Arctera™ Capture Configuration Guide - v1.0

Overview

Capture aids financial service firms in complying with SEC rule 17-a4, CFTC rule 1.31, Dodd-Frank requirements, FINRA and other regulatory agencies. It also greatly reduces legal risks by streamlining the discovery of e-communications data, aiding organizations across all verticals with internal investigations, lawsuits, and audits.

Collectors can be used for targeted discovery within limited time frames using the Do not download data modified before and Do not download data modified after windows, provided the data exists at source. This should be done by creating a second copy of the original steady-state importer and using that for targeted runs.

> **Note:** Capture collectors are designed to be deployed for scheduled ongoing capture runs. Even though collectors can be run against older data for targeted discovery purposes, using the collectors to migrate large amounts of data is not supported. The Capture platform is not built as a migration tool designed to run long term migration tasks with accompanying monitoring/reconciliation/reporting features that are required for such a tool. Running tasks for long periods of time brings the risk of failure to complete successfully.

INTRODUCTION

This section includes the following topics:

Overview

Capture aids financial service firms in complying with SEC rule 17-a4, CFTC rule 1.31, Dodd-Frank requirements, FINRA and other regulatory agencies. It also greatly reduces legal risks by streamlining the discovery of e-communications data, aiding organizations across all verticals with internal investigations, lawsuits, and audits.

Collectors can be used for targeted discovery within limited time frames using the **Do not download data modified before** and **Do not download data modified after** windows, provided the data exists at source. This should be done by creating a second copy of the original steady-state importer and using that for targeted runs.

> **Note:** Capture collectors are designed to be deployed for scheduled ongoing capture runs. Even though collectors can be run against older data for targeted discovery purposes, using the collectors to migrate large amounts of data is not supported. The Capture platform is not built as a migration tool designed to run long term migration tasks with accompanying monitoring/reconciliation/reporting features that are required for such a tool. Running tasks for long periods of time brings the risk of failure to complete successfully.

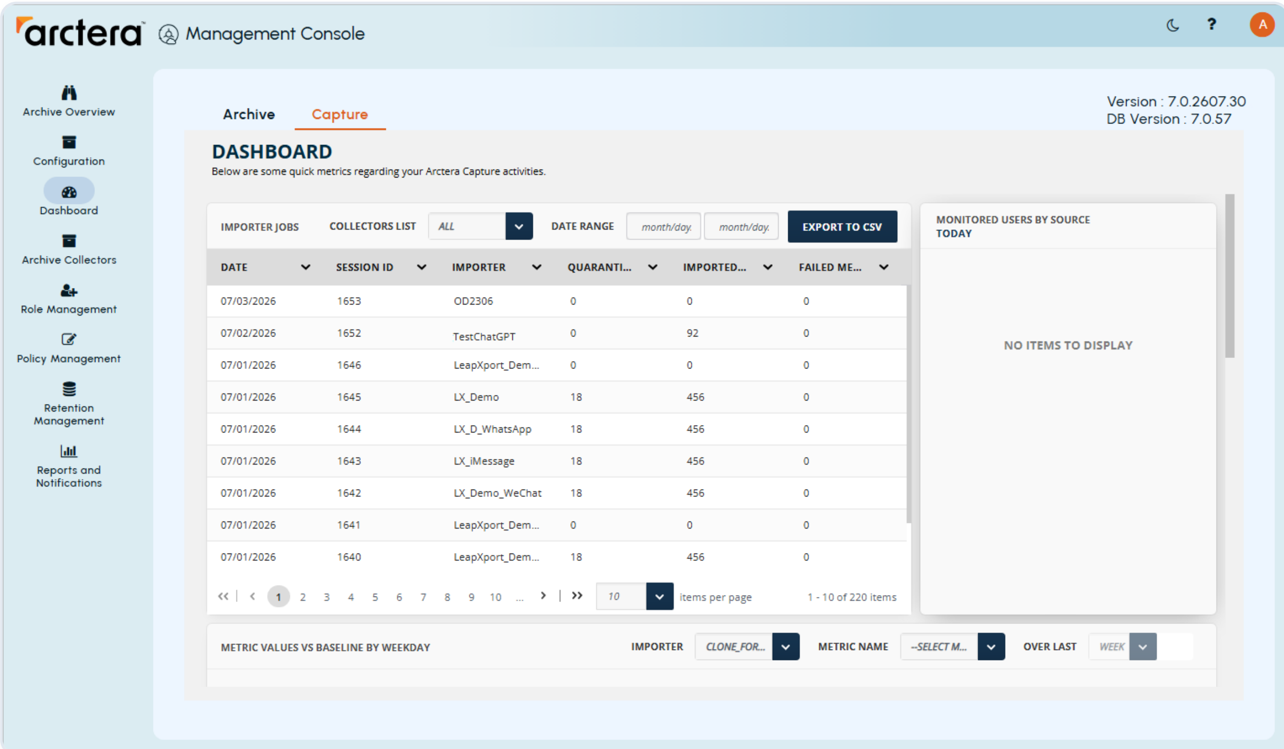
DASHBOARD

This section includes the following topics:

- Overview
- Importer Jobs

Overview

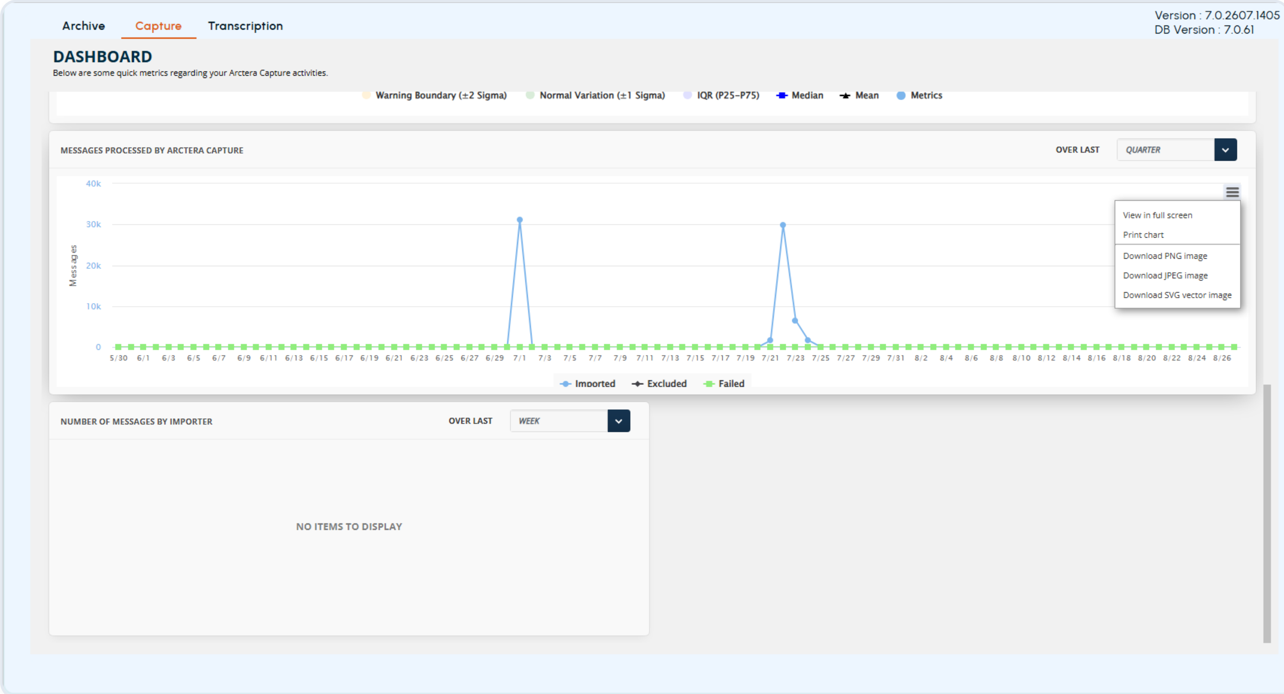
The **Dashboard** provides interactive visual modules that represent statistical and logical information about your activities.



Dashboard consists of the following screens:

- **Importer Jobs**
- **Monitored Users by Source**
- **Metric Values vs Baseline by Weekday**
- **Messages Processed by Arctera Capture**
- **Number of Messages by Importer**

You can view the details of each job, user, or messages by hovering the mouse over the job you want, and you will see the details of it.



You can download the information included in the **Messages Processed by Arctera Capture** and **Number of Messages by Importer** in **JPG**, **PNG** or **SVG** formats. A pop-up list of available formats opens.

Select the format and the dashboard of the messages or the number of messages by importers will be downloaded to your local PC.

Importer Jobs

The paragraphs that follow will describe how you can browse and set the number of entries per page in the importer jobs.

This dashboard is comprised of the following components:

- **Date**
- **Session ID**
- **Importer**
- **Quarantined sources**
- **Failed messages**
- **Imported messages**
- **Reprocessed session**

- **Duration**

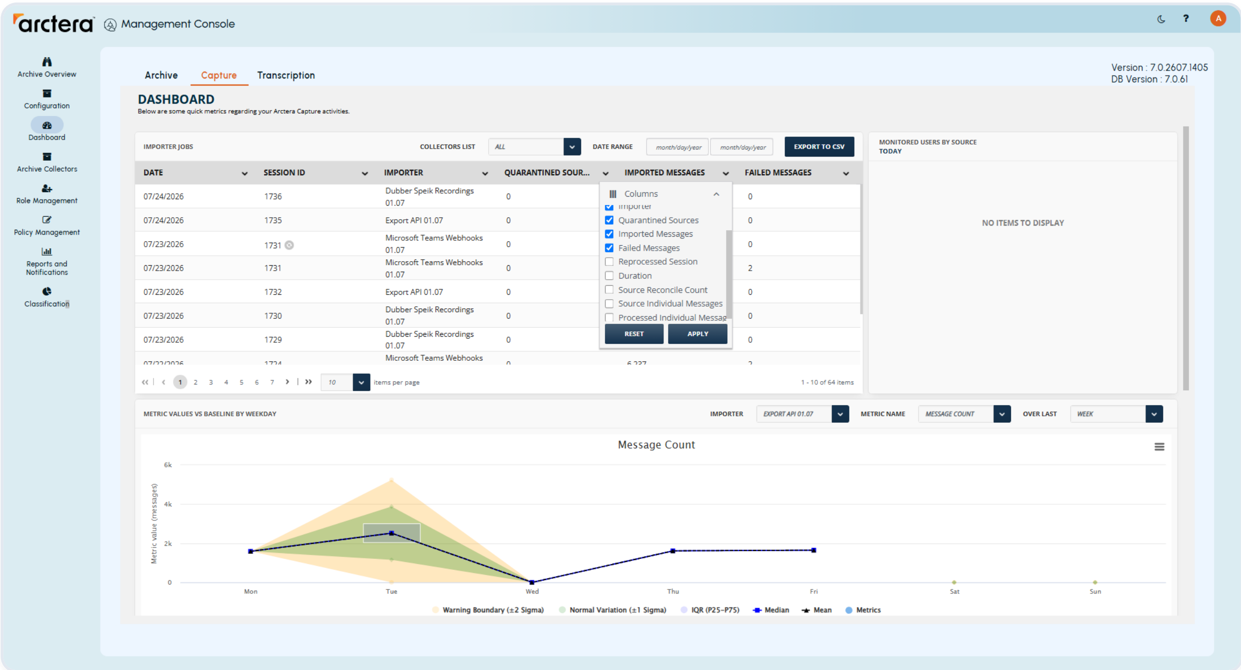
> **Note:** The importer's duration will not be displayed if the job is interrupted or stopped before completion.

> **Note:** You can drag and re-arrange their order in the User interface.

Exporting to CSV

This section allows the user to export the dashboard for:

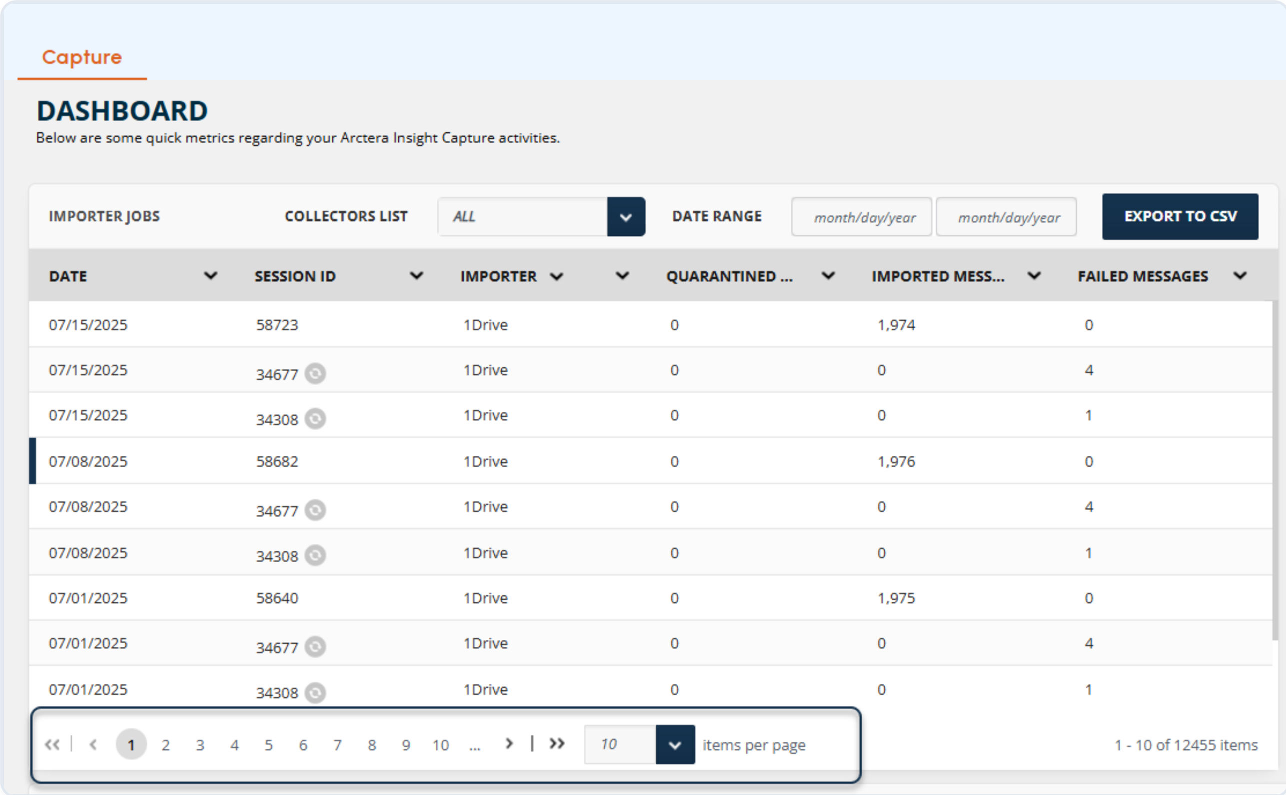
- The specified importer by selecting the collector from the **Collectors list** drop-down list
- The specified date range by selecting **FROM** and **TO** dates from the calendar



Browsing Importer Jobs & Setting the Number of Entries per Page

This sub-section is enhanced with the pagination option. This means that it is enabled with the possibility of splitting the list of records in the sub-section into pages for paged navigation.

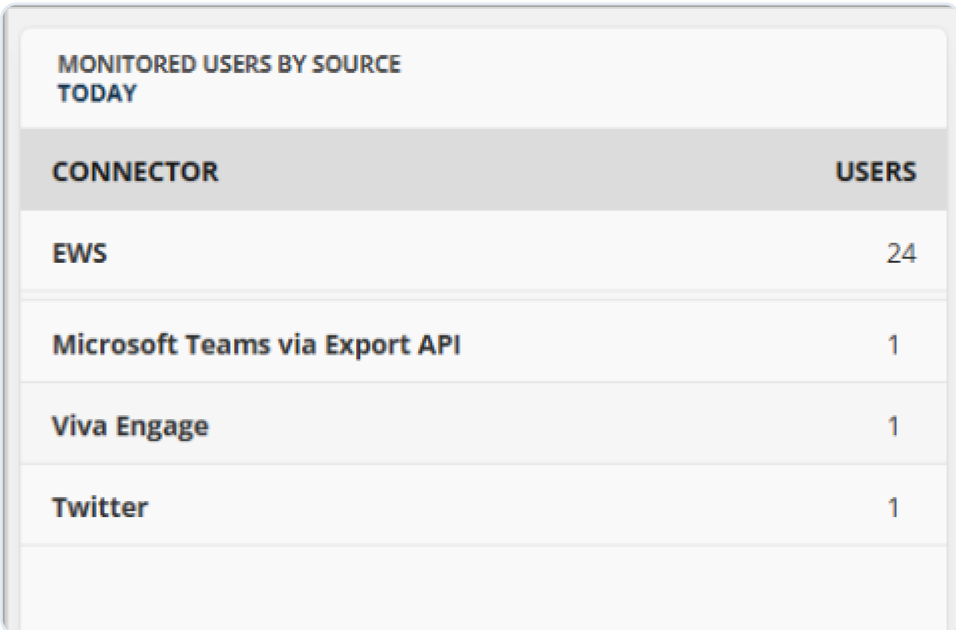
By default, each sub-section is set to display twenty entries per page to ensure fast page loading. However, you can define to view a lower/greater number of entries per page.



DATE	SESSION ID	IMPORTER	QUARANTINED ...	IMPORTED MESS...	FAILED MESSAGES
07/15/2025	58723	1Drive	0	1,974	0
07/15/2025	34677	1Drive	0	0	4
07/15/2025	34308	1Drive	0	0	1
07/08/2025	58682	1Drive	0	1,976	0
07/08/2025	34677	1Drive	0	0	4
07/08/2025	34308	1Drive	0	0	1
07/01/2025	58640	1Drive	0	1,975	0
07/01/2025	34677	1Drive	0	0	4
07/01/2025	34308	1Drive	0	0	1

Monitored Users by Source

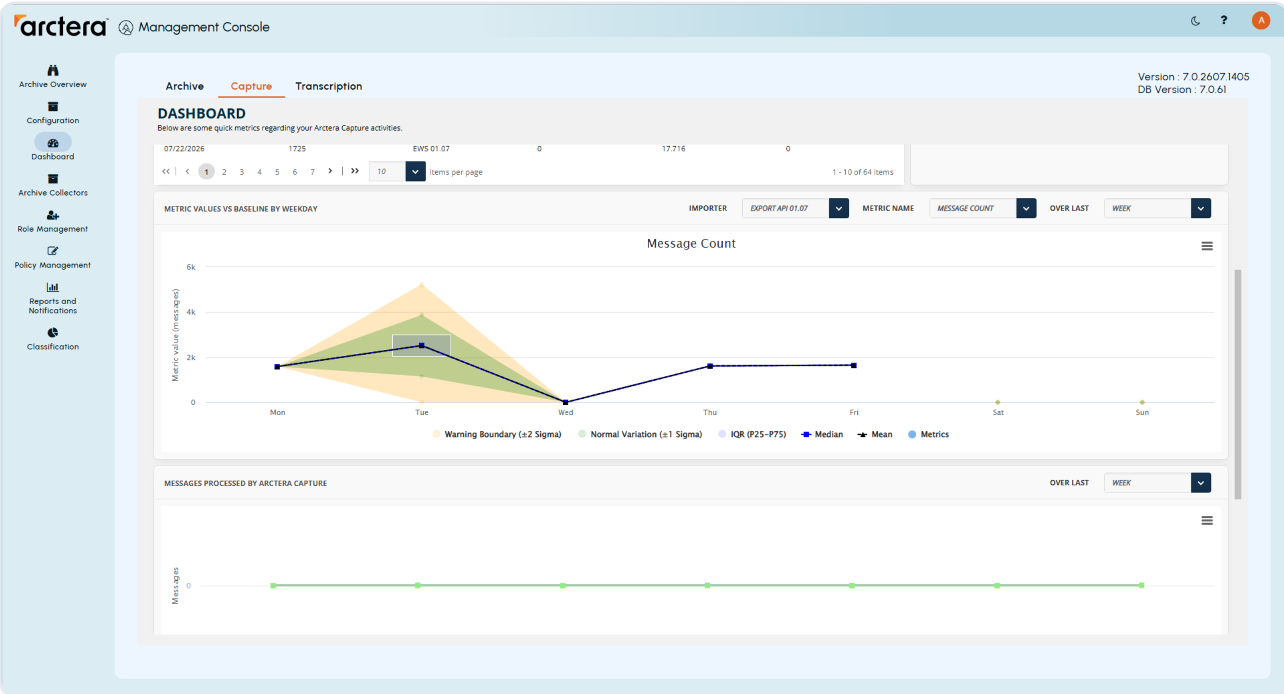
The **Monitored Users by Source** widget displays the number of monitored users per source for the current day.



CONNECTOR	USERS
EWS	24
Microsoft Teams via Export API	1
Viva Engage	1
Twitter	1

Metric Values vs Baseline by Weekday

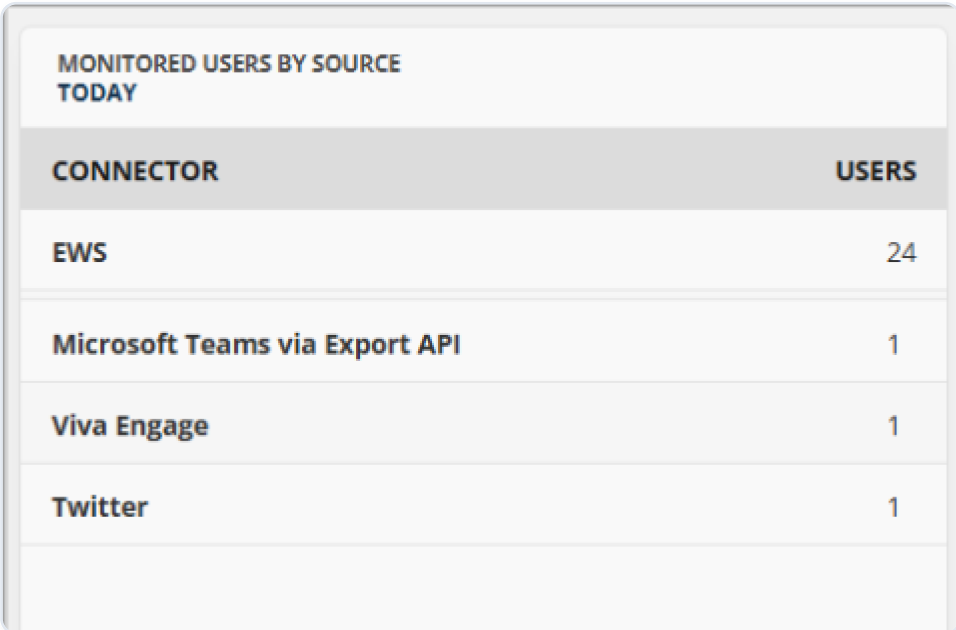
The **Metric Values vs Baseline by Weekday** widget provides a comparative analysis of importer performance metrics against historical averages.



The widget provides the following tools to customize and manage performance analysis:

- **Importer**: Select a specific importer to isolate data for an individual source.
- **Metric Name**: Choose the specific data point to visualize:
    - Message count
    - Delivered messages at target
    - Monitored users
    - Run duration
    - Delivery time (mean) at target
    - Message insert time (mean)
- **Over Last (period)**: Define the historical look-back period used to calculate the performance baseline. The available options are Last week, 2 weeks, 30 days, or Quarter.
- **Viewing and Exporting Reports**: Use the *menu* button to view the widget in full screen, print it, or download the data to your local PC in **PNG**, **JPEG**, or **SVG** format.

> **Note:** The PDF export format is unavailable for the **Metric Values vs Baseline by Weekday** widget.



MONITORED USERS BY SOURCE
TODAY

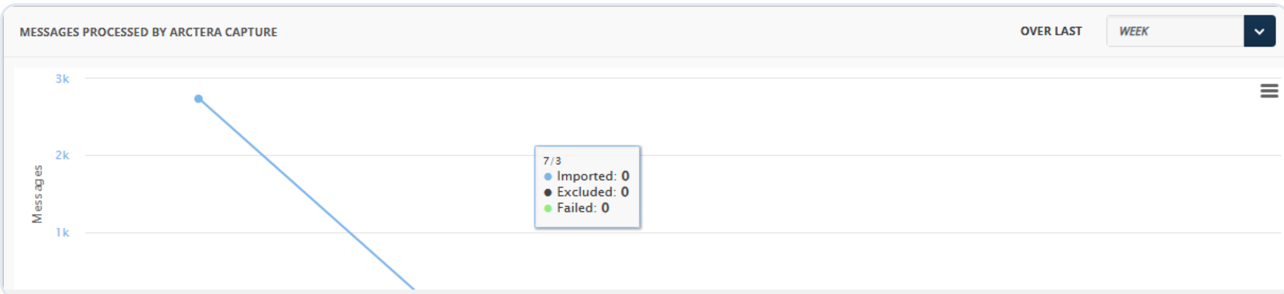
CONNECTOR	USERS
EWS	24
Microsoft Teams via Export API	1
Viva Engage	1
Twitter	1

Messages Processed by Arctera Capture

The **Messages Processed by Arctera Capture** widget provides an overview of the number of messages that were successfully imported, excluded, or failed during processing.

The widget provides the following tools to manage your data view and reporting:

- **Over Last (period)**: See Timeframe Filtering.
- **Viewing and Exporting Reports**: See Viewing and Exporting Reports.



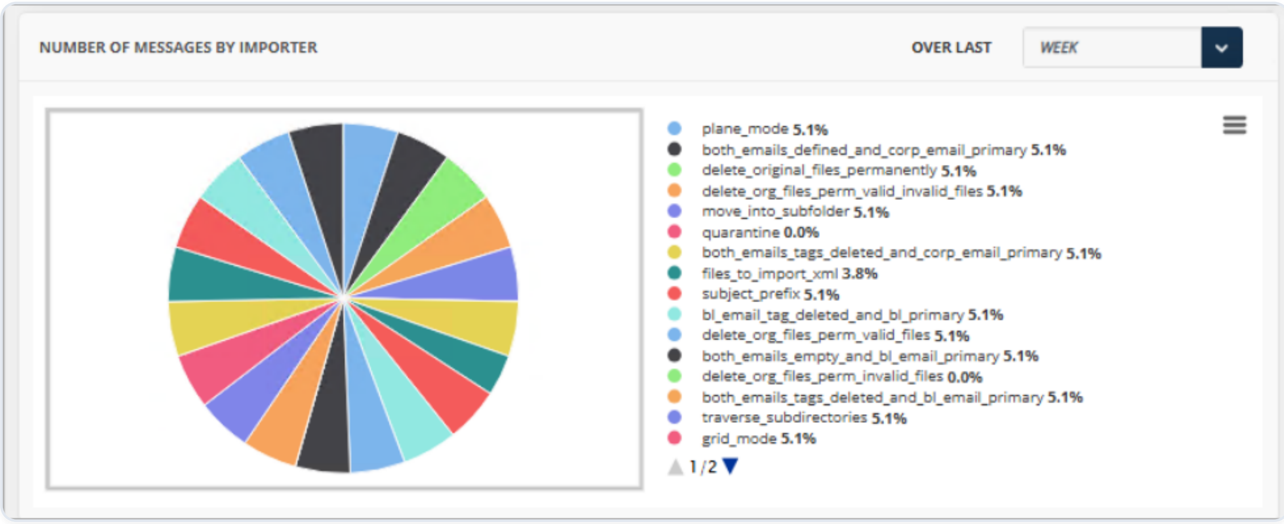
Number of Messages by Importer

The **Number of Messages by Importer** diagram visually represents the distribution of processed messages across different importers.

The widget provides the following tools to manage your data view and reporting:

- **Over Last (period)**: See Timeframe Filtering.

- **Viewing and Exporting Reports**: See Viewing and Exporting Reports.

