

Veritas Alta™ View Compliance and Governance User Guide

Veritas Alta™ View Compliance and Governance User Guide

Last updated: 2023-03-24

Legal Notice

Copyright © 2023 Veritas Technologies LLC. All rights reserved.

Veritas, the Veritas Logo, Enterprise Vault, and Enterprise Vault.cloud are trademarks or registered Trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

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 Veritas Technologies LLC 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. VERITAS TECHNOLOGIES LLC 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.

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

<http://www.veritas.com>

Contents

Chapter 1	Getting started	8
	About Veritas Alta View Compliance and Governance Management Console	8
	Prerequisites for using Veritas Alta View Compliance and Governance Management Console	10
	Veritas Alta View Compliance and Governance Management Console web browser support	10
	What's new in this release	11
	Signing in to Veritas Alta View Compliance and Governance Management Console	11
	Signing out from Veritas Alta View Compliance and Governance Management Console	14
	Resetting a forgotten password	14
	Changing your profile password	16
Chapter 2	Archive Overview	18
	About Archive Overview	18
	Archive Usage	19
	Sync Activity	20
	Roles	21
	Viewing the Archive Usage Snapshot report	21
Chapter 3	Working with Dashboard	23
	About dashboard	23
	Viewing and exporting statistics of Alta Capture-specific archives	24
	Viewing and exporting mail statistics of EVC-specific archives	26
Chapter 4	Managing Configurations	27
	About the Configuration page	27
	Viewing provisioned services	28
	Selecting the User Management options	28
	About Provisioning	30
	Configuring the Alta Personal Archive deployment options	30
	Configuring the administrator notification options	32

CloudLink Sync Summary	33
About Managed Tags	33
Creating a managed tag	34
Assigning a managed tag to users	35
Changing the retention policy associated with a managed tag	36
Deleting a managed tag	37
About Account Management	38
Searching for archive accounts	39
Using search filters	42
Creating an archive account	43
Viewing and editing the archive account details	49
About the Account Details page	51
Deleting an archive account	55
Deploying users	56
Enabling services for existing archive accounts	58
Removing user access	59
Disabling bulk user accounts	61
Editing Mobile Web Access permission for existing archive accounts	63
Unlocking an archive account	65
Exporting archive account information	65
Editing contact details of a system administrator	65

Chapter 5	Managing Archive Collectors	67
	About Archive Collectors	68
	Adding new archive collectors	68
	Updating configuration of existing archive collectors	69
	Stopping the import job of archive collectors	70
	Restarting import job of archive collectors	70
	Viewing the latest status of Archive Collectors	71
	Deleting an existing archive collector	72
	About Exchange Online Archiving	73
	Setting up modern authentication in Azure AD for Exchange Online sync	73
	Configuring Exchange Online sync	77
	About Exchange Online folder synchronization	83
	Prerequisite for migrating Exchange Online Users configured with Folder Sync to Exchange Online Folder Synchronization	84
	Configuring Exchange Online folder synchronization	84
	About Bloomberg Archiving	91

	Configuring the Bloomberg Synchronization	92
	About Microsoft Teams Archiving	93
	Registering a Microsoft Azure App for Teams Collector	94
	Requesting access to protected APIs in Microsoft Graph	98
	Enabling Microsoft Teams Archiving service for customer	101
	Configuring Microsoft Teams Synchronization	102
	About OneDrive for Business Archiving	105
	Registering a Microsoft Azure App for OneDrive for Business Collector	105
	Enabling the OneDrive for Business Archiving service for customer	111
	Configuring OneDrive for Business Synchronization	113
	About Data Uploading	116
	Configuring data uploading collection	116
	About Alta Capture Services Archiving	118
	Enabling Alta Capture Services for Archiving	120
	Configuring Capture Services for Archiving	122
Chapter 6	Managing Roles and Permissions	127
	About Role Management	127
	Editing the built-in administrator roles	128
	Creating custom administrator roles	129
	Assigning administrator roles to an archive account	130
	Assigning the reviewer role to an archive account	132
	Assigning several archive accounts for monitoring	134
Chapter 7	Managing Policies	137
	About Policy Management	137
	Configuring archive options	138
	Enabling and disabling account archiving	141
	Configuring an advanced password policy	143
	Configuring trusted networks for Veritas Alta Archiving access	145
	Managing Custom Headers	145
	Managing Discard Rules	146
Chapter 8	Managing Authentication	148
	Configuring the Veritas Alta Archiving authentication service	148
	Enabling the Authentication Settings permission for the Policy Manager role	149
	Assigning the Policy Manager role to an administrator	150
	Selecting an authentication method	150

	Uploading a token-signing certificate	153
	Validating the Identity Provider URL	154
	Activating single sign-on	155
Chapter 9	Managing Retention Policies	156
	About Retention Management	156
	Configuring the default retention period	157
	Creating a retention policy	158
	Editing a retention policy	159
	Deleting a retention policy	159
	Associating a retention policy with a policy target	160
	Disassociating a retention policy from a policy target	160
	Enabling and disabling the storage expiry setting	161
	Viewing the storage expiry status table	162
Chapter 10	Managing Email Continuity Services	164
	About Email Continuity	164
	Email Continuity prerequisites	165
	Configuring Email Continuity	165
	Provisioning the Email Continuity service for your mail servers	166
	Adding the Email Continuity IP ranges to your firewall and mail server allowlists	167
	Updating your email security provider routing configuration	167
	Testing the Email Continuity configuration	168
	Managing Email Continuity	168
	Email Continuity FAQ	169
Chapter 11	Managing Reports and Notifications	170
	About Veritas Alta Archiving reports, logs, usage, and notifications	170
	Reports	170
	Generating a Messaging Report	170
	Generating a Personal Archive Report	171
	Generating a Mobile Web Access Report	172
	Generating a Discovery Archive Report	173
	Generating an Advanced Supervision specific Report	173
	Usage	174
	Generating a service usage report	174
	Generating a mailbox statistics report	175
	Generating an archived message size report	176
	Logs	177

	Viewing the Activity Log	177
	Viewing the Message Log	178
	Viewing the Usage Log	178
	Creating a Retention Log Report	179
	Viewing the Mobile Browser Log	179
	Viewing the Personal Browser Log	179
	Viewing the Discovery Browser Log	180
	Notifications	180
	Enabling or disabling usage notifications	180
	Changing the usage notification threshold and frequency	181
	Adding or removing email addresses for usage notifications	182
Chapter 12	Classification	183
	About classification	183
	Which emails get classified?	184
	Steps for setting up classification	184
	Accessing the Veritas Alta Classification	185
	Veritas Alta Archiving item properties for use in custom classification policies	186
Chapter 13	Managing Data Import	189
	About Import Data	189
	Importing data into archives	191
Chapter 14	AD FS Configuration Guide	195
	Configuring AD FS to work with Veritas Alta Archiving	195
	Adding a relying party trust for Veritas Alta Archiving	196
	Generating a token-signing certificate	199
Chapter 15	Alta Personal Archive Deployment for IBM Notes	201
	Alta Personal Archive deployment for IBM Notes	201
Chapter 16	Archive Administration Updates in Previous Releases	203
	About the updates for previous releases	203

Getting started

This chapter includes the following topics:

- [About Veritas Alta View Compliance and Governance Management Console](#)
- [Prerequisites for using Veritas Alta View Compliance and Governance Management Console](#)
- [Veritas Alta View Compliance and Governance Management Console web browser support](#)
- [What's new in this release](#)
- [Signing in to Veritas Alta View Compliance and Governance Management Console](#)
- [Signing out from Veritas Alta View Compliance and Governance Management Console](#)
- [Resetting a forgotten password](#)
- [Changing your profile password](#)

About Veritas Alta View Compliance and Governance Management Console

Veritas Alta Archiving is a cloud-based archiving service that lets your organization store, manage, supervise, and discover all of your business-critical communications. Once your organization enables the service, it can journal a copy of all the messages that are sent and received within your organization to Veritas Alta Archiving.

Veritas Alta View Compliance and Governance Management Console is a web-hosted interface that enables administrators to configure and manage Veritas Alta Archiving and perform the following tasks:

- Provision and manage Veritas Alta Archiving archive accounts.
- Configure and manage the archiving of content sources.
- Assign and manage user roles.
- Manage archiving options and policies.
- Manage retention policies and tags.
- Configure classification for all content that meets the enabled classification policies.
- Manage the Email Continuity option.
- Generate usage reports.

Recent updates to Veritas Alta View Compliance and Governance Management Console include the following enhancements:

- With the Import Data feature in Veritas Alta View Compliance and Governance Management Console, you can import legacy email into the archive. Every company has existing emails, whether located in the active user mailboxes, personal stores, document management systems, or other communication libraries. You can consolidate some or all of these legacy email sources into your archive.
- Delegates can now view the mailbox folder structure. Administrators can control whether the delegates can view the mailbox folder structure using Manage.
- Administrators can manage account provisioning remotely. You can sync users from either Exchange Online or CloudLink. If users exist in only one environment, their archives will not be overwritten or removed when they are synchronized by either Exchange Online or CloudLink.
- Administrators can configure the Privilege Delete archive options and determine whether Alta eDiscovery Administrator is enabled to delete emails in Alta eDiscovery permanently.
- With the enhancements in the built-in administrator roles, you cannot edit the System administrator role's permissions. Only the Share Export, Download Export, and Privilege Delete permissions can be edited for the Alta eDiscovery Administrator role.
- With the enhancements in reports, administrators can now create a Alta eDiscovery Report and a Mail Reassignment status report. The 7-Day Rolling Attachment Summary and 7-Day Rolling by User report are no longer available.

The Messaging Report now shows charts for the Number of emails imported and the Size of emails imported and contains a Summary for the selected period.

- The passwords must be minimum of 8 characters long for enhanced security instead of the earlier policy of 6 characters long passwords.
- Office 365 Sync provisioning has been enhanced to include more options, such as **Synchronize User Name from: Email Address** and **User Principal Name and Archive Provisioning: Provision Dynamic Distribution Lists**.

Information about the changes that were included with earlier releases of Veritas Alta View Compliance and Governance Management Console is provided elsewhere in this help.

For full details of all the updates in each release of the Veritas Alta Archiving service suite, see the [Veritas Alta Archiving release notes](#).

Prerequisites for using Veritas Alta View Compliance and Governance Management Console

To use Veritas Alta View Compliance and Governance Management Console, you need the following:

- Your Veritas Alta View Compliance and Governance Management Console URL.
- Your Veritas Alta Archiving user name.
- Your Veritas Alta Archiving password.
- Access permission to use Veritas Alta View Compliance and Governance Management Console.

Note: Contact your administrator if you do not have this information or you need access permission for Veritas Alta View Compliance and Governance Management Console.

Veritas Alta View Compliance and Governance Management Console web browser support

Veritas Alta View Compliance and Governance Management Console supports the web browsers that are listed in the Veritas Alta Archiving Compatibility List. You

can obtain the Compatibility List from the following article on the Veritas Support website:

<http://www.veritas.com/docs/000016792>

What's new in this release

Veritas constantly works on improving the Veritas Alta Archiving product and introduces new features and enhancements release by release. For an easy-to-reference source for all the ways the product is changing, refer to the release notes and product documentation, which is available at:

https://www.veritas.com/support/en_US/article.100040129

We also recommend watching [this space](#) for the most up-to-date information on the updates, patches, and Late Breaking News for Veritas Alta Archiving.

Signing in to Veritas Alta View Compliance and Governance Management Console

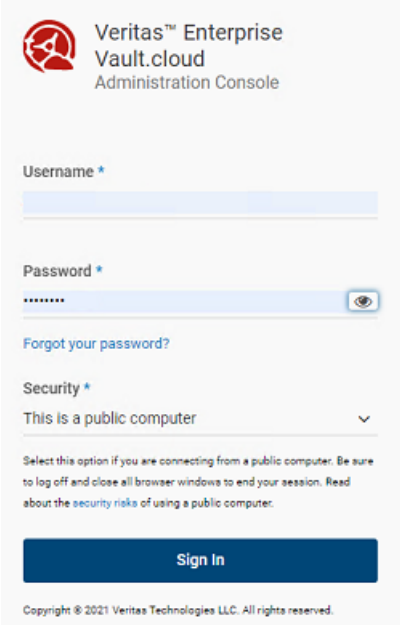
Before you access Veritas Alta View Compliance and Governance Management Console, you must log in using your Veritas Alta Archiving credentials.

To log in to Veritas Alta View Compliance and Governance Management Console

- 1 In a supported browser, enter the Veritas Alta View Compliance and Governance Management Console URL.

Note: Contact your administrator if you do not know your Veritas Alta View Compliance and Governance Management Console URL or you need access permission for Veritas Alta View Compliance and Governance Management Console.

For more information on supported browsers, see [Veritas Alta Archiving Compatibility List](#).



- 2 Enter your username and password on the authentication screen.

Note: Consecutive incorrect password entries lock your account. If you forget your password, you can reset it. See [“Resetting a forgotten password”](#) on page 14.

- 3 Under **Security**, select a security option.

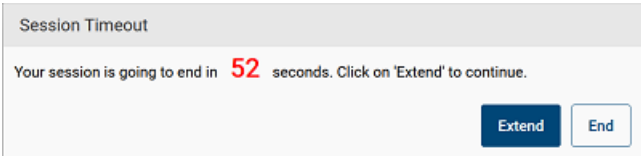
Refer to the following table for more information:

This is a public computer

Veritas Alta View Compliance and Governance Management Console prompts you for your credentials each time you access the **Login** page and automatically logs you out after 20 minutes of inactivity.

This option is the default option selected.

If the ongoing session on the public computer remains idle for 20 minutes, the application displays an alert to extend the session.



- Click **Extend** to extend the session within 60 seconds. Else, the session ends automatically. After you extend the session, the session timeout interval is set to another 20 minutes of the idle session.
- Click **End** to end the session.

This is a private computer

Veritas Alta View Compliance and Governance Management Console caches your credentials for one year and lets you bypass the **Login** page after you log in successfully. To clear your credentials from the cache, log out of Veritas Alta View Compliance and Governance Management Console.

Veritas Alta View Compliance and Governance Management Console automatically logs you out after 10 hours of inactivity.

If the ongoing session on the private computer remains idle for 10 hours, the application displays an alert to extend the session.

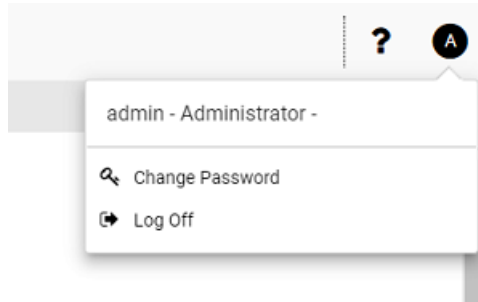
- Click **Extend** to extend the session within 60 seconds. Else, the session ends automatically. After you extend the session, the session timeout interval is set to another 10 hours of the idle session.
- Click **End** to end the session.

4 Click **Sign In**.

Signing out from Veritas Alta View Compliance and Governance Management Console

To sign out from the current session

- 1 In the top-right corner of the page, click on your user profile icon.



- 2 Click **Log Off**.

Important!

If the ongoing session on the public computer remains idle for 20 minutes or the session on the private computer remains idle for 10 hours, the application displays an alert to extend the session.



- Click **Extend** to extend the session within 60 seconds. Else, the session ends automatically. After you extend the session, the session timeout interval is set to another 20 minutes for the public computers and 10 hours for the private computers of the idle session.
- Click **End** to end the session immediately.

Resetting a forgotten password

If you forget your password and need help resetting it, Veritas Alta View Compliance and Governance Management Console can help you by sending a link to your authenticated user name (email address).

To reset your forgotten password

- 1** On the authentication screen, click the **Forgot your password** link.
- 2** In the **User Name** field, provide your user name (email address).
- 3** In the **Validation Code** field, enter the correct captcha from the image, without spaces. Letters are not case-sensitive.

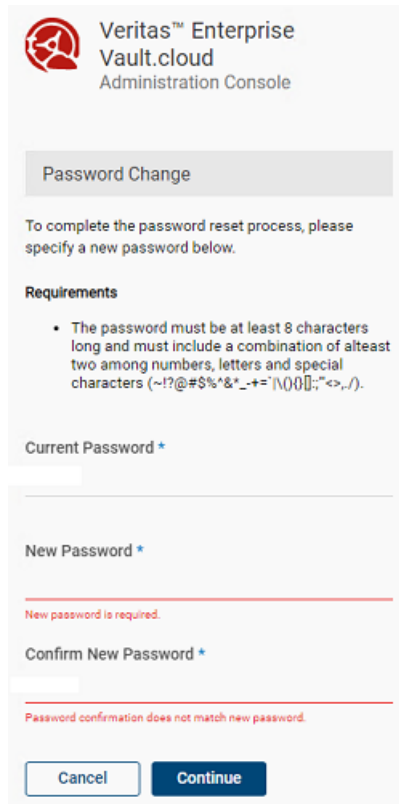
You cannot sign in if your archive fails to authorize your location or computer.
You can contact system administrator for assistance.

- 4** Click **Send**.

The **Password Change** page appears.

Note: After successful validation, you receive an email notification (Inbox, Spam, or Junk emails folder) with the temporary password information.

- 5 In the **Current Password** field, enter the temporary password that is received in email notification.



Veritas™ Enterprise Vault.cloud
Administration Console

Password Change

To complete the password reset process, please specify a new password below.

Requirements

- The password must be at least 8 characters long and must include a combination of atleast two among numbers, letters and special characters (~!@#%&*'_{+~\()0[];:'"<>.,/).

Current Password *

New Password *

New password is required.

Confirm New Password *

Password confirmation does not match new password.

- 6 Type a new password, retype to confirm it, and click **Continue**.

See [“Changing your profile password”](#) on page 16.

After successful validation, you receive an email notification that your password has been changed successfully.

Changing your profile password

You can change the password that you use to access Veritas Alta View Compliance and Governance Management Console whenever required. If your organization uses the default password policy, your new password must be at least eight characters long. In addition, your password must include two of the following character types:

- A number between 0 and 9
- A lowercase letter
- An uppercase letter
- A non-alphanumeric character

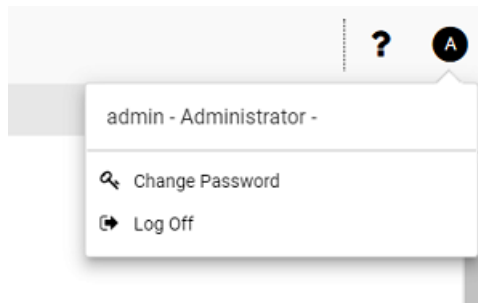
If your organization uses an advanced password policy, your new password must meet the requirements of that policy.

See [“Configuring an advanced password policy”](#) on page 143.

Note: Changing your password for Veritas Alta View Compliance and Governance Management Console also changes your password for other Veritas Alta Archiving products.

To change your password

- 1 In the top-right corner of the page, click on your user profile icon.



- 2 Click **Change Password**.
- 3 On the **Password Change** page, in the **Old Password** field, enter your current password.
- 4 In the **New Password** field, enter your new password.
- 5 In the **Confirm Password** field, enter your new password again.
- 6 Click **Save**.

Archive Overview

This chapter includes the following topics:

- [About Archive Overview](#)
- [Viewing the Archive Usage Snapshot report](#)

About Archive Overview

The **Archive Overview** page automatically displays when you log on to Veritas Alta View Compliance and Governance Management Console. This page provides general information and usage statistics for Veritas Alta Archiving. The information available from the **Archive Overview** includes the following in a tabbed layout:

- Archive Usage
 - The services that your company has purchased, and the usage for which you are currently billed in a dashboard format.
 - The table view shows minimum and actual number of users as well as the total usage percentage.
 - The chart view provides two horizontal bars.
 - The green bar shows the quota of users.
 - The red bar shows the actual count of users of that group.
 - The current company contact details that Veritas can use to contact a system administrator or billing contact with product-specific updates. These contact details can also be accessed from a tab on the Account Management page.
 - You can still automatically provision users to the archive when you reach 100% of usage quota. Note that you are charged for those users monthly in arrears. When the service alert pop-up appears, click **Acknowledge** to dismiss the alert and continuing using the Veritas Alta View Compliance and

Governance Management Console console. When the alert is acknowledged, the Service Alert does not pop up again on subsequent logons into Manage. If you exceed the usage count again, a new pop-up appears.

Note: When your usage approaches your usage quota, your administrators receive a daily email notification from Veritas to logon to Manage and click **Acknowledge** on the service alert pop-up.

- Archive usage snapshot offers
A series of tables and graphs that present a snapshot of your company's archive usage. The archive usage snapshot includes the following information:
 - 10-Day Rolling Mail Volume
 - Top ten Unprovisioned Accounts
- Sync Activity
This tab is populated only if you have setup either Exchange Online Sync or CloudLink.
 - On this tab, you can view the most recent sync details, last sync date and number of active vs. inactive accounts.
 - If a sync has not occurred in 30 days a warning is displayed.
 - Click “see details” under the respective section, to view the [Exchange Online or CloudLink Config](#) page.
- Roles
 - The delegated roles to which your account is assigned.

Archive Usage

This page provides contact details that Veritas can use to contact a system administrator or a billing department for the product-specific updates. These contact details can also be accessed from a tab on the **Account Management** page.

To edit the contact details

- 1 On the **Archive Usage** tab, click **Edit Contact Details**.
- 2 Click **Edit** to enable the page for editing.
- 3 Update the contact details, and click **Save**.

This page outlines the current services that you have purchased and the usage for which you are being billed. The information is provided in a dashboard (tables and graphs) formats. The sample image is shown below.

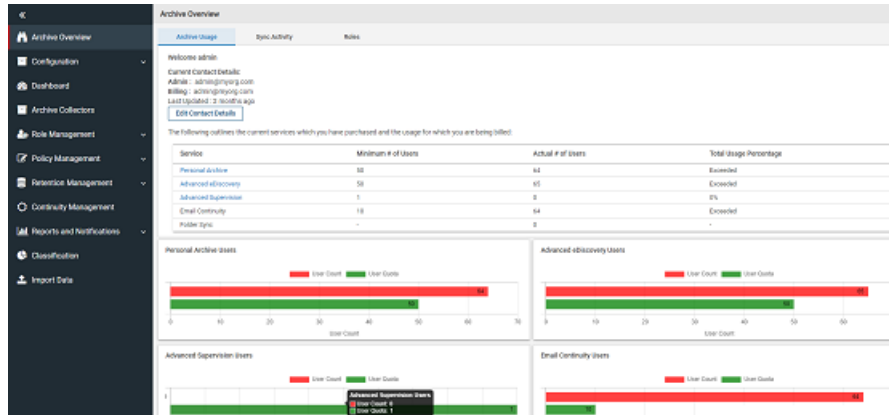


Table view shows minimum and actual number of users as well as the total usage percentage. The chart view provides two horizontal bars. The green bar shows the quota of users, whereas, the red bar shows the actual count of users of that group.

Even if you reach 100% of usage quota, you can still automatically provision users to the archive. However, you are charged for those users monthly in arrears. When the service alert pop-up appears, click **Acknowledge** to dismiss the alert and continuing using the Veritas Alta View Compliance and Governance Management Console console. When the alert is acknowledged, the Service Alert does not pop up again on subsequent logons into Veritas Alta View Compliance and Governance Management Console console. If you exceed the usage count again, a new pop-up appears.

Note: When your usage approaches your usage quota, your administrators receive a daily email notification from Veritas to logon to Veritas Alta View Compliance and Governance Management Console console and click **Acknowledge** on the service alert pop-up.

Archive usage snapshot offers a series of tables and graphs that present a snapshot of your company's archive usage. The archive usage snapshot includes the following information:

- 10-Day Rolling Mail Volume
- Top ten unprovisioned accounts

Sync Activity

This tab is displayed only if you have set up either Exchange Online Sync or CloudLink.



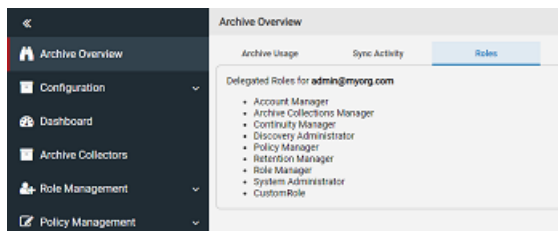
On this page, you can view -

- the most recent sync details
- last sync date
- number of active and inactive accounts
- A warning message if a sync has not occurred in 30 days

To view the [Exchange Online or CloudLink Config](#) page, click **see details** under the respective sections.

Roles

This page displays the delegated roles to which your account is assigned.



Viewing the Archive Usage Snapshot report

In addition to the information available from the **Archive Usage** page, you can access the **Archive Usage Snapshot** report for Veritas Alta Archiving. The information available from the Full Archive Usage Report includes the following:

- 10-Day Rolling Mail Volume report.
- 5-Month Rolling Mail Volume report.
- Total MTD Mail Usage Accounts report.
- 7-Day Rolling Un-provisioned Accounts report.
- Weekly Summary User Activity report.
- Detail 7-Day User Activity report.

Note: In the 7-Day Rolling by User Activity report, External users represent message senders outside your organization sending messages to recipients in your organization. Unrecognized users represent recipients in your organization with the Admin and Unassigned user names. These user names represent the default administrator and unassigned legacy accounts for Veritas Alta Archiving.

To view the Archive Usage Snapshot report

- 1 In the left navigation pane, click **Archive Overview**.
- 2 On the **Archive Usage** tab, click **View Full Report**.

Working with Dashboard

This chapter includes the following topics:

- [About dashboard](#)
- [Viewing and exporting statistics of Alta Capture-specific archives](#)
- [Viewing and exporting mail statistics of EVC-specific archives](#)

About dashboard

To view the dashboard, you must be an Veritas Alta Archiving administrator and the Alta Capture primary and the required secondary services are enabled for you. For example, if you are the administrator, Alta Capture primary service is enabled for you, and only the Yammer and Bloomberg secondary services are enabled, then you can view and export statistical report for Yammer and Bloomberg importers/collectors only. You cannot view the statistics for the importers/collectors for other secondary services that are not enabled.

Dashboard consists of two tabs, namely, **Capture** tab and **EVC** tab.

Note: If you cannot view the **Capture** or the **EVC** tab even though the services are enabled for you, contact Veritas Support.

On the **Capture** tab, you can select the importer/collector to view corresponding metrics for certain duration. The information available from the Capture tab includes the following in a tabbed layout, and you can export the report for future reference.

Importer jobs

This statistic provides information about the import jobs for all or the selected collector type.

You can customize the date range to get the records for a specific duration.

Monitored users by source	This statistic provides information about the number of monitored users for each source.
Messages processed by Alta Capture	<p>This statistic provides information about the number of imported, excluded, and failed messages in certain duration. For example, 7 days.</p> <p>You can print and download the charts as PNG, JPEG, PDF, and SVG Vector format.</p>
Number of messages by importer	This statistic provides information about number of messages by each importer.

For more information about Alta Capture Dashboard, refer to Alta Capture documentation.

On the **EV.C** tab, you can view and export the statistical data about customer's EVC-specific archives. The information available from the EV.C tab includes the following in a tabbed layout, and you can export the report for future reference.

Total emails	Provide total number of emails archived.
Active archives	Provide number of active archives.
Total size of the archives	Provides collective storage size of all archives.
Distribution by attachment	Graphical statistics (in percentage) of the emails with and without attachments.
Distribution by mail types	Graphical statistics (in percentage) based on mail types, such as Exchange Online, Domino, and so on.
Count by message size	Graphical statistics (in numbers) based on messages sizes.
Count by direction type	Graphical statistics (in percentage) of the Inbound and Outbound emails, and internal and instant messages.
Top mail accounts	List of top mail accounts that are getting archived.

Viewing and exporting statistics of Alta Capture-specific archives

You can view and export statistics of Alta Capture collectors in the CSV format only. The procedure to download the statistical report is mentioned below. For more information, refer to the [Alta Capture Collectors Configuration Guide](#).

To view and export statistics of Alta Capture-specific archives

- 1 In the left navigation pane, click **Dashboard**.

The application displays the page that consists of the following tabs:

- Alta Capture
- EV.C

- 2 Select the **Capture** tab to view the **Dashboard** page for Alta Capture archives.

The screenshot shows the 'Dashboard' page for 'Alta Capture' archives. The 'Capture' tab is selected in the top navigation. Below the tabs, there's a section titled 'IMPORTER JOBS' with a table of data. A red box highlights the controls for this section: 'COLLECTORS LIST' (set to 'ALL'), 'DATE RANGE' (set to 'month/day'), and an 'EXPORT TO CSV' button. The table has columns: DATE, IMPORTER, QUARANTINED SOURCES, IMPORTED MESSAGES, and FAILED MESSAGES. It lists several importers and their associated statistics. At the bottom, there's a pagination bar showing '1 - 10 of 297 items' and a section for 'MESSAGES PROCESSED BY ALTA CAPTURE' with a filter for 'OVER LAST 7 DAYS'.

DATE	IMPORTER	QUARANTINED SOURCES	IMPORTED MESSAGES	FAILED MESSAGES
03/15/2023	emihhu	0	0	0
03/15/2023	nhueml	0	0	0
03/15/2023	nhueml	2	0	0
03/15/2023	ringhhu	0	0	0
03/15/2023	ringhhu	0	0	0
03/14/2023	emihhu	0	0	0
03/12/2023	emihhu	2	0	0
03/09/2023	emihhu	0	0	0
03/08/2023	emihhu	0	0	0

- 3 In the Importers Jobs pane, click the Collectors List drop-down to select the collector.

Select *All* to export statistic of all the collectors simultaneously, or a required collector of which you want to export the statistics.

- 4 In the **Date Range** field, select the duration for which you want to export the statistics.

- 5 Click **Export to CSV**.

The application downloads the statistical report (**Dashboard.csv**) in the **Downloads** folder of your computer.

Viewing and exporting mail statistics of EVC-specific archives

You can view mail statistics for all your Veritas Alta Archiving-specific archives on the dashboard, and export the statistical report to share it with the intended authority.

To view and export mail statistics details of the EVC-specific archive

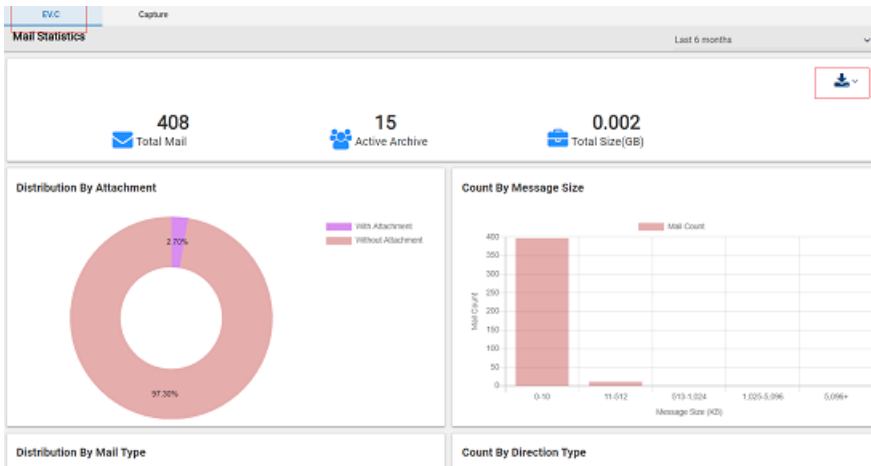
- 1 In the left navigation pane, click **Dashboard**.

The application displays the page that consists of the following tabs:

- Capture
- EV.C

- 2 Select the **EV.C** tab to view the **Mail Statistics** page.

- 3 In the top-right corner of this page, select the duration for which you want to view your mails and archiving statistics.



The statistical information for the selected duration appears.

- 4 Click the **Export** icon to export the report in EXCEL, PDF, CSV, or WORD format.

Managing Configurations

This chapter includes the following topics:

- [About the Configuration page](#)
- [Viewing provisioned services](#)
- [Selecting the User Management options](#)
- [About Provisioning](#)
- [CloudLink Sync Summary](#)
- [About Managed Tags](#)
- [About Account Management](#)

About the Configuration page

The **Configuration** page guides administrators through the administration setup and provisioning process. The page presents:

- A list of the Veritas Alta Archiving services that are available to your company.
- The status of the setup, with information about any steps that are required to complete the configuration.

Note: The displayed configuration steps reflect the account provisioning options that are selected on the **User Management** page.

Viewing provisioned services

The **Services** page displays a read-only information about the services that are provisioned for your company. To make changes to this information, contact [Veritas Services & Support](#).

The page provides information on the following aspects as shown in the sample image below.

- **General configuration**
Expand the row to view general configurations such as Company Name, Parent Partner, Manage Retention Settings, Import Data, Archive Encryption, Last Access Date, and so on.
- **Primary Services**
Expand the row to view the primary services that are either enabled or disabled for your company and number of minimum and actual users.
- **Secondary Services**
Expand the row to view the secondary services that are either enabled or disabled for your company and number of minimum and actual users, and the last archiving date for each product.
- **Capture Secondary Services**
Expand the row to view the Capture secondary services that are either enabled or disabled for your company and number of minimum and actual users, and the last archiving date for each product.
- **Domains**
Expand to view the configured domains.
- **Mail Continuity service**
Expand the row to view the Mail Continuity services that are enabled for IP address and the domains, and the corresponding mail servers.
- **Journal Addresses**
Expand to view the configured Journal Addresses.

Selecting the User Management options

The **User Management** page under **Configuration** lets you select the options that you use to provision and manage your Veritas Alta Archiving archive accounts. You can perform the provisioning and management manually through Veritas Alta View Compliance and Governance Management Console, or you can use remote provisioning. Remote provisioning avoids the need to create a new archive account manually in Veritas Alta View Compliance and Governance Management Console

for each new user in your organization. If you configure remote provisioning, new archive accounts appear automatically in Veritas Alta View Compliance and Governance Management Console when the remote option synchronizes new users.

