting up 69

Department Reviewer role 36, 104, 113, 118–119, 125, 127

Department reviewer role 58, 60

Department reviewers, assigning and removing 60

department roles 36

Department Roles Detail report 138, 140

Department Roles Summary report 138, 141

Department User role 36

departments

- adding employees and groups to 56
- and FIPS compliance 198
- assigning department reviewers 60
- classifying with identity attributes 68
- creating 50
- grouping into partitions 67
- moving 58
- moving employees and groups between 58

Diagnostics configuration settings 156, 159

Differential Sampling Summary by Department report 138, 142

Document Conversion configuration settings 156, 160

documentation 17

Domino directory attributes, mapping to employee properties 30

E

editing

- directory mappings 30
- employee details 32
- hotword sets 98
- hotwords 96
- monitoring policy for employees and groups 56

Effective Roles by User report 138, 143

employees

- adding to departments 56
- assigning roles to 36, 46
- changing directory mappings 30
- deleting 32
- editing 32

employees (*continued*)
 editing monitoring policy for 56
 managing exception employees 64
 mapping properties to directory attributes 30
 moving between departments 58
 Enterprise Vault Accelerator Manager service
 introduction to 14
 performance counter errors at start-up 207
 Escalate Messages permission 36, 40, 118
 escalating items 118
 Escalation Reviewer role 36, 60, 104, 118–119, 125
 escalation statuses, customizing 155
 Evidence of Review by Department/Employee
 reports 143
 Evidence of Review reports 139
 Exception Reviewer role 36, 88, 104, 113, 118, 125
 Exception reviewer role 58, 60, 64, 66–67, 74
 exceptions
 assigning reviewers to 64
 exporting the items of 134
 managing 64
 moving to another department 65
 removing exception status from 66
 searching the items of 88
 setting up 64
 Export Configuration Data permission 36
 Export Escalations permission 36, 40, 130
 export IDs 134
 Export Messages permission 36, 40, 126, 130
 Export Research Items permission 40
 Export role 36, 126
 Export/production configuration settings 156, 160
 exporting
 an exception's items 134
 creating an export run 129
 introduction to 129
 items from folders 126
 limits on number of simultaneous runs 133
 optimizing export runs 133
 troubleshooting 205
 external addresses, defining 100

F

Fax messages 56
 FIPS compliance 198
 FIXMAPI.EXE 205
 folders
 committing items to review set 127
 copying items to 125

folders (*continued*)
 creating 124
 exporting items from 126
 giving other users access to 127
 introduction to 123
 predefined roles for 36
 reviewing the items in 125
 Full Control role 36, 125–127

G

General configuration settings 156, 164
 Grant Users Access permission 36, 40, 46, 56, 60, 65
 groups
 adding to departments 56
 assigning roles to 36, 46
 editing monitoring policy for 56
 moving between departments 58
 setting up 32
 guaranteed sample searches 78

H

Home Page configuration settings 156, 166
 Hotphrases (English).xml 94, 99
 hotword sets
 deleting 99
 editing 98
 introduction to 94
 setting up 97
 hotwords
 creating 94
 deleting 97
 editing 96
 importing 99
 introduction to 94
 Hotwords (English).xml 94, 99
 "How To" articles on Support site 18

I

icons in Compliance Accelerator client 23
 identity attributes
 assigning to departments 70
 overview of 68
 setting up 69
 Import Configuration Data permission 36, 40, 198
 ImportExport command 198
 importing
 configuration data 196, 198
 predefined hotwords 99

- instant messages 56
- internal addresses, defining 100
- InternalSMTPDomains registry value 101
- Item Aging by Department report 139, 144
- Item Prefetch Cache (Advanced) configuration settings 156, 170
- Item Prefetch Cache configuration settings 156, 167
- items
 - committing to review set 127
 - copying to folders 125
 - exporting from folders 126
 - reviewing folder messages 125

J

- Journaling Connector
 - introduction to 15
 - troubleshooting 208

M

- Manage Delegates permission 36, 40
- Manage Department Partitions permission 36, 40, 67
- Manage Department Users permission 36
- Manage Employees permission 32, 36, 40
- Manage Exceptions permission 36, 40, 64–67
- Manage Reviewing Comments permission 36, 40, 120
- Manage Roles permission 36, 40, 44
- Manage Schedules permission 36, 40, 92
- manuals and Help files 17
- mapisvc.inf version 205
- marks
 - assigning in the Review pane 112
- Message Stats Summary report 139, 144
- Message Summary report 139, 145
- Microsoft Exchange 56
- Microsoft Outlook, making export ID visible in 134
- Modify & Delete Hotwords permission 36, 40, 96–99
- Modify System Configuration permission 30, 36, 40, 69, 155–156
- modifying
 - directory mappings 30
 - employee details 32
 - monitoring policy for employees and groups 56
- Monitor Search permission 36, 40
- Monitor Searches tab 86
- Monitored IDs by Department report 139, 145
- monitoring policy 56