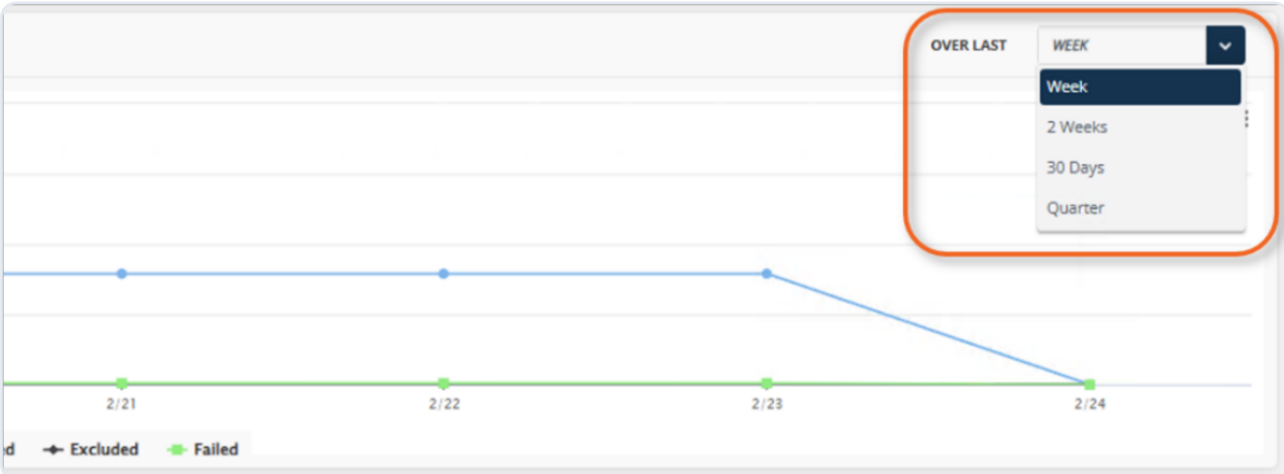


Timeframe Filtering

The **Over Last** drop-down allows you to define the historical look-back period for the data and baselines.

Available Options: Last week, 2 weeks, 30 days, or Quarter.

Function: Adjusting this setting updates the widget to reflect trends and message totals within the selected timeframe. For the **Metric Values vs Baseline by Weekday** widget, this specifically sets the window used to calculate the performance baseline.



Viewing and Exporting Reports

Widgets featuring the *menu* button provide options for detailed viewing and data extraction:

- **Full Screen**: Expand the widget for a more detailed view.

- **Print**: Send the current widget view directly to a printer.
- **Download/Export**: Save the dashboard data to your local PC in the following formats: **PNG**, **JPEG**, or **SVG**.

IMPORTERS

This section includes the following topics:

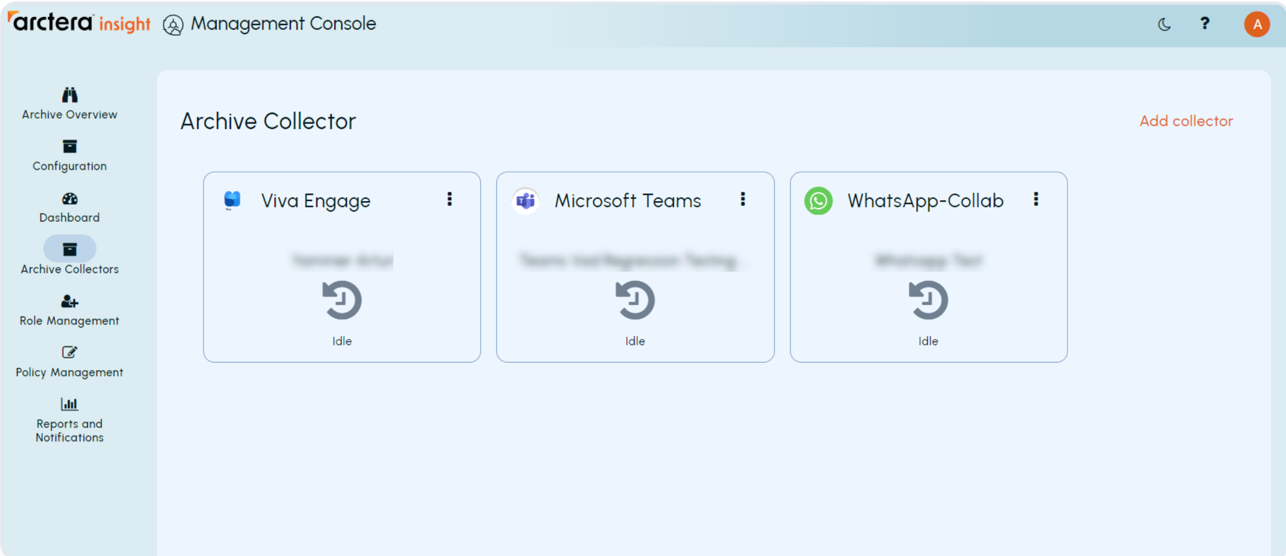
- Adding a New Importer
- Managing an Importer
- File-Based Collector Options
- Amazon S3
- Audio Video
- BlackBerry
- Bloomberg
- Box
- CellTrust
- ChatGPT
- Chatter
- Chatter Cipher Cloud
- Cisco Webex Teams
- Cloud9
- Copilot
- Dropbox Business
- Dubber Speik Recordings
- Dubber Speik SMS
- EML
- EWS
- Exchange Graph API
- FX Connect
- Google Drive
- Google Messages
- IceChat

- iMessage
- JSON
- LeapXpert
- LSEG (Refinitiv)
- LSEG Messenger
- Microsoft Teams
- Microsoft Teams for Audio and Video
- NTR-X
- OneDrive for Business
- Pivot
- Progress ShareFile
- Redtail Speak
- RingCentral
- ServiceNow
- SharePoint
- Slack eDiscovery
- Symphony
- Text-Delimited
- UBS
- Verba
- Verint
- Viva Engage (Yammer)
- Web Page Capture
- WhatsApp
- Workplace from Facebook
- X (Twitter)
- XIP
- XSLT/XML
- Yieldbroker
- YouTube

- Zoom Chat
- Zoom Meetings
- Zoom Meetings Chats
- Zoom Meetings via Archiving API
- Zoom Phone

Adding a New Importer

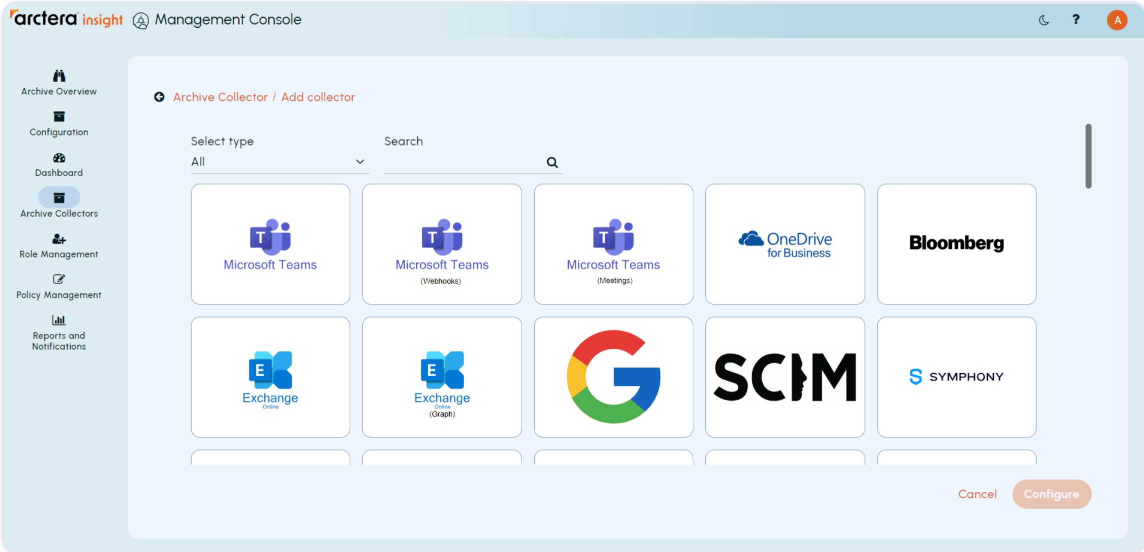
You will see a blank page or the list of already configured collectors.



To add a new importer:

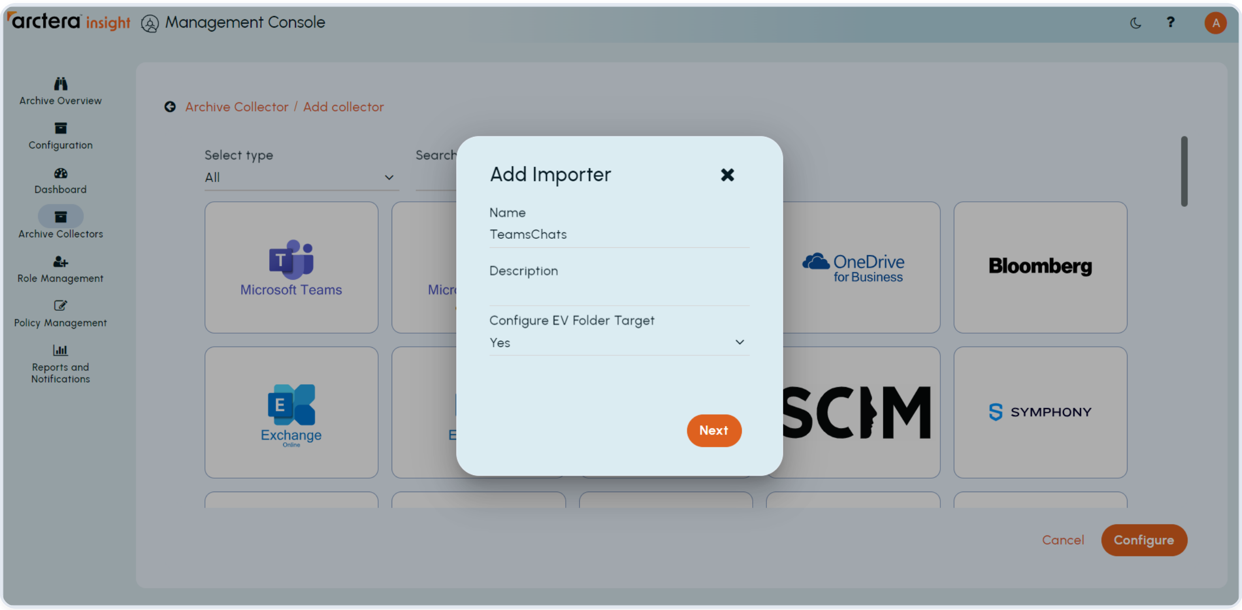
1. Click the **Add collector** button on the top right corner. A configuration wizard of adding a new importer will appear.
2. Select your source and click **Configure**. Here you can make use of:
   - Filtering option - select one of the following source types from the drop-down list above the sources:
     - AI Chatbots
     - Collaboration
     - Enterprise tools
     - File sharing
     - Financial platforms
     - Mobile and text
     - Voice

- Others



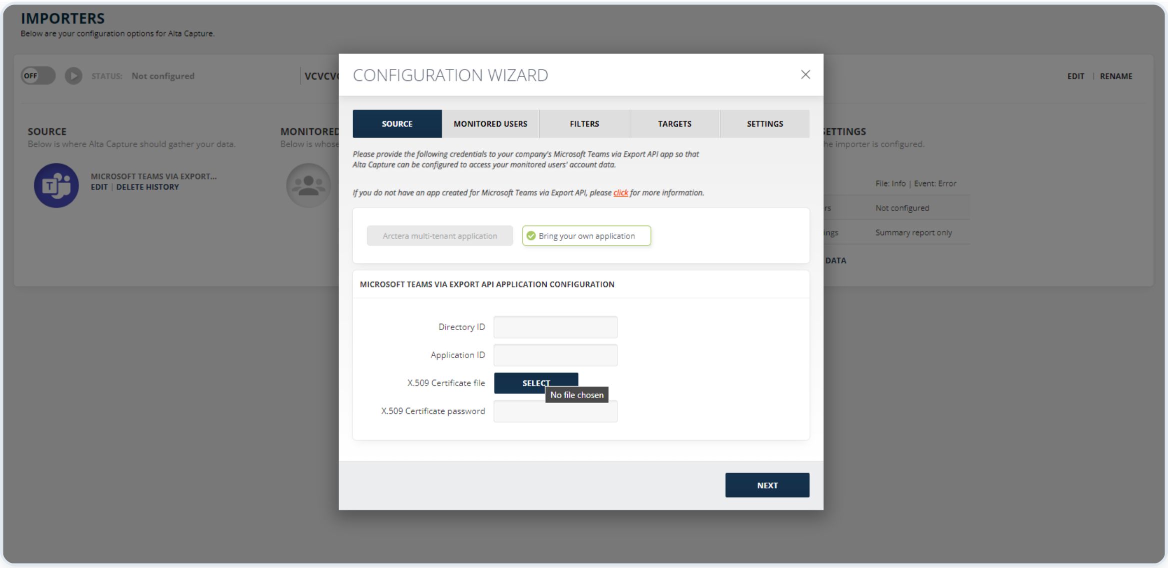
- Searching option - type the name of the source in the search box located above the sources

3. Fill in the **Name** and the **Description** fields, choose whether you want to deliver the collected data to EV folder target, and click **NEXT**.



4. Make the necessary changes.

> **Note:** From collector to collector the **Source** tab may vary.



When integrating an Importer, the **Importer Panel** is added to the **Configuration Screen**. Each **Importer Panel** consists of five main tabs:

- **Source** - here you can find general information about the importer and edit it.
- **Monitored Users** - here you can find information about all the users of the collector monitors, and its configurations.
- **Filters** - here you can set up what information is sent to the target.

> **Note:** Filters are not applicable to the EV folder target.

- **Targets** - here you can set up where the collector information is sent to.
- **Settings** - here you can change all the importer configurations.

> **Note:** It is necessary to configure all the tabs of the **Configuration Wizard** and **SAVE** the settings. When saved, you'll be redirected to the archive collectors list.

Managing an Importer

The options for managing the importers are:

- **Manage** - allows editing the settings of the collector.
- **Delete** - deletes the importer.
- **Stop** - stops the importer.
- **Run Now** - changes the importer status from stopped/idle to running.

- **Refresh** - refreshes the importer.
- **Clone** - allows copying the importer with all the previously configured settings.
- **Rename** - allows changing the name and the description of the importer.
- **Delete Collector Data** - deletes the data associated with the selected importer.

File-Based Collector Options

This section describes how file-based collectors are generally configured.

File Source Configuration

There are the following options to configure the source:

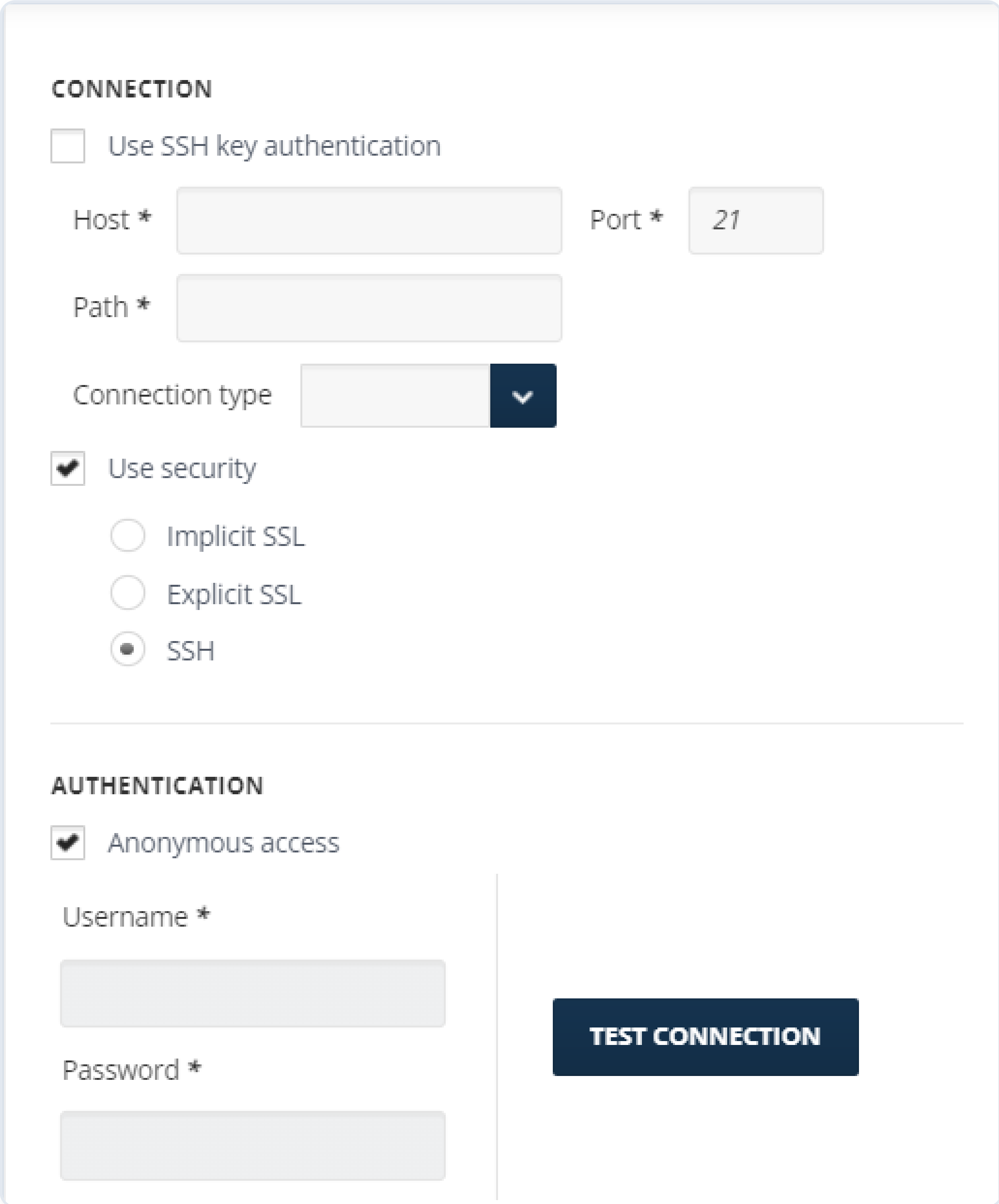
- **SFTP/FTP**
- **Amazon S3**
- **Azure Storage**

> **Note:** It is possible to configure the volume and size limits of the downloaded files. For further guidance, reach out toArctera Support.

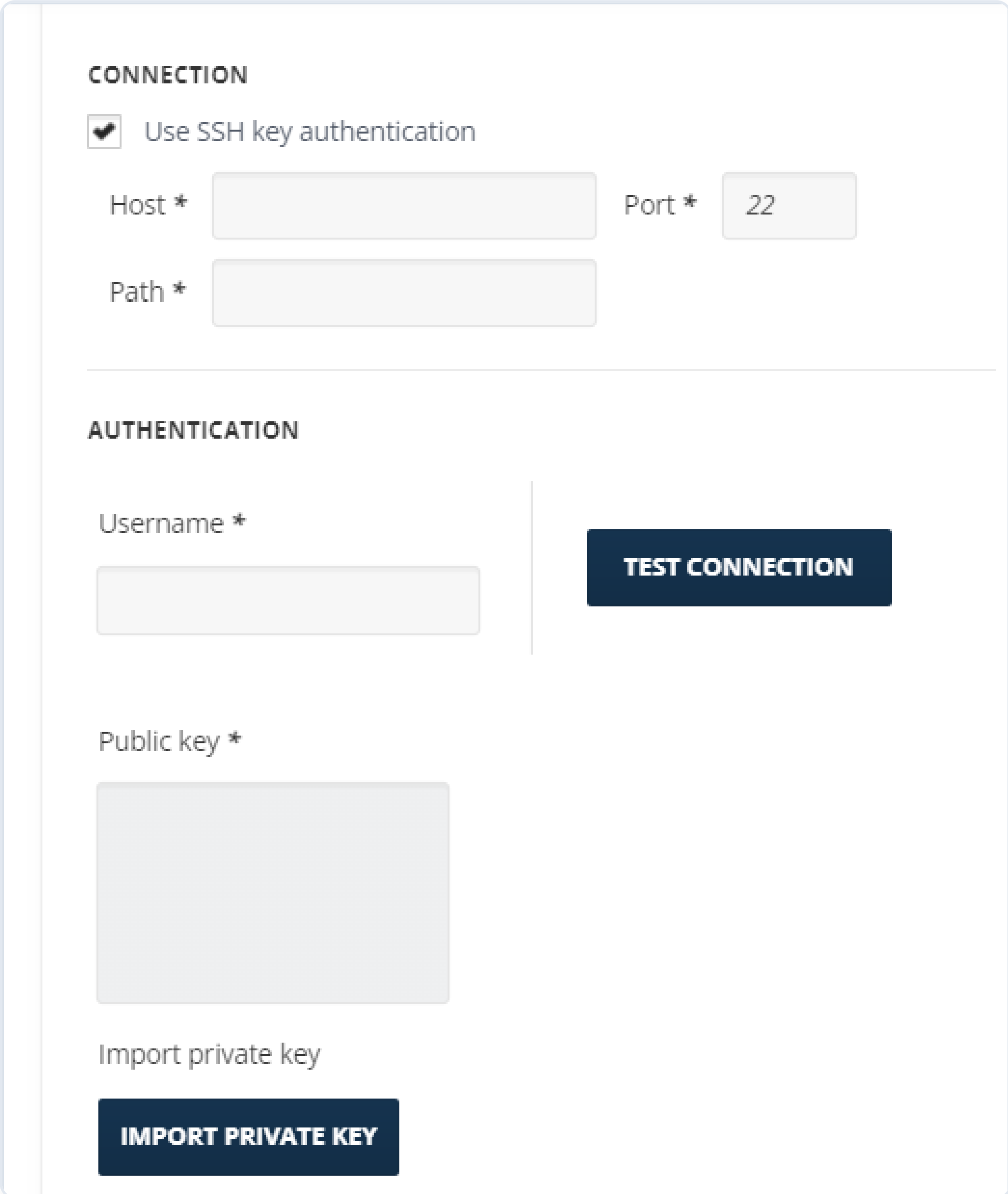
In case **SFTP/FTP** configurations is selected:

For Connection:

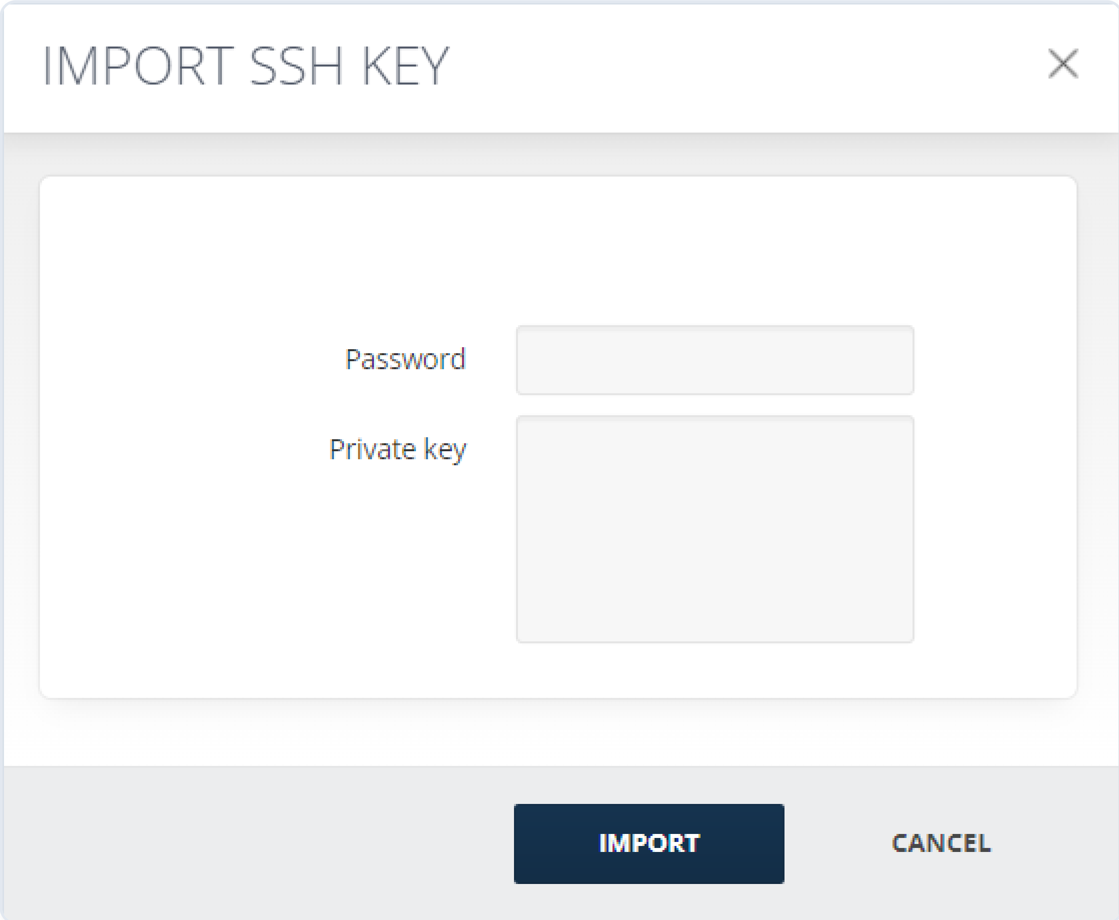
1. Enter the hostname of the remote FTP server and the folder path provided by the source in the **Host** and **Path** fields, respectively. The default ports used for SSH key Authentication by Bloomberg, IceChat, and Redtail Speak collectors is 22. The default FTP port for any Source is 21.



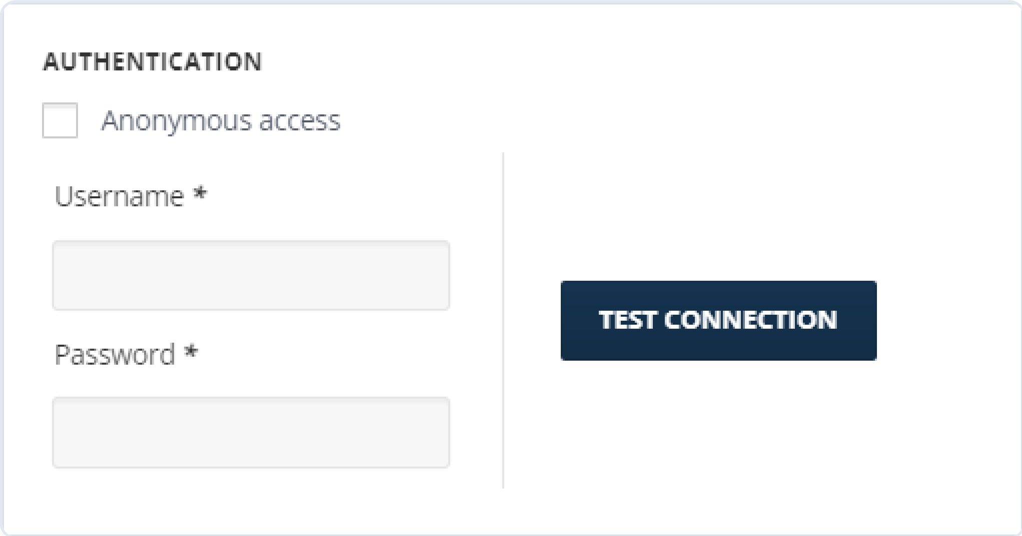
2. Make sure the connection settings match those of the SFTP server. Enter the **Path** to the required folder.
3. Enable **Use SSH Key Authentication** to open the configuration window. SSH Key Authentication is used for connecting to the source SFTP server.
4. For Authentication, enter the **Username** provided by the source.