The remote provisioning options are:

- **CloudLink:** This option lets you use the separately installable ArchiveTools CloudLink tool to manage the provisioning of Microsoft Active Directory and IBM Lotus Domino Directory accounts.
- **Office 365 Sync:** This option provides automatic provisioning for Office 365 accounts.
- **System for Cross-domain Identity Management (SCIM):** This option provides provisioning of accounts by using SCIM.

User accounts can be synchronized with either Office 365 Sync, CloudLink, or SCIM. You have the option to use any of the remote provisioning options together to manage different groups of users. Since the users that are synchronized from different remote options remain independent, the archive accounts that exist in one group are not removed if those accounts do not exist in the other group.

To select the User Management options

- 1 In the left navigation pane, select **Configuration > User Management**.
- 2 On the **User Management** page, select one of the following provisioning options:
 - **Manage account provisioning using the console application**
 - **Manage account provisioning remotely**
- 3 When you select the option to manage account provisioning remotely, select **Using on-premise CloudLink tool**, or **Using Microsoft Office 365**, or both.

Note: Users can be synced from either Exchange Online, CloudLink, and SCIM.

- If users exist in only one environment, their archives cannot be overwritten or removed when they are synchronized by either Exchange Online, CloudLink, or SCIM.
- If users exist in a hybrid environment (setup), ensure that both the above-mentioned options are selected. Otherwise, users that are migrated from on-premise CloudLink to Exchange Online may not be provisioned correctly.

- 4 Click **Save**.
- 5 Click **Go To Next Step**.

Veritas Alta View Compliance and Governance Management Console navigates you to the **My Configuration** page and guides you to perform the required configuration steps for the provisioning options you have selected.

About Provisioning

If you chose to manage account provisioning with the console application, you must configure the settings on the **Provisioning** page, under **Configuration**.

Note: If you chose to manage account provisioning with CloudLink, you must use CloudLink to configure its own provisioning settings. Refer to your CloudLink documentation for more information.

Complete the required options, as follows:

Table 4-1 Provisioning steps for account management with the console application

Provisioning step	Reference for more information
Configure the Alta Personal Archive deployment options	See “Configuring the Alta Personal Archive deployment options” on page 30.
Configure the administrator notification options	See “Configuring the administrator notification options” on page 32.

Configuring the Alta Personal Archive deployment options

If you chose on the **User Management** page to manage account provisioning with the console application, you can specify the Alta Personal Archive deployment options on the **Provisioning** page.

To configure the Alta Personal Archive deployment provisioning options

- 1 In the left navigation pane of Veritas Alta View Compliance and Governance Management Console, select **Configuration > Provisioning**.
- 2 Expand **Personal Archive Deployment Options**, near the bottom of the page.
- 3 Under **Personal Archive Access**, configure whether Veritas Alta Archiving automatically enables access to Alta Personal Archive and sends a welcome message email to each user.

Note: The options you see depend on whether single sign-on authentication is configured for your company in Veritas Alta Archiving. The different options reflect the fact that a welcome message is not essential for users with single sign-on authentication.

If single sign-on authentication is not configured for your company in Veritas Alta Archiving, the options are as follows:

- | | |
|--|---|
| <p>Enable Personal Archive access and send Welcome Message</p> | <p>Select this option to enable Alta Personal Archive access to each account that is provisioned, and to enable welcome messages to be sent to the provisioned users.</p> <p>By default this option is not selected.</p> <p>If you select this option you must select one of the following sub-options:</p> |
| <ul style="list-style-type: none"> ■ Don't send Welcome Message if already sent. | <p>Select this option to send a welcome message to a provisioned user only once. This is the default option.</p> |
| <ul style="list-style-type: none"> ■ Send Welcome Message anyway. | <p>Select this option to send a welcome message every time that Exchange Online Sync synchronizes the account, even if a welcome message was sent previously.</p> |

If single sign-on authentication is configured for your company in Veritas Alta Archiving, the options are as follows:

- | | |
|--|--|
| <p>Enable Personal Archive access</p> | <p>Select this option to enable Alta Personal Archive access to each account that is provisioned.</p> <p>By default this option is not selected.</p> <p>If you select this option you can choose whether Veritas Alta Archiving sends welcome messages to provisioned users:</p> |
| <ul style="list-style-type: none"> ■ Send Welcome Message | <p>Select this option to enable welcome messages to be sent to the provisioned users.</p> <p>By default this option is not selected for new configurations.</p> <p>If you select this option you must select one of the following sub-options:</p> |
| <ul style="list-style-type: none"> ■ Don't send Welcome Message if already sent. | <p>Select this option to send a welcome message to a provisioned user only once. This is the default option.</p> |

- **Send Welcome Message anyway.** Select this option to send a welcome message every time that Exchange Online Sync synchronizes an account, even if a welcome message was sent previously.

4 Under **Welcome Message Template**, complete the details of the templates for the following messages:

- The welcome message that can be sent to provisioned users.
- The notification message that is sent to the chosen administrator roles when Veritas Alta Archiving provisions new archive accounts.

Select Template	<p>Select Account to configure the welcome message template for provisioned users.</p> <p>Select Administrator to configure the administrators' notification message.</p>
From	Enter the sender email address for the message.
Subject	Enter the information you want saved as the subject for the message email.
Body	<p>Edit the body text for the message.</p> <p>You can use the following macros that Veritas Alta Archiving replaces with the relevant information, based on archive information:</p> <ul style="list-style-type: none"> ■ {username} — automatically enters the user's login user name ■ {password} — automatically enters the user's login password ■ {accountlist} — automatically enters a list of newly created email accounts, for use with the Administrator template only

5 Click **Save**.

Configuring the administrator notification options

If you chose on the **User Management** page to manage account provisioning with the console application, you can specify the administrator notification options on the **Provisioning** page.

To configure the administrator notification options

- 1 In the left navigation pane of Veritas Alta View Compliance and Governance Management Console, Select **Configuration > Provisioning**.
- 2 Expand **Notification Options**, near the bottom of the page.
- 3 Under **Administration Roles to Notify**, select the Veritas Alta Archiving administration roles that you want to receive the administrators' notification message when Veritas Alta Archiving creates archive accounts.

Note: To see a list of administrators that are assigned to a role, click that role.

- 4 Click **Save**.

CloudLink Sync Summary

The CloudLink Sync Summary appears in the **Configuration** menu of the Veritas Alta View Compliance and Governance Management Console console.

If you want to receive a warning email when a successful CloudLink Sync has not occurred in the past month, you can enable notifications.

- To enable notifications, select the enable button, enter email addresses in the text box and click **Add**.
- To disable notifications, select the disable button.

About Managed Tags

From the **Managed Tags** page, you can create global tags that you can assign to users. Once you create a managed tag and associate a retention policy, users can apply the tag to archived messages to extend their retention period. The retention period of the retention policy determines how long tagged messages are retained in Veritas Alta Archiving.

[Table 4-2](#) lists the tasks that you can perform that are related to managed tags:

Table 4-2 Tasks with managed tags

Task	Reference
Create new managed tags.	See “Creating a managed tag” on page 34.
Assign managed tags to users.	See “Assigning a managed tag to users” on page 35.

Table 4-2 Tasks with managed tags (*continued*)

Task	Reference
Change the retention policy that is associated with a managed tag.	See “Changing the retention policy associated with a managed tag” on page 36.
Edit and delete managed tags.	See “Deleting a managed tag” on page 37.

Creating a managed tag

You can create a managed tag and assign an existing retention policy to it, if required.

To create a managed tag

- 1 In the left navigation pane, select **Configuration > Managed Tags**.
- 2 In the top-right corner of the page, click **Create New**.
- 3 Under **Create Managed Tag**, do the following:
 - In the **Tag Name** field, enter a new tag name.
 - In the **Policy Name** field, select a policy.

Note: You must create a retention policy before you can associate it with a managed tag.

See [“Creating a retention policy”](#) on page 158.

- 4 Click **Assign Policy** to associate a retention policy with the managed tag. The **Retention Policies** dialog box appears.

Note: To clear the **Policy Name** field, click **Remove Policy**.

- 5 In the **Retention Period (days)** field, check the duration of the assigned policy.
- 6 If required, in the **Description** field, enter a description for the tag.
- 7 From the **Target Type** drop-down, specify the targeted users.

The currently available options are All, Group, and Tags.
- 8 If required, under **Set Managed Tag Permissions**, configure the settings for **Tagged Email Visibility** and **Remove Tags from Emails** sections.

- Selecting the **Tagged Email Visibility** options allow administrators, reviewers, and users to view messages of other users that have the managed tag applied.
- Selecting the **Remove Tags from Emails** options allow administrators, reviewers, and users to remove the managed tag from messages belonging to other users.

9 Click **Save**.

Assigning a managed tag to users

By default, the managed tags you have created are assigned to all users so that any user in your organization can use these tags. If required, you can assign managed tags to selected users.

Note: You can only assign existing managed tags to selected users. You cannot assign a managed tag to selected users while creating a new tag.

To assign a managed tag to users

- 1 In the left navigation pane, select **Configuration > Managed Tags**.
- 2 On the **Managed Tags** page, select an existing managed tag.

The sample image is shown below.

The screenshot shows the 'Managed Tags' configuration page. On the left is a dark navigation pane with the following items: Archive Overview, Configuration (expanded), Summary, Services, User Management, Managed Tags (selected), Account Management, Dashboard, Archive Collectors, Role Management, and Policy Management. The main content area is titled 'Managed Tags' and contains the following sections: 'Create Managed Tag' (with a plus icon), 'Tag Name' (value: 12), 'Policy Name' (value: 1Policy) with 'Remove Policy' and 'Assign Policy' buttons, 'Retention Period (days)' (value: 365), and a 'Description' field. At the bottom, the 'Users Assigned' section shows two radio buttons: 'All Users' (unselected) and 'Selected Users' (selected), with 'Add Users' and 'Remove Checked' buttons below them.

- 3 Under **Users Assigned** section, select **Selected Users**.
- 4 Click **Add Users**, and select the required users.

Email Address	Last Name	First Name
<input type="checkbox"/> account@myorg.com	account	Admin
<input checked="" type="checkbox"/> accountone@myorg.com	one	account
<input type="checkbox"/> accountone-Disabled_On_Mar 7 2021 11:53PM@akshaybheda.onmicrosoft.com	one	account
<input checked="" type="checkbox"/> accounttwo@akshaybheda.onmicrosoft.com	two	account
<input type="checkbox"/> accounttwo@myorg.com	two	account
<input type="checkbox"/> admin@akshaybheda.onmicrosoft.com	Bheda	Akshay
<input type="checkbox"/> admin@bhedaakshay.onmicrosoft.com	Bheda Akshay	Admin
<input type="checkbox"/> admin@fmsms.com	acc	admin

Items per page: 10 1 - 10 of 73

Cancel Add

- 5 To remove the users that are not required, search for and select the users, and click **Remove Checked** as shown below.

Users Assigned

☐ All Users
☒ Selected Users

Add Users Remove Checked

Search...

Email Address	Last Name	First Name
<input checked="" type="checkbox"/> accounttwo@akshaybheda.onmicrosoft.com	two	account

Items per page: 10 0 of 0

Cancel Save

The application prompts you to confirm that you want to perform the operation. Click **OK**.

- 6 If required, under **Set Managed Tag Permissions**, select the required permissions.
- 7 Click **Save**.

Changing the retention policy associated with a managed tag

If required, you can change the retention policy that is associated with a managed tag.

To change the retention policy associated with a managed tag

- 1 In the left navigation pane, select **Configuration > Managed Tags**.
- 2 On the **Managed Tags** page, search for and select an existing managed tag.
- 3 Under **Create Managed Tag** section, click **Remove Policy** as shown in the sample image below.

The screenshot shows the 'Managed Tags' configuration page. On the left, a dark navigation pane has 'Managed Tags' selected. The main area is titled 'Managed Tags' and contains a 'Create Managed Tag' section. This section has several fields: 'Tag Name' with the value '12', 'Policy Name' with the value '1Policy', 'Retention Period (days)' with the value '365', and a 'Description' field. Below these fields are two buttons: 'Remove Policy' and 'Assign Policy'. The 'Remove Policy' button is highlighted with a red rectangular box. At the bottom, there is a 'Users Assigned' section with two radio buttons: 'All Users' (selected) and 'Selected Users'.

- 4 In the **Policy Name** field, select the required policy, and click **Assign Policy**.
- 5 Click **Save**.

Deleting a managed tag

If required, you can delete any managed tags that are no long needed.

Note: You cannot delete a managed tag if it is associated with a retention policy.

To delete a managed tag

- 1 In the left navigation pane, select **Configuration > Managed Tags**.
- 2 On the **Managed Tags** page, search for and select the tag you want to delete.
The application displays the policy details of the tag.

- 3 Click **Remove Policy** to disassociate the retention policy from the managed tag.
- 4 Click **Save**.

About Account Management

From the **Account Management** page, you can manage archive accounts for Veritas Alta Archiving.

[Table 4-3](#) lists the tasks that you can perform from the **Account Management** page, and where to find more information.

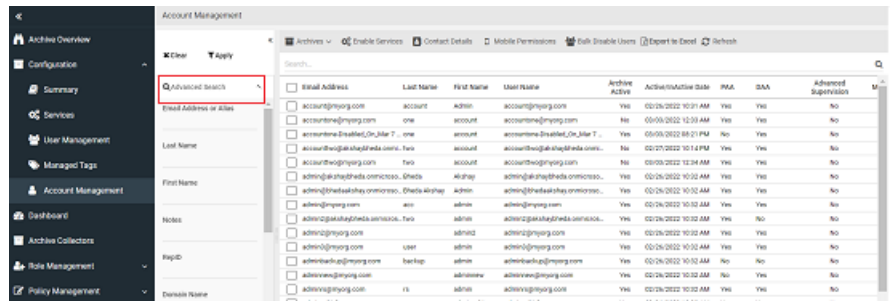
Table 4-3 Account management tasks

Task	Reference
Search for archive accounts	See “Searching for archive accounts” on page 39.
Filter the listed archive accounts	See “Using search filters” on page 42.
Create new archive accounts	See “Creating an archive account” on page 43.
View the details of an archive account	See “Viewing and editing the archive account details” on page 49. See “About the Account Details page” on page 51.
Edit an archive account	
Delete an archive account	See “Deleting an archive account” on page 55.
Deploy users	See “Deploying users” on page 56.
Remove user access	See “Removing user access” on page 59.
Enable services for existing archive accounts	See “Enabling services for existing archive accounts” on page 58.
Edit Mobile Web Access permissions for existing archive accounts	See “Editing Mobile Web Access permission for existing archive accounts” on page 63.
Export archive account information	See “Exporting archive account information” on page 65.
Unlock archive accounts	See “Unlocking an archive account” on page 65.

To use Advanced Search

- 1 In the left navigation pane, select **Configuration > Account Management**.

The application displays a list of archive accounts as shown in the sample image below.



2 Specify your search criteria in the following fields:

Email Address or Alias	Enter an email address or associated alias email address for the user.
Last Name	Enter the last name of a user.
First Name	Enter the first name of a user.
Notes	type some text from the note.
RepID	Specify the RepID.
Domain Name	Specify the domain name.
Department	Specify the mane of department.
Role	Select the type of role that is assigned to the user.
Account Status	Select a status.
Personal Archive Access	Select if the user has access to Alta Personal Archive enabled.
Discovery Archive Access	Select if the user has access to Alta eDiscovery enabled.
Advanced Supervision Access	Select if the user has access to Advanced Supervision enabled.
Welcome Message Sent	Select if the user has received a welcome message.
Account Status	Select if the account status for the user is active or deleted.
Archive	Select if the archive for the user is currently active.
Veritas Alta Archiving Mobile	Select if the user has access to Mobile Web Access.
Account Locked	Select if the user has been locked out of their archive account.
Office 365 PA Collection	Select if the user Office 365 Personal Archive collection enabled. Note: This feature is no longer supported in Veritas Alta Archiving.

3 Click **Apply**.

The application displays only those archive accounts that match with the advanced filter criteria you set.

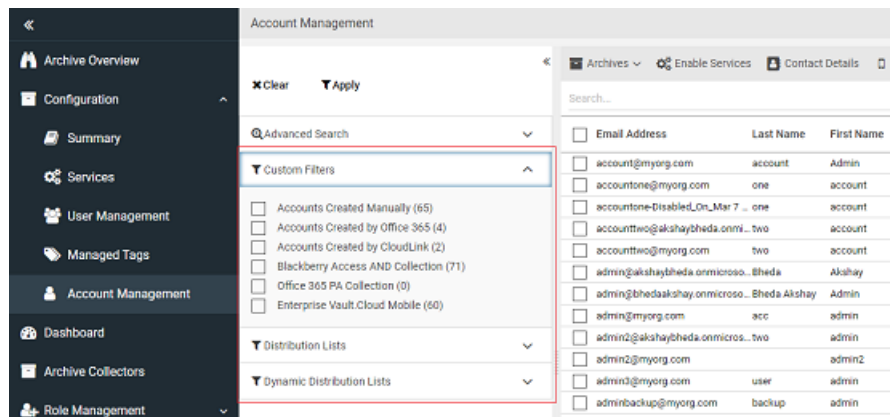
Using search filters

In addition to using Quick Search or Advanced Search, you can use search filters to find archive accounts. You can use one of the predefined custom filters, or filter by distribution lists.

To use search filters

1 In the left navigation pane, select **Configuration > Account Management**.

The application displays a list of archive accounts as shown in the sample image below.



2 Click **Custom Filters**, **Distribution Lists**, or **Dynamic Distribution Lists**.

3 Select a filter from the chosen group.

4 Click the **Apply** icon.

The application displays only those archive accounts that match the selected search filter criteria.

5 To remove the search filter, click the **Clear** icon.

Creating an archive account

To create an archive account

- 1 In the left navigation pane, select **Configuration > Account Management**.

The screenshot shows the 'Account Management' interface. On the left, the navigation pane has 'Account Management' highlighted. The main area displays a table of accounts with columns: Email Address, Last Name, First Name, User Name, Archive Active, Active/Inactive Date, and PAR. A red box highlights the 'Archives' dropdown menu at the top of the table.

Email Address	Last Name	First Name	User Name	Archive Active	Active/Inactive Date	PAR
account@myorg.com	account	admin	account@myorg.com	Yes	02/26/2022 10:31 AM	Yes
accountone@myorg.com	one	account	accountone@myorg.com	No	03/03/2022 12:33 AM	Yes
accounttwo@akshaybhedas.onmicrosoft.com	two	account	accounttwo@akshaybhedas.onmicrosoft.com	Yes	03/03/2022 05:21 PM	No
accountthree@akshaybhedas.onmicrosoft.com	three	account	accountthree@akshaybhedas.onmicrosoft.com	No	03/07/2022 10:14 PM	Yes
accountfour@myorg.com	four	account	accountfour@myorg.com	No	03/03/2022 10:34 AM	Yes
admin@akshaybhedas.onmicrosoft.com	Bheda	Akshay	admin@akshaybhedas.onmicrosoft.com	Yes	02/26/2022 10:32 AM	Yes
admin@bhedasakshay.onmicrosoft.com	Bheda	Akshay	admin@bhedasakshay.onmicrosoft.com	Yes	02/26/2022 10:32 AM	Yes
admin@myorg.com	acc	admin	admin@myorg.com	Yes	02/26/2022 10:32 AM	Yes
admin2@akshaybhedas.onmicrosoft.com	two	admin	admin2@akshaybhedas.onmicrosoft.com	Yes	02/26/2022 10:32 AM	Yes
admin2@myorg.com	admin2	admin	admin2@myorg.com	Yes	02/26/2022 10:32 AM	Yes
admin3@myorg.com	user	admin	admin3@myorg.com	Yes	02/26/2022 10:32 AM	Yes

- 2 Click **Archives > New Archive**.

The screenshot shows the 'Accounts' interface. On the left, the navigation pane has 'Account Management' highlighted. The main area displays the 'New Archive' form. The form has two main sections: 'Archive Detail' and 'Status'. The 'Archive Detail' section includes fields for Email Address, First Name, Last Name, User Name, RepID, Password, Confirm Password, Notes, Time Zone, Role, Account, Departments, and Supervision Roles. The 'Status' section includes checkboxes for Personal cloud, Personal cloud Mobile, Discovery cloud, and Advanced Supervision, and a dropdown for Office 365. The 'Archive Aliases' section has an 'Add' button.

3 On the **Accounts** page, under **Archive Detail**, provide the following details:

Email Address	<p>Enter the primary email address for the user.</p> <p>Note: If your organization has more than one domain, select the correct domain from the drop-down list.</p>
First Name	Enter the first name of the user.
Last Name	Enter the last name of the user.
User Name	<p>The user name for the account. By default Veritas Alta View Compliance and Governance Management Console uses the email address as the user name, but you can change it if you want.</p>
Password	<p>Enter a password for the user that meets the password policy requirements for your organization.</p> <p>See "Configuring an advanced password policy" on page 143.</p> <p>Note: This option does not appear if you selected Enable Personal Archive Access and send Welcome Message under Provisioning > Personal Archive Deployment Options > Personal Archive Access. In that case, Veritas Alta View Compliance and Governance Management Console generates a password automatically to send to the user.</p>
Confirm Password	If you entered a password you must enter the password again to confirm it.
Time Zone	Select the correct time zone for the user.
Role	Indicates the role that is currently configured for this archive account.
RepID	Provide the RepID of the email address.
Notes	Specify any special notes for this archive, if required.

Departments

This option is available exclusively for the customers for whom the Advanced Supervision primary service is enabled, and not for all customers. If the Advanced Supervision primary service is not enabled, the Veritas Alta View Compliance and Governance Management Console console does not display this option.

Click **Edit** to open the **Add/Remove Departments** dialog box. Search for and select one or multiple departments created in Advanced Supervision. Add or remove the monitor employees of the departments, if required. Click **Update** to save the selection.

After updating from Veritas Alta View Compliance and Governance Management Console console, users automatically get listed under the Monitored Employees section of the selected department in Advanced Supervision. If auditing of Monitored employees is enabled in Advanced Supervision, the above action gets audited in Advanced Supervision and the corresponding monitored employee audit record can be viewed in the **Audit Viewer** section of Advanced Supervision application.

However, for this synchronization, the SQL Server and the Audit server must communicate with each other and the *Auditing* service should be enabled for the selected department.

Supervision Roles

This option is available exclusively for the customers for whom the Advanced Supervision primary service is enabled, and not for all customers. If the Advanced Supervision primary service is not enabled, the Veritas Alta View Compliance and Governance Management Console console does not display this option.

After you select this service, you can quickly access departments and users available in Advanced Supervision to manage their roles and permissions.

Click **Add** to search for and select one or multiple departments. View the monitored employees of those departments, and assign roles and permissions to them. Click **Update**.

After updating from Veritas Alta View Compliance and Governance Management Console console, user roles automatically get updated in Advanced Supervision. If auditing of Role Assignments is enabled in Advanced Supervision, the above action gets audited in Advanced Supervision and the corresponding role assignments audit record can be viewed in the **Audit Viewer** section of Advanced Supervision application.

4 Under **Status**, select the status options for the user:

Account	Select whether the account is created in an enabled or disabled state.
Login	Select whether Veritas Alta Archiving account logins are unlocked or locked.
Archiving	<p>Select whether archiving is enabled or disabled.</p> <p>If you select Enabled, the email messages for the user start journaling to Veritas Alta Archiving immediately after you create the archive account.</p>
Folder Sync	<p>Indicates whether the Folder Sync feature is enabled or disabled.</p> <p>Note: This status is for information only. Folder Sync cannot be enabled or disabled from Veritas Alta View Compliance and Governance Management Console. Folder Sync is enabled or disabled at an account level from the Folder Sync application.</p>
External Reviewer	<p>Select whether the user is to be an external reviewer. External reviewers are the users that are not part of your organization, but who need to review archived messages for a Alta eDiscovery matter.</p> <p>The following conditions apply to archive accounts for external reviewers:</p> <ul style="list-style-type: none"> ■ Can only be assigned the Accounts role. ■ Can be assigned to any matter like users with the normal Reviewer role assigned. ■ Can only access the E-Discovery tab in Alta eDiscovery. ■ Can only access the matters that are assigned to them. ■ Can apply labels, review statuses, and notes to messages if granted permission. ■ Cannot access a matter once the matter expires. ■ Cannot restore, forward, or reply to messages regardless of the configuration for your organization. ■ Cannot edit the labels or the review statuses that are already assigned to a message. <p>An external reviewer has their account disabled for archiving.</p>

- 5 Under **Services**, select the services that you want to enable for the archive account:

Alta Personal Archive Lets the user access Alta Personal Archive.

Alta Personal Archive Lets the user access Mobile Web Access.

Mobile

Note: For this service to be enabled, you must also enable the option for Mobile Web Access on the **Archive Options** page.

Alta eDiscovery Lets the user access Alta eDiscovery.

Advanced Supervision Lets the user be granted Advanced Supervision access and permissions.

Exchange Online Enables Exchange Online Personal Archive collections for the user.

Note: This feature is no longer supported in Veritas Alta Archiving and should not be selected.

- 6 Under **Archive Aliases**, if required, enter an alias email addresses that you want to associate with the archive account. Click **Add**. Repeat to add more aliases if necessary.

Note: Any messages that are sent to these alias email addresses are forwarded automatically to the primary email address. If you do not associate an alias email address with the archive account, messages that are sent to alias email address are saved in the Unassigned Legacy Account.

- 7 Click **Save** to save the details you entered and to create the new user.

Viewing and editing the archive account details

You can view the details of an archive account from Account Management.

To view the details of an archive account

- 1 In the left navigation pane, select **Configuration > Account Management**.

The application displays a list of archive accounts.

- 2 Search for and select the archive account of which you want to view the details.

For quick and advance searching, See [“Searching for archive accounts”](#) on page 39.

The application displays the details of the selected archive account as shown in the sample image below.

The screenshot displays the 'Accounts' management interface. On the left is a dark navigation pane with the following menu items: Archive Overview, Configuration (selected), Summary, Services, User Management, Managed Tags, Account Management, Dashboard, Archive Collectors, Role Management, Policy Management, Retention Management, Continuity Management, Reports and Notifications, Classification, and Import Data. The main content area is titled 'Accounts' and is divided into three sections: 'Archive Detail', 'Status', and 'History'. The 'Archive Detail' section shows information for the account 'account@myorg.com', including its email address, first name 'Admin', last name 'account', user name 'account@myorg.com', and various settings like RepID, Notes, Time Zone (GMT+05:30), and Role (Reviewer). The 'Status' section shows a list of services with checkboxes for Personal cloud, Personal cloud Mobile, Discoverycloud, Advanced Supervision, Chatter, Office 365, Blackberry, and Exchange Online Folder Synchronization. The 'History' section on the right lists a series of events such as 'Archive Administration Account Edit', 'Password Changed', and 'Notes Added', each with a date and time. At the bottom right, there are buttons for 'New Archive' and 'Edit'.

- 3 If required, click **Edit** to make changes to the account details.

Be aware that if you manage account provisioning remotely with CloudLink or with Exchange Online Sync, some of the account details cannot be updated from within Veritas Alta View Compliance and Governance Management Console.

Note: If you disable an archive account the user can no longer access Alta Personal Archive and their messages are no longer journaled to Veritas Alta Archiving.

- 4 Click **Save**.

About the Account Details page

If you view the details of an archive account, the account details page displays a number of panels that provide information about the account.

The Archive Detail panel

The **Archive Detail** panel contains the following details for the archive account:

Email Address	The primary email address for the user.
First Name	The first name of the user.
Last Name	The last name of the user.
User Name	By default Veritas Alta View Compliance and Governance Management Console uses the email address as the user name.
Time Zone	The time zone that Veritas Alta Archiving uses for the user.
Role	The role that is currently configured for this archive account.

The Status, Services, and Archive Aliases panel

The **Status**, **Services**, and **Archive Aliases** panel displays the current status of the archive account, the Veritas Alta Archiving services that are currently configured for it, and the account's email aliases.

Note: A red **External** flag next to the Status heading indicates that the archive account is an external reviewer.

The **Status** section shows the following information about the status of the account:

Account	Indicates whether the account is in an enabled or disabled state.
Login	Indicates whether Veritas Alta Archiving logins for the account are unlocked or locked.
Archiving	Indicates whether archiving is enabled or disabled.
Folder Sync	Indicates whether the Folder Sync feature is enabled or disabled.

The **Services** section indicates which Veritas Alta Archiving services the account is enabled for:

 Indicates that the service is enabled for the account.

The **Archive Aliases** section lists all the archive alias email addresses for the account, and the date at which each alias was created.

 Indicates that this email address is the primary administrator account.

The Delegate Access panel

The **Delegate Access** panel appears if one or more users or mail-enabled security groups has synchronized delegate access permissions for the archive account.

Note the following:

- At this release, Veritas Alta Archiving can synchronize the delegate permissions that are set on Exchange on-premises mailboxes and Exchange Online mailboxes. The Exchange or Exchange Online administrator typically sets these permissions. Veritas Alta Archiving does not synchronize the delegate access to mailbox folders that users can set from Outlook.
- For Exchange on-premises mailboxes the synchronization of delegation permissions requires CloudLink version 4.0. For more information, see the [CloudLink Administration Guide](#).
- For Exchange Online mailboxes the delegation permissions synchronization is controlled through the **Mailbox Delegation Permissions** settings on the **Exchange Online Config** page of Veritas Alta View Compliance and Governance Management Console.

The **Delegate Access** panel shows:

- The delegate users and mail-enabled security groups that have synchronized delegate access permissions for the archive account.
- For each of delegate, which delegate access permissions are granted in Veritas Alta Archiving.

The following icons indicate whether a delegate archive access permission is granted:

- Indicates that the permission is granted in Veritas Alta Archiving
- Indicates that the permission is not granted in Veritas Alta Archiving

The following tables list the delegate archive access permissions, and their effect in Veritas Alta Archiving.

Table 4-4 Effect of delegate archive access permissions when granted to a user

Delegate archive access permission	Granted in these circumstances	Effect of granted permission in Alta Personal Archive
READ	The user or a group to which they belong has a synchronized Full Access delegation permission.	The user is able to read the delegated account's archived items in their Alta Personal Archive.
SEND AS	The user or a group to which they belong has a synchronized Send As delegation permission.	No effect in Alta Personal Archive at this release.
ON BEHALF	The user or a group to which they belong has a synchronized Send On Behalf delegation permission.	No effect in Alta Personal Archive at this release.

Table 4-5 Effect of delegate archive access permissions when granted to a mail-enabled security group

Delegate archive access permission	Granted in these circumstances	Effect of granted permission in Alta Personal Archive
READ	The group has a synchronized Full Access delegation permission.	Users who belong to the group can read the delegated account's archived items in their Alta Personal Archive. Note: If the user has a synchronized Deny Full Access delegation permission, the Deny permission takes precedence and the user is not given read access.

Table 4-5 Effect of delegate archive access permissions when granted to a mail-enabled security group (*continued*)

Delegate archive access permission	Granted in these circumstances	Effect of granted permission in Alta Personal Archive
SEND AS	The group has a synchronized Send As delegation permission.	No effect in Alta Personal Archive at this release.
ON BEHALF	The group has a synchronized Send On Behalf delegation permission.	No effect in Alta Personal Archive at this release.

The **Delegate Access** panel does not list any synchronized deny delegation permissions, although Veritas Alta Archiving takes account of these permissions when it determines whether to allow delegated access. If conflicting delegation permissions are synchronized, Veritas Alta Archiving gives precedence to deny permissions. For example, suppose that a user is granted **Full Access** delegation permission for a mailbox. Suppose also that the user belongs to a mail-enabled security group that has **Deny Full Access** delegation permission for the same mailbox. If Veritas Alta Archiving synchronizes both of these delegation permissions, then it does not grant the user read access permission for the mailbox archive.

The following illustration shows the **Delegate Access** panel for an example archive account.

Delegate Access (3)

	READ	SEND AS	ON BEHALF
qagbr3@qa.07exch01.com	●	○	○
qagbrgroup1	○	●	○
QAJournalDDG	●	○	●

The panel shows that three users or groups have delegate archive access permissions for this account:

- User **qagbr3@qa.07exch01.com** has **READ** permission. This permission means that when qagbr3 logs in to Alta Personal Archive, qagbr3 is able to read the archived items for the account.
- Group **qagbrgroup1** has **SEND AS** permission. This **SEND AS** permission has no effect in Veritas Alta Archiving at this release.
- Group **QAJournalDDG** has both **READ** permission and **ON BEHALF** permission. The **READ** permission means that a user who belongs to this group can view the account's archived items from Alta Personal Archive, unless the user has a **Deny Access** delegation permission that Veritas Alta Archiving has

synchronized. The **ON BEHALF** permission has no effect in Veritas Alta Archiving at this release.

The History panel

The **History** panel contains a summary of the most recent changes that were made to the archive account's settings. The panel logs any changes that relate to the details that are shown on the account details page, including any of the following:

- The creation details for the account. This information is always shown at the top of the **History** panel.
- Changes to the first name, last name, user name, primary email address, time zone, or role.
- Changes to the account status, such as account enabling and login enabling.
- Changes to enabled services.
- Changes to archive aliases.

Note: Changes to Folder Sync status are not recorded in the **History** panel.

The **History** panel shows a maximum of 30 changes.

To obtain more details for a particular change, you can click **View logs for more details** at the bottom of the history pane to explore the Veritas Alta Archiving logs. The link takes you to the **Logs** page under **Reporting** in the left pane.

See [“About Veritas Alta Archiving reports, logs, usage, and notifications”](#) on page 170.

Deleting an archive account

You can delete an archive account if it is no longer required. However, you cannot delete an archive account if it is part of a matter in Alta eDiscovery.

Note: If you delete an archive account, the archived messages for the user remain in Veritas Alta Archiving. These archived messages are not searchable by reviewers or administrators because the account and the associated user is not visible in both Veritas Alta View Compliance and Governance Management Console Console and Discovery Archive. Any new email messages that are sent to the user are archived in the Unassigned Legacy account.

