Getting started

This section includes the following topics:

About Arctera Insight Management Console

Arctera Insight 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 Arctera Insight Archiving.

.

Arctera Insight Management Console is a web-hosted interface that enables administrators to configure and manage Arctera Insight Archiving and perform the following tasks:

- Provision and manage Arctera Insight 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 Arctera Insight Management Console include the following enhancements:

- With the Import Data feature in Arctera Insight 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 Arctera Insight Management Console.
- Administrators can remotely manage account provisioning and sync users from CloudLink, Microsoft Office 365, or Google Workspace, and SCIM. If users exist solely in one environment, their archives will not be overwritten or removed during synchronization.
- Administrators can configure the Privilege Delete archive options and determine whether Insight eDiscovery Administrator is enabled to delete emails in Insight 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 Insight eDiscovery Administrator role.
- With the enhancements in reports, administrators can now create a Insight 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.
- The application supports multi-factor authentication (MFA). The email-based authentication and the Time-based One Time Password (TOTP) authentication enhances the access and data security of Management Console.
- The New Features window displays users the latest release updates for all Arctera Insight Archiving applications every time they log in. It can be disabled or enabled for users, if needed.

Information about the changes that were included with earlier releases of Arctera Insight Management Console is provided elsewhere in this help.

For details of all the updates in each release of the Arctera Insight Archiving service suite, see the Arctera Insight Archiving Platform Documentation.

Prerequisites for using Arctera Insight Management Console

To use Arctera Insight Management Console, you need the following:

- Your Arctera Insight Management Console URL.
- Your Arctera Insight Archiving user name.
- Your Arctera Insight Archiving password.
- Access permission to use Arctera Insight Management Console.

> “ ”

Note: Contact your administrator if you do not have this information or you need access permission for Arctera Insight Management Console.

> “ ”

Arctera Insight Management Console web browser support

Arctera Insight Management Console supports the web browsers that are listed in the Arctera Insight Archiving Compatibility List. You can obtain the Compatibility List from this article on the Arctera Support website.

What's new in this release

Arctera constantly works on improving the Arctera Insight 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 Arctera Insight Archiving Platform Documentation.

Signing in to Arctera Insight Management Console

Before you access Arctera Insight Management Console, you must log in using your Arctera Insight Archiving credentials.

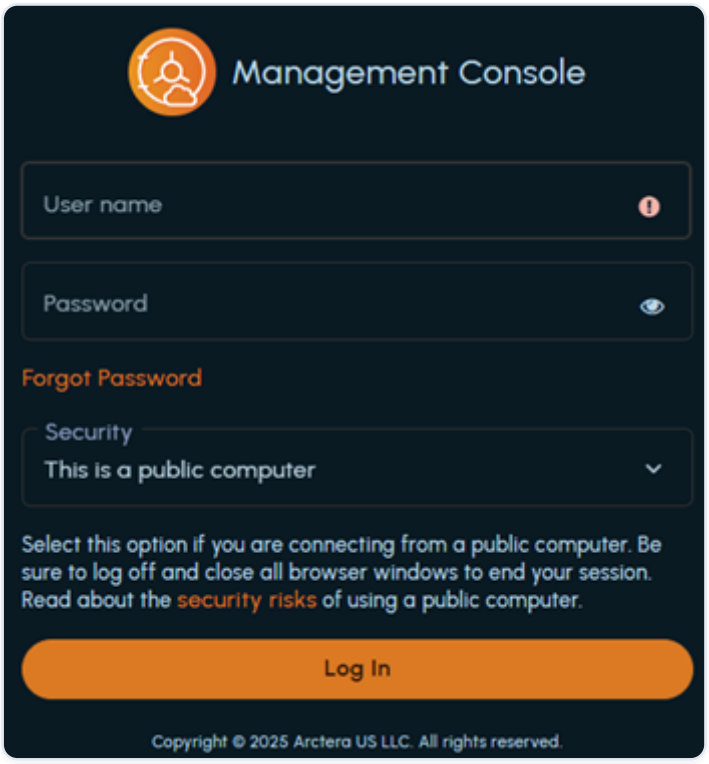
To log in to Arctera Insight Management Console

1. In a supported browser, enter the Arctera Insight Management Console URL.

   > “ ”

   Note: Contact your administrator if you do not know your Arctera Insight Management Console URL or you need access permission for Arctera Insight Management Console. For more information on supported browsers, seeArctera Insight 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. SeeResetting a forgotten password.

   > “ ”

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

Refer to the following table for more information:

THIS IS A PUBLIC COMPUTER	**ARCTERA INSIGHT 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	Arctera Insight 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 Arctera Insight Management Console.
	Arctera Insight 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.

THIS IS A PUBLIC COMPUTER	ARCTERA INSIGHT 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.
	- Click End to end the session.

1. Click **Sign In**.
2. If the multi-factor authentication (MFA) is enabled for you, the **OTP** field appears on the authentication screen.

This email-based authentication and the Time-based One Time Password (TOTP) authentication enhances the access and data security of Management Console. Administrators have the permission to enable or disable multi-factor authentication at the user and tenant level.

- If the **email-based authentication** (EML) is enabled for you, a one-time password (OTP) is sent to your registered email address for authentication and access to the application. This OTP remains valid for 5 minutes from the time of receiving the email.

Manually enter the OTP on the authentication screen within 5 minutes. Copy-pasting the OTP is not allowed. If you fail to provide OTP within 5 minutes of receiving it, the application displays a message that the OTP has expired. To obtain a new OTP, click **Resend OTP**. The application sends a new OTP.

- If the **Time-based One Time Password authentication**(TOTP) is enabled for you, the application redirects you to an**Authenticator Setup** page.

Scan the QR Code using the Google or Microsoft **Authenticator** app on your mobile phone at the time of your first login

Configure the Authenticator app on your mobile phone. See Configuring the Authenticator app on your mobile phone.

Click **Continue** to get a time-based OTP in the Authenticator app.

Enter that OTP in the **OTP**field of the Authentication page, and click**Continue**.

Configuring the Authenticator app on your mobile phone

If you have previously created an account for same user, please remove that entry and attempt to complete the setup again.

To install the Microsoft Authenticator app on your phone

1. While installing the app, if prompted, allow notifications about the app.
2. Upon installation, open the app and click the plus (+) icon at top and select **Work or School account**or**Other account**.
3. Add your work account by using any of the following methods:
    - Use the installed authenticator app to scan the QR Code provided on the authentication page of Arctera Insight Archiving application.
    - Sign in with your application credentials and follow the screen instructions.

Upon successful scanning or signing in, your account gets connected to Microsoft Authenticator.

To install the Google Authenticator app on your phone

1. While installing the app, if prompted, allow notifications about the app.
2. Upon installation, log in with your Google account credentials. Scroll down and click the plus (+) icon.
3. Scan the QR Code with the Google Authenticator app. Your account gets connected to the Google Authenticator app.

Resetting the Authenticator device for users

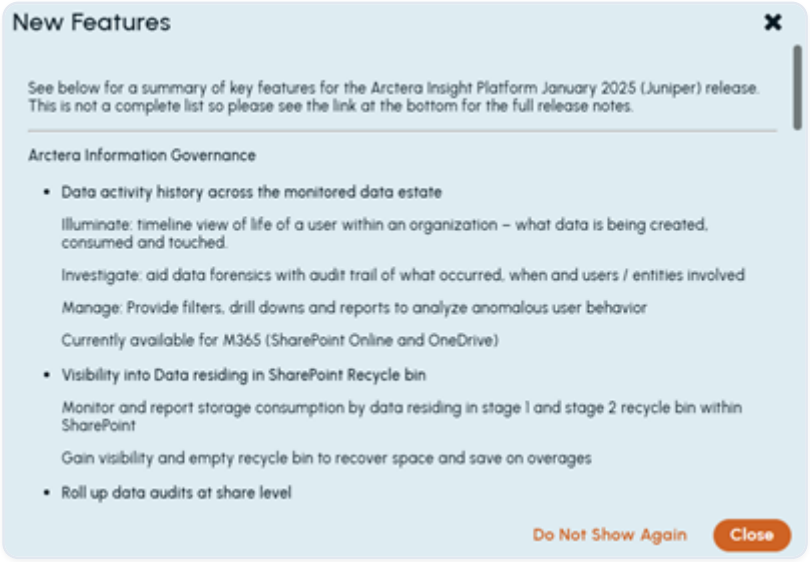
As an administrator, you can reset the Authenticator device for users if the user accidently removes the account from authenticator app or misplaces the device on which the app is installed. Users can request you to setting up a new device at the next login.

To reset the Authenticator device for a user

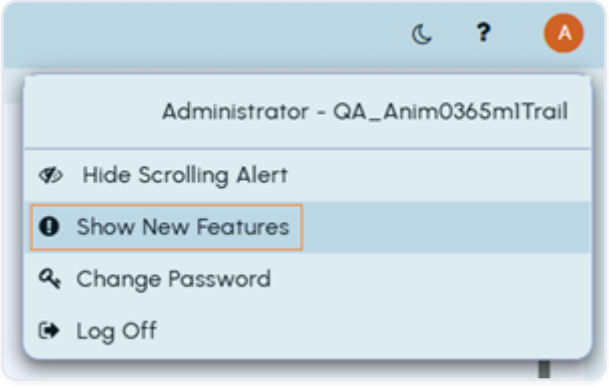
1. On the Arctera Insight Management Console, select **Configuration**>**Account Management**.
2. Search for and select the account for which you want to reset the Authenticator device.
3. Click **Edit** to view the user account details.
4. Under the **Status**section, click**Remove**adjacent to the**Authenticator Device** field.

About the New Features updates

Upon successful sign-in, the New Features window appears, presenting the latest release updates for Arctera Insight Management Console, Insight eDiscovery, Insight Personal Archive, Insight Capture, and Insight Surveillance as shown in the sample image below.



- To temporarily hide this window, click Close.
- To access this window later, click the profile icon and choose Show New Features.



- To permanently hide this window, click Do Not Show Again. Subsequently, upon next login, this window will no longer appear. To enable its visibility, contact your system administrator. However, it will reappear automatically with the next release updates.
- To read the complete release notes document, click View Detailed Release Notes.

Signing out from Arctera Insight 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, Arctera Insight Management Console can help you by sending a Reset Password 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.

1. Click **Send**.

The application sends you an email with a reset password link. Check your email inbox, including the spam or junk folder, for this message. This link expires after 30 minutes from you receive the email.

1. Open the password reset email and click on the provided **Reset Password** link.

The application directs you to a **Reset Password** page.

1. Type your user name, a new password, retype to confirm it, and click **Submit**.

After successful reset, 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 Arctera Insight 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.

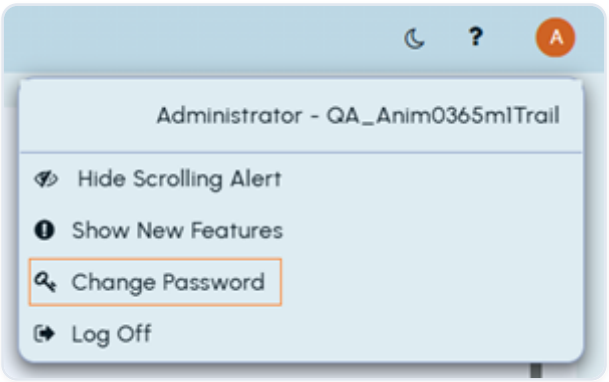
> “ ”

Note: Changing your password for Arctera Insight Management Console also changes your password for other Arctera Insight 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 section includes the following topics:

About Archive Overview

The Archive Overview page automatically displays when you log on to Arctera Insight Management Console. This page provides general information and usage statistics for Arctera Insight 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 Arctera 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 Arctera Insight Management 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 Arctera to logon to Manage and clickAcknowledgeon 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.
- To view the latest status of your provisioned archive collectors, click see details. The application navigates you to the Archive Collector page.
- Roles
- The delegated roles to which your account is assigned.

Archive Usage

This page provides contact details that Arctera 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. In the left navigation pane, select **Archive Overview**.
2. On the **Archive Usage**tab, click**Edit Contact Details**.
3. Click **Edit** to enable the page for editing.
4. 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.

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 Arctera Insight Management Console . When the alert is acknowledged, the Service Alert does not pop up again on subsequent logons into Arctera Insight Management 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 Arctera to logon to Arctera Insight Management Console and clickAcknowledgeon 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 Arctera Insight 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 Arctera Insight 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 section includes the following topics:

About dashboard

To view the dashboard, ensure you have Arctera Insight Archiving administrator privileges and that both the Insight Capture primary service and the necessary secondary services are enabled for your account. For example, if you are the administrator with the Insight Capture primary service enabled, and only the Viva Engage and Bloomberg secondary services are enabled, you can view and export statistical reports for Viva Engage and Bloomberg importers/collectors only. You will not be able to view statistics for importers/collectors of other secondary services that are not enabled.

Based on the services enabled for you, dashboard displays the following tabs:

- Archive tab

See Monitoring a status of active archives.

See Monitoring storage consumption.

- Capture tab

See Monitoring a status of Insight Capture collectors activities.

- Transcription tab
- AI Wallet

See Monitoring a status of AI Wallet usage.

> “ ”

Note: If you cannot view the tabs despite having the services enabled, please contact Arctera Support.

> “ ”

For more information about Insight Capture Dashboard, see Arctera Insight Capture Configuration Guide.

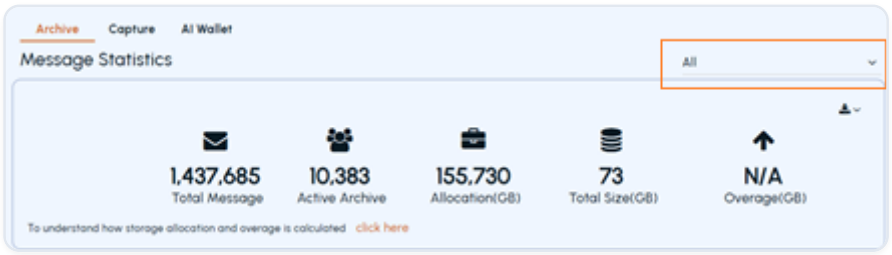
Monitoring a status of active archives

The Archive tab provides statistics about active archives, storage allocation, storage size, storage overage, and more. This statistical data can be exported for analysis or reporting purposes.

Each day, when the Archive dashboard is used to gather statistics for a specified duration, the application fetches only the initial call of the day to query Elasticsearch for data regarding each *date-groupID-period* combination. This data is then stored in a database. Subsequent calls for the same day retrieve data directly from the database, thereby enhancing the performance of the Archive Dashboard.

To monitor a status of active archives and export its statistical report

1. In the left navigation pane, click **Dashboard**and select the**Archive** tab.
2. In the top-right corner of the page, select the duration for which you want to view the archiving statistics.



By default, message statistics duration is set to ***All***, and display the**Overage**details. Upon selecting other predefined durations, the application hides the**Overage** details.

The following statistical data is displayed numerically and graphically. To view the message count in numbers and the corresponding percentage ratio, hover over the colored area of the chart.

> “ ”

Note: Refer to a sample image of theArchive tabcomponents for better visual reference.

> “ ”

MESSAGE STATISTICS
Total Messages
Active Archive
Allocation(GB)
Total Size
Overage(GB)
Distribution By Attachment
Count By Message Size
Distribution By Message Format Type
Count By Direction Type
Storage Consumption By Age
Active Archives Over 12 Months
Total Size Over 12 Months (in GB)
Top Mail Accounts (For Emails only)

1. Click the **Export** icon to export the report in Excel, PDF, CSV, or Word format.

Monitoring storage consumption

It is advisable to regularly monitor your storage utilization to ensure compliance with records retention policies and minimize additional storage costs. This process facilitates the evaluation of data longevity, enabling you to modify storage retention settings or perform a defensible manual data clean-up. In addition, it helps determine whether storage usage falls within the allocated Shared Storage Allowance.

To monitor storage consumption

1. In the left navigation pane, click **Dashboard**and select the**Archive** tab.
2. In the top-right corner of the **Message Statistics**section, select the***All*** option in the duration drop-down list.

> “ ”

Note: TheStorage Consumption By Agesection appears only if the message statistics duration is set toAll. For other predefined duration options, the application does not show this section.

> “ ”

The storage consumption chart is displayed and shows total and year-wise storage consumption (GB), helping make data-driven decisions.

Monitoring a status of Insight Capture collectors activities

The Capture tab provides activities of your Insight Capture collectors/importers for a specified duration. This statistical data can be exported in CSV file format for analysis or reporting purposes.

For more information about Insight Capture collectors/importers, see Arctera Insight Capture Configuration Guide.

To monitor a status of Insight Capture collectors activities and exporting its statistical report

1. In the left navigation pane, click **Dashboard**and select the**Capture** tab.

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 Insight Capture	This statistic provides information about the number of imported, excluded, and failed

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.
	messages in certain duration. For example, 7 days.
	You can print and download the charts as PNG, JPEG, PDF, and SVG Vector format.
Number of messages by importer	This statistic provides information about number of messages by each importer.

2. In the **Importers Jobs** pane, do the following:
    - In the **Collectors List** field, either select a specific collector to view data for that individual collector, or choose *All* to view statistics for all collectors simultaneously.
    - In the **Date Range** field, select the duration for which you want to export the statistics.
3. Click **Export to CSV**.

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

Monitoring a status of AI Wallet usage

The AI Wallet tab displays statistics for total AI units deposited, withdrawn, and the current balance, and lists recent AI-unit transactions from Arctera Insight Surveillance, Arctera Insight eDiscovery, and Arctera Insight Personal Archive across different services. This statistical data can be exported in CSV file format for analysis or reporting purposes.

To monitor a status of AI Units usage and exporting its statistical report

1. In the left navigation pane, click **Dashboard**and select the**AI Wallet** tab. Refer to a sample image for better visualization.

The header of the page provides the following details:

- **AI Units Deposited** \- cumulative units credited to the customer.

- **AI Units Withdrawn** \- cumulative units consumed by the customer.
- **AI Units Balance** \- remaining units available for the customer.

The tabbed transaction panel provides the following details:

- **Recent Withdrawals** \- This tab displays the five latest transactions/records. It includes the transaction date indicating when AI units were debited or credited, the name of the source application that consumed the AI units, and the feature responsible for the consumption. It also shows the number of AI units debited (in red) or credited (in green) and the resulting AI units balance after each transaction.
- **Recent Deposits** \- This tab displays the five latest transactions/records. It includes the transaction date when AI units were credited, the credit type (such as recharged or free credits), the number of AI units added (shown in green), and the updated AI units balance after each deposit.
- **Top Withdrawers** \- This tab displays the five latest records. It includes the user names and email addresses of the accounts that have consumed the highest number of AI units. It also shows the total AI units withdrawn by each user.

1. To check the detailed transaction report, select **Click Here**.

The application navigates you to the **AI Wallet Statement**tab on the**Usage Scorecard** page. Refer to a sample image for better visualization.

1. On the filter options pane, specify the criteria to get the statement.

FILTER FACET	DESCRIPTION
Select Duration	Select a predefined time period or a custom range for transactions.
Applications	Select all or a specific application for which you want the statement.
Features	Select all or a specific feature for which you want the statement.
	Currently, There are two options:
	- Audio Summary
	- InsightBooks

FILTER FACET	DESCRIPTION
Transaction Types	Select all or a specific transaction type for which you want the statement.
	Currently, There are two options:
	- Only deposits
	- Only withdrawal
Filter Accounts	Click Filter Accounts . The Add/Remove Accounts dialog box appears.
	Search for and select one or more accounts, and click Save . The count of selected accounts appears.

2. Click **Apply**.

The AI Wallet statement is generated based on the selected criteria.

Managing Configurations

This section includes the following topics:

About the Configuration page

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

- A list of the Arctera Insight 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 theUser Managementpage.

> “ ”

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 Arctera 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 the list to view the configured domains. If the list is extensive, use the search option to locate a specific domain instead of scrolling. You can also add new domains directly without contacting the support team. In addition, you can export the list of domains for further use. See Managing Domains.

Note: By default, this service is disabled. To enable it, contact your system administrator or the Arctera Support team. To add and update domains, the tenant must possess the Administrator role and must have the Archive Settings privilege.

- 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.

Managing Domains

Prerequisites:

- To add and update domains, the tenant must possess the *Administrator*role and must have the*Archive Settings* privilege.
- By default, this service is disabled. To enable it, contact your system administrator or the Arctera Support team.

Upon expanding the Domains section, you can:

- view the list of already configured domains.
- search for specific domains when the list is extensive.
- add new domains on your own.
- edit the existing domains
- export the list of domains for further use.

1. In the left navigation pane, select **Configuration**>**Services**.
2. **To view domains list**Expand the**Domains** section. The list displays details such as the domain name, indicator, hosting provider, notes, and option to edit the details.
3. **To search a required domain**In the**Search** box, type all or part of the domain name to quickly locate a specific entry. If the list is extensive, either choose the number of records you want the application to display per page or use navigation arrows at the bottom of the section for easy access to the first, previous, next, and last pages.
4. **To add new domain**Click**\+ Add New**in the upper-right corner of the section. Enter the required *domain name*,*Indicator*,*Hosting Provider*, and*notes* if needed in the fields provided. Click**Save** in the same row to add the new domain to the list.

A newly added domain first appears at the top of the list and is then placed in alphabetical order.

1. **To edit a domain**Click**Edit**in the same row to make the fields editable. You cannot modify the domain name. However, you can update the *Indicator*,*Hosting Provider*, and*Notes* fields as needed in the fields provided. Click**Save**.
2. To export a list of domains,

Click **Export** in the upper-right corner of the section to export the domain list in the CSV format for further use.

Selecting options to provision and manage user accounts

To select options to provision and manage user accounts

1. In the left navigation pane, select **Configuration**>**User Management**.
2. On the **User Management** page, select one of the following provisioning options:

You can provision and manage users in the following ways:

- Manually by using Arctera Insight Management Console

Use this option if you need to provision a small number of user accounts or prefer to manually create archive accounts in the Arctera Insight Management Console for each new user.

- Manually and remotely by using the following tools:
    - **On-premise CloudLink**

Use this option to provision user accounts from *Microsoft Active Directory*and*IBM Lotus Domino Directory*.

- **Microsoft Office 365**

Use this option to provision and manage user accounts from *Microsoft Office 365*.

See About Exchange Online Archiving.

- **Google Workspace**

Use this option to provision user accounts from *Google Workspace*.

See About Google Workspace Archiving.

- **System for Cross-domain Identity Management (SCIM)**

Use this option to provision and manage user accounts from across multiple applications and services.

See About SCIM Archiving.

Remote provisioning eliminates the need to manually create archive accounts in the Arctera Insight Management Console for each new user. When configured, it automatically synchronizes new users, and their archive accounts appear in the Arctera Insight Management Console. You can use one or more tools simultaneously.

> “ ”

Note: If users exist in only one environment, the user accounts synchronized through remote provisioning tools remain independent. Their archives cannot be overwritten or removed, even if they do not exist in another group. If users exist in a hybrid environment, you must select one or more remote provisioning tools. Otherwise, migrated users may not be provisioned correctly.

> “ ”

1. Click **Save**.
2. Click **Go To Next Step**.

Arctera Insight 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 remotely with CloudLink, Microsoft Office 365, Google Workspace, or System for Cross-domain Identity Management (SCIM), then you must use corresponding applications to configure the provisioning settings. Refer to the respective documentation for more information.

> “ ”

Complete the required options, as follows:

Table: Provisioning steps for account management with the console application

PROVISIONING STEP	REFERENCE FOR MORE INFORMATION
Configure the Insight Personal Archive deployment options	See Configuring the Insight Personal Archive deployment options .

PROVISIONING STEP	REFERENCE FOR MORE INFORMATION
Configure the administrator notification options	See Configuring the administrator notification options .

Configuring the Insight Personal Archive deployment options

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

To configure the Insight Personal Archive deployment provisioning options

1. In the left navigation pane of Arctera Insight Management Console, select **Configuration**>**Provisioning**.
2. Expand **Personal Archive Deployment Options** , near the bottom of the page.
3. Under **Personal Archive Access** , configure whether Arctera Insight Archiving automatically enables access to Insight 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 Arctera Insight 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 Arctera Insight Archiving, the options are as follows:

ENABLE PERSONAL ARCHIVE ACCESS AND SEND WELCOME MESSAGE	SELECT THIS OPTION TO ENABLE INSIGHT PERSONAL ARCHIVE ACCESS TO EACH ACCOUNT THAT IS PROVISIONED, AND TO ENABLE WELCOME MESSAGES TO BE SENT TO THE PROVISIONED USERS.
	BY DEFAULT THIS OPTION IS NOT SELECTED.
	IF YOU SELECT THIS OPTION YOU MUST SELECT ONE OF THE FOLLOWING 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.

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

ENABLE PERSONAL ARCHIVE ACCESS	SELECT THIS OPTION TO ENABLE INSIGHT PERSONAL ARCHIVE ACCESS TO EACH ACCOUNT THAT IS PROVISIONED.
	BY DEFAULT THIS OPTION IS NOT SELECTED.
	IF YOU SELECT THIS OPTION YOU CAN CHOOSE WHETHER ARCTERA INSIGHT ARCHIVING SENDS WELCOME MESSAGES TO PROVISIONED USERS:
- Send Welcome Message	Select this option to enable welcome messages to be sent to the provisioned users.
	By default this option is not selected for new configurations.

ENABLE PERSONAL ARCHIVE ACCESS	SELECT THIS OPTION TO ENABLE INSIGHT PERSONAL ARCHIVE ACCESS TO EACH ACCOUNT THAT IS PROVISIONED.
	BY DEFAULT THIS OPTION IS NOT SELECTED.
	IF YOU SELECT THIS OPTION YOU CAN CHOOSE WHETHER ARCTERA INSIGHT ARCHIVING SENDS WELCOME MESSAGES TO PROVISIONED USERS:
	If you select this option you must select one of the following 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 an account, even if a welcome message was sent previously.

1. 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 Arctera Insight Archiving provisions new archive accounts.

SELECT TEMPLATE	SELECT ACCOUNT TO CONFIGURE THE WELCOME MESSAGE TEMPLATE FOR PROVISIONED USERS.
	SELECT ADMINISTRATOR TO CONFIGURE THE ADMINISTRATORS' NOTIFICATION MESSAGE.
From	Enter the sender email address for the message.

SELECT TEMPLATE	SELECT ACCOUNT TO CONFIGURE THE WELCOME MESSAGE TEMPLATE FOR PROVISIONED USERS.
	SELECT ADMINISTRATOR TO CONFIGURE THE ADMINISTRATORS' NOTIFICATION MESSAGE.
Subject	Enter the information you want saved as the subject for the message email.
Body	Edit the body text for the message.
	You can use the following macros that Arctera Insight Archiving replaces with the relevant information, based on archive information:
	- {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

2. 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 Arctera Insight Management Console, Select **Configuration**>**Provisioning**.
2. Expand **Notification Options** , near the bottom of the page.

3. Under **Administration Roles to Notify** , select the Arctera Insight Archiving administration roles that you want to receive the administrators' notification message when Arctera Insight 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 Arctera Insight Management 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 Arctera Insight Archiving.

Table: Tasks with managed tags lists the tasks that you can perform that are related to managed tags:

Table: Tasks with managed tags

TASK	REFERENCE
Create new managed tags.	See Creating a managed tag .
Assign managed tags to users.	See Editing managed tags .
Change the retention policy that is associated with a managed tag.	See Changing the retention policy associated with a managed tag .
Edit and delete managed tags.	See Deleting a managed tag .

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. SeeCreating a retention policy.

    > “ ”

4. Click **Assign Policy** to associate a retention policy with the managed tag.

The **Retention Policies** dialog box appears.

> “ ”

Note: To clear thePolicy Namefield, clickRemove Policy.

> “ ”

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

The currently available options:

- All
- Distribution Lists
- Tags
- Active Directory Groups

This option allows customers who sync Azure Active Directory groups using **Active Directory Group synchronization**or**SCIM Group Sync** to use group membership information for retention.

It is recommended to associate all users assigned Managed Tags when a policy is set to target Active Directory Groups. Managed Tags are applied to items based on group membership at the time the items are received when managed tags are associated to the policy. When the Managed Tags are not associated, the group membership is evaluated only at the time of item expiry.

> “ ”

Note: Administrators, reviewers, and users cannot view emails linked to this tag or remove the tag from emails unless they are explicitly granted permissions. To allow permission, SeeEditing managed tags.

> “ ”

1. 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.

2. Click **Save**.

Editing managed tags

When creating a managed tag, you cannot assign users or set permissions to allow them to view emails linked to managed tag or remove the tag from emails. Administrators, reviewers, and users cannot view emails linked to this tag or remove the tag from emails unless they are explicitly granted permissions. Therefore, you need to edit the tag to specify users and set permissions for them.

> “ ”

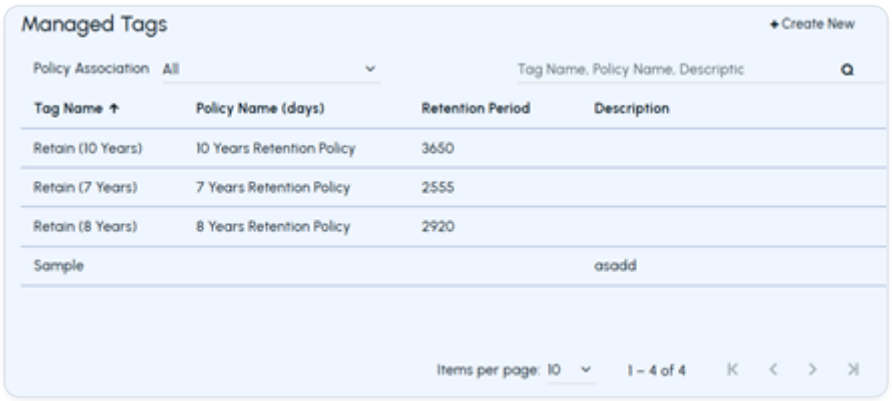
Note: If no permissions are set, only you (the creator of the managed tag) can view emails linked to it or remove the tag from emails.

> “ ”

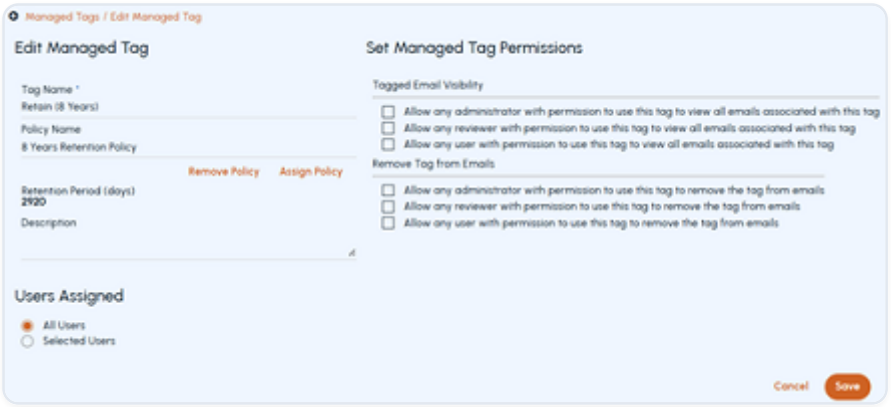
Besides this, you can also modify the tag name, assign or remove policies to the tag.

To edit a managed tag

1. In the left navigation pane, select **Configuration**>**Managed Tags**.
2. On the **Managed Tags** page, click on the tag to edit its details.



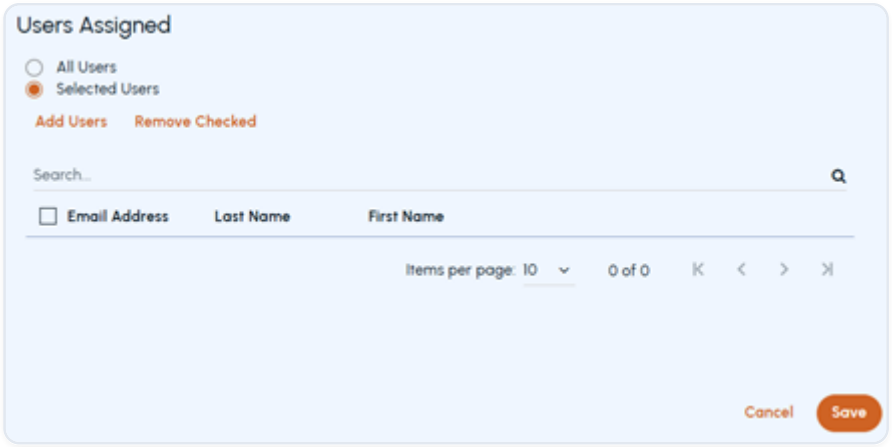
Tag details appear as shown in the sample image below.



1. In the **Tag Name** field, modify the tag name if needed.
2. In the **Policy Name** field, if the policy is already assigned, the policy name is displayed. One tag can have only one policy assigned. You cannot assign multiple policies to one tag.
    - To change the existing policy, click **Assign Policy**. See Associating a retention policy with a policy target.
    - To remove the already assigned policy, click **Remove Policy**.

The retention period and description defined in the policy associated with the tag is displayed.

1. Under **Users Assigned**section, select**Selected Users** to specify tag users.



    - To add new users, click **Add Users** , and select the required users from the list.
    - To remove users who are already added, select the users and click **Remove Checked**.**Note**: Removing a user prevents them from viewing messages assigned to that tag. The application displays a confirmation prompt. Click**OK**to confirm or**Cancel** to stop the removal.
2. Set managed tag permissions as needed.
    - Under **Tagged Email Visibility** , select who can view emails linked to this managed tag. Select one or more options mentioned below.

    - Select to allow all administrators with permission to use this tag.
    - Select to allow all reviewers with permission to use this tag.
    - Select to allow all users with permission to use this tag.

- Under **Remove Tag from Emails** , select who can remove this tag from emails. Select one or more options mentioned below.
    - Select to allow all administrators with permission to use this tag.
    - Select to allow all reviewers with permission to use this tag.
    - Select to allow all users with permission to use this tag.

3. 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**.
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.

1. Click **Remove Policy** to disassociate the retention policy from the managed tag.
2. Click **Save**.

About Account Management

From the Account Management page, you can manage archive accounts for Arctera Insight Archiving.

Table: Account management tasks lists the tasks that you can perform from the Account Management page, and where to find more information.

Table: Account management tasks

TASK	REFERENCE
Search for archive accounts	See Searching for archive accounts .
Filter the listed archive accounts	See Using search filters .
Create new archive accounts	See Creating an archive account .
View the details of an archive account	See Viewing and editing the archive account details .
	See About the Account Details page .
Edit an archive account	See Editing an archive account .
Delete an archive account	See Deleting an archive account .
Deploy users	See Deploying users .
Remove user access	See Removing user access .
Enable services for existing archive accounts	See Enabling services for existing archive accounts .
Edit Mobile Web Access permissions for existing archive accounts	See Editing Mobile Web Access permission for existing archive accounts .

TASK	REFERENCE
Export archive account information	See Exporting archive account information .
Unlock archive accounts	See Unlocking an archive account .

Searching for archive accounts

The Account Management page lists the archive accounts for your organization. If you have a large number of archive accounts, the accounts are displayed on multiple pages. You can scroll through the pages using the controls as the bottom of the main pane.

A Quick Search and an Advanced Search are available to let you search for specific archive accounts. Advanced Search lets you search according to the role that is assigned to the account, or according to other Arctera Insight Archiving access options.

To use Quick Search

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

The application displays a list of archive accounts.

1. In the **Search** field, enter the user name or email address that is associated with the archive account.
2. Click the **Search** icon.

To use Advanced Search

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

The application displays a list of archive accounts.

1. 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.

EMAIL ADDRESS OR ALIAS	ENTER AN EMAIL ADDRESS OR ASSOCIATED ALIAS EMAIL ADDRESS FOR THE USER.
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 Insight Personal Archive enabled.
Discovery Archive Access	Select if the user has access to Insight 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.
Arctera Insight 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 Arctera Insight Archiving.

2. 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.

1. Click **Custom Filters**,**Distribution Lists**, or**Dynamic Distribution Lists**.
2. Select a filter from the chosen group.
3. Click the **Apply** icon.

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

1. 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**.
2. Click **Archives**>**New Archive**.
3. On the **Accounts**page, under**Archive Detail** , provide the following details:

EMAIL ADDRESS	ENTER THE PRIMARY EMAIL ADDRESS FOR THE USER.
	NOTE: IF YOUR ORGANIZATION HAS MORE THAN ONE DOMAIN, SELECT THE CORRECT DOMAIN FROM THE DROP-DOWN LIST.
First Name	Enter the first name of the user.
Last Name	Enter the last name of the user.

EMAIL ADDRESS	ENTER THE PRIMARY EMAIL ADDRESS FOR THE USER.
	NOTE: IF YOUR ORGANIZATION HAS MORE THAN ONE DOMAIN, SELECT THE CORRECT DOMAIN FROM THE DROP-DOWN LIST.
User Name	The user name for the account. By default Arctera Insight Management Console uses the email address as the user name, but you can change it if you want.
Password	Enter a password for the user that meets the password policy requirements for your organization.
	See Configuring an advanced password policy .
	Note: This option does not appear if you selectedEnable Personal Archive Access and send Welcome MessageunderProvisioning>Personal Archive Deployment Options>Personal Archive Access. In that case, Arctera Insight Management Console generates a password automatically to send to the user.
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

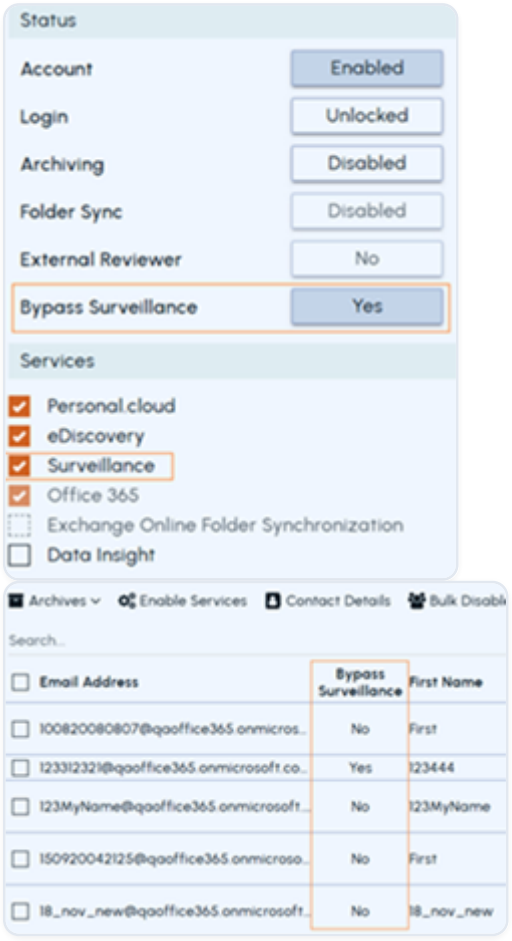
EMAIL ADDRESS	**ENTER THE PRIMARY EMAIL ADDRESS FOR THE USER.**
	NOTE: IF YOUR ORGANIZATION HAS MORE THAN ONE DOMAIN, SELECT THE CORRECT DOMAIN FROM THE DROP-DOWN LIST.
	Supervision primary service is enabled, and not for all customers. If the Advanced Supervision primary service is not enabled, the Arctera Insight Management 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 Arctera Insight Management 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,

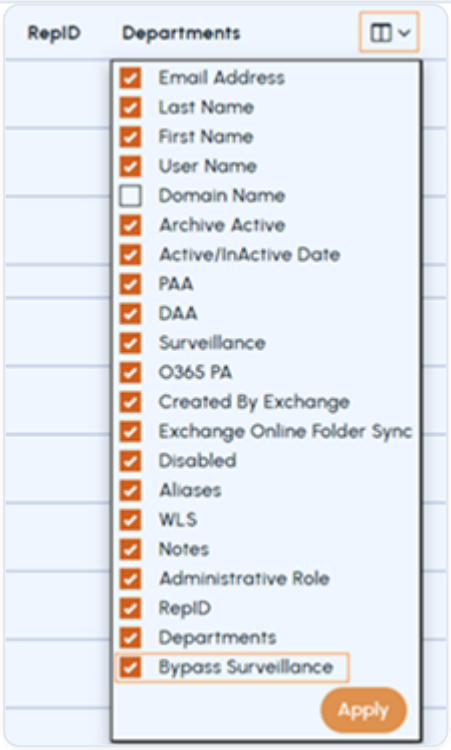
EMAIL ADDRESS	ENTER THE PRIMARY EMAIL ADDRESS FOR THE USER.
	NOTE: IF YOUR ORGANIZATION HAS MORE THAN ONE DOMAIN, SELECT THE CORRECT DOMAIN FROM THE DROP-DOWN LIST.
	the Arctera Insight Management Console does not display this option.
	After you select this service, you can quickly access departments 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 Arctera Insight Management 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 Arctera Insight Archiving account logins are unlocked or locked.