5. Click the **Import Private Key** button and **Import SSH Key** will open.
6. Copy and paste the **Private Key**.

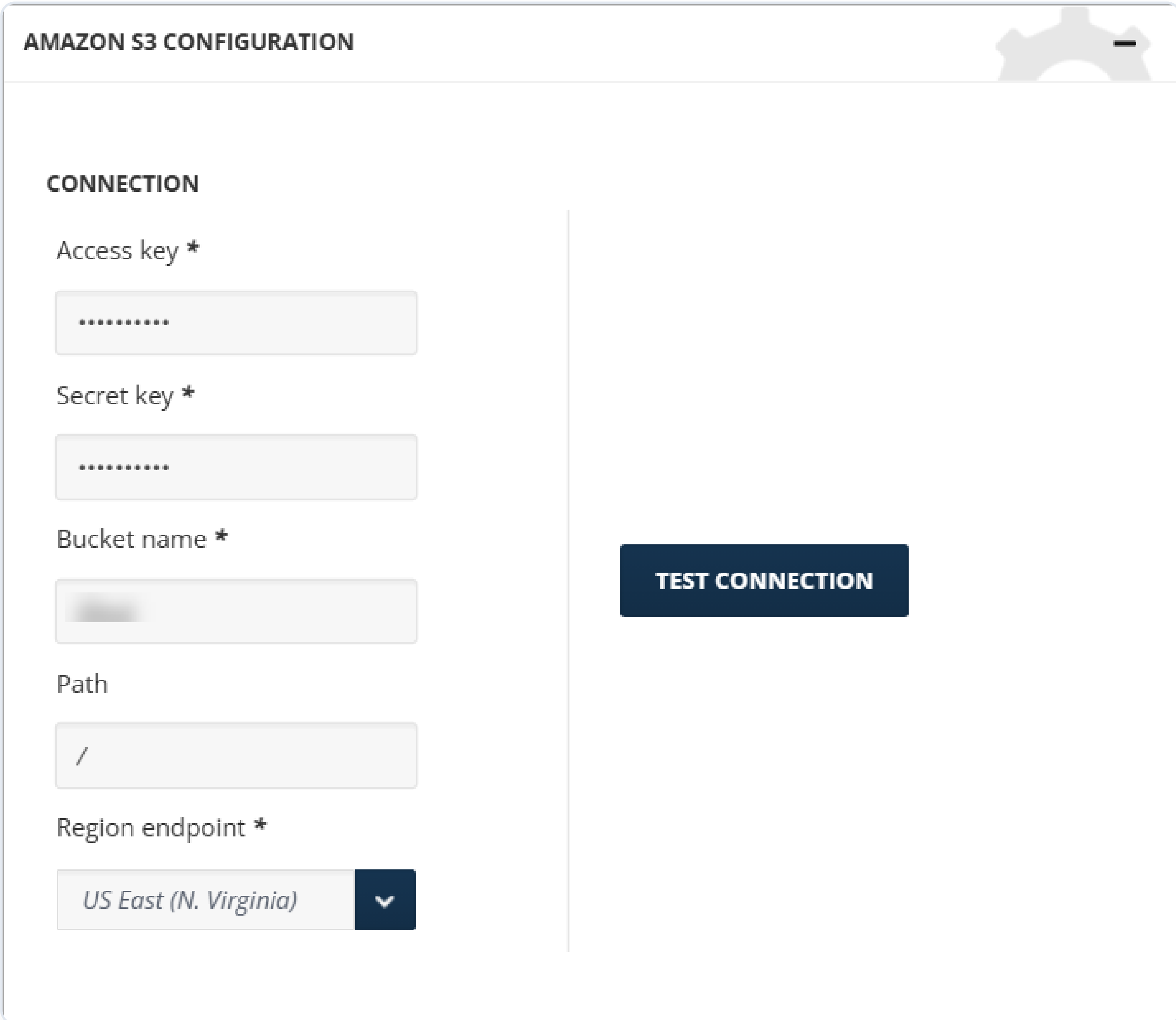


7. Enter **Password**.
8. Click **Import** and the **Public Key** field will be populated automatically.
9. In case you enable **Use Security**, select FTP connection type from the **Connection Type** drop-down list. FTP can run in either passive or active mode. The information about the connection type should be provided by the FTP host. If you wish to use FTP over SSL, enable the **Use Security** checkbox and choose the connection method **Implicit SSL**, **Explicit SSL** or **SSH**.
10. Enter the **Username** and **Password** fields provided by the source.
11. Click **Test Connection**. If the connection is successful, a green check sign is displayed.
12. To enable anonymous FTP connections, enable the **Anonymous Access** checkbox which is the default settings.



To capture data from Amazon S3, triggers and a Lambda function need to be created on the Amazon S3 site. The trigger is run when specific actions occur within a bucket and the source bucket items with their metadata are imported to the archive bucket. the data from the archive bucket are captured.

If the Amazon S3 source is selected, the Amazon S3 Configuration window will open.



The following information is required:

- **Access Key** - enter the access key which you can find in the Users > Security Credentials of your Amazon S3 account.
- **Secret Key** - enter the secret key acquired while setting up the Security Credentials. Save it in a secure place as that secret key is provided only once.
- **Bucket Name** - enter the archive bucket name.
- **Path** - enter the path within the bucket from which data is captured. Defaults to the bucket root (`/`).
- **Region Endpoint** - enter the Region Endpoint which you can find in the Bucket Overview > Properties of your Amazon S3 bucket. Note that if Region Endpoint is not set correctly, the archive content will not be captured and processed.

Click **Test Connection** to verify that the entered credentials and settings can successfully connect to the Amazon S3 bucket.

To capture data stored from different sources in Azure Blob storage, it should be configured accordingly. For more information on how to configure Azure Storage, see the Configuring Azure Storage section. The stored data will then be capture from the storage.

Using custom domains is not supported, the URL must point to one of the well-known Azure Storage endpoints listed below:

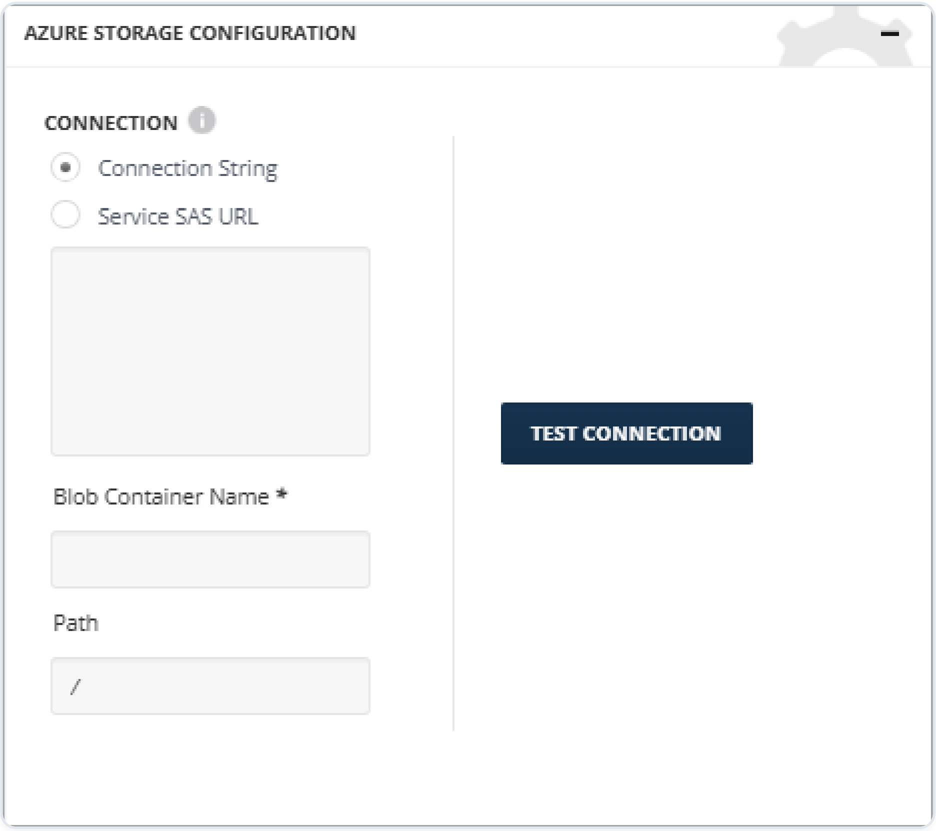
- blob.core.windows.net
- blob.core.usgovcloudapi.net
- blob.core.chinacloudapi.cn

To configure Azure Storage:

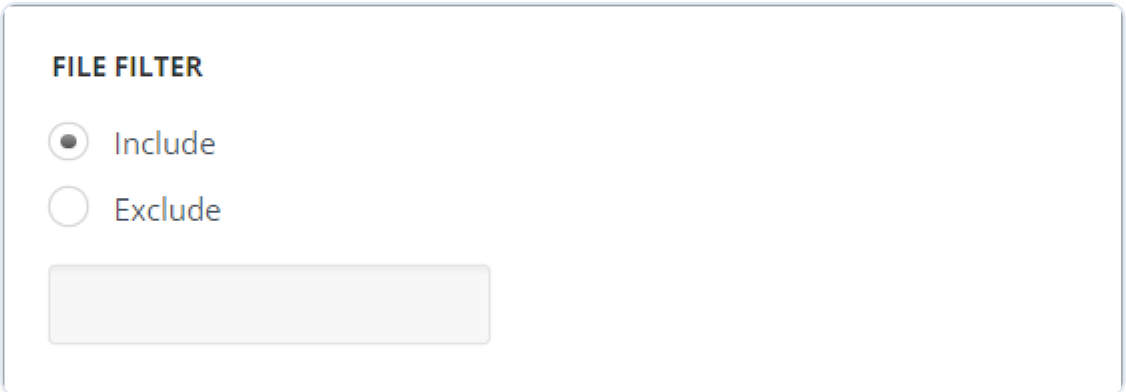
1. Enable **Connection String** and enter the Connection String copied in step 10 of the Configuring Azure Storage section.

OR,

1. Enable **Service SAS URL** and enter the Service SAS URL copied in step 10 of the Configuring Azure Storage section.
2. Enter **Blob Container Name** from step 11th of the Configuring Azure Storage section.
3. Enter the **Path** where the data is captured within the Blob container. The default value is `/`, which captures data from the root of the container.
4. Click **Test Connection** to verify that the configured Azure Storage connection is valid.

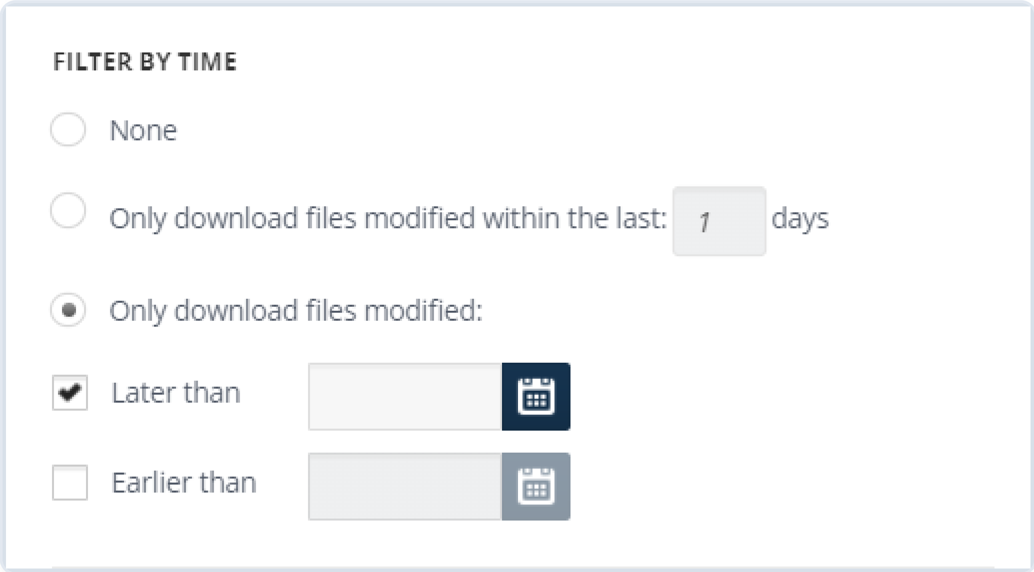


For File Filter a wildcard can be used to denote the file types to be included or excluded. Each type of filter is separated by the vertical pipe character |. For example: *.tar.gz | ".txt.



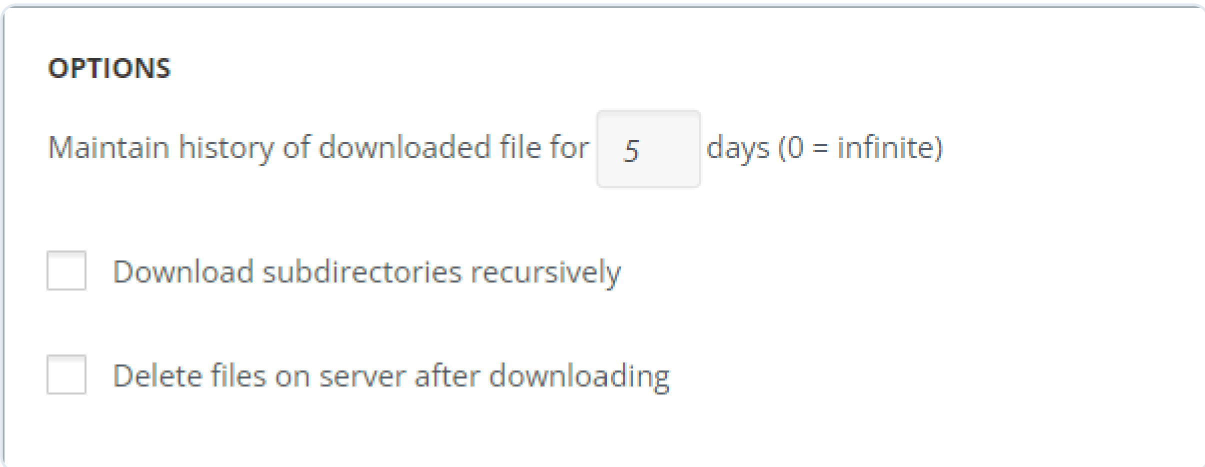
For Filter by Time:

1. If **None** is selected, the data is not filtered by time.
2. When **Only download files modified within the last X days** is selected, only the data modified within the mentioned days will be downloaded.
3. When **Only download files modified earlier than/later than** is selected only the data modified earlier than or later than the mentioned date will be downloaded. Both options can be selected simultaneously to choose a period.



For Options:

1. **Maintain history of downloaded file for X days (0 = infinite)** sets how many days the history of downloaded files will remain. If the number of days is set to 0, the history is maintained forever.
2. If **Download subdirectories recursively** is checked, files from subdirectories of the mentioned path will be downloaded too.
3. If **Delete files on server after downloading** is checked, the downloaded files will be deleted from the server.



Configuring Azure Storage

For Azure Blob storage:

1. Login to your Azure portal account.
2. Navigate to **Storage Accounts**.
3. Click the account Name.

4. On the left side navigation pane, navigate to **Shared Access Signature**.
5. For Allowed services, enable **Blob**.
6. For Allowed resource types, enable **Container** and **Object**.
7. For Allowed permissions, enable
   - **Read**
   - **Delete**

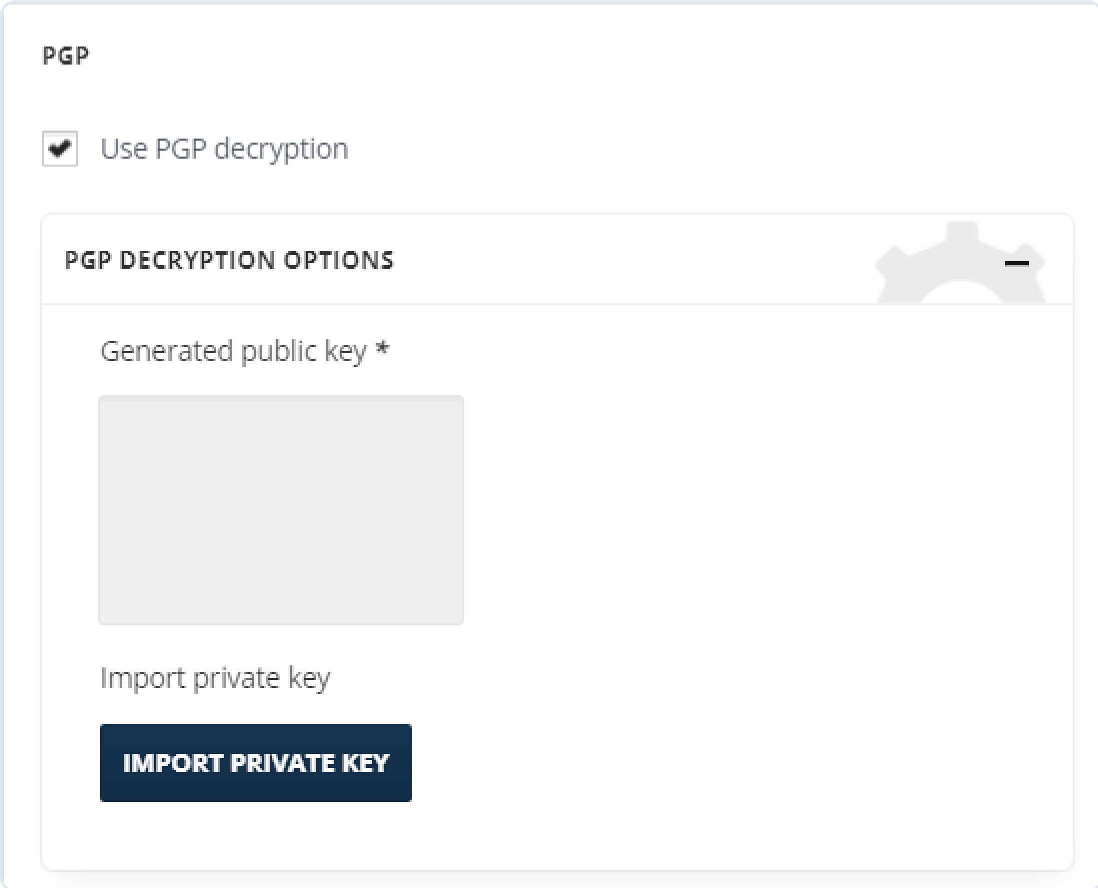
     > **Note:** This is needed in case the 6th step is enabled.

   - **List**
8. For Allowed Blob index permissions, enable **Read/Write** and **Filter**.
9. Specify the Expiration start and end date and click **Generate SAS and connection string**.
10. Copy **Connection string** and **Blob service URL** for Connection configuration.
11. On the left side navigation pane, select **Containers** and click the name of the container you want.

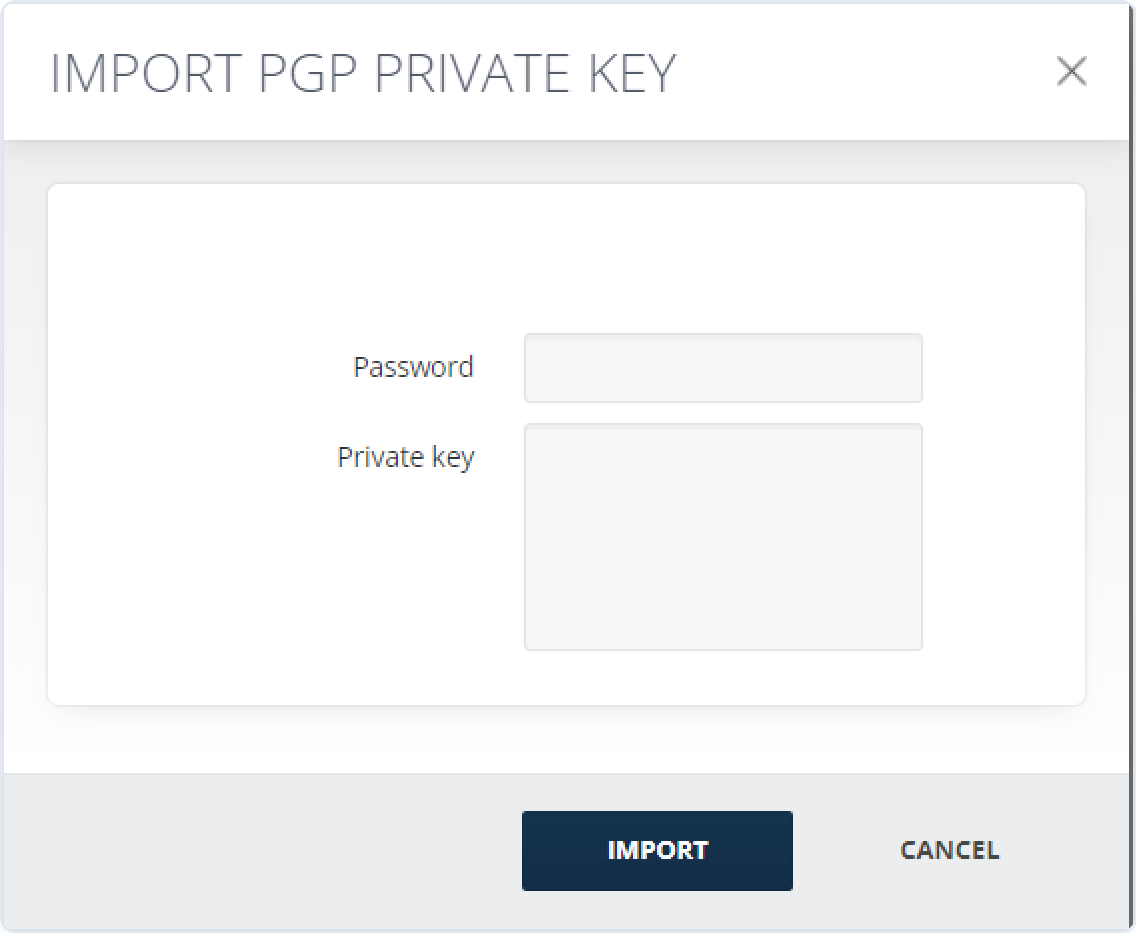
PGP Configurations

For PGP configurations:

1. Enable the **Use PGP Decryption** checkbox and **PGP Decryption Options** will be opened.



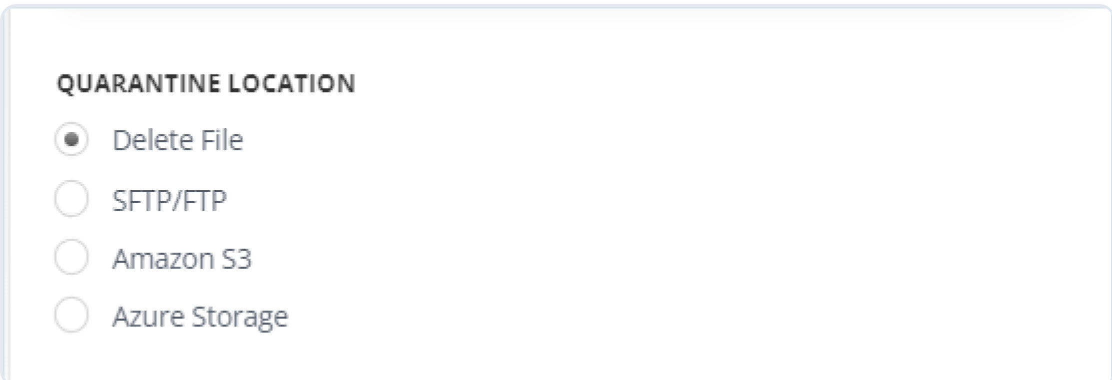
2. Click **IMPORT PRIVATE KEY**. The **Import PGP Private Key** window will appear.
3. Enter **Private Key** generated with the key management tool and click **Import**.



> **Note:** When generating public/private key pairs, it is important to use a reliable PGP key generation tool. Consult with your Security Team to ensure that you are using an approved tool. For instance, Kleopatra is a readily available open-source option. It is important to note that Arctera does not endorse any specific tool.

Quarantine Location

This section allows selecting the location of the quarantined files or deleting them. The following options are available:



- **Delete files** - if selected, quarantined files will be deleted.

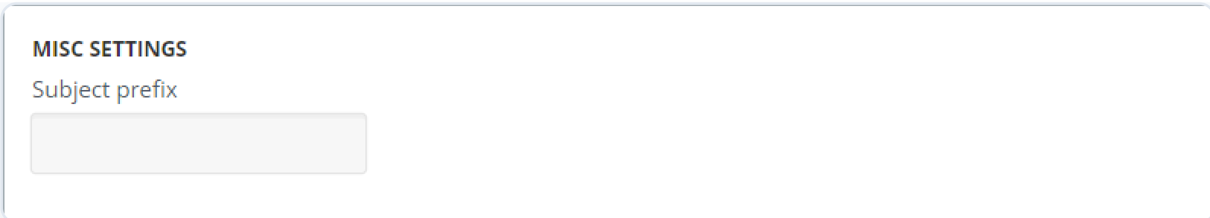
- **SFTP/FTP** - for more information, see SFTP Configuration in File Source Configuration
- **Amazon S3** - for more information, see Amazon S3 Configuration in File Source Configuration
- **Azure Storage** - for more information, see Azure Storage Configuration in File Source Configuration

The same configurations described in File Source Configuration apply here, with one difference: the **Create new folder for each session** checkbox is also available in the quarantine settings. When enabled, a new folder is created for each session in the quarantine location.

Miscellaneous Settings

The **Subject prefix** is added to the subject line of imported emails. This is useful for organizing imported data especially when multiple sources share a common target.

> **Note:** Not applicable to the EV Folder target.



Timestamp Formatting

In addition to the primary stamp, a second timestamp can be enabled with its time zone. From the drop-down menu, you can choose the time zone of the timestamp. The format of the timestamp in the output message can also be specified from the six options in the **Date Time Format** drop-down list.

> **Note:** This section is not applicable to the EV.Cloud target.

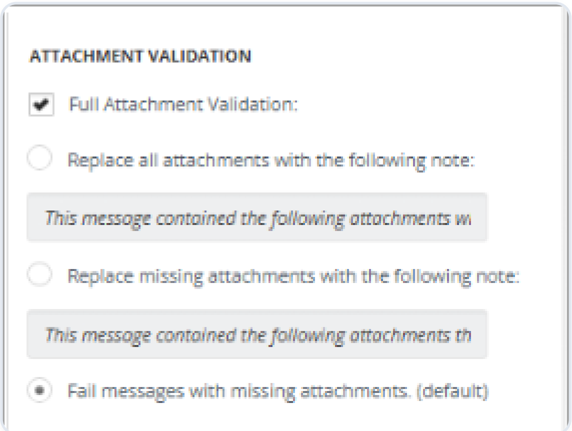
Attachment Validation

Arctera Capture enables you to develop customized notes for attachment validation. The default setting is **Fail Messages with missing Attachments**, as a result of which the messages that do not have attachments are failed and can be viewed under the **Reports**. Note that **Advanced Processing** should not be selected for this to happen.

When **Full Attachment Validation** is enabled, the entire source (file group) is quarantined in case the attachment of a message is missing or corrupted, i.e., the selection under Attachment Validation (**Fail messages with missing attachments**) will be ignored.

If you select the **Replace all the attachments with the following note** and input your custom note, all the attachments to the messages will not be processed and in their place the input note will be added to the message.

If you select the **Replace missing attachments with the following note** and input your custom note, all the missing attachments of the messages will not be processed, and you will see only the custom message that you have entered.



Amazon S3

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance. It provides easy-to-use management features so you can organize your data and configure access controls to meet your business, organizational, and compliance specific requirements.

Activities Captured

- Folder activities - created/renamed
- Files and file operations - created (upload)/renamed/updated (by uploading another file with the same exact name)

To capture Amazon S3 data, triggers and a Lambda function need to be created on the Amazon S3 site. The trigger is run when specific actions occur within a bucket. And the source bucket items with their metadata are imported to the archive bucket. The collector will then capture the data from the archive bucket.

File Formats Supported by the Collector

- .json

Source Configuration

For information on how to configure the following sections of the **Source** tab, see:

- File Source Configuration
- PGP Configurations
- Quarantine Location
- Miscellaneous Settings
- Timestamp Formatting

Supported Notifications

The importer supports the following notification types:

- **Quarantine file**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Failed to quarantine file**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users (N/A)
- Filters
- Targets
- Importer Settings

Audio Video

Arctera Capture Audio Video collector captures audio/video recording files. It allows parsing audio/video metadata files in a .csv format. It transforms source metadata to support the configured output file format. The mapping is done based on the uploaded XML template. It varies from source to source. Contact Arctera Support for more details on the mapping corresponding to the source you are going to use it for.

Activities Captured

- Participants: From, To, CC, and BCC
- Start time
- End time
- Attachments

> **Note:** To process the attachments, add the full path to each attachment in the CSV/TXT document. To prevent files with similar names from clashing, we recommend creating attachments with a folder structure to avoid files with similar names shared on different days and in different conversations.

> **Note:** The CSV/TXT and the ZIP files should have the same name to process the files properly.