To delete an archive account

- 1** In the left navigation pane, select **Configuration > Account Management**.
The application displays a list of archive accounts.
- 2** Search for and select the archive account of which you want to delete.
For quick and advance searching, See [“Searching for archive accounts”](#) on page 39.
- 3** Click **Edit**.
- 4** To delete the selected archive account, click **Delete Archive**.
The application prompts you to confirm that you want to perform the operation.
- 5** Click **Yes**.

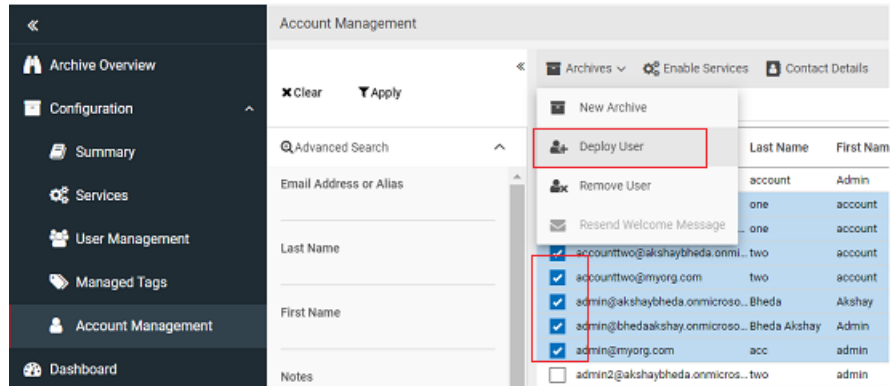
Deploying users

Once you have created new archive accounts you can give the users access to Alta Personal Archive and Alta eDiscovery from Account Management. You can also deploy Alta Personal Archive web folders and send welcome messages to users.

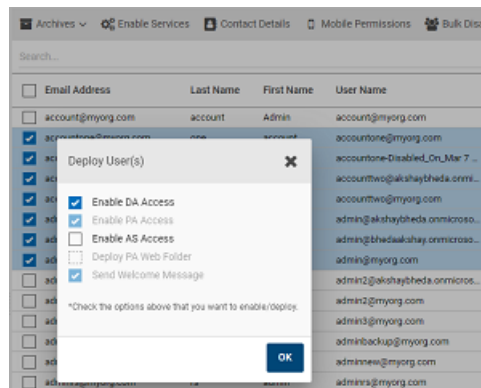
To deploy users

- 1** In the left navigation pane, select **Configuration > Account Management**.
The application displays a list of archive accounts.
- 2** Search for and select the archive account for which you want to deploy users.
For quick and advance searching, See [“Searching for archive accounts”](#) on page 39.
- 3** From the accounts list, select the check box for each archive account that you want to deploy.

- 4 On the action bar, click **Archives** and then click **Deploy User** as shown in the sample image below.



- 5 In the **Deploy Users** window, select one or more of the following deployment tasks:



- **Enable DA Access** — provides access to Alta eDiscovery.
- **Enable VAS Access** — provides access to Advanced Supervision.
- **Enable PA Access** — provides access to Alta Personal Archive.
- **Deploy PA Web Folder** — creates a Microsoft Outlook web folder for accessing Alta Personal Archive.
- **Send Welcome Message** — sends a welcome message with login credentials.

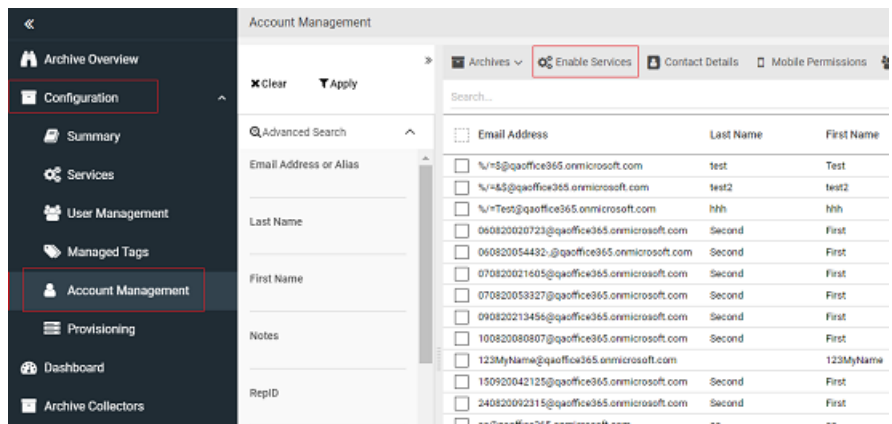
- 6 Click **OK**.

Enabling services for existing archive accounts

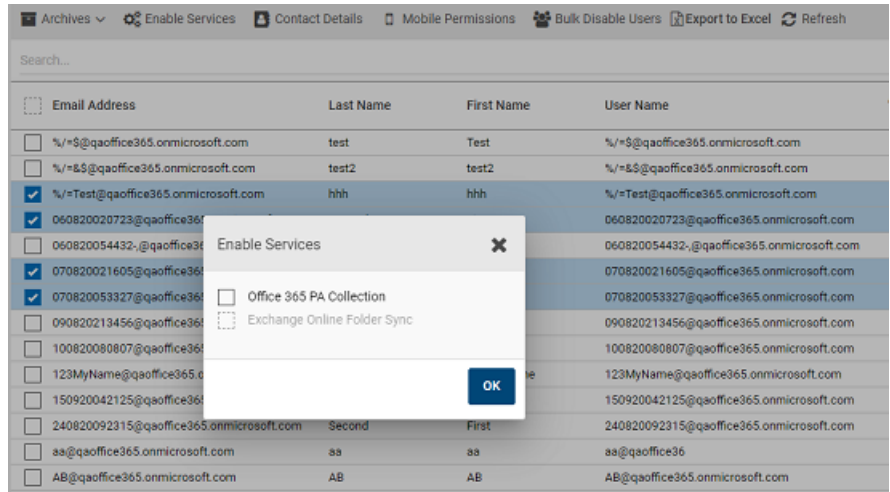
In addition to enabling services when creating new archive accounts, you can enable services for one or more existing archive accounts from the **Account Management** page.

To enable services for existing archive accounts

- 1 In the left navigation pane, select **Configuration > Account Management**.
The application displays a list of archive accounts.
- 2 Search for and select the archive accounts whose services you want to enable.
For quick and advance searching, See [“Searching for archive accounts”](#) on page 39.
- 3 On the action bar, click **Enable Services** as shown in the sample image below.



- 4 In the **Enable Services** window, select one or more of the following option:



- **Office 365 PA Collection** — Enables Exchange Online Personal Archive collections.
- **Exchange Online folder Sync** — Enables Exchange Online folder synchronization.

5 Click **OK**.

If the services are enabled successfully, the application displays the success message.

6 On the account details page, ensure that the selected services are enabled.

Note: The accounts that are not created by using Office 365 or Exchange online does not get enabled for Exchange Online Folder Synchronization. In case you receive such notification, click **Close**.

The application displays the notification for successful enabling of services. In case you receive such notification, click **Close**.

Removing user access

From the **Account Management** page you can remove Alta Personal Archive and Alta eDiscovery user access to the archive accounts that you select.

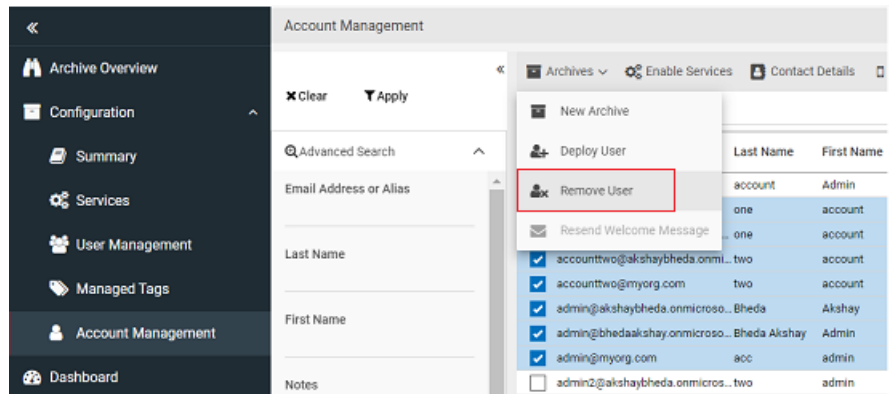
Note: If you want to remove deployed Alta Personal Archive web folders, contact [Veritas Services & Support](#).

To remove user access

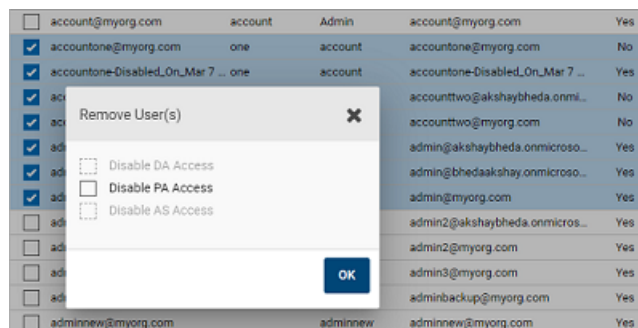
- 1 In the left navigation pane, select **Configuration > Account Management**.
The application displays a list of archive accounts.
- 2 Search for and select the archive account for which you want to remove user access.

For quick and advance searching, See [“Searching for archive accounts”](#) on page 39.

- 3 On the action bar, click **Archives** and then click **Remove User** as shown in the sample image below.



- 4 On the **Remove Users** page, select one or more of the following deployment tasks:



- **Disable DA Access** — removes Alta eDiscovery access.
- **Disable VAS Access** — removes Advanced Supervision access.

- **Disable PA Access** — removes Alta Personal Archive access.

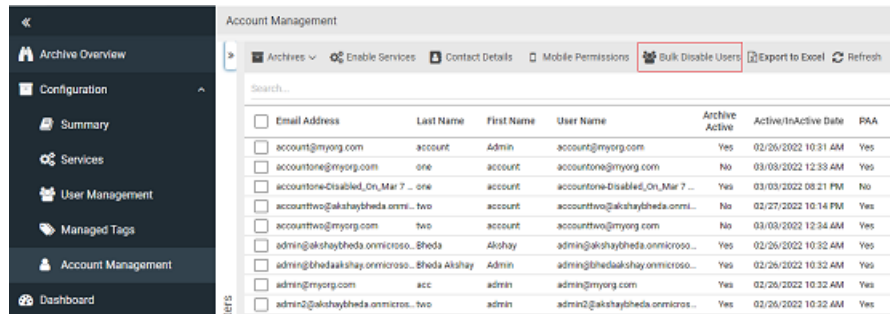
5 Click **OK**.

Disabling bulk user accounts

Prerequisite: Before you disable user accounts in bulk, ensure that the respective customers, who own these user accounts, have unlicensed these users. Otherwise, these user accounts get enabled again when you perform the O365 synchronization.

To disable bulk user accounts

- 1 In the left navigation pane, select **Configuration > Account Management**.
The application displays a list of archive accounts.
- 2 On the action bar, click **Bulk Disable Users** as shown in the sample image below.



The **Bulk Disable Users** dialog box appears.

Bulk Disable Users

☒ Rename with disabled string and datetime

☐ Rename with custom string

☐ Rename with custom prefix string

Note: If the user name is **AAA@test.com**, you need to rename it in the following pattern.

- When you select the **Rename with disabled string and datetime** option, rename it as **AAA-Disabled_On_Feb 11 2021 3:48AM@test.com**
- When you select the **Rename with custom string** option, and the custom string is **Disabled**, rename it as **AAA-Disabled@test.com**
- When you select the **Rename with custom prefix string** option, and the custom prefix string is **ZZZ** or **ZZZ_**, rename it as **ZZZ_AAA@test.com**

Search...

Status	UserName
<input type="checkbox"/>	account@myorg.com
<input checked="" type="checkbox"/>	accountone-Disabled_On_Mar 7 2021 11:53PM@akshaybheda.onmicrosoft.com
<input type="checkbox"/>	admin@akshaybheda.onmicrosoft.com
<input type="checkbox"/>	admin@bhedaakshay.onmicrosoft.com
<input type="checkbox"/>	admin@myorg.com
<input type="checkbox"/>	admin2@akshaybheda.onmicrosoft.com
<input type="checkbox"/>	admin2@myorg.com
<input type="checkbox"/>	admin3@myorg.com
<input type="checkbox"/>	adminbackup@myorg.com
<input type="checkbox"/>	adminnew@myorg.com

Items per page: 30 1 - 30 of 64

Update

- 3 Before you select multiple users for bulk disabling, assuming user name is **AAA@test.com**, select one of the following renaming patterns:

- Select the **Rename with disabled string and datetime** option to rename it as **AAA-Disabled_On_Feb 11 2021 3:48AM@test.com**.
 - Select the **Rename with custom string** option, and specify the custom string is Disabled to rename it as **AAA-Disabled@test.com**.
 - Select the **Rename with custom prefix string** option, and specify the custom prefix string is ZZZ or ZZZ_ to rename it as **ZZZ_AAA@test.com**.
- 4 Search for and select multiple user accounts you want to disable simultaneously.
 - 5 Click **Update** to initiate bulk disabling of user accounts.

Editing Mobile Web Access permission for existing archive accounts

You can edit the Mobile Web Access permission for one or more existing archive accounts.

Note: To make the Mobile Web Access feature available you must also enable Mobile Web Access under **Policy Management > Archive Options**.

See [“Configuring archive options”](#) on page 138.

Use any of the following procedures to set Mobile Web Access permissions for the existing archive accounts, as required.

To edit the Mobile Web Access permission for selected or all existing accounts

- 1 In the left navigation pane, select **Configuration > Account Management**.
The application displays a list of archive accounts.
- 2 Do any of the following as required.
 - To set the permission for the selected accounts, search for and select the archive accounts whose Mobile Web Access permissions you want to edit. Then, click **Mobile Permissions**.
 - To set the permissions for all existing archive accounts, do not select any accounts. Instead, click **Mobile Permissions** on the action bar.
- 3 In the **Mobile Interface Account Permissions** window, select one of the following options:
 - **Permit Mobile Web Access for selected accounts**
This option grants Mobile Web Access permission for the accounts you selected.
 - **Permit Mobile Web Access for all current accounts**

Note: Take care when using this option, as it grants Mobile Web Access permission to all existing archive accounts.

■ Deny Mobile Web Access for selected accounts

This option removes Mobile Web Access permission for the accounts you selected.

■ Deny Mobile Web Access for all current accounts

Note: Take care when using this option, as it removes Mobile Web Access permission for all existing archive accounts.

4 Click **Save**.

To edit the Mobile Web Access permission for a single account

1 In the left navigation pane, select **Configuration > Account Management**.

The application displays a list of archive accounts.

2 Search for and select the archive account whose Mobile Web Access permission you want to edit.

In the account details page, under **Services**, the **Alta Personal Archive Mobile** status indicates whether the Mobile Web Access permission is set.

The screenshot displays the 'Accounts' management interface. On the left is a navigation pane with options like 'Archive Overview', 'Configuration', 'Summary', 'Services', 'User Management', 'Managed Tags', 'Account Management', 'Dashboard', 'Archive Collectors', 'Role Management', and 'Policy Management'. The main area is titled 'Accounts' and shows details for an account with email 'account@myorg.com'. The 'Status' section includes 'Account' (Enabled), 'Login' (Unlocked), 'Archiving' (Enabled), 'Folder Sync' (Disabled), and 'External Reviewer' (No). The 'Services' section lists various services with checkboxes: 'Personal cloud' (checked), 'Personal cloud Mobile' (checked and highlighted with a red box), 'Discoverycloud' (checked), 'Advanced Supervision' (unchecked), 'Chatter' (unchecked), 'Office 365' (checked), 'Blackberry' (checked), and 'Exchange Online Folder Synchronization' (unchecked). Below this is a section for 'Archive Aliases (1)' with a star icon and the email 'account@myorg.com'. On the right, a 'History' tab shows a list of events such as 'Created admin acc', 'Archive Administration Account Edit', 'Password Changed', and 'Archive Administration Account Edit' with associated dates and users.

3 To change the Mobile Web Access permission setting, click **Edit**.

4 Under **Services**, select or clear **Alta Personal Archive Mobile** as required.

5 Click **Save** to save your changes.

Unlocking an archive account

As a security measure, Veritas Alta Archiving temporarily locks users out of their archive accounts if they enter their login credentials incorrectly five times within one hour. After users enter their credentials incorrectly three times, they are notified they have two additional attempts and are required to enter a CAPTCHA Validation Code. After they enter their credentials incorrectly five times, Veritas Alta Archiving locks the archive account. If an account becomes locked, an administrator can remove the lock from Veritas Alta View Compliance and Governance Management Console.

To unlock an archive account

- 1 In the left navigation pane, click **Account Management**.
- 2 From the accounts list, select the archive account that has been locked.
- 3 In the **Services** section of the account details page, clear **Account Locked**.
- 4 Click **Save**.

Exporting archive account information

You can export the account information for all archive accounts in your organization. Password information is not included in the export file.

Note: You can currently only export account information for all of the archive accounts. Even if you select individual accounts from the accounts list before you export the account information, the export file contains information for all accounts.

To export archive account information

- 1 In the left navigation pane, select **Configuration > Account Management**.
The application displays a list of archive accounts.
- 2 On the action bar, click **Export to Excel**.
The application downloads the archive accounts information report on your local computer.

Editing contact details of a system administrator

You can edit the administrator and the billing contact details from two places.

- From **Archive Overview > Archive Usage** page. See [“Archive Usage”](#) on page 19.
- From **Configuration > Account Management** page.

The procedure is explained below.

To edit contact details of a system administrator

- 1** In the left navigation pane, click **Configuration > Account Management**.
- 2** On the action bar, click **Contact Details**.
- 3** Click **Edit** and provide a new admin contact and billing contact details.
- 4** Click **Save**.

Managing Archive Collectors

This chapter includes the following topics:

- [About Archive Collectors](#)
- [Adding new archive collectors](#)
- [Updating configuration of existing archive collectors](#)
- [Stopping the import job of archive collectors](#)
- [Restarting import job of archive collectors](#)
- [Viewing the latest status of Archive Collectors](#)
- [Deleting an existing archive collector](#)
- [About Exchange Online Archiving](#)
- [About Bloomberg Archiving](#)
- [About Microsoft Teams Archiving](#)
- [About OneDrive for Business Archiving](#)
- [About Data Uploading](#)
- [About Alta Capture Services Archiving](#)

About Archive Collectors

In addition to email messages, your organization can use Veritas Alta Archiving to archive items from other content sources. Currently, Veritas Alta Archiving supports archiving of items from the following collectors:

- Exchange Online
- Microsoft Teams
- Bloomberg
- OneDrive for Business
- Enterprise Vault
- Alta Capture services

You can configure the following Alta Capture services if you have subscribed for these services (purchased a user license).

Microsoft Teams via Export API | Microsoft Teams Meeting | Exchange Mailbox Graph | Microsoft Teams via Webhooks | Slack PDGAlta eDiscovery | Bloomberg | IceChat | Twitter | OneDrive for Business | Box | Google Drive | Citrix Workspace & Sharefile | Dropbox Business | SharePoint | Amazon | EML | BlackBerry | Yammer | UBS | XSLT/XML | EWS | Pivot | Text-Delimited | Crowd Compass | CellTrust | Refinitiv | Symphony | Workplace from Facebook | Salesforce Chatter | Chatter Cipher Cloud | FXConnect | XIP | Yieldbroker | Webpage Capture | Redtail Speak | ServiceNow | RingCentral | Zoom Meetings | Zoom Meetings via Archiving API | Cisco Webex Teams | YouTube

From the **Archive Collectors** section, you can access the Veritas Alta View Compliance and Governance Management Console pages to enable the above-mentioned collectors.

Adding new archive collectors

Before you add a collector, ensure that you have purchased its license.

To add a new archive collector

- 1 In the left navigation pane, select **Archive Collectors**.

Note: The **Archive Collectors** node appears in the left navigation pane only if -

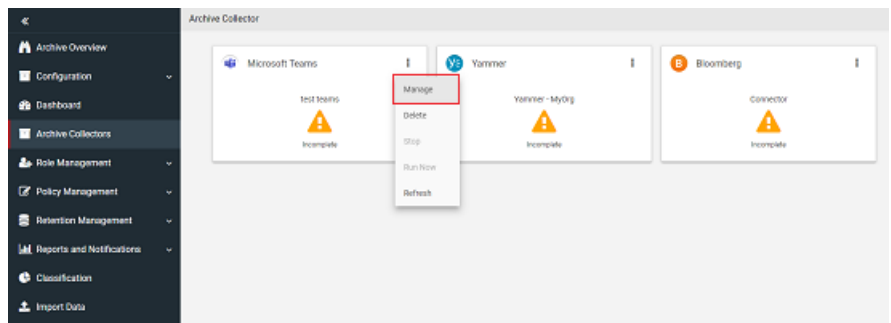
- the customer has purchased the services like Exchange Online, Microsoft Teams, OneDrive for Business and so on.

- The service is enabled for the customer
- 2 On the **Archive collector** page, click **Add collector**.
All the available collector types appears.
- 3 In the **Select type** field, select the category to narrow down the list of collectors.
Alternatively, in the **Search** field, type the collector name you want to search.
- 4 Select the collector, and click **Configure**.
The corresponding collector configuration page appears.

Updating configuration of existing archive collectors

To update configuration of an existing archive collector

- 1 In the left navigation pane, select **Archive Collectors**.
The application displays the available archive collector cards.
- 2 Select the archive collector for which you want to update the configuration.



- 3 Click the kebab icon (three vertical dots) on the archive collector card, and click **Manage**.
- 4 Provide the configuration details in the configuration wizard.

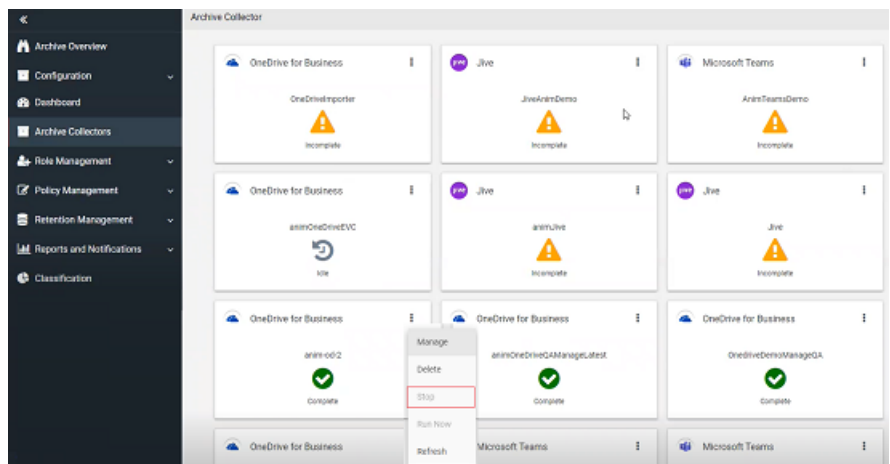
Refer to the [Alta Capture Collectors Configuration Guide](#) to understand configuration fields of corresponding archive collectors (importers) and complete the configuration steps. After successful configuration, the updated archive collector appears in the Veritas Alta View Compliance and Governance Management Console console.

Stopping the import job of archive collectors

You can stop the running or queued import job of only Veritas Alta Archiving specific Teams and OneDrive for Business, and any Alta Capture Archive Collectors.

To stop the import job of an archive collector

- 1 In the left navigation pane, select **Archive Collectors**.
The application displays the available archive collector cards.
- 2 Select the archive collector for which you want to stop the import job.



- 3 Click the kebab icon (three vertical dots) on the archive collector card, and click **Stop**.

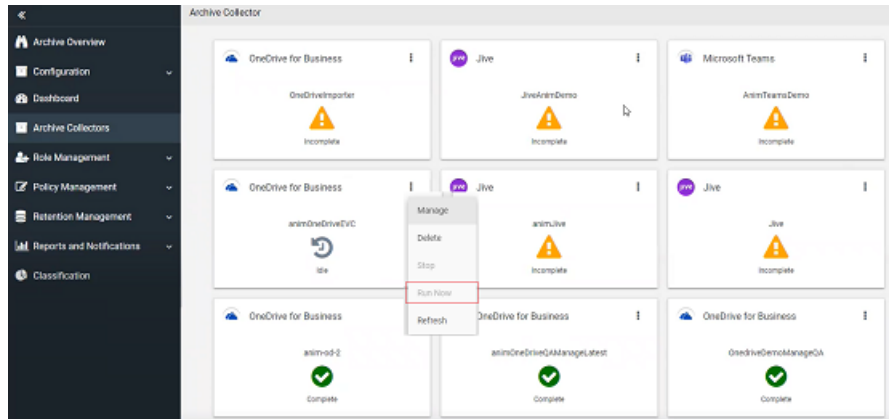
The application stops the import job of the archive collector.

Restarting import job of archive collectors

Instead of waiting for the scheduled run, you can also manually trigger the collection for idle Teams, OneDrive for Business, and any Alta Capture Archive Collectors. When you run the collection job, the application queues up the selected archive collector for collection.

To restart the import job of an archive collector

- 1 In the left navigation pane, select **Archive Collectors**.
The application displays the available archive collector cards.
- 2 Select the stopped archive collector for which you want to restart the import job.



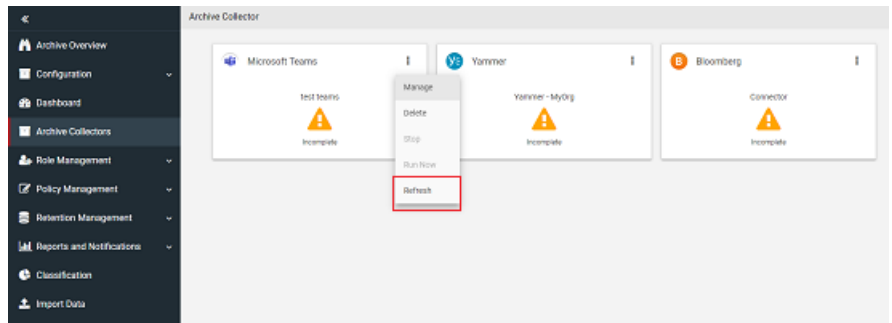
- 3 Click the kebab icon (three vertical dots) on the archive collector card, and click **Run Now**.
the application queue up the selected archive collector, and restarts its import job.

Viewing the latest status of Archive Collectors

You can view the latest statuses (Idle, Queued, Running and Stopping) of the archive collectors.

To view the latest status of Archive Collectors

- 1 In the left navigation pane, select **Archive Collectors**.
The application displays the available archive collector cards.
- 2 Select the archive collector of which you want to view the latest status.
- 3 Click the kebab icon (three vertical dots) on the archive collector card, and click **Refresh**.



The application displays the latest state of the archive collector.

Deleting an existing archive collector

To delete an existing archive collector

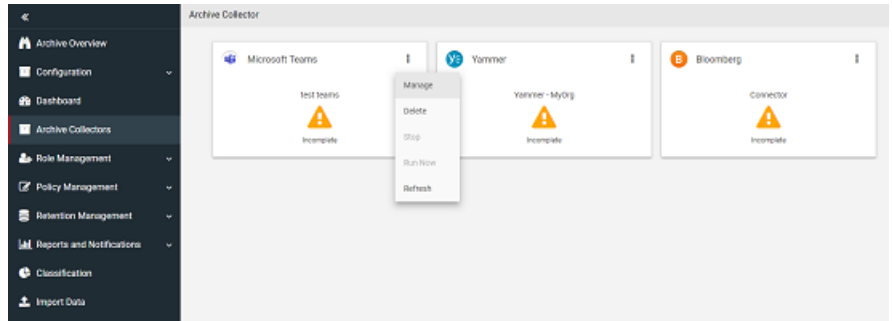
- 1 In the left navigation pane, select **Archive Collectors**.

The application displays the available archive collector cards.

Note: The **Archive Collectors** node appears in the left navigation pane only if -

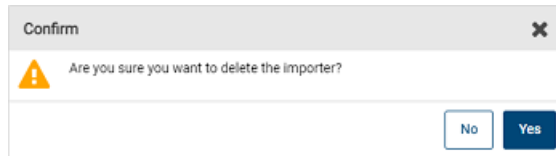
- The customer has purchased the services like Exchange Online, Microsoft Teams, OneDrive for Business and so on.

- The primary and secondary service is enabled for the customer
- 2 Select the archive collector you want to delete.



- 3 Click the kebab icon (three vertical dots) on the archive collector card, and click **Delete**.

The application prompts you to confirm that you want to perform the operation.



- 4 Click **Yes**.

About Exchange Online Archiving

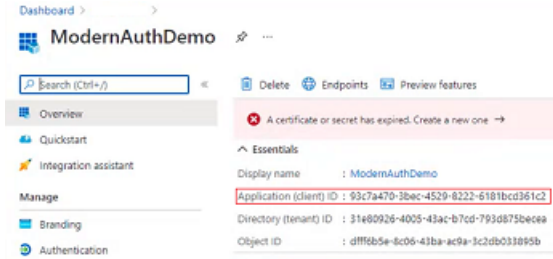
Setting up modern authentication in Azure AD for Exchange Online sync

If you want to use modern authentication for O365 sync, you need to configure an app in Azure AD. After you complete this setup, you get the Application (Client) ID and the primary domain details. These details are required to manage Exchange Online synchronization.

To set up modern authentication in Azure AD for Exchange Online sync

1 Create a new Azure AD app.

To create app on the Azure Active Directory, you need to select **App Registrations** in the left navigation pane. Click **New Registration**, and provide the user-facing display name of the application. Click **Register**.



Copy and note the Application (Client) ID.

- 2 On the Azure AD portal, select **Certificates & secrets**, and upload the public key for a self-signed certificate created by you for the Azure AD app.

Note: You can use any secured method to create a self-signed certificate and a public key. However, in this sample scenario, to create a self-signed certificate and a public key, the Create-SelfSignedCertificate.ps1 script is executed. This script is available with the Exchange Online V2 module. Save or install the module from

<https://www.powershellgallery.com/packages/ExchangeOnlineManagement/2.0.3>

**Example to create a self signed certificate using
Create-SelfSignedCertificate.ps1**

```
< Location where ExchangeOnlineManagement is installed or saved  
>\ExchangeOnlineManagement\2.0.3\Create-SelfSignedCertificate.ps1  
  
-CommonName AnimDemoCert -StartDate (Get-Date).Date -EndDate  
(Get-Date).Date.AddYears(1)
```

After successful execution of this script, a self-signed certificate (.CER) and the public key (.PFX) will be created in the current working directory. You can use the .PFX certificate file in Veritas Alta Archiving, and corresponding .CER certificate file in Azure Active Directory.

Note the password used for the certificate. You need this password later while configuring the Exchange Online sync in Archive Administrator.

In the above example, the self-signed certificate is valid for a year. You can choose the certificate expiry as required.

-
- 3 Upload the certificate (.CER file) that you have created in the previous step.
Select **Certificates & secrets** in the left navigation pane. Upload the certificate (.CER file) that you have created in the previous step.

Note: Certificates are the recommended way to connect to a registered Azure AD app and also Exchange Online V2 module only supports using certificates to connect to Exchange Online using a registered Azure AD app.

- 4 Provide the required API permissions to the app.
The following Azure AD app permissions are required for configuring Exchange Online sync with Modern Authentication:

Note: The following permissions are required to support for full functionality of this feature. Items noted below as **optional** can be omitted if the **API permission use** and the associated functionality is not required for your environment.

Exchange web
service (EWS
APIProxy)

(Optional)

API permission use: Web folder deployment

Note: This permission is required for the initial configuration, but is optional for ongoing use if this functionality is not required. You can remove it after initial configuration.

How to configure: Exchange Online > Application permissions > Other permissions > full_access_as_app

Exchange Online
V2 (PowerShell)

(Required)

API permission use: To get exchange related information like delegated permissions, DL membership, and DDL membership.

API permission path: Exchange Online > Application permissions > Exchange > Exchange.ManageAsApp

Note: Exchange.ManageAsApp permission is required. For reference, see [Set up app-only authentication](#)

Role: One of the following roles is required.

- Need to assign RBAC roles to the app. You can assign any of the following roles:
 - **Exchange Administrator:** Use this role if you want the Exchange Online Sync connector create and manage journal address and journal rules in Exchange automatically for you.

How to configure: AAD->Roles and Administrators->Exchange Administrator->Add Assignments->Search for the app-> Select app-> Add Exchange Administrator
 - **Global Reader:** Use this role if you prefer to create and manage journal address and journal rules in Exchange manually.

How to configure: AAD->Roles and Administrators->Global Reader->Add Assignments->Search for the app-> Select app-> Add Global Reader.

Note: You cannot see the App immediately after creating it. This could take 12-24 or more hours for the app to show up in the list to be selected.
- Need to assign the Exchange Administrator role to add journal address in provisioning configuration automatically in exchange.
- Else, the Global Reader role serves the same purpose for syncs.

Graph API

API permission use: To get user license and other information from Azure AD.

How to configure:

- MS Graph > Application permissions > User > User.Read.All
- MS Graph > Application permissions > Directory > Directory.Read.All

Permissions to be assigned: You need to at least assign the User.Read.All permission to the application.

Reference: See [Permissions](#)

- 5 To add the journal address automatically to Exchange, add app as an **Exchange Administrator**.

Alternatively, if you want to add the journal address manually, assigning the **Global Reader** role is enough.

- 6 From the Azure AD portal, select **Custom domain names** to view domain names for the Tenant.

Copy and note a domain **Name** that is **Available** and contains **.onmicrosoft.com** which is required to use as the **Tenant Name** for full functionality in the configuration of Exchange Online sync in Veritas Alta Archiving.

Example: evcloud.onmicrosoft.com

Configuring Exchange Online sync

You must configure Exchange Online Sync if you selected the option on the User Management page to manage account provisioning with Exchange Online.

To set up Exchange Online Sync, you must first provide the credentials of a Office 365 account. After successful access to the Exchange Online Archiving service, you can do the provisioning and configuring steps. Finally, you need to schedule the Exchange Online sync.