ACCOUNT	SELECT WHETHER THE ACCOUNT IS CREATED IN AN ENABLED OR DISABLED STATE.
Archiving	Select whether archiving is enabled or disabled.
	If you select Enabled , the email messages for the user start journaling to Arctera Insight Archiving immediately after you create the archive account.
Folder Sync	Indicates whether the Folder Sync feature is enabled or disabled.
	Note: This status is for information only. Folder Sync cannot be enabled or disabled from Arctera Insight Management Console. Folder Sync is enabled or disabled at an account level from the Folder Sync application.
External Reviewer	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 Insight eDiscovery matter.
	The following conditions apply to archive accounts for external reviewers:
	- 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 Insight eDiscovery.
	- Can only access the matters that are assigned to them.

ACCOUNT	SELECT WHETHER THE ACCOUNT IS CREATED IN AN ENABLED OR DISABLED STATE.
	- 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.
	An external reviewer has their account disabled for archiving.
Bypass Surveillance	

ACCOUNT	SELECT WHETHER THE ACCOUNT IS CREATED IN AN ENABLED OR DISABLED STATE.
	 This feature is available only if your organization is subscribed to the Insight Surveillance service. Refer to the sample image below.
	It lets you manually bypass (exclude) specific user accounts from being added as monitored employees in any department within Insight Surveillance, even when departments are populated automatically.
	- Set the Bypass Surveillance option to Yes to prevent the user from being added to any department in Insight Surveillance.
	- Set the Bypass Surveillance option to No to allow the user to be included in surveillance departments.
	Note : The Bypass Surveillance column appears on the Account Management page as shown below.

ACCOUNT	SELECT WHETHER THE ACCOUNT IS CREATED IN AN ENABLED OR DISABLED STATE.
	If it is not visible, click the Select columns to show or hide icon and ensure the column is selected for display as shown below.

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

INSIGHT PERSONAL ARCHIVE	LETS THE USER ACCESS INSIGHT PERSONAL ARCHIVE.
Insight Personal Archive Mobile	Lets the user access Mobile Web Access.
	Note: For this service to be enabled, you must also enable the option for Mobile Web Access on theArchive Optionspage.
Insight eDiscovery	Lets the user access Insight 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 Arctera Insight 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.

1. 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.

The application displays the details of the selected archive account.

1. 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 Arctera Insight Management Console.

> “ ”

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

> “ ”

1. Click **Save**.

About the Account Details page

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

- Archive Detail

- Status
- Services
- Archive Aliases
- Delegate Access
- History

Archive Detail

The Archive Detail panel provides 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 Arctera Insight Management Console uses the email address as the user name.
Time Zone	The time zone that Arctera Insight Archiving uses for the user.
Role	The role that is currently configured for this archive account.

Status

The Status panel shows the current state of the archive account and provides the following key details about it.

ACCOUNT	INDICATES WHETHER THE ACCOUNT IS IN AN ENABLED OR DISABLED STATE.
Login	Indicates whether Arctera Insight Archiving logins for the account are unlocked or locked.
Archiving	Indicates whether archiving is enabled or disabled.

ACCOUNT	INDICATES WHETHER THE ACCOUNT IS IN AN ENABLED OR DISABLED STATE.
Folder Sync	Indicates whether the Folder Sync feature is enabled or disabled.

Note: If there is a redExternalflag next to the Status heading, it means that the archive account belongs to an external reviewer.

Services

The Services panel shows the Arctera Insight Archiving services that are currently configured for the archive account and provides the following key details about it.

	INDICATES THAT THE SERVICE IS ENABLED FOR THE ACCOUNT.

Archive Aliases

The Archive Aliases panel lists all the archive alias email addresses for the account, and the date at which each alias was created. It also provides the following key details about it.

	INDICATES THAT THIS EMAIL ADDRESS IS THE PRIMARY ADMINISTRATOR ACCOUNT.

Delegate Access

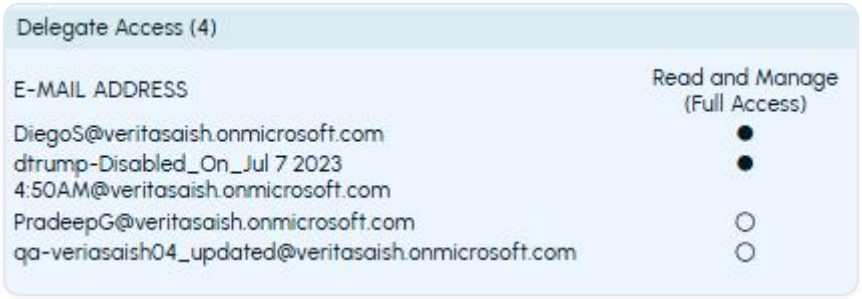
Note: TheDelegate Accesspanel appears only if one or more users or mail-enabled security groups have synchronized delegate permissions for the archive account.

> “ ”

Delegate access allows certain users or groups to access archived emails of another user in Insight Personal Archive. These permissions are typically set by the Exchange or Exchange Online administrator and then synchronized into Insight Personal Archive.

Panel details: This panel lists:

- Users or mail-enabled security groups with synchronized delegate access.
- The type of delegate permissions assigned.
- Icons that show whether the permission is granted or not granted.



Limitation: Permissions manually set by users within Microsoft Outlook are not synchronized.

Supported Environments: Arctera Insight Archiving supports delegate access synchronization for:

- Exchange on-premises mailboxes requires CloudLink v4.0 or later.
- Exchange Online mailboxes, where permissions are controlled through the *Mailbox Delegation Permissions* settings in the Arctera Insight Management Console.

Delegate Permissions Type: The *READ*permission has been renamed to*Read and Manage (Full Access)*.

When the administrator from the customer side accesses the Exchange on-prem or Exchange online mailbox, the same permission name appears as Full Access and Read and Manage (Full Access)respectively.

The *SEND AS*and*ON BEHALF* permissions are currently not supported and have been temporarily removed from the product interface. These permissions do not impact access to archived content at this time. The following tables list the current delegate archive access permission, and its effect in Arctera Insight Archiving.

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

DELEGATE ARCHIVE ACCESS PERMISSION	GRANTED IN THESE CIRCUMSTANCES	EFFECT OF GRANTED PERMISSION IN INSIGHT PERSONAL ARCHIVE
Read and Manage (Full Access)	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 Insight Personal Archive.

Table: 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 INSIGHT PERSONAL ARCHIVE
Read and Manage (Full Access)	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 Insight Personal Archive.
		Note: If the user has a synchronizedDeny Full Accessdelegation permission, the Deny permission takes precedence and the user is not given read access.

History

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 theHistorypanel.

  > “ ”

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 Arctera Insight Archiving logs. The link takes you to the Logs page under Reporting in the left pane.

See About Arctera Insight Archiving reports and notifications.

Editing an archive account

You can edit an archive account, for example to change its status or its configured services.

To edit an archive account

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

The application displays all the available accounts.

1. In the accounts list, double-click the account to display the details of the account.
2. To edit the details, at the bottom-right of the account details page, click **Edit**.
3. Update the account details as required.

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 Arctera Insight Management Console.

> “ ”

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

> “ ”

1. Click **Save** to save your changes.
2. To go back to the archive accounts list, click the back icon displayed in the top-left corner.

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 Insight eDiscovery.

> “ ”

Note: If you delete an archive account, the archived messages for the user remain in Arctera Insight Archiving. These archived messages are not searchable by reviewers or administrators because the account and the associated user is not visible in both Arctera Insight Management 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.

1. Search for and select the archive account of which you want to delete.

For quick and advance searching, See Searching for archive accounts.

1. Click **Edit**.
2. To delete the selected archive account, click **Delete Archive**.

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

1. Click **Yes**.

Deploying users

Once you have created new archive accounts you can give the users access to Insight Personal Archive and Insight eDiscovery from Account Management. You can also deploy Insight 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.

1. Search for and select the archive account for which you want to deploy users.

For quick and advance searching, See Searching for archive accounts.

1. From the accounts list, select the check box for each archive account that you want to deploy.
2. On the action bar, click **Archives**and then click**Deploy User**.
3. In the **Deploy Users** window, select one or more of the following deployment tasks:
    - **Enable DA Access** \- provides access to Insight eDiscovery.
    - **Enable VAS Access** \- provides access to Advanced Supervision.
    - **Enable PA Access** \- provides access to Insight Personal Archive.
    - **Deploy PA Web Folder** \- creates a Microsoft Outlook web folder for accessing Insight Personal Archive.
    - **Send Welcome Message** \- sends a welcome message with login credentials.
4. 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.

1. Search for and select the archive accounts whose services you want to enable.

For quick and advance searching, See Searching for archive accounts.

1. On the action bar, click **Enable Services**.
2. 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.
3. Click **OK**.

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

1. 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, clickClose. The application displays the notification for successful enabling of services. In case you receive such notification, clickClose.

   > “ ”

Configuring the Manage Your Own Keys (MYOK) Feature

Feature overview

The Manage Your Own Keys (MYOK) feature allows customers to encrypt their data using their own Azure-managed encryption keys, instead of Azure-managed encryption keys controlled by Arctera Insight.

If a customer opts to manage its own encryption keys, the Arctera Insight Super Admin enables the MYOK option from the Management Console during the initial provisioning of the customer's account. After MYOK is enabled, the customer gains full control over its Azure-managed keys through the Management Console and uses them to encrypt and protect its data.

MYOK-specific constraints

The MYOK option is available only during initial provisioning of a customer account from the Management Console. If the customer opts to manage its own encryption keys, the Arctera Insight Super Admin must enable MYOK at that stage.

The customer for whom the MYOK feature is not enabled can contact Arctera support to access this option; however, the process incurs additional time and cost. Once enabled, a service alert prompts customer administrators to complete the MYOK configuration. Until it's completed, the Management Console remains restricted, and other features are inaccessible.

Prerequisites

Before installing the Microsoft Azure app, ensure that:

- You have the Application Administrator and Owner (subscription owner) roles to create the encryption keys.
- You must sign up using an Azure Active Directory (Azure AD) organizational account.

  > “ ”

  Note: Personal Microsoft accounts are not supported for this configuration.

  > “ ”

Configuration steps

The stages involved in the MYOK feature configuration are described below.

- To be done by the Arctera Insight Management Console Super Administrator
  - Stage 1: Enabling a customer for the MYOK feature
- To be done by the Customer's Insight Management Console administrator
  - Stage 2: Installing the Azure App and assigning it the Admin role
  - Stage 3: Generating a Storage Key URI
  - Stage 4: Acknowledging a successful configuration
  - Stage 5: Configuring key rotation policy

Enabling a customer for the MYOK feature

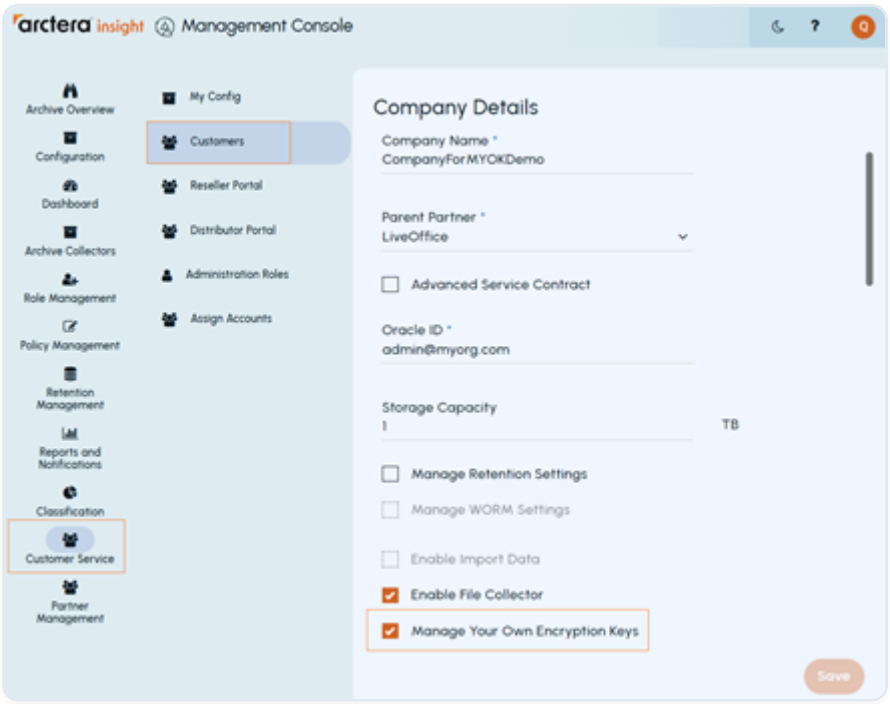
During the provisioning of a new customer, the Insight Archiving Super Administrator can access the MYOK option on the Company Details page. After the customer has been created, this option becomes unavailable.

Note: The customer account administrator is not involved in this procedure. It is performed entirely by the Insight Archiving Management Console Super Administrator. The customer administrator receives a service alert on the Management Console interface upon logging in.

To enable a customer for the MYOK feature

1. In the left navigation pane, select **Customer Service**>**Customers**.
    - To enable MYOK while adding a new customer, click **Add Customer**.
    - To enable MYOK for an existing customer, search for and select the customer, then click **Edit**.

The **Company Details** page appears.

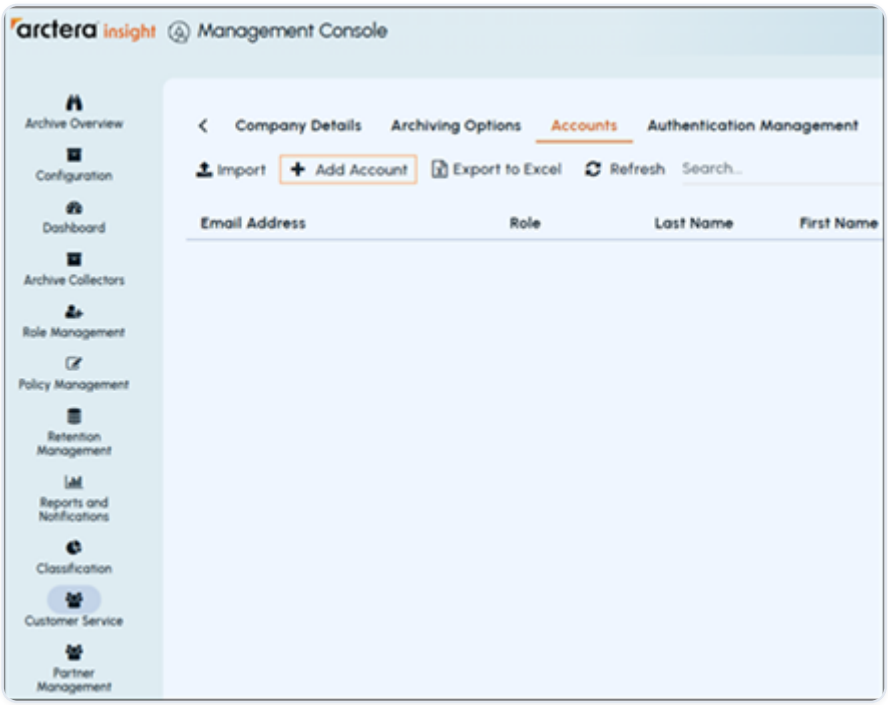


1. Specify the required customer details.
2. Select the **Manage Your Own Encryption Keys** check box.
3. Click **Save**.

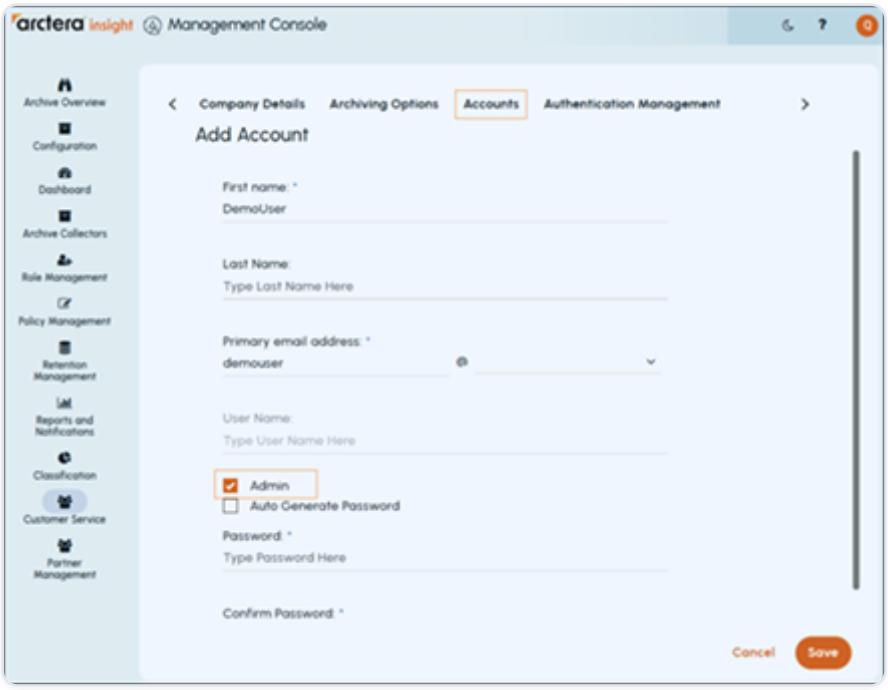
Note: After saving the customer account, the application sends a service alert to the customer. The Insight Archiving Super Administrator must then assign theAdminrole to the customer account user. Only after receiving the Admin role can the customer user independently perform the required next steps.

> “ ”

4. To assign the Admin role to the customer account, select **Customer Service**>**Customers**. The saved company details are displayed.
5. Navigate to the **Accounts**tab and click on**Add Account**.



6. Specify the required details, select the **Admin** check box.



7. Click **Save**.

Installing the Azure App and assigning it the Admin role

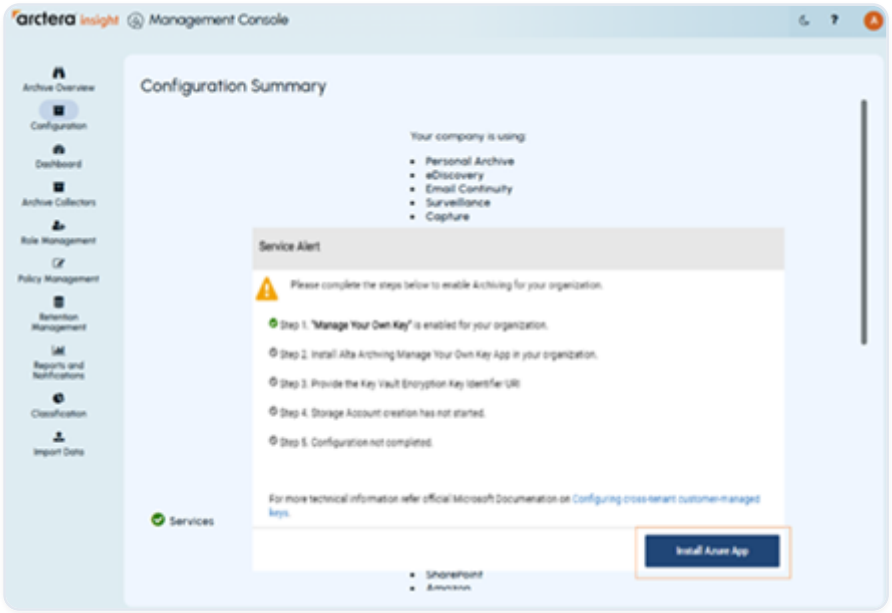
After the Arctera Insight Management Console Super Administrator enables the MYOK feature for the customer account, the customer account administrator receives a service alert upon logging in. The alert prompts the administrator to complete the MYOK configuration.

Note: Until the setup is complete, the Management Console remains restricted, and other features remain inaccessible.

Prerequisites: Ensure that you are the subscription owner of the Azure Subscription where the encryption key will be created.

To install the Azure App and assign a role to it

1. Log in to the Management Console with the administrator credentials.
2. Ensure that the **Service Alert** notification is received and displayed immediately after login.

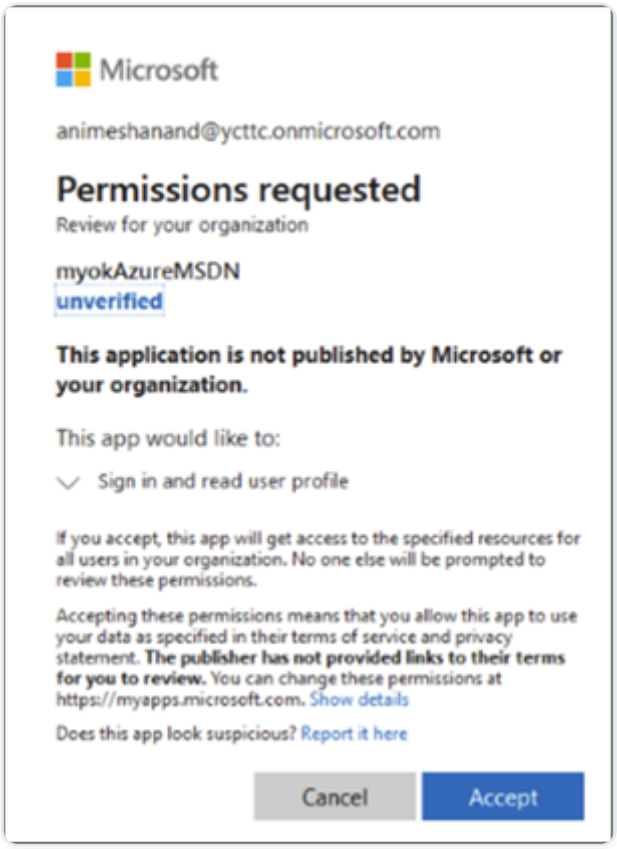


3. On the service alert window, click **Install Azure App**.

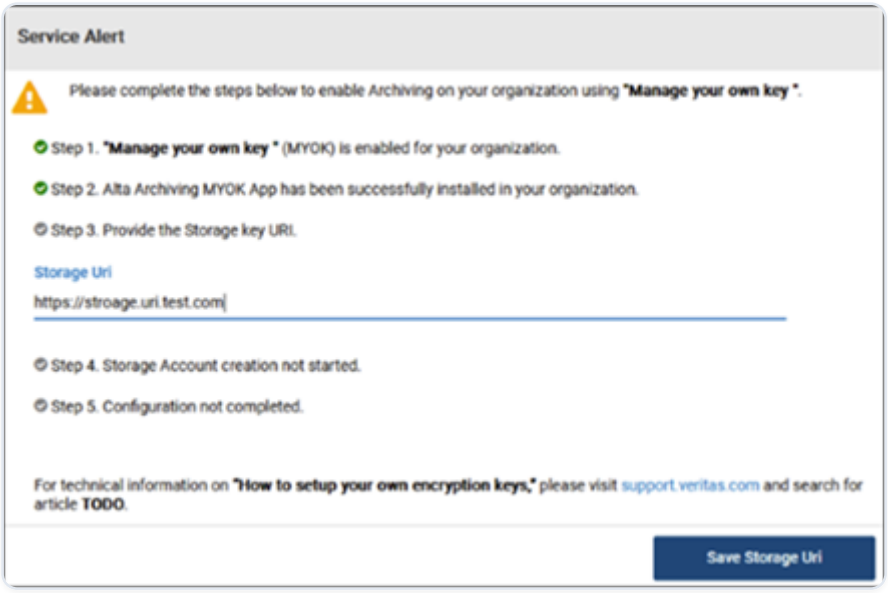
The application redirects you to the Azure Sign-in page.

1. Enter your email and password and click **Sign in**.

If permission to install is denied, click **Retry Install Azure App**.



1. Click **Accept**to allow the requested permissions to initiate the installation. This app gets installed on the customer's Azure subscription. The application redirects you to the**Service Alert** window.
2. On the service alert window, specify the **Storage Key URI**.



> “ ”

Note: To obtain the Storage Key URI, access the Microsoft Azure portal and sign in using the same user credentials that were used to install the Azure app. See SeeGenerating a Storage Key URI..

> “ ”

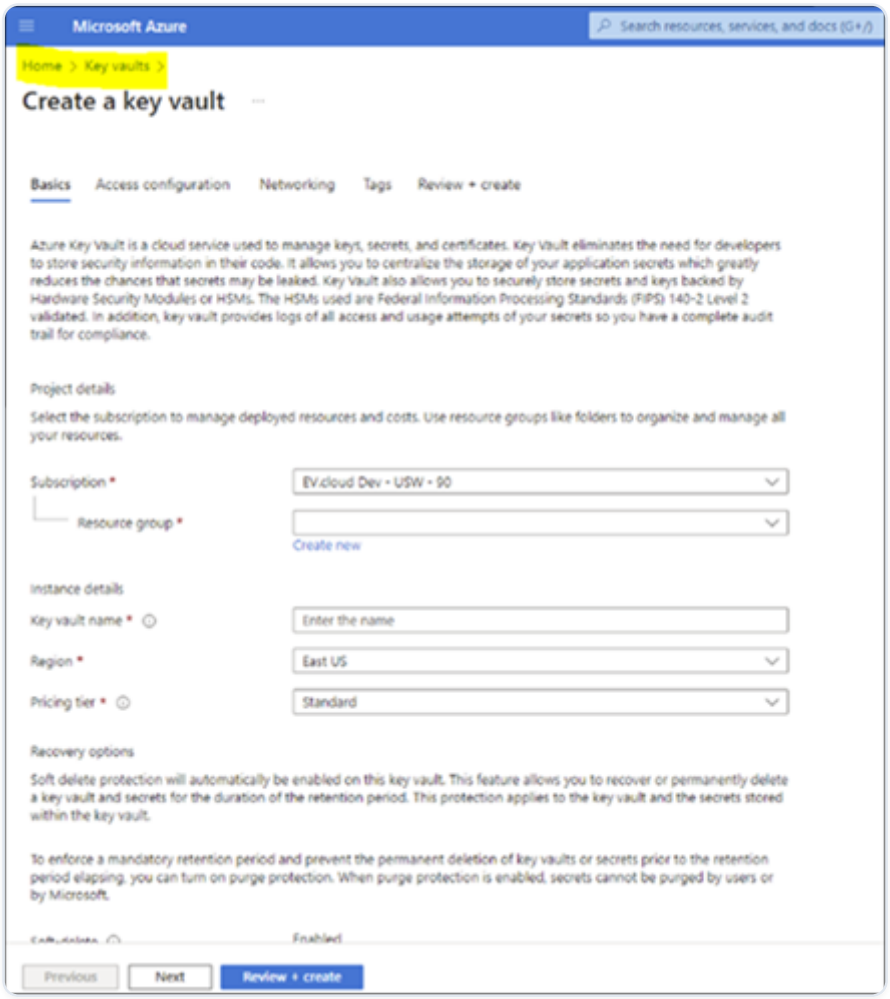
3. Click **Save Storage URI**.

Generating a Storage Key URI

This section briefly navigates you to create a key vault. For detailed information, refer to Create a key vault using the Azure portal.

To generate the Storage key URI

1. On the Microsoft Azure portal, select **Home**>**Create a resource**>**Key Vault**.
2. On the **Key Vaults**page, in the left navigation pane, under**Objects**, select**Keys**, and click**Create**.**Note**: The Azure Key Vault must be created with**Purge Protection** enabled.

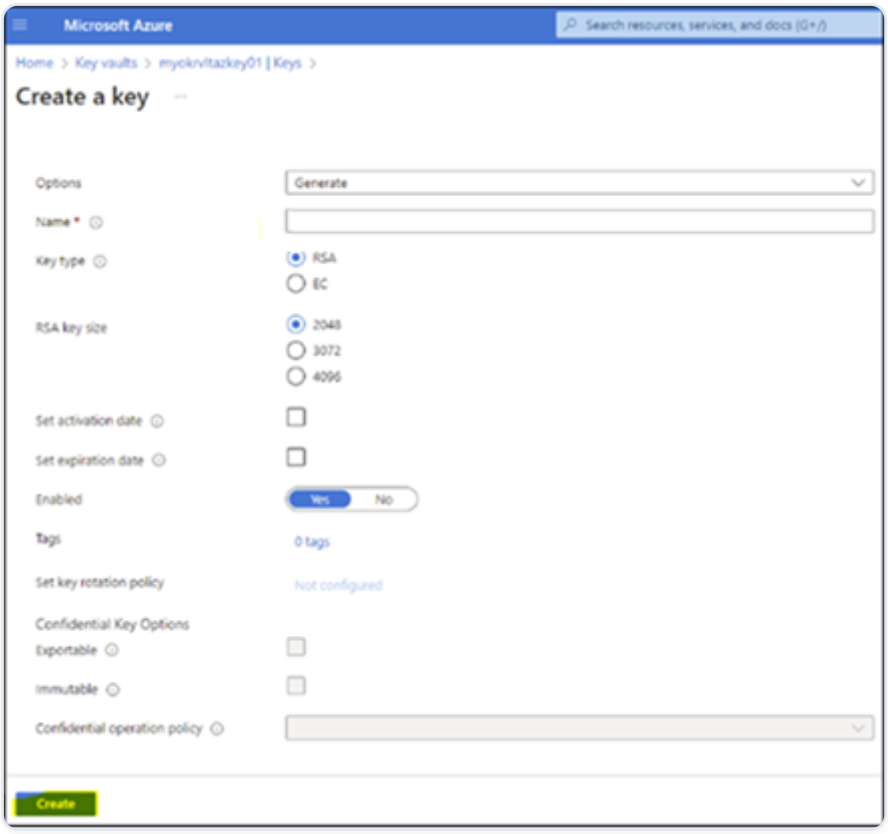


1. Specify the mandatory field details, and click **Next**.
2. Click **Review + Create** to create a Key Vault.
3. Select this Key Vault and click **Keys**.
4. Click **Generate/Import** to create a key.
5. On the **Create a key**page, specify the field details, and click**Create**.

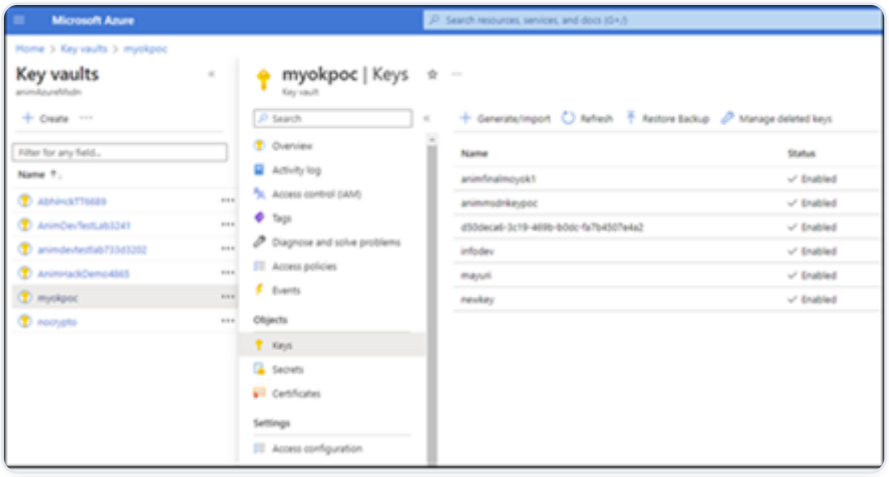
> “ ”

Note: When creating a key, do not select theSet activation dateandSet expiration datecheck boxes. These fields must remain blank.

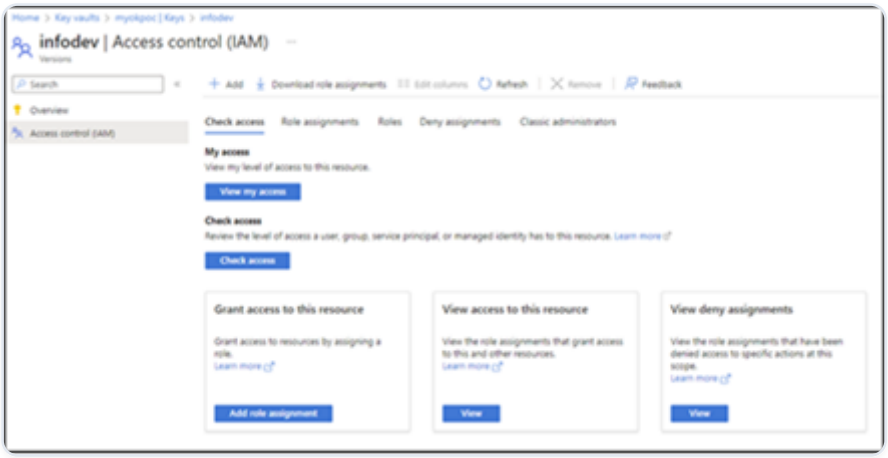
> “ ”



The key is created and listed as shown in the sample image below.



1. Select the key and click **Access Control (IAM)**.

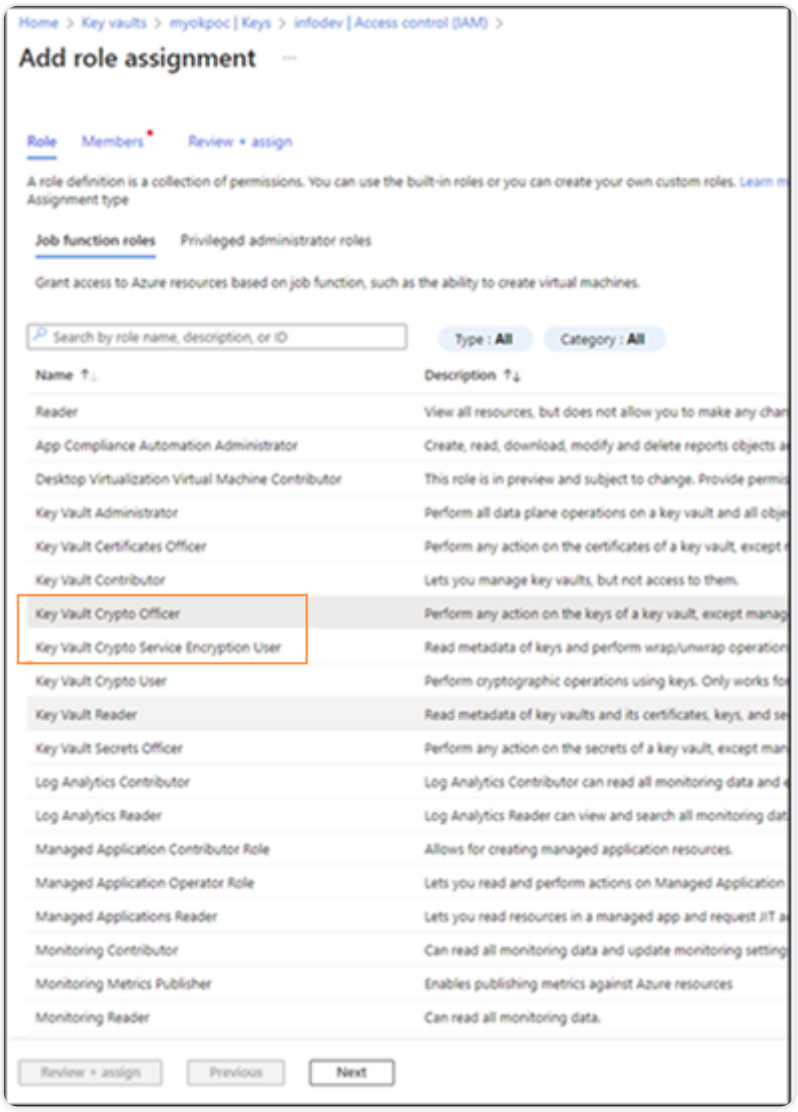


2. Click **Add role assignment**. On the**Add role assignment**page, select the**Role** tab, then select any of the following roles:

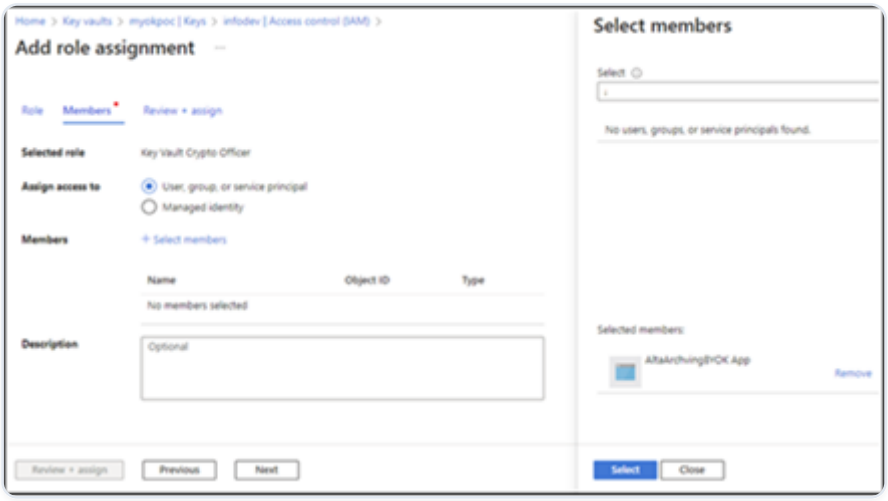
    - *Key Vault Crypto Service Encryption User-Key Vault Crypto Officer*

Note :

- To assign permissions to the application, a user can have either the *Key Vault Crypto Officer*role or the*Key Vault Crypto Service Encryption User* role.
- However, to create an encryption key, the user must have the *Key Vault Crypto Officer* role or a higher-level role with access to Key Vault and permission to create keys.

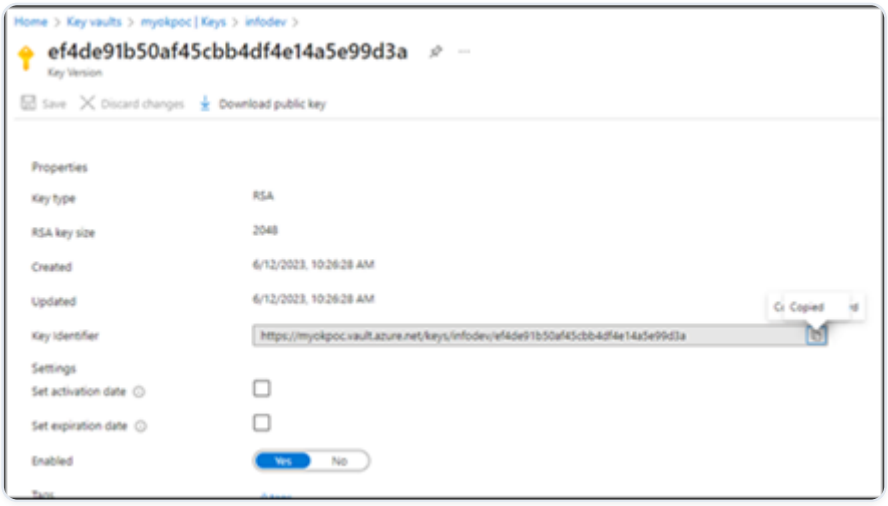


1. Click **Next**to access the**Members** tab.
2. On the Add role assignment page, select the **Members**tab, and click**\+ Select members**.



3. Select the Azure app that you have created and installed. See See Installing the Azure App and assigning it the Admin role..