File Formats Supported by the Collector

- .txt

- .csv

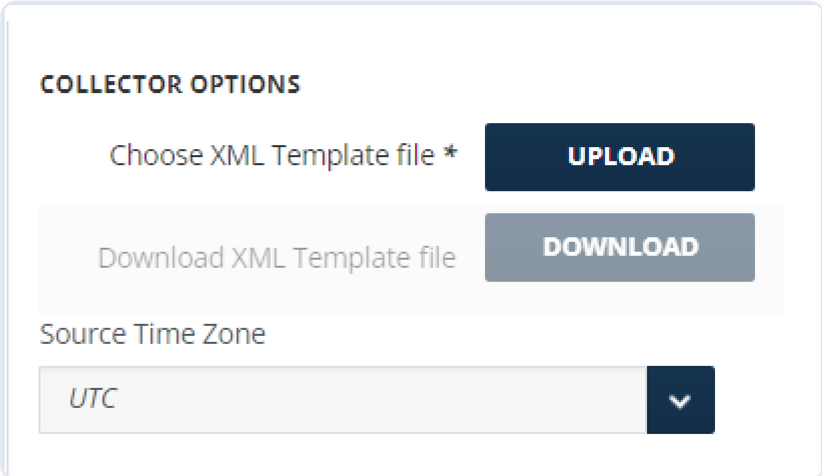
Source Configuration

For information on how to configure the following sections of the **Source** tab, see:

- File Source Configuration
- PGP Configurations
- Quarantine Location
- Miscellaneous Settings

Collector Options

Upload an XML template and select the relevant time zone. Capture will attempt to retrieve the correct time zone from the source automatically.

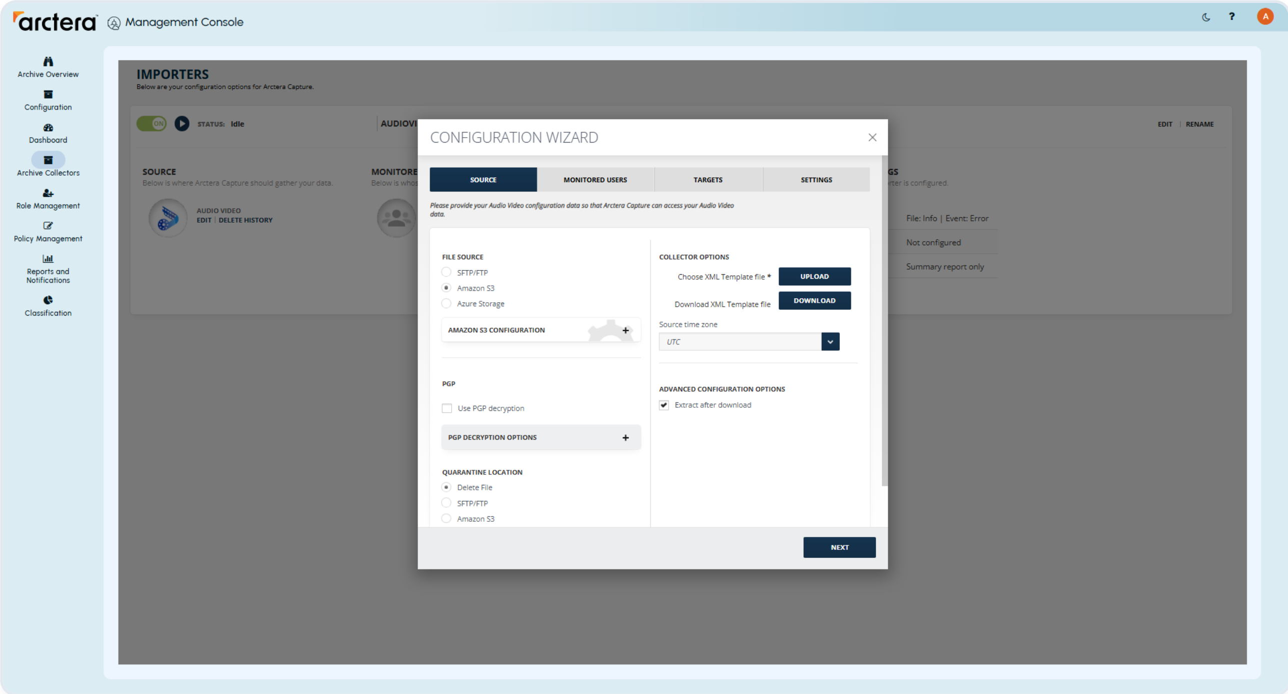


The XML file should contain the information about the file itself. It should specify if the file contains headers, the number of columns, delimiter type and the text qualifier. Next part of the XML file should assign column names, identify data types, and indicate if the columns are optional. Lastly, it should map the columns to the expected data fields: Sender, Participants, Title, ActivityDateTime, and Content.

If you want to manually set up the **Source Time Zone**, select the relevant one from the drop-down list. The Source Time zone setting will attempt to retrieve the time zone from the data itself automatically.

Advanced Configuration Options

To configure advanced options, enable **Extract after download** to extract the contents of downloaded archive files before they are processed.



XML Template Configuration Guideline

To configure XML Template sample:

1. Configure the information about the file itself: if the file contains headers, number of columns, text qualifier and attachment method.

```
<?xml version="1.0" encoding="UTF-8"?>

<configuration> <version>AV_2.0</version>

<options>

<containsHeader>Yes</containsHeader>

<maxCols>8</maxCols>

<delimiter>","</delimiter>

<text_qualifier>"</text_qualifier>

<content_type>PlainText</content_type>

<attachmentMethod>Archive</attachmentMethod>

</options>
```

1. Assign column names, identify data type, and indicate if columns are optional.

```
<columns>

<column>

<order>1</order>

<name>FileName</name>

<datatype>StringList</datatype>

<datatype_options>

<delimiter>";"</delimiter>

<append>""</append>

</datatype_options>

</column>

<column>

<order>3</order>

<name>Start Date</name>

<datatype>DateTime</datatype>

<datatype_options> <format>XX/DD/YYYY HH:MM:SS</format> </datatype_options>

</column>
```

> **Note:** In the DateTime `<format>`, each letter represents a part of the source value: `Y` (year), `X` (month), `D` (day), `H` (hour), `M` (minute), `S` (second), `F` (millisecond), and `Z` (time zone). To parse 12-hour times, add the `TT` token for the AM/PM designator. When `TT` is present, the time is converted to 24-hour format automatically. For example, the format `XX/DD/YYYY HH:MM:SS TT` parses `5/10/2013 3:59:27 PM` as `2013-05-10 15:59:27` and `5/10/2013 12:00:00 AM` as `2013-05-10 00:00:00`.

```
<column>

<order>5</order>
```

```
<name>Username</name>

<datatype>String</datatype>

</column>

<column>

<order>6</order>

<name>User Email</name>

<datatype>String</datatype>

</column>

<column>

<order>7</order>

<name>Participant Name</name>

<datatype>StringList</datatype>

<datatype_options>

<delimiter>";"</delimiter>

<append>""</append>

</datatype_options>

</column>

<column>

<order>8</order>

<name>Participant Email</name>

<datatype>String</datatype>

</column>

</columns>
```

1. The last part of the XML file maps the columns to the expected data fields: Sender, Participants, Title, ActivityDateTime, and Body:

```
<mappings>

<mapping can_be_empty = "Yes">

<property>Sender</property>

<items>

<item>User Email</item>

</items>

</mapping>

<mapping can_be_empty = "Yes">

<property>SenderName</property>

<items>

<item>Username</item>

</items>

</mapping>

<mapping can_be_empty = "Yes">

<property>Participants</property>

<items>

<item Role="To">Participant Email

</item>

</items>

</mapping>

<mapping can_be_empty = "Yes">

<property>ParticipantNames</property>
```

`<items>`

`<item Role="To">Participant Name</item>`

`</items>`

`</mapping>`

`<mapping can_be_empty = "Yes">`

`<property>Title</property>`

`<items>`

`<item>Call Id</item>`

`<string>" "</string>`

`</items>`

`</mapping>`

`<mapping can_be_empty = "Yes">`

`<property>Content</property>`

`<items>`

`<string>"Call Id: "</string>`

`<item>Call Id</item>`

`<string>" "</string>`

`<string>"Start Date UTC: "</string>`

`<item>Start Date</item>`

`<string>"`

`"</string>`

`<string>"End Date UTC: "</string>`

`<item>End Date</item>`

`<string>"`

```
"</string>
</items>
</mapping>
<mapping can_be_empty = "Yes">
<property>ActivityDateTime</property>
<items>
<item>Start Date</item>
</items>
</mapping>
<mapping can_be_empty = "Yes">
<property>Attachments</property>
<items>
<item>FileName</item>
</items>
</mapping>
<mapping can_be_empty = "Yes">
<property>X-KVS-MessageType</property>
<items> <string>"IM.AudioVideo"</string>
</items>
</mapping>
</mappings>
</configuration>
```

Supported Notifications

The importer supports the following notification types:

- **Quarantine file**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Failed to quarantine file**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users (N/A)
- Filters
- Targets
- Importer Settings

BlackBerry

The BlackBerry smart phone was once the most popular mobile device for enterprise use. Arctera Capture captures BlackBerry communications and stores them in existing email archive, whether on-prem or in the Cloud.

Activities Captured

- Pin-to-pin
- Messenger

- SMS/MMS

File Formats Supported by the Collector

- .csv

Source Configuration

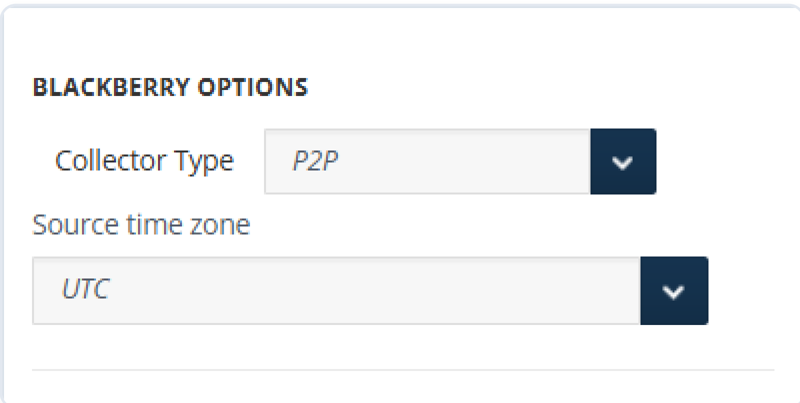
For information on how to configure the following sections of the **Source** tab, see:

- File Source Configuration
- PGP Configurations
- Quarantine Location
- Miscellaneous Settings

BlackBerry Options

The BlackBerry source can only process one format at a time. You have the following Collector Types to choose from the drop-down list:

- P2P (default)
- SMS
- Messenger (BBM)
- Video chat

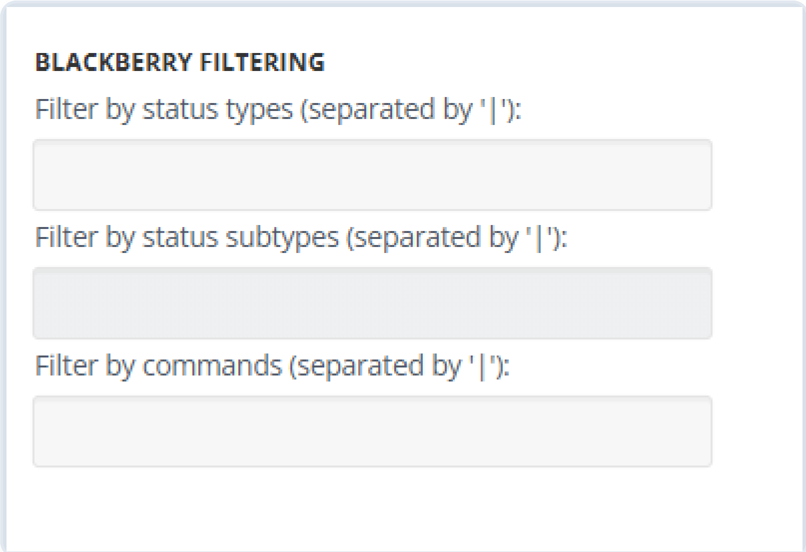


Once you have selected the **Collector Type**, you can also provide the **Source time zone** information. It is assumed that the messages in the source file are of the set time zone and based on that data, the dates in the messages are processed to UTC time zone. By default, Arctera Capture sets the Source time zone as Local time zone.

BlackBerry Filtering

Use BlackBerry Filtering configurations to determine which status types, subtypes, or commands will be imported. Separate each name with the following symbol: |. Note, that wildcards are not supported for the following field.

Each source type has different filtering options. P2P type can be filtered with status types and commands. SMS sources can be filtering by all displayed options. The Messenger type can be filtered only by commands. Video chats cannot be filtered. If you want to process the whole data, leave all three fields blank.



Supported Notifications

The importer supports the following notification types:

- **Quarantine file**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Failed to quarantine file**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**

- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users (N/A)
- Filters
- Targets
- Importer Settings

Bloomberg

Bloomberg delivers business and markets news, data, analysis, and video to the world, featuring stories from Business week and Bloomberg News. Bloomberg Vault is a hosted end-to-end information management service that delivers compliance and IT solutions by leveraging the scalability and reliability of Bloomberg's global infrastructure. It provides secure digital storage for corporate clients of Bloomberg, primarily email and messaging content. Capture imports and processes the files from Bloomberg.

Activities Captured

- Disclaimers (.dscl)
- Instant Bloomberg Messages (.ib), attachments (.att)
- Email Messages (.msg), attachments (.att)

> **Note:** To process current schema files, the file filter should be configured with the following extensions: *.ib19.*.xml*.gpg | *.msg.*.xml*.gpg | *.dscl.*.xml*.gpg | *.ib19.att.*.tar.gz*.gpg | *.msg.att.*.tar.gz*.gpg.

File Formats Supported by the Collector

- .ib19..xml
- .msg..xml

- .dscl..xml
- .ib19.att..tar.gz
- .msg.att..tar.gz

Source Configuration

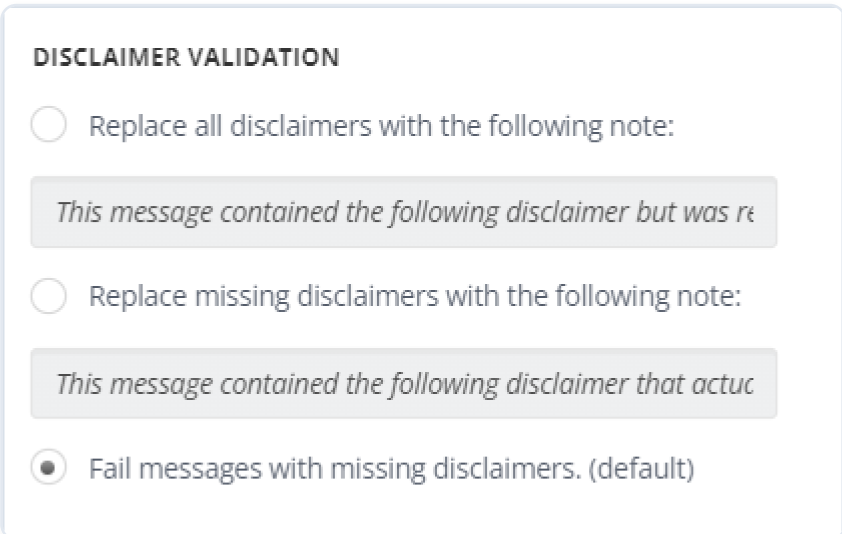
For information on how to configure the following sections of the **Source** tab, see:

- File Source Configuration
- PGP Configurations
- Quarantine Location
- Miscellaneous Settings
- Attachment Validation

Disclaimer Validation

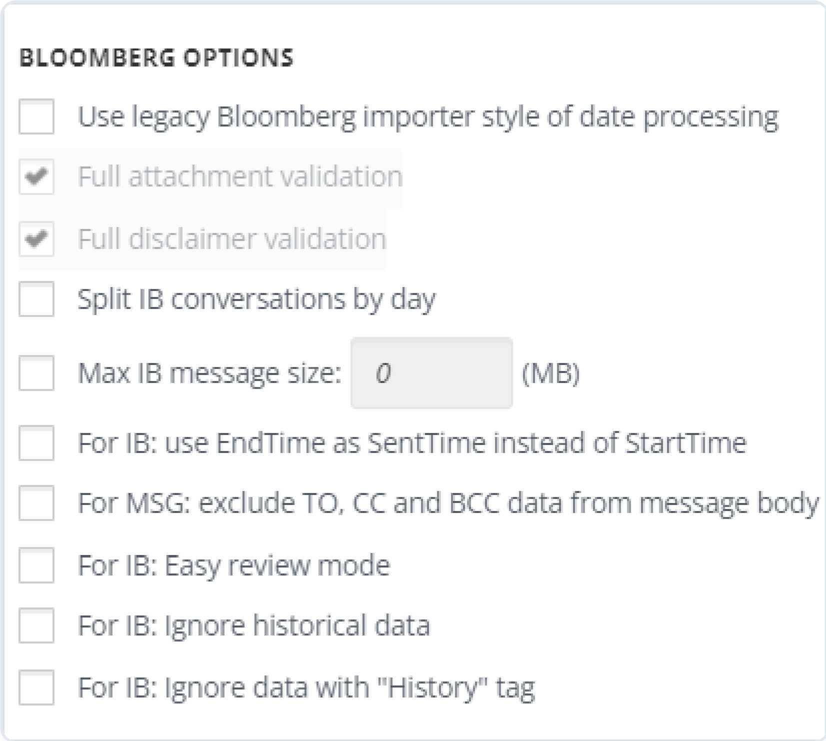
Develop customized notes for disclaimer validation. The default setting is **Fail messages with missing disclaimers**, so the messages that do not have disclaimers are failed.

If you select the **Replace all disclaimer with the following note** and input your custom note, all the disclaimers will not be processed and instead of them the input note will be added to the message. If you select the **Replace missing disclaimers with the following note** and input your custom note, all the missing disclaimers will not be processed and instead of them the input note will be added to the message.



Bloomberg Options

The following options are available:



- **Use Legacy Bloomberg Importer style of date processing** - Scans the date and time stamp of dump files and ensures their time zones correspond with those of the device on which Capture is running (recommended for dump files created before March of 2009). If this option is not selected, it is assumed that date processing should be accomplished based on the Universal Time Coordinated (UTC) time zone, which is used for all current Bloomberg files. However, Bloomberg files created before March 2009 will be processed successfully, even if this option is not selected (selection, however, is recommended).
- **Full attachment validation** - By default enabled, the entire source (file group) is quarantined, in case the attachment of a message is missing or corrupted, i.e., the selection under Attachment Validation (Fail messages with missing attachments) will be ignored.
- **Full disclaimer validation** - By default enabled, the entire source (file group) is quarantined, in case the disclaimer of a message is missing or corrupted, i.e., the selection under Disclaimer Validation (Fail messages with missing disclaimers) will be ignored.
- **Split IB Conversations by day** - If checked, messages with the same UTC day will be imported into one message.
- **Max IB Message Size: (MB)** - When this option is checked and the maximum size is set, the messages with larger message size will be split. Note that attachments with larger size will not be split.
- **For IB: use EndTime as SentTime instead of StartTime** - The SentTime in the imported message of IB source files will be replaced with the EndTime of the message, instead of StartTime.

> **Note:** If 'Split IB Messages by day' is enabled, DateTimeUTC is prioritized.

- **For MSG: exclude TO, CC and BCC data from message body** - When this option is checked, TO, CC, and BCC data of the source MSG message is removed from the body of the message.
- **For IB: Easy Review Mode** - When this option is checked, Participant Entered and Participant Left events are shown in a separate table at the bottom of the message.
- **For IB: Ignore Historical Data** - When this option is checked, there will not be any historical events from prior days.
- **For IB: Ignore Data with History Tag** - When this option is checked, data with "History" tag will be ignored.

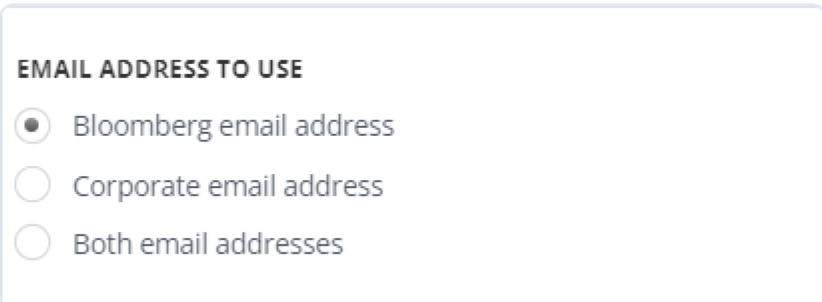
> **Note:** In the below examples, the time stamps in the body message are UTC, while the SentTime of the generated output is UTC +4. The SentTime of the message is adjusted to the time zone of the device it is opened on.

The mapping of SentDate (10:26 PM) can be changed using the "For IB: use EndTime as SentTime instead of StartTime" checkbox. By default, SentTime of the email is shown the same as StartTime.

If For IB: use EndTime as SentTime instead of StartTime is enabled the SentTime of the generated email is shown the same as the EndTime of the message.

Email Address to Use

Select the email address type you would like to use when processing data from users that have both their personal email address and their corporate email address registered on Bloomberg.

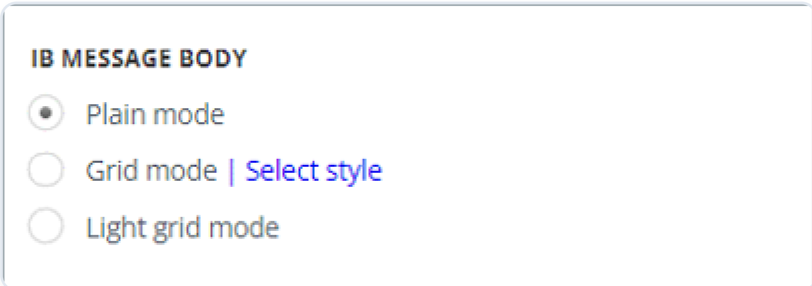


In case **Both email addresses** is selected, you can make either the Bloomberg or Corporate email address primary by clicking the corresponding button.

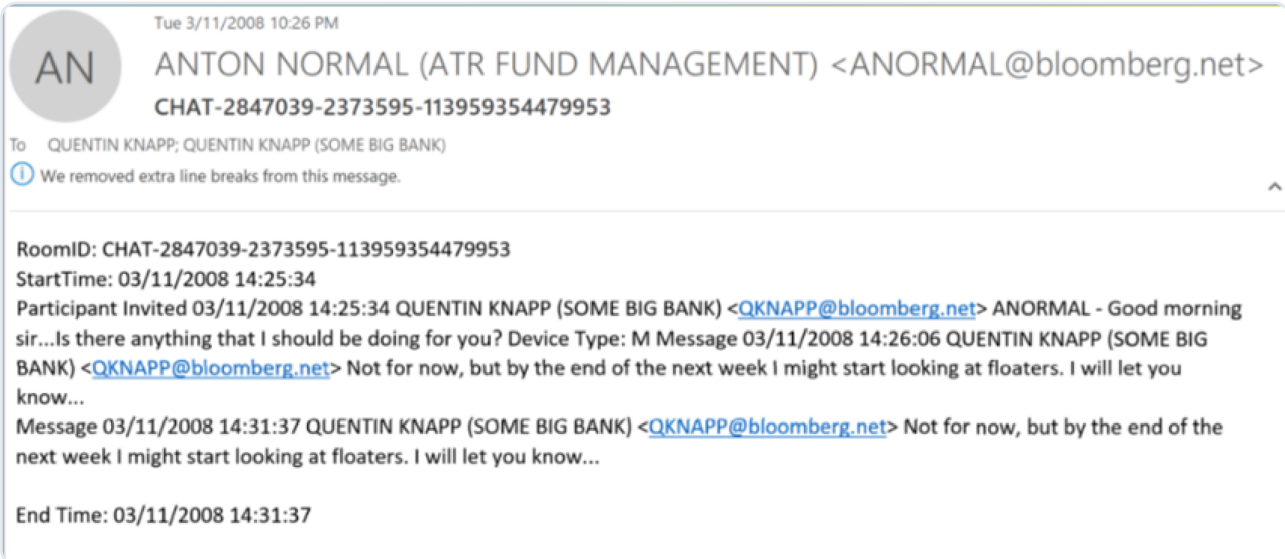
IB Message Body

In the Bloomberg collector, you can choose from the following IB message body options:

- **Plain mode**
- **Grid mode |Select style**
- **Light grid mode**



When you select the Plain mode option (default), you will see the interactions below each other. Plain mode displays the message in its basic form.

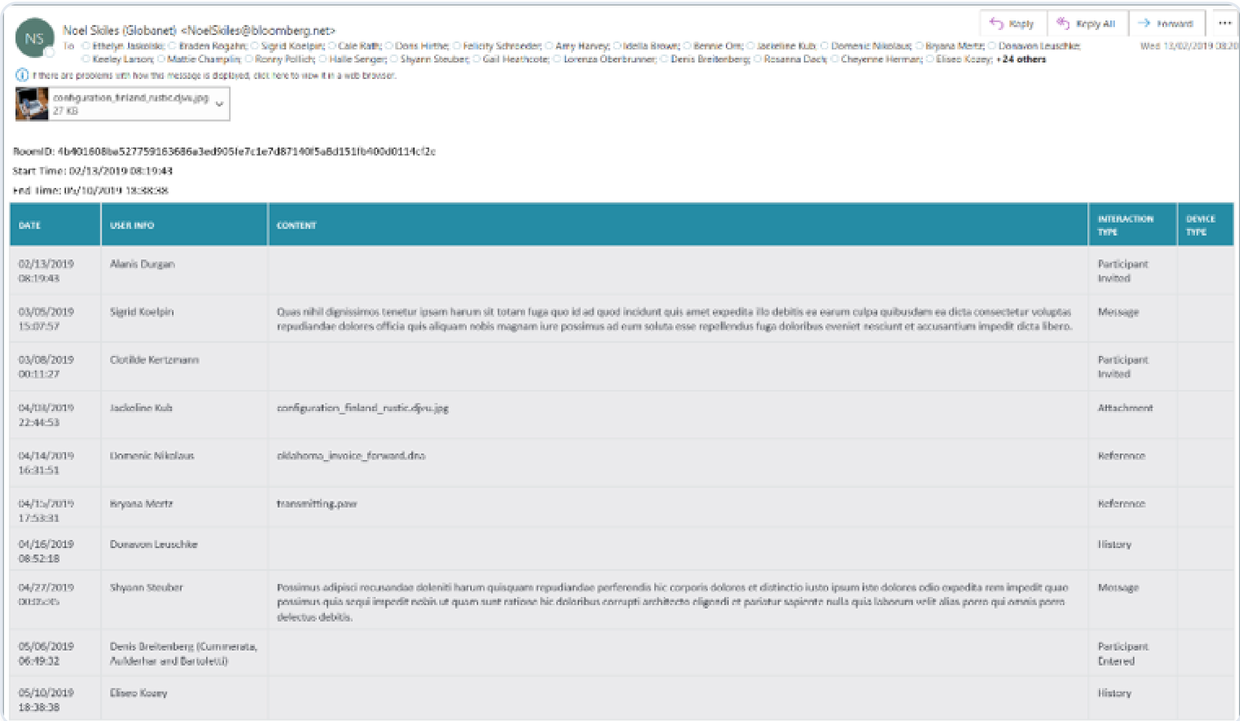

Tue 3/11/2008 10:26 PM
AN
ANTON NORMAL (ATR FUND MANAGEMENT) <ANORMAL@bloomberg.net>
CHAT-2847039-2373595-113959354479953
To QUENTIN KNAPP; QUENTIN KNAPP (SOME BIG BANK)
We removed extra line breaks from this message.

RoomID: CHAT-2847039-2373595-113959354479953
StartTime: 03/11/2008 14:25:34
Participant Invited 03/11/2008 14:25:34 QUENTIN KNAPP (SOME BIG BANK) <QKNAPP@bloomberg.net> ANORMAL - Good morning sir...Is there anything that I should be doing for you? Device Type: M Message 03/11/2008 14:26:06 QUENTIN KNAPP (SOME BIG BANK) <QKNAPP@bloomberg.net> Not for now, but by the end of the next week I might start looking at floaters. I will let you know...
Message 03/11/2008 14:31:37 QUENTIN KNAPP (SOME BIG BANK) <QKNAPP@bloomberg.net> Not for now, but by the end of the next week I might start looking at floaters. I will let you know...

End Time: 03/11/2008 14:31:37

If you enable the Grid mode option, you will see the information in the following columns:

- Interaction Type, which contains information about participants and messages, such as Participant Entered, Participant Left, Participant Invited, Message, Attachment.
- Date, which shows the date and time the message was sent.
- User Info, where you can view the user's Full Name (Company Name), Email Address
- Content
- Device Type, if the message was sent from a mobile device, it will be displayed as M in that field.