To configure Exchange Online sync

- 1 Navigate to the Veritas Alta View Compliance and Governance Management Console portal. Do any of the following:

- In the left navigation pane, select **Configuration > User Management**. On the User Management page, ensure that the **Using Office 365** check box is selected. Click **Save** and then click **Go to next step**. Click the **Exchange Online** link to navigate to the Archive Collectors portal.

Veritas Alta View Compliance and Governance Management Console navigates you to the **My Configuration** page and guides you to perform the required configuration steps for the provisioning options you have selected.

- In the left navigation pane, select **Archive Collectors**.
The Archive Collectors portal appears.

Note: The Archive Collectors node appears in the left navigation pane, only when either of the following secondary services is selected:

- When the Using Microsoft Office 365 check box is selected on the **User Management** page.
- When the **Bloomberg Archiving** check box is selected on the **Customer Details** page of the **Customer Service** tab.

By default, the **Exchange Online** page appears.

- 2 On the **Credential Management** page, select the appropriate credential type to connect to the Exchange Online portal.

You can switch between the modern and the legacy authentication process. This affects how Veritas Alta Archiving connects to Microsoft to get your tenant information.

- If you want to select the modern authentication method, select the **Azure AD registered app configuration** option. Specify the following:

Client ID	Client ID (also known as Registered Azure AD application ID) is the unique identifier that gets generated while setting up the modern authentication in Azure AD. Provide this application ID in this field.
Tenant Name	This is a Primary Domain for the Azure AD tenant. You can get this ID from the Tenant Information section on Overview page of Azure AD portal.
Certificate	Certificate is the Self-signed .PFX file. If a certificate is already uploaded, the Use existing certificate option appears by default. The thumbprint and expiry details of this certificate appears. To upload a new certificate, select the Use new certificate option, and upload the .PFX file.

Certificate	This is a password used for the self-signed certificate.
Password	Provide this password when you upload a new certificate.

- If you want to use legacy authentication option, select the **PowerShell credential + Exchange services credentials** option. Specify the following:

PowerShell credentials	<p>Provide the credentials for an Exchange Online account under which Exchange Online Sync can run the PowerShell commands to synchronize the accounts.</p> <p>Username: Enter the email address of an Exchange Online account that has the required permissions.</p> <p>Password: Enter the password for the Exchange Online account.</p>
Exchange web services credentials	<p>Provide the credentials for an Exchange Online account under which Exchange Online Sync can run the Exchange web services commands to synchronize the accounts.</p> <p>Use the same credentials as PowerShell: It is recommended to select this check box, to use the same account that you specified for running the PowerShell commands. Unless you have a requirement to use a different account, ensure that this check box is selected, and go on to the next step. To use a different Exchange Online account to deploy the web folders, clear this check box and enter the account's Username and Password.</p>

3 Click **Test** to verify connection with Exchange Online endpoint.

4 Click **Save** to navigate to the **Provisioning and configuration** tab.

Else, you can manually to the **Provisioning and configuration** tab. The application displays the connection confirmation notification and the last successful connection date and time. This notification disappears in a few seconds.

5 On the **Provisioning** page, do the following steps:

Synchronize user name from	<p>Select one of the following options:</p> <p>Email Address: Select this option to match the Username with the primary email address associated with the archive account.</p> <p>User Principal Name: Select this option to match the Username with the user principal name associated with the archive account.</p>
----------------------------	---

Domain
Provisioning

Select one of the following options:

Provision specific domains: Select this option to choose the Exchange Online domains for which you want to provision archive accounts. Then click **Specify Domains** and select the required domains from the list. The **Select Domains** check box lists all the domains that are associated with the configured Exchange Online account. To set a primary domain, select Set as Primary for the required domain. When you have chosen the domains, click **OK** to save the options you selected.

Provision all domains: Select this option to provision archive accounts for all the Exchange Online domains that are associated with the configured Exchange Online account.

Archive
Provisioning

Select one of the following options:

Provision Distribution Lists: Select this option to create archive accounts for the users that are associated with specific Exchange Online distribution lists for your company. Then click Specify Lists and select the required distribution lists. When you have chosen the distribution lists, click **OK** to save the options you selected.

Provision Dynamic Distribution Lists: Select this option to create archive accounts for the users that are associated with specific Exchange Online dynamic distribution lists for your company. Then click Specify Lists and select the required dynamic distribution lists. When you have chosen the dynamic distribution lists, click **OK** to save the options you selected.

Provision all users: Select this option to provision archive accounts for all the users in the domains that you specified in the previous step.

SMTP Journaling Select whether to provision journaling for Exchange Online Sync manually or automatically:

Manually provision journaling in Exchange Online: Select this option if you want to configure Exchange Online journaling manually from within the Exchange Online interface. If you choose this option, you must configure a suitable journaling rule manually in Exchange Online before you attempt to run a synchronization.

Choose manual provisioning if you want to configure specific journaling rules, for example to journal for a named distribution group. Otherwise you can choose automatic provisioning.

For information on how to configure journaling manually for Exchange Online Sync, see [Setting up Exchange Online journaling in the Veritas Alta Archiving Journaling Guide](#).

Note: The journal address that you must provide if you configure Exchange Online journaling manually is shown in the Journal address box under the Automatically provision journaling in Exchange Online option.

Automatically provision journaling in Exchange Online: Select this option to let Veritas Alta View Compliance and Governance Management Console configure a journaling rule automatically in Exchange Online. Veritas Alta View Compliance and Governance Management Console attempts to create the journaling rule when you click **Next** at the end of this procedure. The rule journals all items to the assigned Exchange Online journal address. Veritas Alta View Compliance and Governance Management Console prepopulates the Journal address box with the Exchange Online journal address that Veritas Alta Archiving has assigned to your company.

Note: You must also set up a send connector for Exchange Online. See [Setting up Exchange Online journaling in the Veritas Alta Archiving Journaling Guide](#).

Personal Archive Deployment Options

Under Web Folder Configuration, specify the following details:

- **Deploy Web Folder to Exchange Online:** Select this check box if you want Exchange Online Sync to deploy a Alta Personal Archive web folder when it provisions an archive account.
- **Archive Folder Name:** Enter the name to use for the Alta Personal Archive web folder, such as Personal Archive.
- **Archive Folder URL:** Enter your access URL for Alta Personal Archive.

Under Personal Archive Access, configure whether Veritas Alta Archiving automatically enables access to Alta Personal Archive and sends a welcome message email to each user.

- **Enable Personal Archive access and send Welcome Message:** Select this option to enable Alta Personal Archive access to each account that is provisioned, and to enable welcome messages to be sent to the provisioned users. If you select this option, you must select one of the sub-options.
- **Don't send Welcome Message if already sent:** Select this option to send a welcome message to a provisioned user only once. This is the default option.
- **Send Welcome Message anyway:** Select this option to send a welcome message every time that Exchange Online Sync synchronizes the account, even if a welcome message was sent previously.

Click the **Compose Welcome Message Template** link to create a new welcome message notification.

Notification Options

Under **Administration Roles to Notify**, do the following:

Show Notify Roles: Click this option to select the roles you want to get notified. Expand the role to view number of users available under that role.

Show Custom Roles: Click this option to select the customized roles you have created.

- 6 Click **Next** to save the provisioning details, and navigate to the **Configuration** page.

7 On the **Configuration** page, do the following steps:

- | | |
|------------------------------|--|
| Synchronize Shared Mailboxes | Select this check box to target every shared mailbox for synchronization in all of your Exchange Online domains. |
| Mailbox Delegate Permissions | <p>Select one of the following options to decide further action.</p> <p>Do not synchronize delegation permissions: Perform no synchronization of mailbox delegation permissions. If any mailbox delegation permissions are already synchronized, these remain unaffected.</p> <p>Synchronize delegation permissions: Synchronize the delegation permissions that are applied to the targeted mailboxes. In Alta Personal Archive a user is then able to access the archived content for each mailbox to which they have been granted delegate access.</p> <p>Remove synchronized delegation permissions: Remove any synchronized Exchange Online delegation permissions. All delegated access to Exchange Online archives is removed.</p> |

8 Click **Next** to save the configuration details, and navigate to the **Exchange Online Sync Scheduler** page.

9 On the **Exchange Online Sync Scheduler** page, do the following steps:

- | | |
|----------------|--|
| Sync Scheduler | Select this option to set up a synchronization schedule. Specify the start date and time for initiating the sync. |
| Sync Now | Select this option to run the Exchange Online synchronization on demand. Click Run Now for initiating the sync. |

10 Click **Next** to navigate to the **Summary** page.

11 On the **Summary** page, ensure the details. In case, you want to modify anything, click **Edit** to navigate to corresponding page.

About Exchange Online folder synchronization

Exchange Online folder synchronization is an add-on service for Veritas Alta Archiving to synchronize Exchange Online mailbox folders of users to Alta Personal Archive.

At present, customers are using the **Folder Sync** feature for folder synchronization of the on premise and exchange online users . However, the Exchange Online users are recommended to use the **Exchange Online Folder Sync** feature. Using Exchange Online folder synchronization is easy and beneficial for the following reasons:

- No need of any on premise hardware
- No need of any licenses like SQL Server, Windows Server, and so on
- Everything can be managed using Veritas Alta View Compliance and Governance Management Console console.

You must perform the following activities while managing Exchange Online folder synchronization.

- Enabling the Exchange Online Folder Synchronization service
- Enabling individual users for folder synchronization
- Configuring App in Azure AD with required permissions. See [“Setting up modern authentication in Azure AD for Exchange Online sync”](#) on page 73.
- Configuring Exchange Online folder synchronization
- Viewing status of individual users for Exchange Online folder synchronization

Prerequisite for migrating Exchange Online Users configured with Folder Sync to Exchange Online Folder Synchronization

Before you migrate users from the **Folder Sync** option to the **Exchange Online Folder Sync** option, you must understand the following aspects:

- Before you enable users for Exchange Online Folder Synchronization, make sure that these users are disabled in Folder Sync.
- If the users are enabled at both the places, then only the data received from the Exchange Online Folder Sync option is updated. However, the data received from the Folder Sync option is not considered while updating the folder structure.

Configuring Exchange Online folder synchronization

After specifying the required credentials, provisioning and configuring exchange online, you can schedule the Exchange Online folder synchronization.

Like Exchange Online Sync, the Exchange Online folder synchronization process uses modern authentication to use Graph APIs for fetching the folders related data from Exchange Online. To use modern authentication, you need to create and register an application Azure Active Directory for the tenant/domain in which the user accounts are available.

To understand the procedure to create an app in Azure Active Directory and assign Graph API permissions, See [“Setting up modern authentication in Azure AD for Exchange Online sync”](#) on page 73. You can use the same app that is used for Exchange Online Sync with the additional **Mail.ReadBasic.All** permission. The

Mail.ReadBasic.All permission needs to be an *Application* type permission and not a *Delegated* permission. Else, you can have a completely separate app for Exchange Online Folder Synchronization.

To configure Exchange Online folder synchronization

- 1 In the left navigation pane, select **Archive Collectors**.

The **Archive collector** page appears.

Note: The Archive Collectors node appears in the left navigation pane, only when either of the following secondary services is selected:

- When the Using Microsoft Office 365 check box is selected on the **User Management** page.
- When the **Bloomberg Archiving** check box is selected on the **Customer Details** page of the **Customer Service** tab.

- 2 Click **Add collector** to view available collector cards.

Note: At the time of adding the first collector, the **Add collector** button appears in the middle of the screen. If one or more collectors are already added, the **Add collector** option appears on the top right-hand corner.

If you select the collector that is not supported in Veritas Alta Archiving, the **Configure** button gets disabled. You cannot configure such collectors.

- 3 Select the Exchange Online collector for which you want to configure the folder synchronization.

Note: If Exchange Online archive collector that you want to configure for folder synchronization is not listed, add a new collector. See [“Adding new archive collectors”](#) on page 68.

- 4 Click on the Kebab icon (three vertical dots), and click **Manage**.

- 5 On the **Credential Management** page, ensure that the **O365 Sync** check box is selected by default. Select the **Folder Sync** check box.

6 Under **Folder Sync**, specify the following:

Use same credentials used in O365 Sync	<p>Select this check box to use the same Azure AD application that is configured for O365 sync.</p> <p>Note: If you do not select the Use same credentials used in O365 Sync check box, specify other configuration parameters explained in table below.</p>
Client ID	<p>Provide the client ID of the application registered in the Azure Active Directory.</p> <p>One tenant can have different client IDs and certificates.</p>
Tenant Name	Provide the Tenant or Domain name.
Certificate	<p>Select the Use existing certificate option if you have already created the .PFX certificate for the registered application.</p> <p>Select the Add new certificate option to browse and select the new certificate.</p>
Thumbprint	Specify the thumbprint which is used to validate the certificate.
Expires On	Specify the date of expiry for the mentioned certificate

7 Click **Test** below the Folder Sync option to test information provided for Folder Sync.

8 Click **Save** to navigate to the **Provisioning and configuration** tab.

Else, you can manually go to the **Provisioning and configuration** tab. The application displays the connection confirmation notification and the last successful connection date and time. This notification disappears in a few seconds.

Note: If the Exchange Online collector is already provisioned and configured, you can directly navigate to the **Folder Sync Configuration** tab (16). Else, follow step 9 to step 15 to provision and configure the collector.

9 On the **Provisioning** page, do the following steps:

Synchronize user name from	<p>Select one of the following options:</p> <p>Email Address: Select this option to match the Username with the primary email address associated with the archive account.</p> <p>User Principal Name: Select this option to match the Username with the user principal name associated with the archive account.</p>
Domain Provisioning	<p>Select one of the following options:</p> <p>Provision specific domains: Select this option to choose the Exchange Online domains for which you want to provision archive accounts. Then click Specify Domains and select the required domains from the list. The Select Domains check box lists all the domains that are associated with the configured Exchange Online account. To set a primary domain, select Set as Primary for the required domain. When you have chosen the domains, click OK to save the options you selected.</p> <p>Provision all domains: Select this option to provision archive accounts for all the Exchange Online domains that are associated with the configured Exchange Online account.</p>
Archive Provisioning	<p>Select one of the following options:</p> <p>Provision Distribution Lists: Select this option to create archive accounts for the users that are associated with specific Exchange Online distribution lists for your company. Then click Specify Lists and select the required distribution lists. When you have chosen the distribution lists, click OK to save the options you selected.</p> <p>Provision Dynamic Distribution Lists: Select this option to create archive accounts for the users that are associated with specific Exchange Online dynamic distribution lists for your company. Then click Specify Lists and select the required dynamic distribution lists. When you have chosen the dynamic distribution lists, click OK to save the options you selected.</p> <p>Provision all users: Select this option to provision archive accounts for all the users in the domains that you specified in the previous step.</p>

SMTP Journaling Select whether to provision journaling for Exchange Online Sync manually or automatically:

Manually provision journaling in Exchange Online: Select this option if you want to configure Exchange Online journaling manually from within the Exchange Online interface. If you choose this option, you must configure a suitable journaling rule manually in Exchange Online before you attempt to run a synchronization.

Choose manual provisioning if you want to configure specific journaling rules, for example to journal for a named distribution group. Otherwise you can choose automatic provisioning.

For information on how to configure journaling manually for Exchange Online Sync, see Setting up Exchange Online journaling in the Veritas Alta Archiving Journaling Guide.

Note: The journal address that you must provide if you configure Exchange Online journaling manually is shown in the Journal address box under the Automatically provision journaling in Exchange Online option.

Automatically provision journaling in Exchange Online: Select this option to let Veritas Alta View Compliance and Governance Management Console configure a journaling rule automatically in Exchange Online. Veritas Alta View Compliance and Governance Management Console attempts to create the journaling rule when you click **Next** at the end of this procedure. The rule journals all items to the assigned Exchange Online journal address. Veritas Alta View Compliance and Governance Management Console prepopulates the Journal address box with the Exchange Online journal address that Veritas Alta Archiving has assigned to your company.

Note: You must also set up a send connector for Exchange Online. See Setting up Exchange Online journaling in the [Veritas Alta Archiving Journaling Guide](#).

Personal Archive Deployment Options

Under Web Folder Configuration, specify the following details:

- **Deploy Web Folder to Exchange Online:** Select this check box if you want Exchange Online Sync to deploy a Alta Personal Archive web folder when it provisions an archive account.
- **Archive Folder Name:** Enter the name to use for the Alta Personal Archive web folder, such as Personal Archive.
- **Archive Folder URL:** Enter your access URL for Alta Personal Archive.

Under Personal Archive Access, configure whether Veritas Alta Archiving automatically enables access to Alta Personal Archive and sends a welcome message email to each user.

- **Enable Personal Archive access and send Welcome Message:** Select this option to enable Alta Personal Archive access to each account that is provisioned, and to enable welcome messages to be sent to the provisioned users. If you select this option, you must select one of the sub-options.
- **Don't send Welcome Message if already sent:** Select this option to send a welcome message to a provisioned user only once. This is the default option.
- **Send Welcome Message anyway:** Select this option to send a welcome message every time that Exchange Online Sync synchronizes the account, even if a welcome message was sent previously.

Click the **Compose Welcome Message Template** link to create a new welcome message notification.

Notification Options

Under **Administration Roles to Notify**, do the following:

Show Notify Roles: Click this option to select the roles you want to get notified. Expand the role to view number of users available under that role.

Show Custom Roles: Click this option to select the customized roles you have created.

10 Click **Next** to save the provisioning details, and navigate to the **Configuration** page.

11 On the **Configuration** page, do the following steps:

Synchronize Shared Mailboxes	<p>Select this check box to view the following options:</p> <ul style="list-style-type: none"> ■ Synchronize Shared Mailboxes: Select this check box to target every shared mailbox for synchronization in all of your Exchange Online domains. ■ Keep Personal Archive Login enabled for all Shared Mailboxes: Select this check box to allow users (who are blocked by Microsoft to access Exchange Online) to access their shared mailboxes available on Personal Archive. Usually, when Microsoft blocks the sign-in status of a user, the Veritas Alta Archiving administrator also blocks that user to access Exchange Online and Personal Archive. After you select this check box, all the shared mailboxes, which are in the scope of synchronization, with a sign-in status as Blocked from Microsoft, remain enabled in Veritas Alta Archiving.
Mailbox Delegate Permissions	<p>Select one of the following options to decide further action.</p> <p>Do not synchronize delegation permissions: Perform no synchronization of mailbox delegation permissions. If any mailbox delegation permissions are already synchronized, these remain unaffected.</p> <p>Synchronize delegation permissions: Synchronize the delegation permissions that are applied to the targeted mailboxes. In Alta Personal Archive a user is then able to access the archived content for each mailbox to which they have been granted delegate access.</p> <p>Remove synchronized delegation permissions: Remove any synchronized Exchange Online delegation permissions. All delegated access to Exchange Online archives is removed.</p>

12 Click **Next** to save the configuration details, and navigate to the **Exchange Online Sync Scheduler** page.

13 On the **Exchange Online Sync Scheduler** page, specify the following:

Sync Scheduler	Select this option to set up a synchronization schedule. Specify the start date and time for initiating the sync.
Sync Now	Select this option to run the Exchange Online synchronization on demand. Click Run Now for initiating the sync.

14 Click **Next** to navigate to the **Summary** page.

15 On the **Summary** page, ensure the details. In case, you want to modify anything, click **Edit** to navigate to corresponding page.

16 On the **Folder Sync Configuration** page, specify the following:

Mailbox Settings

Autoselect new Mailboxes	Select this option to enable folder synchronization for the shared and user mailboxes of a newly added user.
Deselect disabled Mailboxes	Select this option to disable folder synchronization for the mailboxes of the deleted user.
Concurrent Mailboxes	Select the number of user mailboxes to be processed at the same time.

Schedule

Next run at	Scheduled date and time at which folder synchronization will take place.
Repeat	Frequency at which folder synchronization takes place, such as daily, weekly, monthly.
Skip these folders while syncing	Select the folders that need to be skipped while performing folder synchronization.

17 Click **Save**.

18 To view your folder synchronization job progress and status, select the **Job List** tab.

The page displays the last successful run date and time, total number of exchange online accounts available, and number of accounts that are enabled for folder synchronization.

- To view Exchange Online Folder Synchronization jobs, select **Exchange Online Sync**.
- To view Folder Sync jobs, select **Folder Sync**.
- To refresh the page details, click the **Refresh** icon.
- If required, click the **Export** icon to export the job list in the CSV format.

About Bloomberg Archiving

The Bloomberg Archiving service is an add-on feature that lets customers archive the files and instant messages that are associated with their Bloomberg L.P. Professional service (Bloomberg Terminal). A Veritas Veritas Alta Archiving super administrator can only enable the Bloomberg Archiving secondary service for the customers.

The administrator from the customer's side can then configure the Bloomberg collector. This collector lets customers archive the Bloomberg Terminal emails and also Bloomberg Terminal instant message transcripts of their configured users in Veritas Alta Archiving. At the time of archiving, the Bloomberg emails and instant message transcripts are converted to email messages.

Before Bloomberg Archiving service can archive files, you must do the following for the Bloomberg firm code:

- Add the details of the firm code and its FTP login credentials.
- Upload the associated PGP private key file for the firm code.

Veritas Alta Archiving uses this information to log on to the Bloomberg FTP site on a scheduled basis and download the encrypted files for the Bloomberg firm code. Veritas Alta Archiving then decrypts the files and reconstitutes the messages for archiving.

Configuring the Bloomberg Synchronization

To configure the Bloomberg Synchronization

- 1 In the left navigation pane, select **Archive Collectors**.

The **Archive Collector** page appears.

Note: The **Archive Collectors** node appears in the left navigation pane, only when either of the following secondary services is selected:

- When the **Using Microsoft Exchange Online** check box is selected on the **User Management** page.
- When the **Bloomberg Archiving** check box is selected on the **Customer Details** section of the **Customer Service** tab.

- 2 Click **Add collector** to view available collector cards.

Note: At the time of adding the first collector, the **Add collector** button appears in the middle of the screen. If one or more collectors are already added, the **Add collector** option appears on the top right-hand corner.

If you select the collector that is not supported in Veritas Alta Archiving, the **Configure** button gets disabled. You cannot configure such collectors.

- 3 Select **Bloomberg**, and click **Configure**.

The **Bloomberg** page appears.

4 Under **Bloomberg Settings**, specify the following and click **Save**.

Firm Code Enter the Bloomberg firm code that identifies the Bloomberg customer whose Bloomberg messages you want to be able to archive

Note: Firm Code cannot be edited once it has been saved.

FTP Login Enter the FTP login name for the Bloomberg firm code.

FTP Password Enter the FTP password for the Bloomberg firm code.

Confirm Password Enter the same FTP password again for the Bloomberg firm code.

5 Under **Encryption Key**, do the following:

Upload encryption key Click Browse to access the encryption key, and click Upload.

Note: The token-signing certificate that you upload must have a .CER, .CRT or .PGP extension.

Passphrase Enter the pass phrase for the PGP private key.

Confirm passphrase Enter the same pass phrase for the PGP private key.

6 Click **Upload** to upload the encryption keys to Veritas Alta Archiving.

7 To view the configuration-specific logs, navigate to the **History** pane.

The application displays the available history of the last 20 changes.

8 To obtain more details for a particular change, click **View logs for more details**.

Alternatively, in the left navigation pane, select **Reports and Notifications > Logs**, where you can view Activity Log, Message Log, Usage Log, Mobile Browser Log, Personal Browser Log, and Discovery Browser Log.

About Microsoft Teams Archiving

The Microsoft Teams service is an add-on feature that lets customers archive the files that are associated with their Microsoft Teams service. A Veritas Veritas Alta Archiving super administrator can only enable the Microsoft Teams secondary service for the customers.

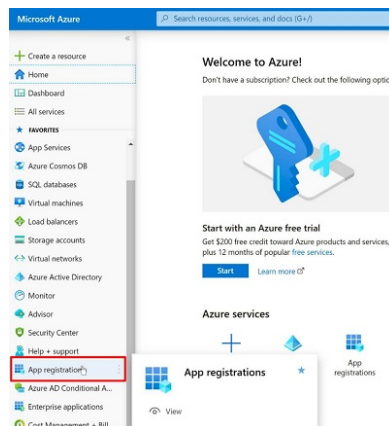
The administrator from the customer's side can then configure the Microsoft Teams collector. This collector lets customers archive the Microsoft Teams collaboration data (chats and files) of their configured users in Veritas Alta Archiving.

Registering a Microsoft Azure App for Teams Collector

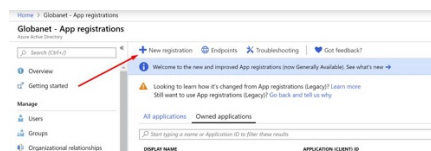
You need to register an app on Microsoft Azure Portal to use Microsoft Teams Collector. After you create this app, you get the Azure Tenant ID, Azure Client ID, and the primary domain details. These details are required for Microsoft Teams collector configuration.

To create a Microsoft Azure App for Teams Collector

- 1 Access the [Azure Portal](#) using the O365 (Global Admin) credentials.
- 2 In the left navigation pane, select **App registrations**.



- 3 Click **+ New registration**.



4 Provide a unique application name.

Ask the Veritas support team to provide the **Redirect URI** (along with the certificate) that you require while performing **step 7**.

Under **Redirect URI (optional)**, select **Web** and enter the Redirect URI provided by the Veritas support team. Veritas support provides this complete URL.

Register an application

* Name

The user-facing display name for this application (this can be changed later).

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Slobarek)

☐ Accounts in any organizational directory

☐ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

[Help me choose...](#)

Redirect URI (optional)

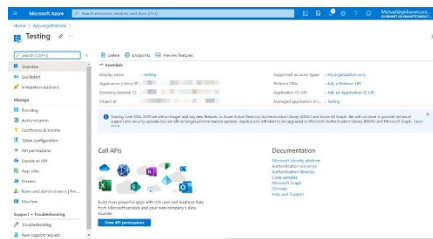
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

[By proceeding, you agree to the Microsoft Platform Policies](#) [↗](#)

[Register](#)

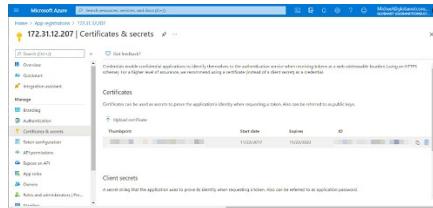
5 Click **Register**.

6 On the **Overview** page, search and note down the **Azure Tenant ID** and the **Azure Client ID**. These IDs are required for configuring the Microsoft Teams source in Archive Collectors.

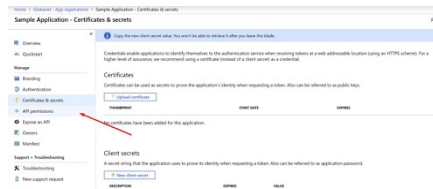


- 7 In the left navigation pane, select **Certificates & secrets**. Upload the certificate provided by Veritas.

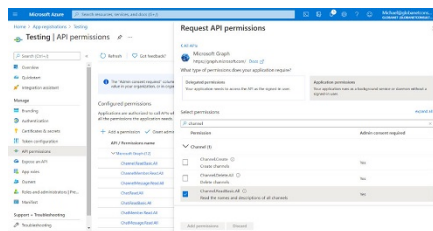
Veritas provides this certificate.



- 8 In the left navigation pane, select **API permissions**.



- 9 Click **Microsoft Graph**, and in the opened pane select **Application permissions**.

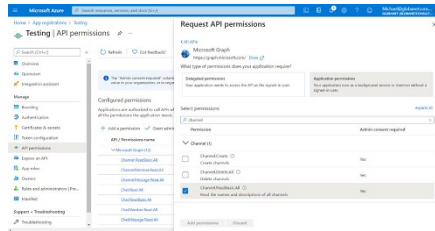


- 10 Select the following permissions:

- Channel:Channel.ReadBasic.All
- ChannelMember: ChannelMember.Read.All
- ChannelMessage: ChannelMessage.Read.All
- Chat: Chat.Read.All; Chat.ReadBasic.All
- ChatMember: ChatMember.Read.All
- ChatMessage: ChatMessage.Read.All

- Files: Files.Read.All
- Group: Group.Read.All
- Team: Team.ReadBasic.All
- User: User.Read.All

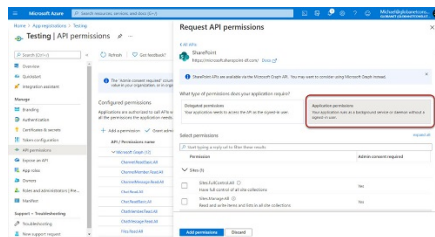
11 After you select all these check boxes, click **Add permissions**.



12 Navigate to the **API permissions** section, click **+ Add a permission**. Select **SharePoint > Application permissions**. Grant the following permissions:

- Sites: Sites.Read.All
- User: User.Read.All

13 After you select all these check boxes, click **Add permissions**.



14 After you select all these check boxes, click **Grant Admin Consent**.

Note: Due to the Microsoft API issues, you may encounter the following issues:

- If the message contains hosted content, there could be a delay in synchronizing the messages with attachments in chats and conversations.
- After deleting, the deleted messages are available for capture for 21 days only.

Requesting access to protected APIs in Microsoft Graph

After creating the Microsoft Teams app on the Azure Portal, you need to request access to the protected APIs in Microsoft Graph. For more information, see [Protected APIs in Microsoft Teams](#).

To request access to protected APIs

- 1 Open <https://aka.ms/teamsgraph/requestaccess>.

Request access to protected APIs in Microsoft Graph

** May 6, 2020 -- We have resumed regular regular protected API approvals. Earlier we had suspended approvals due to increased load from COVID-19. **

Microsoft Teams APIs in Microsoft Graph that access sensitive data are considered protected APIs. These APIs require that you have additional validation, beyond permissions, and consent, before you can use them. See <https://aka.ms/teamsgraph/protectedapis> for more details.

To request access to these protected APIs, complete the following request form. We review access requests weekly. If you would like to provide information in addition to the form, you can contact teamsgraph@microsoft.com.

* Required

1. Your email address and any others you want to list as an owner (semicolon separated) *
2. May we contact you about your app's use of non-protected APIs? (E.g., reliability issues, advanced notice of breaking changes, throttling, etc) *
3. Publisher name *
4. App name *
5. App id(s) to enable application permissions for *
6. What does your app do? Why does it exist? (2-3 sentences explaining to an admin who has never heard of your app what it is and why they want it) *
7. Why does your app need read access to all messages in the tenant? (If you don't, you don't need protected APIs) *
8. Data retention - select one of these options: *
9. What are the tenant ID's that this app needs to run in? (semicolon-separated. Put "all" if you're writing software for other organizations to use.) *
10. Does your organization own all those tenants? (If no, your answer above should be "all", or you should get the tenant owner to submit the request) *

Next

Never give out your password. Report abuse

2 Provide the required information, click **Next**.

Request access to protected APIs in Microsoft Graph

Required info if the app publisher does not own all the tenants the app will be run in.
If you do not have a homepage/terms of service/privacy statement yet because your app is under development, create a single-tenant appid and request protected API access for that.

11. What is the homepage URL registered for the appid? (Requests for multitenant access will be denied without this)

Enter your answer

12. Terms of service URL? (Requests for multitenant access will be denied without this)

Enter your answer

13. Privacy statement URL? (Requests for multitenant access will be denied without this)

Enter your answer

Back Next

Never give out your password. Report abuse

This content is created by the owner of the form. The data you submit will be sent to the form owner.
Powered by Microsoft Forms | Privacy and cookies | Terms of use

3 Provide the required information, click **Next**.

Request access to protected APIs in Microsoft Graph

Misc

14. Anything else we need to know that doesn't fit in the above?

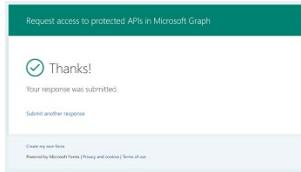
No

Back Submit

Never give out your password. Report abuse

This content is created by the owner of the form. The data you submit will be sent to the form owner.
Powered by Microsoft Forms | Privacy and cookies | Terms of use

- 4 Provide the required information, click **Submit**.



- 5 After Microsoft grants access to the protected APIs, contact [Veritas Support](#), and mention your organization name and e-mail address, and request an account.

Enabling Microsoft Teams Archiving service for customer

On the Veritas Alta View Compliance and Governance Management Console console, only the super administrator can view the **Customer Service** tab. Therefore, to enable the Microsoft Teams Archiving service for customers, you must possess the super administrator role . Before you enable the Microsoft Teams Archiving service for a customer, ensure that the customer is added to the Veritas Alta Archiving. See *Creating the archive instance for a customer* in the Veritas Alta Archiving **Customer Administration Guide**.

To enable the Microsoft Teams Archiving service

- 1 In the left navigation tab, select **Customer Service**.
- 2 In the left navigation pane, click **Customers**.
- 3 On the **Customers** page, search for and select the customer for whom you want to enable this service.

Note: If the customer is new, you need to add the customer in Veritas Alta Archiving. See *Creating the archive instance for a customer* in the Veritas Alta Archiving Customer Administration Guide.

- 4 In the **Services** section, do the following:
 - Ensure that, under **Primary Services**, the **Discovery Archive** service is already enabled for the customer. If this service is not enabled, select the **Discovery Archive** check box in the **Enabled** column to enable the service. Unless the **Discovery Archive** service is enabled, you cannot enable the **Microsoft Teams Archiving** service for this customer.
 - Under **Secondary Services**, select the **Microsoft Teams** check box in the **Enabled** column.

- 5 Click **Save**.
- 6 To verify if the Microsoft Teams service is enabled for the customer, login as a Customer Administrator.
- 7 In the left navigation pane, select **Configuration > Services**.

This page displays the services your company has purchased and been provisioned for. Please call your customer service representative if you want to add or change any of these services.