4. Click **Next and Save**.
5. Select the key and click **Overview**.

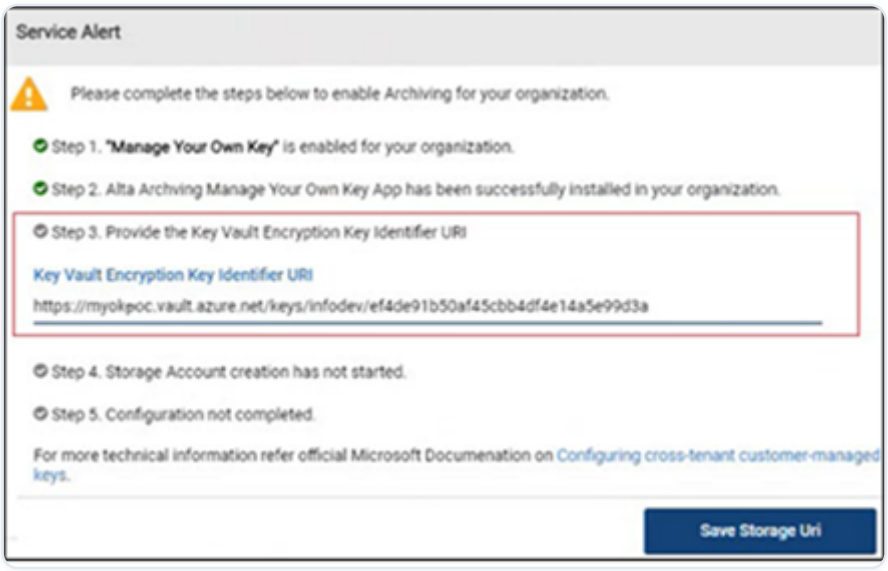


6. Copy the key Identifier value and go to the **Service Alert** window of the Management Console.

Acknowledging a successful configuration

To acknowledge a successful configuration

1. On the **Service Alert**window, paste the key identifier, which you have copied as explained in the previous task, into the**Storage URI** field.



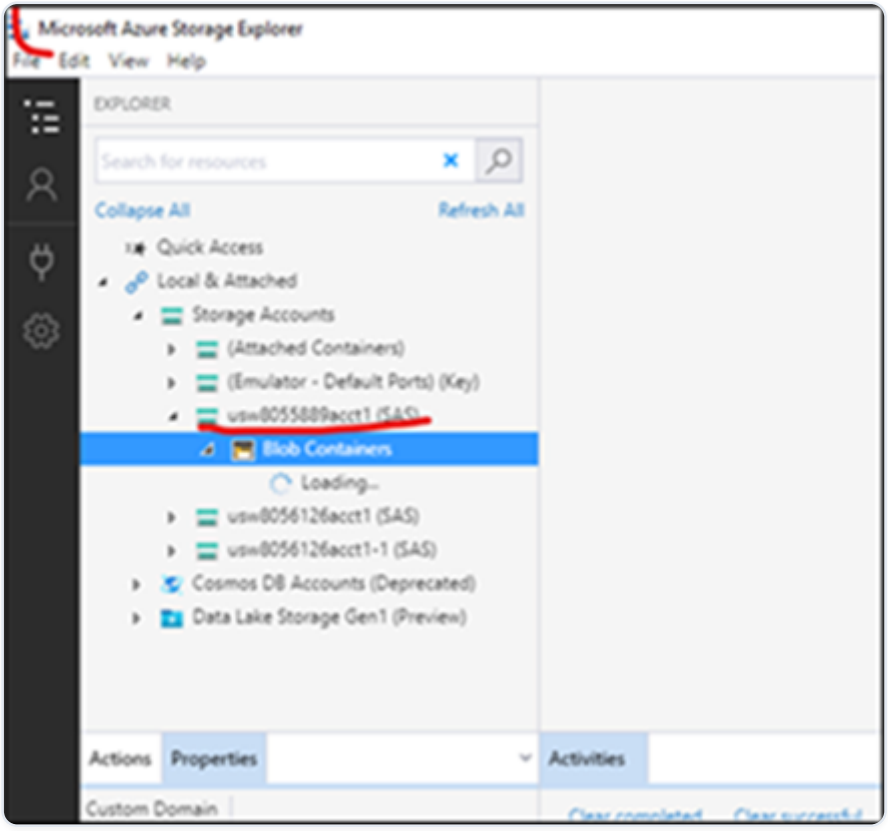
2. Click **Save Storage Uri**.

The application saves the Key Vault Encryption Key Identifier.

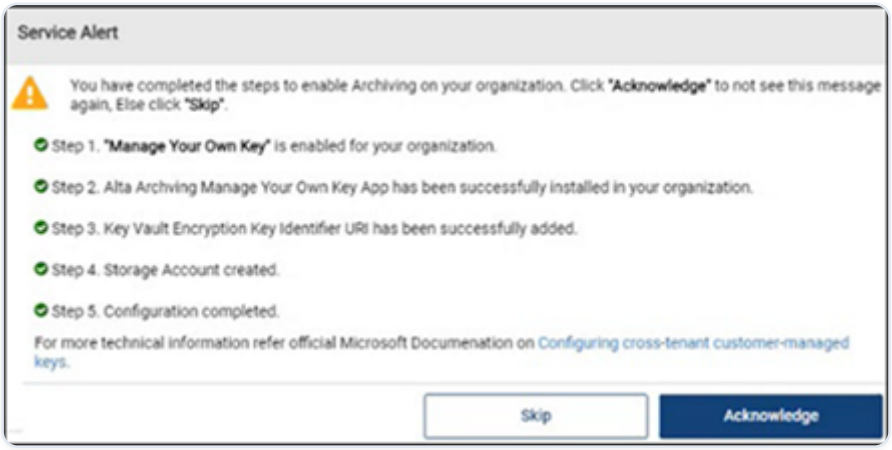
1. Ensure that the **Storage Account** is created on the Azure portal.

After the *Key Vault Encryption Key Identifier* is successfully added, the system automatically creates a corresponding storage account.

- To locate the storage account on the Azure portal, go to **Storage Accounts** and search using the following format:\< *environment*\>\<*groupID*\>. For example,*usw8054120acct*.
- To access the data downloaded from the storage account, go to **Microsoft Azure Storage Explorer**.



1. Ensure that the **Service Alert** window displays all the steps marked as completed.



Note: The application proceeds with the remaining steps mentioned on the Service Alert window only if the providedStorage Key URIis valid.

> “ ”

2. Click **Acknowledge**to confirm successful provisioning and prevent further display of this service alert. If you are not sure, click**Skip**.
3. To confirm if the MYOK feature is enabled for you, on the Management Console, select **Policy Management**>**Archive Options**.
4. Ensure that the *status* under the **Manage Your Own Keys** section is set to *Enabled*.

Configuring key rotation policy

It is recommended to rotate encryption keys at regular intervals to protect your keys. Azure Key Vault allows you to configure each key to automatically generate a new version at a specified interval. You can set up key rotation by configuring a key rotation policy, which can be defined individually for each key.

Key Vault key rotation feature requires key management permissions. You can assign the Key Vault Crypto Officer role to manage key rotation policies and perform on-demand key rotations. For the latest information about configuring the key rotation policy, refer to Key Rotation Policy.

Removing user access

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

> “ ”

Note: If you want to remove deployed Insight Personal Archive web folders, contactArctera Services & Support.

> “ ”

To remove user access

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

The application displays a list of archive accounts.

1. 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.

1. On the action bar, click **Archives**and then click**Remove User**.
2. On the **Remove Users** page, select one or more of the following deployment tasks:
   - **Disable DA Access** \- removes Insight eDiscovery access.
   - **Disable VAS Access** \- removes Advanced Supervision access.
   - **Disable PA Access** \- removes Insight Personal Archive access.
3. 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.

1. On the action bar, click **Bulk Disable Users**.

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

1. 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 asAAA-Disabled@test.com.
   - Select the **Rename with custom prefix string**option, and specify the custom prefix string is ZZZ or ZZZ_ to rename it asZZZ_AAA@test.com.
2. Search for and select multiple user accounts you want to disable simultaneously.
3. 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 underPolicy Management>Archive Options. SeeConfiguring archive options.

> “ ”

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.

1. 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.
2. 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.

1. 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.

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

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

1. To change the Mobile Web Access permission setting, click **Edit**.
2. Under **Services**, select or clear**Insight Personal Archive Mobile** as required.
3. Click **Save** to save your changes.

Unlocking an archive account

As a security measure, Arctera Insight 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 additionally attempts and are required to enter a CAPTCHA Validation Code. After they enter their credentials incorrectly five times, Arctera Insight Archiving locks the archive account. If an account becomes locked, an administrator can remove the lock from Arctera Insight 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.

1. 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.
- From Configuration > Account Management page.

The procedure is explained below.

To edit contact details of a system administrator

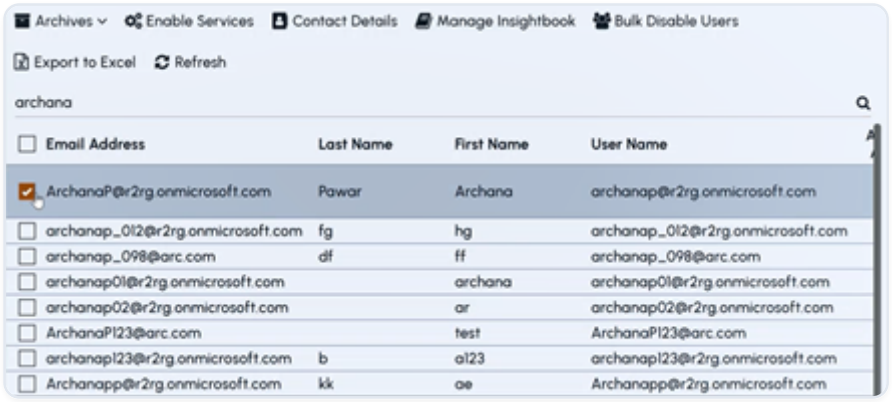
1. In the left navigation pane, click **Configuration**>**Account Management**.
2. On the action bar, click **Contact Details**.
3. Click **Edit** and provide a new admin contact and billing contact details.
4. Click **Save**.

Managing InsightBooks permissions

Before you configure InsightBook permissions for a user account, you need to enable the Personal Archive InsightBooks option. See Configuring archive options.

To configure InsightBooks permissions

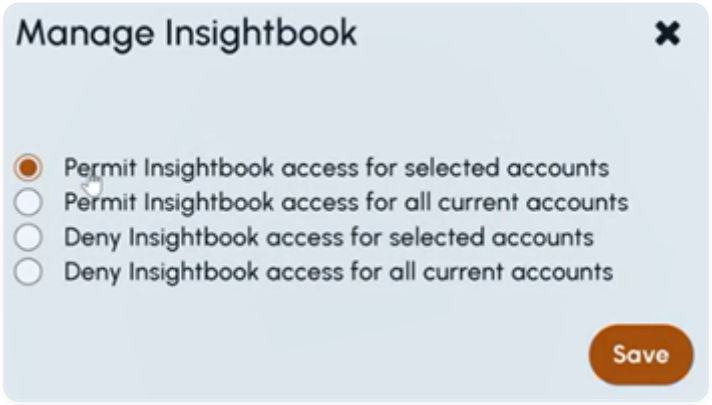
1. In the left navigation pane, click **Configuration**>**Account Management**.
2. Search for and select a user account to which you want to grant the manage InsightBooks permission.



3. On the action bar, click **Manage InsightBooks**.

The *Manage InsightBooks* pop-up appears.

1. Select one of the following options, as needed.



   - **Permit InsightBook access for selected accounts** \- To grant InsightBook access only to the accounts you manually choose.
   - **Permit InsightBook access for all current accounts** \- To grant InsightBook access to all existing accounts in the organization.
   - **Deny InsightBook access for selected accounts** \- To block InsightBook access only for the accounts you manually choose.
   - **Deny InsightBook access for all current accounts** \- To block InsightBook access for all existing accounts in the system.

2. Click **Save**.

Managing Archive Collectors

This section includes the following topics:

- About Signal Archiving
- About Verint Archiving
- About WeChat Archiving
- About WhatsApp Archiving
- About Cloud9 Archiving
- About Verba Archiving
- About Copilot Archiving
- About Zoom Phone Archiving

About Archive Collectors

In addition to email messages, your organization can use Arctera Insight Archiving to archive items from other content sources. For a comprehensive list and detailed instructions on the available Insight Capture connectors and their setup procedures, see Arctera Insight Capture Configuration Guide.

Access Arctera Insight Management Console and select the Archive Collectors node to enable the required 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** : This 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.

1. On the **Archive collector**page, click**Add collector**.

All the available collector types appears.

1. 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.

1. 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.

1. Select the archive collector for which you want to update the configuration.
2. Click the kebab icon (three vertical dots) on the archive collector card, and click **Manage**.
3. Provide the configuration details in the configuration wizard.

Refer to the Arctera Insight Capture 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 Arctera Insight Management Console .

Stopping or restarting import job of archive collectors

You may want to stop an import job in case of errors, incorrect or incomplete data, unexpected time consumption, necessary updates to requirements, or to address any specific issues. When you stop the collection job, the application removes the job from the queue.

Similarly, you may want to restart an import job waiting for the scheduled run. When you run the collection job, the application queues up the selected archive collector for collection.

To stop or restart the import job

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

The application displays the available archive collector cards.

1. To stop the import job, select the archive collector for which you want to stop the import job. Click the kebab icon (three vertical dots) on the archive collector card, and click **Stop**.
2. To restart the import job, select the archive collector for which you want to restart the import job. Click the kebab icon (three vertical dots) on the archive collector card, and click **Run Now**.

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.

1. Select the archive collector of which you want to view the latest status.
2. 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.

Cloning archive collectors

You can create a clone of archive collectors if you want to perform specific operations on an archive collector without disrupting its intended configuration and functions.

The cloned archive collector will keep the same configuration. You can change the configuration of the cloned archive collector as needed. You can create a clone of archive collectors in any state, whether it is idle, incomplete, or completed. The list of monitored users is not fixed. If new users have been added since the last run, the users list may vary, even for the same archive collector. Therefore, it is recommended to synchronize the user list before each run.

To create a clone of existing collector

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

The **Archive Collector** page appears.

1. Select the archive collector from which you want to create a clone.
2. Click the kebab icon (three vertical dots) on the archive collector card, and click **Clone**.
3. Provide a new unique name and description for the cloned archive collector.
4. Click **Next**.

The application displays a notification that cloning is successful.

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

1. Select the archive collector you want to delete.
2. 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.

1. Click **Yes**.

Deleting a history of archive collectors

You can delete all the pre-specified data of archive collectors and use them just like new collectors.

> “ ”

Note: Be careful while deleting the data associated with the selected archive collector as you cannot retrieve it by any means.

> “ ”

To delete history of archive collectors

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

The **Archive Collector** page appears.

1. Select the archive collector from which you want to delete the data.
2. Click the kebab icon (three vertical dots) on the archive collector card, and click **Delete Collector Data**.
3. The application prompts you to confirm that you want to perform the operation. Click **Yes**.

About Exchange Online Archiving

As an administrator, you can create and enable an Exchange Online collector to collect items from the synchronized user accounts.

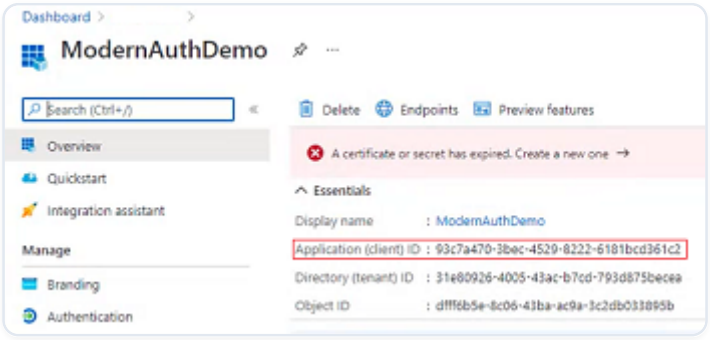
Setting up modern authentication in Azure AD for Exchange Online sync

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.

1. 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 fromhttps://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 Arctera Insight 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.

> “ ”

2. 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.

> “ ”

1. 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 asoptionalcan be omitted if theAPI permission useand the associated functionality is not required for your environment.

> “ ”

EXCHANGE WEB SERVICE	(OPTIONAL)
(EWS API\PROXY)	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 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 Exchange Online > Application permissions > Exchange > Exchange.ManageAsApp
	Note: Exchange.ManageAsApp permission is required. For reference, seeSet 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

EXCHANGE WEB SERVICE	(OPTIONAL)
(EWS API\PROXY)	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 EXCHANGE ONLINE > APPLICATION PERMISSIONS > OTHER PERMISSIONS > FULL_ACCESS_AS_APP
	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

EXCHANGE WEB SERVICE	(OPTIONAL)
(EWS API\PROXY)	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 EXCHANGE ONLINE > APPLICATION PERMISSIONS > OTHER PERMISSIONS > FULL_ACCESS_AS_APP
	Permissions to be assigned: You need to at least assign the User.Read.All permission to the application.
	Reference: See Permissions

1. 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.

1. 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 Arctera Insight 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 Arctera Insight 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.

Arctera Insight 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.

1. On the **Credential Management** page, specify the following:

CHOOSE OPTION TO CONNECT	SELECT THE OPTION THAT REPRESENTS THE MODERN AUTHENTICATION METHOD FOR CONNECTING TO THE EXCHANGE ONLINE PORTAL.
\> AZURE AD REGISTERED APP CONFIGURATION	
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 Password	This is a password used for the self-signed certificate.
	Provide this password when you upload a new certificate.

2. Click **Test** to verify connection with Exchange Online endpoint.
3. Click **Save**to navigate to the**Provisioning and configuration** tab.

Else, you can manually navigate 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.

1. On the **Provisioning** page, do the following steps:

SYNCHRONIZE USER NAME FROM	SELECT ONE OF THE FOLLOWING OPTIONS\:
	EMAIL ADDRESS: SELECT THIS OPTION TO MATCH THE USERNAME WITH THE PRIMARY EMAIL ADDRESS ASSOCIATED WITH THE ARCHIVE ACCOUNT.
	USER PRINCIPAL NAME: SELECT THIS OPTION TO MATCH THE USERNAME WITH THE USER PRINCIPAL NAME ASSOCIATED WITH THE ARCHIVE ACCOUNT.
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\:

SYNCHRONIZE USER NAME FROM	SELECT ONE OF THE FOLLOWING OPTIONS\:
	EMAIL ADDRESS: SELECT THIS OPTION TO MATCH THE USERNAME WITH THE PRIMARY EMAIL ADDRESS ASSOCIATED WITH THE ARCHIVE ACCOUNT.
	USER PRINCIPAL NAME: SELECT THIS OPTION TO MATCH THE USERNAME WITH THE USER PRINCIPAL NAME ASSOCIATED WITH THE ARCHIVE ACCOUNT.
	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\:

SYNCHRONIZE USER NAME FROM	SELECT ONE OF THE FOLLOWING OPTIONS\:
	EMAIL ADDRESS: SELECT THIS OPTION TO MATCH THE USERNAME WITH THE PRIMARY EMAIL ADDRESS ASSOCIATED WITH THE ARCHIVE ACCOUNT.
	USER PRINCIPAL NAME: SELECT THIS OPTION TO MATCH THE USERNAME WITH THE USER PRINCIPAL NAME ASSOCIATED WITH THE ARCHIVE ACCOUNT.
	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 Arctera Insight 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.

SYNCHRONIZE USER NAME FROM	SELECT ONE OF THE FOLLOWING OPTIONS\:
	EMAIL ADDRESS: SELECT THIS OPTION TO MATCH THE USERNAME WITH THE PRIMARY EMAIL ADDRESS ASSOCIATED WITH THE ARCHIVE ACCOUNT.
	USER PRINCIPAL NAME: SELECT THIS OPTION TO MATCH THE USERNAME WITH THE USER PRINCIPAL NAME ASSOCIATED WITH THE ARCHIVE ACCOUNT.
	Automatically provision journaling in Exchange Online: Select this option to let Arctera Insight Management Console configure a journaling rule automatically in Exchange Online. Arctera Insight 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.
	Arctera Insight Management Console prepopulates the Journal address box with the Exchange Online journal address that Arctera Insight Archiving has assigned to your company.
	Note: You must also set up a send connector for Exchange Online. See theSetting up Exchange Online journalingsection in theArctera Insight 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 Insight Personal Archive web folder when it provisions an archive account.

SYNCHRONIZE USER NAME FROM	SELECT ONE OF THE FOLLOWING OPTIONS\:
	EMAIL ADDRESS: SELECT THIS OPTION TO MATCH THE USERNAME WITH THE PRIMARY EMAIL ADDRESS ASSOCIATED WITH THE ARCHIVE ACCOUNT.
	USER PRINCIPAL NAME: SELECT THIS OPTION TO MATCH THE USERNAME WITH THE USER PRINCIPAL NAME ASSOCIATED WITH THE ARCHIVE ACCOUNT.
	- Archive Folder Name: Enter the name to use for the Insight Personal Archive web folder, such as Personal Archive.
	- Archive Folder URL: Enter your access URL for Insight Personal Archive.
	Under Personal Archive Access, configure whether Arctera Insight Archiving automatically enables access to Insight Personal Archive and sends a welcome message email to each user.
	- Enable Personal Archive access and send Welcome Message: Select this option to enable Insight 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.

SYNCHRONIZE USER NAME FROM	SELECT ONE OF THE FOLLOWING OPTIONS\:
	EMAIL ADDRESS: SELECT THIS OPTION TO MATCH THE USERNAME WITH THE PRIMARY EMAIL ADDRESS ASSOCIATED WITH THE ARCHIVE ACCOUNT.
	USER PRINCIPAL NAME: SELECT THIS OPTION TO MATCH THE USERNAME WITH THE USER PRINCIPAL NAME ASSOCIATED WITH THE ARCHIVE ACCOUNT.
	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.

2. Click **Next**to save the provisioning details, and navigate to the**Configuration** page.
3. 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	Select one of the following options to decide further action.

SYNCHRONIZE SHARED MAILBOXES	SELECT THIS CHECK BOX TO TARGET EVERY SHARED MAILBOX FOR SYNCHRONIZATION IN ALL OF YOUR EXCHANGE ONLINE DOMAINS.
	Do not synchronize delegation permissions: Perform no synchronization of mailbox delegation permissions. If any mailbox delegation permissions are already synchronized, these remain unaffected.
	Synchronize delegation permissions: Synchronize the delegation permissions that are applied to the targeted mailboxes. In Insight Personal Archive a user is then able to access the archived content for each mailbox to which they have been granted delegate access.
	Remove synchronized delegation permissions: Remove any synchronized Exchange Online delegation permissions. All delegated access to Exchange Online archives is removed.

4. Click **Next**to save the configuration details, and navigate to the**Exchange Online Sync Schedular** page.
5. On the **Exchange Online Sync Schedular** page, do the following steps:

SYNC SCHEDULAR	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.

6. Click **Next**to navigate to the**Summary** page.
7. 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 Arctera Insight Archiving to synchronize Exchange Online mailbox folders of users to Insight 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 Arctera Insight Management 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.
- 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. 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.

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

> “ ”

Note: At the time of adding the first collector, theAdd collectorbutton appears in the middle of the screen. If one or more collectors are already added, theAdd collectoroption appears on the top right-hand corner. If you select the collector that is not supported in Arctera Insight Archiving, theConfigurebutton gets disabled. You cannot configure such collectors.

> “ ”

2. 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. SeeAdding new archive collectors.

> “ ”

3. Click on the Kebab icon (three vertical dots), and click **Manage**.
4. On the **Credential Management**page, ensure that the**O365 Sync**check box is selected by default. Select the**Folder Sync** check box.
5. Under **Folder Sync** , specify the following:

USE SAME CREDENTIALS USED IN O365 SYNC	SELECT THIS CHECK BOX TO USE THE SAME AZURE AD APPLICATION THAT IS CONFIGURED FOR O365 SYNC.
	NOTE: IF YOU DO NOT SELECT THEUSE SAME CREDENTIALS USED IN O365 SYNCCHECK BOX, SPECIFY OTHER CONFIGURATION PARAMETERS EXPLAINED IN TABLE BELOW.
Client ID	Provide the client ID of the application registered in the Azure Active Directory.
	One tenant can have different client IDs and certificates.
Tenant Name	Provide the Tenant or Domain name.

USE SAME CREDENTIALS USED IN O365 SYNC	SELECT THIS CHECK BOX TO USE THE SAME AZURE AD APPLICATION THAT IS CONFIGURED FOR O365 SYNC.
	NOTE: IF YOU DO NOT SELECT THEUSE SAME CREDENTIALS USED IN O365 SYNCCHECK BOX, SPECIFY OTHER CONFIGURATION PARAMETERS EXPLAINED IN TABLE BELOW.
Certificate	Select the Use existing certificate option if you have already created the .PFX certificate for the registered application.
	Select the Add new certificate option to browse and select the new certificate.
Thumbprint	Specify the thumbprint which is used to validate the certificate.
Expires On	Specify the date of expiry for the mentioned certificate

6. Click **Test** below the Folder Sync option to test information provided for Folder Sync.
7. 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 theFolder Sync Configurationtab (16). Else, follow step9to step15to provision and configure the collector.

> “ ”

1. On the **Provisioning** page, do the following steps:

SYNCHRONIZE USER NAME FROM	SELECT ONE OF THE FOLLOWING OPTIONS\:
	EMAIL ADDRESS: SELECT THIS OPTION TO MATCH THE USERNAME WITH THE PRIMARY EMAIL ADDRESS ASSOCIATED WITH THE ARCHIVE ACCOUNT.
	USER PRINCIPAL NAME: SELECT THIS OPTION TO MATCH THE USERNAME WITH THE USER PRINCIPAL NAME ASSOCIATED WITH THE ARCHIVE ACCOUNT.
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.

SYNCHRONIZE USER NAME FROM	SELECT ONE OF THE FOLLOWING OPTIONS\:
	EMAIL ADDRESS: SELECT THIS OPTION TO MATCH THE USERNAME WITH THE PRIMARY EMAIL ADDRESS ASSOCIATED WITH THE ARCHIVE ACCOUNT.
	USER PRINCIPAL NAME: SELECT THIS OPTION TO MATCH THE USERNAME WITH THE USER PRINCIPAL NAME ASSOCIATED WITH THE ARCHIVE ACCOUNT.
	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

SYNCHRONIZE USER NAME FROM	SELECT ONE OF THE FOLLOWING OPTIONS\:
	EMAIL ADDRESS: SELECT THIS OPTION TO MATCH THE USERNAME WITH THE PRIMARY EMAIL ADDRESS ASSOCIATED WITH THE ARCHIVE ACCOUNT.
	USER PRINCIPAL NAME: SELECT THIS OPTION TO MATCH THE USERNAME WITH THE USER PRINCIPAL NAME ASSOCIATED WITH THE ARCHIVE ACCOUNT.
	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 Arctera Insight 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 Arctera Insight Management Console configure a journaling rule automatically in Exchange Online. Arctera Insight Management Console attempts to create the journaling rule when you click Next at the end of this procedure. The rule journals all

SYNCHRONIZE USER NAME FROM	SELECT ONE OF THE FOLLOWING OPTIONS\:
	EMAIL ADDRESS: SELECT THIS OPTION TO MATCH THE USERNAME WITH THE PRIMARY EMAIL ADDRESS ASSOCIATED WITH THE ARCHIVE ACCOUNT.
	USER PRINCIPAL NAME: SELECT THIS OPTION TO MATCH THE USERNAME WITH THE USER PRINCIPAL NAME ASSOCIATED WITH THE ARCHIVE ACCOUNT.
	items to the assigned Exchange Online journal address.
	Arctera Insight Management Console prepopulates the Journal address box with the Exchange Online journal address that Arctera Insight 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 theArctera Insight 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 Insight Personal Archive web folder when it provisions an archive account.
	- Archive Folder Name: Enter the name to use for the Insight Personal Archive web folder, such as Personal Archive.
	- Archive Folder URL: Enter your access URL for Insight Personal Archive.

SYNCHRONIZE USER NAME FROM	SELECT ONE OF THE FOLLOWING OPTIONS\:
	EMAIL ADDRESS: SELECT THIS OPTION TO MATCH THE USERNAME WITH THE PRIMARY EMAIL ADDRESS ASSOCIATED WITH THE ARCHIVE ACCOUNT.
	USER PRINCIPAL NAME: SELECT THIS OPTION TO MATCH THE USERNAME WITH THE USER PRINCIPAL NAME ASSOCIATED WITH THE ARCHIVE ACCOUNT.
	Under Personal Archive Access, configure whether Arctera Insight Archiving automatically enables access to Insight Personal Archive and sends a welcome message email to each user.
	- Enable Personal Archive access and send Welcome Message: Select this option to enable Insight 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\:

SYNCHRONIZE USER NAME FROM	SELECT ONE OF THE FOLLOWING OPTIONS\:
	EMAIL ADDRESS: SELECT THIS OPTION TO MATCH THE USERNAME WITH THE PRIMARY EMAIL ADDRESS ASSOCIATED WITH THE ARCHIVE ACCOUNT.
	USER PRINCIPAL NAME: SELECT THIS OPTION TO MATCH THE USERNAME WITH THE USER PRINCIPAL NAME ASSOCIATED WITH THE ARCHIVE ACCOUNT.
	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.

2. Click **Next**to save the provisioning details, and navigate to the**Configuration** page.
3. On the **Configuration** page, do the following steps:

SYNCHRONIZE SHARED MAILBOXES	SELECT THIS CHECK BOX TO VIEW THE FOLLOWING OPTIONS\:
	- 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 ARCTERA INSIGHT 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 ARCTERA INSIGHT ARCHIVING.
Mailbox Delegate Permissions	Select one of the following options to decide further action.
	Do not synchronize delegation permissions: Perform no synchronization of mailbox delegation permissions. If any mailbox delegation permissions are
	already synchronized, these remain unaffected.
	Synchronize delegation permissions: Synchronize the delegation permissions that are applied to the targeted mailboxes. In Insight Personal Archive a user is then able

SYNCHRONIZE SHARED MAILBOXES	SELECT THIS CHECK BOX TO VIEW THE FOLLOWING OPTIONS\:
	- 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 ARCTERA INSIGHT 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 ARCTERA INSIGHT ARCHIVING.
	to access the archived content for each mailbox to which
	they have been granted delegate access.
	Remove synchronized delegation permissions: Remove any synchronized Exchange Online delegation permissions. All delegated access to Exchange Online archives is removed.

4. Click **Next**to save the configuration details, and navigate to the**Exchange Online Sync Schedular** page.
5. On the **Exchange Online Sync Schedular** page, specify the following:

SYNC SCHEDULAR	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.

6. Click **Next**to navigate to the**Summary** page.
7. On the **Summary**page, ensure the details. In case, you want to modify anything, click**Edit** to navigate to corresponding page.
8. On the **Folder Sync Configuration** page, specify the following:

MAILBOX SETTINGS
Autoselect new Mailboxes
Deselect disabled Mailboxes
Concurrent Mailboxes
Next run at
Repeat
Skip these folders while syncing

> “ ”

Schedule

> “ ”

9. Click **Save**.
10. 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.

Configuring Microsoft Azure Active Directory Group synchronization

Active Directory Group synchronization is an additional service for Arctera Insight Archiving. After configuring, it synchronizes user groups, nested groups, and their respective users between Microsoft Azure AD and the Arctera Insight Archiving database. This synchronization is unidirectional, occurring solely from Azure AD to the Arctera Archiving database.

To configure Microsoft Azure AD Group synchronization

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

Ensure that the **Using Microsoft Office 365**check box is selected. Click**Save**and then click**Go To Next Step**.

1. In the left navigation pane, select **Archive Collectors** , and do any of the following:
    - To add a new Exchange Online collector, click **Add Collector**.
    - To edit configuration of an existing collector, select the Exchange Online collector, click the kebab icon and click **Manage**.
2. On the **Credential Management** page, perform the actions mentioned in the next steps.
3. Configure O365 Account Synchronization. See Configuring Exchange Online sync.
4. After configuring O365 Account synchronization, expand the **Active Directory Group Sync Configuration** section, and specify the following details:

USE THE SAME CREDENTIAL AS O365 SYNC	SELECT THIS CHECK BOX IF YOU WANT TO UTILIZE THE SAME CREDENTIALS THAT YOU HAVE USED FOR O365 ACCOUNT SYNCHRONIZATION.
	THE CLIENT ID AND TENANT NAME VALUES THAT ARE UTILIZED DURING O365 ACCOUNT SYNCHRONIZATION APPEARS AUTOMATICALLY IN THE CORRESPONDING FIELDS.
Client ID	Client ID (or Azure AD App ID) is a unique identifier generated during modern authentication setup in Azure AD.
	Enter the Azure AD App ID.
	The configured Azure AD needs the following permissions to fetch the client ID.
	- Mandatory permission required : User.Read.All
	- Any one of the following (from least to most privileged) permissions required: GroupMember.Read.All Group.Read.All Directory.Read.All
	If required, refer to the Microsoft help on Graph Permissions
Tenant Name	Tenant name is a Primary Domain for the Azure AD tenant.
	Enter the primary domain ID.
	You can get this ID from the Tenant Information section on the Overview page of Azure AD portal.
Choose certificate > Use new certificate	Certificate is the Self-signed .PFX file.
	Select this option to upload a new certificate.

USE THE SAME CREDENTIAL AS O365 SYNC	SELECT THIS CHECK BOX IF YOU WANT TO UTILIZE THE SAME CREDENTIALS THAT YOU HAVE USED FOR O365 ACCOUNT SYNCHRONIZATION.
	THE CLIENT ID AND TENANT NAME VALUES THAT ARE UTILIZED DURING O365 ACCOUNT SYNCHRONIZATION APPEARS AUTOMATICALLY IN THE CORRESPONDING FIELDS.
	Click Choose Certificate to select the appropriate certificate, and provide the password. This is a password used for the self-signed certificate.
Choose certificate > Use existing certificate	Select this option to upload an existing certificate.
	If a certificate is already uploaded, this option is selected by default. The thumbprint and expiry details of the certificate appears automatically.
Thumbprint	Specify the certificate's thumbprint for validation purposes.
Expires on	Specify the certificate's expiration date.

5. Click **Test** to verify connection with the O365 account.
6. If the tested connection is successful, click **Save**to navigate to the**Provisioning and Configuration** tab.
7. Ensure that the **Active Directory Groups** tab appears on the Exchange Online page. Select the tab to view the synchronized Active Directory Groups.
8. Select the **Job List** tab to view your folder synchronization job progress and status for Exchange Online, Folder Sync, and AD Groups.

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). When this service is enabled, such items are archived by using the Arctera Insight Archiving application and are available for discovery by using the Insight eDiscovery application.

For more information on Bloomberg Archiving, refer to the Bloomberg section of Insight Capture Configuration Guide.

About Google Chat Archiving

You can capture the Google Chat items by using Google's built-in third-party archiving solution. When the Google Chat service is enabled, the chats that are converted to emails are sent to a journal/archive address during regular intervals. Such items are then archived by using the Arctera Insight Archiving application and are available for discovery by using the Insight eDiscovery application.

For more information on Google Chat Archiving, refer to the Google Chat section of Insight Capture Configuration Guide.

Configuring Google Chat Archiving

To set up a third-party archiving solution:

1. Sign in to Google Admin console by using your administrator account.
2. Select **Menu**>**Apps**>**Google Workspace**>**Google Chat**.
3. Click **Third-party Archiving Settings**.
4. To apply the setting to everyone, leave the top organizational unit selected. Otherwise, select a child organizational unit.
5. Check **Archiving enabled**.
6. In **Destination** address, enter the email address where you want to send journal messages.

This will be an email address at the third-party archiving provider. You can enter only one address.

1. In the **Archival frequency** field, enter how often messages should be generated (every 1-24 hours).
2. (Optional) In **Custom headers** , enter a comma-separated list of any email message headers that should be used to uniquely identify Chat messages.
3. Click **Save**.
4. For more information, see Integrate Chat with a third-party archiving solution - Google Workspace Admin Help.

Here are additional observations about this process:

- Google does not have the name of the room/space, only a GUID is provided.
- Each participant will get a copy of the chat in their archive. Hence custodians can be targeted for search individually.
- Use a period of 24hrs and not less for Archival frequency.

About Google Workspace Archiving

Arctera Insight Management Console supports archiving user data and mail-enabled user groups from Google Workspace without the need for additional licenses from Google. Administrators must have adequate privileges to configure Single Sign-On (SSO) settings that enable data archiving from Google Workspace. For a successful configuration:

Step 1: Configuring Google Workspace for SAML and SSO authentication to your custom SAML app

Step 2: Enabling the Google Workspace service

Step 3: Configuring Google Workspace Archiving Collector

Configuring Google Workspace for SAML and SSO authentication to your custom SAML app

Prerequisites

You must have the super administrator role/privileges to configure Google Workspace for SAML and SSO authentication to your custom SAML app. Upon successful configuration, the SSO sends a SAML request to the Google Workspace as an Identity Provider (IdP) and then sends a SAML response to the SSO confirming the user identity.

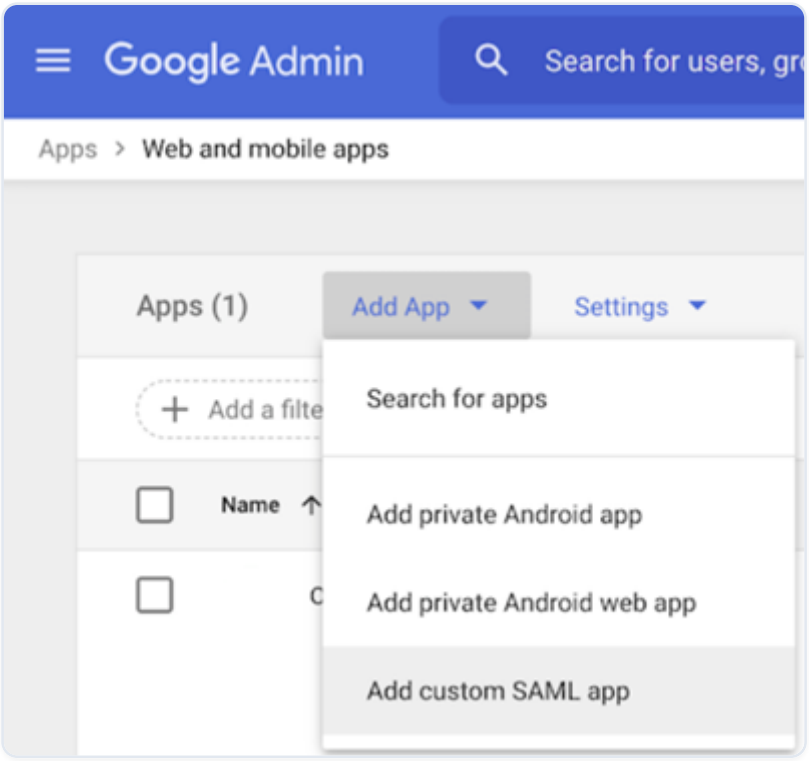
> “ ”

Note: This section provides a quick references for configuring Google Workspace for SAML and SSO authentication. However, for precise configuration procedure, refer to Google Workspace Admin Help documentation:Set up you own custom SAML application.