Noel Skiles (Globanet) <NoelSkiles@bloomberg.net>

To: Ethelyn Jaskolski; Braden Kogahn; Sigrid Koelpin; Cale Rath; Doris Hirthe; Felicity Schroeder; Amy Harvey; Idella Brown; Bennie Orn; Jackeline Kub; Domenic Nikolaus; Bryana Mertz; Donavon Leuschke; Keeley Larson; Mattie Champlin; Ronny Pollich; Halle Senger; Shyann Steuber; Gail Heathcote; Lorenza Oberbrunner; Denis Breitenberg; Rosanna Dach; Cheyenne Herman; Eliseo Kozey; +24 others

Wed 13/02/2019 08:20

If there are problems with how this message is displayed, click here to view it in a web browser.

configuration_finland_rustic.djvu.jpg 27 KB

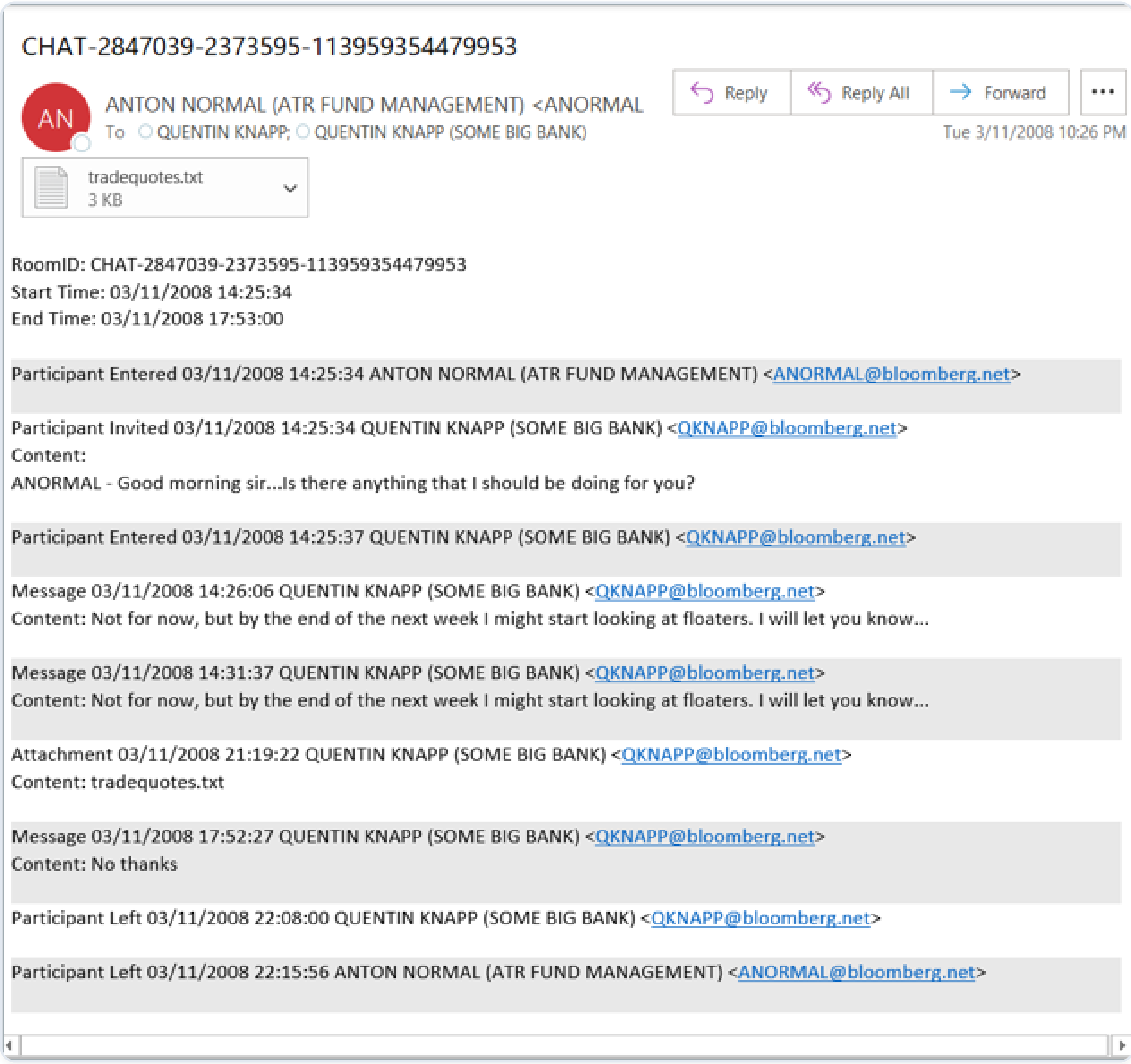
RoomID: 4b401608ba527759163686a3ed905fe7c1e7d87140f5a8d151fb400d0114cf2c

Start Time: 02/13/2019 08:19:43

End Time: 05/10/2019 18:38:38

DATE	USER INFO	CONTENT	INTERACTION TYPE	DEVICE TYPE
02/13/2019 08:19:43	Alanis Durgan		Participant Invited	
03/05/2019 15:07:57	Sigrid Koelpin	Quas nihil dignissimos tenetur ipsam harum sit totam fuga quo id ad quod incidunt quis amet expedita illo debitis ea earum culpa quibusdam ea dicta consectetur voluptas repudiandae dolores officia quis aliquam nobis magnam iure possimus ad eum soluta esse repellendus fuga doloribus eveniet nesciunt et accusantium impedit dicta libero.	Message	
03/08/2019 00:11:27	Clotilde Kertzmann		Participant Invited	
04/08/2019 22:44:53	Jackeline Kub	configuration_finland_rustic.djvu.jpg	Attachment	
04/14/2019 16:31:51	Domenic Nikolaus	oklahoma_invoice_forward.dna	Reference	
04/15/2019 17:53:31	Bryana Mertz	transmitting.paw	Reference	
04/16/2019 08:52:18	Donavon Leuschke		History	
04/27/2019 00:02:05	Shyann Steuber	Possimus adipisci recusandae deleniti harum quisquam repudiandae perferendis hic corporis dolores et distinctio iusto ipsum iste dolores odio expedita rem impedit quae possimus quia sequi impedit nobis ut quam sunt ratione hic doloribus corrupti architecto eligendi et pariatur sapiente nulla quia laborum velit alias porro qui omnis porro delectus debitis.	Message	
05/06/2019 06:49:32	Denis Breitenberg (Cummerata, Aufderhar and Bartoletti)		Participant Entered	
05/10/2019 18:38:38	Eliseo Kozey		History	

When you enable Light grid mode, the data is two-toned an easy to be viewed with limited metadata.



Processing Bloomberg Firm-Level Files

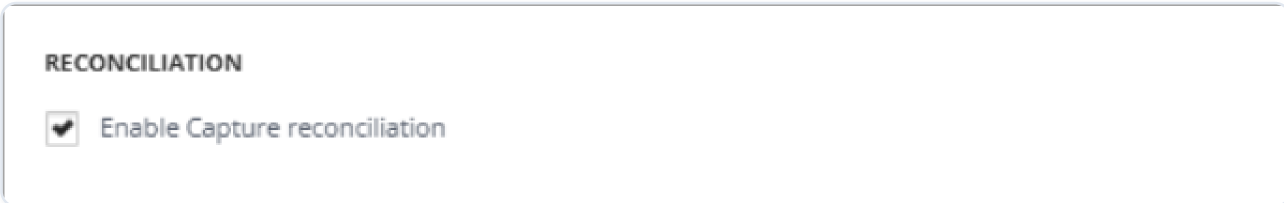
An ideal technique for processing Bloomberg's firm-level files is to set Ignored Target as the default. Then a filter should be configured to match segments for the necessary account numbers and route them to a secondary target, and likewise, another filter to match segments to account numbers that are unnecessary and route them to a Failed Target.

This way, new account numbers can be discovered using the reporting feature in Reporting & Message Tracking. **Unconditional hit default target** and **Process all filters** must be disabled from Filtering.

However, if you intend to set other Targets for your importer, click the exact target type to see how it is set up.

Reconciliation

Select **Enable Capture reconciliation** to reconcile the number of messages that Arctera Capture processes against the message count reported by the source. For Bloomberg, the reconciliation file is delivered through file transfer together with the data files in the same run.



Supported Notifications

The importer supports the following notification types:

- **Quarantine file**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Failed to quarantine file**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with configuration of:

- Monitored Users (N/A)
- Filters

- Targets
- Importer Settings

Box

Box platform is a cloud content management platform and can be accessed using the Box Content API. Box provides a suite of cloud content services that lets build content apps quickly.

Activities Captured

- Uploads
- Downloads and task assignments

> **Note:** During the first run, we will only get folder structure.

- Comments
- Box quick notes (in Box generated special format)
- New version upload (in the message subject event type is displayed as edited)
- Task completed and task rejected (displayed in the message body as task deleted)
- Comment deletion
- Move
- Copy
- Edits(only Box quick notes)
- Preview
- Rename
- Report export

> **Note:** Original files are attached for all the events unless the files have been deleted previously. In that case, the message about the captured event will include information about the deleted file.

Creating a Box Application

To create a Box application:

1. Go to https://developer.box.com/, sign into an existing account or create a new one.
2. Click **Create New App**.
3. Choose **Custom App** and click **Next**.
4. Select the **User Authentication (OAuth 2.0)** method, enter the name of the app in the **App name** field, and click **Create App**.
5. Go to the **Configuration** section, copy, and save **Client ID** and **Client Secret**.
6. Add Arctera Capture IP address to **Redirect URI**.

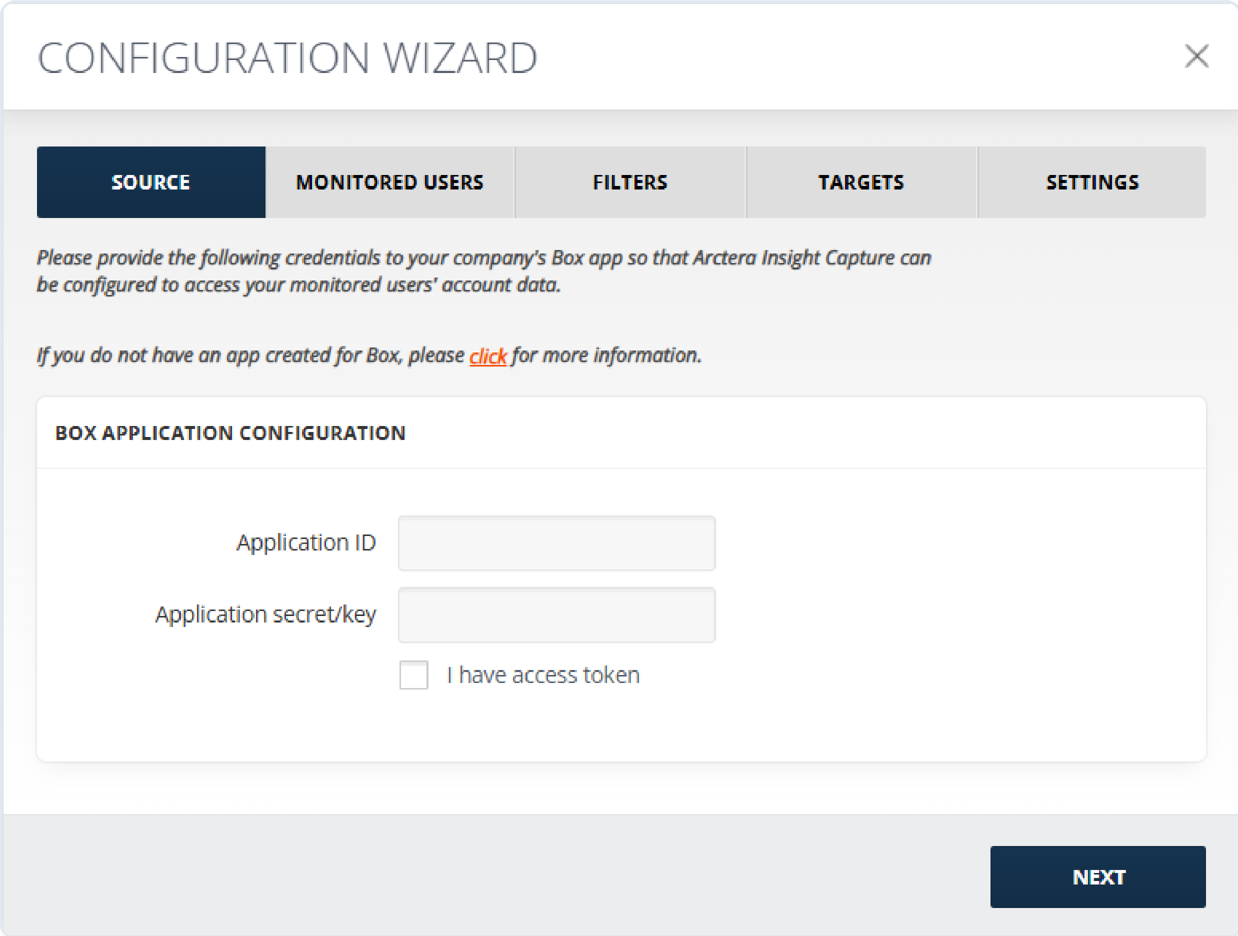
> **Note:** The **Redirect URI** can be found in the Click information of the collector source configuration.

7. Set the following permissions:
   - Application Scopes:
     - **Read all files and folders stored in Box**
     - **Write all files and folders stored in Box**
     - **Manage users**
     - **Manage enterprise properties**
   - Advanced Features: **Make API calls the as-user header**.
8. Click **Save Changes**.

Source Configuration

For configuring the Box application:

1. After entering a **Name** and a **Description** (optional) for the collector and then selecting the collector from the list, in the **Application ID** field, add the Client ID copied previously, and in the field of **Application Secret/Key**, enter copied Client Secret, click **NEXT**.



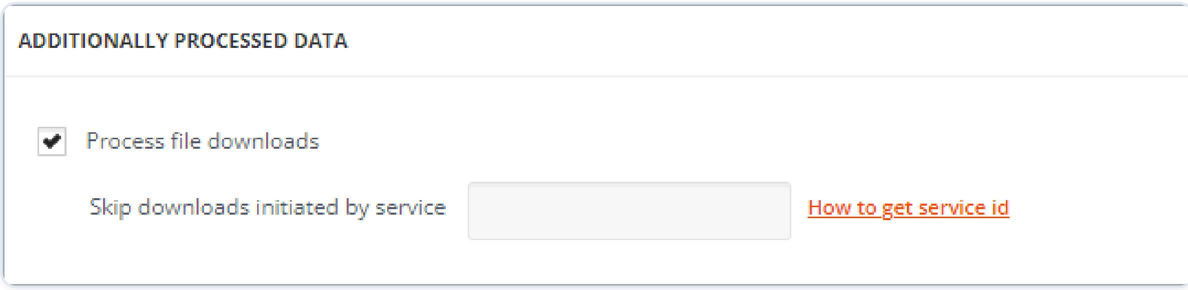
2. Grant access to Box in the opened pop-up window. Make sure that pop-ups are not blocked by your browser.

Additionally Processed Data

Once you are through setting up the Box application, you can also configure a few optional settings.

- If **Process file downloads** is checked, it will process the download file events from the events feed in Box. The files from Box are downloaded and attached to the messages. The downloads are recorded as download events in Box.
- If the **Process file downloads** box is checked, the download events are processed too, and again recorded as downloads in the Box, and so on. So each consequent time, the number of imported download events is increased exponentially.
- In the **Skip downloads initiated by service** field, the application ID that downloads the file, can be added so that the downloads done by that application are ignored and not processed. To retrieve the ID:
    - Log in to Box and navigate to Box Platform.

- At the top right corner, click **My Apps** and select your application to navigate to its details page.
- Copy the last number from the URL in the browser address field: e.g., `https://<yourdomain>.app.box.com/developers/console/app/THIS-NUMBER`.



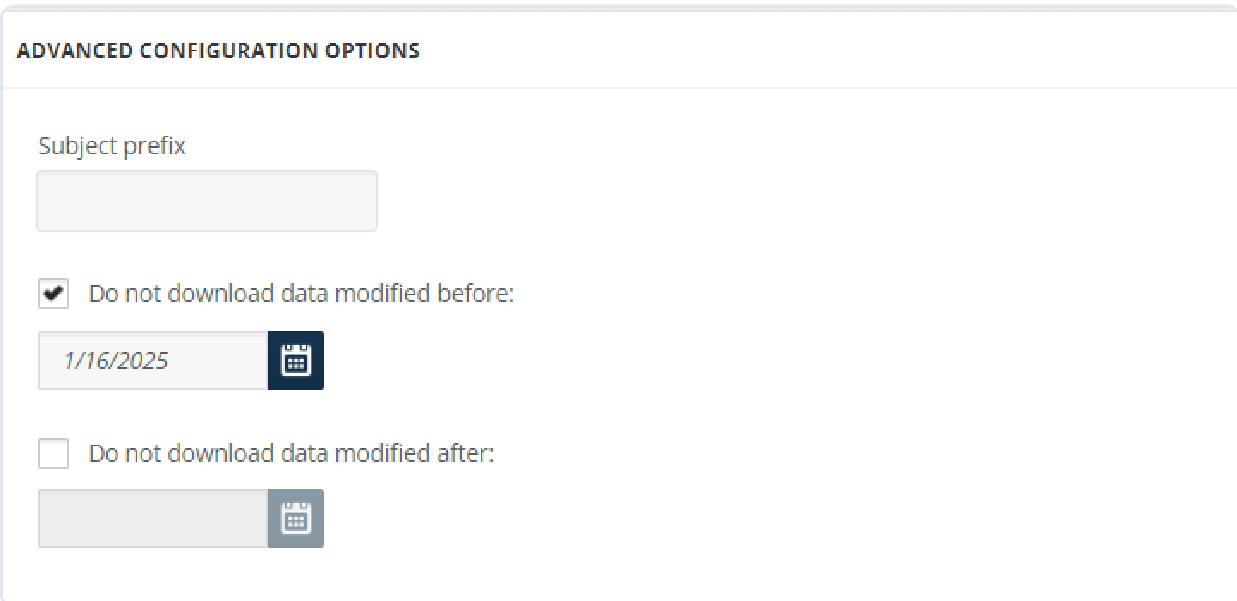
Advanced Configuration Options

To configure advanced options:

1. Specify the **Subject Prefix** in the subject line of imported emails. This is useful for organizing imported data, i.e., when multiple sources share a common target.

   > **Note:** Not applicable to the EV Folder target.

2. Specify **Do not download data modified before** and **Do not download data modified after** to allow cutting off data outside the set date range. If the before date is set to 08/17/2023 and the after date is set to 08/25/2023, only the data between these two dates will be downloaded. Data outside that range will be ignored. Note that both options can be used independently as well.



Supported Notifications

The importer supports the following notification types:

- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users
- Filters
- Targets
- Importer Settings

CellTrust

CellTrust is a leading provider of compliant and secure mobile communications for regulated industries. CellTrust SL2™ is a communication platform for voice, text / SMS and chat that integrates with leading providers of archiving and e-discovery.

Activities Captured

- Messages

Captured messages can contain:

- Message subject
- Message headers
- Participants: From, To, CC, and BCC
- Activity datetime
- Message body

File Formats Supported by the Collector

- .xml

Source Configuration

For information on how to configure the following sections of the **Source** tab, see:

- File Source Configuration
- PGP Configurations
- Quarantine Location
- Miscellaneous Settings

Supported Notifications

The importer supports the following notification types:

- **Quarantine file**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Failed to quarantine file**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**

- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users (N/A)
- Filters
- Targets
- Importer Settings

ChatGPT

ChatGPT is a generative AI platform from OpenAI that allows organizations to enhance productivity by generating content, summarizing information, and automating tasks using natural language. It functions as a critical channel for internal communication, research, and data creation, and its interactions require proper governance and archiving.

The ChatGPT collector captures communication that occurs between users and the AI assistant.

Activities Captured

- User prompts
- User uploaded files
- AI responses
- Codex data

> **Note:** Due to current API limitations, the following items are not captured:
>
> - User-uploaded files that have expired under the ChatGPT Chat and File Retention Policies.
> - Files generated as output of AI responses.

Acquiring an API Key and Workspace ID

The owners of your organization must complete the steps below to generate an API Key and Workspace ID for the ChatGPT collector configuration.

To create a new API key:

1. Navigate to the OpenAI Platform and log in. Verify that the correct organization is selected in the organization picker menu (usually found in the top right corner).
2. Click **Create new secret key**.
3. In the pop-up window, click **Create secret key**, leave **Project** set to **Default Project** and **Permissions** set to **All**.
4. Copy the generated API key immediately and store it securely (it can only be viewed once).

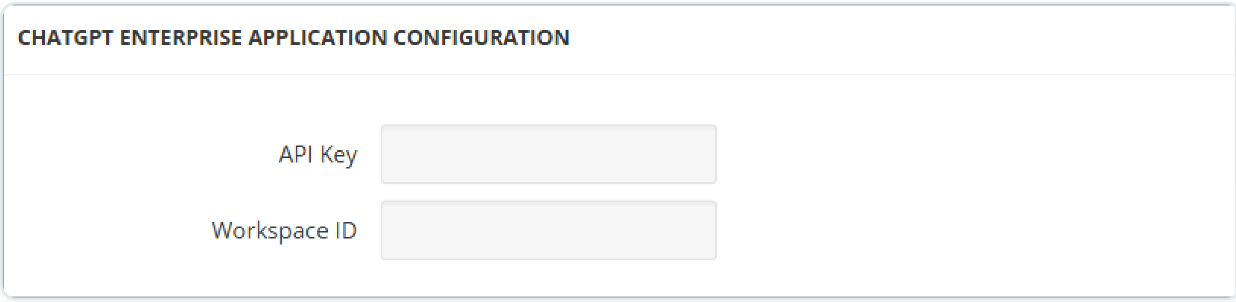
> **Note:** The generated API Key must be verified and granted the necessary scope by Open AI Support for collector functionality.

5. Send an email to mailto:support@openai.com with the subject line, "API Key Verification and Scope Granting Request", including the following details in the body and wait for confirmation from OpenAI:
   - The Key Name
   - Last 4 digits of the API Key
   - Created By name
   - Requested scope: read.
6. Once approved, the organization owner can use the securely stored API Key to configure the collector or share it with a partner for Compliance API integration.
7. To retrieve the Workspace ID, navigate to the ChatGPT Enterprise Admin Console.
8. Copy the **Workspace ID** to use it for configuring the collector.

Source Configuration

To set up ChatGPT Enterprise Application Configuration:

1. Enter **API key** stored in the 4th step.
2. Enter **Workspace ID** copied in 8th step.



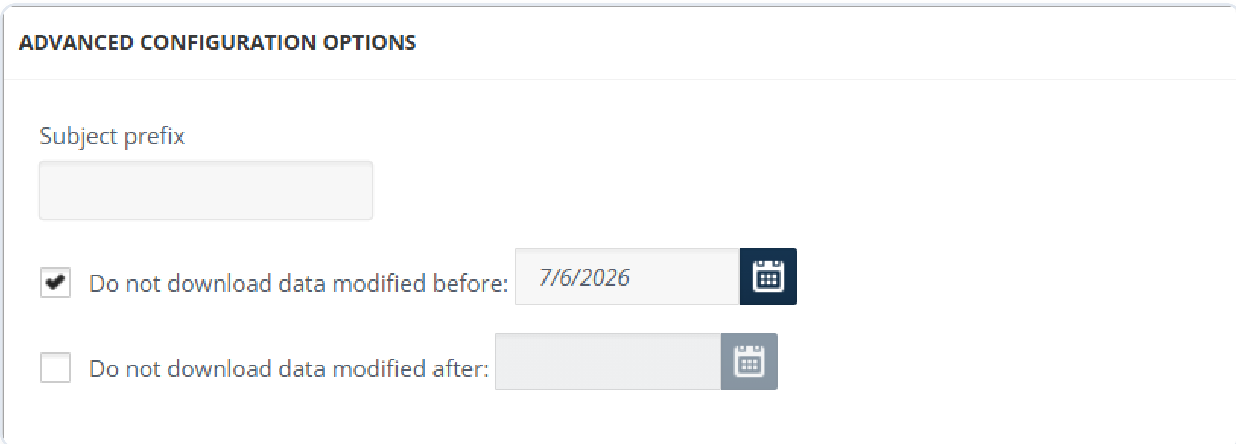
Advanced Configuration Options

To configure advanced options:

1. Specify the **Subject Prefix** in the subject line of imported emails. This is useful for organizing imported data, i.e., when multiple sources share a common target.

   > **Note:** Not applicable to the EV Folder target.

2. Specify **Do not download data modified before** and **Do not download data modified after** to allow cutting off data outside the set date range. If the before date is set to 08/17/2025 and the after date is set to 08/25/2025, only the data between these two dates will be downloaded. Data outside that time frame will be ignored. Note that both options can be used independently.

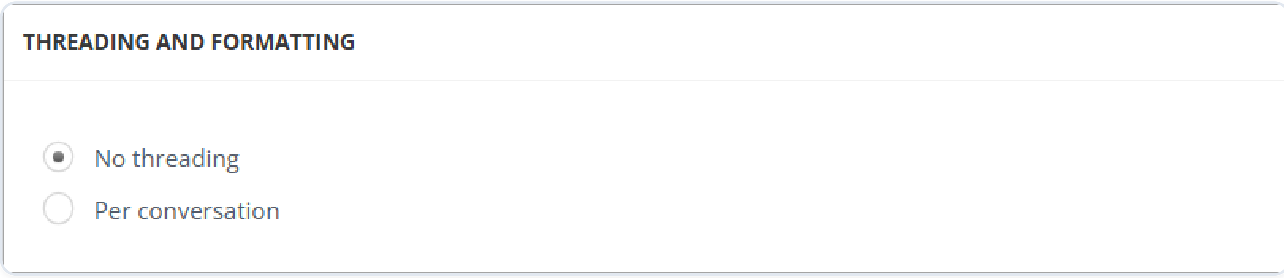


Threading and Formatting

> **Note:** This section is not applicable to the EV.Cloud target.

> You can control how messages are grouped in the output message using the following options:

- **No threading**: If selected, only a single message will be generated for each user prompt or AI response.
- **Per conversation**: If selected, a threaded message will be generated for each ChatGPT conversation.

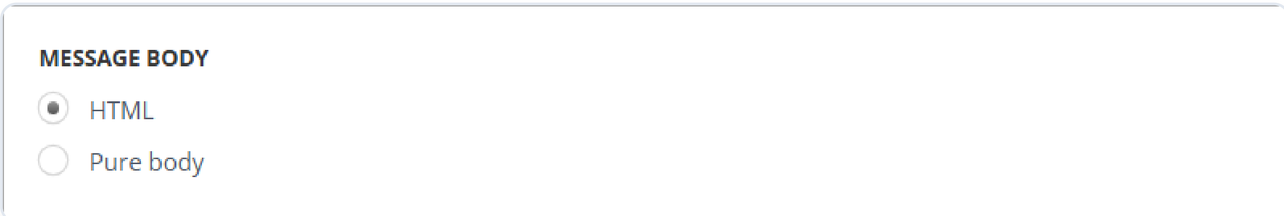


Message Body

> **Note:** This section is not applicable to the EV.Cloud target.

> This setting determines how imported messages are displayed in the target. There are the following output message body options:

- **HTML**: Displays the message in HTML format.
- **Pure body**: Displays the output message as plain text, without formatting or additional details.



