Veritas Compliance Accelerator™ 12.2 ReadMeFirst

Last updated: 03-Jul-2017

The latest version of this document is available from the Veritas Support website in the following languages: English, Japanese, and Simplified Chinese.

For the latest news about this release, including any hotfixes, subscribe to http://www.veritas.com/docs/000115776.

This document describes the new features in Veritas Compliance Accelerator 12.2.

If you are performing a new installation of Compliance Accelerator, follow the instructions in the *Installation Guide*. If you are upgrading, follow the instructions in *Upgrade Instructions*. These documents are in the `Veritas Enterprise Vault Compliance Accelerator\Documentation\English` folder on the Compliance Accelerator media.

Contents

New features in Compliance Accelerator 12.2

Compliance Accelerator 12.2 includes the following new features. For more information on these features, see the *Administrator's Guide*.

Option to prevent exception employees from self-reviewing the items that they have sent or received

For those users who have a department reviewer role in Compliance Accelerator but whom you have also designated as exception employees, this release lets you prevent such users from reviewing the items that they themselves have sent or received. By default, Compliance Accelerator allows such users to self-review their items. This can lead to the situation where, for example, an item that an exception employee has sent to a non-exception employee can appear in both of the following review sets:

- The exception reviewer's review set, because the sender is an exception employee. The exception employee does not have access to this review set.

- The department review set, because the recipient is not an exception employee. The exception employee who sent the item may be able to access this review set through the department reviewer role, and so assign a review mark to the item.

To prevent exception employees from self-reviewing items, follow these steps:

1. In the Compliance Accelerator client, click the **Configuration** tab and then click the **Settings** tab.
2. Expand the **Reviewing** section to show the available options.
3. In the **Prevent self-review** row, select the option in the **Value** column.
4. Click **Save**.

Effects of setting the Prevent self-review option

Setting the **Prevent self-review** option has the following consequences for Compliance Accelerator users who are reviewing the items in a department where they are also exception employees:

- These users cannot preview, mark, or add comments to the items that they have sent or received. For example, the users now receive the following message when they attempt to preview a message that they are blocked from viewing:

  ```
  You are not authorized to review this item.
  Contact your administrator for help.
  ```

  In addition, these users cannot display printable versions of the items, view the history of the items, download them in their original form, or view the comments that other reviewers have added.

- When these users mark or add comments to multiple items at once, Compliance Accelerator processes only those items that the users are eligible to review. It ignores the items that these users are blocked from viewing. Note that Compliance Accelerator takes longer than normal to process bulk-reviewed items in these circumstances.
- The same restrictions on marking and adding comments to items in the department review set apply to research folders as well. However, exception employees may still commit their own items from a research folder to the department review set, delete these items from the research folder, or copy them to another research folder.

For the best results, note the following when choosing to prevent self-reviews:

- The **Prevent self-review** option is an application-wide option that applies to all Compliance Accelerator customers.
- The option does not apply to escalation reviewers, who can continue to self-review their own items. Therefore, you should not give users the role of escalation reviewer in a department where they are also exception employees. However, it is fine to give users the role of escalation reviewer in one department and exception employee in another.
- If possible, avoid making exception employees the delegates for other reviewers or supervisors. The exception employees may be unable to fulfil all their delegate responsibilities because they are blocked from reviewing their own items.

- Take care when explicitly assigning items to others for review. If you assign items to exception employees that they have sent or received, they cannot review them.
- Users who have a reviewing role in a department where they are also exception employees can still self-review items that Compliance Accelerator has added to the review set from the *mailbox* archives. However, this is not the case for items that Compliance Accelerator has added to the review set from the *journal* archive.

Known issues and limitations

If the temporary folders that Compliance Accelerator uses do not meet security requirements, it stops running [3134031]

On both server and client computers, Compliance Accelerator performs a check every minute to verify that only authorized users can access various folders that it uses for temporary storage. On server computers, Compliance Accelerator checks the security of these folders:

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

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

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

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

If the security check fails on the Compliance Accelerator server, the Enterprise Vault Accelerator Manager service stops and the following error event is recorded in the Veritas Enterprise Vault event log:

```
Source:    Accelerator Manager
Event ID:  585
Level:     Error
Description:
The Accelerator Manager service will be stopped because the temporary folder
folder_name does not satisfy security requirements.
```

If the security check fails on a Compliance Accelerator client computer, the user must choose to rerun the check or close the client.

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

For more information on Compliance Accelerator temporary folder requirements, see the following article on the Veritas Support website:

http://www.veritas.com/docs/000023496

A security warning may appear when you preview certain items in the Review pane of the Compliance Accelerator client [3512512]

The following message may appear in the Review pane of the Compliance Accelerator client when you try to display an HTML preview of certain items:

```
Content within this application coming from the
website listed below is being blocked by Internet
Explorer Enhanced Security Configuration.

about:security_AcceleratorClient.Exe
```

To resolve the issue, add `about:security_AcceleratorClient.Exe` to the Local intranet zone or Trusted sites zone in Internet Explorer. See the Internet Explorer documentation for guidelines on how to do this.

TNEF-encoded attachments to Internet Mail (.eml) messages may not be readable after you export the messages from a department review set [3481292]

After you export Internet Mail (`.eml`) messages in their original form from a department review set, the contents of any TNEF-encoded attachments to the messages may not be readable.

TNEF-encoded attachments are commonly created by dragging and dropping a file into an Outlook mailbox folder. They are usually named `winmail.dat`.

Display issues when you run the Compliance Accelerator client in Windows 8 or later [3151239]

You may experience display issues in certain areas of the Compliance Accelerator client when you run it in Windows 8 or later. If you experience these issues, you can work around them by running the client in compatibility mode for Windows 7 or Windows XP (Service Pack 3).

Documentation

The Compliance Accelerator 12.2 documentation is available in English, Japanese, Simplified Chinese, and Traditional Chinese in the `Veritas Enterprise Vault Compliance Accelerator\Documentation` folder on the Compliance Accelerator media. The latest versions of the documentation are available on the Veritas Support website at http://www.veritas.com/docs/000115777.

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 12.2.
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.
ReadMeFirst (this file)	Provides late-breaking information that you may need to be aware of before you install and use Compliance Accelerator.
Compatibility Charts	Provides compatibility information for Enterprise Vault, Compliance Accelerator, and Discovery Accelerator. To obtain this guide, go to the following page of the Veritas Support website: http://www.veritas.com/docs/000097605

White papers

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 Veritas Support website:

http://www.veritas.com/docs/000002529

For extensive information on the enhanced reporting features in Compliance Accelerator, see the white paper that is available from the following page:

http://www.veritas.com/docs/000100833

Legal notice

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com