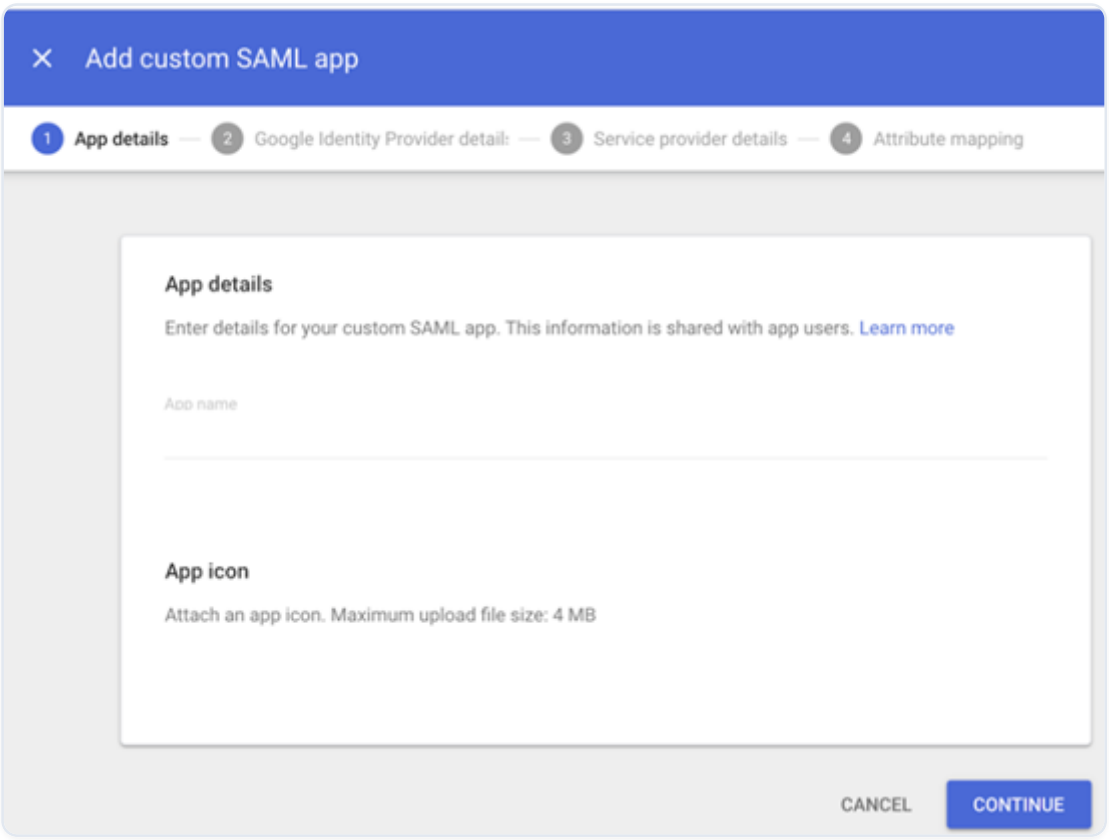
> “ ”

To configure Google Workspace for SAML and SSO authentication to your custom SAML app

1. Log in to the Google Admin console as a super administrator.
2. Select **Apps**>**Web and mobile apps**.



3. Click **Add App**and select**Add custom SAML app** as shown in the sample image below, and perform the following steps:

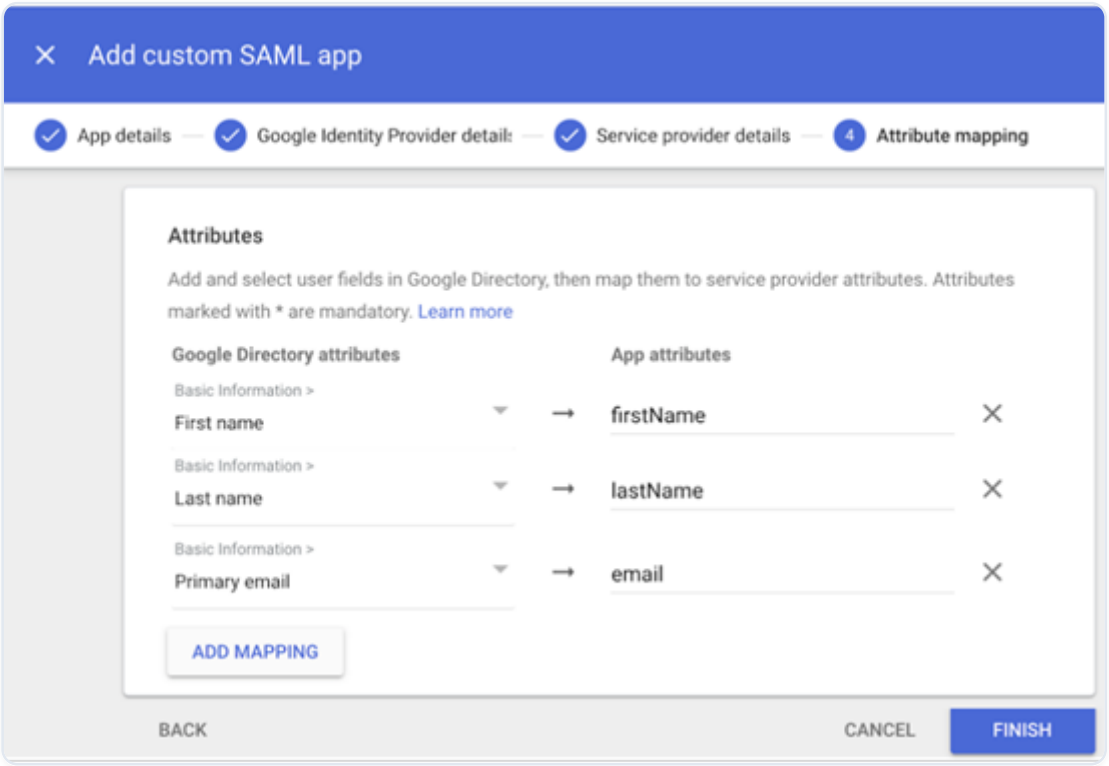


- On the **App details**page, specify a unique app name, description, and app icon, and then click**Continue**.

Uploading an app icon is optional. If you do not upload the icon, Google Workspace creates a new icon using the first two letters of your app name. This information is shared with the custom SAML app users. (This icon will be shown on the **App settings**page and in the**Web and mobile apps** list.)

- On the **Google Identity Provider details** page, use one of the following options to get the required setup information. These crucial parameters are needed to configure the SSO Integration and verify connectivity between Google Workspace and the custom SAML app.
  - **Option 1** : Download the IDP metadata file.
  - **Option 2** : Copy the SSO URL, Entity ID, and SAML 2.0 Certificate. Save this information securely to use while setting up a service provider.
- On the **Service provider details** page, enter the following details:
  - **ACS URL** : Enter the URL that should receive the SAML response after authentication. It must begin with https://.
  - **Entity ID** : Enter the Entity ID copied from the previous step.

- **Start URL** : (Optional) Enter the URL to which the SAML app should redirect users after successful login/authentication to the app.
- **Signed Response** : (Optional) Select if the service provider requires the entire SAML authentication response to be signed. Do not select this option if the service provider requires only the assertion within the response to be signed.
- **Name ID format** : Define the naming format supported by Google Workspace. Select the *Email* format from the drop-down list.
- **Name ID** : Select *Basic Information>Primary email*.
- On the **Attribute mapping**page, click**Add Mapping** and use the *Username*,*Primary email*.*First name*, and*Last name* Google Directory attributes and App attributes as shown in the sample image below.



1. Click **Finish**.
2. Select **Apps**>**Web and mobile apps** , and open your custom SAML app.
3. Ensure that the parameters configured for the app are appearing correctly.
4. On the **User Access**pane, click**View details** , and do the following:

- Select the required users, groups, or organizational units (OUs) to which you want to enable the service. By default, no users, groups, or organizational units have permission to access the app.

- In the **Service status**section, click**ON for everyone**, and then click**Save** to activate the service for all selected users.

1. On the **User Access**pane, in the left pane, click**Test SAML login**.

The SAML app should open in a separate tab. If it does not open, check the error messages, update your Identity Provider and Service Provider settings as needed, and then test the SAML login again.

Usually, the change takes place quickly but sometimes it may take up to 24 hours.

Enabling the Google Workspace service

After successful SAML-Based Single Sign-On configuration, administrators need to enable the Google Workspace service in the Arctera Insight Management Console.

To enable the Google Workspace service

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

On the User Management page, select **Manage Account Provisioning Remotely**>**Using Google Workspace**.

1. Click **Save**and then click**Go to next step**.
2. Ensure the **Configuration Summary** page displays the completion of the Google Workspace configuration.

Configuring Google Workspace Archiving Collector

Administrator need to set up Google Workspace archive collector in Arctera Insight Management Console for archiving user data and mail-enabled user groups from Google Workspace.

To configure Google Workspace archive

1. In the left navigation pane, select **Archive Collectors**.
2. On the **Archive Collector**page, click**Add collector** to view available collector cards.

> “ ”

Note: At the time of adding the first collector, theAdd collectorbutton appears in the middle of the screen. If one or more collectors are already added, theAdd collectoroption appears on the

top right-hand corner. If you select an unsupported collector, it disables theConfigurebutton to prevent its configuration.

> “ ”

3. Select the **Google Workspace**card and click**Configure**.

The **Google Workspace Account Provisioning** page appears.

1. On the **Provisioning and Configuration**tab, specify the following information and click**Next** to proceed to the next page.

PROVISIONING
Provisioning Domains scope
Archive Provisioning
Provision Groups in scope as Archives
Personal Archive Deployment Options
Impersonate User Email
Choose Certificate
Service User Email
Sync Scheduler
Run Now
Go to Job List
Configuration Summary

> “ ”

Credential Management Upon accessing this page, a notification is shown that prompts you to enable the API Client OAuth 2.0 scopes based on the selected provisioning options. You need to create a service account and setup a client with the necessary API Client OAuth 2.0 Scopes.

To better understand the procedures, refer to the following documentation. Create a Google Cloud Service Account Set up domain-wide delegation for a client After creating a Google Cloud Service Account and configuring domain-wide delegation for a client, click Test Connection to verify if the connection works. Scheduler Summary

> “ ”

2. After successful synchronization of accounts, in the left navigation pane, select **Configuration**>**Account Management**. Ensure that the accounts for which you have created archives are available. You can view the account user details, the status, services subscribed and enabled or disabled for users, archive aliases, and history of the account.

If the data is not getting synchronized properly, contact your system administrator.

About ChatGPT conversation data Archiving

An administrator can add a ChatGPT collector that uses the OpenAI Enterprise Compliance API to collect enterprise-level ChatGPT conversation data. The collected data includes prompts, responses, and associated metadata from the organization's ChatGPT workspace. The collector archives and indexes the data for search, legal hold, and investigation in Insight eDiscovery to support enterprise compliance, audit, and legal workflows.

You can view and configure ChatGPT chats archiving only if you are subscribed to the Capture under Primary Service and then the ChatGPT service under Capture Secondary services.

Configuring ChatGPT archive collectors

To configure a ChatGPT archive collector

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

The **Archive Collector** page appears.

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

> “ ”

Note: At the time of adding the first collector, theAdd collectorbutton appears in the middle of the screen. If one or more collectors are already added, theAdd collectoroption appears on the

top right-hand corner. If you select the collector that is not supported in Arctera Insight Archiving, theConfigurebutton gets disabled. You cannot configure such collectors.

> “ ”

2. Select the **ChatGPT**card, and click**Configure**.
3. Enter a unique name and a brief description for the collector.
4. In the **Configure EV Folder Target**drop-down, select**Yes**to allow configuring targeted EV folder or select**No** to restrict it.
5. Click **Next**.

The application creates the ChatGPT collector.

1. To configure the properties, refer to the Insight Capture Configuration Guide.

About Google Messages Archiving

An administrator can add a Google Messages collector to collect enterprise-level Google Messages conversation data. The collected data includes SMS and RCS messages and associated metadata from managed devices. The collector archives and indexes the data for search, legal hold, and investigation in Insight eDiscovery to support enterprise compliance, audit, and legal workflows.

You can view and configure Google Messages archiving only if you are subscribed to the Capture under Primary Service and then the Google Messages service under Capture Secondary services.

See Configuring Google Messages archiving collectors.

Configuring Google Messages archiving collectors

To configure a Google Messages archive collector

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

The **Archive Collector** page appears.

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

> “ ”

Note: At the time of adding the first collector, theAdd collectorbutton appears in the middle of the screen. If one or more collectors are already added, theAdd collectoroption appears on the top right-hand corner. If you select the collector that is not supported in Arctera Insight Archiving, theConfigurebutton gets disabled. You cannot configure such collectors.

> “ ”

2. Select the **Google Messages**card, and click**Configure**.
3. Enter a unique name and a brief description for the collector.
4. In the **Configure EV Folder Target**drop-down, select**Yes**to allow configuring targeted EV folder or select**No** to restrict it.
5. Click **Next**.

The application creates the Google Messages collector.

1. To configure the properties, refer to the Insight Capture Configuration Guide.

About SCIM Archiving

System for Cross-domain Identity Management (SCIM) is an open standard specification designed to manage user identity information by providing distinct schema for authentication to automate the task of data provisioning.

To archive customer data from Exchange and Active Directory, Arctera Insight Archiving relies on the O365 service that needs customer administrator credentials. To adhere with their data security policy, customers either share minimal data with Arctera Insight Archiving or want to configure SCIM independently.

Customers can use the SCIM feature to specify the data they want to share with Arctera Insight Archiving through a schema. The *Azure Active Directory Provisioning* service subsequently transfers this data from the customer's environment to the SCIM endpoint. This approach empowers customers with full control over their data.

> “ ”

Note: At present, SCIM relies on additional supporting provisioning services, such as CloudLink or O365, for functionalities like delegate permission, web folder push, and more. Consequently, it is

essential to configure any other supporting provisioning service separately from SCIM to achieve complete user provisioning.

> “ ”

The Email Alias for provisioning users accepts unregistered domains, which initially remain inactive. Upon receiving the SCIM request, Arctera Insight Archiving automatically includes these unregistered domains in the group domain. However, emails from these inactive domains cannot be archived. Customers seeking updates on such unregistered domains can contact the SCIM support team.

The following sections explain the procedure to configure SCIM, its database details, location of logs, troubleshooting solutions, and the necessary infrastructure.

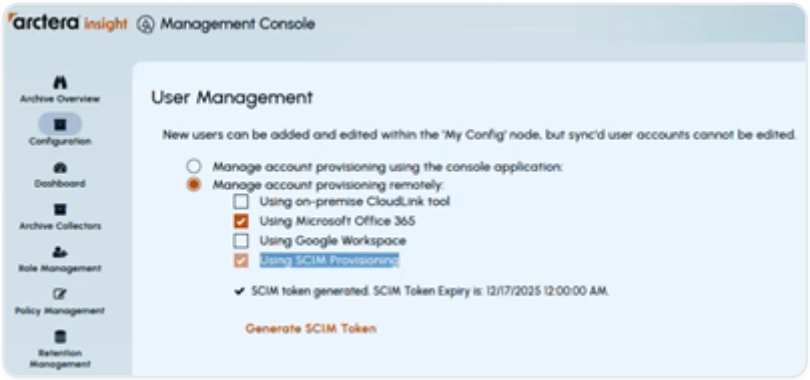
Configuring SCIM archiving by using Azure Active Directory

Configuring SCIM collectors by using SCIM provisioning

Configuring SCIM collectors by using SCIM provisioning

Prerequisite

Before configuring the SCIM collector with SCIM provisioning, ensure you select the Using SCIM Provisioning option under Manage account provisioning remotely on the User Management page in the management console.



To configure Signal archiving collectors

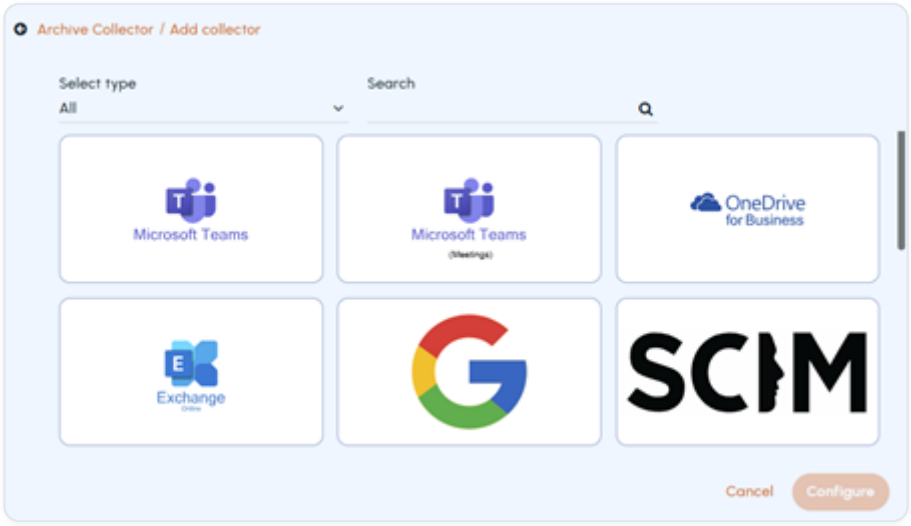
1. In the left navigation pane, select **Archive Collectors**.

The **Archive Collector** page appears.

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

Note: At the time of adding the first collector, theAdd collectorbutton appears in the middle of the screen. If one or more collectors are already added, theAdd collectoroption appears on the top right-hand corner. If you select the collector that is not supported in Arctera Insight Archiving, theConfigurebutton gets disabled. You cannot configure such collectors.

2. Select the **SCIM**card, and click**Configure**.



The **SCIM Account Provisioning** page appears.

1. In the **Credential Management**section, click**Generate New SCIM** to generate a new .

Note: Keep the SCIM secure, as you cannot copy it again after generating it. The expiry date of the is displayed for your reference.

Close the details pop-up and click **Next**.

1. In the **Provisioning**section, select options to enable Personal Archive access for provisioned accounts and to send a welcome message. Click**Compose Welcome Message Template** to define the welcome message content.

Close the welcome message pop-up and click **Next**.

1. In the **Summary**section, ensure the details. In case, you want to modify anything, click**Edit**to navigate to corresponding page. Then click**Next**.

Upon successful provisioning, the SCIM collector card is displayed on the **Archive Collectors** page. You can manage this collector from that location as well.

Configuring SCIM archiving by using Azure Active Directory

Before configuring SCIM archiving, review the following points to ensure proper configuration.

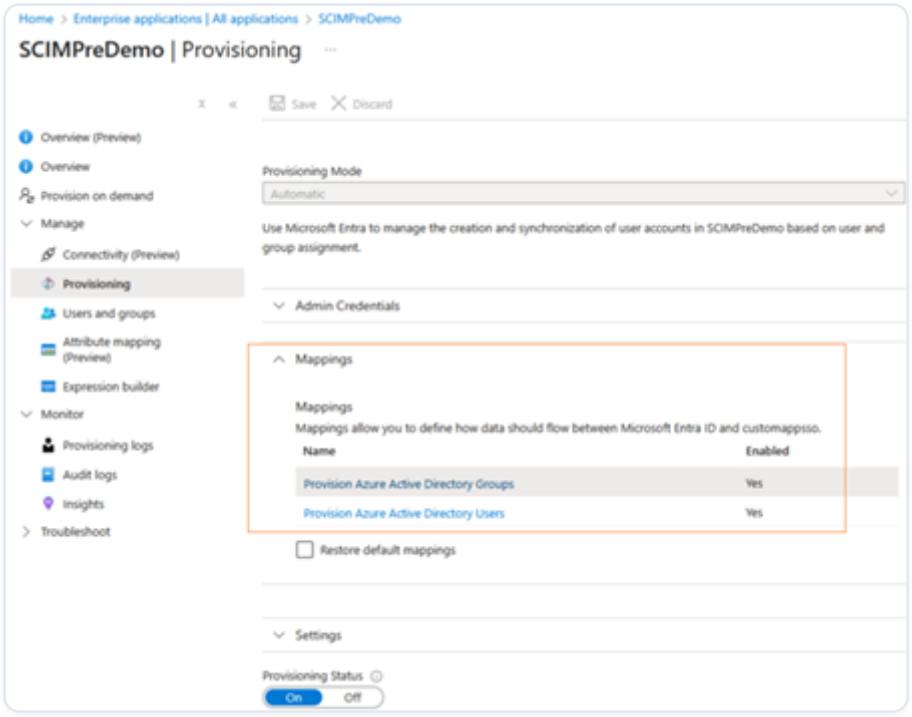
- The SCIM app pushes user and group objects along with any membership delta.
- Only direct members can be provisioned.
- Nested groups are not automatically flattened. Native recursion is not supported. Groups containing sub-groups require flat expansion.
- Users must be provisioned before groups. Azure AD enforces this sequence. If Insight Archiving rejects membership references, groups are created but members remain empty until users exist.
- Guest users with object IDs in Azure AD can be provisioned and assigned as members in Insight Archiving.
- Shared mailboxes are supported if they are in scope and active.

To configure SCIM archiving by using Azure Active Directory

1. Ensure that your enterprise application is added to your Azure Active Directory tenant.

For more information, refer to Adding an application on Azure AD portal

1. Sign in to the Microsoft Entra admin center as an Administrator.
2. Browse to **Entra ID**>**Enterprise Applications** , and select your application.
3. In the left navigation pane, select **Provisioning**.
4. On the Provisioning page, expand the **Mappings** section.



5. To provision the **Users** attribute mapping, perform the following steps:

   - Ensure that the **Provision Azure Active Directory Users** option is enabled. Click to select it.
   - On the **Attribute Mapping**page, the existing mapping properties are displayed. To add more mapping properties, click**Add New Mappings**. To edit existing properties, select the**Show Advanced Options**check box and click**Edit attribute list for customappsso**.
   - Refer the user attribute mappings below:

     > “ ”

     Note: Create the SCIM schema in enterprise application. While creating the SCIM schema, you can set the attribute precedence ofPrimaryEmailAddressandUsernameas 1 or 2, as required. For example, if you set the attribute precedence ofPrimaryEmailAddressas 1, then the attribute precedence ofUsernameis consequently set as 2. If you set the attribute precedence ofUsernameas 1, then the attribute precedence ofPrimaryEmailAddressis consequently set as 2.

     > “ ”

For more information, refer to Creating schema in enterprise application.

AD ATTRIBUTE	ARCTERA SCIM ATTRIBUTES / MATCHING PRECEDENCE	ARCTERA INSIGHT ARCHIVING SOURCE ATTRIBUTES	EXAMPLE DATA
User.Mail	emails\[type eq "work"\].value, IsPrimary=true	PrimaryEmailAddress	jsmith@organization1.com
	/ 1		
Append(\[extensionAttribute1\] + @organization1.com)	userName	UserName	abc1abc@organization1.com
	/ 2		
givenName	name.givenName	FirstName	John
Surname	name.familyName	LastName	Smith
displayName	displayName	DisplayName	John Smith
accountEnabled	active	IsArchive	TRUE
proxyAddresses	emails\[type eq "work"\].value,IsPrimary=false	EmailAliases	"smtp:user1@organization1.mail.on
			"smtp:user1_alias@organization1.C

1. To provision **Groups** , perform the following steps:
    - Ensure that the **Provision Azure Active Directory Groups** option is enabled. Click to select it.
    - On the **Attribute Mapping**page, the existing mapping properties are displayed. To add more mapping properties, click**Add New Mappings**. To edit existing properties, select the**Show Advanced Options**check box and click**Edit attribute list for customappsso**.
    - Refer the group attribute mappings below:

> “ ”

Note: UseDisplayNameas Primary Mapping attribute.

> “ ”

GROUP ATTRIBUTE	APP ATTRIBUTE NAME	IS CUSTOM ATTRIBUTE
displayName	displayName	No
objectId	externalId	No
members	members	No
description	urn:ietf:params:scim:schemas:extension:veritas:2.0:Group:description	Yes
Mail	urn:ietf:params:scim:schemas:extension:veritas:2.0:Group:mail	Yes
securityEnabled	urn:ietf:params:scim:schemas:extension:veritas:2.0:Group:securityEnabled	Yes
mailEnabled	urn:ietf:params:scim:schemas:extension:veritas:2.0:Group:mailEnabled	Yes

2. After all of the required mappings are configured, select **Save**.
3. After successful configuration, generate a token from Management Console.
4. Click **Generate**.
5. Copy the generated token, and click **OK**.
6. Click **Save**.
7. Enter the copied token in the Secret field in the Azure enterprise application.
8. Click **Test connection** to complete the configuration.

If the testing is successful, configuration is considered as complete. If the testing is unsuccessful, contact the support team.

About Import Collector

As an administrator, you can create and enable the Data Uploading archive collector in Arctera Insight Management Console.

The data import collector can collect files with ZIP, PDF, DOC, DOCX, PPT, PPTX, XLS, XLSX, CSV, PST, EML, MSG, and DAT extensions. You can bundle files with these extensions into a ZIP file for importing.

Configuring an Import collector

You must have a *Customer Administrator* role to configure an Import collector.

To configure an Import collector

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

The **Archive Collector** page appears.

> “ ”

Note: TheArchive Collectorsnode 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.

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

Alternatively, in the **Select Type**drop-down, select**File Sharing**. The corresponding collector cards are displayed.

1. Select the **Import**card and click**Configure**.
2. 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.

3. Click **Save**.

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

> “ ”

Note: If theFile Importarchive collector is no more required, select this collector on theArchive Collectorspage. Click the kebab icon (three vertical dots) on the archive collector card, and clickDelete. The application prompts you to confirm that you want to perform the operation. ClickYes.

> “ ”

About Insight Capture Services Archiving

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

The customers who are enabled for only the Insight Capture primary service get lesser administration options when they login to the Arctera Insight Management 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.

- 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 Insight Capture Secondary Services if you have subscribed for these services (purchased a user license).

Microsoft Teams via Export API | Microsoft Teams (Audio Video) | Exchange Mailbox Graph | Microsoft Teams via Webhooks | Slack Insight eDiscovery | Bloomberg | IceChat | Twitter | OneDrive for Business | Box | Google Drive | Citrix Workspace & Sharefile | Dropbox Business | SharePoint | Amazon | EML | Blackberry | Viva Engage | 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 | Cloud9 | Verba

Enabling Insight Capture Services for Archiving

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

To enable Insight 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 Arctera Insight Archiving Customer Administration Guide.

> “ ”

Note: The customers who are enabled for the Insight Capture services only can see lesser Administration options when they login to the Arctera Insight Management Console . Such customers do not requireJournaling Address. In addition, while adding the customer account, on theAccounts>Add Accountpage, theAdmincheck 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.

1. In the **Services** section.

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

  > “ ”

  Note: Unless theCaptureoption is enabled under primary services, you cannot enable theCapture Secondary Servicessecondary 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.

1. Click **Save**.
2. To verify if the selected Capture secondary services are enabled for the customer, in Arctera Insight Management Console , login as a Customer Administrator.
3. In the left navigation pane, select **Configuration**>**Services**.
4. 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, selectCustomer Service>Customers. Select the customer and clear the check box of the selected Capture secondary services in theEnabledcolumn.

   > “ ”

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.

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

> “ ”

Note: At the time of adding a collector for the first time, theAdd collectorbutton appears in the middle of the screen. If one or more collectors are already added, theAdd collectoroption appears on the top right-hand corner. If you select the collector that is not supported in Arctera Insight Archiving, theConfigurebutton gets disabled. You cannot configure such collectors.

> “ ”

2. 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.

1. Select the collector that you want to configure, and click **Configure**.

The **Add Importer** dialog box appears.

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

The application redirects you to the Insight Capture portal. On the Insight 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.

1. 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.

> “ ”

2. Provide the configuration details in the configuration wizard.

> “ ”

Note: Refer to theArctera Insight Capture Configuration Guideto understand configuration fields of corresponding archive collectors (importers) and complete the configuration steps.

> “ ”

After successful configuration, the archive collector appears in the Arctera Insight Management Console .

1. On the Arctera Insight Management Console , select **Archive Collectors**.

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

1. 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.

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

About Microsoft Teams (Audio Video) Archiving

You can view and configure Microsoft Teams audio-video archiving collector only if you are subscribed to the Capture under Primary Service and then the Microsoft Teams (Audio Video) service under Capture Secondary services.

Configuring Microsoft Teams (Audio Video) archiving collectors

To configure Microsoft Teams (Audio Video) archiving collectors

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

The **Archive Collector** page appears.

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

> “ ”

Note: At the time of adding the first collector, theAdd collectorbutton appears in the middle of the screen. If one or more collectors are already added, theAdd collectoroption appears on the top right-hand corner. If you select the collector that is not supported in Arctera Insight Archiving, theConfigurebutton gets disabled. You cannot configure such collectors.

> “ ”

2. Select the **Microsoft Teams (Audio Video)card, and clickConfigure**.
3. Enter a unique name and a brief description for the collector.
4. In the **Configure EV Folder Target**drop-down, select**Yes**to allow configuring targeted EV folder or select**No** to restrict it.
5. Click **Next**.

The application creates the Microsoft Teams (Audio Video) collector.

1. To configure the properties, refer to the Insight Capture Configuration Guide.

About Audio-Video Archiving

You can view and configure audio-video archiving only if you are subscribed to the Capture under Primary Service and then the Audio-Video service under Capture Secondary services.

Configuring audio-video archiving collectors

To configure audio-video archiving collectors

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

The **Archive Collector** page appears.

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

> “ ”

Note: At the time of adding the first collector, theAdd collectorbutton appears in the middle of the screen. If one or more collectors are already added, theAdd collectoroption appears on the

top right-hand corner. If you select the collector that is not supported in Arctera Insight Archiving, theConfigurebutton gets disabled. You cannot configure such collectors.

> “ ”

2. Select the **Audio-Video**card, and click**Configure**.
3. Enter a unique name and a brief description for the collector.
4. In the **Format Type** drop-down, select the required audio-video collection type. Currently, you can select format type from the following available options:

FORMAT TYPE	FORMAT TYPE ID
Zoom	150
Teams	155
Webex Teams	151
Vodafone	157
IPC	158
Cisco	159
Avaya	160
Audio File	153
Video File	154

If you do not select any of the available options, by default the format type ID 156 is applied.

1. In the **Configure EV Folder Target**drop-down, select**Yes**to allow configuring targeted EV folder or select**No** to restrict it.
2. Click **Next**.

The application creates the Audio-Video collector.

1. To configure the properties, refer to the Insight Capture Configuration Guide.

About Audio-Video Archiving using NTR-X Collectors

You can view and configure audio-video archiving by using the NTR-X collector only if you are subscribed to the Capture under Primary Service and then the Audio-Video service under Capture Secondary services.

Configuring audio-video archiving using NTR-X collectors

To configure audio-video archiving by using the NTR-X collector

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

The **Archive Collector** page appears.

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

> “ ”

Note: At the time of adding the first collector, theAdd collectorbutton appears in the middle of the screen. If one or more collectors are already added, theAdd collectoroption appears on the top right-hand corner. If you select the collector that is not supported in Arctera Insight Archiving, theConfigurebutton gets disabled. You cannot configure such collectors.

> “ ”

2. Select the **NTR-X**card, and click**Configure**.
3. Enter a unique name and a brief description for the collector.
4. In the **Format Type** drop-down, select the required format type. Currently, you can select format type from the following available options:

FORMAT TYPE	FORMAT TYPE ID
Audio-Video	156
IPC	158

5. In the **Configure EV Folder Target**drop-down, select**Yes**to allow configuring targeted EV folder or select**No** to restrict it.
6. Click **Next**.

The application navigates you to the *Configuration Wizard* for further configuration.

1. To configure the properties, refer to the Insight Capture Configuration Guide.
    - If you do not select any of the available options, by default the **Audio-Video** format type is applied.
    - If you select the **Audio-Video** format type, it appears as below.
    - If you select the **IPC** format type, it appears as below.

About Dubber Speik SMS Archiving

You can view and configure Dubber Speik SMS archiving only if you are subscribed to the Capture under Primary Service and then the Dubber Speik SMS service under Capture Secondary services.

Configuring Dubber Speik SMS archiving collectors

To configure a Dubber Speik SMS archive collector

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

The **Archive Collector** page appears.

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

    > “ ”

    Note: At the time of adding the first collector, theAdd collectorbutton appears in the middle of the screen. If one or more collectors are already added, theAdd collectoroption appears on the top right-hand corner. If you select the collector that is not supported in Arctera Insight Archiving, theConfigurebutton gets disabled. You cannot configure such collectors.

    > “ ”

2. Select the **Dubber Speik SMS**card, and click**Configure**.
3. Enter a unique name a brief description for the collector.
4. In the **Configure EV Folder Target**drop-down, select**Yes**to allow configuring targeted EV folder or select**No** to restrict it.
5. Click **Next**.

The application creates the Dubber Speik SMS collector.

1. To configure the properties, refer to the Insight Capture Configuration Guide.

About Dubber Speik Recordings Archiving

You can view and configure Dubber Speik Recordings archiving only if you are subscribed to the Capture under Primary Service and then the Dubber Speik Recordings service under Capture Secondary services.

Configuring Dubber Speik Recordings archive collectors

To configure a Dubber Speik Recordings archive collector

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

The **Archive Collector** page appears.

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

   > “ ”

   Note: At the time of adding the first collector, theAdd collectorbutton appears in the middle of the screen. If one or more collectors are already added, theAdd collectoroption appears on the top right-hand corner. If you select the collector that is not supported in Arctera Insight Archiving, theConfigurebutton gets disabled. You cannot configure such collectors.

   > “ ”

2. Select the **Dubber Speik Recordings**card, and click**Configure**.
3. Enter a unique name a brief description for the collector.
4. In the **Format Type** drop-down, select the required recording format type. Currently, you can select format type from the following available options:

FORMAT TYPE	FORMAT TYPE ID
Zoom	150
MS Teams	155

FORMAT TYPE	FORMAT TYPE ID
Mobilephone	Not Applicable
Webex Teams	151

The collector card's name and icon vary depending on the selected format type. When you select *Zoom*,*MS Teams*, or*Webex Teams*as format types, the collector card exhibits the relevant name and icon. For instance, after selecting the format type as Zoom, the collector card displays the name as*Zoom Meetings*and showcases the*Zoom* icon, as shown in the sample image below:

However, when you select *Mobilephone*as format type or when you do not select any of the available options, the collector card displays the name as*Dubber Speik Recordings*and showcases the*Dubber Speik Recording* icon.

1. In the **Configure EV Folder Target**drop-down, select**Yes**to allow configuring targeted EV folder or select**No** to restrict it.
2. Click **Next**.

The application creates the Dubber Speik Recording collector.

1. To configure the properties, refer to the Insight Capture Configuration Guide.

About Text-Delimited Archiving

You can view and configure Text-Delimited archiving only if you are subscribed to the Capture under Primary Service and then the Text-Delimited service under Capture Secondary services.

Configuring Text-Delimited archiving collectors

To configure Text-Delimited archiving collectors

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

The **Archive Collector** page appears.

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

> “ ”

Note: At the time of adding the first collector, theAdd collectorbutton appears in the middle of the screen. If one or more collectors are already added, theAdd collectoroption appears on the top right-hand corner. If you select the collector that is not supported in Arctera Insight Archiving, theConfigurebutton gets disabled. You cannot configure such collectors.

> “ ”

2. Select the **Text-Delimited**card, and click**Configure**.
3. Enter a unique name a brief description for the collector.

In the **Format Type** drop-down, select the required Text-Delimited collection type. Currently, you can select format type from the following available options:

FORMAT TYPE	FORMAT TYPE ID
SMS	109
WhatsApp	110
Twitter (EML)	135
ZoomChat (EML)	137
Carbon	181
ENMACC Energy	182
Legato Chat	183
LiquidNet	184
Markets Manager	185
Saphyre	186
Skytel-Pager	187
Social	188
Web CHAT	189
WeChat	190

If you do not select any of the available options, by default the format type ID 156 is applied.

1. Click **Next**.

The application creates the Text-Delimited collector.

1. To configure the properties, refer to the Insight Capture Configuration Guide.

About XSLT-XML Archiving

You can view and configure XSLT-XML archiving only if you are subscribed to the Capture under Primary Service and then the XSLT-XML service under Capture Secondary services.

Configuring XSLT-XML archiving collectors

To configure XSLT-XML archiving collectors

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

The **Archive Collector** page appears.

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

> “ ”

Note: At the time of adding the first collector, theAdd collectorbutton appears in the middle of the screen. If one or more collectors are already added, theAdd collectoroption appears on the top right-hand corner. If you select the collector that is not supported in Arctera Insight Archiving, theConfigurebutton gets disabled. You cannot configure such collectors.

> “ ”

2. Select the **XSLT-XML**card, and click**Configure**.
3. Enter a unique name a brief description for the collector.

In the **Format Type** drop-down, select the required XSLT-XML collection type. Currently, you can select format type from the following available options:

FORMAT TYPE	FORMAT TYPE ID
UBS	104

FORMAT TYPE	FORMAT TYPE ID
Pivot	107
SMS	109
WhatsApp	110
CellTrust	114
Social	188
WeChat	190
Facetime	192
LinkedIn Audit	193
Merrill-DataSite	194
Trade Web	195

If you do not select any of the available options, by default the format type ID 156 is applied.

1. Click **Next**.

The application creates the XSLT-XML collector.

1. To configure the properties, refer to the Insight Capture Configuration Guide.

About JSON Archiving

You can view and configure JSON archiving only if you are subscribed to the Capture under Primary Service and then the JSON service under Capture Secondary services.

Configuring JSON archiving collectors

To configure JSON archiving collectors

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

The **Archive Collector** page appears.

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

> “ ”

Note: At the time of adding the first collector, theAdd collectorbutton appears in the middle of the screen. If one or more collectors are already added, theAdd collectoroption appears on the top right-hand corner. If you select the collector that is not supported in Arctera Insight Archiving, theConfigurebutton gets disabled. You cannot configure such collectors.

> “ ”

2. Select the **JSON**card, and click**Configure**.
3. Enter a unique name a brief description for the collector.
4. In the **Format Type** drop-down, select the required JSON collection type. Currently, you can select format type from the following available options:

FORMAT TYPE	FORMAT TYPE ID
Workplace from Facebook	117
Sharepoint (EML)	133

If you do not select any of the available options, by default the format type ID 156 is applied.

1. In the **Configure EV Folder Target**drop-down, select**Yes**to allow configuring targeted EV folder or select**No** to restrict it.
2. Click **Next**.

The application creates the JSON collector.

1. To configure the properties, refer to the Insight Capture Configuration Guide.

About iMessage Archiving

You can view and configure iMessage archiving only if you are subscribed to the Capture under Primary Service and then the iMessage service under Capture Secondary services.

Configuring iMessage archiving collectors

To configure iMessage archiving collectors

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

The **Archive Collector** page appears.

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

> “ ”

Note: At the time of adding the first collector, theAdd collectorbutton appears in the middle of the screen. If one or more collectors are already added, theAdd collectoroption appears on the top right-hand corner. If you select the collector that is not supported in Arctera Insight Archiving, theConfigurebutton gets disabled. You cannot configure such collectors.

> “ ”

2. Select the **iMessage**card, and click**Configure**.
3. Enter a unique name a brief description for the collector.
4. In the **Configure EV Folder Target**drop-down, select**Yes**to allow configuring targeted EV folder or select**No** to restrict it.
5. Click **Next**.

The application creates the iMessage collector.

1. To configure the properties, refer to the Insight Capture Configuration Guide.

About LinkedIn Archiving

You can view and configure LinkedIn archiving only if you are subscribed to the Capture under Primary Service and then the LinkedIn service under Capture Secondary services.

Configuring LinkedIn archiving collectors

To configure LinkedIn archiving collectors

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

The **Archive Collector** page appears.

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

> “ ”

Note: At the time of adding the first collector, theAdd collectorbutton appears in the middle of the screen. If one or more collectors are already added, theAdd collectoroption appears on the top right-hand corner. If you select the collector that is not supported in Arctera Insight Archiving, theConfigurebutton gets disabled. You cannot configure such collectors.

> “ ”

2. Select the **LinkedIn**card, and click**Configure**.
3. Enter a unique name a brief description for the collector.
4. Click **Next**.

The application creates the LinkedIn collector.

1. To configure the properties, refer to the Insight Capture Configuration Guide.

About Signal Archiving

You can view and configure Signal archiving only if you are subscribed to the Capture under Primary Service and then the Signal service under Capture Secondary services.

Configuring Signal archiving collectors

To configure Signal archiving collectors

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

The **Archive Collector** page appears.

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

> “ ”

Note: At the time of adding the first collector, theAdd collectorbutton appears in the middle of the screen. If one or more collectors are already added, theAdd collectoroption appears on the top right-hand corner. If you select the collector that is not supported in Arctera Insight Archiving, theConfigurebutton gets disabled. You cannot configure such collectors.

> “ ”

2. Select the **Signal**card, and click**Configure**.
3. Enter a unique name a brief description for the collector.
4. Click **Next**.

The application creates the Signal collector.

1. To configure the properties, refer to the Insight Capture Configuration Guide.

About Verint Archiving

You can view and configure Verint archiving only if you are subscribed to the Capture under Primary Service and then the Verint service under Capture Secondary services.

Configuring Verint archiving collectors

To configure Verint archiving collectors

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

The **Archive Collector** page appears.

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

> “ ”

> **Note:** At the time of adding the first collector, theAdd collectorbutton appears in the middle of the screen. If one or more collectors are already added, theAdd collectoroption appears on the top right-hand corner. If you select the collector that is not supported in Arctera Insight Archiving, theConfigurebutton gets disabled. You cannot configure such collectors.

> “ ”

2. Select the **Verint**card, and click**Configure**.
3. Enter a unique name a brief description for the collector.
4. Click **Next**.

The application creates the Verint collector.

1. To configure the properties, refer to the Insight Capture Configuration Guide.

About WeChat Archiving

You can view and configure WeChat archiving only if you are subscribed to the Capture under Primary Service and then the WeChat service under Capture Secondary services.

Configuring WeChat archiving collectors

To configure WeChat archiving collectors

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

The **Archive Collector** page appears.

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

   > “ ”

   Note: At the time of adding the first collector, theAdd collectorbutton appears in the middle of the screen. If one or more collectors are already added, theAdd collectoroption appears on the top right-hand corner. If you select the collector that is not supported in Arctera Insight Archiving, theConfigurebutton gets disabled. You cannot configure such collectors.