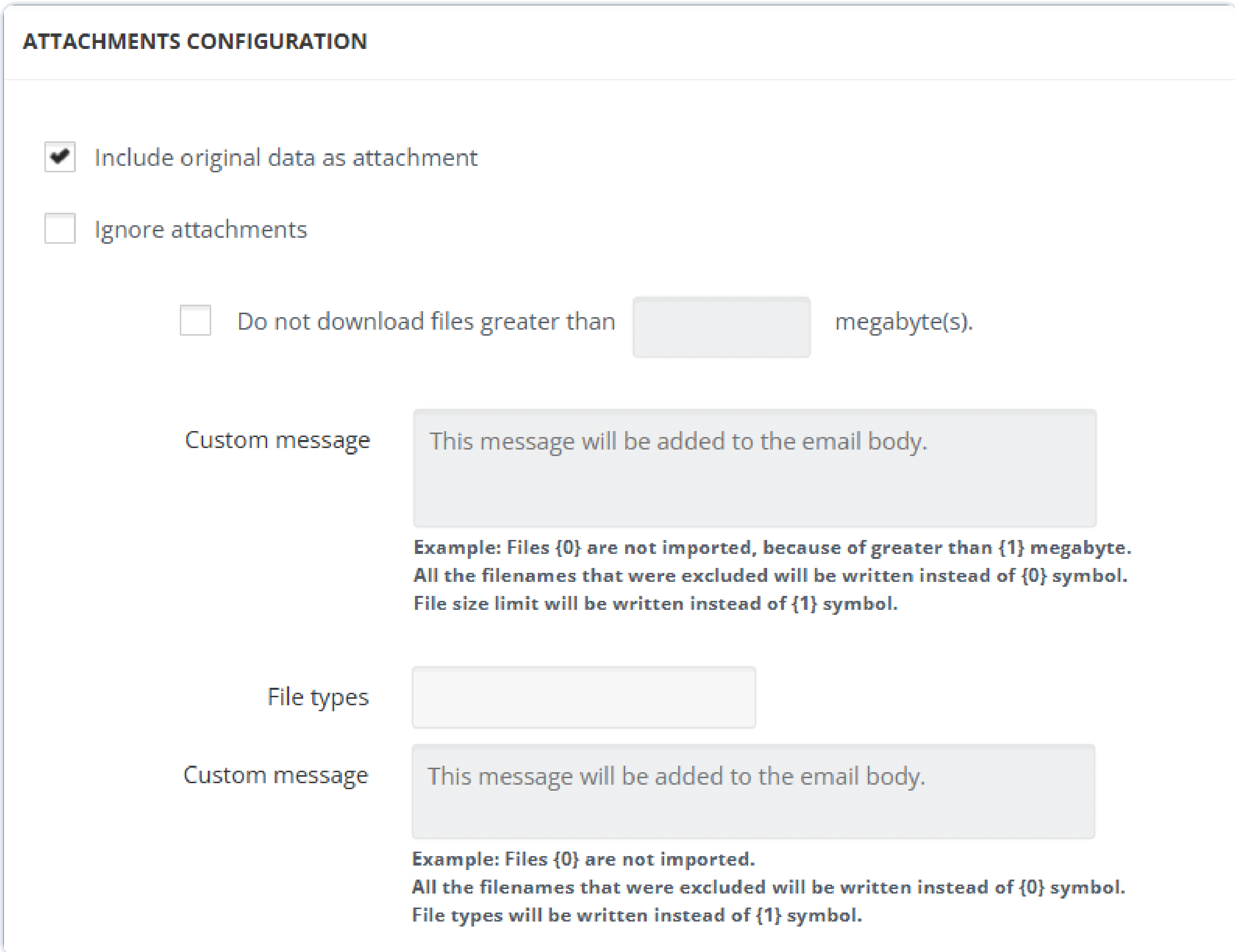
Attachments Configuration

- **Include original data as attachment**: If checked, the message original data is attached to the output file.

  > **Note:** Not applicable to the EV Folder target.

- **Ignore attachments**: If checked, all the attachments are excluded from the message enhancing the collector performance. Each message will contain info and the link to the excluded attachment.

- When **Do not download files greater than X megabyte(s)** is selected, the files bigger than the filled-in number of megabytes are not downloaded. In the **Custom Message** field, a text for those excluded files can be specified. For example, "Files {0} are not imported, because they are greater than {1} megabytes". {0} is used to add the name of the file and {1} is used to add the number of megabytes specified above.
- In the **File Types** field, the types of files that should not be downloaded can be specified in the following format: e.g., .txt | .xml. The vertical bar is used to separate the file types.



Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users
- Filters
- Targets
- Importer Settings

Supported Notifications

The importer supports the following notification types:

- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Chatter

Chatter is an enterprise collaboration platform from Salesforce, a cloud-based customer relationship management (CRM) vendor. The Chatter collector needs to log into the Salesforce account with an Admin user and get user personal token to import data. Besides, triggers need to be published on the Chatter site to be able to capture updates, deletions, and edits. The triggers will create a post in a channel and Capture will capture the information from the channel.

Shield Platform Encryption is supported without any additional configuration, since the data is encrypted by Salesforce "At rest" and the API provides the data decrypted.

Activities Captured

- Posts
- Files
- Comments
- Shares (including group posts)

- Comments of shared posts
- Deletes and edits (require triggers)
- Links
- Polls
- Private and group chats
- Feed poll choices (If Modify all data permission is enabled)
- New event/task contact/opportunity/case/lead
- All online communication, including attachments and deleted information (if the triggers are set)

> **Note:** Call logs and topics are not captured.

Creating a Salesforce Application

To perform the steps below you will need a Salesforce account with a System Administrator profile. If you do not have access to a System Administrator user, contact your Salesforce admin and ask for permissions.

Step 1: Creating a profile

1. Login to Salesforce using an account that has the System Administrator profile and switch to Salesforce Classic (if you are using the Lightning Experience).
2. Click **Setup**, then expand **Manage Users** and click **Profiles**.
3. Find the Read-Only profile and click the **Clone** button.
4. Enter a Name in the **Profile Name** field and click the **Save** button.
5. When saved, click **Edit**.
6. The required administrative permissions for data collection are:
    - **API Enabled**
    - **Select Files from Salesforce**
    - **Manage Chatter Messages and Direct Messages**
    - **Manage Unlisted Groups** (Required only if the Unlisted Groups feature is enabled in the given Salesforce environment.)
    - **View All Data**

- **Modify All Data** (Only if capturing Feed poll Choices is required, otherwise can be ignored but errors will be present in the collector log. This is a limitation from Salesforce)

7. Under **General User Permissions**, make sure the following permissions are enabled:

    - **Access Activities**
    - **Allow View Knowledge**
    - **Knowledge One**

8. Under **Standard Object Permissions**, disable all the **Create**, **Edit**, **Delete** and **Modify All** options. Only the **Read** and **View All** permissions should stay.
9. Scroll down and click **Save**.

Step 2: Creating a User (Service Account)

1. Go to the **Users** page and click **New User**.
2. Fill out the required fields and select Salesforce as **User License**, and the profile will be created, then scroll down and click **Save**.

Step 3: Retrieving Access Token

1. Click your Username at the top right corner of the screen and select **My Settings**.
2. In the navigation pane to the left, under the **Personal** section, choose **Reset My Security Token**, then click **Reset Security Token**. The new token will be sent to the email associated with your account.

To collect deleted or updated comments and posts in Chatter, ask your Salesforce administrator to perform the following steps in the Chatter UI:

1. Create a new Private Group ensuring they do not automatically archive this group and **Private** option and **Broadcast Only** are selected.
2. Locate and make a note of the Group ID in the page URL.
3. Create a new label Private Group Id.

    - Go to **Setup** > **Custom Labels**.
    - Click **New Custom Label**.
    - For **Short Description** - Private Group Id.
    - **Value** - Insert Group Id of Private group.

To install triggers:

1. Create a new label named as Private Group Id.

   - Go to **Setup** > **Custom Labels**.
   - Click **New Custom Label**.
   - Fill in the **Short Description**, **Name**, and **Value** fields.

2. Create Apex Classes.

   - Go to **Setup** > **Apex Classes**.
   - Click **New**.
   - Insert content from desired class (You can find all classes in classes folder) and click **Save**.

The following is the order in which all classes should be added.

`TriggerHandler.cls`

`TriggerHandlerTest.cls`

`ContentVersionManager.cls`

`FeedCommentManager.cls`

`FeedItemManager.cls`

`ContentVersionTriggerHandler.cls`

`FeedCommentTriggerHandler.cls`

`FeedItemTriggerHandler.cls`

`ContentVersionTriggerTest.cls`

`FeedCommentTriggerTest.cls`

`FeedItemTriggerTest.cls`

1. Create Apex Triggers.

   - Go to **Setup** > **Apex Triggers**.
   - Click **New**.
   - Insert content from desired class.
   - Click **Save**.

The following is the order in which all classes should be added.

`ContentVersionTrigger.trigger`

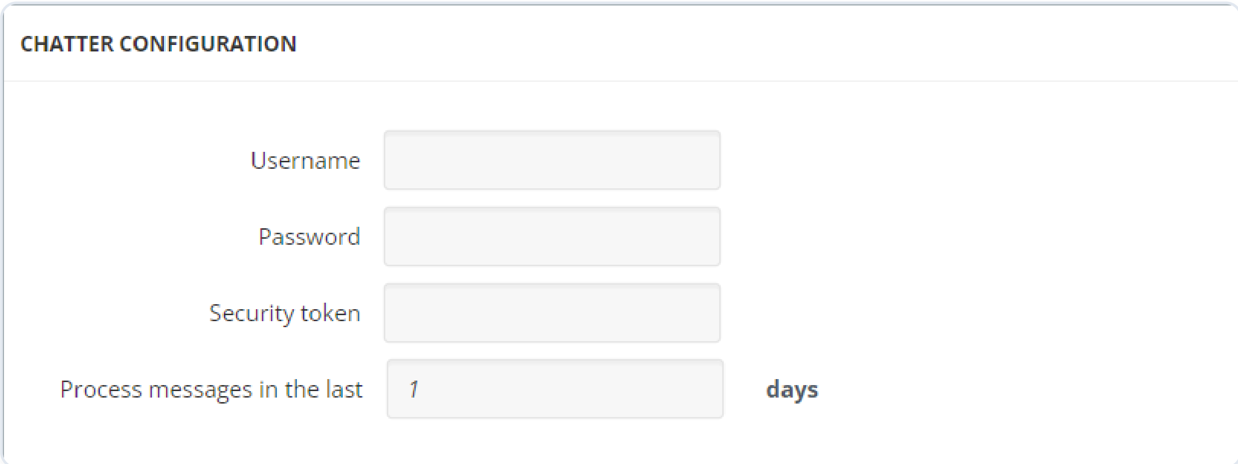
`FeedCommentTrigger.trigger`

`FeedItemTrigger.trigger`

Source Configuration

For Chatter configuration:

1. Enter the **Username** and **Password** of the Chatter Admin account used for app creation.
2. Enter the previously copied **Security Token**.
3. Specify the days for messages that should be processed.



Advanced Configuration Options

To configure advanced options:

1. Specify the **Subject Prefix** in the subject line of imported emails. This is useful for organizing imported data, i.e., when multiple sources share a common target.

> **Note:** Not applicable to the EV Folder target.

2. Specify **Do not download data modified before** and **Do not download data modified after** to allow cutting off data outside the set date range. If the before date is set to 08/17/2024 and the after date is set to 08/25/2024, only the data between these two dates will be downloaded. Data outside that range will be ignored. Note that both options can be used independently.

Supported Notifications

The importer supports the following notification types:

- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users
- Filters
- Targets
- Importer Settings

Chatter Cipher Cloud

Chatter is an enterprise collaboration platform from Salesforce, a cloud-based customer relationship management (CRM) vendor. The Chatter collector needs to log into the Salesforce account with an Admin user and get user personal token to import data. Besides, triggers need to be published on the Chatter site to be able to capture updates, deletions, and edits. The triggers will create a post in a channel and Capture will capture the information from the channel.

Shield Platform Encryption is supported without any additional configuration, since the data is encrypted by Salesforce "At rest" and the API provides the data decrypted.

Activities Captured

- Posts
- Files
- Comments
- Shares (including group posts)
- Comments of shared posts
- Deletes and edits (require triggers)
- Links
- Polls
- Private and group chats
- Feed poll choices (If Modify all data permission is enabled)
- New event/task contact/opportunity/case/lead
- All online communication, including attachments and deleted information (if the triggers are set)

> **Note:** Call logs and topics are not captured.

Creating a Salesforce Application

To perform the steps below you will need a Salesforce account with a System Administrator profile. If you do not have access to a System Administrator user, contact your Salesforce admin and ask for permissions.

Step 1: Creating a profile

1. Login to Salesforce using an account that has the System Administrator profile and switch to Salesforce Classic (if you are using the Lightning Experience).
2. Click **Setup**, then expand **Manage Users** and click **Profiles**.
3. Find the Read-Only profile and click the **Clone** button.
4. Enter a Namein the **Profile Name** field and click the **Save** button.
5. When saved, click **Edit**.
6. The required administrative permissions for data collection are:

- **API Enabled**
- **Select Files from Salesforce**
- **Manage Chatter Messages and Direct Messages**
- **Manage Unlisted Groups** (Required only if the Unlisted Groups feature is enabled in the given Salesforce environment.)
- **View All Data**
- **Modify All Data** (Only if capturing Feed poll Choices is required, otherwise can be ignored but errors will be present in the collector log. This is a limitation from Salesforce)

7. Under **General User Permissions**, make sure the following permissions are enabled:
    - **Access Activities**
    - **Allow View Knowledge**
    - **Knowledge One**
8. Under **Standard Object Permissions**, disable all the **Create**, **Edit**, **Delete** and **Modify All** options. Only the **Read** and **View All** permissions should stay.
9. Scroll down and click **Save**.

Step 2: Creating a User (Service Account)

1. Go to the **Users** page and click **New User**.
2. Fill out the required fields and select Salesforce as **User License**, and the profile will be created, then scroll down and click **Save**.

Step 3: Retrieving Access Token

1. Click your Username at the top right corner of the screen and select **My Settings**.
2. In the navigation pane to the left, under the **Personal** section, choose **Reset My Security Token**, then click **Reset Security Token**. The new token will be sent to the email associated with your account.

To collect deleted or updated comments and posts in Chatter, ask your Salesforce administrator to perform the following steps in the Chatter UI:

1. Create a new Private Group ensuring they do not automatically archive this group and **Private** option and **Broadcast Only** are selected.
2. Locate and make a note of the Group ID in the page URL.

3. Create a new label Private Group Id.

    - Go to **Setup** > **Custom Labels**.
    - Click **New Custom Label**.
    - For **Short Description** - Private Group Id.
    - **Value** - Insert Group Id of Private group.

To install triggers:

1. Create a new label named as Private Group Id.

    - Go to **Setup** > **Custom Labels**.
    - Click **New Custom Label**.
    - Fill in the **Short Description**, **Name**, and **Value** fields.

2. Create Apex Classes.

    - Go to **Setup** > **Apex Classes**.
    - Click **New**.
    - Insert content from desired class (You can find all classes in classes folder) and click **Save**.

The following is the order in which all classes should be added.

`TriggerHandler.cls`

`TriggerHandlerTest.cls`

`ContentVersionManager.cls`

`FeedCommentManager.cls`

`FeedItemManager.cls`

`ContentVersionTriggerHandler.cls`

`FeedCommentTriggerHandler.cls`

`FeedItemTriggerHandler.cls`

`ContentVersionTriggerTest.cls`

`FeedCommentTriggerTest.cls`

`FeedItemTriggerTest.cls`

1. Create Apex Triggers.

   - Go to **Setup** > **Apex Triggers**.
   - Click **New**.
   - Insert content from desired class.
   - Click **Save**.

The following is the order in which all classes should be added.

`ContentVersionTrigger.trigger`

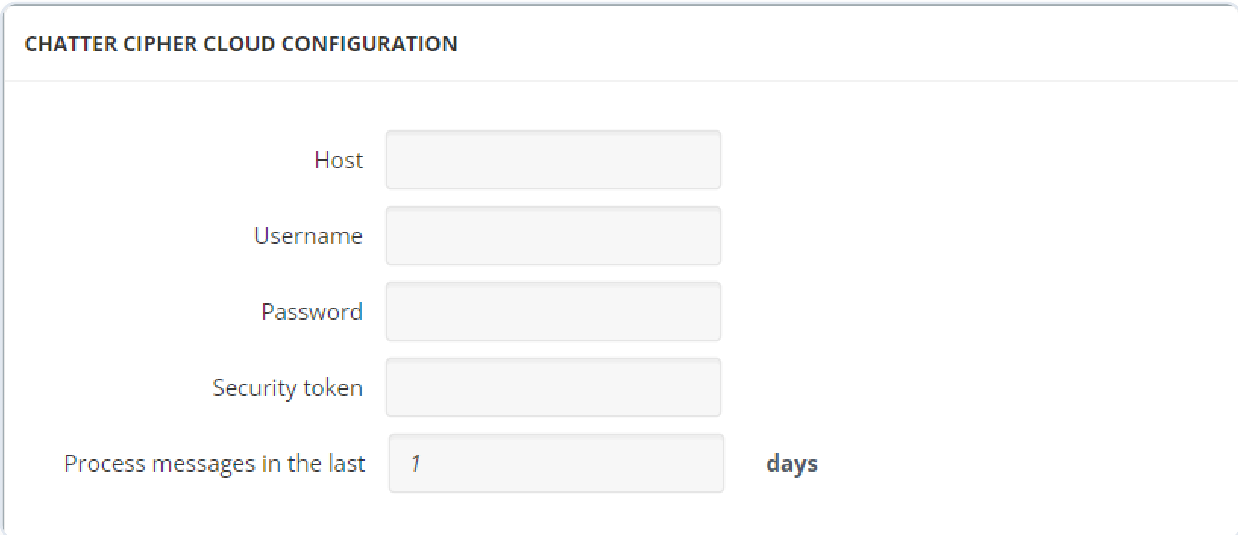
`FeedCommentTrigger.trigger`

`FeedItemTrigger.trigger`

Source Configuration

For Chatter configuration:

1. Specify **Host**.
2. Enter the **Username** and **Password** of the Chatter Admin account used for app creation.
3. Enter the previously copied **Security Token**.
4. Specify the days for messages that should be processed.



Advanced Configuration Options

To configure advanced options:

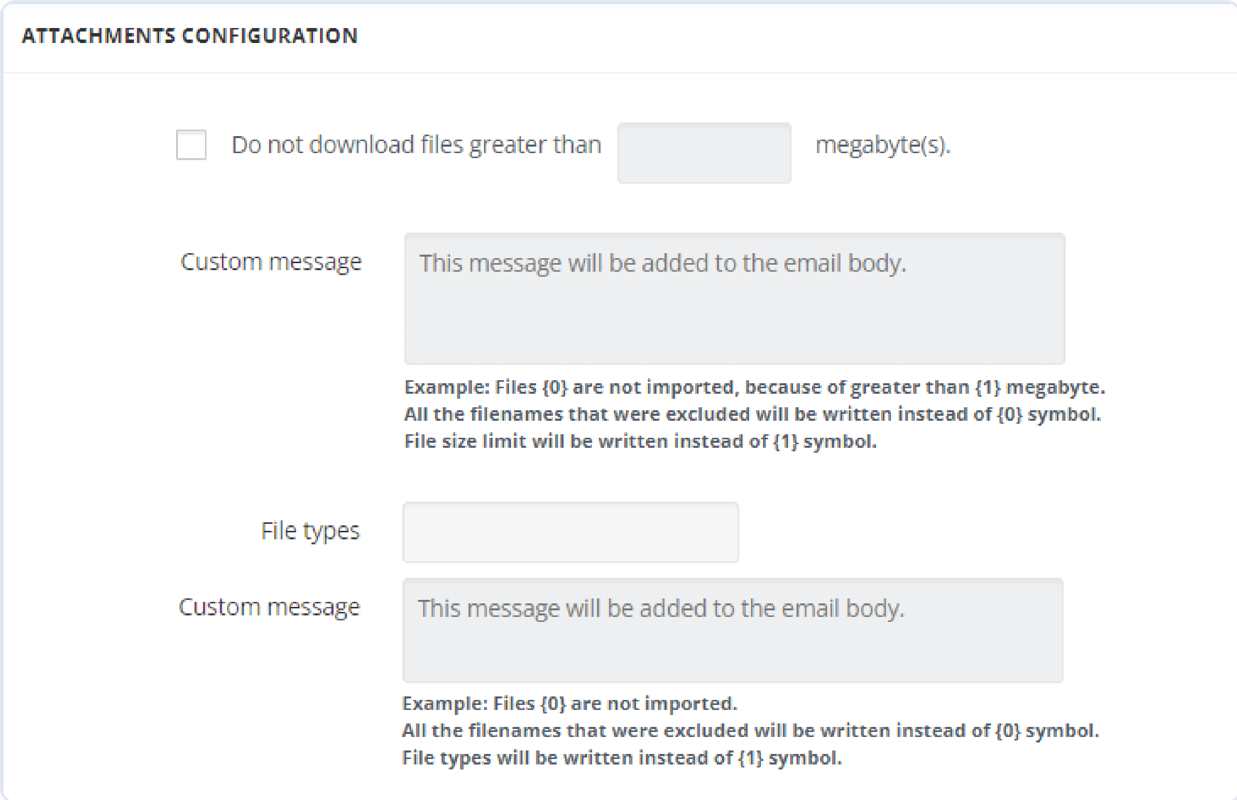
1. Specify the **Subject Prefix** in the subject line of imported emails. This is useful for organizing imported data, i.e., when multiple sources share a common target.

   > **Note:** Not applicable to the EV Folder target.

2. Specify **Do not download data modified before** and **Do not download data modified after** to allow cutting off data outside the set date range. If the before date is set to 08/17/2024 and the after date is set to 08/25/2024, only the data between these two dates will be downloaded. Data outside that range will be ignored. Note that both options can be used independently.

Attachments Configuration

- When the **Ignore Attachments** checkbox is enabled, all the attachments are excluded from the message which will enhance the collector performance. Each message will contain only information and the link of the excluded attachment.
- When **Do not download files greater than X megabyte(s)** is selected, the files bigger than the filled-in number of megabytes, are not downloaded. In **Custom Message** field, a text for those excluded files can be specified. E.g.,"Files {0} are not imported, because they are greater than {1) megabytes". {0} is used to add the name of the file and {1} is used to add the number of megabytes specified above.
- In the **File Types** field, the types of files that should not be downloaded can be specified in the following format: e.g., .txt | .xml. The vertical bar is used to separate the file types.



Supported Notifications

The importer supports the following notification types:

- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users
- Filters
- Targets
- Importer Settings

Cisco Webex Teams

Cisco Webex Teams enables people to meet, message, share, whiteboard, and call in a secure way, that meets legal, regulatory, and compliance mandates, and provides comprehensive business insights. All Cisco Webex Teams meetings allow screen sharing and a variety of tools for interactive creative work.

Activities Captured

- Direct messages during a call
- Persistent chats and channels
- Group members in a group or persistent chat
- Attachments

> **Note:** Deleted attachments are not captured due to API temporary limitations.

- Emojis
- Edited/Deleted messages
- Conversations related to all newly added users
- Message threading/post threading/group chats threading

> **Note:** The Webex environment allows inviting users from the other networks/domains (i.e., external users). These users can then create groups and teams like internal users. The chats/teams created by the External users are stored outside of the internal domain, i.e., in the Consumer organization storage. Consumer Organization owns this space. So, the data in the external domain are not captured by the collector.

Creating Cisco Webex Teams Application

To create an app:

1. Go to https://developer.webex.com/and log into your account.

> **Note:** The account should have the Full administrator permission and be a Compliance Officer. Permissions for full administrator privileges can be checked at https://admin.webex.com/users > Select User > Administrator Roles under Organization Administrator Roles and Functional Administrator Roles accordingly.

2. When you are logged in and permissions are set, click **Start Building Apps**.
3. Choose **Create an Integration**.
4. Fill in the **Integration Name**, **Contact Email**, **Icon**, **Description** fields.
5. In the **Redirect URI(s)** field, add the Redirect URL.

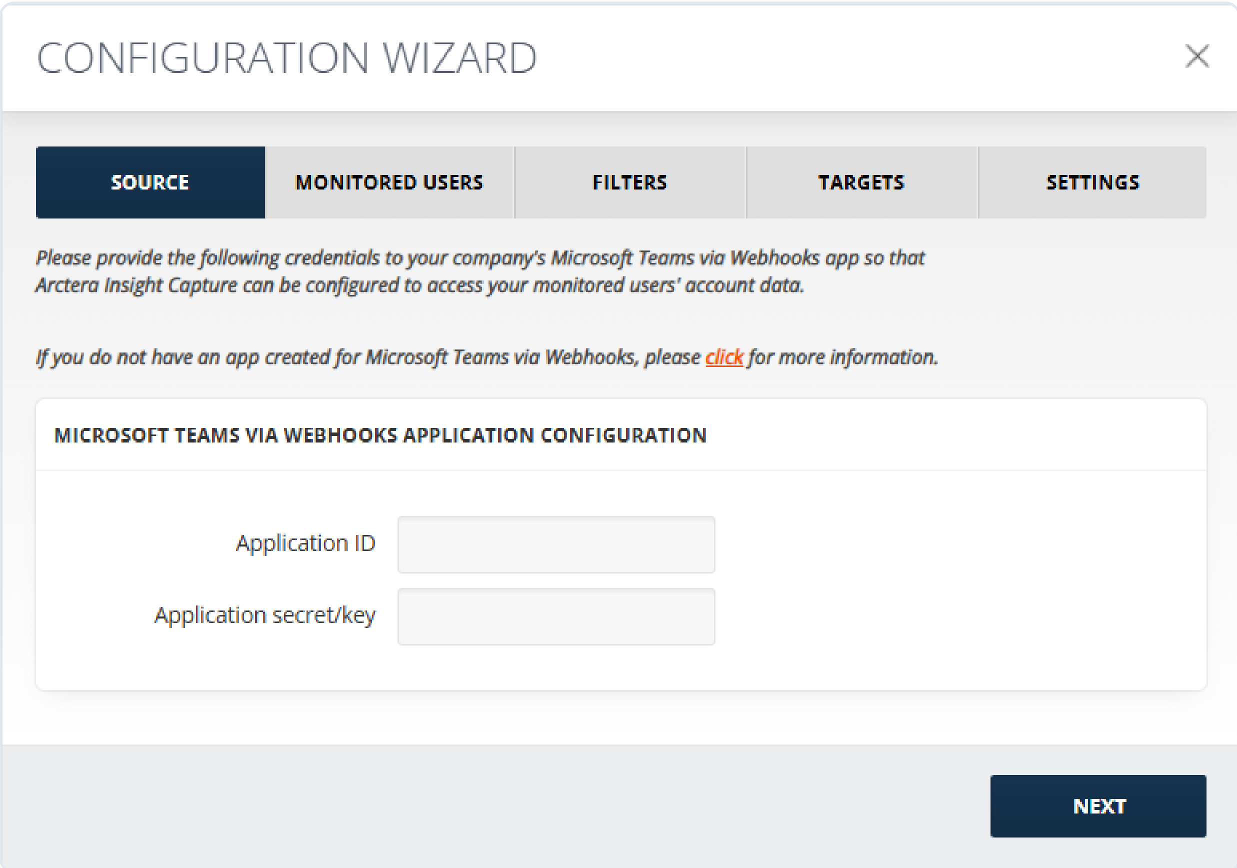
> **Note:** This can be found in the click information of the Source configuration.

6. Scroll down and select the following scopes:
    - **spark-admin:license_read**
    - **spark-admin:organizations_read**
    - **spark-admin:people_read**
    - **spark-admin:roles_read**
    - **spark-compliance:events_read**
    - **spark-compliance:memberships_read**
    - **spark-compliance:messages_read**
    - **spark-compliance:rooms_read**
    - **spark-compliance:team_memberships_read**
    - **spark-compliance:teams_read**
7. Click **Add Integration** at the bottom of the page.
8. Copy the **Client ID** and **Client Secret** and save them in a secure location.

Source Configuration

To configure the collector:

1. Add the Client ID into **Application ID** field.
2. Fill in **Application Secret/Key** with the Client Secret.
3. Click **NEXT**.