General Configuration

> Primary Services

Product	Enabled	# Users (Minimum)	# Users (Actual)
Personal Archive	<input checked="" type="checkbox"/>	0	346
Discovery Archive	<input checked="" type="checkbox"/>	0	363
Advanced Supervision	<input checked="" type="checkbox"/>	0	127
Manager	<input checked="" type="checkbox"/>	0	0
Email Confidentiality	<input type="checkbox"/>	0	0

Note: If a customer purchases Personal Archive without Discovery Archive, this is for the number of active archives rather than the explicit number of users with the Personal Archive designation.

>> Secondary Services

Product	Enabled	# Users (Minimum)	# Users (Actual)	Last Archived Date
Exchange Folder Synchronization	<input checked="" type="checkbox"/>	0	0	Not Applicable
Exchange Online Folder Synchronization	<input checked="" type="checkbox"/>	0	0	Not Applicable
Office 365 Personal Archive Collection	<input checked="" type="checkbox"/>	0	122	No Data
Veritas Information Classifier	<input checked="" type="checkbox"/>	0	363	Not Applicable
Microsoft Teams Archiving	<input checked="" type="checkbox"/>	0	363	Not Applicable
Onshore for Business Archiving	<input checked="" type="checkbox"/>	0	363	Not Applicable

- 8 Ensure that the **Microsoft Teams Archiving** service is selected under the **Secondary Services** section.

Note: You cannot disable or enable this service from this page. To disable this service, select **Customer Service > Customers**. Select the customer and clear the check box of the Microsoft Teams Archiving service in the **Enabled** column.

Configuring Microsoft Teams Synchronization

You must have a Customer Administrator role to configure Microsoft Teams synchronization.

To configure Microsoft Teams Synchronization

- 1 In the left navigation pane, select **Archive Collectors**.
The **Archive Collector** page appears.
- 2 Click **Add collector** to view available collector cards.

Note: At the time of adding the first collector, the **Add collector** button appears in the middle of the screen. If one or more collectors are already added, the **Add collector** option appears on the top right-hand corner.

If you select the collector that is not supported in Veritas Alta Archiving, the **Configure** button gets disabled. You cannot configure such collectors.

- 3 Select the **Microsoft Teams** card and click **Configure**.

4 On the **Configuration** tab, specify the following:

Name	Provide a unique name for this collector.
Description	Provide appropriate description to easily identify the collector.
X509 Certificate thumbprint	Specify the thumbprint to validate the certificate.
Azure Tenant ID	Use the Azure Tenant ID that you have noted down while registering the Azure App for OneDrive for Business. (Azure Tenant ID is a property of the Subscription.)
Azure Client ID	<p>Azure Client ID is generated when you register an App on the Azure portal. After registering an App, you need to note down this ID.</p> <p>Use the Azure Client ID that you have noted down while registering the Azure App for OneDrive for Business.</p>
Advanced configuration options	<p>Select the Capture all activities check box to include all Microsoft Teams activities in collector.</p> <p>Select the Capture certain activities check box to select the activities (Chats, Public Channel, and Private Channel) you want in collector.</p>
Primary time zone	By default, user's time zone is displayed. If required, select your preferred time zone.
Import scheduler	<p>Select the Run every hour option to schedule hourly import job frequency.</p> <p>Select the Schedule time option to schedule the import job to be applied on a specific day and time.</p>

5 Click **Save and Next** to navigate to the **User Source** tab.

6 On the **User Source** tab, under **User source configuration**, select any of the following options:

- Select the **All users** option to include all the available users.
- Select the **Select users from list** option to open the list of all users. Select the users whose activities you want to archive, and click **Confirm**.

7 Click **Save and Next** to navigate to the **Review** tab.

8 On the **Review** tab, do the following:

- Check the configuration information to ensure accuracy.

- To modify configuration information, click the corresponding **Edit** link.
- 9 If the data is correct, click **Complete**.

The Microsoft Teams archive collector appears on the **Archive collectors** page.

About OneDrive for Business Archiving

The OneDrive for Business service is an add-on feature that lets customers archive the files that are associated with their OneDrive for Business service. A Veritas Veritas Alta Archiving super administrator can only enable the OneDrive for Business secondary service for the customers.

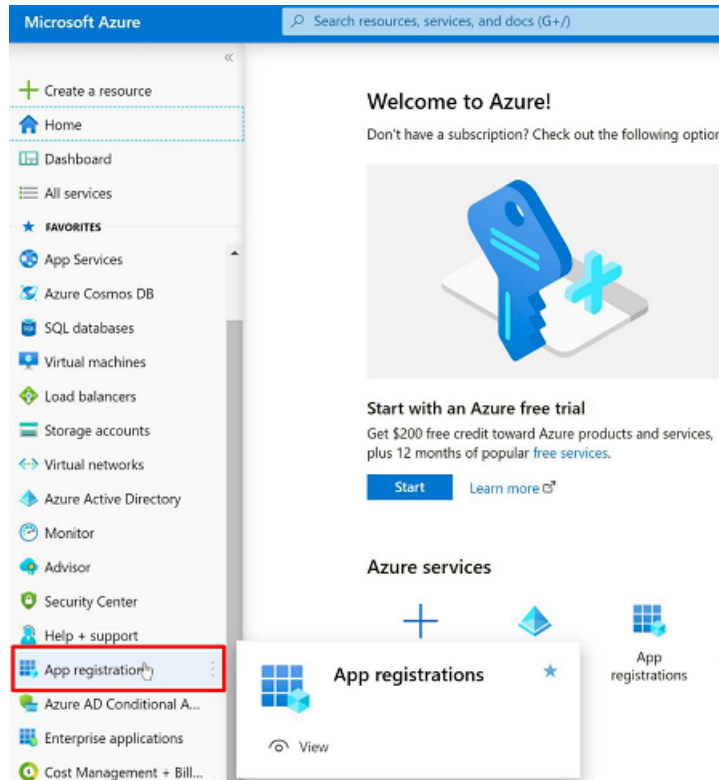
The administrator from the customer's side can then configure the OneDrive for Business collector. This collector lets customers archive the OneDrive files and folders of their configured users in the Veritas Alta Archiving.

Registering a Microsoft Azure App for OneDrive for Business Collector

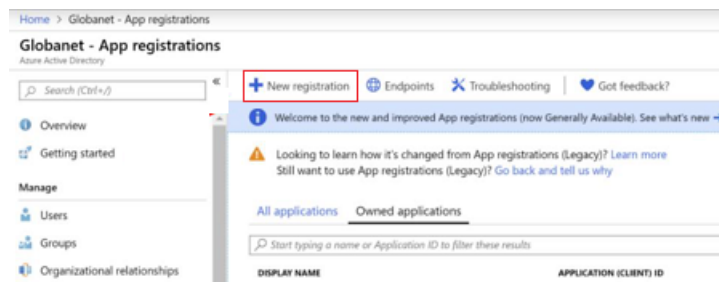
You need to create a OneDrive for Business App to use OneDrive for Business Collector. After you create this app, you get the Azure Tenant ID, Azure Client ID, and Azure Client Secret. These details are required for OneDrive for Business collector configuration.

To create a Microsoft Azure App for OneDrive for Business Collector

- 1 Access the [Microsoft Azure Portal](#) using the O365 (Global Admin) credentials.
- 2 In the left navigation pane, select **App registrations**.



- 3 Click **+ New registration**.



4 Provide a unique application name.

Ask the Veritas support team to provide the **Redirect URI** (along with the certificate) that you require while performing step **step 7**.

Under **Redirect URI (optional)**, select **Web** and enter the Redirect URI provided by the Veritas support team. Veritas support provides this complete URL.

Register an application

*** Name**

The user-facing display name for this application (this can be changed later).

Sample Application ✓

Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Globanet)
- ☐ Accounts in any organizational directory
- ☐ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web ✓

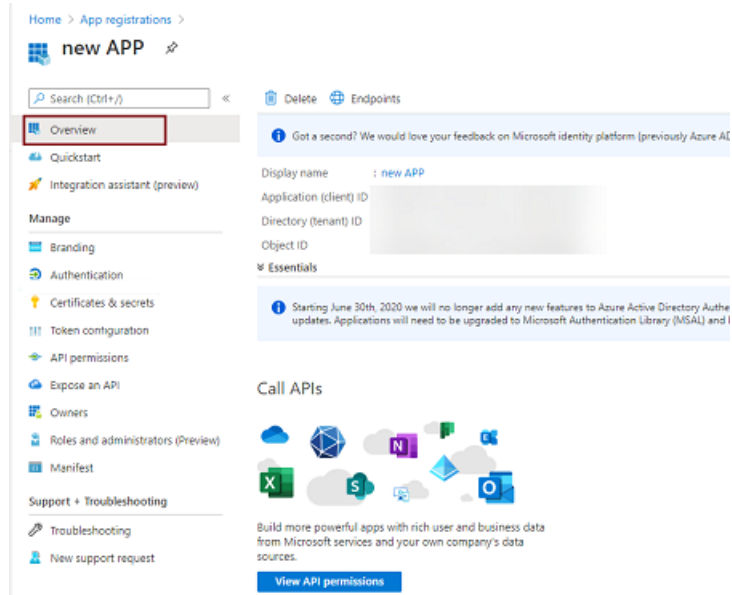
By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

5 Click **Register**.

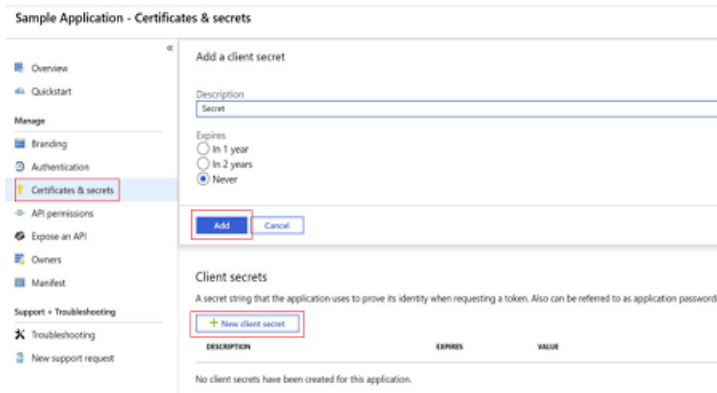
- 6 On the **Overview** page, search and note down the **Azure Tenant ID**, the **Azure Client ID**.

Note down these IDs as these are required for configuring the OneDrive for Business source in Archive Collectors.

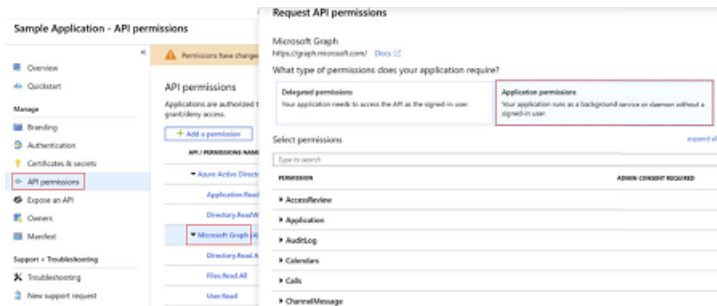


- 7 In the left navigation pane, select **Certificates & secrets**, do the following:
 - Click **Upload certificate** to upload the certificate that is provided by Veritas.
 - Click **New client secret**, provide a description, specify a duration, and click **Add**.

Note down the **Azure Client Secret** immediately as this secret value is required for configuring the OneDrive for Business source in Archive Collectors.

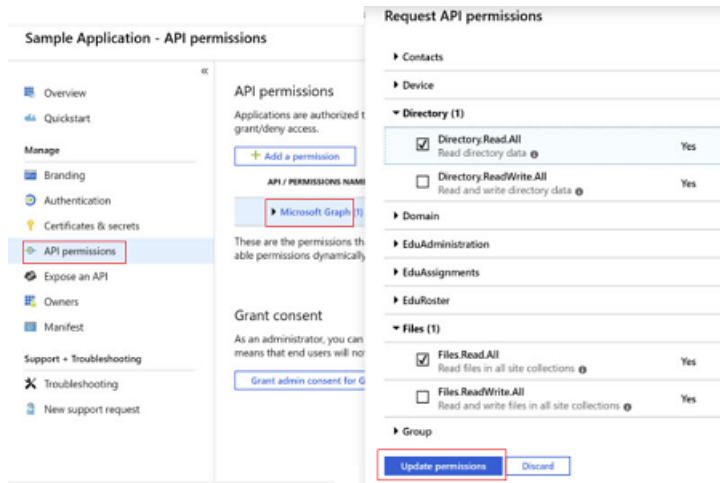


- 8 In the left navigation pane, select **API permissions**.
- 9 Click **Microsoft Graph**, and in the opened pane select **Application permissions**.



- 10 Select the following permissions:
 - Files: Files.Read.All
 - Directory: Directory.Read.All
 - User: User.Read.All
 - Applications: Applications.Read.All
 - Applications: Applications.ReadWrite.All
This permission is required only if the certificate has not been already uploaded to the Azure App.

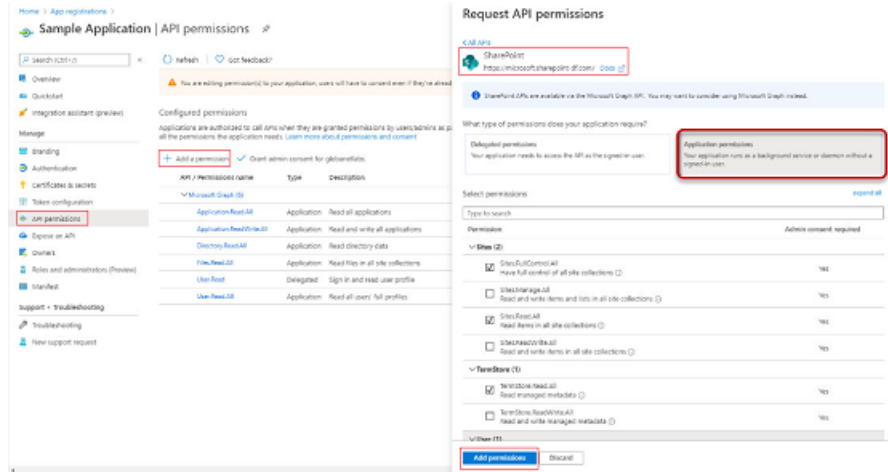
- 11 After you select all these check boxes, click **Update permissions**.



- 12 Navigate to the **API permissions** section, click **+ Add a permission**. Select **SharePoint > Application permissions**. Grant the following permissions:

- Sites: Sites.Read.All
- User: User.Read.All
- TermStore: TermStore.Read.All

13 After you select all these check boxes, click **Add permissions**.



14 After you select all these check boxes, click **Grant Admin Consent**.

Enabling the OneDrive for Business Archiving service for customer

On the Veritas Alta View Compliance and Governance Management Console console, only the super administrator can view the **Customer Service** tab. Therefore, to enable the OneDrive for Business Archiving service for customers, you must possess the super administrator role. Before you enable the OneDrive for Business Archiving service for a customer, ensure that the customer is added to the Veritas Alta Archiving. See *Creating the archive instance for a customer* in the Veritas Alta Archiving **Customer Administration Guide**.

To enable the OneDrive for Business Archiving service

- 1 In the left navigation tab, select **Customer Service**.
- 2 In the left navigation pane, click **Customers**.
- 3 On the **Customers** page, search for and select the customer for whom you want to enable this service.

Note: If the customer is new, you need to add the customer in Veritas Alta Archiving. See *Creating the archive instance for a customer* in the Veritas Alta Archiving Customer Administration Guide.

- 4 In the **Services** section, do the following:

- Ensure that, under **Primary Services**, the **Discovery Archive** service is already enabled for the customer. If this service is not enabled, select the **Discovery Archive** check box in the **Enabled** column to enable the service. Unless the **Discovery Archive** service is enabled, you cannot enable the **OneDrive for Business Archiving** secondary service for this customer.
 - Under **Secondary Services**, select the **OneDrive for Business Archiving** check box in the **Enabled** column.
- 5 Click **Save**.
 - 6 To verify if the OneDrive for Business Archiving service is enabled for the customer, login as a Customer Administrator.
 - 7 In the left navigation pane, select **Configuration > Services**.

Services

This page displays the services your company has purchased and been provisioned for. Please call your customer service representative if you want to add or change any of these services.

General Configuration

> **Primary Services**

Product	Enabled	# Users (Minimum)	# Users (Actual)
Personal Archive	<input checked="" type="checkbox"/>	20	20
Discovery Archive	<input checked="" type="checkbox"/>	20	52
Email Continuity	<input type="checkbox"/>	0	0
Advanced Supervision	<input type="checkbox"/>	0	0

Note: If a customer purchases Personal Archive without Discovery Archive, then they will be charged for the number of active archives rather than the explicit number of users assigned with...

>> **Secondary Services**

Product	Enabled	# Users (Minimum)	# Users (Actual)	Last Archived Date
Personal Archive for BlackBerry	<input checked="" type="checkbox"/>	0	20	Not Applicable
Exchange Folder Synchronization	<input checked="" type="checkbox"/>	20	52	Not Applicable
SharePoint Archiving	<input checked="" type="checkbox"/>	0	0	Not Applicable
Salesforce Chatter Archiving	<input checked="" type="checkbox"/>	0	0	Not Applicable
Box File Archiving	<input checked="" type="checkbox"/>	0	0	Not Applicable
Veritas Information Classifier	<input checked="" type="checkbox"/>	0	0	Not Applicable
Microsoft Teams	<input checked="" type="checkbox"/>	20	52	Not Applicable
Exchange Online Folder Synchronization	<input type="checkbox"/>	20	0	Not Applicable
Office 365 Personal Archive Connection	<input type="checkbox"/>	0	0	Not Applicable
Lync On-Premise Archiving	<input type="checkbox"/>	0	0	Not Applicable
Bloomberg Archiving	<input type="checkbox"/>	0	0	Not Applicable
OneDrive for Business	<input checked="" type="checkbox"/>	20	52	Not Applicable

- 8 Ensure that the **OneDrive for Business Archiving** service is displayed under the **Secondary Services** section.

Note: You cannot disable or enable this service from this page. To disable this service, select **Customer Service > Customers**. Select the customer and clear the check box of the OneDrive for Business Archiving service in the **Enabled** column.

Configuring OneDrive for Business Synchronization

You must have a Customer Administrator role to configure OneDrive for Business synchronization.

Customers enabled for MS Teams and OneDrive for Business secondary services can now configure OneDrive collectors by using the Alta Capture native user interface instead of a custom user interface. The simplified target configuration required for the Veritas Alta Archiving data collection is set up for customers, by default. The additional configuration workflow remains similar. Refer to the Alta Capture Collectors Configuration Guide.

The existing Teams and OneDrive connectors that were created in V6 cannot be migrated over to Alta Capture V7. However, The record of such connectors, such as previously run import jobs and data populated from the importers, remains available in the database.

To configure OneDrive for Business Synchronization

- 1 In the left navigation pane, select **Archive Collectors**.

The **Archive Collector** page appears.

Note: The **Archive Collectors** node appears in the left navigation pane, only when either of the following secondary services is selected:

- When the **Using Microsoft Exchange Online** check box is selected on the **User Management** page.
- When the **Bloomberg Archiving** check box is selected on the **Customer Details** section of the **Customer Service** tab.

- 2 Click **Add collector** to view available collector cards.

Note: At the time of adding the first collector, the **Add collector** button appears in the middle of the screen. If one or more collectors are already added, the **Add collector** option appears on the top right-hand corner.

If you select the collector that is not supported in Veritas Alta Archiving, the **Configure** button gets disabled. You cannot configure such collectors.

3 Select the **OneDrive for Business** card, and click **Configure**.

The **Add Importer** dialog box appears.

Name	Provide a unique name for this collector.
Description	Provide appropriate description to easily identify the collector.

4 Click **Next**.

The **Configuration Wizard** appears.

5 On the **Source** tab, specify the following information:

Application ID	Application ID is generated when you register an App on the Azure portal. After registering an App, you need to note down this ID. Use this Application ID for OneDrive for Business.
Application Secret Key	Use the application secret key value configured in the Microsoft Azure App under Certificates & secrets
X509 Certificate file	Click Change to browse to the X509 Certificate file of your OneDrive app.
X509 Certificate Password	Provide the X509 Certificate Password.

- 6 Click **Next** to specify the advanced configuration options and the attachment options.

Advanced Configuration Options

Subject Prefix	Specify the Subject Prefix that you want to add to the subject line of imported items. This is useful for organizing imported data especially when multiple sources share a common target.
Do not download data modified before	Select this check box to set the cut off date to capture data. Click the calendar icon to specify the cut off date.
Include original data as attachment	Select or clear this check box to include or exclude the original data as attachment.

Attachment Configuration

Ignore attachments	Select or clear this check box to exclude or include the attachments during the import job. Ignoring attachments enhance the connector performance. Each message will contain only information and the link of the excluded attachment.
Do not download files greater than...megabytes	Specify the cut off size of the attached files in megabytes. For example, if you have specified the cut off size of the attached files as 500 MB, and selected this check box, the application will not download the attachments that are more than 500 MB size.
Custom Message	Specify the text for the excluded attachments. For example: "Files {0} are not imported, because they are greater than {1} megabytes". {0} is used to add the name of the file and {1} is used to add the number of megabytes specified above.
Primary time zone	By default, user's time zone is displayed. If required, select your preferred time zone.
Import scheduler	Select the Do not schedule option to restrict Import Scheduler from importing OneDrive files. Select the Run every hour option to schedule hourly import job frequency. Select the Schedule time option to schedule the import job to be applied on a specific day and time.

- 7 Click **Next**. On the **Monitored Users** tab, provide the required information.
For more information on configuring monitored users for OneDrive, refer to the [Alta Capture Collectors Configuration Guide](#).
- 8 Click **Next** to open the **Target** tab.
For OneDrive for Business, the **Target** configuration is already populated. Optionally, you can also replace the Empty **TO** field by specifying an SMTP address in this field. For more information on configuring target for OneDrive, refer to the [Alta Capture Collectors Configuration Guide](#).
- 9 Click **Next**. On the **Settings** tab, configure the required parameter.
For more information on configuring settings for OneDrive, refer to the [Alta Capture Collectors Configuration Guide](#).
- 10 If the data is correct, click **Save and Finish**.
The OneDrive for Business archive collector appears on the **Archive collectors** page.

About Data Uploading

Configuring data uploading collection

You must have a Customer Administrator role to configure data uploading collection.

To configure data uploading collection

- 1 In the left navigation pane, select **Archive Collectors**.
The **Archive Collector** page appears.

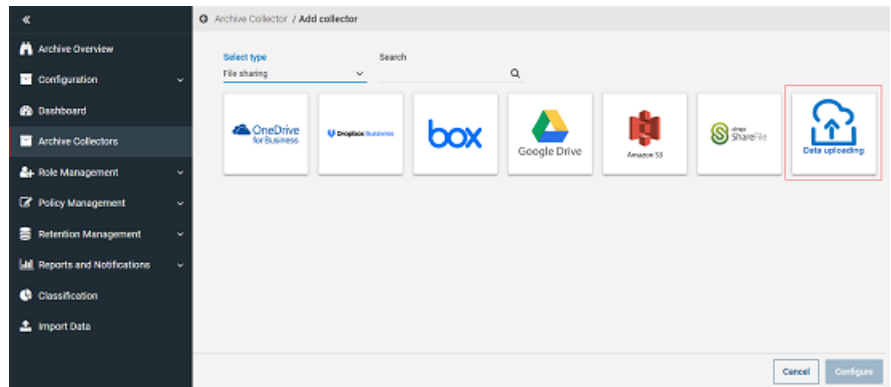
Note: The **Archive Collectors** node appears in the left navigation pane, only when either of the following secondary services is selected:

- When the **Using Microsoft Exchange Online** check box is selected on the **User Management** page.

- When the **Bloomberg Archiving** check box is selected on the **Customer Details** section of the **Customer Service** tab.

2 Click **Add collector** to view available collector cards.

Alternatively, in the **Select Type** drop-down, select **File Sharing**. The corresponding collector cards are displayed as shown in the sample image below:



3 Select the **Data uploading** card and click **Configure**.

4 On the **Add Importer** tab, specify the following:

Name	Provide a unique name for this file import collector.
Description	Provide appropriate description to easily identify the file import collector.

5 Click **Save**.

The **File Import** archive collector appears on the **Archive collectors** page.

Note: If the **File Import** archive collector is no more required, select this collector on the **Archive Collectors** page. Click the kebab icon (three vertical dots) on the archive collector card, and click **Delete**. The application prompts you to confirm that you want to perform the operation. Click **Yes**.

About Alta Capture Services Archiving

The existing Alta Capture customers can now use Veritas Alta Archiving to enable Alta Capture primary and secondary services, and configure archive collectors accordingly.

The customers who are enabled for only the Alta Capture primary service get lesser administration options when they login to the Veritas Alta View Compliance and Governance Management Console console.

- Under **Account Management**, they can create new users (who will be Administrators by default) and update the administrator contact details. These customers do not require **Journaling Address**.

While adding the customer account, on the **Accounts > Add Account** page, the **Admin** check box is available but not selected by default,. If you are creating the administrator account, select it manually. See the sample image below.

Add Account

First name: *

PDGAdmin

Last Name:

Type Last Name Here

Primary email address: *

PDGAdmin @ toggle.com

User Name: *

Type User Name Here

☒ Admin

☐ Auto Generate Password

Password: *

.....

Confirm Password: *

.....

Cancel

Save

- These administrators can do the following operations:
 - Configure archive collectors (importers) for the selected/enabled Capture secondary services under **Archive Collectors**.
 - Manage policies for Trusted Networks, Password Policy, and Authentication Management under **Policy Management**.

You can configure the following Alta Capture Secondary Services if you have subscribed for these services (purchased a user license).

Microsoft Teams via Export API | Microsoft Teams Meeting | Exchange Mailbox Graph | Microsoft Teams via Webhooks | Slack Alta eDiscovery | Bloomberg | IceChat | Twitter | OneDrive for Business | Box | Google Drive | Citrix Workspace & Sharefile | Dropbox Business | SharePoint | Amazon | EML | Blackberry | Yammer | UBS | XSLT/XML | EWS | Pivot | Text-Delimited | Crowd Compass | CellTrust |

Refinitiv | Symphony | Workplace from Facebook | Salesforce Chatter | Chatter
 Cipher Cloud | FXConnect | XIP | Yieldbroker | Webpage Capture | Redtail Speak
 | ServiceNow | RingCentral | Zoom Meetings | Zoom Meetings via Archiving API |
 Cisco Webex Teams | YouTube

Enabling Alta Capture Services for Archiving

On the Veritas Alta View Compliance and Governance Management Console console, only the super administrator can view the **Customer Service** tab. Therefore, to enable the Alta Capture services for customers, you must possess the super administrator role . Before you enable the Alta Capture services for a customer, ensure that the customer is added to the Veritas Alta Archiving. See *Creating the archive instance for a customer* in the Veritas Alta Archiving **Customer Administration Guide**.

To enable Alta Capture Services for Archiving

- 1 In the left navigation tab, select **Customer Service > Customers**.
- 2 On the **Customers** page, do any of the following:
 - If the customer is new, click **Add Customer** and specify the required details. See *Creating the archive instance for a customer* in the Veritas Alta Archiving Customer Administration Guide.

Note: The customers who are enabled for the Alta Capture services only can see lesser Administration options when they login to the Veritas Alta View Compliance and Governance Management Console console. Such customers do not require **Journaling Address**. In addition, while adding the customer account, on the **Accounts > Add Account** page, the **Admin** check box is selected, but remains disabled.

- If the customer already exists, search for and select the customer for whom you want to enable this service.
- 3 In the **Services** section, do the following as shown in the sample image below.

Services

Primary Services

Product	Enabled	#Users (Min)	Add #Users (Min)
Personal Archive	<input type="checkbox"/>	0	
eDiscovery	<input type="checkbox"/>	0	
Email Continuity	<input type="checkbox"/>	0	
Surveillance	<input type="checkbox"/>	0	
Capture	<input type="checkbox"/>	0	

Secondary Services

Product
Exchange Folder Synchronization
Exchange Online Folder Synchroniza
Office 365 Personal Archive Collecti
Classification
Bloomberg Archiving

Note: If a customer purchases Personal Archive without eDiscovery, then they will be charged for the number of active archives rather than the exp

Capture Secondary Services

Product	Enabled	#Users (Min)
EWS	<input type="checkbox"/>	0
XIP	<input type="checkbox"/>	0
Crowd Compass	<input type="checkbox"/>	0
EML	<input type="checkbox"/>	0
Exchange Mailbox Graph	<input type="checkbox"/>	0

- Under **Primary Services**, select **Capture**.

Note: Unless the **Capture** option is enabled under primary services, you cannot enable the **Capture Secondary Services** secondary service for this customer.

- Under **Capture Secondary Services**, in the **Enabled** column, select the check box next to the service that you want to enable.

- Click **Save**.
- To verify if the selected Capture secondary services are enabled for the customer, in Veritas Alta View Compliance and Governance Management Console console, login as a Customer Administrator.
- In the left navigation pane, select **Configuration > Services**.
- Ensure that the selected Capture secondary services are selected under the **Secondary Services** section.

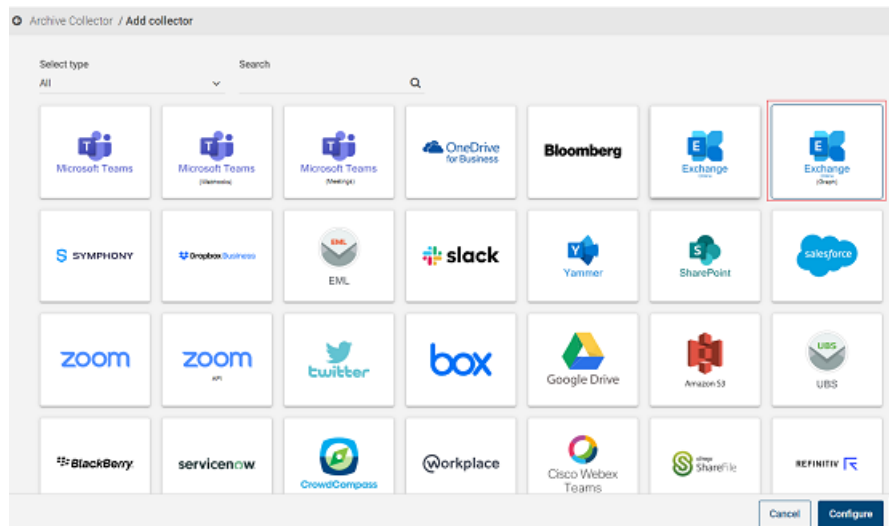
Note: You cannot disable or enable this service from this page. To disable this service, select **Customer Service > Customers**. Select the customer and clear the check box of the selected Capture secondary services in the **Enabled** column.

Configuring Capture Services for Archiving

You must have a Customer Administrator role to configure Capture services synchronization.

To configure Capture Services for Archiving

- 1 In the left navigation pane, select **Archive Collectors**.
The **Archive Collector** page appears.
- 2 Click **Add collector** to view available collector cards as shown in the sample image below.

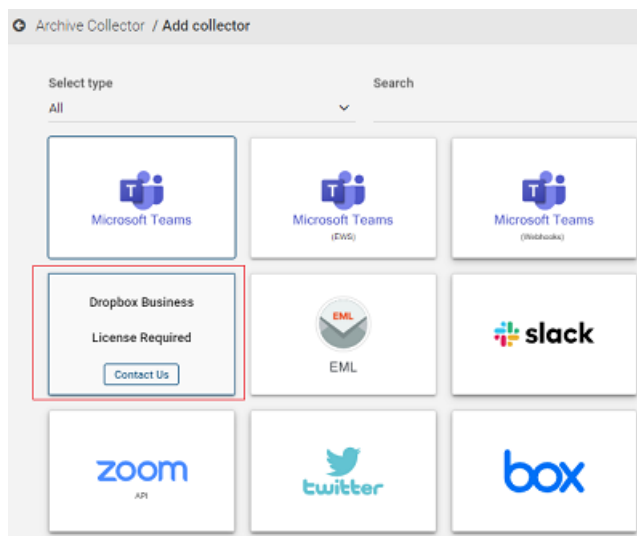


Note: At the time of adding a collector for the first time, the **Add collector** button appears in the middle of the screen. If one or more collectors are already added, the **Add collector** option appears on the top right-hand corner.

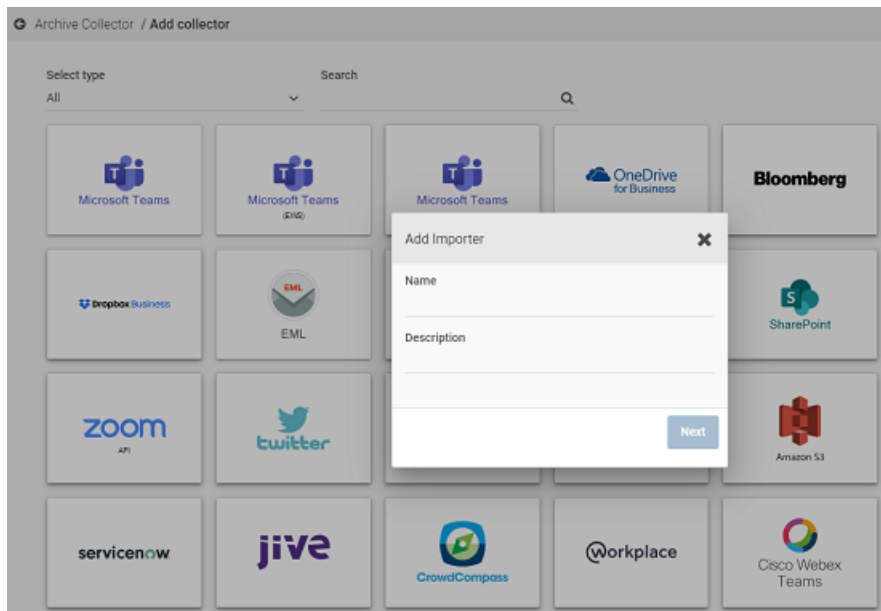
If you select the collector that is not supported in Veritas Alta Archiving, the **Configure** button gets disabled. You cannot configure such collectors.