   > “ ”

2. Select the **WeChat**card, and click**Configure**.
3. Enter a unique name a brief description for the collector.
4. Click **Next**.

The application creates the WeChat collector.

1. To configure the properties, refer to the Insight Capture Configuration Guide.

About WhatsApp Archiving

You can view and configure WhatsApp archiving only if you are subscribed to the Capture under Primary Service and then the WhatsApp service under Capture Secondary services.

Configuring WhatsApp archiving collectors

To configure WhatsApp archiving collectors

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

The **Archive Collector** page appears.

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

> “ ”

Note: At the time of adding the first collector, theAdd collectorbutton appears in the middle of the screen. If one or more collectors are already added, theAdd collectoroption appears on the top right-hand corner. If you select the collector that is not supported in Arctera Insight Archiving, theConfigurebutton gets disabled. You cannot configure such collectors.

> “ ”

2. Select the **WhatsApp**card, and click**Configure**.
3. Enter a unique name a brief description for the collector.
4. Click **Next**.

The application creates the WhatsApp collector.

1. To configure the properties, refer to the Insight Capture Configuration Guide.

About Cloud9 Archiving

You can view and configure Cloud9 archiving collector only if you are subscribed to the Capture under Primary Service and then the Cloud9 service under Capture Secondary services.

Configuring Cloud9 archiving collectors

To configure Cloud9 archiving collectors

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

The **Archive Collector** page appears.

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

> “ ”

Note: At the time of adding the first collector, theAdd collectorbutton appears in the middle of the screen. If one or more collectors are already added, theAdd collectoroption appears on the top right-hand corner. If you select the collector that is not supported in Arctera Insight Archiving, theConfigurebutton gets disabled. You cannot configure such collectors.

> “ ”

2. Select the **Cloud9**card, and click**Configure**.
3. Enter a unique name and a brief description for the collector.
4. In the **Configure EV Folder Target**drop-down, select**Yes**to allow configuring targeted EV folder or select**No** to restrict it.
5. Click **Next**.

The application creates the Cloud9 collector.

1. To configure the properties, refer to the Insight Capture Configuration Guide.

About Verba Archiving

You can view and configure Verba archiving only if you are subscribed to the Capture under Primary Service and then the Verba service under Capture Secondary services.

Configuring Verba archiving collectors

To configure Verba archiving collectors

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

The **Archive Collector** page appears.

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

> “ ”

Note: At the time of adding the first collector, theAdd collectorbutton appears in the middle of the screen. If one or more collectors are already added, theAdd collectoroption appears on the

top right-hand corner. If you select the collector that is not supported in Arctera Insight Archiving, theConfigurebutton gets disabled. You cannot configure such collectors.

> “ ”

2. Select the **Verba**card, and click**Configure**.
3. Enter a unique name and a brief description for the collector.
4. In the **Format Type** drop-down, select the required Verba collection type. Currently, you can select format type from the following available options:

FORMAT TYPE	FORMAT TYPE ID
Zoom	150
Teams Audio and Video	155
Cisco	159

If you do not select any of the available options, by default the format type ID 156 is applied.

1. In the **Configure EV Folder Target**drop-down, select**Yes**to allow configuring targeted EV folder or select**No** to restrict it.
2. Click **Next**.

The application creates the Verba collector.

1. To configure the properties, refer to the Insight Capture Configuration Guide.

About Copilot Archiving

You can view and configure Copilot archiving only if you are subscribed to the Capture under Primary Service and then the Copilot service under Capture Secondary services.

Configuring Copilot archiving collectors

To configure Copilot archiving collectors

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

The **Archive Collector** page appears.

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

> “ ”

Note: At the time of adding the first collector, theAdd collectorbutton appears in the middle of the screen. If one or more collectors are already added, theAdd collectoroption appears on the top right-hand corner. If you select the collector that is not supported in Arctera Insight Archiving, theConfigurebutton gets disabled. You cannot configure such collectors.

> “ ”

2. Select the **Copilot**card, and click**Configure**.
3. Enter a unique name and a brief description for the collector.
4. In the **Configure EV Folder Target**drop-down, select**Yes**to allow configuring targeted EV folder or select**No** to restrict it.
5. Click **Next**.

The application creates the Copilot collector.

1. To configure the properties, refer to the Insight Capture Configuration Guide.

About Zoom Phone Archiving

You can view and configure Zoom Phone archiving only if you are subscribed to the Capture under Primary Service and then the Zoom Phone service under Capture Secondary services.

Configuring Zoom Phone archiving collectors

To configure Zoom Phone archiving collectors

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

The **Archive Collector** page appears.

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

> “ ”

Note: At the time of adding the first collector, theAdd collectorbutton appears in the middle of the screen. If one or more collectors are already added, theAdd collectoroption appears on the top right-hand corner. If you select the collector that is not supported in Arctera Insight Archiving, theConfigurebutton gets disabled. You cannot configure such collectors.

> “ ”

2. Select the **Zoom Phone**card, and click**Configure**.
3. Enter a unique name and a brief description for the collector.
4. In the **Configure EV Folder Target**drop-down, select**Yes**to allow configuring targeted EV folder or select**No** to restrict it.
5. Click **Next**.

The application creates the Zoom Phone collector.

1. To configure the properties, refer to the Insight Capture Configuration Guide.

Managing Roles and Permissions

This section includes the following topics:

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.

> “ ”

Note: After each administrative roles or permissions modification, the resultingActivity Logreport displays logs/events for added or removed roles and permissions in both built-in and custom roles, along with a user who modified the permissions, users who are modified for which roles and permissions, and date/time of modification. TheActivity Logprovides detailed logs for events when a user's built-in role is changed during a bulk account import, including which role has been

assigned or unassigned, which user made the changes, and the event date and time. For more information on Activity Log, SeeViewing the Activity Log.

> “ ”

Editing the built-in administrator roles

Arctera Insight 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)
- Insight eDiscovery Administrator - configures and manages Arctera Insight eDiscovery usage
- System administrator - oversees all Insight 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 editShare Export,Download Export, andPrivilege Deletepermissions for the Insight 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 theArchive Overviewpermission.

   > “ ”

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 Arctera Insight 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

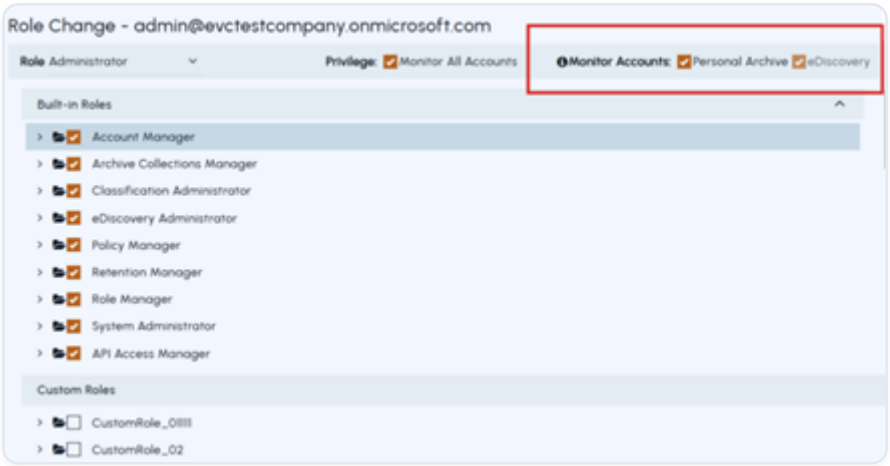
1. In the left navigation pane, select **Role Management**>**Assign Accounts**.
2. Search for and select the archive account to which you want to assign the administrator role. The **Role Change** page appears.

To search for the required archive account, you can use any of the following methods.

- Enter the user name or email of the archive account in the search field, and click the **Search** icon.
- In *Advanced Search* , enter the email, name, or role, and click **Apply**.
- Select a role in the *Roles* section. The filtered options appears automatically.

1. In the **Role**drop-down, select**Administrator**.
2. In the **Privilege**field, select the**Monitor All Accounts** check box.

Administrators can control the visibility of monitored accounts in Insight eDiscovery and Insight Personal Archive. Both the options are selected by default as shown in the image below.



- **Insight eDiscovery** \- This option is available if your organization has subscribed to Arctera Insight eDiscovery primary service.
    - Select this option if you want to monitor user accounts in your Arctera Insight eDiscovery.

    - Clear this option if you do not want to monitor user accounts in your Arctera Insight eDiscovery.

- **Insight Personal Archive** \- This option is available if your organization has subscribed to Insight Personal Archive primary service.
    - Select this option if you want to monitor user accounts in your Insight Personal Archive.
    - Clear this option if you do not want to monitor user accounts in your Insight Personal Archive.

1. 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.
2. Click **Save**.

Assigning the reviewer role to an archive account

If your organization subscribes to Insight eDiscovery and Insight Personal Archive, you can assign the reviewer role to an archive account. The reviewer role includes an additional functionality of searching and reviewing an organization's data to respond to any discovery or investigation request.

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 **Role Change** page appears.

To search for the required archive account, you can use any of the following methods.

- Enter the user name or email of the archive account in the search field, and click the **Search** icon.
- In *Advanced Search* , enter the email, name, or role, and click **Apply**.
- Select a role in the *Roles* section. The filtered options appears automatically.

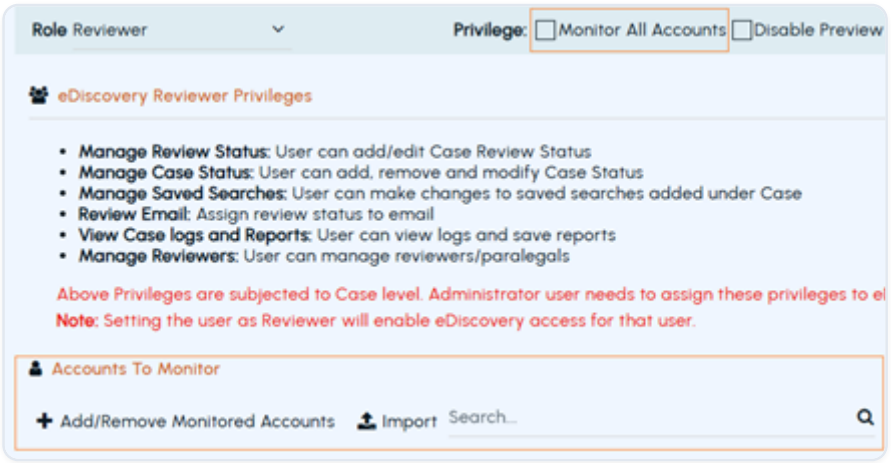
1. In the **Role**drop-down, select**Reviewer**.

The **Privilege** field displays the following options.

- **Monitor All Accounts** :

- Select this option to allow the selected user account to 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.
- Clear this option to allow the selected user account to view the archived messages of specific archive accounts.

Upon clearing this option, the **Accounts to Monitor** section appears.

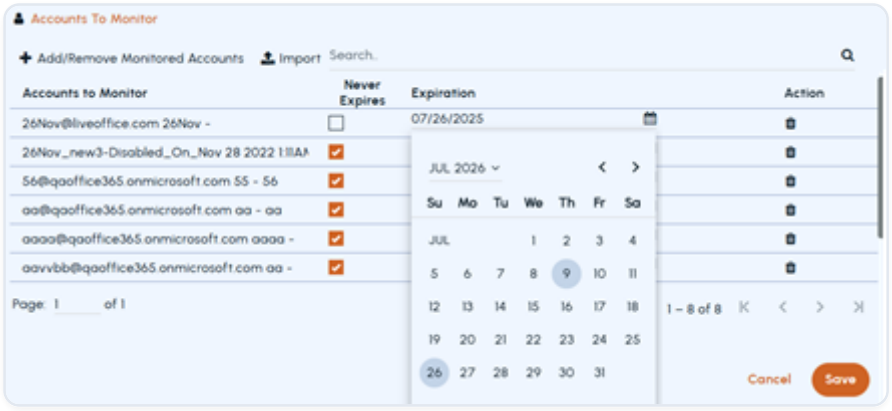


Click **Add/Remove Monitored Accounts**and select the archive accounts that you want the reviewer to monitor. Click**Save**.

If you want to import monitored accounts, click **Import**. See Assigning multiple archive accounts for monitoring.

- **eDiscovery Reviewer** : This option is selected by default. When you define a user as a reviewer, this user gets access to the Insight eDiscovery application. The *eDiscovery 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 eDiscovery Reviewers to perform various actions while reviewing the cases.
- **Disable Preview Emails** : Select this option to prevent the reviewer from previewing emails from other archive accounts.
- **Case Creation** : Select this option to allow the reviewer to create cases in Insight eDiscovery.

1. To set an expiry date for a reviewer's access to monitored accounts, clear the checkbox under **Never Expires**, then click the**Calendar**icon in the**Expiration** column and select the desired date.



2. If a previously added monitored account is no longer required, click the **Delete** icon in its row.
3. Click **Save**.

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

> “ ”

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

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 Insight 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.

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

The **Import Monitor Accounts** window appears.

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

1. 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.
2. Retain (do not delete) the **PrimaryEmailAddress** column heading in the .CSV file.
3. Delete all the text (including these instructions) below the **PrimaryEmailAddress** column heading.
4. Use only primary email addresses of the archive accounts.
5. 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.
6. Click **Import**in the**Import Monitor Accounts** window.
7. On the **Role Change**page, click**Save**.

Assigning the Department Reviewer Role

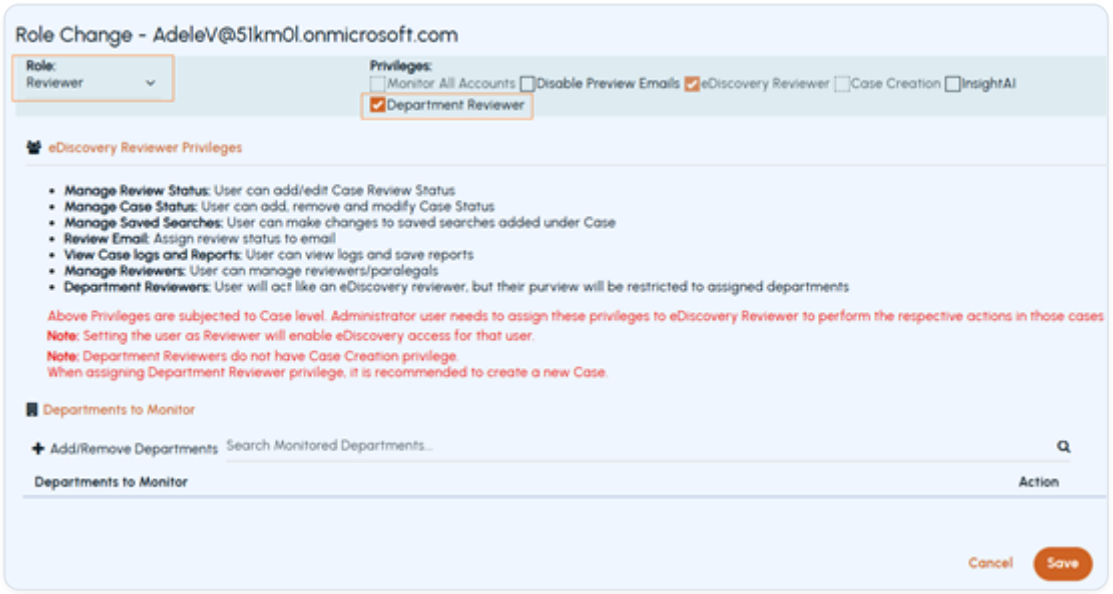
If your organization subscribes to Insight eDiscovery, you can assign the *Department Reviewer* role to a user. This role provides additional privileges for searching and reviewing department-specific data to support discovery and investigation requests.

Some important facts about this role:

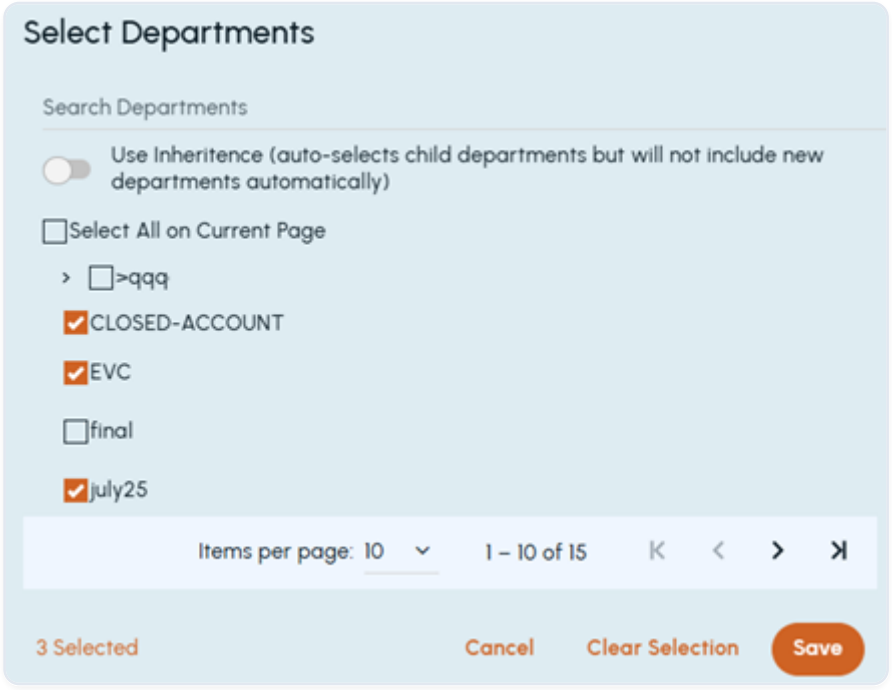
- A Department Reviewer can see emails, collaboration messages, and files only from the departments assigned to them.
- A Department Reviewer cannot access the *On-going Search* node and cannot create ongoing searches.
- A Department Reviewer role cannot access Legal Hold, Tag, or Retention Tag functionalities, as these features are not yet available for this role.
- If the Department Reviewer previously served as a normal *Reviewer*(to review custodian), any saved searches created under that role remain accessible under the*Standard Searches* node even after being a Department Reviewer. You must rerun the search to view results specific to your assigned departments.
- When switching between the Reviewer and the Department Reviewer roles, the application displays a notification indicating that the search was created with a different role. The user must rerun the search to generate accurate results.

To assign the Department Reviewer Role

1. In the left navigation pane, select **Role Management**>**Assign Accounts**.
2. Search for and select the user to assign the Department Reviewer role. The **Role Change**page appears.**Note**: To search for the required user, enter the user name or email in the search field and click the**Search**icon. Or, expand**Advanced Search**, enter the email, name, or role, and click Apply. Or, expand the**Roles** section and select a role.
3. In the **Role**drop-down, select**Reviewer**.



4. Under **Privilege**, select the**Department Reviewer**checkbox. The application disables the**Monitor All Accounts**and**Case Creation**privilege options.**Note**: To grant access to the**InsightAI**feature in Insight eDiscovery, also select the**InsightAI** checkbox.
5. Under **Departments to Monitor**, click**Add/Remove Departments**. The**Select Departments** dialog appears.



6. In the **Select Departments** dialog box, do the following as needed:
   - (Optional) Turn on **Use Inheritance to auto-select child departments (new departments are not included automatically)**.
   - To select all departments on the page, select the **Select All on Current Page** checkbox.
   - To select specific departments, manually select the required check boxes. Use navigation arrows to move between pages if the list is long. Review the count of selected departments at the bottom (for example, 1 Selected). Click **Save**.
   - To clear the field values in the dialog box, click **Clear Selection**. To exit without saving, click**Cancel**.
7. To remove a department, click the **Delete** icon in the corresponding row.
8. On the **Role Change**page, click**Save**.

Assigning roles, privileges, and monitored accounts to Azure AD groups

The Management Console supports synchronizing Azure Active Directory (AD) groups through SCIM or AD Sync. This capability allows administrators to centrally manage access to AD groups.

The Assign Active Directory Groups feature enables administrators to assign roles and privileges to AD groups directly from the Management Console. This reduces the need to manage reviewer roles on individual users-basis.

Before you use this feature, note the following facts:

- By default, all synchronized AD groups are assigned the None role. At this stage, effective role and privileges of each member will be either their individual user role or other AD groups the user belongs to.
- When administrators assign the Reviewer role at the AD group level, all direct members of the AD group automatically inherit the assigned reviewer privileges. A maximum of 100 members (user accounts) from a single AD group can be assigned case-level reviewer privileges.
- Only the direct group members can be assigned the Reviewer role. The nested groups and their members cannot be assigned the Reviewer role.
- The administrator can add, remove, and import monitored accounts while assigning roles and privileges to the AD group.
- The Expiry date for monitored accounts will be highest date assigned from Individual user and all AD groups.
- AD groups assigned with the Reviewer role can be selected as reviewers in Insight eDiscovery. However, the AD group role cannot be changed using Insight eDiscovery.
- Administrators can assign case-level reviewer privileges to an AD group. All direct members of the AD group automatically inherit the assigned reviewer privileges for the selected case. When an AD group is added as a case reviewer, all its members are added as reviewers for the case.
- If an AD group is deleted during synchronization, members of that AD group no longer retain the roles and privileges that were assigned to them through that AD group. In this scenario, each member's effective role and privileges will be either their individual user role or other AD groups the user belongs to.
- If an AD group with case-level reviewer privileges is removed, the expiry date for its members is set to the group removal date. The members still remain listed as case reviewers. However, when such members log in to Insight eDiscovery with an expired reviewer role, the associated cases are not displayed to them.

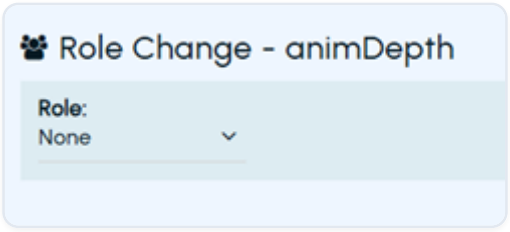
To assign roles to Azure AD groups

1. In the left navigation pane, select **Role Management**>**Assign Active Directory Groups**.

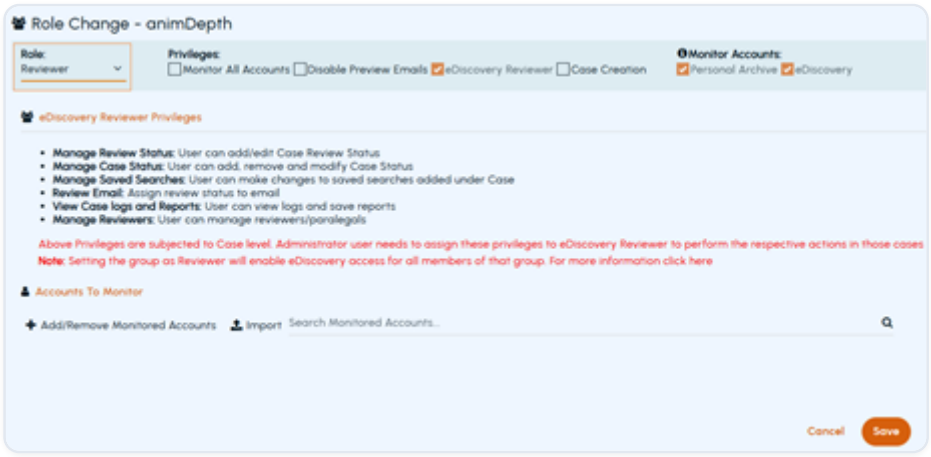
The list of available AD groups is displayed.

1. Search for and select the AD group. You can use *Advanced Search* to filter the list of AD groups or enter the keywords of AD group name. Perform the following as needed:

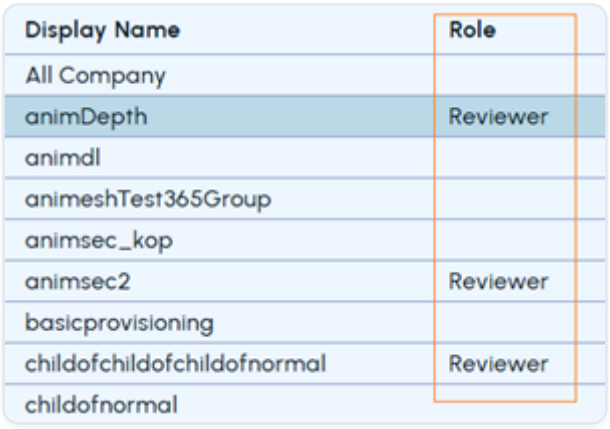
If the selected AD group has no assigned roles, the **Role**drop-down on the**Role Change**page displays**None** by default.



1. From the **Role**drop-down menu, select**Reviewer**, and then click**Save**.



When you view the list, AD groups are displayed with their assigned roles. The **Role** column displays *Reviewer* when the reviewer role is assigned; otherwise, it is blank. Refer to the sample image below.



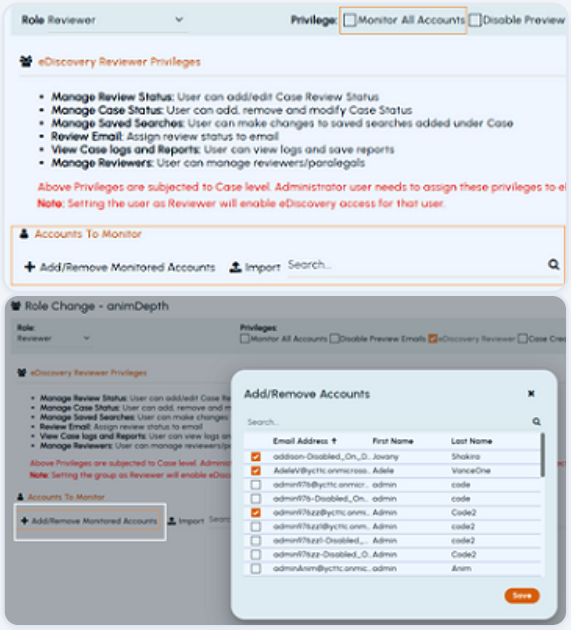
Display Name	Role
All Company	
animDepth	Reviewer
animdl	
animeshTest365Group	
animsec_kop	
animsec2	Reviewer
basicprovisioning	
childofchildofchildofnormal	Reviewer
childofnormal	

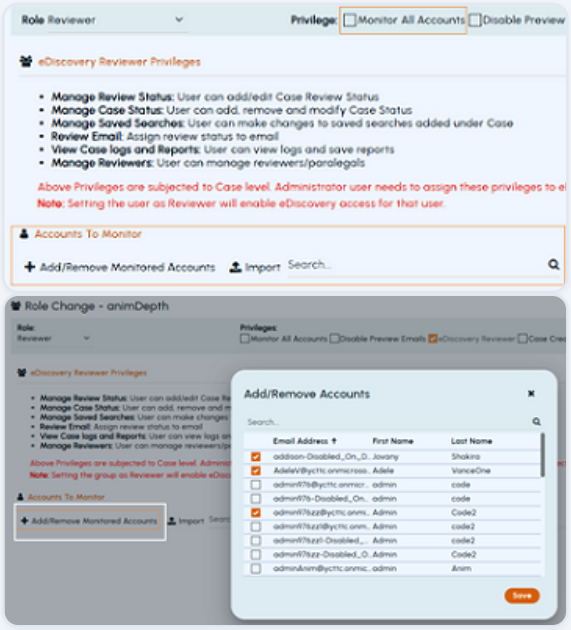
To assign privileges to Azure AD groups

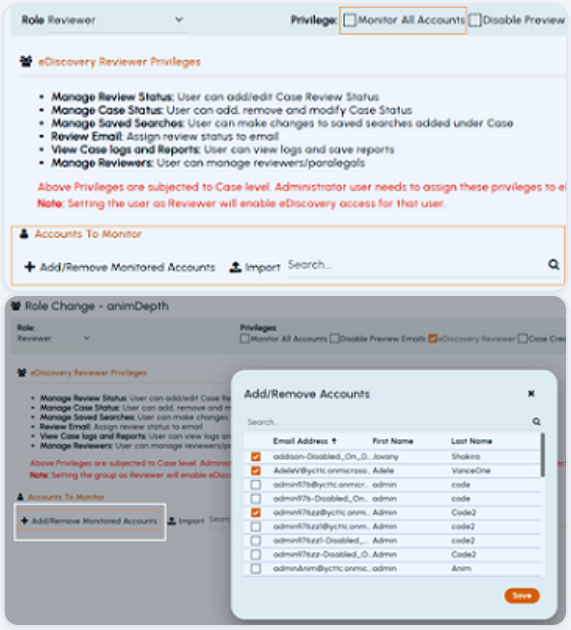
1. In the left navigation pane, select **Role Management**>**Assign Active Directory Groups**.

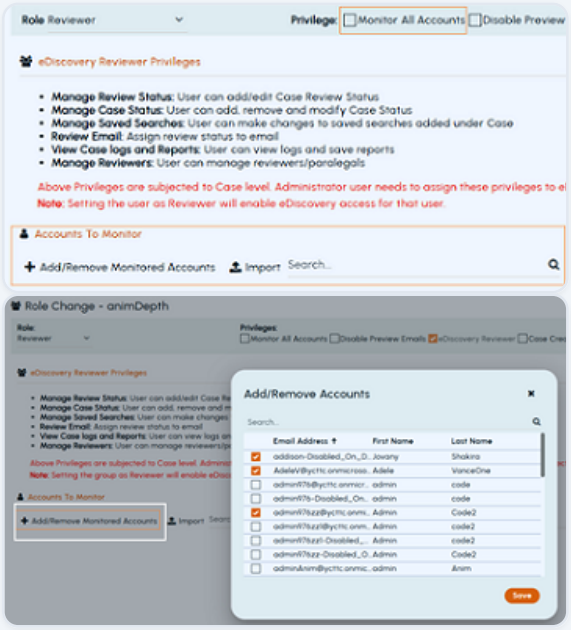
The list of available AD groups is displayed.

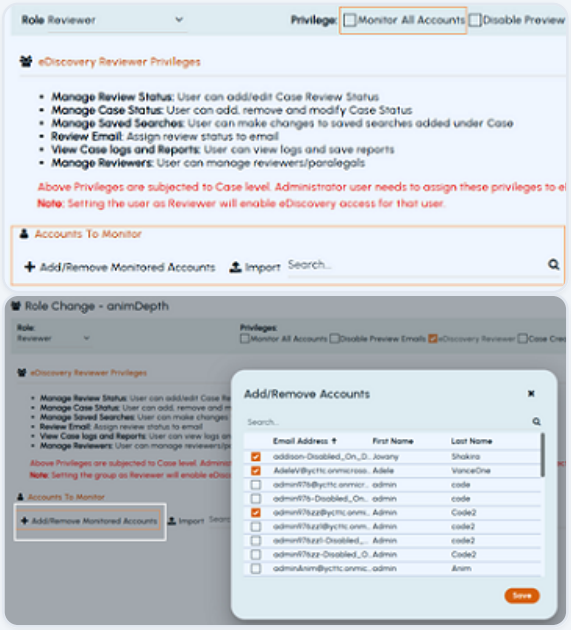
1. Search for and select the AD group. You can use *Advanced Search* to filter the list of AD groups or enter the keywords of AD group name.
2. Under **Privileges** , select one or more of the following options:

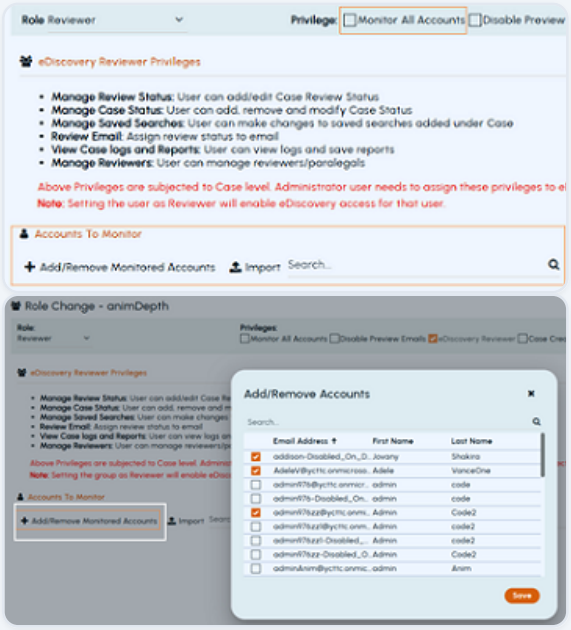
MONITOR ALL ACCOUNTS	 - SELECT THIS OPTION TO ALLOW THE AD GROUP TO VIEW ARCHIVED MESSAGES FOR ALL ARCHIVE ACCOUNTS. WHEN THIS OPTION IS SELECTED, THERE IS NO NEED TO COMPLETE THE STEPS IN THE ACCOUNTS TO MONITOR SECTION.
	- CLEAR THIS OPTION TO ALLOW THE SELECTED AD GROUP TO VIEW ARCHIVED MESSAGES FOR SPECIFIC ARCHIVE ACCOUNTS. WHEN THIS OPTION IS NOT SELECTED, THE ACCOUNTS TO MONITOR SECTION IS DISPLAYED, ALLOWING ARCHIVE ACCOUNTS AND AD GROUPS TO BE ADDED, REMOVED, AND IMPORTED.
	- TO ADD MONITORED ACCOUNTS, CLICK ADD/REMOVE MONITORED ACCOUNTS . SELECT THE ARCHIVE ACCOUNTS THAT YOU WANT THE REVIEWER TO MONITOR, AND CLICK SAVE .
	- TO IMPORT MONITORED ACCOUNT, CLICK IMPORT , AND DO THE FOLLOWING: A. IN THE IMPORT MONITOR ACCOUNTS WINDOW, DOWNLOAD THE SAMPLE .XLS FILE, SAVE IT AS A .CSV FILE. B. RETAIN THE PRIMARYEMAILADDRESS COLUMN HEADING, AND ENTER ONLY THE PRIMARY EMAIL ADDRESSES OF THE ARCHIVE ACCOUNTS. DELETE ALL CONTENT BELOW THE PRIMARYEMAILADDRESS COLUMN

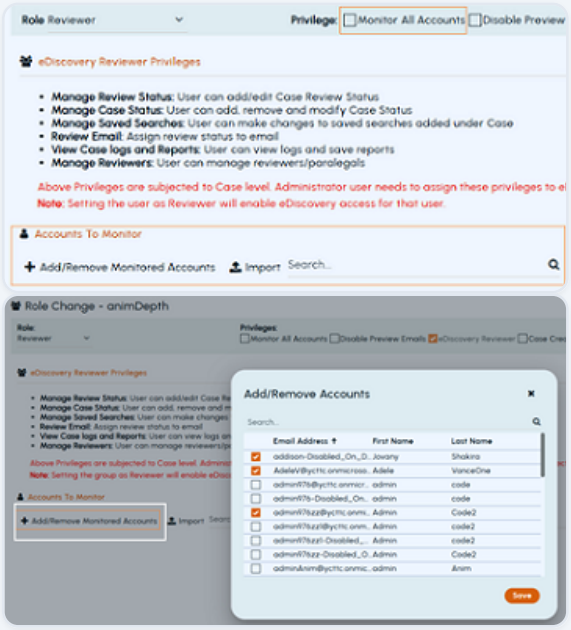
MONITOR ALL ACCOUNTS	 - SELECT THIS OPTION TO ALLOW THE AD GROUP TO VIEW ARCHIVED MESSAGES FOR ALL ARCHIVE ACCOUNTS. WHEN THIS OPTION IS SELECTED, THERE IS NO NEED TO COMPLETE THE STEPS IN THE ACCOUNTS TO MONITOR SECTION.
	- CLEAR THIS OPTION TO ALLOW THE SELECTED AD GROUP TO VIEW ARCHIVED MESSAGES FOR SPECIFIC ARCHIVE ACCOUNTS. WHEN THIS OPTION IS NOT SELECTED, THE ACCOUNTS TO MONITOR SECTION IS DISPLAYED, ALLOWING ARCHIVE ACCOUNTS AND AD GROUPS TO BE ADDED, REMOVED, AND IMPORTED.
	- TO ADD MONITORED ACCOUNTS, CLICK ADD/REMOVE MONITORED ACCOUNTS . SELECT THE ARCHIVE ACCOUNTS THAT YOU WANT THE REVIEWER TO MONITOR, AND CLICK SAVE .
	- TO IMPORT MONITORED ACCOUNT, CLICK IMPORT , AND DO THE FOLLOWING: A. IN THE IMPORT MONITOR ACCOUNTS WINDOW, DOWNLOAD THE SAMPLE .XLS FILE, SAVE IT AS A .CSV FILE. B. RETAIN THE PRIMARYEMAILADDRESS COLUMN HEADING, AND ENTER ONLY THE PRIMARY EMAIL ADDRESSES OF THE ARCHIVE ACCOUNTS. DELETE ALL CONTENT BELOW THE PRIMARYEMAILADDRESS COLUMN

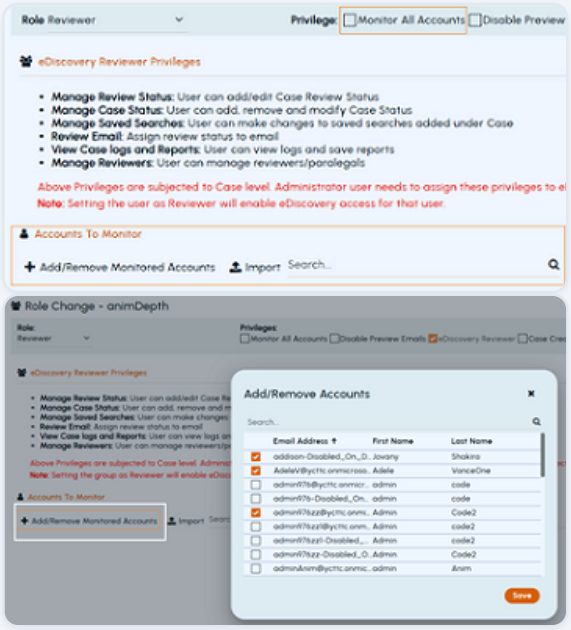
MONITOR ALL ACCOUNTS	 - SELECT THIS OPTION TO ALLOW THE AD GROUP TO VIEW ARCHIVED MESSAGES FOR ALL ARCHIVE ACCOUNTS. WHEN THIS OPTION IS SELECTED, THERE IS NO NEED TO COMPLETE THE STEPS IN THE ACCOUNTS TO MONITOR SECTION.
	- CLEAR THIS OPTION TO ALLOW THE SELECTED AD GROUP TO VIEW ARCHIVED MESSAGES FOR SPECIFIC ARCHIVE ACCOUNTS. WHEN THIS OPTION IS NOT SELECTED, THE ACCOUNTS TO MONITOR SECTION IS DISPLAYED, ALLOWING ARCHIVE ACCOUNTS AND AD GROUPS TO BE ADDED, REMOVED, AND IMPORTED.
	- TO ADD MONITORED ACCOUNTS, CLICK ADD/REMOVE MONITORED ACCOUNTS . SELECT THE ARCHIVE ACCOUNTS THAT YOU WANT THE REVIEWER TO MONITOR, AND CLICK SAVE .
	- TO IMPORT MONITORED ACCOUNT, CLICK IMPORT , AND DO THE FOLLOWING: A. IN THE IMPORT MONITOR ACCOUNTS WINDOW, DOWNLOAD THE SAMPLE .XLS FILE, SAVE IT AS A .CSV FILE. B. RETAIN THE PRIMARYEMAILADDRESS COLUMN HEADING, AND ENTER ONLY THE PRIMARY EMAIL ADDRESSES OF THE ARCHIVE ACCOUNTS. DELETE ALL CONTENT BELOW THE PRIMARYEMAILADDRESS COLUMN