Timestamp Formatting

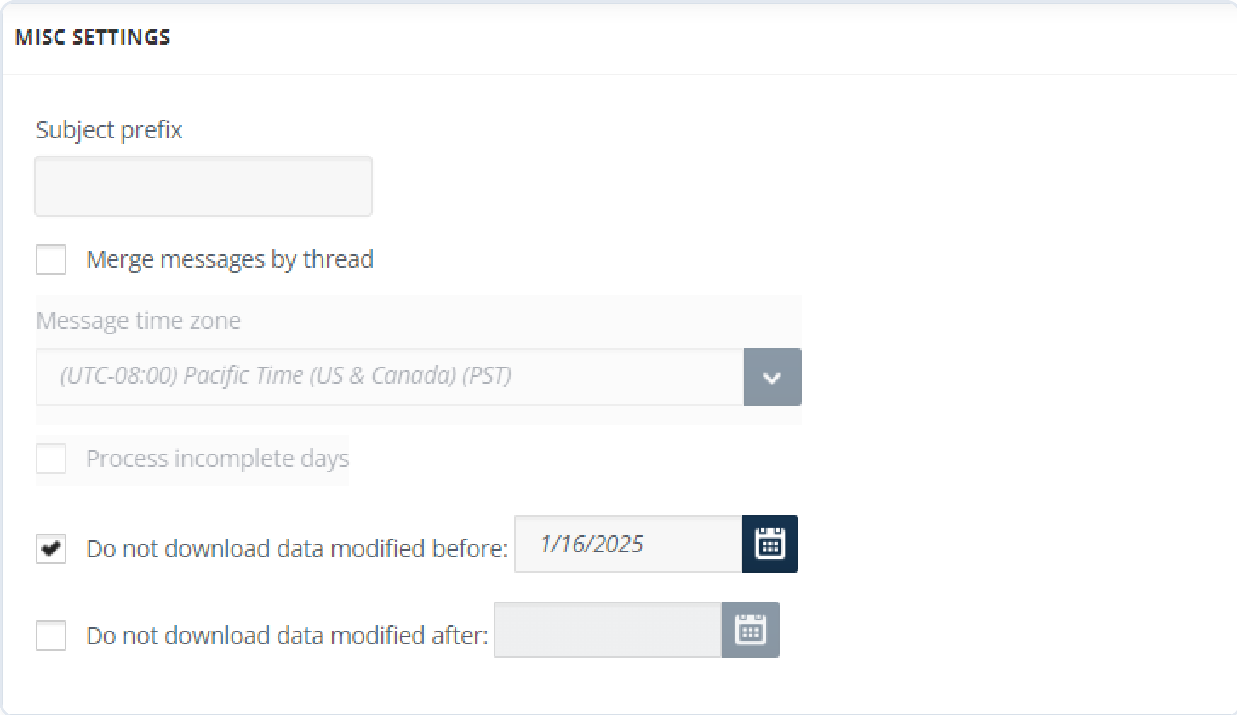
In addition to the primary stamp, a second timestamp can be enabled with its time zone. From the drop-down menu you can choose the time zone of the timestamp. The format of the timestamp in the output message can also be specified from the six options in the **Date Time Format** drop-down list.

Miscellaneous Settings

- The **Subject Prefix** is added to the subject line of imported emails. This is useful for organizing imported data, i.e., when multiple sources share a common target.

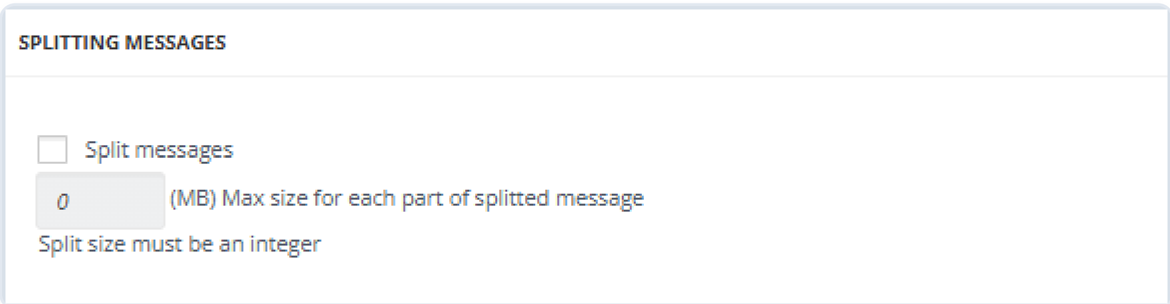
> **Note:** Not applicable to the EV Folder target.

- If the option **Merge Messages by Thread** is enabled, Arctera Capture retrieves the data from a thread and archives it as one message.
- Options **Do not download data modified before** and **Do not download data modified after** allow cutting off data outside the set date range. If the before date is set to 08/17/2021 and the after date is set to 08/25/2021, only the data between these two dates will be downloaded. Data outside that time frame will be ignored. Note that both options can be used independently as well.



Splitting Messages

Check the **Splitting messages** box in case you want to split big files into smaller files. The size of a split part of the message can be specified so that each part does not exceed the set size.



Attachments Configuration

- **Include original data as attachment**: If checked, the message original data is attached to the output file.

  > **Note:** Not applicable to the EV Folder target.

- **Ignore attachments**: If checked, all the attachments are excluded from the message enhancing the collector performance. Each message will contain info and the link to the excluded attachment.
- When **Do not download files greater than X megabyte(s)** is selected, the files bigger than the filled-in number of megabytes are not downloaded. In the **Custom Message** field, a text for

those excluded files can be specified. For example, "Files {0} are not imported, because they are greater than {1} megabytes". {0} is used to add the name of the file and {1} is used to add the number of megabytes specified above.

- In the **File Types** field, the types of files that should not be downloaded can be specified in the following format: e.g., .txt | .xml. The vertical bar is used to separate the file types.

Supported Notifications

The importer supports the following notification types:

- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users
- Filters
- Targets
- Importer Settings

Cloud9

Cloud9 Symphony is a unified communication and data capture platform designed for financial markets, enabling firms to securely store and analyze voice, video, and messaging interactions for trading, compliance, and auditing.

The Cloud9 collector allows organizations to capture and archive Cloud9 Symphony communications, integrating them into existing compliance and data retention systems. This ensures seamless access, regulatory compliance, and efficient management of critical financial interactions.

Activities Captured

- Calls

Setting up Cloud9

The Firm Admin of your organization must complete the following steps to generate an App Key and Secret in Cloud9.

1. Sign in to Cloud9 Portal.
2. In the left-hand navigation pane, click **API Keys**.
3. Under **Manage your Cloud9 API Keys**, select the firm.
4. Click **Generate API Key**.

To generate a Call Data App Key and App Secret

1. From the **API** drop-down list, select **Calls Data**.
2. Choose the appropriate **Environment**.
3. Enter allowed IP addresses in the **Whitelisted IP(s)** field.

   > **Note:** For more information, see How to allow IP addresses for correct operation of Arctera Capture.

4. Enter the relevant email(s) under **Owner Email(s)**.
5. Under **Scope of Access**, select **Read-Only**, then choose the following permissions:
   - **metadata**
   - **recordings**

6. Click **Generate Key & Secret.** Copy and securely store the generated Call Data API Key and Call Data Secret Key for source configuration.

To generate a **Management App Key** and **App Secret**:

1. From the **API** drop-down list, select **Management**.
2. Choose the appropriate **Environment**.
3. Enter allowed IP addresses in the **Whitelisted IP(s)** field.

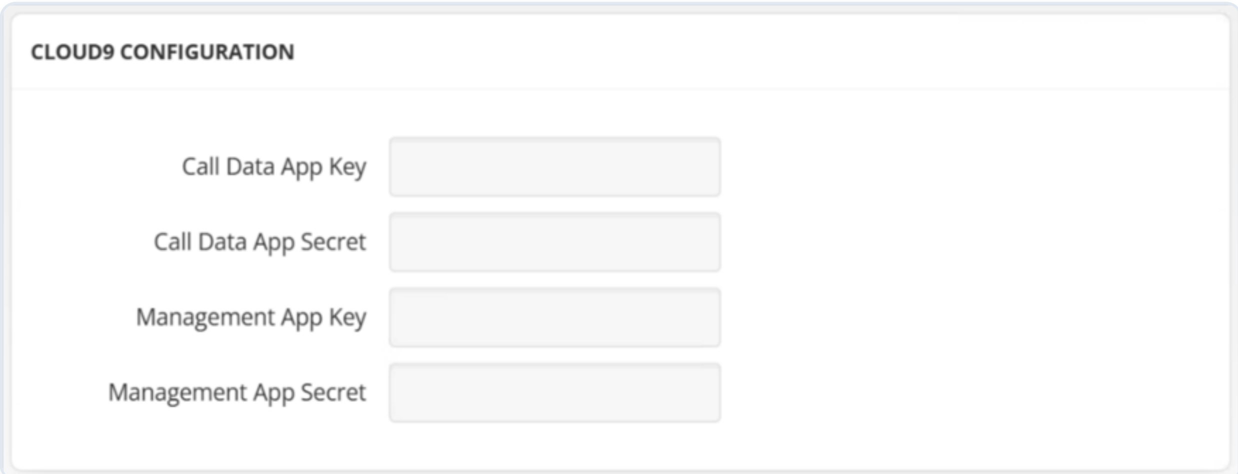
> **Note:** For more information, see How to allow IP addresses for correct operation of Arctera Capture.

4. Enter the relevant email(s) under **Owner Email(s)**.
5. Under **Scope of Access**, select **Read-Only**, then choose the following permission:
   - **users**
6. Click **Generate Key & Secret.** Copy and securely store the generated Management API Key and Management Secret Key for source configuration.

Source Configuration

To configure the Cloud9 application in Arctera Capture:

1. Enter the saved **Call Data API Key** and **Call Data Secret Key**.
2. Enter the saved **Management API Key** and **Management Secret Key**.



Advanced Configuration Options

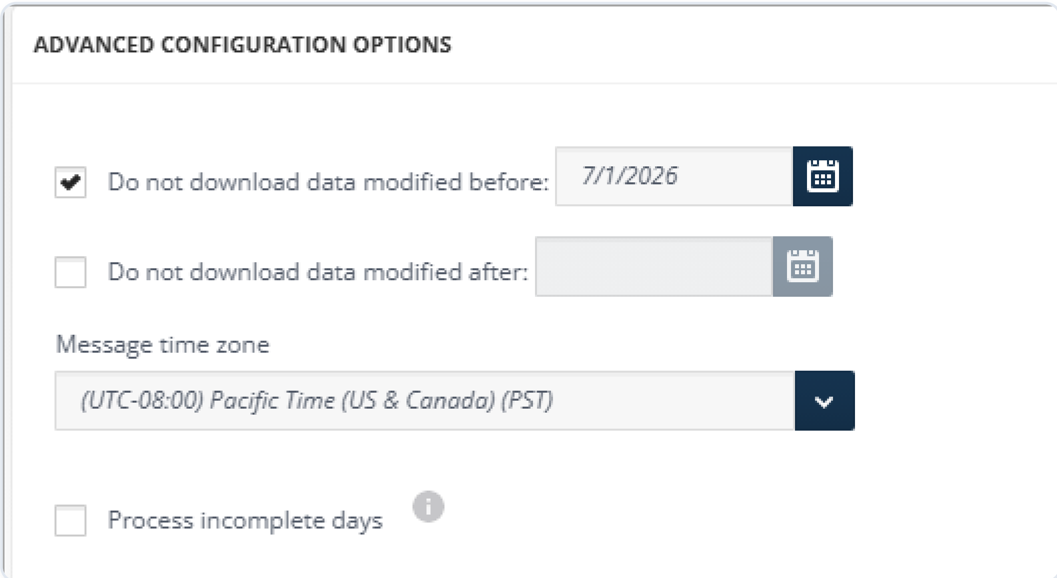
To configure the advanced options:

1. Specify **Subject Prefix** in the subject line of imported emails. This feature allows organizing imported data when multiple sources share a common target.

   > **Note:** Not applicable to the EV Folder target.

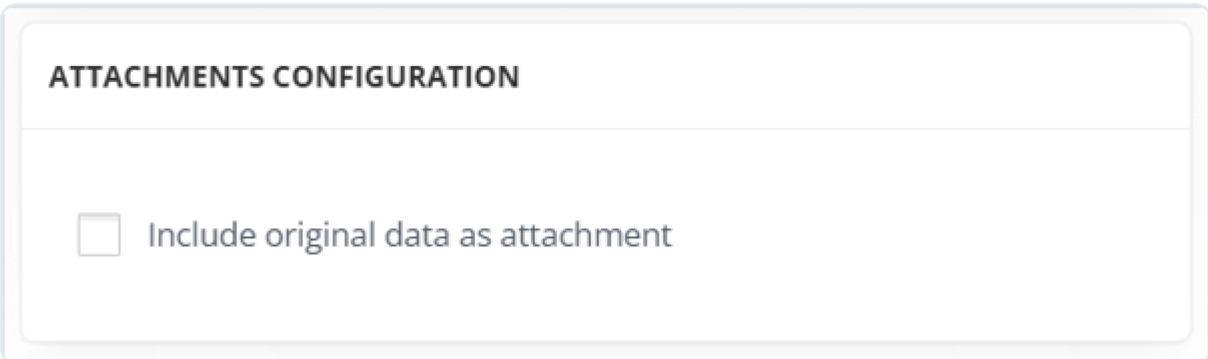
2. Specify **Do not download data modified before** and **Do not download data modified after** to allow cutting off data outside the set date range. If the before date is set to 08/17/2022 and the after date is set to 08/25/2022, only the data between these two dates will be downloaded. Data outside that time frame will be ignored. Note that both options can be used independently as well.

3. When the **Process incomplete days** option is enabled, the messages of the days that have not yet ended will be imported in a separate email.



Attachments Configuration

If **Include original data as attachment** is enabled, the JSON file will be attached to the output message.



Supported Notifications

The importer supports the following notification types:

- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users
- Filters
- Targets
- Importer Settings

Copilot

Copilot is an advanced AI-powered productivity assistant designed to enhance workplace efficiency by integrating seamlessly with Microsoft 365 applications. It helps users generate content, summarize information, automate tasks, and interact with enterprise data using natural language.

The Copilot collector captures Copilot-generated interactions, including prompts, responses, and contextual metadata. This enables organizations to archive AI-assisted communications for compliance, auditing, and knowledge management purposes. By integrating with enterprise archiving systems, the Copilot collector ensures transparency and governance in AI-driven workflows.

> **Note:** Copilot Studio is not supported by the collector.

Activities Captured

- User prompts
- AI responses

> **Note:** Messages may include attachments in case Copilot has been used directly within the document.

Notes

> **Note:** Due to current API limitations, the following constraints apply:

1. Captured data may contain auto-generated and progress reporting messages.
2. When Copilot is used directly within a Microsoft Word or Microsoft PowerPoint document, one AI response may include the attachment. All other AI responses and UI prompts will provide a URL to the attachment instead of including it.
3. The API may return identical AI-generated text responses multiple times, each with slightly different timestamps and unique `messageId` values.
4. Some API responses may contain repeated text blocks within the same adaptive card element, while the user interface displays only one version.
5. Some transient messages may appear in the conversation flow but disappear later, even though they remain in API responses.
6. Some Copilot messages may contain auto-generated filler text or unintelligible responses unrelated to the input.
7. Interaction logs are not captured. Copilot conversation history can be retrieved for up to 30 days at a time (an Arctera Capture limitation). For longer periods, multiple sessions are required.

Creating a Microsoft Entra ID Application

To authenticate via OAuth during the collector configuration, you need to create a Microsoft Entra ID Application.

To create an app:

1. Create an O365 account and open Azure Portal using the same credentials as for O365 (Global Admin).
2. Click **Microsoft Entra ID** at the top of the page and select **App Registration** from the left-side navigation pane.
3. Click the **+New registration** button.
4. Enter a **Name** for the application and click **Register**.
5. Find and make a note your **Application (client) ID** and **Directory(tenant) ID** as this is needed for configuring the collector in Arctera Capture.
6. In the navigation pane to the left, go to **Certificates & secrets**.
7. Click the **Upload certificate** button.
8. Select a certificate (public key) with one of the following file types: .cer,.pem, .crt, and click **Add**. For more information on how to create a certificate, see Creating a Certificate (Private and Public Keys).

Microsoft Entra ID Permissions

For permissions:

1. In the navigation pane to the left, click **API permissions**.
2. Click Microsoft Graph, and in the opened pane select **Application permissions**.
3. Get back to API permissions section, click \+ **Add a permission**, select Graph API and then **Application permissions**. These are the permissions you need to grant:
    - **AiEnterpriseInteraction: AiEnterpriseInteraction.Read.All**
    - **User: User.Read.All**
4. Grant all the above-mentioned permissions.
5. Get back to API permissions section, click \+ **Add a permission**, select SharePoint and then **Application permissions**. These are the permissions you need to grant:
    - **Sites: Sites.Read.All**

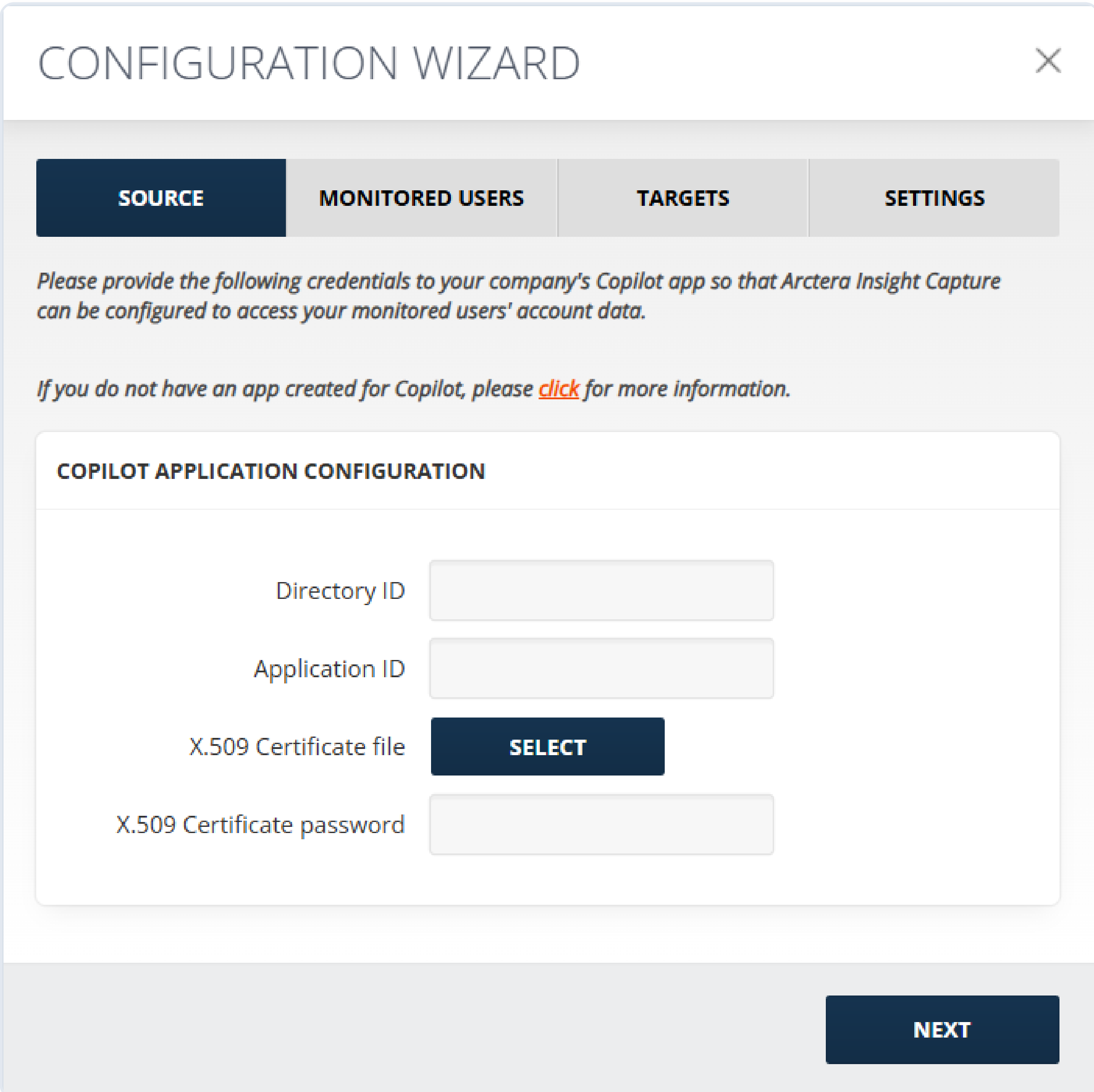
- **TermStore: TermStore.Read.All**
- **User: User.Read.All**

6. Grant all the above-mentioned permissions.

Source Configuration

For configuring the Copilot application:

1. Add the previously saved Directory (tenant) ID and Application (client) ID in the **Directory ID** and **Application ID** fields, respectively.
2. Click the **Select** button to upload the certificate and provide **X.509 Certificate password**. Click **Next**.



Timestamp Formatting

In addition to the primary stamp, a second timestamp can be enabled with its time zone. From the drop-down menu you can choose the time zone of the timestamp. The format of the timestamp in the output message can also be specified from the six options in the **Date Time Format** drop-down list.

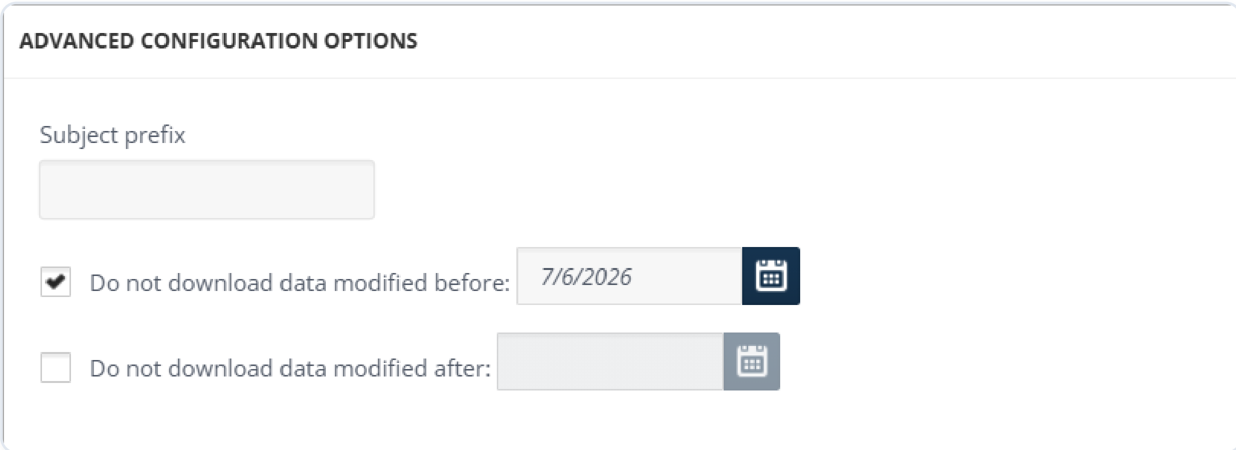
Advanced Configuration Options

To configure advanced options:

1. Specify the **Subject Prefix** in the subject line of imported emails. This is useful for organizing imported data, i.e., when multiple sources share a common target.

   > **Note:** Not applicable to the EV Folder target.

2. Specify **Do not download data modified before** and **Do not download data modified after** to allow cutting off data outside the set date range. If the before date is set to 08/17/2024 and the after date is set to 08/25/2024, only the data between these two dates will be downloaded. Data outside that range will be ignored. Note that both options can be used independently.

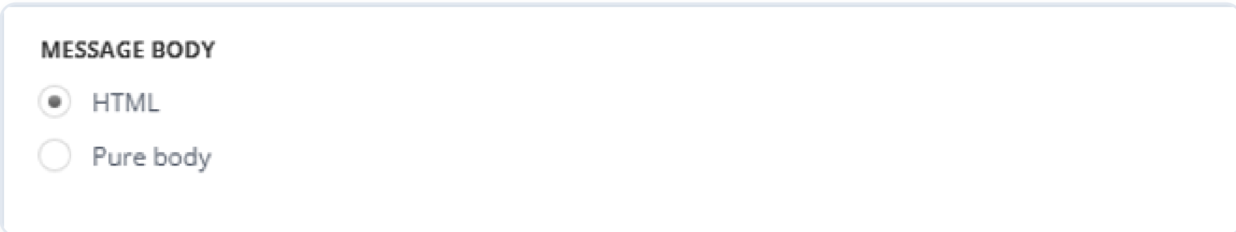


Message Body

> **Note:** This section is not applicable to the EV.Cloud target.

> This setting determines how imported messages are displayed in the target. There are the following output message body options:

- **HTML**: Displays the message in HTML format.
- **Pure body**: Displays the output message as plain text, without formatting or additional details.



Attachments Configuration

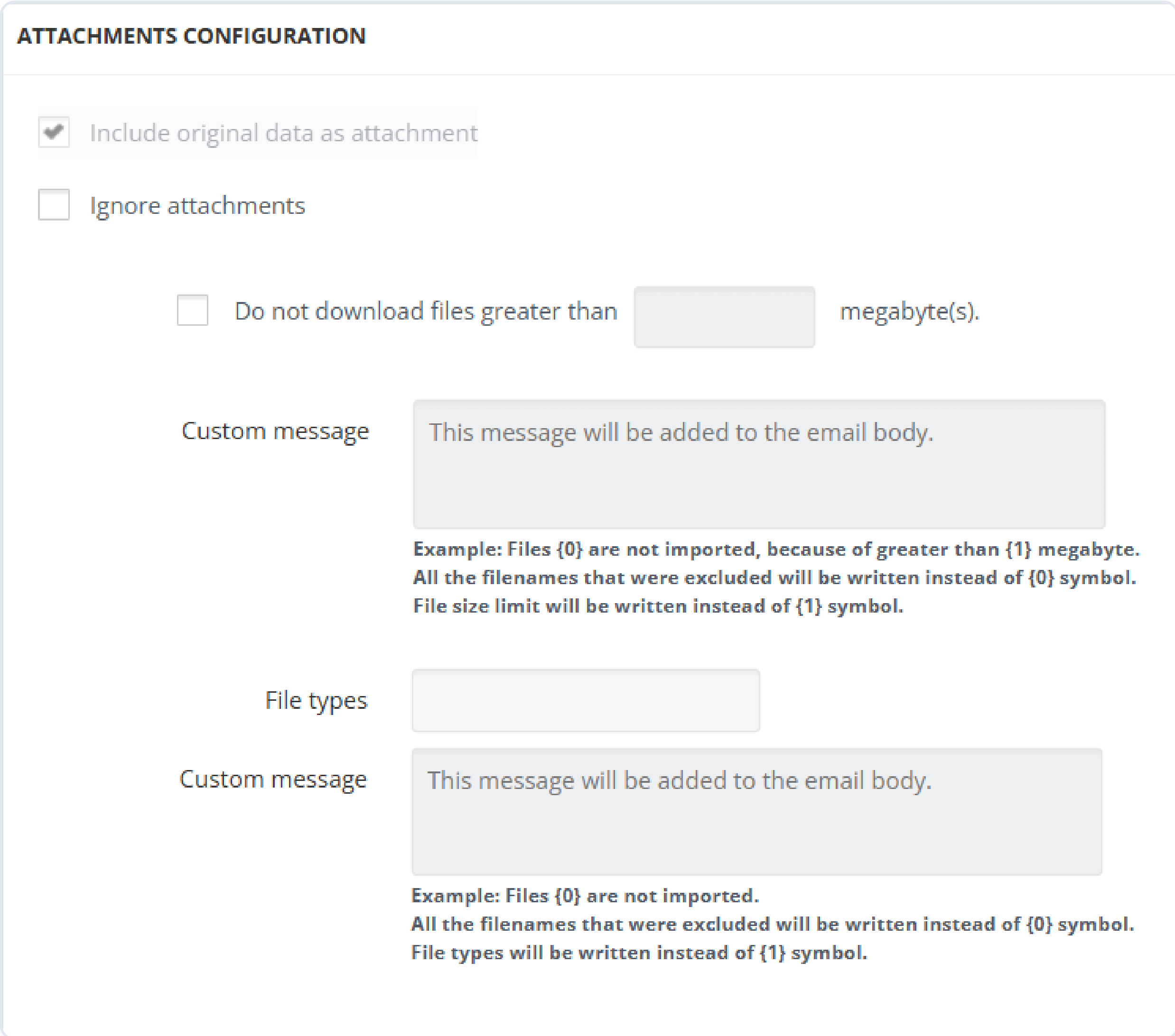
- **Include original data as attachment**: If checked, the message original data is attached to the output file.

  > **Note:** Not applicable to the EV Folder target.

- **Ignore attachments**: If checked, all the attachments are excluded from the message enhancing the collector performance. Each message will contain info and the link to the excluded attachment.
- When **Do not download files greater than X megabyte(s)** is selected, the files bigger than the filled-in number of megabytes, are not downloaded. In **Custom Message** field, a text for

those excluded files can be specified. E.g.,"Files {0} are not imported, because they are greater than {1) megabytes". {0} is used to add the name of the file and {1} is used to add the number of megabytes specified above.

- In the **File Types** field, the types of files that should not be downloaded can be specified in the following format: e.g., .txt | .xml. The vertical bar is used to separate the file types.



Supported Notifications

The importer supports the following notification types:

- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**

- **Importer data deleted**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users
- Filters
- Targets
- Importer Settings

Dropbox Business

Dropbox Business is a cloud-based file storage system. It is a secure storage for all your tools, content, and collaborators. This platform keeps your teams productive and your content safe by driving transformation across industries.