3 Hover over the collector card that you want to configure.

You will be able to select the collector card if the customer has purchased the software license for this service. If the customer has not purchased the software license for this service, after hover over, the card flips and informs that the software license is required to add a collector.



- 4 Select the collector that you want to configure, and click **Configure**.
The **Add Importer** dialog box appears.



- 5 Enter a unique name and description for the archive collector (importer), and click **Next**.

The application redirects you to the Alta Capture portal. On the Alta Capture portal, when you attempt to configure the archive collector of every secondary service for the first time, a software license agreement appears. After that, when you add another archive collector of the same secondary service, the application does not show the software license agreement. The sample software license agreement image is shown below.



- 6 Scroll down to read the software license agreement carefully and accept the agreement to proceed to the configuration wizard for this archive collector (importer).

Note: The configuration wizard fields vary with the archive collector (importer) you have selected.

- 7 Provide the configuration details in the configuration wizard.

Note: Refer to the [Capture Collectors Configuration Guide](#) to understand configuration fields of corresponding archive collectors (importers) and complete the configuration steps.

After successful configuration, the archive collector appears in the Veritas Alta View Compliance and Governance Management Console console.

- 8 On the Veritas Alta View Compliance and Governance Management Console console, select **Archive Collectors**.

The application displays the successfully configured archive collector of the selected Capture service.

- 9 To update the configuration of selected Capture specific archive collector, click the kebab icon (three vertical dots) on the archive collector card, and click **Manage**.

The application navigates you to the configuration wizard. Modify the details and save the configuration.

- 10 To delete the selected Capture specific archive collector, click the kebab icon (three vertical dots) on the archive collector card, and click **Delete**.

Managing Roles and Permissions

This chapter includes the following topics:

- [About Role Management](#)
- [Editing the built-in administrator roles](#)
- [Creating custom administrator roles](#)
- [Assigning administrator roles to an archive account](#)
- [Assigning the reviewer role to an archive account](#)
- [Assigning several archive accounts for monitoring](#)

About Role Management

From the **Role Management** section, you can customize permissions for the archive administrator roles for your organization. You can also assign these roles to archive accounts within your organization.

You can perform the following tasks from this section:

- Edit permissions for built-in administrator roles.
- Create and edit permission for custom administrator roles.
- Assign roles to archive accounts.

Additionally, from the **Role Management** page you can view the built-in and custom administrator roles that are currently in use. The number that appears next to each administrator role indicates the number of archive accounts that have that role assigned.

Editing the built-in administrator roles

Veritas Alta View Compliance and Governance Management Console includes a set of built-in administrator roles to assign to archive accounts. By default, each role has a different set of permissions granted. You can edit these roles by customizing the permissions that are granted to each role.

The built-in administrator roles include:

- Account manager — manages users, aliases, settings, and passwords
- Role manager — configures administrator roles and permissions for archive accounts
- Policy manager — specifies archiving options and settings
- Retention manager — specifies archive retention policies and settings
- Continuity manager — manages email continuity feature (only available if your organization subscribes to the email continuity service)
- Alta eDiscovery Administrator — configures and manages Veritas Alta eDiscovery usage
- System administrator — oversees all Alta Personal Archive accounts including other administrators
- Archive collections manager — configures and manages archiving from third-party content sources

Note: You cannot edit the permissions for the System administrator roles. You can only edit **Share Export**, **Download Export**, and **Privilege Delete** permissions for the Alta eDiscovery Administrator role.

To edit the built-in administrator roles

- 1 In the left navigation pane, click **Role Management > Administration Roles**.
- 2 In the **Built-in Roles** section, click the expand icon next to the role for which you want to edit the permissions.

Note: You cannot remove the *Archive Overview* permission.

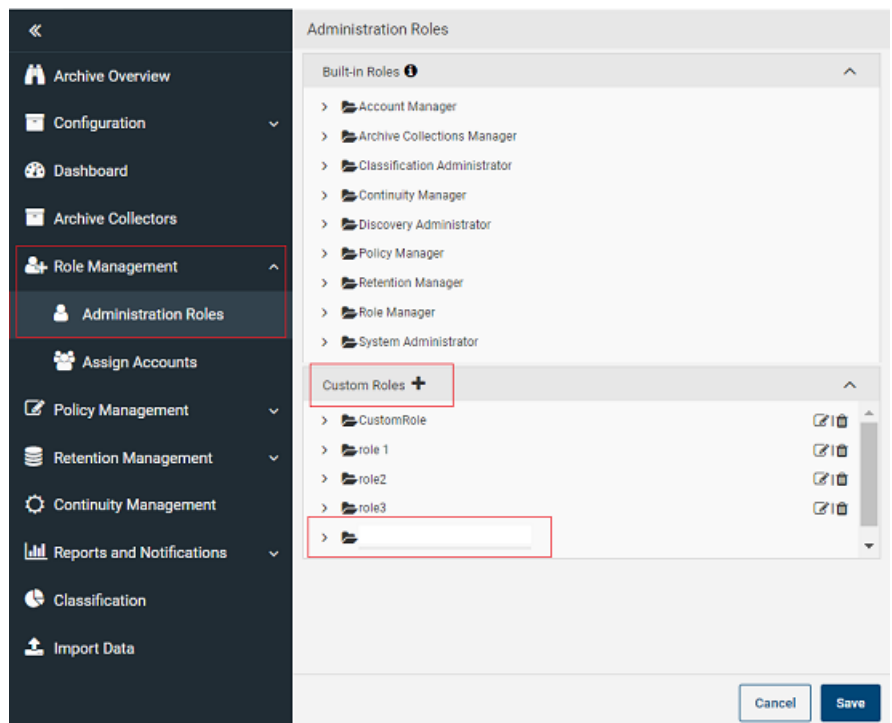
- 3 Select or clear the check boxes next to the permissions you want to add or remove for the selected role.
- 4 Click **Save**.

Creating custom administrator roles

If required, you can also create custom administrator roles to assign to archive accounts. After you create a custom administrator role, you can edit the permissions for the role.

To create custom administrator roles

- 1 In the left navigation pane, click **Role Management > Administration Roles**.
- 2 In the **Custom Roles** section, click the plus icon.

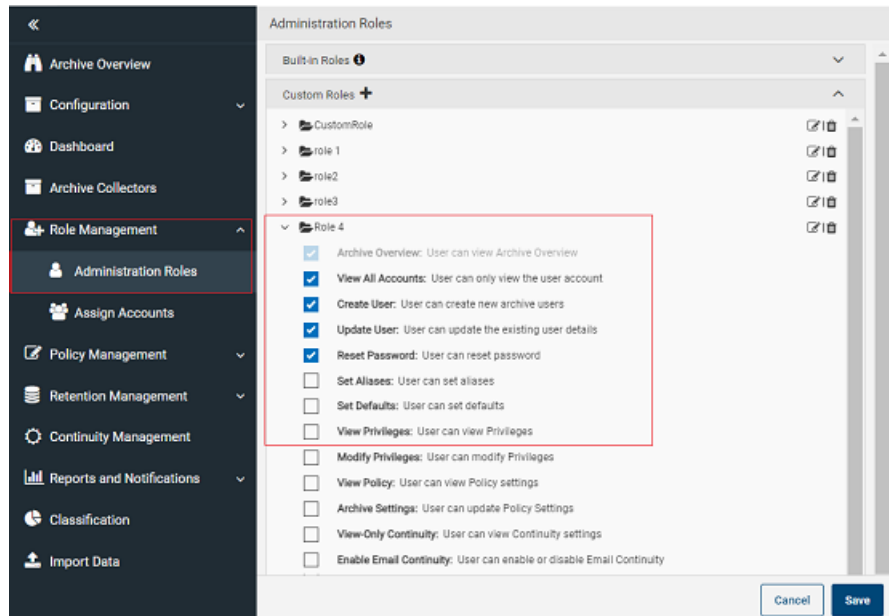


- 3 In the blank text box, enter a name for the custom administrator role.

Note: After creating the custom roles, you can do the following:

- To rename the custom role you have created, click the **Edit** icon in the corresponding row.
- To delete the custom role that is no more required, click the **Delete** icon in the corresponding row.

- 4 Click the expand icon next to the role added for which you want to configure the permissions.



- 5 Select the check box next to the permissions you want to add for the custom role.
- 6 Click **Save**.

Assigning administrator roles to an archive account

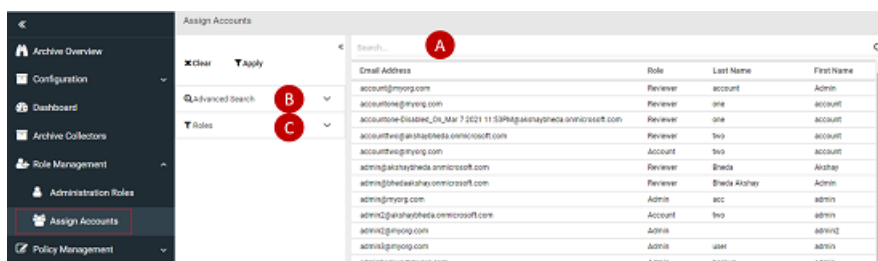
By default, all archive accounts that you create in Veritas Alta View Compliance and Governance Management Console are automatically assigned the Accounts role. If required, you can assign the built-in administrator roles or custom administrator roles you created to an archive account.

To assign administrator roles to an archive account

- 1 In the left navigation pane, select **Role Management > Assign Accounts**.
- 2 Search for and select the archive account to which you want to assign the administrator role.

The application displays the **Role Change** page.

Note: To search for the required archive account, you can use any of the following methods. The sample image for better understanding is given below.



A. Quick search: In the search field, enter the user name or email address that is associated with the archive account, and click the **Search** icon.

B. Advanced search: Under the **Advanced Search** section, specify the email address, last name, first name, or role, and then click **Apply**.

C. Roles-based search: Under the **Roles** section, select the role from the available options. The result appears in the right pane. You do not need to click **Apply**.

- 3 In the **Role** drop-down, select **Administrator**.
- 4 In the **Privilege** field, select the **Monitor All Accounts** check box to let the selected account view the archived messages of all other archive accounts.

Note: This option is only available if your organization subscribes to Veritas Alta eDiscovery.

- Under **Built-in Roles** section, select one or more built-in administrator roles or custom a new role you want to assign. (See “[Creating custom administrator roles](#)” on page 129.)
- Click **Save**.

Role Change - admin@akshaybheida.onmicrosoft.com

Role: **Reviewer**

Privilege: ☐ Monitor All Accounts ☐ Disable Preview Emails ☒ **Discovery Reviewer**

Discovery Reviewer Privileges

- **Manage Review Status:** User can add, edit, and delete Case Review Status.
- **Manage Case Status:** User can add, remove, and modify Case Status.
- **Manage Search Searches:** User can make changes to search searches added under Case.
- **Review Email:** User can review status to email.
- **View Case Logs and Reports:** User can view logs and save reports.
- **Manage Reviews:** User can manage reviews/permissions.

Below Privileges are subject to Case level. Administrator user needs to assign these privileges to discovery reviewers to perform the respective actions in those cases.

Note: Setting the user as Reviewer will enable Advanced Discovery access for that user.

Accounts To Monitor

[Add/Remove Monitored Accounts](#) [Import](#)

Accounts to Monitor	Never Expires	Expiration	Action
account@myorg.com Admin - account	<input checked="" type="checkbox"/>		
accountone@myorg.com account - one	<input checked="" type="checkbox"/>		
accountone@akshaybheida.onmicrosoft.com account - one	<input checked="" type="checkbox"/>		

Page 1 of 1 Items per page: 20 1 - 3 of 3

[Cancel](#) [Save](#)

After you select the **Reviewer** option, the **Privilege** field displays the following check boxes. Do the following as required.

- **Discovery Reviewer:** This option is selected by default. When you define a user as a reviewer, this user gets access to the Alta eDiscovery application. The *Discovery Reviewer Privileges* section lists all the privileges for your reference. These privileges vary with the case levels. As an administrator, you can assign these privileges to the Discovery Reviewers to perform various actions while reviewing the cases.
- **Monitor All Accounts:** Select this option if you want to let the selected account view the archived messages of all other archive accounts. If you select this option, you do not need to complete the steps in the **Accounts to Monitor** section.
- **Disable Preview Emails:** Select this option if you want to prohibit the reviewer to preview content of emails.

- 4 Under **Accounts to Monitor**, perform the following steps as required.
- 5 To add or remove monitored accounts, click **Add/Remove Monitored Accounts**. In the **Add/Remove Accounts** window, search for and select the archive accounts that you want the reviewer to monitor. Click **Save**.
- 6 To specify expiry of a reviewer privilege of monitored accounts, clear the check box in the **Never Expires** column. Then, in the **Expiration** column, click the **Calendar** icon and select the date that you want the reviewer privilege to expire.

- 7 To remove the previously added monitored accounts, click the **Delete** icon in the corresponding rows.
- 8 On the **Role Change** page, click **Save**.

Assigning several archive accounts for monitoring

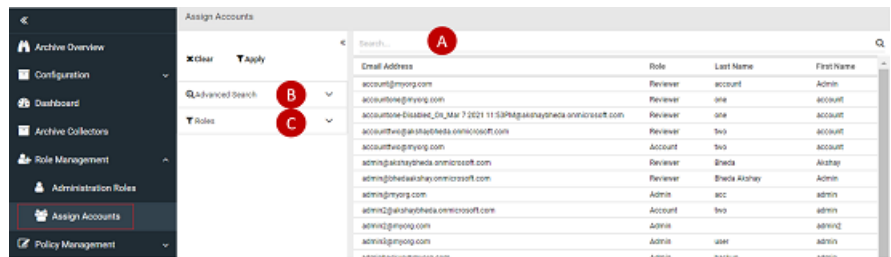
You can simultaneously assign multiple archive accounts to the reviewer by importing the .CSV file. The .CSV file is not directly available. Instead, you can download the sample .XLS file and save it as .CSV. The sample .XLS file is available when you click Import under the Accounts to Monitor section.

To assign the reviewer role to an archive account

- 1 In the left navigation pane, select **Role Management** > **Assign Accounts**.
- 2 Search for and select the archive account to which you want to assign the administrator role.

The application displays the **Role Change** page.

Note: To search for the required archive account, you can use any of the following methods. The sample image for better understanding is given below.



- A. Quick search:** In the search field, enter the user name or email address that is associated with the archive account, and click the **Search** icon.
- B. Advanced search:** Under the **Advanced Search** section, specify the email address, last name, first name, or role, and then click **Apply**.
- C. Roles-based search:** Under the **Roles** section, select the role from the available options. The result appears in the right pane. You do not need to click **Apply**.

- 3** In the **Role** drop-down, select **Reviewer**.

Refer to the sample image below.

Role Change - admin@akshaybhedas.onmicrosoft.com

Role: **Reviewer**

Privilege: ☐ Monitor All Accounts ☐ Disable Preview Emails ☒ **Discovery Reviewer**

Discovery Reviewer Privileges

- **Manage Review Status:** User can add, edit, remove and modify Case Review Status.
- **Manage Case Status:** User can add, remove and modify Case Status.
- **Manage Search Searches:** User can make changes to saved searches added under Case.
- **Review Email:** User can review status to email.
- **View Case Logs and Reports:** User can view logs and save reports.
- **Manage Reviews:** User can manage reviews/permissions.

Above Privileges are subjected to Case level. Administrator user needs to assign these privileges to discovery reviewers to perform the respective actions in those cases.
Note: Setting the user as Reviewer will enable Advanced Discovery access for that user.

Accounts To Monitor

+ Add/Remove Monitored Accounts **Import** Search...

Accounts to Monitor	Never Expires	Expiration	Action
account@myorg.com Admin - account	<input checked="" type="checkbox"/>		
accountone@myorg.com account - one	<input checked="" type="checkbox"/>		
accountone@akshaybhedas.onmicrosoft.com account - one	<input checked="" type="checkbox"/>		

Page 1 of 1 Items per page: 20 1 - 3 of 3

Cancel **Save**

After you select the **Reviewer** option, the **Privilege** field displays the following check boxes. Do the following as required.

- **Discovery Reviewer:** This option is selected by default. When you define a user as a reviewer, this user gets access to the Alta eDiscovery application. The *Discovery Reviewer Privileges* section lists all the privileges for your reference. These privileges vary with the case levels. As an administrator, you can assign these privileges to the Discovery Reviewers to perform various actions while reviewing the cases.
- **Monitor All Accounts:** Select this option if you want to let the selected account view the archived messages of all other archive accounts. If you select this option, you do not need to complete the steps in the **Accounts to Monitor** section.
- **Disable Preview Emails:** Select this option if you want to prohibit the reviewer to preview content of emails.

4 Under **Accounts to Monitor**, click **Import**.

The **Import Monitor Accounts** window appears.

Import Monitor Accounts

Account Name: **accounttwo@akshaybhedas.onmicrosoft.com**
(Please choose ".csv" file format) (Sample ".xls" file)

File Location: **Choose File** **No file chosen**

Import

Before you import the file, understand and perform the following steps.

- 5 Click **Sample ".xls" file** to download the sample file. The sample file available to download is the .XLS file. Save this file as .CSV to provide email addresses of archive accounts you want to assign to reviewers for monitoring purpose.
- 6 Retain (do not delete) the **PrimaryEmailAddress** column heading in the .CSV file.
- 7 Delete all the text (including these instructions) below the **PrimaryEmailAddress** column heading.
- 8 Use only primary email addresses of the archive accounts.
- 9 After the .CSV file (in which you have mentioned the primary email addresses of the archive accounts that you want to assign in bulk for monitoring) is ready and saved, click **Browse** and select it.
- 10 Click **Import** in the **Import Monitor Accounts** window.
- 11 On the **Role Change** page, click **Save**.

Managing Policies

This chapter includes the following topics:

- [About Policy Management](#)
- [Configuring archive options](#)
- [Enabling and disabling account archiving](#)
- [Configuring an advanced password policy](#)
- [Configuring trusted networks for Veritas Alta Archiving access](#)
- [Managing Custom Headers](#)
- [Managing Discard Rules](#)

About Policy Management

You can perform the following tasks from the **Policy Management** section:

- Configure various archiving options.
- Disable archiving for selected archive accounts.
- Configure an advanced policy for passwords.
- Configure trusted networks for Veritas Alta Archiving access.

Note: From the **Policy Management** section the administrators with the required privileges can also configure authentication management for Veritas Alta Archiving.

See [“Configuring the Veritas Alta Archiving authentication service”](#) on page 148.

Configuring archive options

The **Archive Options** page under the **Policy Management** node lets you configure the following options for Veritas Alta Archiving:

- **Email Direction** — determines whether inbound, outbound, and internal messages are archived in Veritas Alta Archiving.
- **Active Folder Synchronization** — determines whether Outlook folder synchronization is enabled, for those organizations that subscribe to the Folder Sync service.
- **Veritas Alta Archiving Actions** — determines whether Alta Personal Archive users can send, reply, forward, print, or save messages.
- **Time Zone and Date Format** — sets the default time zone and date format for Veritas Alta Archiving.
- **Mobile Web Access** — determines whether Mobile Web Access is enabled or disabled, and controls related settings.
- **Privilege Delete** — determines whether Alta eDiscovery Administrator is enabled to permanently delete emails in Alta eDiscovery.

To configure archive options

- 1 In the left navigation pane, select **Policy Management > Archive Options**.
- 2 Click **Edit**.
- 3 Under **Email Direction**, select the check box for one or more of the following message types:
 - **Inbound Emails** — archive the email messages that are sent to email addresses within your domain from outside your domain.
 - **Outbound Emails** — archive the email messages that are sent to email addresses outside your domain from inside your domain.
 - **Internal Emails** — archive the email messages that are sent between email addresses within your domain.

Note: By default, all message types are selected.

- 4 Under **Active Folder Synchronization**, choose whether folder synchronization is **Enabled** or **Disabled**.

Note: This feature uses the Folder Sync application to synchronize Microsoft Outlook folders to Veritas Alta Archiving. The option is only available if your organization subscribes to the service and has the Folder Sync application configured.

- 5 Under **Veritas Alta Archiving Actions**, select the check boxes for the actions that you want to enable in Alta Personal Archive:

- **Send, Reply and Forward** — enables the options to send, reply, and forward messages in Alta Personal Archive.
- **Save** — enables the option to save archived messages to your computer from Alta Personal Archive.
- **Print** — enables the option to print archived messages from Alta Personal Archive.

- 6 Under **Time Zone and Date Format**, configure the following options:

- **Personal Time Zone** — the time zone for your archive account.
- **Default Company Time Zone** — the default time zone for your organization.
- **Date Format** — the default date format for your organization.

- 7 Under **Mobile Web Access**, select the required options:

- Select the **Status** option as **Enabled** or **Disabled** to determine whether Mobile Web Access is enabled or disabled for all archive accounts that have Mobile Web Access permission.

Note: An archive account must have Mobile Web Access permission before the user can use this feature.

See [“Editing Mobile Web Access permission for existing archive accounts”](#) on page 63.

- Select **Automatically grant Mobile Web Access permission for new accounts** if you want Veritas Alta Archiving to grant Mobile Web Access permission for new archive accounts when you create them manually in Veritas Alta View Compliance and Governance Management Console.

Note: This option does not apply to archive accounts that are created through CloudLink or Exchange Online Sync.

- Select **Send, Reply and Forward from Mobile Web Access** to enable the **Send**, **Reply**, and **Forward** options in Mobile Web Access.
- 8** Under **Privilege Delete**, do the following as required:
- Toggle the switch adjacent to **Alta eDiscovery** to choose whether to enable or disable the delete emails permission for Alta eDiscovery users.
 - Toggle the switch adjacent to **Personal Archive** to choose whether to enable or disable the delete emails permission for Personal Archive users.

Note: To use this feature, the Alta eDiscovery Administrator requires **Privilege Delete** permission. You can set **Privilege Delete** for the Alta eDiscovery Administrator role. See [“Editing the built-in administrator roles”](#) on page 128.

- 9** Under **View Delegate Folder Structure**, choose whether the ability to view delegate archive folders in PA is **Enabled** or **Disabled**.

Note: To use this feature, Folder Sync must be enabled for the account and delegate archives. For delegate archives with Folder Sync enabled, user would be able to see the folder structure on selection in Alta Personal Archive.

If you have over 4,000 synchronized monitored and delegate archive folders, the loading time in the **Active Folders** tab might take up to five minutes.

The delegate archive folder structure keeps synchronizing even though the **View Delegate Folder Structure** option in manage is enabled or disabled. When the delegate account users logs in to Alta Personal Archive, they can view their folder structure.

- 10 Under **Export to Azure private storage location**, if the status is set to *Enabled*, the **Create new Storage Account** button is displayed. Click **Create new Storage Account** to allow a customer to create an Azure storage account during exporting items from Alta eDiscovery.

Note: This is an on-demand feature and is enabled for the customers only after their request for it. It allows customers to create their private storage account and get a storage account SAS URL to work with their storage account. You can configure the status (*Enabled* or *Disabled*) and the retention period of this feature from the database only. If the status is set to *Disabled*, you cannot see the **Create new Storage Account** button.

You can generate only one Azure storage account per customer. After creating a storage account, the **Create new Storage Account** button gets disabled. If you hover over the disabled button, the *Storage account is already created* tooltip is displayed.

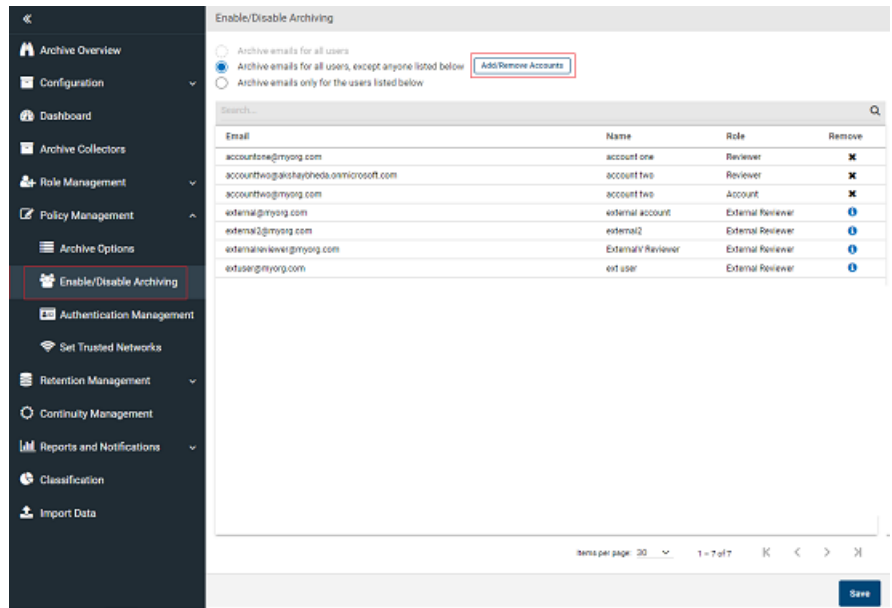
- 11 Click **Save**.

Enabling and disabling account archiving

By default, the messages for all archive accounts are automatically journaled to Veritas Alta Archiving. From the **Enable/Disable Archiving** page, you can disable archiving for certain archive accounts. However, you cannot disable the external users as archiving for these users is disabled by default.

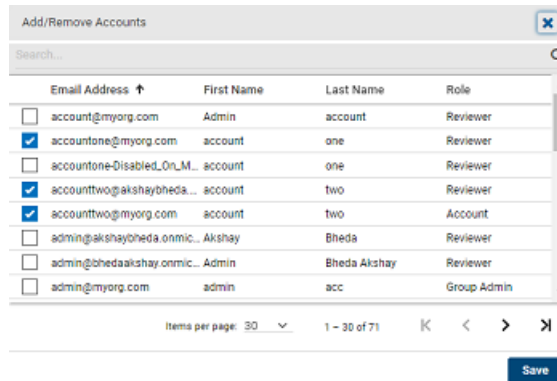
To disable account archiving

- 1 In the left navigation pane, select **Policy Management > Enable/Disable Archiving**.



- 2 Select one of the following archiving options:
 - **Archive emails for all users** — archives the email messages for all archive accounts.
 - **Archive emails for all users, except anyone listed below** — archives the email messages for all archive accounts except the ones that you select.
 - **Archive emails only for the users listed below** — only archives email messages for the archive accounts that you select.
- 3 If required, click **Add/Remove Accounts** to select the archive accounts that you want to exclude or include for archiving.

- 4 In the **Add/Remove Accounts** window, search for and select the archive accounts that you want to exclude or include for archiving.



The screenshot shows the 'Add/Remove Accounts' window. It has a search bar at the top. Below it is a table with columns: Email Address, First Name, Last Name, and Role. There are checkboxes in the first column for each row. The table contains 8 rows of account information. At the bottom, there is a 'Save' button.

	Email Address ↑	First Name	Last Name	Role
<input type="checkbox"/>	account@myorg.com	Admin	account	Reviewer
<input checked="" type="checkbox"/>	accountone@myorg.com	account	one	Reviewer
<input type="checkbox"/>	accountone-Disabled_On_M...	account	one	Reviewer
<input checked="" type="checkbox"/>	accounttwo@akshaybheda...	account	two	Reviewer
<input checked="" type="checkbox"/>	accounttwo@myorg.com	account	two	Account
<input type="checkbox"/>	admin@akshaybheda.onmic...	Akshay	Bheda	Reviewer
<input type="checkbox"/>	admin@bhedaakshay.onmic...	Admin	Bheda Akshay	Reviewer
<input type="checkbox"/>	admin@myorg.com	admin	acc	Group Admin

Items per page: 30 1 - 30 of 71

Save

- 5 Click **Save** to close the **Add/Remove Accounts** window.
- 6 On the **Enable/Disable Archiving** page, click **Save**.

Configuring an advanced password policy

The default password policy for Veritas Alta Archiving requires that all account passwords be at least eight characters long. Additionally, all passwords must contain at least two of the following character types:

- A number between 0 and 9
- A lowercase letter
- An uppercase letter
- A non-alphanumeric character

From the **Password Policy** page, you can configure an advanced password policy for all archive accounts.

Note: The **Password Policy** page is not available if you have configured Single Sign-On for account authentication.

To configure an advanced password policy

- 1 In the left navigation pane, under **Policy Management**, click **Password Policy**.
- 2 In the **Password Policy** section, under **Advanced Password Policy**, select the requirements you want to include in your password policy.

Refer to the following table for more information:

Enforce Password History	Select this requirement and enter a value for the number of past passwords that you want stored. Users cannot change their current password to a stored password.
Maximum Password Age	Select this requirement and enter a value for the number of days between required password changes.
Minimum Password Age	Select this requirement and enter a value for the minimum of days between password changes. This option controls how often users can change their passwords.
Minimum Password Length	Select this requirement and enter a value for the minimum password length.
Password Must Meet Complexity Requirements	<p>Select this requirement and choose up to three of the following password complexity requirements:</p> <ul style="list-style-type: none">■ Use base-10 digits characters in password — requires at least one number between 0 and 9■ Use lowercase characters in password — requires at least one lowercase letter■ Use non-alphanumeric characters in password — requires at least one symbol■ Use uppercase characters in password — requires at least one uppercase letter
Prevent Username in Passwords	Select this requirement to prevent users from using their user name in their password.

- 3 If required, select **Enforce the password policies for all users** if you want to require all users to change their passwords during their next login.

Note: If you select this option, all users must change their password during their next login even if the password meets the specified requirements. If you do not select this option, users do not have to change their password until it expires even if the password does not meet the specified requirements.

- 4 Click **Save**.

Configuring trusted networks for Veritas Alta Archiving access

By default, users can access Veritas Alta Archiving from any Internet Protocol (IP) address. From the **Set Trusted Networks** page, you can restrict access to specific IP address range.

To configure trusted networks for Veritas Alta Archiving access

- 1 In the left navigation pane, select **Policy Management > Set Trusted Networks**.

The **Add Trusted Network** window appears.



- 2 In the **Starting** field, enter the starting IP address of the address range.
- 3 In the **Ending** field, enter the ending IP address of the address range.
- 4 Under **Select Application**, select the check box for the Veritas Alta Archiving products that you want access restricted.
- 5 Click **Save**.
- 6 To modify the trusted network, click the **Edit** icon in the corresponding rows. Modify the IP address range, and click **Save**.
- 7 To delete the trusted network, click the **Delete** icon in the corresponding rows.

Managing Custom Headers

A custom header is a title or a description that a user can customize to label specific review items. To add new custom headers and mark these headers as active or inactive, you must have access to the **Policy Management** page.

Note: You cannot edit or delete the custom header name and datatype values. However, you can activate the required custom headers and deactivate the headers that are no more required.

To add a new custom header

- 1 In the left navigation pane, select **Policy Management > Custom Header**.
- 2 Click **Add Row**.
- 3 In the newly added row, in the **Name** field, type a custom header title/description.

Note: This is a mandatory field. It can be an alphanumeric value and can contain space. You can use only dot(.) and hyphen(-) as special characters.

- 4 In the **Datatype** drop-down, specify if the data type is a number, a string, or a date.
- 5 Ensure that the **Active** check box is selected.

If the Active check box is selected, the custom header remains available for use. You cannot use the custom header if it is not Active.
- 6 Click **Save**.

The application prompts you to confirm that you want to perform the operation.
- 7 Click **Yes**.

Managing Discard Rules

A Discard Rule was previously referred as a Bypass Rule. A discard rule is an instruction that bypasses specific review items when the rule is active and applied. To add new discard rules and mark these rules as active or inactive, you must have access to the **Policy Management** page.

Note: You cannot edit or delete the discard rule. However, you can activate the required rules and deactivate the rules that are no more required.

To add a new discard rule

- 1 In the left navigation pane, select **Policy Management > Discard Rules**.
- 2 Click **Add Row**.

- 3 In the newly added row, specify the following details:

SenderAddress	Specify the value in the <i>name@example.com</i> format only.
RecipientAddress	Specify the value in the <i>name@example.com</i> format only.
Subject	Specify text, number, or an alphanumeric value. You can include spaces and special characters if required.
AttachmentType	Specify the type of attachment. If you do not explicitly specify the attachment type, the application considers all types of attachments in the rule.

- 4 Ensure that the **Active** check box is selected.

If the Active check box is selected, the discard rule remains available for use. You cannot use the discard rule if it is not Active.
- 5 Click **Save**.

The application prompts you to confirm that you want to perform the operation.
- 6 Click **Yes**.

Managing Authentication

This chapter includes the following topics:

- [Configuring the Veritas Alta Archiving authentication service](#)
- [Enabling the Authentication Settings permission for the Policy Manager role](#)
- [Assigning the Policy Manager role to an administrator](#)
- [Selecting an authentication method](#)
- [Uploading a token-signing certificate](#)
- [Validating the Identity Provider URL](#)
- [Activating single sign-on](#)

Configuring the Veritas Alta Archiving authentication service

This section describes how to configure the Veritas Alta Archiving authentication service to work with your Active Directory Federation Services (AD FS) environment.

Note: The Veritas Alta Archiving Compatibility List provides information about other single sign-on solutions and how to get assistance with configuring them.

[See the Veritas Alta Archiving Compatibility List](#)

After you configure the Veritas Alta Archiving authentication service and your AD FS environment, you can provide single sign-on access to Veritas Alta Personal Archive users.

Note: These instructions apply to the provision of single sign-on access for Alta Personal Archive users only. For assistance with the provision for Alta eDiscovery and Veritas Alta View Compliance and Governance Management Console, contact [Veritas Services & Support](#).

[Table 8-1](#) summarizes the steps to configure the Veritas Alta Archiving authentication service to work with your AD FS environment.