N

- nested departments 50

O

- Outlook, making export ID visible in 134

P

- partitions
 - creating 67
 - introduction to 49, 67
- Passive Reviewer role 36, 60
- Passive reviewer role 104
- Perform Ad Hoc Searches permission 36, 40, 124–125
- permissions, overview of 40
- Personal Folders (.pst) files 134
- Policy Integration configuration settings 156, 172
- printable versions of review items 114
- product documentation 17
- Profile Synchronization configuration settings 156, 175
- profiles
 - changing directory mappings 30
 - deleting 32
 - editing 32
 - mapping properties to directory attributes 30
- Promote Research to Department permission 40

Q

- Questioned Items by Department report 139, 146

R

- Random Capture configuration settings 157, 176
- removing
 - employee details 32
 - exception reviewers 67
 - exception status from employees 66
 - hotword sets 99
 - hotwords 97
 - reports 151
- reports
 - Compliance Supervisor Responsibility 138, 140
 - creating 137
 - deleting 151
 - Department Roles Detail 138, 140
 - Department Roles Summary 138, 141

reports *(continued)*

- Differential Sampling Summary by Department 138, 142
 - Effective Roles by User 138, 143
 - Evidence of Review 139
 - Evidence of Review by
 - Department/Employee 143
 - in Crystal Reports format 152
 - introduction to 137
 - Item Aging by Department 139, 144
 - Message Stats Summary 139, 144
 - Message Summary 139, 145
 - Monitored IDs by Department 139, 145
 - Questioned Items by Department 139, 146
 - Responsibility by Department 139, 146
 - Responsibility by Reviewer 139, 147
 - Review Activity Summary 139
 - Review Activity Summary by Department 139, 147
 - Reviewer Activity by Department 148
 - Reviewer Activity Detail 148
 - Reviewer Activity Detail 139
 - Reviewer Mapping 139, 149
 - troubleshooting 209
 - Unreviewed Departments 140, 150
 - Unsupervised Departments 140, 150
 - viewing 151
- research folders. *See* folders
- Responsibility by Department report 139, 146
 - Responsibility by Reviewer report 139, 147
 - Review Activity Summary by Department report 139, 147
 - Review Activity Summary report 139
 - Review Escalations permission 36, 40
 - Review Messages permission 40, 115, 125
 - Review pane
 - adding comments to items in 113
 - areas of 104
 - assigning review marks in 112
 - changing the appearance of 115
 - closing escalated items with 119
 - copying the item list in 115
 - customizing columns in 191
 - displaying printable items in 114
 - downloading the original versions of items with 114
 - escalating items in 118
 - filtering the items in 108
 - reassigning escalated items with 119

Review pane *(continued)*

- setting display and operation preferences 116
 - viewing the history of items in 113
- Review role 36, 125, 127
- Reviewer Activity by Department report 148
- Reviewer Activity Detail report 139, 148
- Reviewer Mapping report 139, 149
- Reviewing configuration settings 157, 179
- reviewing items
 - adding comments to items 113
 - assigning escalated items to another reviewer 119
 - assigning review marks 112
 - closing escalated items 119
 - committing to review set 127
 - configuring status marks 155
 - copying the item list to the Clipboard 115
 - copying to folders 125
 - displaying printable versions of items 114
 - downloading the original versions of items 114
 - escalating items 118
 - exporting from folders 126
 - exporting or producing 129
 - in folders 125
 - introduction to 103
 - storing comments for reuse 120
 - viewing comments and audit history 113
- roles
 - assigning to employees and groups 36, 46
 - associated permissions 40
 - creating 44
 - predefined roles 36
- Rule Admin role 32, 36, 56, 64, 66–67, 74, 94, 96–99

S

- Search Capture permission 36, 40, 74
- Search configuration settings 157, 182
- search criteria file 204
- search schedules
 - examples of 93
 - introduction to 91
 - setting up 92
- searches
 - about the criteria options 76
 - and deduplication 17
 - creating and running 74
 - guidelines on conducting 85
 - introduction to 74
 - pausing and resuming 86

searches *(continued)*

- searching the items of an exception employee 88
- selecting the archives to search 89
- troubleshooting 204

Security configuration settings 157, 187

setting up

- department attributes 69
- department partitions 67
- departments 50
- employee groups 32
- exception employees 64
- folders 124
- hotword sets 97
- hotwords 94
- new directory mappings 30
- reports 137
- reviewing comments 120
- roles 44
- search schedules 92
- searches 74

Show Reviewer Summaries On Home Page

- permission 36, 40

SQL Server Agent service 91–92

SQL Server Enterprise Manager 92

storing comments for reuse 120

Support for Crystal Reports Web site

- introduction to 14
- viewing reports in 152

System configuration settings 157, 188, 204

T

tabs in Compliance Accelerator client 23

U

Unreviewed Departments report 140, 150

Unsupervised Departments report 140, 150

User Admin role 36, 46, 56, 58, 60, 64–67, 70

V

Vault Directory Synchronization configuration

- settings 157, 189

vaults, selecting the vaults to search 89

View Reports permission 40, 151

View System Configuration permission 30, 36, 40, 69

viewing reports 151–152

W

white papers 18

X

XML dataload files 99, 196, 198