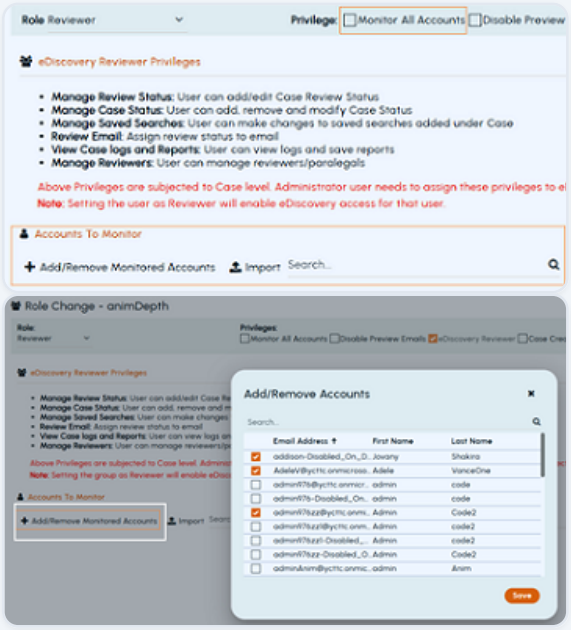
MONITOR ALL ACCOUNTS	 - SELECT THIS OPTION TO ALLOW THE AD GROUP TO VIEW ARCHIVED MESSAGES FOR ALL ARCHIVE ACCOUNTS. WHEN THIS OPTION IS SELECTED, THERE IS NO NEED TO COMPLETE THE STEPS IN THE ACCOUNTS TO MONITOR SECTION.
	- CLEAR THIS OPTION TO ALLOW THE SELECTED AD GROUP TO VIEW ARCHIVED MESSAGES FOR SPECIFIC ARCHIVE ACCOUNTS. WHEN THIS OPTION IS NOT SELECTED, THE ACCOUNTS TO MONITOR SECTION IS DISPLAYED, ALLOWING ARCHIVE ACCOUNTS AND AD GROUPS TO BE ADDED, REMOVED, AND IMPORTED.
	- TO ADD MONITORED ACCOUNTS, CLICK ADD/REMOVE MONITORED ACCOUNTS . SELECT THE ARCHIVE ACCOUNTS THAT YOU WANT THE REVIEWER TO MONITOR, AND CLICK SAVE .
	- TO IMPORT MONITORED ACCOUNT, CLICK IMPORT , AND DO THE FOLLOWING: A. IN THE IMPORT MONITOR ACCOUNTS WINDOW, DOWNLOAD THE SAMPLE .XLS FILE, SAVE IT AS A .CSV FILE. B. RETAIN THE PRIMARYEMAILADDRESS COLUMN HEADING, AND ENTER ONLY THE PRIMARY EMAIL ADDRESSES OF THE ARCHIVE ACCOUNTS. DELETE ALL CONTENT BELOW THE PRIMARYEMAILADDRESS COLUMN

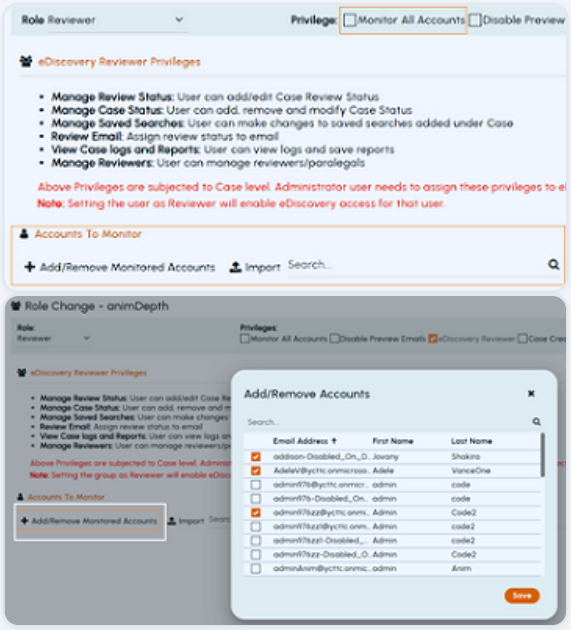
MONITOR ALL ACCOUNTS	 - SELECT THIS OPTION TO ALLOW THE AD GROUP TO VIEW ARCHIVED MESSAGES FOR ALL ARCHIVE ACCOUNTS. WHEN THIS OPTION IS SELECTED, THERE IS NO NEED TO COMPLETE THE STEPS IN THE ACCOUNTS TO MONITOR SECTION.
	- CLEAR THIS OPTION TO ALLOW THE SELECTED AD GROUP TO VIEW ARCHIVED MESSAGES FOR SPECIFIC ARCHIVE ACCOUNTS. WHEN THIS OPTION IS NOT SELECTED, THE ACCOUNTS TO MONITOR SECTION IS DISPLAYED, ALLOWING ARCHIVE ACCOUNTS AND AD GROUPS TO BE ADDED, REMOVED, AND IMPORTED.
	- TO ADD MONITORED ACCOUNTS, CLICK ADD/REMOVE MONITORED ACCOUNTS . SELECT THE ARCHIVE ACCOUNTS THAT YOU WANT THE REVIEWER TO MONITOR, AND CLICK SAVE .
	- TO IMPORT MONITORED ACCOUNT, CLICK IMPORT , AND DO THE FOLLOWING: A. IN THE IMPORT MONITOR ACCOUNTS WINDOW, DOWNLOAD THE SAMPLE .XLS FILE, SAVE IT AS A .CSV FILE. B. RETAIN THE PRIMARYEMAILADDRESS COLUMN HEADING, AND ENTER ONLY THE PRIMARY EMAIL ADDRESSES OF THE ARCHIVE ACCOUNTS. DELETE ALL CONTENT BELOW THE PRIMARYEMAILADDRESS COLUMN

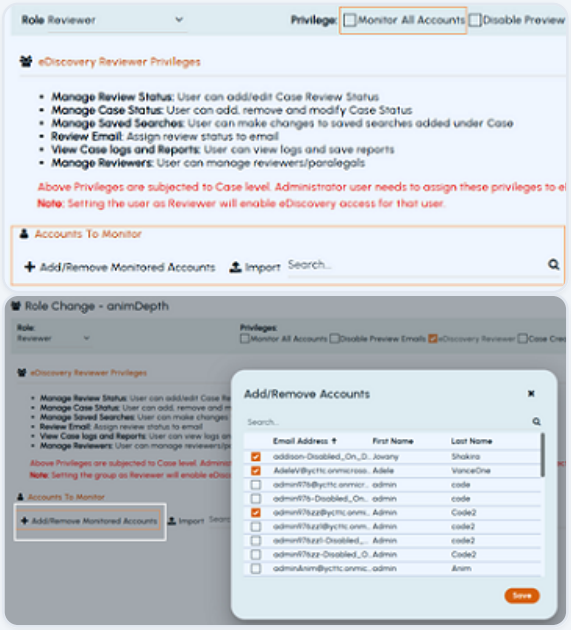
MONITOR ALL ACCOUNTS	 - SELECT THIS OPTION TO ALLOW THE AD GROUP TO VIEW ARCHIVED MESSAGES FOR ALL ARCHIVE ACCOUNTS. WHEN THIS OPTION IS SELECTED, THERE IS NO NEED TO COMPLETE THE STEPS IN THE ACCOUNTS TO MONITOR SECTION.
	- CLEAR THIS OPTION TO ALLOW THE SELECTED AD GROUP TO VIEW ARCHIVED MESSAGES FOR SPECIFIC ARCHIVE ACCOUNTS. WHEN THIS OPTION IS NOT SELECTED, THE ACCOUNTS TO MONITOR SECTION IS DISPLAYED, ALLOWING ARCHIVE ACCOUNTS AND AD GROUPS TO BE ADDED, REMOVED, AND IMPORTED.
	- TO ADD MONITORED ACCOUNTS, CLICK ADD/REMOVE MONITORED ACCOUNTS . SELECT THE ARCHIVE ACCOUNTS THAT YOU WANT THE REVIEWER TO MONITOR, AND CLICK SAVE .
	- TO IMPORT MONITORED ACCOUNT, CLICK IMPORT , AND DO THE FOLLOWING: A. IN THE IMPORT MONITOR ACCOUNTS WINDOW, DOWNLOAD THE SAMPLE .XLS FILE, SAVE IT AS A .CSV FILE. B. RETAIN THE PRIMARYEMAILADDRESS COLUMN HEADING, AND ENTER ONLY THE PRIMARY EMAIL ADDRESSES OF THE ARCHIVE ACCOUNTS. DELETE ALL CONTENT BELOW THE PRIMARYEMAILADDRESS COLUMN

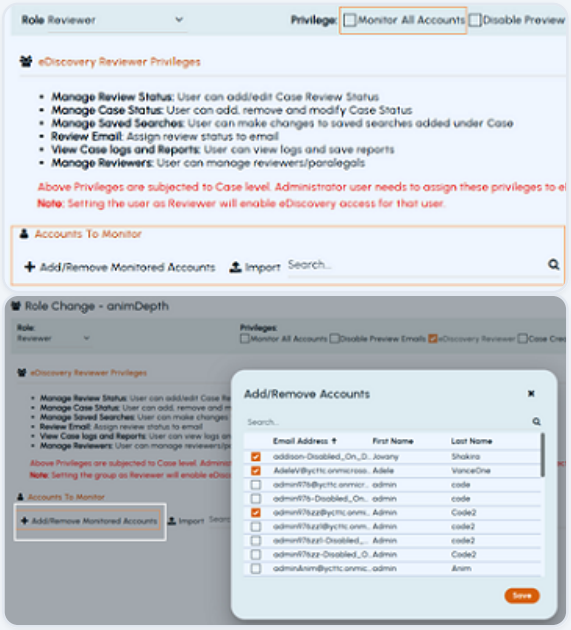
MONITOR ALL ACCOUNTS	 - SELECT THIS OPTION TO ALLOW THE AD GROUP TO VIEW ARCHIVED MESSAGES FOR ALL ARCHIVE ACCOUNTS. WHEN THIS OPTION IS SELECTED, THERE IS NO NEED TO COMPLETE THE STEPS IN THE ACCOUNTS TO MONITOR SECTION.
	- CLEAR THIS OPTION TO ALLOW THE SELECTED AD GROUP TO VIEW ARCHIVED MESSAGES FOR SPECIFIC ARCHIVE ACCOUNTS. WHEN THIS OPTION IS NOT SELECTED, THE ACCOUNTS TO MONITOR SECTION IS DISPLAYED, ALLOWING ARCHIVE ACCOUNTS AND AD GROUPS TO BE ADDED, REMOVED, AND IMPORTED.
	- TO ADD MONITORED ACCOUNTS, CLICK ADD/REMOVE MONITORED ACCOUNTS . SELECT THE ARCHIVE ACCOUNTS THAT YOU WANT THE REVIEWER TO MONITOR, AND CLICK SAVE .
	- TO IMPORT MONITORED ACCOUNT, CLICK IMPORT , AND DO THE FOLLOWING: A. IN THE IMPORT MONITOR ACCOUNTS WINDOW, DOWNLOAD THE SAMPLE .XLS FILE, SAVE IT AS A .CSV FILE. B. RETAIN THE PRIMARYEMAILADDRESS COLUMN HEADING, AND ENTER ONLY THE PRIMARY EMAIL ADDRESSES OF THE ARCHIVE ACCOUNTS. DELETE ALL CONTENT BELOW THE PRIMARYEMAILADDRESS COLUMN

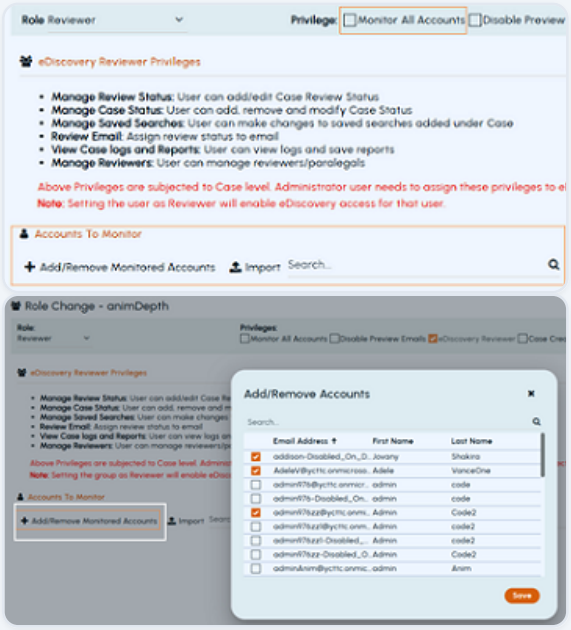
MONITOR ALL ACCOUNTS	 - SELECT THIS OPTION TO ALLOW THE AD GROUP TO VIEW ARCHIVED MESSAGES FOR ALL ARCHIVE ACCOUNTS. WHEN THIS OPTION IS SELECTED, THERE IS NO NEED TO COMPLETE THE STEPS IN THE ACCOUNTS TO MONITOR SECTION.
	- CLEAR THIS OPTION TO ALLOW THE SELECTED AD GROUP TO VIEW ARCHIVED MESSAGES FOR SPECIFIC ARCHIVE ACCOUNTS. WHEN THIS OPTION IS NOT SELECTED, THE ACCOUNTS TO MONITOR SECTION IS DISPLAYED, ALLOWING ARCHIVE ACCOUNTS AND AD GROUPS TO BE ADDED, REMOVED, AND IMPORTED.
	- TO ADD MONITORED ACCOUNTS, CLICK ADD/REMOVE MONITORED ACCOUNTS . SELECT THE ARCHIVE ACCOUNTS THAT YOU WANT THE REVIEWER TO MONITOR, AND CLICK SAVE .
	- TO IMPORT MONITORED ACCOUNT, CLICK IMPORT , AND DO THE FOLLOWING: A. IN THE IMPORT MONITOR ACCOUNTS WINDOW, DOWNLOAD THE SAMPLE .XLS FILE, SAVE IT AS A .CSV FILE. B. RETAIN THE PRIMARYEMAILADDRESS COLUMN HEADING, AND ENTER ONLY THE PRIMARY EMAIL ADDRESSES OF THE ARCHIVE ACCOUNTS. DELETE ALL CONTENT BELOW THE PRIMARYEMAILADDRESS COLUMN

MONITOR ALL ACCOUNTS	 - SELECT THIS OPTION TO ALLOW THE AD GROUP TO VIEW ARCHIVED MESSAGES FOR ALL ARCHIVE ACCOUNTS. WHEN THIS OPTION IS SELECTED, THERE IS NO NEED TO COMPLETE THE STEPS IN THE ACCOUNTS TO MONITOR SECTION.
	- CLEAR THIS OPTION TO ALLOW THE SELECTED AD GROUP TO VIEW ARCHIVED MESSAGES FOR SPECIFIC ARCHIVE ACCOUNTS. WHEN THIS OPTION IS NOT SELECTED, THE ACCOUNTS TO MONITOR SECTION IS DISPLAYED, ALLOWING ARCHIVE ACCOUNTS AND AD GROUPS TO BE ADDED, REMOVED, AND IMPORTED.
	- TO ADD MONITORED ACCOUNTS, CLICK ADD/REMOVE MONITORED ACCOUNTS . SELECT THE ARCHIVE ACCOUNTS THAT YOU WANT THE REVIEWER TO MONITOR, AND CLICK SAVE .
	- TO IMPORT MONITORED ACCOUNT, CLICK IMPORT , AND DO THE FOLLOWING: A. IN THE IMPORT MONITOR ACCOUNTS WINDOW, DOWNLOAD THE SAMPLE .XLS FILE, SAVE IT AS A .CSV FILE. B. RETAIN THE PRIMARYEMAILADDRESS COLUMN HEADING, AND ENTER ONLY THE PRIMARY EMAIL ADDRESSES OF THE ARCHIVE ACCOUNTS. DELETE ALL CONTENT BELOW THE PRIMARYEMAILADDRESS COLUMN

MONITOR ALL ACCOUNTS	 - SELECT THIS OPTION TO ALLOW THE AD GROUP TO VIEW ARCHIVED MESSAGES FOR ALL ARCHIVE ACCOUNTS. WHEN THIS OPTION IS SELECTED, THERE IS NO NEED TO COMPLETE THE STEPS IN THE ACCOUNTS TO MONITOR SECTION.
	- CLEAR THIS OPTION TO ALLOW THE SELECTED AD GROUP TO VIEW ARCHIVED MESSAGES FOR SPECIFIC ARCHIVE ACCOUNTS. WHEN THIS OPTION IS NOT SELECTED, THE ACCOUNTS TO MONITOR SECTION IS DISPLAYED, ALLOWING ARCHIVE ACCOUNTS AND AD GROUPS TO BE ADDED, REMOVED, AND IMPORTED.
	- TO ADD MONITORED ACCOUNTS, CLICK ADD/REMOVE MONITORED ACCOUNTS . SELECT THE ARCHIVE ACCOUNTS THAT YOU WANT THE REVIEWER TO MONITOR, AND CLICK SAVE .
	- TO IMPORT MONITORED ACCOUNT, CLICK IMPORT , AND DO THE FOLLOWING: A. IN THE IMPORT MONITOR ACCOUNTS WINDOW, DOWNLOAD THE SAMPLE .XLS FILE, SAVE IT AS A .CSV FILE. B. RETAIN THE PRIMARYEMAILADDRESS COLUMN HEADING, AND ENTER ONLY THE PRIMARY EMAIL ADDRESSES OF THE ARCHIVE ACCOUNTS. DELETE ALL CONTENT BELOW THE PRIMARYEMAILADDRESS COLUMN

MONITOR ALL ACCOUNTS	 - SELECT THIS OPTION TO ALLOW THE AD GROUP TO VIEW ARCHIVED MESSAGES FOR ALL ARCHIVE ACCOUNTS. WHEN THIS OPTION IS SELECTED, THERE IS NO NEED TO COMPLETE THE STEPS IN THE ACCOUNTS TO MONITOR SECTION.
	- CLEAR THIS OPTION TO ALLOW THE SELECTED AD GROUP TO VIEW ARCHIVED MESSAGES FOR SPECIFIC ARCHIVE ACCOUNTS. WHEN THIS OPTION IS NOT SELECTED, THE ACCOUNTS TO MONITOR SECTION IS DISPLAYED, ALLOWING ARCHIVE ACCOUNTS AND AD GROUPS TO BE ADDED, REMOVED, AND IMPORTED.
	- TO ADD MONITORED ACCOUNTS, CLICK ADD/REMOVE MONITORED ACCOUNTS . SELECT THE ARCHIVE ACCOUNTS THAT YOU WANT THE REVIEWER TO MONITOR, AND CLICK SAVE .
	- TO IMPORT MONITORED ACCOUNT, CLICK IMPORT , AND DO THE FOLLOWING: A. IN THE IMPORT MONITOR ACCOUNTS WINDOW, DOWNLOAD THE SAMPLE .XLS FILE, SAVE IT AS A .CSV FILE. B. RETAIN THE PRIMARYEMAILADDRESS COLUMN HEADING, AND ENTER ONLY THE PRIMARY EMAIL ADDRESSES OF THE ARCHIVE ACCOUNTS. DELETE ALL CONTENT BELOW THE PRIMARYEMAILADDRESS COLUMN

MONITOR ALL ACCOUNTS	 - SELECT THIS OPTION TO ALLOW THE AD GROUP TO VIEW ARCHIVED MESSAGES FOR ALL ARCHIVE ACCOUNTS. WHEN THIS OPTION IS SELECTED, THERE IS NO NEED TO COMPLETE THE STEPS IN THE ACCOUNTS TO MONITOR SECTION.
	- CLEAR THIS OPTION TO ALLOW THE SELECTED AD GROUP TO VIEW ARCHIVED MESSAGES FOR SPECIFIC ARCHIVE ACCOUNTS. WHEN THIS OPTION IS NOT SELECTED, THE ACCOUNTS TO MONITOR SECTION IS DISPLAYED, ALLOWING ARCHIVE ACCOUNTS AND AD GROUPS TO BE ADDED, REMOVED, AND IMPORTED.
	- TO ADD MONITORED ACCOUNTS, CLICK ADD/REMOVE MONITORED ACCOUNTS . SELECT THE ARCHIVE ACCOUNTS THAT YOU WANT THE REVIEWER TO MONITOR, AND CLICK SAVE .
	- TO IMPORT MONITORED ACCOUNT, CLICK IMPORT , AND DO THE FOLLOWING: A. IN THE IMPORT MONITOR ACCOUNTS WINDOW, DOWNLOAD THE SAMPLE .XLS FILE, SAVE IT AS A .CSV FILE. B. RETAIN THE PRIMARYEMAILADDRESS COLUMN HEADING, AND ENTER ONLY THE PRIMARY EMAIL ADDRESSES OF THE ARCHIVE ACCOUNTS. DELETE ALL CONTENT BELOW THE PRIMARYEMAILADDRESS COLUMN

MONITOR ALL ACCOUNTS	 - SELECT THIS OPTION TO ALLOW THE AD GROUP TO VIEW ARCHIVED MESSAGES FOR ALL ARCHIVE ACCOUNTS. WHEN THIS OPTION IS SELECTED, THERE IS NO NEED TO COMPLETE THE STEPS IN THE ACCOUNTS TO MONITOR SECTION.
	- CLEAR THIS OPTION TO ALLOW THE SELECTED AD GROUP TO VIEW ARCHIVED MESSAGES FOR SPECIFIC ARCHIVE ACCOUNTS. WHEN THIS OPTION IS NOT SELECTED, THE ACCOUNTS TO MONITOR SECTION IS DISPLAYED, ALLOWING ARCHIVE ACCOUNTS AND AD GROUPS TO BE ADDED, REMOVED, AND IMPORTED.
	- TO ADD MONITORED ACCOUNTS, CLICK ADD/REMOVE MONITORED ACCOUNTS . SELECT THE ARCHIVE ACCOUNTS THAT YOU WANT THE REVIEWER TO MONITOR, AND CLICK SAVE .
	- TO IMPORT MONITORED ACCOUNT, CLICK IMPORT , AND DO THE FOLLOWING: A. IN THE IMPORT MONITOR ACCOUNTS WINDOW, DOWNLOAD THE SAMPLE .XLS FILE, SAVE IT AS A .CSV FILE. B. RETAIN THE PRIMARYEMAILADDRESS COLUMN HEADING, AND ENTER ONLY THE PRIMARY EMAIL ADDRESSES OF THE ARCHIVE ACCOUNTS. DELETE ALL CONTENT BELOW THE PRIMARYEMAILADDRESS COLUMN

	create cases in Insight eDiscovery.

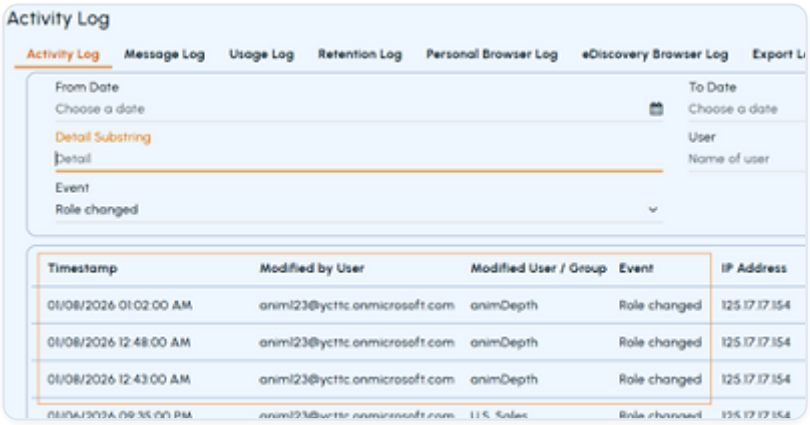
3. On the **Role Change**page, click**Save**.

After you save the changes made to the selected AD group, they are updated in the application and can be verified as follows.

- **Application-level changes**a. In the left navigation pane, select**Reports and Notifications**>**Logs**.

b. On the **Activity Log** page, specify the time period, Detail Substring, or a user name as available.

c. From the **Event**drop-down list, select *Role changed* option. Click**Search** to view the log as shown in the sample image below.

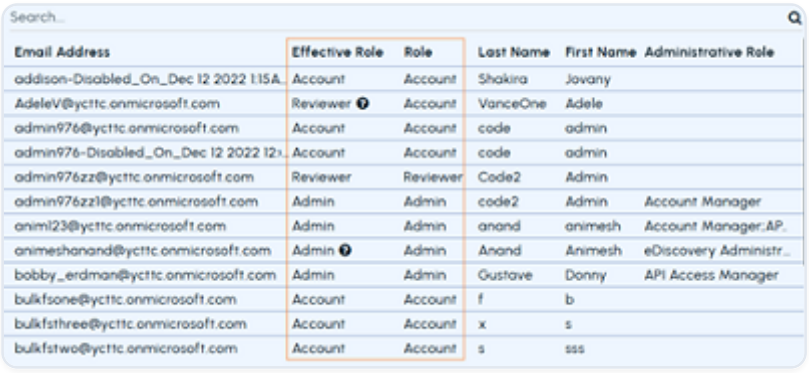


d. (Optional) Click the **Download** icon to save the report locally.

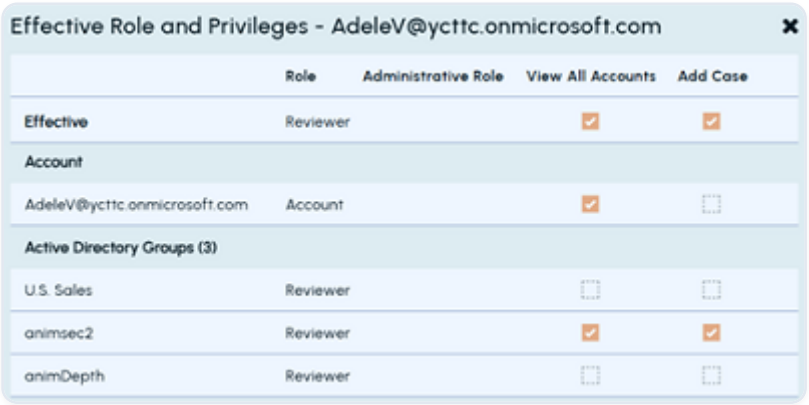
- **Account-level changes**a. In the left navigation pane, select**Role Management**>**Assign Accounts**. A list of archive accounts appears.

b. Search for the required archive account. Use any of the following methods.

- Expand the **Advanced Search**section, specify the input, and click**Apply**.
- Expand the **Roles** section, click on the required role.
- In the **Search**field, enter the username or email of the archive account and click the**Search** icon.
- Refer to the *Effective Role*and*Role* column values for the required archive account to verify the role changes.



- Click the **question mark** (?) icon (if appears) in the *Effective Role* column to view how the effective role is determined based on AD group membership. The details appear as shown in the sample image below.



Managing Policies

This section includes the following topics:

About Policy Management

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

- Configure various archiving options.
- Enabling or disabling archiving for selected archive accounts.
- Configuring the InsightAI feature
- Configure an advanced policy for passwords.
- Configure trusted networks for Arctera Insight Archiving access.

See Configuring the InsightAI feature.

> “ ”

Note: From thePolicy Managementsection the administrators with the required privileges can also configure authentication management for Arctera Insight Archiving. SeeConfiguring the Arctera Insight Archiving authentication service.

> “ ”

Configuring archive options

Administrator can enable or disable the archive options to configure archiving policies and AI-driven capabilities for the Arctera Insight applications subscribed by a customer.

To configure archive options

1. In the left navigation pane, select **Policy Management**>**Archive Options**.
2. Click **Edit** to configure the required features.

Refer to the details in the table below.

ARCHIVE OPTION	DESCRIPTION
Manage Your Own Encryption Keys (MYOK)	This option is informational only and cannot be configured through this interface. This configuration is available only during initial provisioning, before any data is stored.
	See Configuring the Manage Your Own Keys (MYOK) Feature . or contact Arctera support .
Email Direction	Specifies which types of emails are archived. By default, all message types are selected. Select the email direction, as needed.
	- Inbound Emails - Select this option to enable archiving email messages sent to addresses within your domain from external domains.
	- Outbound Emails - Select this option to enable archiving email messages sent from addresses within your domain to external domains.
	- Internal Emails - Select this option to enable archiving email messages exchanged between addresses within your domain.
Archiving Actions	Determines whether the Insight Personal Archive users can
	send, reply, forward, print, or save messages.

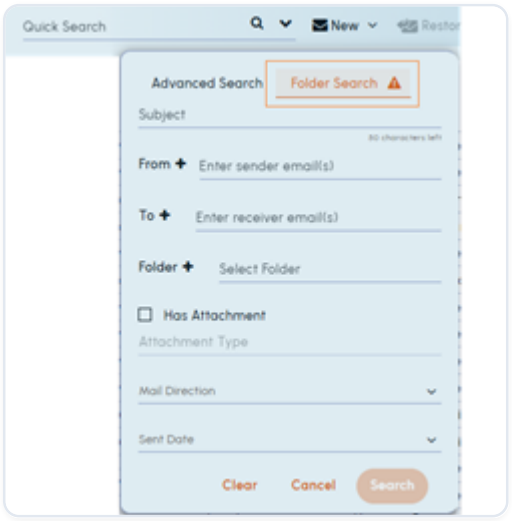
ARCHIVE OPTION	DESCRIPTION
	- Send, Reply, and Forward - Select this option to allow users to send, reply to, and forward messages in Insight Personal Archive.
	- Save - Select this option to allow users to save archived messages to your computer from Insight Personal Archive.
	- Print - Select this option to allow users to print archived messages from Insight Personal Archive.
Time Zone and Date Format	Specifies the time zone and date format.
	- Personal Time Zone - Select the appropriate archiving time zone.
	- Default Company Time Zone - Select the default time zone for your company.
	- Date Format - Select the default date format for your company.
Mobile Web Access	Determines which permissions to be enabled for Mobile Web Access users.
	- Status - Select this option to enable or disable Mobile Web Access permission.
	- Automatically grant Mobile Web Access permission for new accounts - Select this option to grant Mobile Web Access permission for new archive accounts when you create them manually in Arctera Insight Management Console. **Note:** This option does not apply to archive accounts that are created through CloudLink or Exchange Online Sync.
	- Send, Reply and Forward from Mobile Web Access - Select this option to enable the

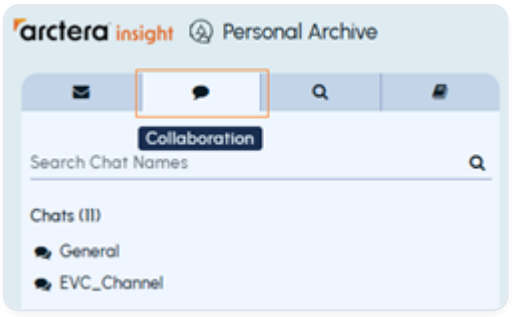
ARCHIVE OPTION	DESCRIPTION
	Send , Reply , and Forward options in Mobile Web Access.
	To use this feature, Insight Personal Archive administrator requires the Mobile Web Access permission. You can set it for the Insight Personal Archive administrator role.
	See Editing Mobile Web Access permission for existing archive accounts .
Privileged Delete	Determines if the permanent delete access to be enabled in Insight eDiscovery or Insight Personal Archive.
	- eDiscovery - Toggle the switch to enable or disable the delete emails permission for Insight eDiscovery users.
	- Personal Archive - Toggle the switch adjacent to Insight Personal Archive to choose whether to enable or disable the delete emails permission for Insight Personal Archive users.
	To use this feature, the Insight eDiscovery and Insight Personal Archive administrator requires the Privilege Delete permission. You can set it for the administrator role. See Editing the built-in administrator roles .
View Delegate Archives Folder Structure	Determines if the ability to view
	delegate archive folders in Insight Personal Archive to be 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 Insight Personal Archive. If you have over 4,000 synchronized monitored and delegate archive folders, the

ARCHIVE OPTION	DESCRIPTION
	loading time in theActive Folderstab might take up to five minutes. The delegate archive folder structure keeps synchronizing even though theView Delegate Archive Folder Structureoption in Management Console is enabled or disabled. When the delegate account users logs in to Insight Personal Archive, they can view their folder structure.
Export to Azure private storage location	Determines if the Insight eDiscovery data can be exported to the Azure location. Toggle the switch to enable or disable this feature.
	If the status is set to Enabled , the Create new Storage Account button is displayed in Insight eDiscovery. Click Create new Storage Account to allow a customer to create an Azure storage account during exporting items from Insight 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 (EnabledorDisabled) and the retention period of this feature from the database only. If the status is set toDisabled, you cannot see theCreate new Storage Accountbutton. You can generate only one Azure storage account per customer. After creating a storage account, theCreate new Storage Accountbutton gets disabled. If you hover over the disabled button, theStorage account is already createdtooltip is displayed. Contact Arctera Customer Service representative to enable it.
OCR Status	Determines whether the Optical Character Recognition (OCR) service is enabled or disabled for customers and displays all the

ARCHIVE OPTION	DESCRIPTION
	supported file types like `.pdf` , `.jpeg` , `.png` , and more.
	Toggle to enable or disable this feature in Management Console, Insight eDiscovery, and Insight Personal Archive.
	If the status is set to Enabled , customers can extract text from scanned documents, images, or non-editable files, converting them into searchable and editable formats archived in Management Console, Insight eDiscovery, and Insight Personal Archive.
	Note: This feature is now visible as a read-only section, allowing customers to verify the service activation status. Customers must contact Arctera Support to activate or deactivate the service.
Show Display Name	Determines whether the Show Display Name service configured for users.
	Toggle to enable or disable viewing the display names of the sender and recipient instead of only email addresses in Insight eDiscovery, Insight Personal Archive, and Insight Personal Archive Mobile Web Applications.
AI Features > eDiscovery InsightAI	This feature is available to customers only if the Insight eDiscovery primary service is subscribed by them.
	Toggle to enable or disable this option to view the InsightAI feature in Insight eDiscovery.
	If the status is set to Enabled , users can efficiently analyze and manage documents by receiving instant summaries, extracting key topics, and performing sentiment analysis across various content types like emails, collaboration messages, and files. users can

ARCHIVE OPTION	DESCRIPTION
	also query specific documents or search results, customize analysis preferences, and monitor resource usage with AI Wallet.
	If the status is set to Disabled , users cannot access InsightAI services.
AI Features > Personal Archive InsightBooks	This feature is available to customers only if the Insight eDiscovery primary service is subscribed by them.
	Toggle to enable or disable this option to view the InsightBooks feature in Insight Personal Archive.
	If the status is set to Enabled , users can create, view, and manage InsightBooks, and use GenAI to analyze emails and collaboration content. They can also share InsightBooks with other users and monitor resource usage with AI Wallet.
	If the status is set to Disabled , customers cannot access InsightBooks services.
AI Features > Surveillance Translation	This feature is available to customers only if the Insight Surveillance primary service is subscribed by them.
	Toggle to enable or disable this option to view the Translation feature in Insight Surveillance.
	If the status is set to Enabled , users can view the Translate button and manage the translation of email content. All changes to the Surveillance Translation option are audited and can be reviewed on the Logs page.
	If the status is set to Disabled , customers cannot access translation services.

ARCHIVE OPTION	DESCRIPTION
Show Item ID Filter	Determines whether the Show Item ID Filter service is configured for users. It allows users to locate a single email using its unique, encrypted Item ID.
	If the status is set to Enabled , the display name appears alongside the email address, providing clearer identification.
	In the Insight Personal Archive application, the archive list shows the display name for each archive. If the display name is not available, the first name and last name are shown. If neither is present, the email address is displayed instead.
Enable Folder Search For Personal Archive	 Determines whether the Enable Folder Search For Personal Archive service is configured for customer/tenant.
	If the status is set to Enabled , the Folder Search tab appears in Insight Personal Archive as shown in the sample image below.

ARCHIVE OPTION	DESCRIPTION
Enable Collaboration View For Personal Archive	 Determines whether the Enable Collaboration View for Personal Archive service is configured for customer/tenant.
	If the status is set to Enabled , and collaboration tools such as Microsoft Teams, Slack, or other supported platforms are integrated for a user account, then the users can view the Collaboration tab in the left pane of Insight Personal Archive as shown in the sample image below.

1. Click **Save**.

Enabling and disabling account archiving

By default, the messages for all archive accounts are automatically journaled to Arctera Insight 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.
5. Click **Save**to close the**Add/Remove Accounts** window.
6. On the **Enable/Disable Archiving**page, click**Save**.

Configuring the InsightAI feature

Overview

InsightAI, a cutting-edge generative AI assistant, streamlines document review and analysis by delivering rapid summaries, key topic identification, and sentiment evaluations. It supports diverse content types such as emails, files, and chats, enabling users to efficiently manage and understand large volumes of information.

Salient Features

Document Insights: Generates instant summaries, highlights crucial topics, and analyzes sentiment for individual documents.

Search Integration: Consolidates summaries and identifies key topics from multiple search results across diverse content sources.

Query Support: Provides precise answers to queries related to specific documents or search outcomes, improving clarity and decision-making.

Customizable Preferences: Adapts analysis outputs to user-defined preferences for personalized and relevant results.

AI Units transaction Transparency: Ensures visibility of all Azure OpenAI transactions, allowing system administrators to monitor AI Units usage through the Management Console.

Real-Time AI Units Estimation: Displays immediate usage estimates for queries, promoting efficient resource management.

Detailed Breakdown: Offers a granular view of usage for each query, fostering accountability and transparency.

To configure this feature, See Configuring archive options.

For more details about InsightAI, refer to the InsightAI: Frequently Asked Questions article.

Configuring an advanced password policy

The default password policy for Arctera Insight 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: ThePassword Policypage 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.

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.
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	Select this requirement and choose up to three of the following password complexity requirements\:
	- 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.

1. 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.

> “ ”

2. Click **Save**.

Configuring trusted networks for Arctera Insight Archiving access

By default, users can access Arctera Insight 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 Arctera Insight Archiving access

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

The **Add Trusted Network** window appears.

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

1. Click **Save**.

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

1. Click **Yes**.

Managing Discard Rules

A *Discard Rule*was previously referred as a*Bypass Rule*. This rule is an instruction that bypasses specific review items when the rule is active and applied. To manage discard rules, 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.

> “ ”

Adding Discard Rules

To add a new discard rule

1. In the left navigation pane, select **Policy Management**>**Discard Rules**.
2. On the action bar, click **Add Row** , and specify the following details in the newly added row.

SENDERADDRESS	SPECIFY THE VALUE IN THE NAME@EXAMPLE.COM 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.

3. Activate or deactivate the rule.
   - To save this rule in the *Active* state, select the **Active** check box. The activated discard rule remains available for use.
   - To save this rule in the *Inactive* state, do not select the **Active** check box. The deactivated discard rule remains unavailable for use.
4. On the action bar, click **Save**.

Upon saving a rule, you cannot modify the *SenderAddress*,*Subject*, and*Attachment Type* values. You can only activate or deactivate it. Therefore, the application prompts you to confirm that you want to perform the operation.

1. Click **Yes**to save the rule. Else, click**No** to abort the operation.

Searching for discard rules

In the action bar of the Discard Rules page, enter partial or full keywords in the search field. Else, in the item grid, click on the column headings to sort the list. The application displays the relevant rules. You can activate or deactivate the rules, but you cannot edit them.

Importing discard rules in bulk

Before importing discard rules in bulk, it is crucial to understand that the existing discard rules will be completely replaced or overwritten during the import. Make sure to review the procedures carefully.

To import discard rules in bulk

1. Ensure that you have a list of discard rules in the standard *DiscardRule Bulk Import Template*. Refer to Discard Rules Bulk Import Template article if assistance is required.
2. In the left navigation pane, select **Policy Management**>**Discard Rules**.
3. On the action bar, click **Import**.
4. In the **Discard Rules Import** dialog box, do the following as needed:
    - Click the **Sample ".csv" file** to get the sample template.
    - Click **Choose File** to browse and select the CSV file of discard rules.
5. Click **Import**.

The application imports the rules in bulk and replaces/overwrites the currently available rules.

To retain existing discard rules during bulk import

1. Click Export on the action bar to download the current rules as a *DiscardRules.csv* file.
2. Copy or add these rules to the discard rules template.
3. Import the updated template.
4. On the **Discard Rules** page, search any previously available rule to ensure the existing rule is preserved.

Managing Index Exclusion

The *Index Exclusion* feature lets administrators define specific text strings - such as disclaimers, signatures, or repetitive phrases - to be excluded from indexing. This helps improve the accuracy of search before classification of items by ignoring non-essential or irrelevant content.

It is an instruction that excludes specific review items when the index exclusion text is active and applied. To manage Index Exclusion, you must have access to the Policy Management page.

Access to the Index Exclusion feature requires the *Manage Exclusion Texts*privilege. This privilege is enabled by default for users assigned the*System Administrator*or*Policy Manager*roles.*System Administrator*can revoke this privilege from the*Policy Manager* role if needed.

> “ ”

Note: Once you save the index exclusion record, you cannot modify it. However, you can activate or deactivate the index exclusion as needed.