Table 8-1 Veritas Alta Archiving authentication service configuration

Step	Action	Reference
Step 1	In Veritas Alta View Compliance and Governance Management Console, enable the Authentication Settings permission for the Policy Manager role.	See “Enabling the Authentication Settings permission for the Policy Manager role” on page 149.
Step 2	Assign the Policy Manager role with the Authentication Settings permission enabled to an administrator.	See “Assigning the Policy Manager role to an administrator” on page 150.
Step 3	On the Authentication Management page, select AD FS as the authentication method for your organization.	See “Selecting an authentication method” on page 150.
Step 4	Upload the token-signing certificate that you generated from your AD FS environment.	See “Uploading a token-signing certificate” on page 153.
Step 5	Validate the Identity Provider URL for your organization.	See “Validating the Identity Provider URL” on page 154.
Step 6	Activate single sign-on for Alta Personal Archive users.	See “Activating single sign-on” on page 155.

Enabling the Authentication Settings permission for the Policy Manager role

The **Authentication Management** page in Veritas Alta View Compliance and Governance Management Console lets you configure the Veritas Alta Archiving authentication service. Only the administrators that have the **Authentication Settings** permission enabled can access the **Authentication Management** page.

By default, only the **System Administrator** role has the **Authentication Settings** permission enabled. If required, you can enable this permission for the **Policy Manager** role and assign the role to an administrator that is not a system administrator. Since the **Policy Manager** role has limited permissions, you can provide the **Authentication Settings** permission to an administrator without providing them the full system administrator permissions.

To enable the Authentication Settings permission for the Policy Manager role

- 1 In the left navigation pane, under **Role Management**, click **Administration Roles**.
- 2 In the **Built-in Roles** section, click **Policy Manager**, and then select **Authentication Settings**.
- 3 At the top of the **Administration Roles** page, click **Save**.

Assigning the Policy Manager role to an administrator

After you enable the Authentication Settings permission for the Policy Manager role, you can assign the role to the administrator that you want to manage the Veritas Alta Archiving authentication service.

Note: The administrator may need to log out and log back in to Veritas Alta View Compliance and Governance Management Console before they can access the **Authentication Management** page.

To assign the Policy Manager role to an administrator

- 1 In the left navigation pane, click **Assign Accounts**.
- 2 From the user list, select the administrator to which you want to assign the role.
- 3 On the **Role Change** page, select **Policy Manager**, and then click **Save** at the top of the page.

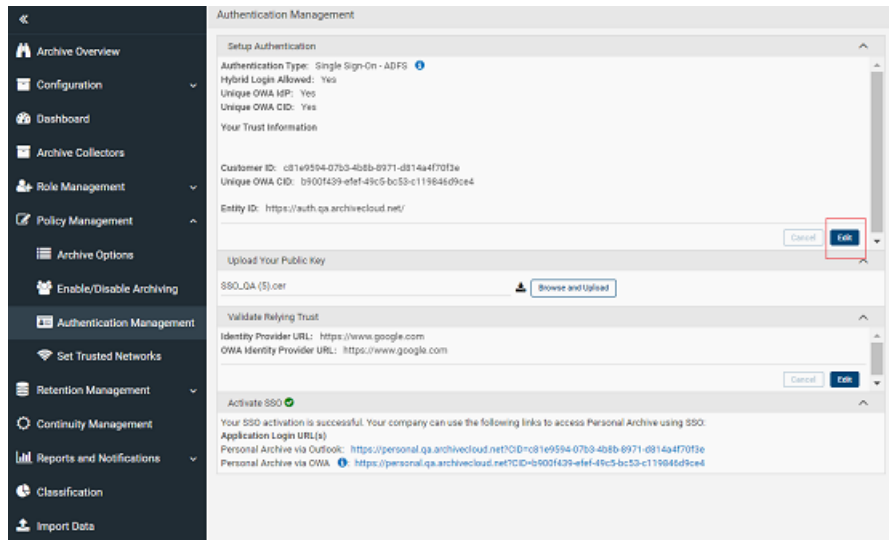
Selecting an authentication method

You can configure the Veritas Alta Archiving authentication service from the **Authentication Management** page. To begin the configuration process, you must select AD FS as the authentication method that you want to use for authenticating Alta Personal Archive users.

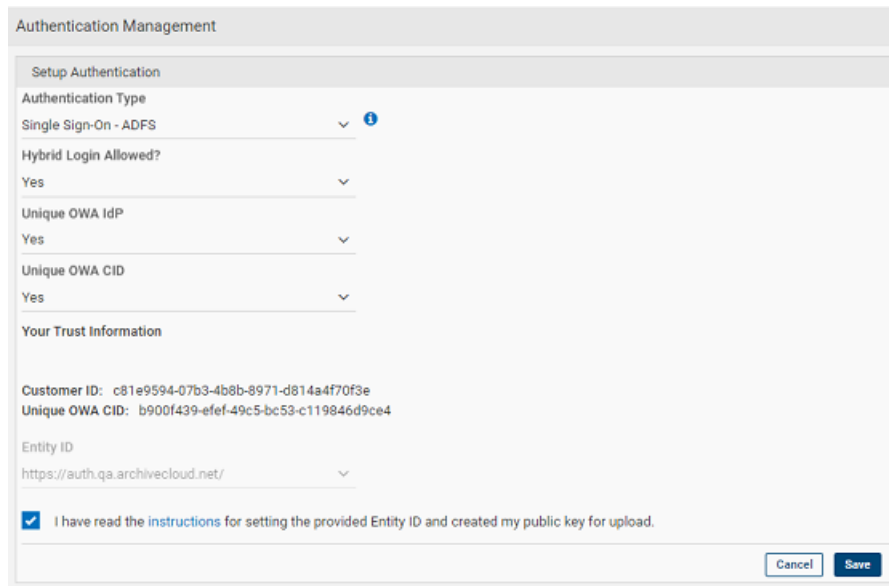
Note: The **Your Trust Information** section displays after you select AD FS as the authentication method that you want to use. You must use the value that is provided in the **Entity ID** field of this section when you configure your AD FS environment. The Entity ID varies based on the location of your organization. If you cannot find the Entity ID for your organization, contact [Veritas Services & Support](#).

To select an authentication method

- 1 In the left navigation pane, select **Policy Management > Authentication Management**.



- 2 Under the **Setup Authentication** section, click **Edit**.



- 3 In the **Authentication Type** drop-down, select **Single Sign-On ADFS**.
- 4 In the **Hybrid Login Allowed?** drop-down, select **Yes**.
- 5 If required, in the **Unique OWA IdP** field, select **Yes** if you have set up a unique Identity Provider (IdP) URL for logging in to Alta Personal Archive.
- 6 If required, in the **Unique OWA CID** field, select **Yes** if you want a unique Customer ID (CID) associated with the OWA IdP URL.

Note: The **Unique OWA CID** field only displays if you selected **Yes** in the **Unique OWA IdP** field. It is recommend that you do not select **Yes** in the **Unique OWA CID** field unless Veritas Services & Support instructs you to do so. If you select **Yes** for this option, Veritas Alta View Compliance and Governance Management Console automatically appends the value to the OWA IdP URL that is provided when you activate single sign-on.

- 7 Ensure that, under **Your Trust Information**, The customer ID and the Unique OWA CID details are displayed.
- 8 Select **I have read the instructions for setting the provided Entity ID and created my public key for upload** after you review the provided instructions.
- 9 Click **Save** to proceed to the next step.

Uploading a token-signing certificate

After you select AD FS as the authentication method for your organization, you must upload a token-signing certificate from your AD FS environment.

See [“Configuring AD FS to work with Veritas Alta Archiving”](#) on page 195.

From the **Upload Your Public Key** section on the **Authentication Management** page, you can upload your token-signing certificate. The **Upload Your Public Key** section displays after you complete the **Setup Authentication** section.

To upload a token-signing certificate

- 1 In the left navigation pane, select **Policy Management > Authentication Management**.
- 2 Under the **Upload Your Public Key** section, click **Browse and Upload**.

- 3 Select the token-signing certificate that you have generated.

Note: The token-signing certificate that you upload must have a `.cer` or `.cert` file extension.

- 4 In the **Public Key Upload** confirmation window, click **Return to Setup** to proceed to the next step.

Validating the Identity Provider URL

After you upload a token-signing certificate, you must validate the Identity Provider URL for your organization. From the Validate Relying Trust section on the **Authentication Management** page, you can validate the Identity Provider URL and the OWA Identity Provider URL, if necessary. The Validate Relying Trust section displays after you complete the **Upload Your Public Key** section.

To validate the Identity Provider URL

- 1 In the left navigation pane, select **Policy Management > Authentication Management**.
- 2 Under the **Validate Relying Trust** section, enter the Identity Provider URL for your organization in the **Identity Provider URL** field.

Note: The Identity Provider URL is normally the fully qualified domain name of the AD FS server or AD FS proxy, followed by `adfs/ls`. For example, the Identity Provider URL for an AD FS server named `adfs` with a fully qualified domain name of `example.com` is `https://adfs.example.com/adfs/ls`. The Veritas Alta Archiving authentication service currently does not support Identity Provider URLs that contain a dash. If you have an Identity Provider URL that contains a dash, contact [Veritas Services & Support](#).

- 3 If required, enter the OWA Identity Provider URL for your organization in the **OWA Identity Provider URL** field.

Note: The OWA Identity Provider URL field only displays if you selected **Yes** in the Unique OWA IdP field in the Setup Authentication section.

- 4 Click **Validate**.
- 5 After the **Validation Successful** message displays, click **Save** to proceed to the next step.

Activating single sign-on

After you validate the Identity Provider URL, you must activate single sign-on for Alta Personal Archive users. From the **Activate SSO** section on the **Authentication Management** page, you can activate single sign-on. The **Activate SSO** section displays after you complete the **Validate Relying Trust** section.

To activate single sign-on

- 1 In the **Activate SSO** section, click **Activate SSO**.
- 2 After the **Activation Successful** message displays, you can provide the URLs that are listed in the Application Login URL(s) section to Alta Personal Archive users.

Note: The Veritas Alta Archiving credentials that you provided to users before you configured the authentication service and activated single sign-on can still be used to log in to Alta Personal Archive.

Managing Retention Policies

This chapter includes the following topics:

- [About Retention Management](#)
- [Configuring the default retention period](#)
- [Creating a retention policy](#)
- [Editing a retention policy](#)
- [Deleting a retention policy](#)
- [Associating a retention policy with a policy target](#)
- [Disassociating a retention policy from a policy target](#)
- [Enabling and disabling the storage expiry setting](#)
- [Viewing the storage expiry status table](#)

About Retention Management

From the **Retention Management** section, you can manage the settings and policies that determine how long archived messages are retained in Veritas Alta Archiving. By default, Veritas Alta Archiving retains archived messages indefinitely (although this is not recommended since it will result in Storage overages in future). If required, you can configure Veritas Alta Archiving to collect archived messages for removal after those messages have been retained for a defined retention period.

The default retention period is a global setting that determines how long archived messages are retained before they are collected for removal. After you configure

the global retention period and enable the storage expiry setting, the collection of archived messages for removal begins. During the daily collection events, any messages that have been retained for longer than the default retention period are scheduled for removal 14 days later. The Retention Administrator receives daily notification emails during the 14-day grace period informing them of the number of archived messages that are scheduled for removal.

Note: Any archived messages that have a matter-level, search-level, or message-level legal hold applied from Veritas Alta eDiscovery are not removed.

Beyond the global retention period, the retention period for archived messages can be reduced or extended by creating retention policies to associate with the following policy targets:

- **Managed tags** — A global tag that you create and assign to users. Once you create a managed tag and associate a retention policy, users can apply the tag to archived messages to reduce or extend their retention period. The retention period of the associated retention policy determines how long tagged messages are retained in Veritas Alta Archiving.
- **Active Directory distribution groups** — The distribution groups that are synchronized from Active Directory using ArchiveTools CloudLink. Associating a retention policy with a distribution group reduces or extends the retention period of the archived messages for all members of that group. The retention period of the associated retention policy determines how long the messages for the distribution group members are retained in Veritas Alta Archiving.

Note: Because archived messages are retained in accordance with the longest retention period, you should create retention policies with retention periods that exceed the default retention period.

Configuring the default retention period

The default retention period determines how long archived messages are retained in Veritas Alta Archiving. To begin the process of removing messages from Veritas Alta Archiving, you configure the default retention period and enable the storage expiry setting.

Note: If Advanced Supervision service is enabled, Default Retention Period appears as read only and cannot be modified.

To configure the default retention period

- 1 In the left navigation pane, click **Retention Policies**.
- 2 In the **Default Retention Period** section, click **Edit**.
- 3 In the **Days** field, enter the retention period.
- 4 Click **Save**.

Note: After you configure the default retention period for the first time, you can only edit the existing period. If you no longer want to collect archived messages for removal from Veritas Alta Archiving, you can disable the storage expiry setting.

Creating a retention policy

Beyond the default retention period, the retention period for archived messages can be extended by creating retention policies to associate with policy targets. The policy targets that can be associated with a retention policy include managed tags and Active Directory distribution groups.

To create a retention policy

- 1 In the left navigation pane, select **Retention Management > Retention Policies**.
- 2 Click **Create New**.
- 3 On the **Retention Policy** page, specify the following: in the **Policy Name** field.

Policy Name	Enter a unique name for the retention policy.
Retention Period (in days)	Enter the retention period for the policy in days.
Description	Provide a short description for the retention policy.
Policy Status	Set the status as Enabled if you want the retention policy to be enabled once you create it. Set the status as Disabled if you want to create a policy, but do not want the retention policy to be disabled till further decision.

- 4 Click **Save**.

Editing a retention policy

If required, you can edit the details of existing retention policies. The details you can edit include the policy name, the retention period, the policy status, and the policy description.

To edit a retention policy

- 1 In the left navigation pane, select **Retention Management > Retention Policies**.
- 2 In the **Policy Name** column of the retention policies list, click the name of the retention policy you want to edit.
- 3 In the top-right corner of the **Retention Policy** page, click **Edit**.
- 4 Edit the following details of the retention policy.

Policy Name	Update a unique name for the retention policy, if required.
Retention Period (in days)	Change the retention period for the policy in days, if required.
Description	Provide a short description for the retention policy.
Policy Status	Set the status as Enabled if you want the retention policy to be enabled once you create it. Set the status as Disabled if you want to create a policy, but do not want the retention policy to be disabled till further decision.

- 5 Click **Save**.

Deleting a retention policy

You can delete any retention policies that are no longer needed. However, you cannot delete a retention policy if it is associated with a policy target.

To delete a retention policy

- 1 In the left navigation pane, select **Retention Management > Retention Policies**.
- 2 Select the policy you want to delete.

- 3 In the **Delete** column of the retention policies list, click the **Delete** icon in the corresponding row.
The application prompts you to confirm that you want to perform the operation.
- 4 Click **Yes**.

Associating a retention policy with a policy target

After you create a retention policy, you can associate it with a policy target. The policy targets that can be associated with a retention policy include managed tags and Active Directory distribution groups.

Note: You can associate a retention policy with more than one policy target. However, each policy target can only be associated with one retention policy.

To associate a retention policy with a policy target

- 1 In the left navigation pane, select **Retention Management > Retention Policies**.
- 2 Under **Policy Details**, ensure that the policy details are appropriate.
- 3 Under **Targets**, click **Add Targets**.
The **Policy Target** window appears.
- 4 In the **Target Type** drop-down, search for and select the check boxes of the target you want to associate.

Note: You can filter the target types to show all targets, only managed tags, or only distribution groups.

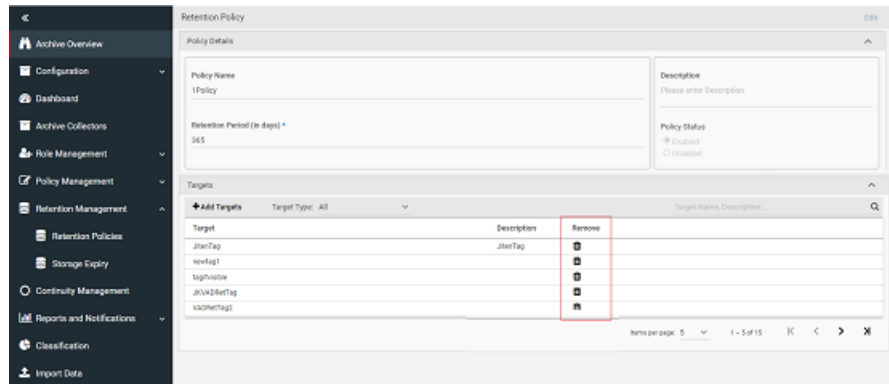
- 5 Click **Add**.

Disassociating a retention policy from a policy target

If required, you can disassociate a retention policy from a policy target.

To disassociate a retention policy from a policy target

- 1 In the left navigation pane, select **Retention Management > Retention Policies**.
- 2 Under **Policy Details**, ensure that the policy details are appropriate.
- 3 Under **Targets**, select the target you want to disassociate.



- 4 In the **Remove** column of the target list, click the **Delete** icon.
The application prompts you to confirm that you want to perform the operation.
- 5 Click **Yes**.

Enabling and disabling the storage expiry setting

After you configure a default retention period, you must enable the storage expiry setting before the collection of archived messages for removal begins.

Any archived messages that meet one or more of the following conditions are not removed from Veritas Alta Archiving:

- Messages that have a matter-level, a search-level, or message-level legal hold applied from Veritas Alta eDiscovery.
- Messages that have a managed tag applied that is associated with a retention policy that has a retention period that exceeds the default retention period.
- Messages of an Active Directory distribution group member that is associated with a retention policy that has a retention policy that exceeds the default retention period.

Note: Any archived messages that are removed from Veritas Alta Archiving cannot be retrieved after removal is complete.

If Advanced Supervision service is enabled, **Storage Expiry** is set to **Daily** by default and cannot be modified.

To enable or disable the storage expiry setting

- 1 In the left navigation pane, select **Retention Management > Storage Expiry**.
- 2 On the top-right corner of the page, click **Edit**.
- 3 In the **Storage Expiry** section, do one of the following:
 - Select **Daily** to enable the storage expiry setting.
 - Select **Never** to disable the storage expiry setting.
- 4 Click **Save**.

Viewing the storage expiry status table

After you configure the default retention period and enable the storage expiry setting, the collection of archived messages for removal begins. From the **Storage Expiry** page, you can view a status table with the following information about each batch of messages being removed:

Date	Indicates the date and time the batch was created
Number of Emails	Indicates the number of archive messages in the batch.
Expiration Status	Indicates the current status for the batch. <ul style="list-style-type: none"> ■ Completed — the batch of messages have been removed. ■ In progress — the batch of messages are in the process of being removed. ■ Not started — the batch of messages are in the queue for removal.

To view the storage expiry status table

- 1 In the left navigation pane, select **Retention Management > Storage Expiry**.
- 2 If required, select one of the following options in the **Expiration Status** field to filter the table:
 - **All** — select to view the status of all batches of messages being removed.

- **Not Started** — select to view only the batches of messages that are in the queue for removal.
- **In Progress** — select to view only the batches of messages that are in the process of being removed.
- **Completed** — select to view only the batches of messages that have been removed.

Managing Email Continuity Services

This chapter includes the following topics:

- [About Email Continuity](#)
- [Email Continuity prerequisites](#)
- [Configuring Email Continuity](#)
- [Provisioning the Email Continuity service for your mail servers](#)
- [Adding the Email Continuity IP ranges to your firewall and mail server allowlists](#)
- [Updating your email security provider routing configuration](#)
- [Testing the Email Continuity configuration](#)
- [Managing Email Continuity](#)
- [Email Continuity FAQ](#)

About Email Continuity

Email Continuity is an add-on feature that allows Alta Personal Archive users to send and receive email messages during a mail server outage.

Incoming email messages are typically routed through your email security provider to your mail server. After the messages reach the mail server, they are journaled to Veritas Alta Archiving. Outgoing messages from your mail server are typically journaled to Veritas Alta Archiving before they reach their recipients. However, during a mail server outage your mail server cannot receive, send, or journal email messages.

Email Continuity lets you configure your email security provider to use Veritas Alta Archiving as a secondary gateway for your email when your mail server is unavailable. During a mail server outage your email security provider routes mail to Veritas Alta Archiving, and users can receive and send email messages through Alta Personal Archive. When the mail server outage ends the Email Continuity service automatically flushes all the email messages that were sent and received during the outage to your mail server or relay server, for normal delivery.

Note: During an outage, the Email Continuity service attempts to flush messages to your mail server every 5 minutes for up to 7 days.

Email Continuity prerequisites

Before you can configure Email Continuity you must ensure that you use a compatible email security platform.

For information about the email security platforms that Email Continuity supports, refer to the [Veritas Alta Archiving Compatibility List](#).

Configuring Email Continuity

[Table 10-1](#) lists the steps you need to take to configure Email Continuity.

Table 10-1 Steps to configure Email Continuity

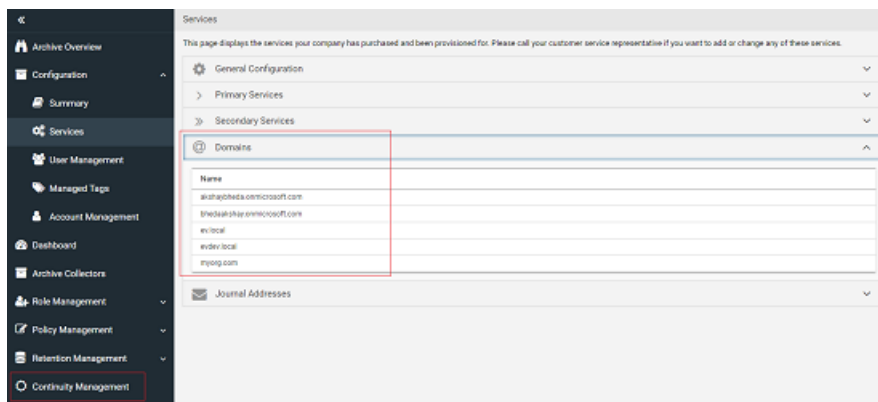
Step	Action	Reference
Step 1	Get Veritas Services & Support to provision the Email Continuity service for your mail servers.	See “Provisioning the Email Continuity service for your mail servers” on page 166.
Step 2	Add the Email Continuity IP ranges to your firewall and to your mail server allowlists, as required.	See “Adding the Email Continuity IP ranges to your firewall and mail server allowlists” on page 167.
Step 3	Configure your email security provider to use Email Continuity as a secondary route for email.	See “Updating your email security provider routing configuration” on page 167.
Step 4	Test the new setup to ensure that Email Continuity is configured correctly.	See “Testing the Email Continuity configuration” on page 168.

Provisioning the Email Continuity service for your mail servers

You must get Veritas Services and Support to provision the Email Continuity service for your company, and to give you the additional information, you need to set up Email Continuity.

To provision the Email Continuity service for your mail servers

- 1 Obtain a list of all the inbound domains that your mail server uses.
- 2 Log on to the Veritas Alta Archiving Veritas Alta View Compliance and Governance Management Console console.
- 3 In the left navigation pane, select **Configuration > Services**.
- 4 Under the **Domains** section, check whether all of your mail server's inbound domains are listed.



If any of the domains are not present, make a note of the missing domains.

- 5 Contact [Veritas Services & Support](#) and do as follows:
 - Inform Veritas Services & Support that you want to add Email Continuity as an Veritas Alta Archiving service for your organization.
 - If you found in step 4 that any of your mail server inbound domains were not configured in Veritas Alta View Compliance and Governance Management Console, ask Veritas Services & Support to add the required inbound domains to your Veritas Alta Archiving company configuration.
 - Provide Veritas Services & Support with the IP address and the domain name for each mail server for which you want to enable Email Continuity. They can then provision the Email Continuity service for your company.

Note: Email Continuity can be configured for only one mail server per domain.

- From Veritas Services & Support, obtain the following information that needs to be used in the next steps:
 - The Veritas Alta Archiving Email Continuity IP ranges for your Veritas Alta Archiving instance.
 - The Veritas Alta Archiving Email Continuity mail server domain for your geographical region.

Adding the Email Continuity IP ranges to your firewall and mail server allowlists

You must add the Email Continuity IP ranges that you obtained from Veritas Services & Support to your firewall allowlist and your mail server allowlist, as appropriate.

To add the Email Continuity IP ranges to your firewall and mail server allowlists

- 1 Log on to the control panel for your firewall or mail server.
- 2 Add the IP ranges for your Veritas Alta Archiving instance to port 25 (SMTP).
- 3 If Email Continuity is to flush back messages to your mail server rather than to a relay server, add the same IP address range to your Exchange receive connector or to your Domino allowed hosts. This step enables the mail server to relay the flushed back messages on to your users.

Updating your email security provider routing configuration

You must configure your email security provider to route email to Email Continuity as the last route in its routing list. The email security provider needs to route the mail to the Email Continuity server domain when your normal message routes fail.

For this procedure you need the Veritas Alta Archiving Email Continuity mail server domain that you obtained from Veritas Services & Support.

To update your email security provider routing configuration

- 1 Log on to the control panel for your email security provider.
- 2 Add the Veritas Alta Archiving Email Continuity mail server domain as the last domain to use when routing mail.

Testing the Email Continuity configuration

You must confirm that Email Continuity has been configured correctly and that it works successfully in the event of a mail server failure.

To test the Email Continuity configuration

- 1 Contact [Veritas Services & Support](#), and have them test the Email Continuity connectivity, to confirm that flush back is configured correctly.
- 2 At a convenient time such as out of normal office hours, pause the SMTP receiver of your mail server to simulate a mail server failure. This action should now trigger your email security provider to fail over to Email Continuity. Then try each of the following:
 - Test that you can receive email from external email addresses to your account in Alta Personal Archive.
 - Test that you can send email from Alta Personal Archive to an external email address.
 - Test that you can send email from Alta Personal Archive to an internal email address.
- 3 Restart your email service and verify that the test emails you sent and received in Alta Personal Archive in the previous step are flushed back to your mail server.

Managing Email Continuity

You can configure the option to display the Email Continuity status to users and to view a summary of the service. The **Continuity Management** option is available only if your organization subscribes to Email Continuity.

To manage Email Continuity

- 1 In the left navigation pane, select **Continuity Management**.
- 2 Under **Email Continuity Settings**, select the **Indicate EC Active** check box to notify users during a mail server outage.
- 3 In the summary table, review the information that is provided about the Domain Names, respective Mail Servers, and the Email Continuity service during outages is active or not.

Email Continuity FAQ

The following frequently asked questions provide more information about Email Continuity.

- **During Email Continuity configuration, which IP address ranges do I need to add to my firewall or mail server allowlist?**

The IP ranges vary by region. For details, contact [Veritas Services & Support](#).

- **How do I enable Email Continuity during a mail server outage?**

Email Continuity is enabled automatically during an outage.

- **How do I flush email messages to our mail server after an outage?**

After an outage, the Email Continuity service automatically flushes all the email messages that were sent and received during the outage to your mail server.

- **Where do the email messages that are flushed to our mail server appear in Microsoft Outlook?**

All the email messages that were sent and received during the outage appear in your Outlook Inbox folder.

- **After a mail server outage, do I receive a notification once email messages are flushed to our mail server?**

No, no notification is provided after the Email Continuity service finishes flushing email messages back to your mail server.

- **Do distribution lists get expanded by the Email Continuity service?**

No, the Email Continuity service does not expand distribution lists. However, distribution lists are expanded for the email messages that are flushed back to your mail server after an outage.

Managing Reports and Notifications

This chapter includes the following topics:

- [About Veritas Alta Archiving reports, logs, usage, and notifications](#)
- [Reports](#)
- [Usage](#)
- [Logs](#)
- [Notifications](#)

About Veritas Alta Archiving reports, logs, usage, and notifications

From the **Reports and notifications** section, you can access the logs, reports, and notifications that provide information about Veritas Alta Archiving usage by your organization. You can export the logs and reports in various file formats.

Reports

This section describes procedures to generate various reports in Veritas Alta View Compliance and Governance Management Console console.

Generating a Messaging Report

The Messaging Report displays information about Veritas Alta Archiving usage based on the following parameters:

- The average size of archived messages by user.
- The average number of messages that are archived per user each day.
- The average size of message attachments.
- The average search speed for users in your organization.
- The total number of archived messages that have been imported and their sizes. This report contains a summary for the selected period. Click on any date to view corresponding detailed report.

To generate a Messaging Report

- 1 In the left navigation pane, select **Reports and Notifications > Reports**.
- 2 On the **Archiving Scorecard** page, select the **Messaging** tab.
- 3 In the top-right corner of the page, select the parameter for which you want to generate a report.
- 4 Select a predefined duration, or select **Custom** if you want to specify a start and end date for the report.
- 5 If required, select **Compare to All Companies** to compare your usage to other organizations.
- 6 Click **Apply**.
- 7 If required, switch between the **Line Chart** and **Bar Chart** display options to view chart in the report.
- 8 To export the report in EXCEL, PDF, CSV, or WORD format., click the **Export** icon.

Generating a Personal Archive Report

The Personal Archive report displays information about Alta Personal Archive usage based on the following parameters:

- The number of users that have logged in to Alta Personal Archive.
- The number of managed tags that have been created per user.
- The number of managed tags that have been applied per user.
- The number of searches that have been performed.
- The average search speed for users in your organization.
- A list of the search strings that have been used.
- A list of user accounts who have crossed 80 percent limit of their folder count.

Additionally, you can compare the Alta Personal Archive usage of your organization with the usage of other organizations

To generating a Personal Archive Report

- 1 In the left navigation pane, select **Reports and Notifications > Reports**.
- 2 On the **Archiving Scorecard** page, select the **Personal Archive** tab.
- 3 In the top-right corner of the page, select the parameter for which you want to generate a report.
- 4 Select a predefined duration, or select **Custom** if you want to specify a start and end date for the report.
- 5 If required, select **Compare to All Companies** to compare your usage to other organizations.
- 6 Click **Apply**.
- 7 If required, switch between the **Line Chart** and **Bar Chart** display options to view chart in the report.
- 8 To export the report in EXCEL, PDF, CSV, or WORD format., click the **Export** icon.

Generating a Mobile Web Access Report

The Mobile Web AccessMobile Web Access report displays information about usage based on the following parameters:

- The number of users that have logged in to Mobile Web Access.
- The number of searches that have been performed.
- A list of the search strings that have been used.

Additionally, you can compare the Mobile Web Access usage of your organization with the usage of other organizations.

To generate a Mobile Web Access Report

- 1 In the left navigation pane, select **Reports and Notifications > Reports**.
- 2 On the **Archiving Scorecard** page, select the **Mobile Web Access** tab.
- 3 In the top-right corner of the page, select the parameter for which you want to generate a report.
- 4 Select a predefined duration, or select **Custom** if you want to specify a start and end date for the report.
- 5 If required, select **Compare to All Companies** to compare your usage to other organizations.

- 6 Click **Apply**.
- 7 If required, switch between the **Line Chart** and **Bar Chart** display options to view chart in the report.
- 8 To export the report in EXCEL, PDF, CSV, or WORD format., click the **Export** icon.

Generating a Discovery Archive Report

The Discovery Archive report displays information about Alta eDiscovery administration actions based on the following parameters:

- Hidden Emails – shows detailed report of hidden emails from end users.
- Unhidden Emails – shows detailed report of unhidden emails to end users.
- Delete Emails – shows detailed report of deleted emails of end users.
- Mail Reassignment – shows detailed report of reassigned emails of end users.

To generate a Discovery Archive Report

- 1 In the left navigation pane, select **Reports and Notifications > Reports**.
- 2 On the **Archiving Scorecard** page, select the **Discovery Archive** tab.
- 3 In the top-right corner of the page, select the parameter for which you want to generate a report.
- 4 Select a predefined duration, or select **Custom** if you want to specify a start and end date for the report.
- 5 If required, select **Compare to All Companies** to compare your usage to other organizations.
- 6 Click **Apply**.
- 7 If required, switch between the **Line Chart** and **Bar Chart** display options to view chart in the report.
- 8 To export the report in EXCEL, PDF, CSV, or WORD format., click the **Export** icon.

See [“About Veritas Alta Archiving reports, logs, usage, and notifications”](#) on page 170.

Generating an Advanced Supervision specific Report

You can generate the Account Mapping report for Advanced Supervision.

To generate the Account Mapping report for Advanced Supervision

- 1** In the left navigation pane, select **Reports and Notifications > Reports**.
- 2** On the **Archiving Scorecard** page, select the **Advanced Supervision** tab.
- 3** In the top-right corner of the page, select the **Account Mapping** option for which you want to generate a report.
- 4** Provide the ail address, RepID, and last name of the account in the respective fields.
- 5** Click **Apply**.
- 6** If required, switch between the **Line Chart** and **Bar Chart** display options to view chart in the report.
- 7** To export the report in EXCEL, PDF, CSV, or WORD format., click the **Export** icon.

See [“About Veritas Alta Archiving reports, logs, usage, and notifications”](#) on page 170.

Usage

This section describes procedures to generate various usage-specific reports in Veritas Alta View Compliance and Governance Management Console console.

Generating a service usage report

The Service Usage tab provides run usage reports based on date range and interval. You can run and export reports based on the following services.

Note: Data can take up to 24 hours to refresh once you’ve enabled or disabled mailboxes.

- **User Statistics:** Generates a report for the number of user(s) that are enabled and disabled.
- **Personal Archive:** Generates a report for the number of Personal Archive User(s) enabled and quota (minimum license count).
- **Discovery Archive:** Generates a report for the number of Discovery Archive User(s) enabled and quota (minimum license count).
- **Folder Synchronization (Vault Solution):** Generates a report for the number of Folder Sync User(s) enabled and quota (minimum license count) for Vault Solution.

- **Folder Synchronization (EV.C)**: Generates a report for the number of Folder Sync User(s) enabled and quota (minimum license count) for Veritas Alta Archiving.
- **Email Continuity**: Generates a report for the number of Email Continuity User(s) enabled and quota (minimum license count).

To generate a service usage report

- 1 In the left navigation pane, select **Reports and Notifications > Usage**.
- 2 On the **User Scorecard** page, select the **Service Usage** tab.
- 3 In the top-right corner of the page, select the any of the above-mentioned services for which you want to generate a user report.
- 4 Select a predefined duration, or select **Custom** if you want to specify a start and end date for the report.
- 5 Select the predefined frequency (Daily, Weekly, Monthly, Quarterly, or Yearly.)
- 6 Click **Apply**.
- 7 If required, switch between the **Line Chart** and **Bar Chart** display options to view chart in the report.
- 8 To export the report in EXCEL, PDF, CSV, or WORD format., click the **Export** icon.