> “ ”

Adding index exclusion text

To add a new index exclusion text

1. In the left navigation pane, select **Policy Management**>**Index Exclusion**.
2. On the action bar, click **Add Row** , and enter the text you want to exclude in the newly added row.
3. Activate or deactivate the index exclusion text.
    - To save this index exclusion text in the *Active* state, select the **Active** check box. The activated index exclusion text remains available for use.
    - To save this index exclusion text in the *Inactive* state, do not select the **Active** check box. The deactivated index exclusion text remains unavailable for use.
4. On the action bar, click **Save**.

Upon saving a text, you can only activate or deactivate it. Therefore, the application prompts you to confirm that you want to perform the operation.

1. Click **Yes**to save the record. Else, click**No** to abort the operation.

A notification appears that the index exclusion text is saved successfully.

Searching for index exclusion text

In the action bar of the Index Exclusion page, enter partial or full keywords in the search field. Else, in the item grid, click on the column headings to sort the list. The application displays the relevant index exclusion records. You can activate or deactivate the records, but you cannot edit them.

Importing index exclusion records in bulk

Before importing index exclusion records in bulk, it is crucial to understand that the existing index exclusion records will be completely replaced or overwritten during the import. Make sure to review the procedures carefully.

To import index exclusion records in bulk

1. Ensure that you have a list of index exclusion records in the standard Index Exclusion Bulk Import Template.
2. In the left navigation pane, select **Policy Management**>**Index Exclusion**.
3. On the action bar, click **Import**.
4. In the **Index Exclusion Import** dialog box, do the following as needed:
    - Click the **Sample ".csv" file** to get the sample template.
    - Click **Choose File** to browse and select the CSV file of index exclusion records.
5. Click **Import**.

The application imports the index exclusion records in bulk and replaces/overwrites the currently available records.

To retain existing index exclusion records during bulk import

1. Click **Export** on the action bar to download the current records as a *IndexExclusions.csv* file.
2. Copy or add these records to this template.
3. Import the updated template.
4. On the **Index Exclusion** page, search any previously available record to ensure the existing record is preserved.

Managing Authentication

This section includes the following topics:

Configuring the Arctera Insight Archiving authentication service

This section describes how to configure the Arctera Insight Archiving authentication service to work with the following environments:

- Cloud Archive Database
- Single Sign-On Authentication (SSO) Active Directory Federation Services (ADFS)
- Single Sign-On Authentication (SSO)

Before using Cloud Archive Database, do the following:

1. See Configuring an advanced password policy. to understand password complexity rules.
2. Provide your username and password when accessing Insight Personal Archive.

Before using SSO and SSO-ADFS environments, do the following:

1. Configure your federation server to work with the *Archiving Single Sign-On* authentication service.
2. Set up Active Directory user synchronization either with CloudLink or Office 365 Sync through the Provisioning options.

For additional details on the supported Single Sign-On providers and guidance on configuring them, refer to the Arctera Insight Archiving Compatibility List

After configuring the Arctera Insight Archiving authentication service and your ADFS environment, you can provide single sign-on access to Arctera Insight Personal Archive users.

Table: Arctera Insight Archiving authentication service configuration summarizes the steps to configure the Arctera Insight Archiving authentication service to work with your AD FS environment.

Table: Arctera Insight Archiving authentication service configuration

STEP	ACTION	REFERENCE
Step 1	In Arctera Insight Management Console, enable the Authentication Settings permission for the Policy Manager role.	See Enabling the Authentication Settings permission for the Policy Manager role .
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 .
Step 3	On the Authentication Management page, select ADFS as the authentication method for your organization.	See Selecting an authentication method .
Step 4	Upload the -signing certificate that you generated from your ADFS environment.	See Uploading a -signing certificate .
Step 5	Validate the Identity Provider URL for your organization.	See Validating the Identity Provider URL .
Step 6	Activate single sign-on for Insight Personal Archive users.	See Activating single sign-on .

Enabling the Authentication Settings permission for the Policy Manager role

The Authentication Management page in Arctera Insight Management Console lets you configure the Arctera Insight 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. 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 Arctera Insight Archiving authentication service.

> “ ”

Note: The administrator may need to log out and log back in to Arctera Insight Management Console before they can access theAuthentication Managementpage.

> “ ”

To assign the Policy Manager role to an administrator

1. In the left navigation pane, click **Assign Accounts**.
2. From the user list, search for and select the *Administrator* to which you want to assign the role.

You can use the filters to search for the required *Administrator*.

1. On the **Role Change**page, in the**Role** drop-down, select *Administrator*.

2. Expand the **Built-in Roles**section and select**Policy Manager**.
3. Click **Save**.

Selecting an authentication method

To manage secured user access to other Insight Archiving applications for example, Insight Personal Archive, you must configure the authentication service in Arctera Insight Management Console. You can select your preferred authentication method. This helps customers to centrally control access to archived databases across multiple cloud platforms by using corporate Single Sign-On (SSO) policies.

Prerequisite

Before you configure SSO authentication, you must:

- Refer to the Arctera Insight Management Console Compatibility List for supported SSO providers.
- Configure your enterprise server to integrate with the archiving SSO authentication service.
- Set up Active Directory user synchronization using CloudLink or MS Office 365 Sync in the *Provisioning* options.

To select an authentication method

1. In the left navigation pane, select **Policy Management**>**Authentication Management**, and click**Edit**.
2. Under **Setup Authentication**, in the**Authentication Type** field, select the required type of authentication method and perform the corresponding actions.

AUTHENTICATION TYPE	DESCRIPTION
Cloud Archive Database	Upon selecting this option, specify the following options\:
	1. Password Change Required? : Select Yes to ask users to change their password during their initial login after configuring their authentication setup. Users need to provide their username and password when accessing the application that is configured for SSO. For example, Insight Personal Archive. To understand password complexity

AUTHENTICATION TYPE	DESCRIPTION
	rules, See Configuring an advanced password policy . Select No if users do not need to change their password during their initial login.
	2. Multi Factor Authentication Required? Select Yes to set requirement for multi-factor authentication. Upon selecting Yes , the Type Of Authentication Required? field appears. Currently, users can use either Email or TOTP authentication option. Selecting Email requires users to verify via a link or OTP sent to their registered email. Selecting TOTP requires users to authenticate using a time-based one-time password via an authenticator app. Select No if multi-factor authentication is not required.
	3. Click Save to finish the configuration.
Single Sign-On ADFS	Upon selecting this option, specify the following options\:
	1. Hybrid Login Allowed? : Select Yes to enable hybrid login. The Multi Factor Authentication Required? option remains available. Select No to disable hybrid login. The Multi Factor Authentication Required? option becomes unavailable. **Note:** This option is supported only if theSingle Sign-On - ADFSauthentication type is selected. For other Multi Factor Authentication options, such as Azure, Okta, OneLogin, and so on, this option remainsdisabled.
	2. Role Claims Enabled? : Select Yes to assign role-based SSO response. Select No to avoid role-based SSO response.
	3. Multi Factor Authentication Required? : Select Yes to assign role-based SSO response. When Hybrid Login is enabled,

AUTHENTICATION TYPE	DESCRIPTION
	multi factor authentication applies only when users log in with the CloudArchive credentials to access Insight Archiving applications. Upon selecting Yes , the Type Of Authentication Required? field appears. Currently, users can use either Email or TOTP authentication option. Selecting Email requires users to verify via a link or OTP sent to their registered email. Selecting TOTP requires users to authenticate using a time-based one-time password via an authenticator app. Select No to avoid role-based SSO response.
	4. Unique OWA IdP : Specifies if you want to set any external authentication service to verify user credentials while accessing Outlook. Select Yes to specify a separate identity provider for Outlook access. Upon selecting Yes , the Unique OWA CID field appears. Select Yes to assign a distinct client ID for each session to enhance security by preventing unauthorized access and session hijacking. Select No to avoid assigning a distinct client ID for each session. Select No to avoid specifying a separate identity provider.
	5. Your Trust Information : Upon saving, the application displays the Customer ID , Unique OWA Client ID , and Entity ID , if enabled during configuration.
	6. Select the I have read the instructions for setting the provided Entity ID and created my public key for upload. check box to confirm your configuration.
	7. Click Save to finish the configuration.

AUTHENTICATION TYPE	DESCRIPTION
Single Sign-On - SAML 2.0 based :	Upon selecting this option, specify the following options\:
	1. Hybrid Login Allowed? : Select Yes to enable hybrid login. The Multi Factor Authentication Required? option remains available. Select No to disable hybrid login. The Multi Factor Authentication Required? option becomes unavailable. **Note:** This option is supported only if theSingle Sign-On - SAML 2.0authentication type is selected.
	2. Role Claims Enabled? : Select Yes to assign role-based SSO response. Select No to avoid role-based SSO response.
	3. Multi Factor Authentication Required? : Select Yes to assign role-based SSO response. When Hybrid Login is enabled, multi factor authentication applies only when users log in with the CloudArchive credentials to access Insight Archiving applications. Upon selecting Yes , the Type Of Authentication Required? field appears. Currently, users can use either Email or TOTP authentication option. Selecting Email requires users to verify via a link or OTP sent to their registered email. Selecting TOTP requires users to authenticate using a time-based one-time password via an authenticator app. Select No to avoid role-based SSO response.
	4. Unique OWA IdP : Specifies if you want to set any external authentication service to verify user credentials while accessing Outlook. Select Yes to specify a separate identity provider for Outlook access. Upon selecting Yes , the Unique OWA CID field appears. Select Yes to assign a distinct client ID for each session to enhance security by

AUTHENTICATION TYPE	DESCRIPTION
	preventing unauthorized access and session hijacking. Select No to avoid assigning a distinct client ID for each session. Select No to avoid specifying a separate identity provider.
	5. Your Trust Information : Upon saving, the application displays the Customer ID , Unique OWA Client ID , and Entity ID , if enabled during configuration.
	6. Select the I have read the instructions for setting the provided Entity ID and created my public key for upload. check box to confirm your configuration.
	7. Click Save to finish the configuration.

Uploading a -signing certificate

After you select AD FS as the authentication method for your organization, you must upload a -signing certificate from your AD FS environment.

See Configuring AD FS to work with Arctera Insight Archiving.

From the Upload Your Public Key section on the Authentication Management page, you can upload your -signing certificate. The Upload Your Public Key section displays after you complete the Setup Authentication section.

To upload a -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 -signing certificate that you have generated.

> “ ”

Note: The -signing certificate that you upload must have a.ceror.certfile 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 -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 byadfs/ls. For example, the Identity Provider URL for an AD FS server namedadfswith a fully qualified domain name ofexample.comishttps://adfs.example.com/adfs/ls. The Arctera Insight 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, contactArctera 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 selectedYesin 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 Insight 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 Insight Personal Archive users.

> “ ”

Note: The Arctera Insight 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 Insight Personal Archive.

> “ ”

Managing Retention Policies

This section includes the following topics:

About Retention Management

From the Retention Management section, you can manage the settings and polices that determine how long archived messages are retained in Arctera Insight Archiving. By default, Arctera Insight Archiving retains archived messages indefinitely (although this is not recommended since it will result in Storage overages in future). If required, you can configure Arctera Insight 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 Arctera Insight eDiscovery are not removed.

> “ ”

Beyond the global retention period, the retention period for archived messages can be modified by creating retention policies to associate with the following policy targets. See Supported retention scenarios for WORM and non-WORM Insight Archiving customers.

- Managed Tags-based retention: 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 modify their retention period. The retention period of the associated retention policy determines how long tagged messages are retained in Arctera Insight Archiving.
- Active Directory Groups and Distribution List based retention: The Active Directory Groups or Distribution List are synchronized using provisioning services. Associating a retention policy with the active directory groups or distribution list modify the retention period of the archived messages for all members of that group or list. The retention period of the associated retention policy determines how long the messages for the members are retained in Arctera Insight Archiving.
- Classification-based retention: The retention period applied to items during archiving is determined by several factors. See Supported retention scenarios for WORM and non-WORM Insight Archiving customers.. Retention is applied in the following order:
    - If a classification-based retention policy is not applied to the item, then the longest retention policy among the multiple applicable retention policies gets applied to it.
    - If a classification-based retention policy is applied to the item, and this classification policy has an associated retention policy, then retention of that item is determined by the retention policy associated with the applied classification policy. Classification-based retention supersedes retention set by other means, irrespective of whether it is shorter or longer than any other applicable retention policies for that item.

In the above-mentioned example, if the item is responsive to more than one classification policy with associated retention policies, then the longest retention policy is applied. Classification-based retention supersedes retention set by other means as mentioned above.

Supported retention scenarios for WORM and non-WORM Insight Archiving customers

This section provides the retention scenarios that are supported for the WORM and non-WORM Insight Archiving customers.

WORM storage-specific scenarios

- Setting retention of items as these are archived:
  - Default retention
  - Per user
  - AD Group membership
  - Classification-based retention
  - Search and tagging
- Extending retention of items:
  - Search and tagging (WORM policy on items is not updated)
  - Classification-based retention (via paid *Reindex* option)
- Shortening retention of items:
  - Not supported if the item is already archived.
  - Supported only at the time of archiving.

During archiving, every item is assessed/evaluated for its retention period. If the retention period of an item is shorter than the tenant-level WORM policy (typically 7 or 10 years), both periods are set to the same value. This process occurs automatically, without any direct involvement from end users. It is executed using one of the following scenarios according to the policy.

- Per user
- AD Group Membership
- Classification-based retention

Non-WORM storage-specific scenarios

- Setting retention of items as these are archived
  - Default retention
  - Per user

    - AD Group membership
    - Classification-based retention
    - Search and tagging
- Extending retention of items
    - Search and tagging (WORM policy on items is not updated)
    - Classification-based retention (via paid *Reindex* option)
- Shortening retention of items
    - Search and tagging
    - Classification-based retention (via paid *Reindex* option)

Configuring the default retention period

The default retention period determines how long archived messages are retained in Arctera Insight Archiving. To begin the process of removing messages from Arctera Insight 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 Arctera Insight 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, active directory groups, and distribution list.

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.

1. 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 List.

> “ ”

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. Click on the policy you want to associate with a target.
3. Under **Policy Details** , ensure that the policy details are appropriate.
4. Under **Targets**, click**Add Targets**.

The **Policy Target** window appears.

1. In the **Target Type** drop-down, one of the following targeted users to associate with the policy. The currently available options:
    - All
    - Distribution Lists
    - Tags
    - **Active Directory Groups** :

This option allows customers who sync Azure Active Directory groups using **ADGroupSync**or**SCIM Group Sync** to use group membership information for retention.

You must associate Managed Tags when a policy is set to target Active Directory Groups. Managed Tags are applied to items based on group membership at the time the items are received. Therefore, when the Managed Tags are not associated, the group membership is evaluated only at the time of item expiry.

1. 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.

1. 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 Arctera Insight Archiving:

- Messages that have a matter-level, a search-level, or message-level legal hold applied from Arctera Insight 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 Arctera Insight Archiving cannot be retrieved after removal is complete. If Advanced Supervision service is enabled,Storage Expiryis set toDailyby 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.
	- 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.

> “ ”

Note: The 14-day cool-off period begins when items are batched for expiry. During this period, items remain on the storage expiry list. After 14 days, the items are permanently deleted.

> “ ”

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 section includes the following topics:

About Email Continuity

Email Continuity is an add-on feature that allows Insight 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 Arctera Insight Archiving. Outgoing messages from your mail server are typically journaled to Arctera Insight 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 Arctera Insight 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 Arctera Insight Archiving, and users can receive and send email messages through Insight 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 Arctera Insight Archiving Compatibility List.

Configuring Email Continuity

Table: Steps to configure Email Continuity lists the steps you need to take to configure Email Continuity.

Table: Steps to configure Email Continuity

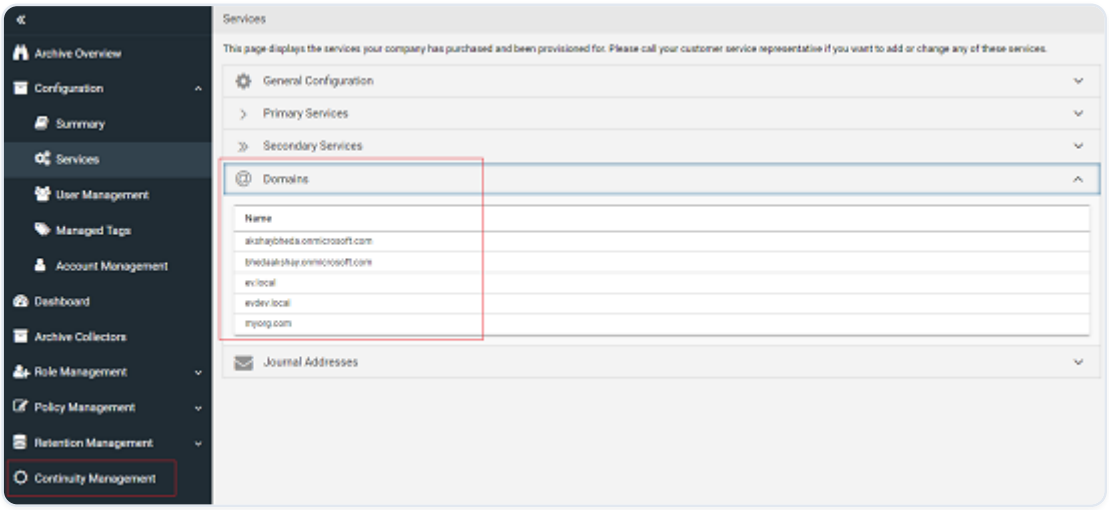
STEP	ACTION	REFERENCE
Step 1	Get Arctera Services & Support to provision the Email Continuity service for your mail servers.	See Provisioning the Email Continuity service for your mail servers .
Step 2	Add the Email Continuity IP ranges to your firewall and to your mail server allowlists, as required.	See Adding the Email Continuity IP ranges to your firewall and mail server allowlists .
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 .
Step 4	Test the new setup to ensure that Email Continuity is configured correctly.	See Testing the Email Continuity configuration .

Provisioning the Email Continuity service for your mail servers

You must get Arctera 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 Arctera Insight Archiving Arctera Insight Management 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.

1. Contact Arctera Services & Support and do as follows:

    - Inform Arctera Services & Support that you want to add Email Continuity as an Arctera Insight Archiving service for your organization.
    - If you found in step 4 that any of your mail server inbound domains were not configured in Arctera Insight Management Console, ask Arctera Services & Support to add the required inbound domains to your Arctera Insight Archiving company configuration.
    - Provide Arctera 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 Arctera Services & Support, obtain the following information that needs to be used in the next steps:
  - The Arctera Insight Archiving Email Continuity IP ranges for your Arctera Insight Archiving instance.
  - The Arctera Insight 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 Arctera 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 Arctera Insight 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 Arctera Insight Archiving Email Continuity mail server domain that you obtained from Arctera 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 Arctera Insight 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 Arctera 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 Insight Personal Archive.
    - Test that you can send email from Insight Personal Archive to an external email address.
    - Test that you can send email from Insight Personal Archive to an internal email address.
3. Restart your email service and verify that the test emails you sent and received in Insight 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 Arctera 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 section includes the following topics:

About Arctera Insight Archiving reports and notifications

This section explains you about generating various Arctera Insight Archiving and Insight Capture-specific reports, logs and notifications for your organization. You can export the logs and reports in various file formats.

Reports

This section describes procedures to generate various reports in Arctera Insight Management Console .

Generating Messaging reports

The Messaging Report displays information about Arctera Insight 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.

The available options are *Message Size*,*Message User*,*Search Speed*,*Emails Imported*.

1. Select a predefined duration, or select **Custom** if you want to specify a start and end date for the report.
2. If required, select **Compare to All Companies** to compare your usage to other organizations.
3. Click **Apply**.
4. If required, switch between the **Line Chart**and**Bar Chart** display options to view chart in the report.
5. To export the report in EXCEL, PDF, CSV, or WORD format., click the **Export** icon.

Generating Insight Personal Archive reports

The Insight Personal Archive report displays information about Insight Personal Archive usage based on the following parameters:

- The number of users that have logged in to Insight 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 Insight Personal Archive usage of your organization with the usage of other organizations

To generating a Insight 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.

The available options are *User Logins*,*Tags Created*,*Tags Applied*,*Search Performed*,*Search Speed*,*Search Strings*,*Folder Counts*, and*Delete Emails*.

> “ ”

Note: If you select theDelete Emailsoption, specify the date range for which you want to view the details of the deleted emails of end users, email address of sender-recipient, email address of the person who executed the delete activity, and subject of email. ClickSearch. These parameters are available only if you want to view and export deleted emails report.

> “ ”

1. For other options (except the *Delete Emails* option), select a predefined duration, or select **Custom** if you want to specify a start and end date for the report.
2. If required, select **Compare to All Companies** to compare your usage to other organizations.
3. Click **Search**.
4. If required, switch between the **Line Chart**and**Bar Chart** display options to view chart in the report.
5. To export the report in EXCEL, PDF, CSV, or WORD format., click the **Export** icon.

Generating Insight eDiscovery reports

Insight eDiscovery reports display information about Insight eDiscovery administration actions based on the following parameters:

To generate an Insight eDiscovery report

1. In the left navigation pane, select **Reports and Notifications**>**Reports**.
2. On the **Archiving Scorecard**page, select the**eDiscovery** tab.
3. In the top-right corner of the page, select the parameter for which you want to generate a report.

The available options are as follows:

- **Hidden Emails** : Lets you view detailed report of hidden emails from end users.

- **Unhidden Emails** : Lets you view detailed report of unhidden emails to end users.
- **Delete Emails**: Lets you view detailed report of deleted emails of end users. Specify the date range for which you want to view the details, email address of sender-recipient, email address of the person who executed the delete activity, and subject of email. Click**Search**. These parameters are available only if you want to view and export deleted emails report.
- **Mail Reassignment** : Lets you view detailed report of reassigned emails of end users.

1. For other options (except the *Delete Emails* option), select a predefined duration, or select **Custom** if you want to specify a start and end date for the report.
2. If required, select **Compare to All Companies** to compare your usage to other organizations.
3. Click **Search**.
4. If required, switch between the **Line Chart**and**Bar Chart** display options to view chart in the report.
5. To export the report in EXCEL, PDF, CSV, or WORD format., click the **Export** icon.

See About Arctera Insight Archiving reports and notifications.

Generating Transcription reports

The Transcription report displays information about the transcription service usage within a specified duration. This report lets users analyze unprocessed files and identify reasons for transcription failure. The following parameters are displayed on the report.

- The total files processed for transcription.
- The total files transcribed successfully.
- The total files for which transcription failed.

To generate a Transcription report

1. In the left navigation pane, select **Reports and Notifications**>**Reports**.
2. On the **Archiving Scorecard**page, select the**Transcription** tab.
3. Specify the duration (From date-To date) for which you want to generate a report.
4. Click **Search** to view the transcription-specific statistics.

It displays the number of files processed for transcription, files successfully transcribed, and files for which transcription failed for some reason. The report shows file names, the user who

processed each file, processing date and time, transcription status (successful or failed), and reasons for transcription failure.

If the list is extensive, follow these steps for your convenience:

- Choose the number of files you want the application to display per page.
- Use navigation arrows at the bottom of the page for easy access to the first, previous, next, and last pages.

1. To export the report in Excel, PDF, CSV, or Word format, click the **Export**icon located near the**Search** button.

Generating Mobile Web Access reports

This report displays information about Mobile Web Access 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.

The available options are *User Logins*,*Search Performed*, and*Search Strings*.

1. Select a predefined duration, or select **Custom** if you want to specify a start and end date for the report.
2. If required, select **Compare to All Companies** to compare your usage to other organizations.
3. Click **Apply**.
4. If required, switch between the **Line Chart**and**Bar Chart** display options to view chart in the report.
5. To export the report in EXCEL, PDF, CSV, or WORD format., click the **Export** icon.

Generating message reconciliation report

Only users for whom the Reconciliation Report Notifications feature is enabled. To enable this feature, contact your system administrator.

Users can generate, view, and download reconciliation report that provides users with a real-time insight into message flow and reconciliation metrics, enhancing their operational control and efficiency through direct data access.

To generate a message reconciliation report

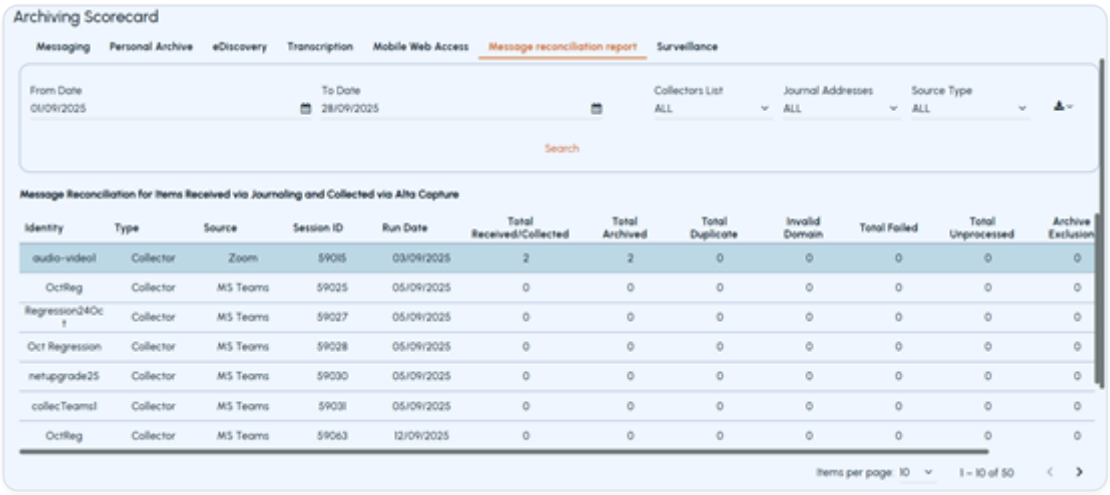
1. In the left navigation pane, select **Reports and Notifications**>**Reports**.
2. On the **Archiving Scorecard**page, select the**Message reconciliation report** tab.
3. Specify the duration (From date-To date) for which you want to generate a report.
4. Click **Search** to view the transcription-specific statistics.

The reconciliation data table provides a detailed view of items that are received through journaling addresses and collected by the archive collectors configured for the user. This information is also represented graphically in a bar chart, which categorizes the data by collector and references the entries in the Collectors List for correlation.

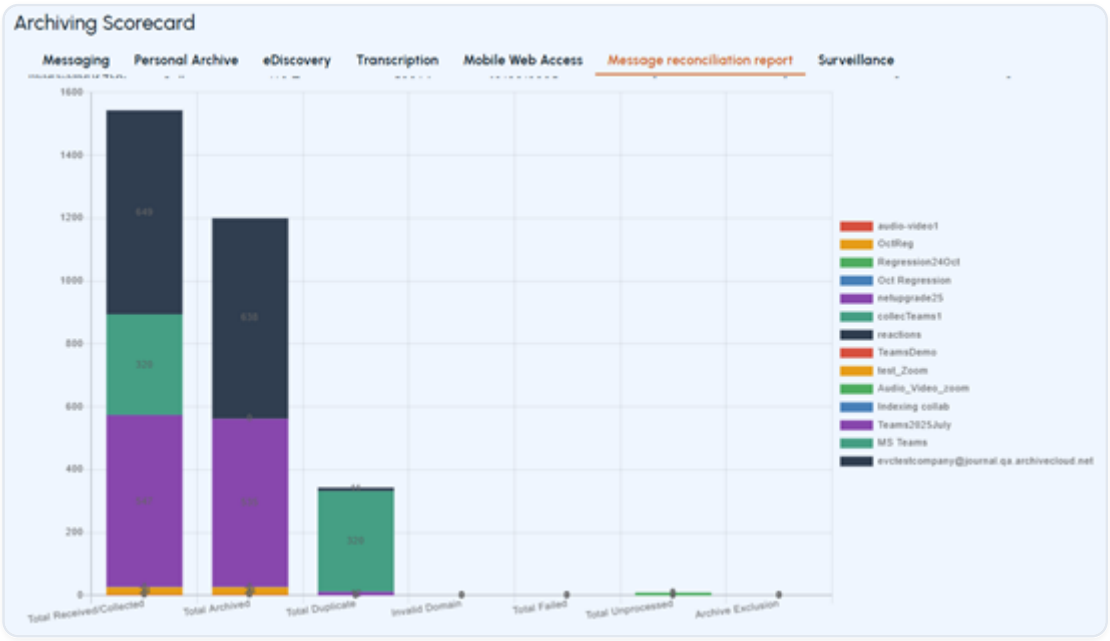
If the list is extensive, follow these steps for your convenience, and click **Search**. The reconciliation data table and graph update automatically based on the selected criteria.

- From the **Collectors List** drop-down, choose a specific collector or select ALL to include every configured collector.
- From the **Journal Addresses** drop-down, choose a specific journaling address or select ALL to include all addresses.
- From the **Source Type** drop-down, choose a specific source type or select ALL to include all types.
- Choose the number of items you want the application to display per page.
- Use navigation arrows at the bottom of the page for easy access to the first, previous, next, and last pages.

Reconciliation data in tabular format



Reconciliation data in graphical format



1. To download the report, click the **Download** icon, and then select either PDF or CSV as the format.

Generating an Insight Surveillance specific Report

You can generate the Account Mapping report for Insight Surveillance.

To generate the Account Mapping report for Insight Surveillance

1. In the left navigation pane, select **Reports and Notifications**>**Reports**.
2. On the **Archiving Scorecard**page, select the**Surveillance** 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 Email address, RepID, and last name of the account holder 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 Arctera Insight Archiving reports and notifications.

Usage

This section describes procedures to generate various usage-specific reports in Arctera Insight Management Console .

Generating a service usage report

The Service Usage tab provides service 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 have enabled or disabled mailboxes.

> “ ”

- User Statistics: Generates a report showing the number of enabled and disabled users. Additionally, it displays a horizontal red line indicating the number of licenses purchased by the customer. Active users above this red line are considered overage (additional active users). Refer to the sample image for enhanced visualization and understanding of this report.

This report alerts customers to consider purchasing more licenses or to begin paying for the additional users.

- 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 (Arctera Insight Archiving): Generates a report for the number of Folder Sync User(s) enabled and quota (minimum license count) for Arctera Insight 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.

Generating a capacity trend report

While adding a customer or a partner profile in Management Console, the administrator specifies the number of licenses, with a default storage limit of 15 GB per license. For instance, provisioning 10 licenses results in a default storage capacity of 150 GB. Additionally, the administrator can allocate a requested amount of storage to customers and their partners.

Although the overall storage capacity usage can be checked during the editing of customer or partner profiles, situations may arise where they utilize either less or more than the allocated storage, potentially impacting them financially through overage charges. Consequently, customers or partners may seek a report to make decisions regarding their storage capacity.

The Capacity Trend report provides the allowed and consumed storage capacity details for customers or their partners in graphical or chart format. This report helps customers or their partners understand their proximity to the licensed (allowed) and actually used storage limit. By reviewing this report, they can proactively make decisions, such as acquiring extra storage or receiving advance notifications to prevent overage charges.

The Capacity Trend tab provides a storage capacity trend report based on date range and frequency. 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.

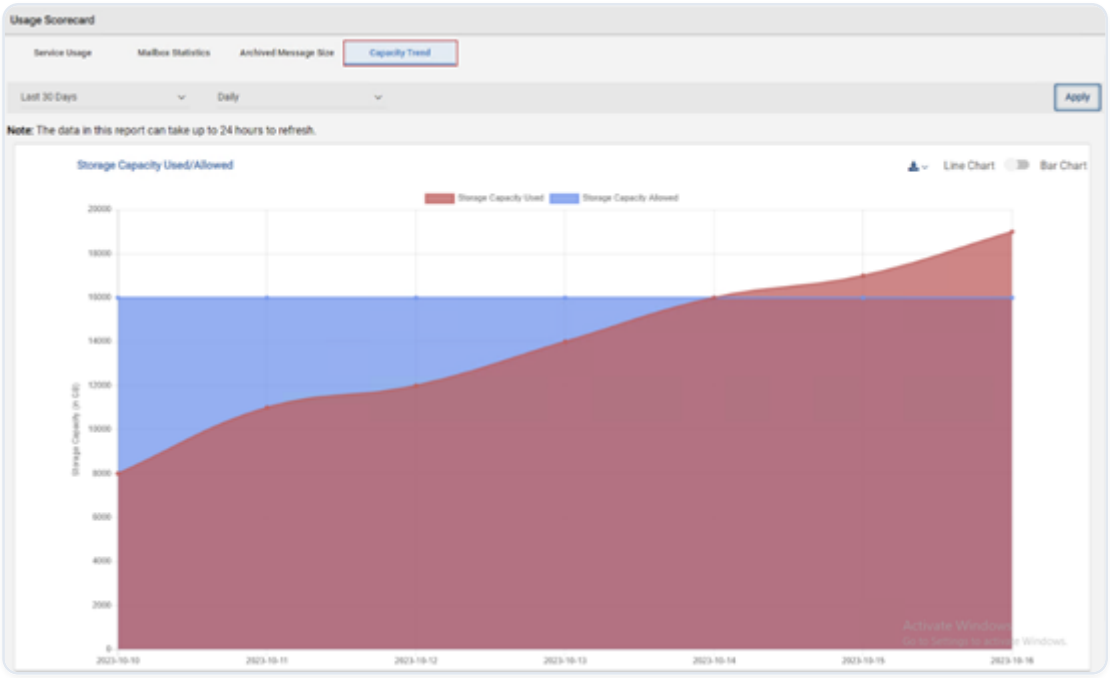
> “ ”

To generate a storage capacity trend report

1. In the left navigation pane, select **Reports and Notifications**>**Usage**.
2. On the **User Scorecard**page, select the**Capacity Trend** tab.

3. Select a predefined duration, or select **Custom** if you want to specify a start and end date for the report.
4. Select the predefined frequency (Daily, Weekly, Monthly, Quarterly, or Yearly.)
5. Click **Apply**.

The application generates a report indicating the licensed (allowed) and actually utilized storage limit by the customer or their partners, as shown in the sample image below.



1. If required, switch between the **Line Chart**and**Bar Chart** display options to view chart in the report.
2. To export the report in EXCEL, PDF, CSV, or WORD format., click the **Export** icon.

Generating a transcription trend report

The Transcription Trend report provides the allowed and consumed transcription length (in hours) details for customers or their partners in graphical or chart format. This report helps customers or their partners understand their proximity to the licensed (allowed) and actually used transcription limit. By reviewing this report, they can proactively make decisions.

> “ ”

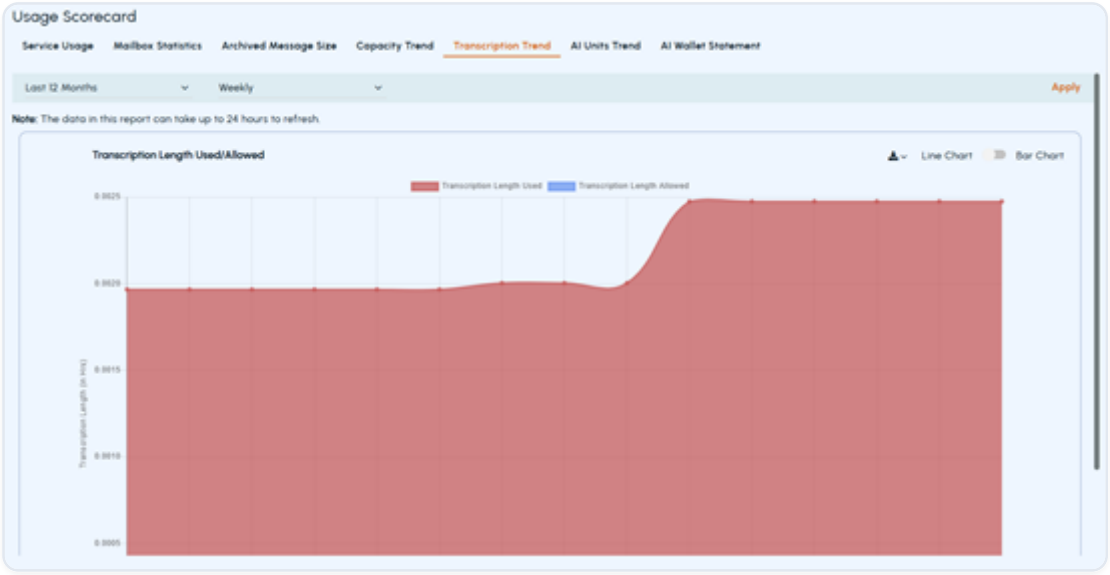
Note: Data can take up to 24 hours to refresh once you've enabled or disabled mailboxes.

> “ ”

To generate a transcription trend report

1. In the left navigation pane, select **Reports and Notifications**>**Usage**.
2. On the **User Scorecard**page, select the**Transcription Trend** tab.
3. Select a predefined duration, or select **Custom** if you want to specify a start and end date for the report.
4. Select the predefined frequency (Daily, Weekly, Monthly, Quarterly, or Yearly.)
5. Click **Apply**.

The application generates a report indicating the licensed (allowed) and actually utilized transcription limit by the customer or their partners, as shown in the sample image below.



1. If required, switch between the **Line Chart**and**Bar Chart** display options to view chart in the report.
2. To export the report in EXCEL, PDF, CSV, or WORD format, click the **Export** icon.

Generating a AI units trend report

The AI Units Trend report provides the allowed and consumed AI unit details for customers or their partners in graphical or chart format. This report helps customers or their partners understand their proximity to the licensed (allowed) and actually used AI Units limit. By reviewing this report, they can proactively make decisions.

> “ ”

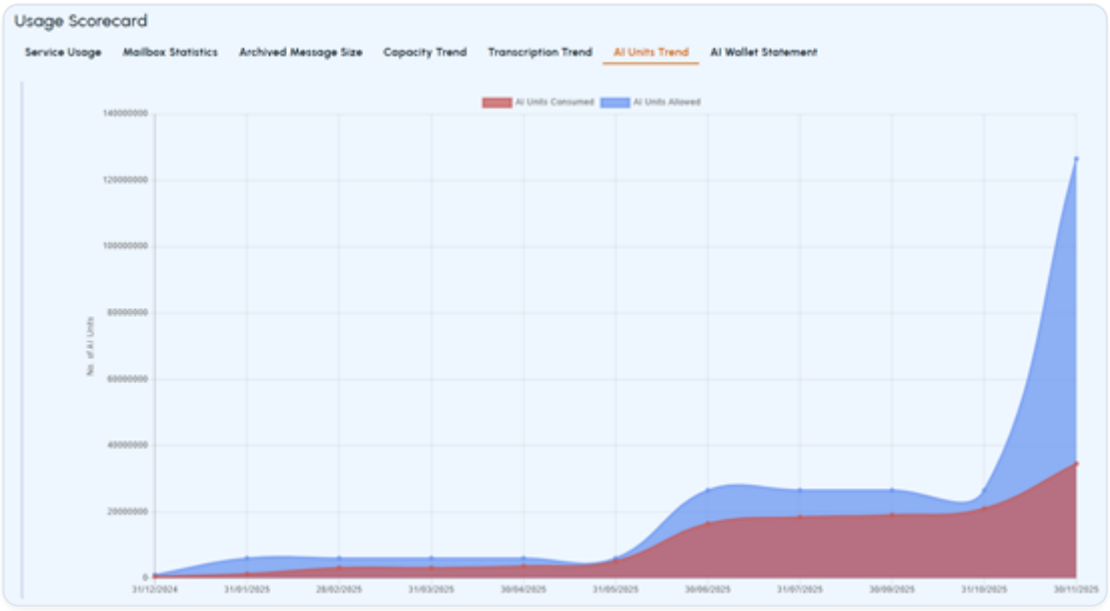
Note: Data can take up to 24 hours to refresh once you've enabled or disabled mailboxes.

> “ ”

To generate a AI units trend report

1. In the left navigation pane, select **Reports and Notifications**>**Usage**.
2. On the **User Scorecard**page, select the**AI Units Trend** tab.
3. Select a predefined duration, or select **Custom** if you want to specify a start and end date for the report.
4. Select the predefined frequency (Daily, Weekly, Monthly, Quarterly, or Yearly.)
5. Click **Apply**.

The application generates a report indicating the licensed (allowed) and actually utilized AI Units limit by the customer or their partners, as shown in the sample image below.



1. If required, switch between the **Line Chart**and**Bar Chart** display options to view chart in the report.
2. To export the report in EXCEL, PDF, CSV, or WORD format, click the **Export** icon.

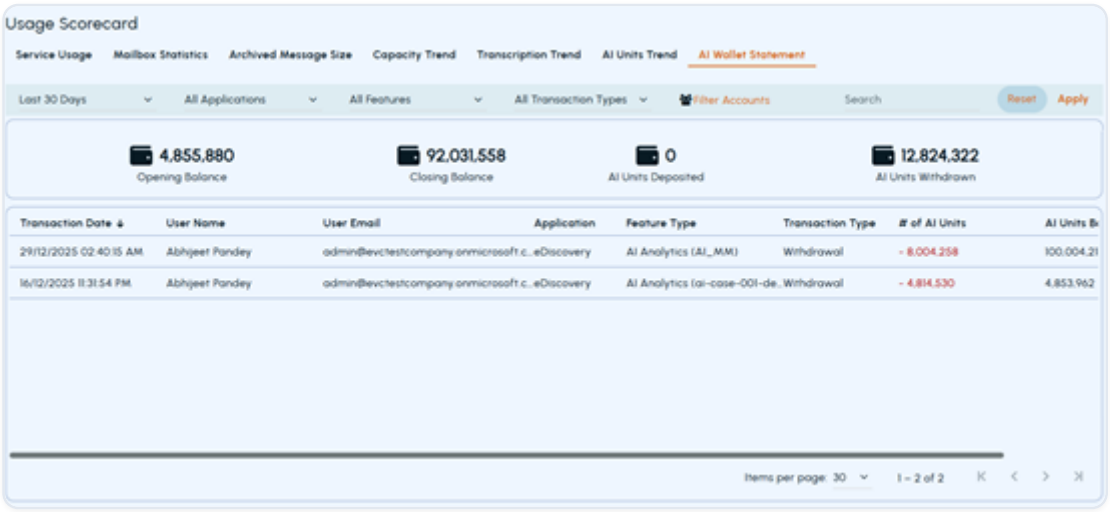
Generating the AI Wallet Statement

As an administrator, you can generate an AI wallet statement to track AI unit consumption by applications and their associated features. Each recorded transaction can be traced to a specific user account for review.

To generate the AI wallet statement

1. In the left navigation pane, select **Reports and Notifications**.
2. Access the **Usage** tab.
3. On the **Usage Scorecard**page, select the**AI Wallet Statement** tab.

By default, the page shows a 30-day summary of AI unit consumption by all applications, features, and associated user accounts.



1. To view the specific record, do the following:

DURATION	SELECT THE PERIOD FOR WHICH YOU WANT TO VIEW AI UNIT CONSUMPTION.
All Applications	Select the application for which you want to view AI unit consumption.
All Features	Select all or a specific feature of the selected application.
All Transaction Types	Select All or choose a specific transaction type to view only deposited or only withdrawn AI units.
Filter Accounts	Click to open the Add/Remove Accounts pop-up, and then select the required user accounts.
Search field	Enter keywords to filter the records by user name or email.

Note: If required, click**Reset** to clear the selected filters and apply new filter selections.

1. Click **Apply**to view the record based on the selected filters.**Scenario**: To view AI unit consumption by the**AI Analytics** feature of the Insight eDiscovery application

a. From the application drop-down list, select **eDiscovery**.

b. From the features drop-down list, select **AI Analytics**.

c. Select a specific user account if required.

d. Click **Apply** to review the AI units transactions.

Logs

This section describes procedures to generate various log reports in Arctera Insight Management Console .

Viewing the Activity Log

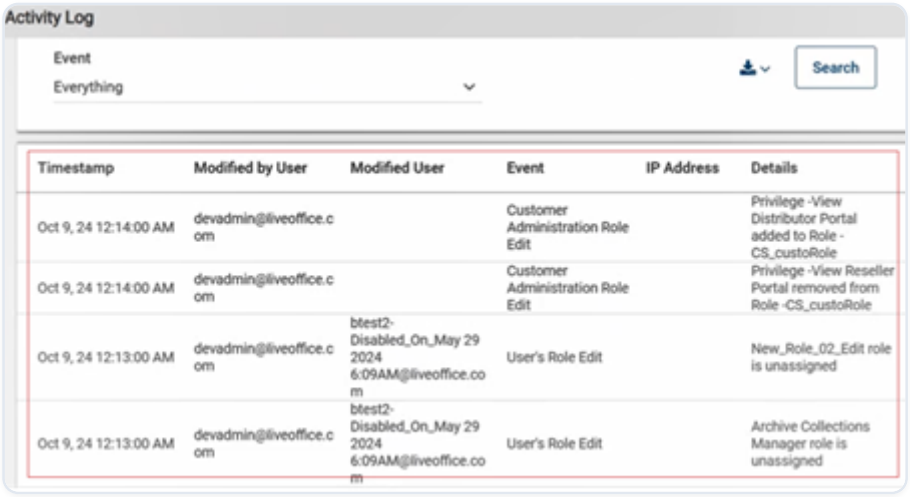
The Activity Log displays all events that occur in Arctera Insight Archiving including user logins, password resets, and user role changes. From the Activity Log page, you can view the full log or filter the log by date range, user name, events, or event details.

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, displaying logs/events for added or removed roles and permissions in both built-in and custom roles, along with a user who modified the permissions, users who are modified for which roles and permissions, and date/time of modification.

The **Activity Log** provides detailed logs for events when a user's built-in role is changed during a bulk account import, including which role has been assigned or unassigned, which user made the changes, and the event date and time.



> “ ”

Note: The report does not display the private IP addresses of events that the Arctera Insight Archiving services have logged. Instead theIP Addresscolumn displaysInternal Service.

> “ ”

1. 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 Arctera Insight 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 Arctera Insight 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 Insight Archiving 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 Arctera Insight 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 Arctera Insight 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.

Subscribing to receive SIEM/SOAR Logs

The SIEM/SOAR Logs feature allows customers to retrieve all logs and transfer them to other tools, such as *Splunk* , for further processing.

To receive SIEM/SOAR Logs, customers need to contact Arctera Support and request enabling the SIEM/SOAR Log shipping service for their environment. Customers must specify which of the following storage options they require:

- AWS
- Microsoft Azure
- SFTP

This service collects the following details:

- Search logs from the Arctera Insight Management Console
- Message logs, Activity logs, and Browser logs (including Mobile Browser, Discovery Browser, and Personal Browser) from the Insight eDiscovery portal

The SIEM/SOAR service identifies the collected logs by their name and creation date, and generates a separate CSV file for each log. If the customer has subscribed to this service, these CSV files are securely uploaded to their storage managed by the customer. The service employs the following components:

- APIs provided by Amazon/Microsoft Azure/SFTP for uploading the CSV files.
- Advanced Encryption Standard (AES-256) for secured data transmission. Each object is encrypted with a unique data key, providing additional protection for the data.

Refer to the following related knowledge base article to see sample SIEM/SOAR sample log reports in CSV format.

> “ ”

Note: To ensure seamless and secured data transmission, customers are recommended to set up the necessary firewall rules to accomplish secure data upload to their storage of choice

> “ ”

Notifications

The Notifications node is visible only when you are logged in with the System Administrator role. Only users with this role can enable or disable usage, capacity, and retention-specific notifications. This section describes how to configure notification-specific parameters in the Arctera Insight Management Console .

Usage Notification

This feature allows system administrators to monitor active archive usage and committed capacity usage. By configuring this feature, administrators can proactively manage active archive usage and committed capacity overage.

As a system administrator, you can configure this feature by performing the following actions:

- Enable notifications
- Set notification threshold
- Set notification frequency
- Manage recipients who will receive notifications
- Track the history of configuration changes

See Configuring the usage notifications feature.

> “ ”

Note: Users are notified when either the active archive usage or the committed capacity usage exceeds the configured threshold.

> “ ”

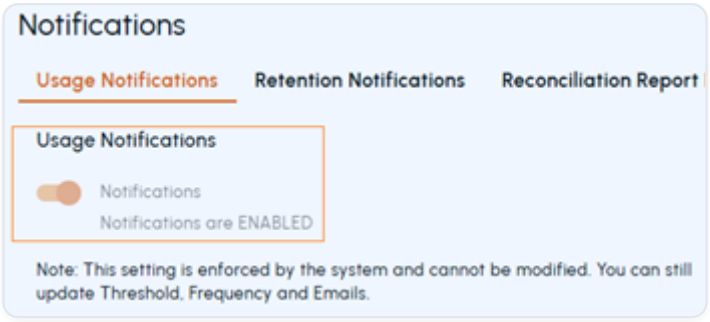
Configuring the usage notifications feature

To configure the usage notifications feature

1. In the left navigation pane, select **Reports and Notifications**>**Notifications**.
2. Select the **Usage Notifications**tab, and click**Edit**.

3. **Enable notifications**

To enable notifications, slide the switch to the right.



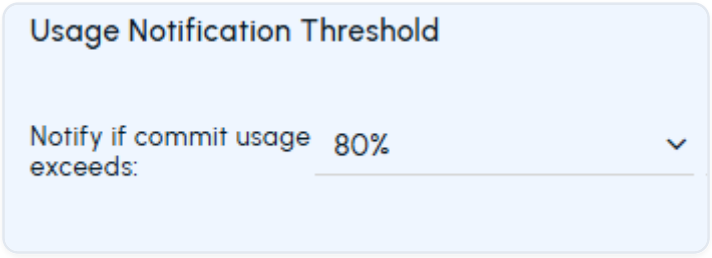
> “ ”

Note: After this feature is enabled, it cannot be disabled. The restriction is enforced at the system level to ensure continued compliance and operational awareness. Critical alerts remain active so administrators are always aware of capacity risks. However, administrators can adjust the thresholds and frequency at any time.

> “ ”

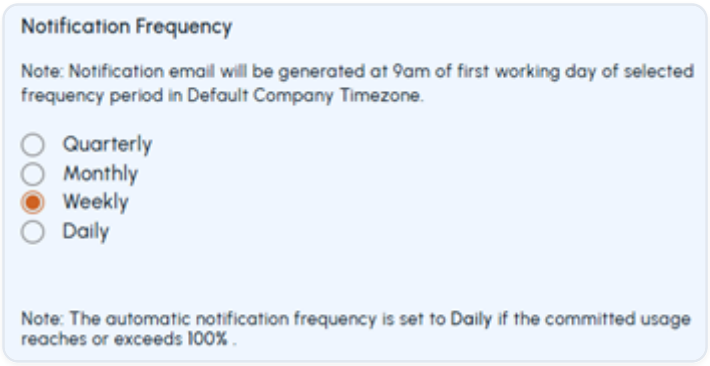
1. **Set notification threshold**

In the *Notify if committed usage exceeds* field, select the desired threshold percentage (for example 80%) from the predefined values.



1. **Set notification frequency**

Select one of the following intervals:



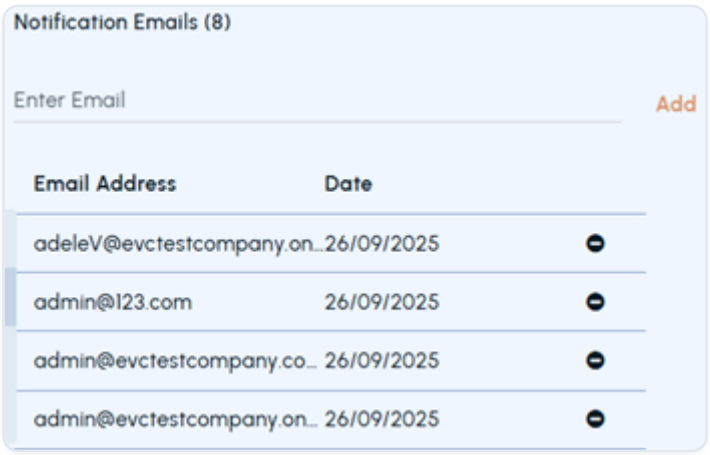
- **Quarterly** \- Notifications are sent on the first Monday of each quarter. The quarters start in January, April, July, and October.
- **Monthly** \- Notifications are sent on the first Monday of each month.
- **Weekly** \- Notifications are sent every Monday. This setting is the default frequency.
- **Daily** \- Notifications are sent every day.

> “ ”

Note: Notification emails are sent at 9:00 A.M. in the default company time zone. If committed usage reaches or exceeds 100%, the notification frequency is automatically set toDaily.

> “ ”

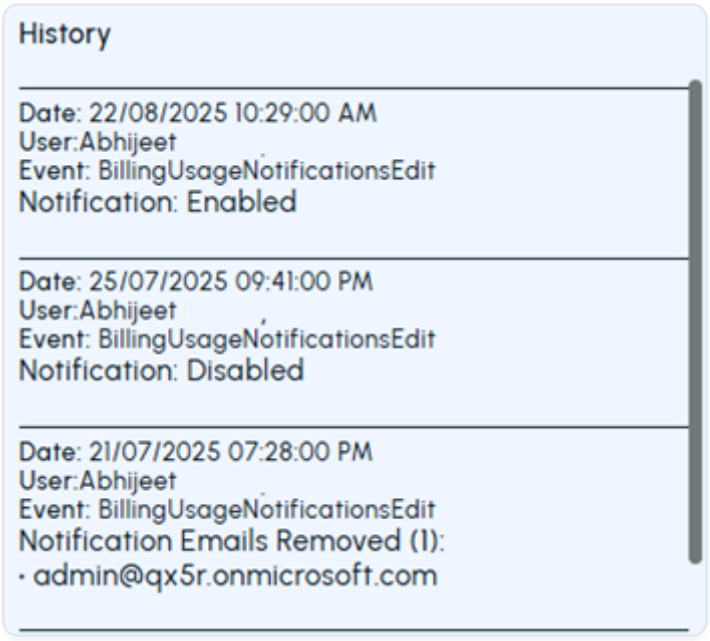
1. **Manage recipients**Under**Notification Emails** , do the following as needed:



- To add an address, enter the email address and click **Add**.
- To remove an email address, select the email address and click the **Remove** icon in the corresponding row.

1. **Track the history of configuration changes**

This is a read-only section. You can monitor the logs such as who made changes, when they were made, and what updates were applied.



1. Click **Save**.

Retention Notifications

The system administrator can enable or disable this feature to configure retention batch notification settings for designated retention administrators and additional recipient email addresses.

The list of *Retention Administrators*appears as their email addresses. As a system administrator, you can set these retention administrators to*active*or*inactive* state. When set to active, a retention administrator receives retention batch notifications at the listed email address. When set to inactive, the retention administrator does not receive notifications.

Administrators can also add additional recipient email addresses, including third-party addresses that are not associated with customer accounts. These additional recipients can also receive retention batch notifications.

Notification frequency is fixed to Daily and cannot be customized. A History section displays a chronological record of configuration changes for audit and tracking purposes.

More Information

Enabling or disabling retention notifications

Adding or excluding email addresses for retention notifications

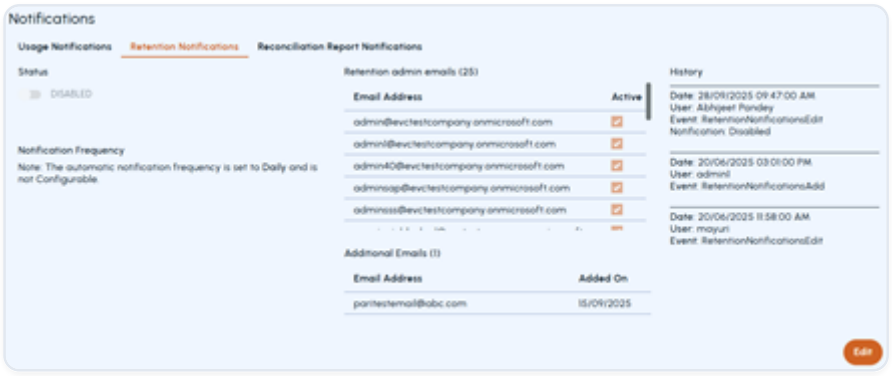
Viewing retention notification configuration history

Enabling or disabling retention notifications

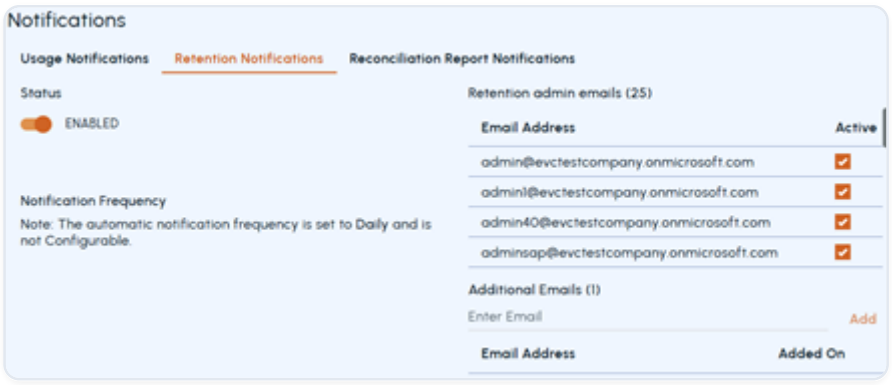
Only users with the *System Administrator* role can enable or disable retention batch notification setting.

To enable or disable retention batch notifications

1. In the left navigation pane, select **Reports and Notifications**>**Notifications**.
2. Select the **Retention Notifications**tab, and click**Edit**.



3. Under **Status** , slide the switch to the right to enable, or to the left to disable retention batch notification setting.



4. Click **Save**.

See Adding or excluding email addresses for retention notifications.

See Viewing retention notification configuration history.

Adding or excluding email addresses for retention notifications

System administrator email addresses are automatically included in the notification recipient list and can be activated or deactivated as needed. You can add up to 50 additional email addresses.

Retention administrators on the customer side can now enable retention notifications and manage recipient email addresses directly through the management console, eliminating the need for support team intervention.

To add or remove email addresses for retention notifications

1. In the left navigation pane, select **Reports and Notifications**>**Notifications**.
2. Select the **Retention Notifications**tab, and click**Edit**.
3. Under **Retention Admin Emails** , the system automatically populates the email addresses of all existing administrators and users assigned retention-related roles.

To prevent a specific address from receiving notifications, clear the **Active** check box for that entry.

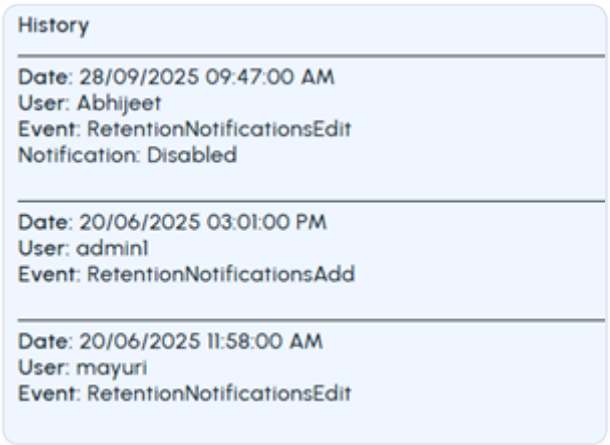
1. To add recipients who are not assigned retention roles, enter their email addresses under **Additional Emails**and click**Add**. These addresses can include external or third-party addresses that are not associated with customer accounts.
2. Click **Save**.

See Enabling or disabling retention notifications.

See Viewing retention notification configuration history.

Viewing retention notification configuration history

The History section displays a chronological record of configuration changes to the retention notification settings for audit and tracking purposes. Each entry logs the date and time, user, event type, notification status (enabled or disabled), selected notification frequency, and any added or removed email addresses. Refer to the sample screen shot below:



This audit trail helps administrators track who made changes, when the changes occurred, and what specific updates were applied to the retention notification configuration.

Reconciliation Report Notifications

System administrator can enable or disable this feature to control user access to the Message reconciliation report tab on the *Archiving Scorecard*page under*Reports and Notifications > Reports*.

Only users for whom this feature is enabled can generate, view, and download reconciliation reports. The message reconciliation report provides users with a real-time insight into message flow and reconciliation metrics, enhancing their operational control and efficiency through direct data access.

Users for whom this feature is disabled cannot access or use reconciliation reports.

Notification frequency is fixed to Daily and cannot be customized. Reports are retained for 30 days to serve as a short-term historical reference.

More Information

Enabling or disabling reconciliation report notifications

Adding or removing email addresses for reconciliation report notifications

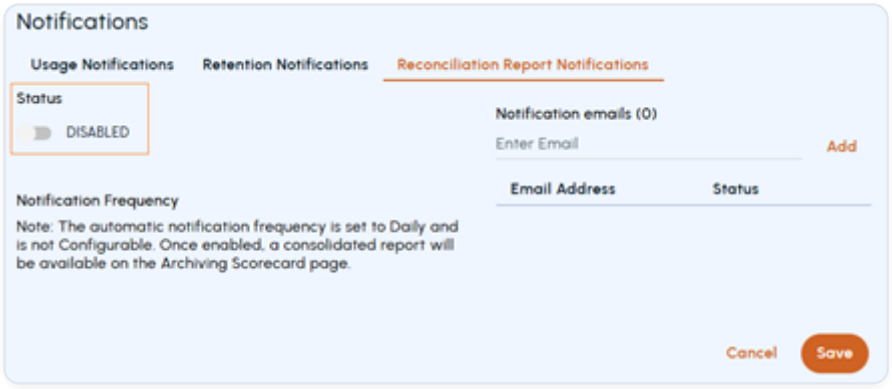
Enabling or disabling reconciliation report notifications

Only users with the *System Administrator* role can enable or disable reconciliation report notifications setting.

To enable or disable reconciliation report notifications

1. In the left navigation pane, select **Reports and Notifications**>**Notifications**.
2. Select the **Reconciliation Report Notifications**tab, and click**Edit**.

3. Under **Status** , slide the switch to the right to enable, or to the left to disable the setting.



4. Click **Save**.

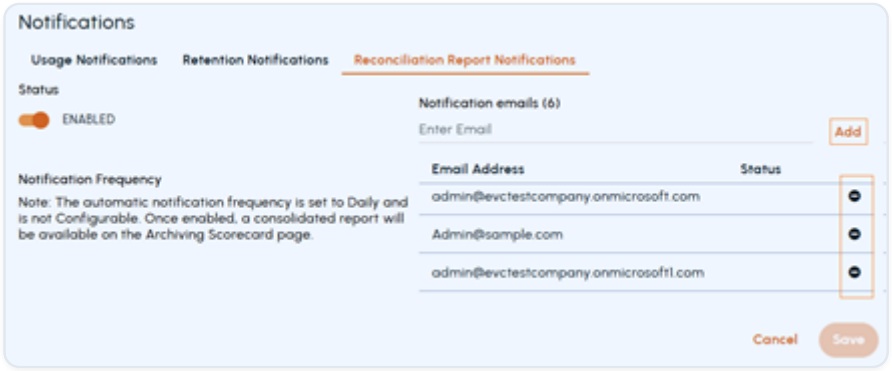
See Adding or excluding email addresses for retention notifications.

Adding or removing email addresses for reconciliation report notifications

Administrators on the customer side can now enable reconciliation report notifications and manage recipient email addresses directly through the management console, eliminating the need for support team intervention.

To add or remove email addresses for reconciliation report notifications

1. In the left navigation pane, select **Reports and Notifications**>**Notifications**.
2. Select the **Reconciliation Report Notifications**tab, and click**Edit**.
3. Under **Notification emails** , do the following as needed:



   - To add an address, enter the email address and click **Add**.
   - To remove an email address, select the email address and click the **Remove** icon in the corresponding row.

4. Click **Save**.

More Information

Enabling or disabling reconciliation report notifications

Capture Notifications

The Capture Notifications tab allows system administrators to configure the Insight Capture-specific notification preferences and view related event notifications in the Management Console.

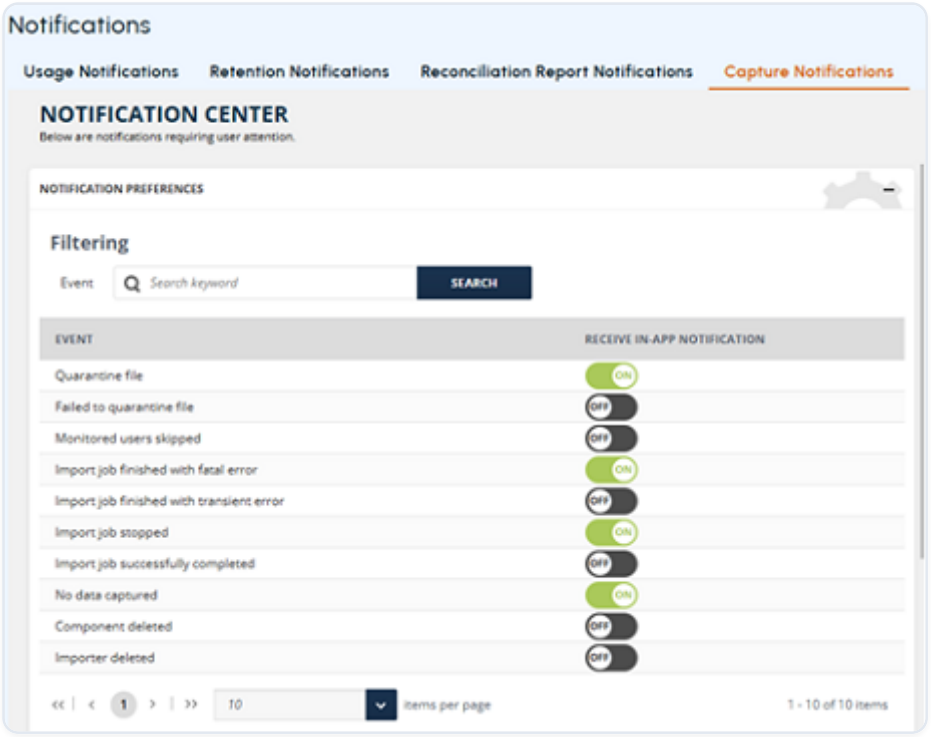
This tab is available under Reports > Notifications only if any of the following services is enabled:

- Capture Primary Service
- OneDrive for Business
- Microsoft Teams Secondary Service

To view the Insight Capture-specific notifications

1. In the left navigation pane, select **Reports and Notifications**>**Notifications**, and access the**Capture Notifications** tab.
2. Configure the notification preferences.

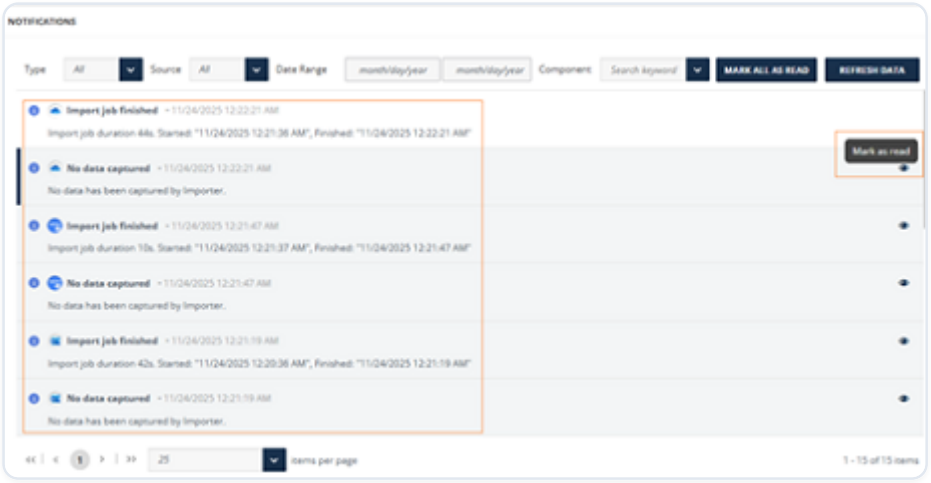
On the NOTIFICATION CENTER page, expand the NOTIFICATION PREFERENCES section by clicking the plus (+) icon or the section header. The list of available events is displayed.



1. To find a specific event, use the navigation arrows to move between pages, or enter a keyword in the **Event**field and click**Search**.
2. For the searched event, use the *Receive In-App Notification* toggle. Turn ***ON***to enable notifications for the event, turn***OFF*** to disable it. Repeat the steps to configure notification preferences for additional events as and when needed.

3. After enabling the required events, scroll down to view the **NOTIFICATIONS** section.

The system displays notifications based on the configured event preferences as shown in the sample image below.



- Click **Refresh Data** to load the latest notifications.
- If the list is extensive, use the available filters to refine the results. You can sort notifications by **Status**(Read, Unread, Failure, Warning, Info, Success),**Source**(System, Importer),**Component**, or**time period**. Use navigation arrows to move between the pages.
- To mark all displayed notifications as read, click **MARK ALL AS READ**. To mark individual notification as read, click the eye icon next to a notification.

Insight Capture

The Insight Capture node is visible under the *Reports and Notifications* node only if:

- your user account is enabled for the Insight Capture services.
- your role is Archive Administrator or System Administrator.

For more information, See Generating Insight Capture-specific reports.

Generating Insight Capture-specific reports

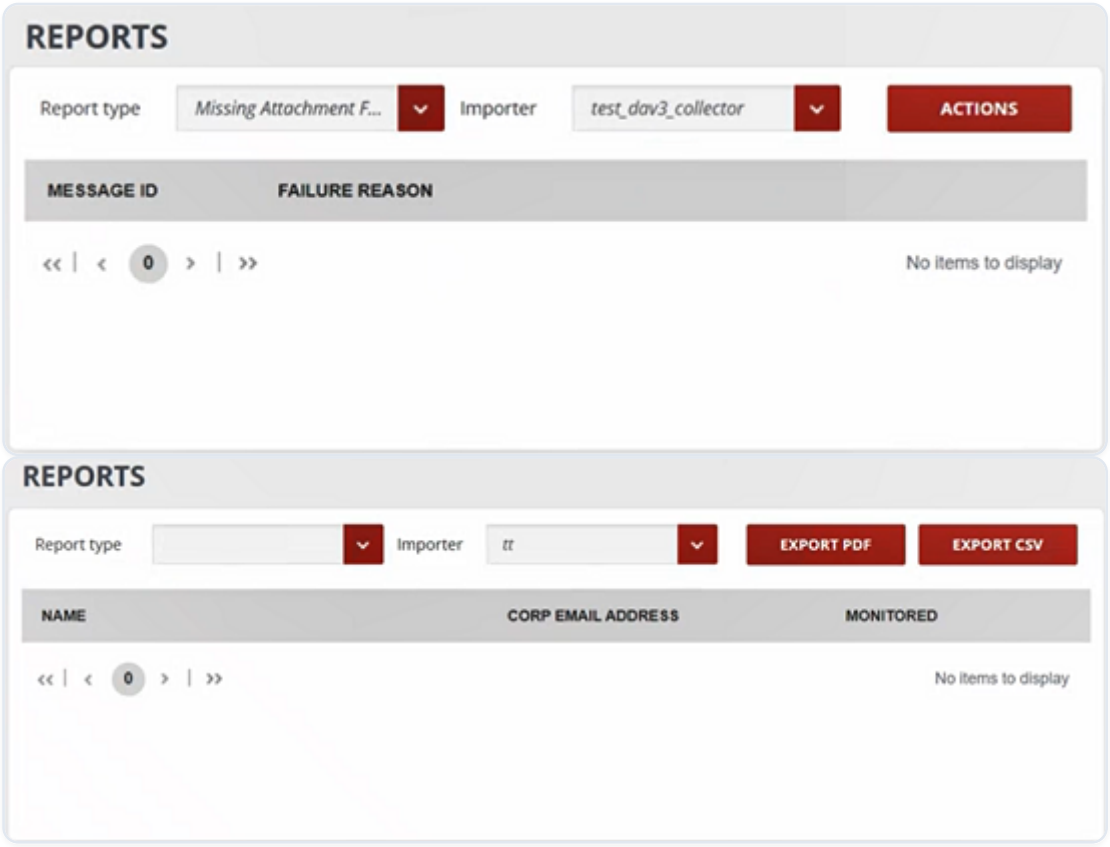
To generate Insight Capture-specific reports from the Arctera Insight Management Console

1. In the left navigation pane, select **Reports and Notifications**>**Insight Capture**.

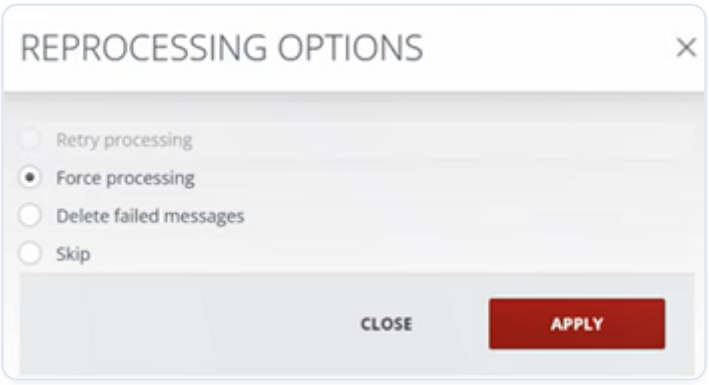
The Management Console opens the **REPORTS** page interface of the Insight Capture application in the same window.

1. Specify the **Report type**.

The **REPORTS**interface varies with the selected reports. For example, in the image below the**ACTIONS**button is available, while in the next interface, the**EXPORT PDF**and**EXPORT CSV** buttons are available.



1. Select the **Importer** for which you want to generate a report.
2. Click **ACTIONS**. On the**REPROCESSING OPTIONS**window, select the skip, delete, or force processing option as needed, and click**APPLY**.



Or, click **EXPORT PDF/EXPORT CSV** to export a report as PDF or CSV.

For more information about the Insight Capture reports, see Arctera Insight Capture Configuration Guide.

Classification

This section includes the following topics:

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 Arctera Insight Classification service enabled, the service can apply classification tags to Arctera Insight Archiving's incoming emails that match the enabled policies in the Arctera Insight Classification. Insight eDiscovery users can then search for the emails that are tagged with the classification tags, during investigations and Insight eDiscovery.

Administrators with the classification administrator role can access the Arctera Insight Classification from Arctera Insight 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 Arctera Insight Archiving matches the criteria for the policy, the associated PII classification tag is assigned in the email header. Insight 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, refer to Arctera Insight Classification online help.

For information on working with the emails that contain classification tags, refer to the Insight eDiscovery User Guide.

Which emails get classified?

If your company has the Arctera Insight Classification service enabled, the service can apply classification tags to Arctera Insight Archiving's incoming emails that match the enabled policies in the Arctera Insight Classification.

Once a policy is enabled in the Arctera Insight Classification, the classification process is performed for the new emails that Arctera Insight Archiving ingests. Note that:

- The classification tags that are associated with a policy get applied only to matching emails that are ingested into Arctera Insight 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 Arctera Insight 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 Arctera Insight Archiving.

  > “ ”

  Note: Classification tags are only assigned through the Arctera Insight Classification. Unlike other types of tag, you cannot assign or remove classification tags manually.

  > “ ”

Steps for setting up classification

Table: Process for setting up classification provides the steps for setting up classification of emails that are ingested into Arctera Insight Archiving, using the Arctera Insight Classification.

Table: Process for setting up classification

STEP	DESCRIPTION	FURTHER INFORMATION
Step 1	Ensure that the Arctera Insight Classification service is enabled for your company in Arctera Insight Archiving.	To enable your organization for classification, contact Arctera Services & Support .
Step 2	Set up the required account access to the Arctera Insight Classification.	Assign the classification administrator role to the required accounts.
		See About Role Management .
Step 3	Access the Arctera Insight Classification.	You can access the Arctera Insight Classification directly from Arctera Insight Management Console.
		See Accessing the Arctera Insight Classification .
Step 4	Decide on the classification policies you require, and enable those policies.	See the Arctera Insight Classification help.
	You can create custom policies if required.	See Arctera Insight Archiving item properties for use in custom classification policies .

Accessing the Arctera Insight Classification

You must possess the Classification Administrator role if you want to access Arctera Insight Classification from Arctera Insight Management Console .

To access the Arctera Insight Classification

1. In the left navigation pane, click **Classification**.

The **Policies** page of the Arctera Insight Classification application appears. The first classification policy in the list is selected by default.

> “ ”

Note: If you click theClassificationnode again while the Arctera Insight Classification tab is open, the Arctera Insight Classification user interface gets refreshed.

> “ ”

1. Clear the check box of the first policy
2. Search for and select the policies that you want to enable.

For more information about enabling classification policies, refer to Arctera Insight Classification online help.

Arctera Insight Archiving item properties for use in custom classification policies

When Arctera Insight 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. Arctera Insight Archiving passes this subset of properties and their associated values to the Arctera Insight Classification for use in classification. When you create a custom Arctera Insight 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: Item properties passed to the Arctera Insight Classification lists the item properties that Arctera Insight Archiving passes to the Arctera Insight Classification.

Table: Item properties passed to the Arctera Insight 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.
auea	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.

PROPERTY	TYPE	DESCRIPTION
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: Attachment properties passed to the Arctera Insight Classification lists the properties of message attachments that Arctera Insight Archiving passes to the Arctera Insight Classification.

Table: Attachment properties passed to the Arctera Insight 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.
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, refer to Arctera Insight Classification online help.

Managing Data Import

This section includes the following topics:

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 Arctera Insight Archiving Arctera Insight 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 Arctera 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. . SeeGenerating Messaging reports.

> “ ”

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 Arctera Insight Management Console .

To import data into archives

1. On the Arctera Insight Management Console , in the left navigation pane, click **Import Data**.

> “ ”

Note: You must launchImport Datafrom the Arctera Insight Management Console . Never use a direct URL ofImport 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.

1. 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.
2. Click **Import**.

The application displays the **Upload PST or ZIP(MSG/EML) file and import data** page.

1. 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 theDeleteicon in the corresponding row.

   > “ ”

2. 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.

1. In the **Journal Address** column, select an appropriate journal address for each item.
2. 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

1. 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.
2. Ensure that all the error messages for the selected messages are resolved. Else, the **Upload** button remains disabled.
3. 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.

1. 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.

STATUS	DESCRIPTION
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 Arctera Insight Management Console . SeeGenerating Messaging reports.

AD FS Configuration Guide

This section includes the following topics:

Configuring AD FS to work with Arctera Insight Archiving

Configuring AD FS to work with Arctera Insight Archiving

This section describes how to configure your Active Directory Federation Services (AD FS) environment to work with the Arctera Insight Archiving authentication service. After you configure your AD FS environment and the Arctera Insight Archiving authentication service, you can provide single sign-on access to Arctera Insight Personal Archive users.

For information about the supported AD FS versions, see the Arctera Insight Archiving Compatibility List.

> “ ”

Note: These instructions apply to the provision of single sign-on access for Insight Personal Archive users only. For assistance with the provision for Insight eDiscovery and Arctera Insight Management Console, contactArctera Services & Support.

> “ ”

The following table describes the required steps to configure AD FS to work with the Arctera Insight Archiving authentication service.

Table: Steps to configure AD FS to work with the Arctera Insight Archiving authentication service

ACTION	REFERENCE
Use the AD FS Management to add a relying party trust for Arctera Insight Archiving.	See Adding a relying party trust for Arctera Insight Archiving .
Generate and export a -signing certificate from the AD FS Management for upload in Arctera Insight Management Console.	See Generating a -signing certificate .

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

Arctera Insight 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 Arctera Insight 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. Arctera Insight 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.Arctera.com/docs/000097921

Adding a relying party trust for Arctera Insight Archiving

The first step to configure your AD FS environment is to add a relying party trust for Arctera Insight 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 Arctera Insight Archiving authentication service from working properly with your AD FS environment.

> “ ”

To add a relying party trust for Arctera Insight 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 Arctera Insight 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 Arctera Insight 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, contactArctera 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, selectI 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 -signing certificate

The second step to configure your AD FS environment is to generate a -signing certificate for upload on the Authentication Management page in Arctera Insight 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 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.1. In the left pane of the AD FS Management console, expandService**, and then select**Certificates**.

2. In the **Certificates** pane, select the certificate that is listed under the -signing section.
3. In the **Actions**pane, click**View Certificate**.
4. In the **Certificate**window, select the**Details**tab, and then click**Copy to File**.
5. In the **Welcome**panel of the Certificate Export Wizard, click**Next**.
6. In the **Export File Format**panel, select**Base-64 encoded X.509 (.CER)**, and then click**Next**.
7. In the **File to Export**panel, enter a file path in the**File Name**field, and then click**Next**.
8. In the **Completion**panel, review the specified information, and then click**Finish**.
9. Click **OK** to close the export confirmation dialog box. You can find the exported certificate in the file location you previously designated.