Generating a mailbox statistics report

The Mailbox Statistics tab provides reports for the number of mailboxes that are added and deleted, and enabled and disabled. You can run and export reports based on the following services.

Note: Data can take up to 24 hours to refresh once you've enabled or disabled mailboxes.

- **Mailboxes Added/Deleted**: Generates a report for the number of mailboxes that are added or deleted for a group.
- **Mailboxes Enabled/Disabled**: Generates a report for the number of mailboxes that are enabled and disabled.

To generate a service usage report

- 1 In the left navigation pane, select **Reports and Notifications > Usage**.
- 2 On the **User Scorecard** page, select the **Mailbox Statistics** tab.

- 3 In the top-right corner of the page, select the any of the above-mentioned services for which you want to generate a report.
- 4 Select a predefined duration, or select **Custom** if you want to specify a start and end date for the report.
- 5 Select the predefined frequency (Daily, Weekly, Monthly, Quarterly, or Yearly.)
- 6 Click **Apply**.
- 7 If required, switch between the **Line Chart** and **Bar Chart** display options to view chart in the report.
- 8 To export the report in EXCEL, PDF, CSV, or WORD format., click the **Export** icon.

Generating an archived message size report

The Archived Message Size tab provides reports for the total archive size in GB and GB archived per account. You can run and export reports based on the following parameters.

Note: Data can take up to 24 hours to refresh once you've enabled or disabled mailboxes.

- **GB archived:** Generates a report to display total size in GB and count of the messages that are archived for a group.
- **GB archived per account:** Generates a report to display total size in GB and count of the messages that are archived per account.

To generate a service usage report

- 1 In the left navigation pane, select **Reports and Notifications > Usage**.
- 2 On the **User Scorecard** page, select the **Archived Message Size** tab.
- 3 In the top-right corner of the page, select the any of the above-mentioned services for which you want to generate a report.
- 4 Select a predefined duration, or select **Custom** if you want to specify a start and end date for the report.
- 5 Select the predefined frequency (Daily, Weekly, Monthly, Quarterly, or Yearly.)
- 6 Click **Apply**.

- 7 If required, switch between the **Line Chart** and **Bar Chart** display options to view chart in the report.
- 8 To export the report in EXCEL, PDF, CSV, or WORD format., click the **Export** icon.

Logs

This section describes procedures to generate various log reports in Veritas Alta View Compliance and Governance Management Console console.

Viewing the Activity Log

The Activity Log displays all events that occur in Veritas Alta Archiving including user logins, password resets, and user role changes. From the **Activity Log** page, you can view the full log or filter the log by date range, user name, events, or event details.

To view the Activity Log

- 1 In the left navigation pane, select **Reports and Notifications > Logs**.
- 2 Select the **Activity Log** tab.
- 3 If required, filter the log using the following criteria:
 - **From Date/To Date** — filter the log by entering a date range.
 - **Detail Substring** — filter the log by entering event detail keywords such as success or failure.
 - **User** — filter the log by entering a user name or email address.
 - **Event** — filter the log by selecting a specific event type.
- 4 Click **Search**.

The resulting Activity Log report appears in the main pane.

Note: The report does not display the private IP addresses of events that the Veritas Alta Archiving services have logged. Instead the **IP Address** column displays **Internal Service**.

- 5 To export the log in EXCEL, PDF, CSV, or WORD format, click the **Export** icon.

Viewing the Message Log

The Message Log displays information about the archived messages in Veritas Alta Archiving. From the **Message Log** page, you can view the full log or filter the log by date range, message sender, message recipient, or subject.

To view the Message Log

- 1 In the left navigation pane, select **Reports and Notifications > Logs**.
- 2 Select the **Message Log** tab.
- 3 If required, filter the log using the following criteria:
 - **From Date/To Date** — filter the log by entering a date range.
 - **Sender** — filter the log by entering the message sender email address.
 - **Recipient** — filter the log by entering the message recipient email address.
 - **Subject** — filter the log by entering message subject keywords.
 - **Has Attachment** — filter the log by selecting **Yes** for messages with attachments or **No** for messages without attachments.
- 4 Click **Search**.
- 5 To export the log in EXCEL, PDF, CSV, or WORD format, click the **Export** icon.

Viewing the Usage Log

The Usage Log displays information about Veritas Alta Archiving usage. You can view the following information:

- The total number of messages that have been archived.
- The number of new messages that have been archived in the last 24 hours.
- The average number of messages that are archived each day.
- The average size of messages that have been archived.
- The total storage that has been used for archiving messages.

To view the Usage Log

- 1 In the left navigation pane, click **Reports and Notifications > Logs**.
- 2 Select the **Usage Log** tab.
- 3 To export the log in EXCEL, PDF, CSV, or WORD format, click the **Export** icon.

Creating a Retention Log Report

A Retention Log Report displays usage information for retention policies. You can create a report with the full log. You can also filter the log by date range, user name, action type, or policy name.

To create a Retention Log Report

- 1 In the left navigation pane, click **Reports and Notifications > Logs**.
- 2 Select the **Retention Log** tab.
- 3 If required, filter the log using the following criteria:
 - **From Date/To Date** — filter the log by entering a date range.
 - **User Name** — filter the log by entering a user name.
 - **Action Type** — filter the log by selecting a specific type of action.
 - **Policy Name** — filter the log by entering the name of a retention policy.
- 4 Click **Search**.
- 5 To export the log in EXCEL, PDF, CSV, or WORD format, click the **Export** icon.

Viewing the Mobile Browser Log

The Mobile Browser Log displays information about Enterprise Vault.cloud Mobile Web Access usage. You can view the full log or filter the log by date range.

To view the Mobile Browser Log

- 1 In the left navigation pane, click **Reports and Notifications > Logs**.
- 2 Select the **Mobile Browser Log** tab.
- 3 If required, filter the log by date range using the **From Date** and **To Date** fields.
- 4 Click **Search**.
- 5 To export the log in EXCEL, PDF, CSV, or WORD format, click the **Export** icon.

Viewing the Personal Browser Log

The Personal Browser Log displays information about Veritas Alta Personal Archive usage. From the Personal Browser Log tab, you can view the full log or filter the log by date range.

To view the Personal Browser Log

- 1 In the left navigation pane, click **Reports and Notifications**.
- 2 Select the **Personal Browser Log** tab.
- 3 If required, filter the log by date range using the **From Date** and **To Date** fields.
- 4 Click **Search**.
- 5 If required, click **Export** icon to export the log in EXCEL, PDF, CSV, or WORD format.

Viewing the Discovery Browser Log

The Discovery Browser Log displays information about Veritas Alta eDiscovery usage. You can view the full log or filter the log by the date range.

To view the Discovery Browser Log

- 1 In the left navigation pane, click **Reports and Notifications > Logs**.
- 2 Select the **Discovery Browser Log** tab.
- 3 If required, filter the log by date range using the **From Date** and **To Date** fields.
- 4 Click **Search**.
- 5 To export the log in EXCEL, PDF, CSV, or WORD format, click the **Export** icon.

Notifications

This section describes procedures to configure notification-specific parameters in Veritas Alta View Compliance and Governance Management Console console.

Enabling or disabling usage notifications

You can enable or disable the usage notifications only if you possess a System Administrator role. However, if you disable the notifications, the notification threshold and frequency are reset to the default settings.

To enable or disable usage notifications

- 1 In the left navigation pane, select **Reports and Notifications > Notifications**.
The **Notifications** option appears only if you are logged in with a System Administrator role.
- 2 Click **Edit**.

- 3 Under **Usage Notifications**, click **Enabled** or **Disabled**.
- 4 Click **Save**.
- See [“Changing the usage notification threshold and frequency”](#) on page 181.
- See [“Adding or removing email addresses for usage notifications”](#) on page 182.

Changing the usage notification threshold and frequency

As a system administrator, you can change the percentage at which notification emails are sent and the frequency of notification emails.

To change usage notification threshold and frequency

- 1 In the left navigation pane, select **Reports and Notifications > Notifications**.

The **Notifications** option appears only if you are logged in with a System Administrator role.
- 2 Click **Edit**.
- 3 Do any of the following:

To do this	Do this
To change the percentage at which notification emails are sent	Under Usage Notification Threshold , in the Notify if committed usage exceeds option, select a new percentage.
To change the frequency of notification emails	<div>Under Notification Frequency, select the interval you want to use.</div> <div>The following intervals are available:</div> <div><ul style="list-style-type: none">■ Quarterly - Notifications are sent on the first Monday of each quarter. The quarters start in January, April, July, and October.■ Monthly - Notifications are sent on the first Monday of each month.■ Weekly - Notifications are sent every Monday. This setting is the default frequency.■ Daily - Notifications are sent every day.</div> <div>Notification emails are sent at 9:00 A.M. in the default company time zone.</div>

- 4 Click **Save**.
- See [“Enabling or disabling usage notifications”](#) on page 180.
- See [“Adding or removing email addresses for usage notifications”](#) on page 182.

Adding or removing email addresses for usage notifications

Any system administrator's email addresses are added automatically to the list of notification recipients. You can add up to 50 additional email addresses.

To add or remove email addresses for usage notifications

- 1 In the left navigation pane, select **Reports and Notifications > Notifications**.
- 2 Click **Edit**.
- 3 Under **Notification Emails**, do any of the following as required:
 - To add an email address, type an email address, and click **Add**.
 - To remove an email address, select an email address and click the **Delete** icon in the corresponding row.
- 4 Click **Save**.

See [“Enabling or disabling usage notifications”](#) on page 180.

See [“Changing the usage notification threshold and frequency”](#) on page 181.

Classification

This chapter includes the following topics:

- [About classification](#)
- [Which emails get classified?](#)
- [Steps for setting up classification](#)
- [Accessing the Veritas Alta Classification](#)
- [Veritas Alta Archiving item properties for use in custom classification policies](#)

About classification

With the continuous growth of unstructured data in the business environment, taking decisions to archive and delete content of business or legal value is a challenge. You can simplify data management decisions by categorizing and organizing data based on classification policies.

If your company has the Veritas Alta Classification service enabled, the service can apply classification tags to Veritas Alta Archiving's incoming emails that match the enabled policies in the Veritas Alta Classification. Alta eDiscovery users can then search for the emails that are tagged with the classification tags, during investigations and PDGAlta eDiscovery.

Administrators with the **classification administrator** role can access the Veritas Alta Classification from Veritas Alta View Compliance and Governance Management Console, to enable the policies that your organization wants to use. Each policy specifies the conditions that an email must meet to be assigned one or more related classification tags. The built-in policies address many of the regulatory requirements and corporate standards for which you may want to classify emails.

For example, you can help meet privacy regulations, including the General Data Protection Regulation (GDPR), through the policies that detect personally identifiable

information. The Personally Identifiable Information (PII) policies look for content like credit card numbers, email addresses, dates of birth, passport numbers, and driver's license numbers. When an email that is incoming to Veritas Alta Archiving matches the criteria for the policy, the associated PII classification tag is assigned in the email header. Alta eDiscovery reviewers can search for emails with the assigned PII tag. In this way, classification can help to reduce the number of emails to review as part of meeting your organization's regulatory requirements.

For information on how to configure classification policies and classification tags, see the help that is provided with the Veritas Alta Classification.

For information on working with the emails that contain classification tags, see the *Alta eDiscovery User Guide*.

Which emails get classified?

If your company has the Veritas Alta Classification service enabled, the service can apply classification tags to Veritas Alta Archiving's incoming emails that match the enabled policies in the Veritas Alta Classification.

Once a policy is enabled in the Veritas Alta Classification, the classification process is performed for the new emails that Veritas Alta Archiving ingests. Note that:

- The classification tags that are associated with a policy get applied only to matching emails that are ingested into Veritas Alta Archiving after the policy is enabled. Any previously archived emails do not get tagged.
- If the system administrator changes or disables a classification policy, the changes affect the emails that are subsequently ingested into Veritas Alta Archiving. The changes are not reflected in the existing archived emails. For example if you disable a previously enabled classification policy, any archived emails that were tagged as a result of matching the policy remain tagged in Veritas Alta Archiving.

Note: Classification tags are only assigned through the Veritas Alta Classification. Unlike other types of tag, you cannot assign or remove classification tags manually.

Steps for setting up classification

[Table 12-1](#) provides the steps for setting up classification of emails that are ingested into Veritas Alta Archiving, using the Veritas Alta Classification.

Table 12-1 Process for setting up classification

Step	Description	Further Information
Step 1	Ensure that the Veritas Alta Classification service is enabled for your company in Veritas Alta Archiving.	To enable your organization for classification, contact Veritas Services & Support .
Step 2	Set up the required account access to the Veritas Alta Classification.	Assign the classification administrator role to the required accounts. See “About Role Management” on page 127.
Step 3	Access the Veritas Alta Classification.	You can access the Veritas Alta Classification directly from Veritas Alta View Compliance and Governance Management Console. See “Accessing the Veritas Alta Classification” on page 185.
Step 4	Decide on the classification policies you require, and enable those policies. You can create custom policies if required.	See the Veritas Alta Classification help. See “Veritas Alta Archiving item properties for use in custom classification policies” on page 186.

Accessing the Veritas Alta Classification

You must possess the **Classification Administrator** role if you want to access Veritas Alta Classification from Veritas Alta View Compliance and Governance Management Console console.

To access the Veritas Alta Classification

- 1
- In the left navigation pane, click **Classification**.
- The **Policies** page of the Veritas Alta Classification application appears. The first classification policy in the list is selected by default.

Note: If you click the **Classification** node again while the Veritas Alta Classification tab is open, the Veritas Alta Classification user interface gets refreshed.

- 2
- Clear the check box of the first policy
- 3
- Search for and select the policies that you want to enable.
- For more information about enabling classification policies, refer to the Veritas Alta Classification Online Help.

Veritas Alta Archiving item properties for use in custom classification policies

When Veritas Alta Archiving indexes an item, it populates the item's metadata properties with information about the item. Some examples of this information include the display name and email address of the message author, the archived date, and the file size of the item.

Indexed items can have a large number of properties, but only a subset is relevant for classification purposes. Veritas Alta Archiving passes this subset of properties and their associated values to the Veritas Alta Classification for use in classification. When you create a custom Veritas Alta Classification policy you can enter the names of these properties in the custom date, custom number, or custom string fields, when you define the policy conditions.

Table [Table 12-2](#) lists the item properties that Veritas Alta Archiving passes to the Veritas Alta Classification.

Table 12-2 Item properties passed to the Veritas Alta Classification

Property	Type	Description
adat	Date	The date on which the item was archived.
audn	String	The display names of the author and, if applicable, of the person on whose behalf the item was sent.

Table 12-2 Item properties passed to the Veritas Alta Classification
(continued)

Property	Type	Description
aua	String	The email addresses of the author and, if applicable, of the person on whose behalf the item was sent.
date	Date	The created, sent, received, or archived date.
natc	Number	The number of attachments.
nrcp	Number	The number of recipients (the total of the To, CC, and BCC recipients)
rbdn	String	The display names of the BCC recipients.
rbea	String	The email addresses of the BCC recipients.
rcdn	String	The display names of the CC recipients.
rcea	String	The email addresses of the CC recipients.
rtdn	String	The display names of the To recipients.
rtea	String	The email addresses of the To recipients.
size	Number	The size of the item in KB.
subj	String	The subject or title.

Table [Table 12-3](#) lists the properties of message attachments that Veritas Alta Archiving passes to the Veritas Alta Classification.

Table 12-3 Attachment properties passed to the Veritas Alta Classification

Property	Type	Description
a_dat	Date	The created, sent, received, or archived date of the attachment.
a_dtyp	String	The data type of the attachment. For example, DOCX, XSLX, or MSG.

Table 12-3 Attachment properties passed to the Veritas Alta Classification
(continued)

Property	Type	Description
a_size	Number	The size of the attachment in KB.
a_subj	String	The file name of the attachment or, if it is a message, the subject.

Note: The classification feature treats attachments as files. So if an attachment is an email message, its sender information and recipient information are not available for classification.

For more information on creating custom classification policies, see the Veritas Alta Classification help.

Managing Data Import

This chapter includes the following topics:

- [About Import Data](#)
- [Importing data into archives](#)

About Import Data

Every company has existing emails, whether located in active user mailboxes, personal stores, document management systems, or other communication libraries. You can consolidate some or all of these legacy email sources into your Archive. This section outlines the data import process, explaining how your company's legacy email can be transferred to the Archive correctly-- and in its entirety.

Legacy email refers to data sitting on local archives on desktops or laptops, email storage on servers, or email on backup tapes. By moving your legacy email into the Cloud Archive, you have a complete, living record of your past and present email history.

The legacy email has context, unlike active email that is saved into your Archive via journaling. A journaled message is captured in transit and saved in its original, pristine form, while legacy email may have been altered before it is placed in the Archive. Legacy messages have previously arrived within the user mailbox and may have been copied into a folder, forwarded to other recipients, or otherwise acted on by the user.

Messages may also have metadata fields altered when information is copied into PST files. To capture the additional information of a legacy message, the import process into the Archive is entirely different than the transfer of journal email. During this process, all legacy email contextual elements are preserved.

You can import legacy email into the archive using Veritas Alta Archiving Veritas Alta View Compliance and Governance Management Console. You can use the

Import Data feature to import items into archives. You can upload items up to 12 GB per calendar year (January 1 to December 31). Over the period of one year, you may choose to upload an item of 12 GB in one go or upload multiple smaller items with a collective size of a maximum of 12 GB.

You need to collect the legacy email in the proper format from your email environment and then send-- either electronically or physically-- to Veritas for import into the archive in the following scenarios:

- If the file that you want to import is larger than 12 GB and less than 20 GB.
- If the file format is .NSF

Guidelines to use the **Import Data** feature:

- To Import MSG or EML files, It needs to compressed MSG or EML files in ZIP file.
The Quota limit for zip files will be calculated at Import time. So please check content size manually before creating ZIP file.
- PST and ZIP file names should not contain commas. However, special or double-byte characters are allowed.
- PST and ZIP files need to be 12 GB or less in size.
- PST and ZIP files cannot be password protected.
- Run *scanpst.exe*, a utility included with Microsoft® Outlook, to determine if your PST files are corrupt before uploading the data to ensure the ingestion of the PST's into the archive.
- A message size limit of 50 MB is applicable for imported and journaled email messages. Any oversized messages will not be imported. A report is provided for any message that exceeds this limit.
- Non-email items such as drafts, tasks, and calendar entries are not imported. Read receipts and calendar notice acceptances can be imported.

The **Import Data** feature is available for administrators of those customers for whom the **Enable Import Data** check-box is selected while creating or updating the customer. The users who have the Import Data privilege can view the **Import Data** option.

Note: Summary and detailed report for the uploaded PST and ZIP files with the count and size of emails imported is available in the reports section of Manage Archive. See [“Generating a Messaging Report”](#) on page 170..

Importing data into archives

Before you use the **Import Data** feature, note that:

- The **Import Data** feature is available for administrators of those customers for whom the **Enable Import Data** option is selected while creating or updating customer details. The users who have the Import Data privilege can view the **Import Data** option.
- The yearly quota limit indicator is available that indicates the available data limit for the current year and the consumed limit. The in-progress upload data is considered as a consumed limit. In case of upload failure for upload in-progress files, the data is added back to the available limit within 5 to 10 minutes of the upload failure. (The duration of the yearly quota period is considered from January 1 to December 31.)
- When you consume the data limit you are entitled, you would be notified when you attempt to upload a file.
- Only PST, MSG, and EML files can be imported. To import the MSG and EML files, you must create a ZIP file.
- While uploading a ZIP file, the application does not identify its actual content size. The quota limit changes as per the actual data size imported. It is recommended to check and ensure the actual content size manually while creating a ZIP file. Else, the import batch may fail due to exceeded quota limit.
- You can select and upload multiple PST and ZIP files simultaneously.
- You can select multiple PST files and/or one CSV file. If the CSV file has a valid account mapping, then account IDs automatically populate on the user interface, along with the valid PST file name. Only PST files are displayed on the user interface.
- For PST files, the messages are archived in sender's and recipients' archives by default.
- For PST files, you can archive messages in the PST owner's archive.
In this case, an account must be mapped with the specified email address of the PST owner. If required, create an account for the PST owner's email address in the Veritas Alta View Compliance and Governance Management Console Console.

To import data into archives

- 1 On the Veritas Alta View Compliance and Governance Management Console console, in the left navigation pane, click **Import Data**.

Note: You must launch **Import Data** from the Veritas Alta View Compliance and Governance Management Console Console. Never use a direct URL of **Import Data**.

If you have uploaded data earlier using **Import Data**, the import data page displays the details about the uploaded PST and ZIP (MSG and EML) files and the status of upload process. Else, the page does not show any record.

- 2 On the top-right corner of the page, the application displays the available limit for uploading the files. Ensure that you have sufficient limit available for uploading the files.

The screenshot shows the 'Import Data' page in the Veritas Alta View console. The left sidebar contains a navigation menu with options like 'Archive Overview', 'Configuration', 'Dashboard', 'Archive Collectors', 'Role Management', 'Policy Management', 'Retention Management', 'Reports and Notifications', 'Classification', and 'Import Data'. The 'Import Data' option is selected. The main content area has a header 'Import Data' and a sub-header 'Available limit for upload' which states '12288 MB available of 12288 MB yearly quota. 0 MB data upload is in progress.' Below this is a table with columns: File name, Import Type, ID, Status, File size, and Uploaded on. The table contains several rows of data, including files like 'mypst.pst', 'punitmpasas@anandmishraonmicrosof.com.pst', 'punitmpasas@anandmishraonmicrosof.com.pst', 'punitmp.pst', and 'punitmp.pst'. The status of these files is either 'Error' or 'Import complete'. At the bottom of the table, there is a pagination control showing 'Items per page: 5' and '1 - 5 of 10'.

- 3 Click **Import**.

The application displays the **Upload PST or ZIP(MSG/EML) file and import data** page.

- 4 To browse for the files that you want to upload, either click **Add upload items** or click **Browse**. Search for and select the required files.

Note: The application displays a list of selected PST, ZIP, and CSV files. You can upload multiple PST and ZIP (MSG and EML) files, and one CSV mapping files simultaneously.

To remove the files that are added but do not need to be uploaded for some reason, click the **Delete** icon in the corresponding row.

- 5 In the **Import Type** column, do the following:
 - If you have selected a PST file for uploading, ensure that the **Import Type** is displayed as PST by default.

The list of PST files is displayed along with the mapped email IDs that are populated in the **Owner Email** field from the selected CSV file.
 - If you have selected a ZIP file for uploading, select the **Import Type** as MSG or EML.

For example, if the ZIP file contains the MSG files, you must select Import type as MSG. If the ZIP file contains the EML files, you must select Import type as EML.
 - If you have selected the CSV mapping file and if that file finds a valid PST and Account ID, then the account email ID appears in the **Owner Email** field.

You can select or clear this check box for your entries and update the owner email field.
- 6 In the **Journal Address** column, select an appropriate journal address for each item.
- 7 By default, the **Archive message in sender's and recipients' archive** check box is selected for all the selected files.

If you clear this check box, the application displays the following error message.

At least one archive option should be selected to process the PST file.
- 8 Select the **Archive messages in PST owner's archive** check box if you need to archive messages in the PST owner's archive along with the sender's and recipients' archive.
- 9 Ensure that all the error messages for the selected messages are resolved. Else, the **Upload** button remains disabled.
- 10 Click **Upload** to send the file to the server, and do not refresh the page during the upload of the files.

The **Import Data** page displays the status of files that you have uploaded.
- 11 Expand individual rows to view the import history of items uploaded. It provides details such as import start and end dates, total items in a file, number of items imported, number of items failed, number of non-email items, number of oversized items, and error messages if any.

The following statuses are shown with file entry:

Status	Description
Upload in progress	Uploading the files
Upload complete	File upload process completed.
Import in progress	File is in import process.
Queued For import	Job is in queue and waiting to be picked for Import process.
Error	Error occurred while importing file.
Import complete	All found items are imported.
Import partially successful	All found items are not imported (contains some non email items or failed to import some items or oversized items).

Note: Summary and detailed report for the uploaded PST and ZIP files with the count and size of emails imported is available in the reports section of Veritas Alta View Compliance and Governance Management Console console. See [“Generating a Messaging Report”](#) on page 170..

AD FS Configuration Guide

This chapter includes the following topics:

- [Configuring AD FS to work with Veritas Alta Archiving](#)
- [Adding a relying party trust for Veritas Alta Archiving](#)
- [Generating a token-signing certificate](#)

Configuring AD FS to work with Veritas Alta Archiving

This section describes how to configure your Active Directory Federation Services (AD FS) environment to work with the Veritas Alta Archiving authentication service. After you configure your AD FS environment and the Veritas Alta Archiving authentication service, you can provide single sign-on access to Veritas Alta Personal Archive users.

For information about the supported AD FS versions, see the [Veritas Alta Archiving Compatibility List](#).

Note: These instructions apply to the provision of single sign-on access for Alta Personal Archive users only. For assistance with the provision for Alta eDiscovery and Veritas Alta View Compliance and Governance Management Console, contact [Veritas Services & Support](#).

The following table describes the required steps to configure AD FS to work with the Veritas Alta Archiving authentication service.

Table 14-1 Steps to configure AD FS to work with the Veritas Alta Archiving authentication service

Action	Reference
Use the AD FS Management Console to add a relying party trust for Veritas Alta Archiving.	See “ Adding a relying party trust for Veritas Alta Archiving ” on page 196.
Generate and export a token-signing certificate from the AD FS Management Console for upload in Veritas Alta View Compliance and Governance Management Console.	See “ Generating a token-signing certificate ” on page 199.

These instructions do not provide information on how to set up your AD FS environment. Refer to the following Microsoft documentation for information on to set up your AD FS environment:

- [AD FS 2.0 \(Windows Server 2008 R2\)](#)
- [AD FS 2.1 \(Windows Server 2012\)](#)
- [AD FS 3.0 \(Windows Server 2012 R2\)](#)

Network clock synchronization requirements for SSO

Veritas Alta Archiving honors the **NotBefore** and **NotOnOrAfter** conditions that are presented during Secure Assertion authentication and authorization exchanges.

We recommend that you review your SSO Authority/Identity Provider settings to understand the values that are presented to Veritas Alta Archiving during the SAML exchange. You need to ensure that the **NotBefore** and **NotOnOrAfter** values and drift values are configured in a way that is secure but that does not inadvertently cause authentication issues. Veritas Alta Archiving synchronizes with several external UTC time sources and we recommend that you do the same to minimize the drift between our networks. Refer to your Microsoft documentation for information about configuring these values in an AD FS environment.

For information on how to set a **NotBeforeSkew** condition to allow for time discrepancies, see the following article on our Support website:

<http://www.veritas.com/docs/000097921>

Adding a relying party trust for Veritas Alta Archiving

The first step to configure your AD FS environment is to add a relying party trust for Veritas Alta Archiving.

Note: We recommend that you do not change the Index Value of the Endpoint from its default value. Changing the Index Value of the Endpoint can prevent the Veritas Alta Archiving authentication service from working properly with your AD FS environment.

To add a relying party trust for Veritas Alta Archiving

- 1 Access the **AD FS Management** console.
- 2 In the left pane of the AD FS Management console, expand **Trust Relationships**, right-click **Relying Party Trusts**, and then click **Add Relying Party Trust**.
- 3 In the **Welcome** panel of the Add Relying Party Trust Wizard, click **Start**.
- 4 In the **Select Data Source** panel, select **Enter data about the relying party manually**, and then click **Next**.
- 5 In the **Specify Display Name** panel, enter **Cloud Archive** in the **Display Name** field, and then click **Next**.
- 6 In the **Choose Profile** panel, select a profile, and then click **Next**.
- 7 In the **Configure Certificate** panel, click **Next** to skip this optional step.

Note: We recommend that you do not configure a certificate. Configuring a certificate prevents the Veritas Alta Archiving authentication service from working properly with your AD FS environment.

- 8 In the **Configure URL** panel, select **Enable support for the SAML 2.0 WebSSO protocol**.
- 9 In the **Configure URL** panel, enter the Entity ID from the **Your Trust Information** section on the **Authentication Management** page of Veritas Alta View Compliance and Governance Management Console in the **Relying party SAML 2.0 SSO service URL** field, and then click **Next**.

Note: The Entity ID varies based on the location of your organization. If you cannot find the Entity ID for your organization, contact [Veritas Services & Support](#).

- 10 In the **Configure Identifiers** panel, enter the Entity ID again in the **Relying party trust identifier** field, click **Add** to add the identifier, and then click **Next**.

- 11 For AD FS 3.0 only, in the **Configure Multi-factor Authentication Now?** panel, select **I do not want to configure multi-factor authentication settings for this relying party trust at this time**, and then click **Next**.
- 12 In the **Choose Issuance Authorization Rules** panel, select **Permit all users to access this relying party**, and then click **Next**.
- 13 In the **Ready to Add Trust** panel, review the configured settings, and then click **Next**.
- 14 In the **Finish** panel, select **Open the Edit Claim Rules dialog for this relying party trust when the wizard closes**, and then click **Close**.
- 15 In the **Edit Claim Rules for Cloud Archive** window, click **Add Rule**.
- 16 In the **Select Rule Template** panel of the Add Transform Claim Rule Wizard, select **Send LDAP Attributes as Claims** in the **Claim rule template** field, and then click **Next**.
- 17 In the **Configure Rule** panel, enter **Send Claims to Cloud Archive** in the **Claim rule name** section.
- 18 In the **Configure Rule** panel, select **Active Directory** in the **Attribute store** section.
- 19 In the **Configure Rule** panel, select the following sets of LDAP attributes and outgoing claim types in the **Mapping of LDAP attributes to outgoing claim types** section.

LDAP attribute	Outgoing claim type
E-Mail-Addresses	E-Mail Address
Given-Name	Given Name
Surname	Surname

- 20 In the **Configure Rule** panel, click **Finish** to close the **Add Transform Claim Rule Wizard**.
- 21 In the **Edit Claim Rules for Cloud Archive** window, click **OK** to close the window.
- 22 In the AD FS Management Console, select **Cloud Archive** in the **Relying Party Trusts** pane.
- 23 In the **Cloud Archive** section of the **Actions** pane, click **Properties**.
- 24 In the **Cloud Archive Properties** window, select the **Advanced** tab.
- 25 In the **Secure hash algorithm** field, select one of the following algorithms:

- SHA-1
- SHA-256

Note: We recommend that you select the SHA-1 algorithm.

26 Click **OK** to close the **Cloud Archive Properties** window.

Generating a token-signing certificate

The second step to configure your AD FS environment is to generate a token-signing certificate for upload on the Authentication Management page in Veritas Alta View Compliance and Governance Management Console.

Note: We recommend that you use the default key size for the certificate, which is 2048 bits. The largest certificate key size that we currently support is 4096 bits.

To generate a token signing certificate

- 1 Do one of the following to access the AD FS Management console:
 - For AD FS 2.0 click **Start**, select **Administrative Tools**, and then click **AD FS 2.0 Management**.
 - For AD FS 2.1, click **Start**, enter **AD FS Management** in the **Search** field, and then press **Enter**.
 - For AD FS 3.0, click **Tools** in **Server Manager**, and then select **AD FS Management**.
- 2 In the left pane of the AD FS Management console, expand **Service**, and then select **Certificates**.
- 3 In the **Certificates** pane, select the certificate that is listed under the Token-signing section.
- 4 In the **Actions** pane, click **View Certificate**.
- 5 In the **Certificate** window, select the **Details** tab, and then click **Copy to File**.
- 6 In the **Welcome** panel of the Certificate Export Wizard, click **Next**.
- 7 In the **Export File Format** panel, select **Base-64 encoded X.509 (.CER)**, and then click **Next**.
- 8 In the **File to Export** panel, enter a file path in the **File Name** field, and then click **Next**.

- 9** In the **Completion** panel, review the specified information, and then click **Finish**.
- 10** Click **OK** to close the export confirmation dialog box. You can find the exported certificate in the file location you previously designated.

Alta Personal Archive Deployment for IBM Notes

This chapter includes the following topics:

- [Alta Personal Archive deployment for IBM Notes](#)

Alta Personal Archive deployment for IBM Notes

From IBM Notes, users can access the Internet using the Notes browser or Notes with Internet Explorer. The functionality lets Notes users access Alta Personal Archive from within the Notes application. Using the Active Directory Group Policies in a Microsoft Windows environment, you can deploy the Alta Personal Archive access URL to Notes users as a Favorite.

Note: You must be familiar with basic Active Directory concepts such as managing Group Policies to deploy the Alta Personal Archive access URL. We recommend that you test the deployment on a group of test users before deploying the access URL to all users.

To deploy the Alta Personal Archive access URL

- 1 In the **Group Policy Management** console, expand **User Configuration** and then expand **Internet Explorer Maintenance**.
- 2 In **Internet Explorer Maintenance**, select **URLs**.
- 3 In the right pane, double-click **Favorites and Links**.

- 4 In the **Favorites and Links** window, click **Add URL**.

Note: Do not select **Place favorites and links at the top of the list in the order specified below**.

- 5 In the **Details** window, enter **Alta Personal Archive** in the **Name** field and then enter the Alta Personal Archive access URL in the **URL** field.
- 6 Click **OK** to close the **Details** window and then close the **Favorites and Links** window.

Archive Administration Updates in Previous Releases

This chapter includes the following topics:

- [About the updates for previous releases](#)

About the updates for previous releases

The introduction to this help includes a description of the most recent updates for Veritas Alta View Compliance and Governance Management Console:

See “[About Veritas Alta View Compliance and Governance Management Console](#)” on page 8.

For full details of all the updates in each release of the Veritas Alta Archiving service suite, see the Veritas Alta Archiving release notes. You can access the release notes from the following article on the Veritas Support website:

https://www.veritas.com/support/en_US/article.100040129