Activities Captured

- Files and file operations - added/copied/deleted/downloaded/edited/moved/ permanently deleted/renamed/restored/reverted/rolled back
- Comments - added/deleted/edited
- Sharing:
  - Shared content - add invitees/add members
  - Shared content - copy, view, unshare
  - Shared folder - create/mount/unmount
  - Shared link - copy/create/download/view

> **Note:** Events generated by external (anonymous) users are not captured.

Creating a Dropbox Application

The owner of your organization's Dropbox folder must perform these steps to create a Dropbox application.

To create an app:

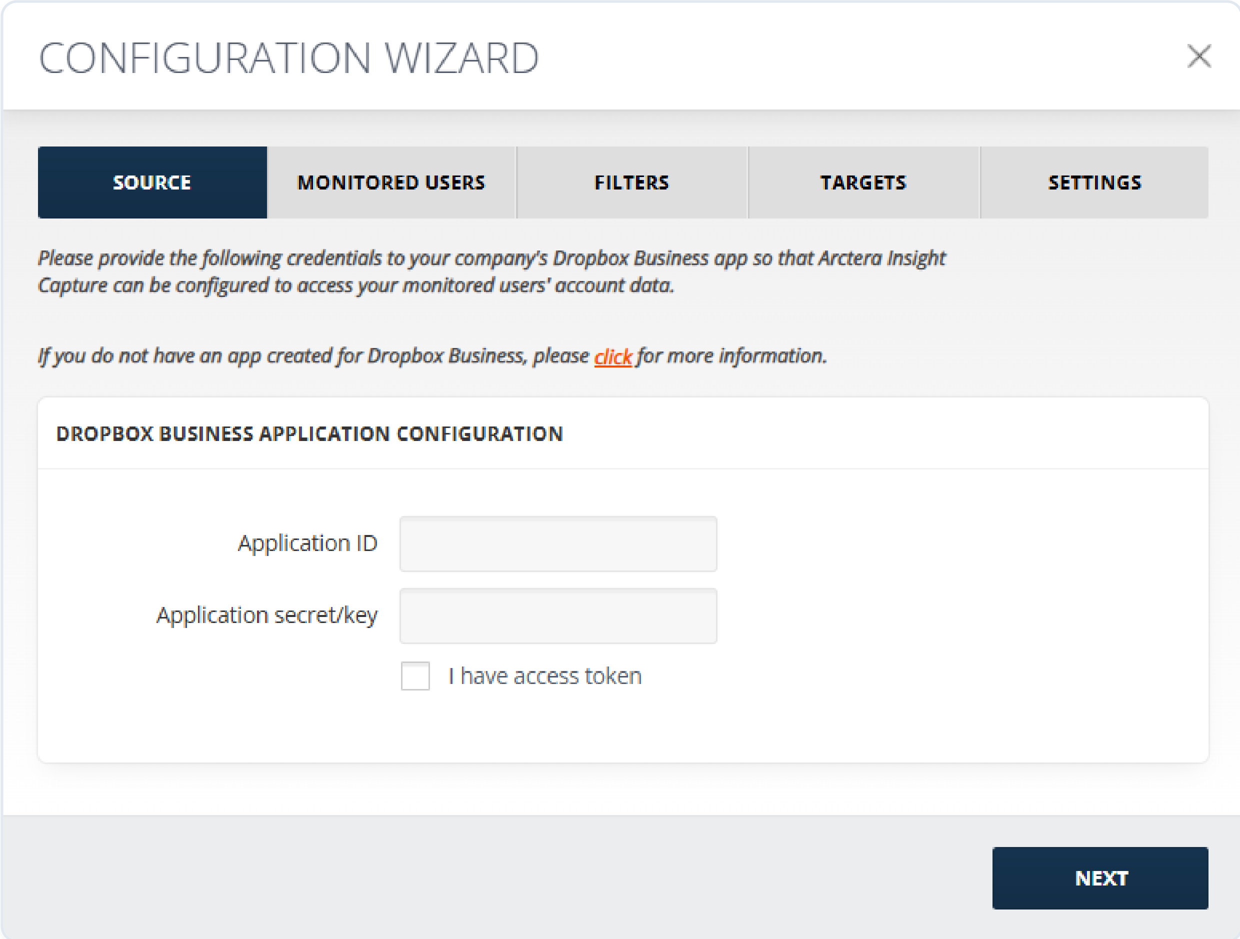
1. Log in to Dropbox and navigate to https://www.dropbox.com/developers.
2. At the top right corner, click **App console**.
3. Click **Create app**.
4. Choose an API: **Scoped access** and the type of access you need: **Full Dropbox** - Access to all files and folders in a user's Dropbox.
5. Name your app and click **Create app**.
6. On the opened **Settings** tab, copy and save the **App key** and **App secret** and then in the **Redirect URIs** field, add the redirect URL address.

    > **Note:** This can be found in the click information of the Source configuration.

Source Configuration

To configure the Dropbox Business collector:

1. In the **Application ID** field, add the App Key copied previously, and in **Application Secret/Key**, enter the copied Secret, click **NEXT**.



2. Grant Access to Box in the opened pop-up window. Make sure that pop-ups are not blocked by your browser.

Timestamp Formatting

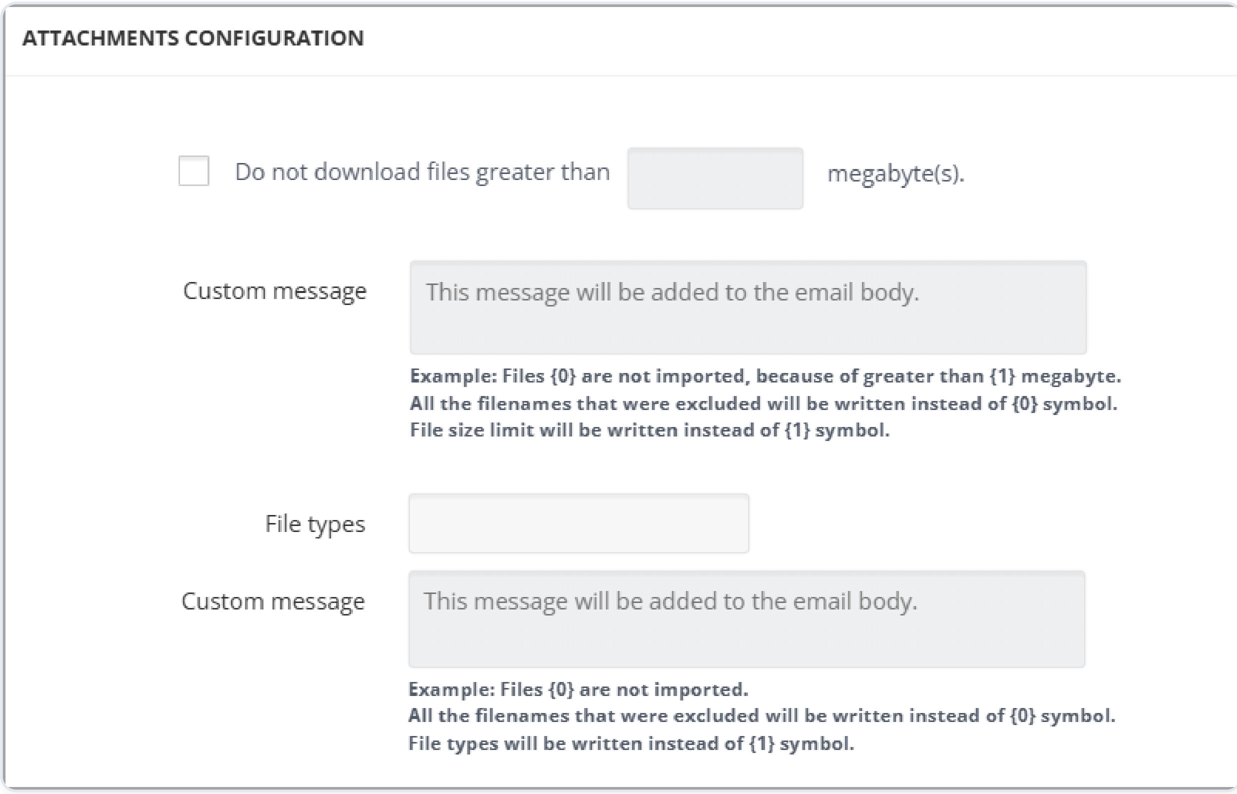
In addition to the primary stamp, a second timestamp can be enabled with its time zone. From the drop-down menu you can choose the time zone of the timestamp. The format of the timestamp in the output message can also be specified from the six options in the **Date time Format** drop-down list.

Attachments Configuration

- **Include original data as attachment**: If checked, the message original data is attached to the output file.

> **Note:** Not applicable to the EV Folder target.

- **Ignore attachments**: If checked, all the attachments are excluded from the message enhancing the collector performance. Each message will contain info and the link to the excluded attachment.
- When **Do not download files greater than X megabyte(s)** is selected, the files bigger than the filled-in number of megabytes are not downloaded. In the **Custom Message** field, a text for those excluded files can be specified. For example, "Files {0} are not imported, because they are greater than {1} megabytes". {0} is used to add the name of the file and {1} is used to add the number of megabytes specified above.
- In the **File Types** field, the types of files that should not be downloaded can be specified in the following format: e.g., .txt | .xml. The vertical bar is used to separate the file types.



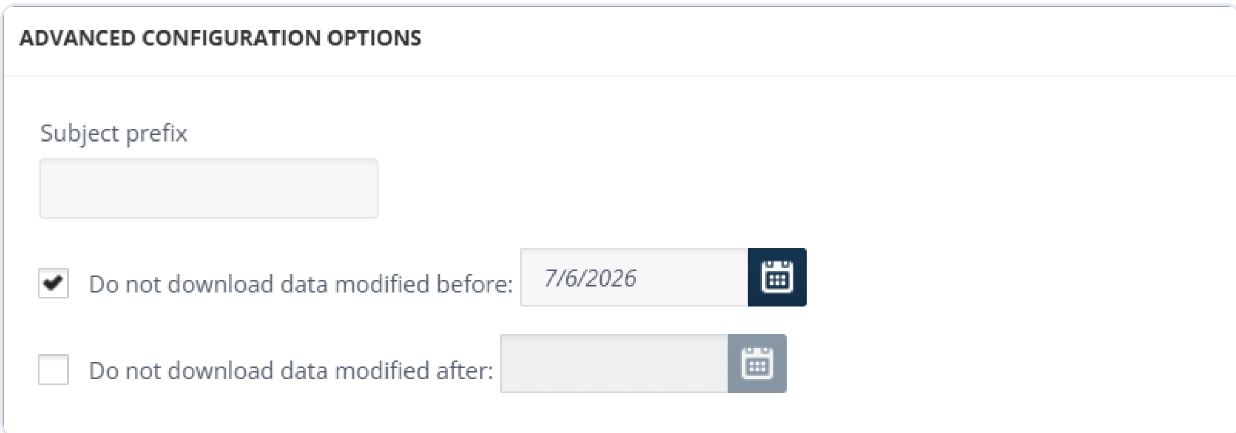
Advanced Configuration Options

To configure advanced options:

1. Specify the **Subject Prefix** in the subject line of imported emails. This is useful for organizing imported data, i.e., when multiple sources share a common target.

> **Note:** Not applicable to the EV Folder target.

2. Specify **Do not download data modified before** and **Do not download data modified after** to allow cutting off data outside the set date range. If the before date is set to 08/17/2024 and the after date is set to 08/25/2024, only the data between these two dates will be downloaded. Data outside that range will be ignored. Note that both options can be used independently.



Supported Notifications

The importer supports the following notification types:

- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users
- Filters
- Targets
- Importer Settings

Dubber Speik Recordings

Dubber Speik unified data capture and streaming engine not only captures conversation data (video, chat, SMS, voice) across your networks but also from any OTT Unified Communications platform.

> **Note:** Please reach out to your Dubber Speik representative to obtain your credentials.

Activities Captured

- Microsoft Teams calls
- Mobile phone calls

> **Note:** These activities must be recorded by Dubber Speik.

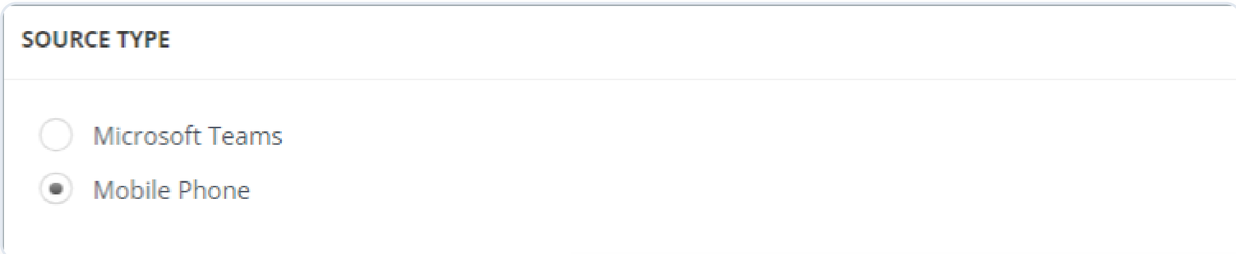
Source Configuration

> **Note:** These credentials should be provided to configure the Dubber Speik Recordings collector. Reach out to your Dubber/Speik representative to obtain your credentials.

Source Type

For Source Type configuration:

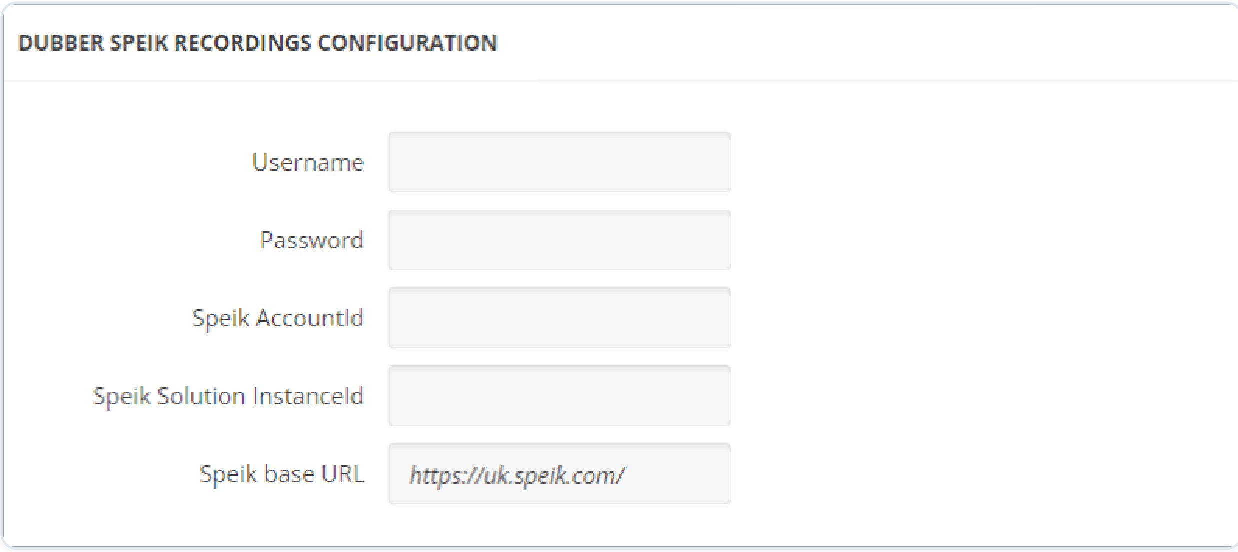
1. Enable **Microsoft Teams** to collect recordings from Microsoft Teams.
2. Enable **Mobile Phone** to collect recordings from mobile phone calls.



Dubber Speik Recordings Configuration

For Dubber Speik Recordings Configuration:

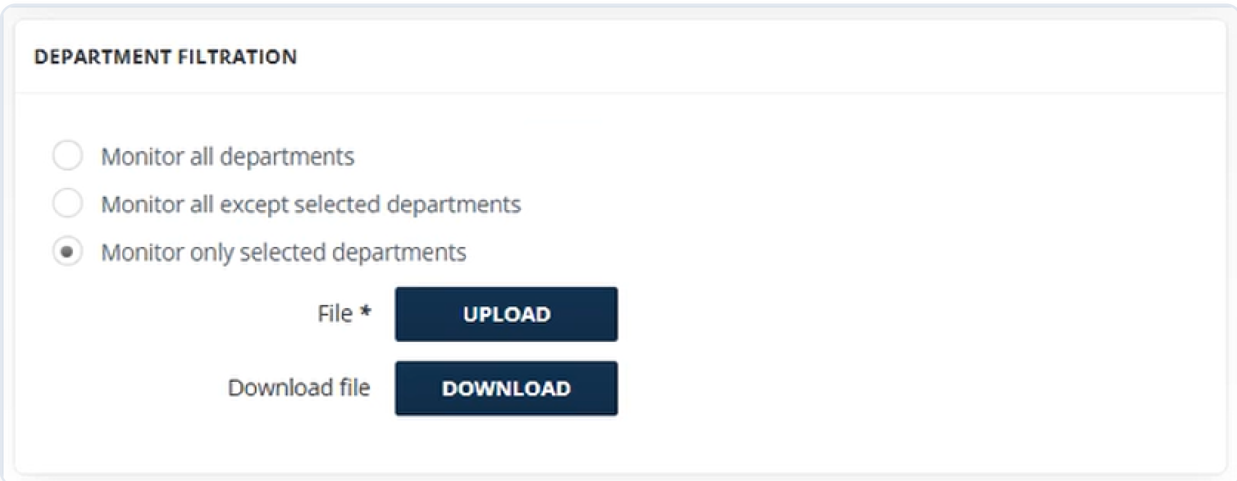
1. Enter Dubber Speik **Username** and **Password**.
2. Enter Speik **AccountId**.
3. Enter Speik **Solution InstanceId** and Speik **base URL**.



Department Filtration

To customize how departments are monitored, select one of the following options:

- **Monitor all departments**: All departments will be monitored. No further input is required.
- **Monitor all except selected departments**: Monitoring will exclude the departments you specify. A CSV upload interface will appear to allow you to provide the list of departments to exclude.
- **Monitor only selected departments**: Monitoring will be limited to the departments you specify. A CSV upload interface will appear to allow you to provide the list of departments to include.



To ensure proper functionality, uploaded CSV files must meet the following criteria:

- File Format: Must be a CSV file.
- File Size: Must be greater than 0 KB. Empty files will be rejected.
- Content Structure: Must contain a single column listing department names. No headers or additional columns are allowed.

Advanced Configuration Options

There are the following advanced options:

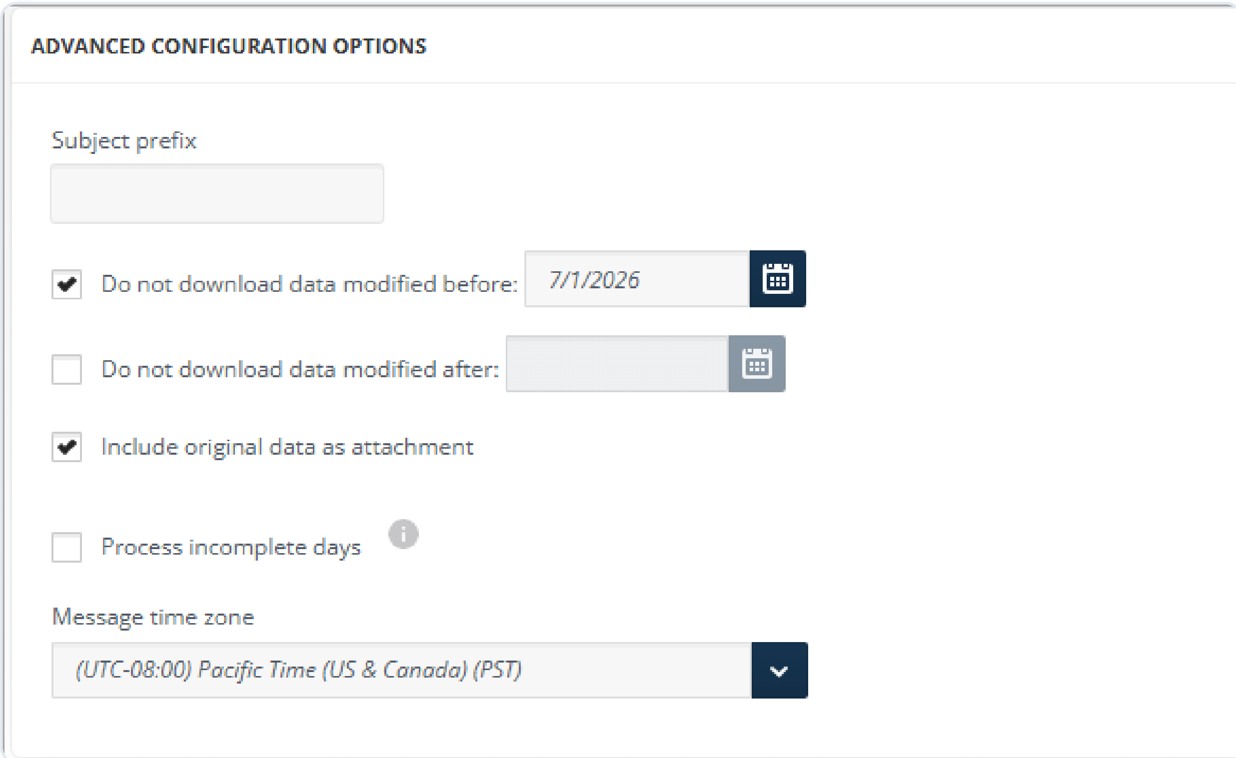
- The **Subject Prefix** feature will add a prefix before the message subject to facilitate the search in the target.

> **Note:** Not applicable to the EV Folder target.

- Options **Do not download data modified before** and **Do not download data modified after** allow cutting off data outside the set date range. If the before date is set to 08/17/2023 and the after date is set to 08/25/2022, only the data between these dates will be downloaded. Data outside that time frame will be ignored.

> **Note:** Both options can be used independently as well.

- The **Include original data as attachment** feature allows including/excluding original data as attachment by enabling/disabling the corresponding checkbox.



- When the **Process incomplete days** option is enabled, the messages of the days that have not yet ended will be imported in a separate email.

Reconciliation

Select **Enable Capture reconciliation** to reconcile the number of messages that Arctera Capture processes against the message count reported by the source.

Supported Notifications

The importer supports the following notification types:

- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users (N/A)
- Filters
- Targets
- Importer Settings

Dubber Speik SMS

Dubber Speik unified data capture and streaming engine not only captures conversation data (video, chat, SMS, voice) across your networks but also from any OTT Unified Communications platform.

> **Note:** Please reach out to your Dubber Speik representative to obtain your credentials.

Activities Captured

- SMSs

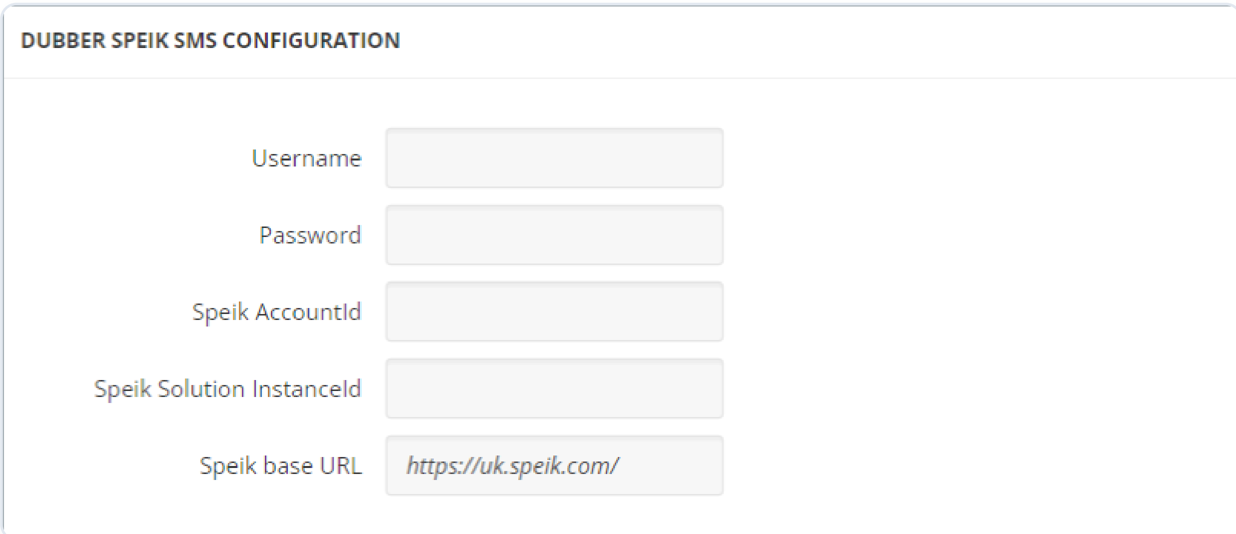
Source Configuration

To set up the collector in Arctera Capture, please reach out to your Dubber Speik representative to obtain your credentials.

Dubber Speik SMS Configuration

For Dubber Speik SMS Configuration:

1. Enter Dubber Speik **Username** and **Password**.
2. Enter Speik **AccountId**.
3. Enter Speik **Solution InstanceId** and Speik **base URL**.



> **Note:** These credentials should be provided to configure the Dubber Speik SMS collector. Please reach out to your Dubber/Speik representative to obtain your credentials.

Advanced Configuration Options

There are the following advanced options:

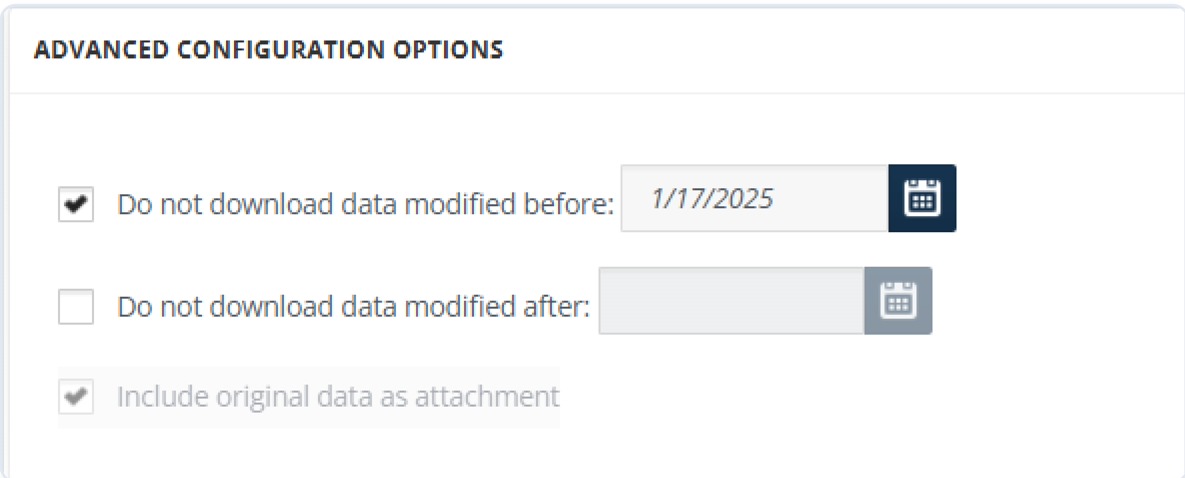
- The **Subject Prefix** feature will add a prefix before the message subject to facilitate the search in the target.

> **Note:** Not applicable to the EV Folder target.

- Options **Do not download data modified before** and **Do not download data modified after** allow cutting off data outside the set date range. If the before date is set to 08/17/2023 and the after date is set to 08/25/2022, only the data between these dates will be downloaded. Data outside that time frame will be ignored.

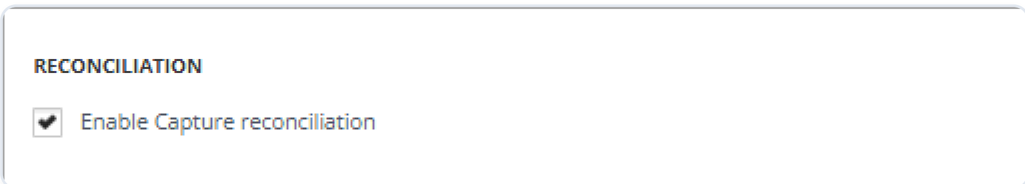
> **Note:** Both options can be used independently as well.

- The **Include original data as attachment** feature allows including/excluding original data as attachment by enabling/disabling the corresponding checkbox.



Reconciliation

Select **Enable Capture reconciliation** to reconcile the number of messages that Arctera Capture processes against the message count reported by the source.



Supported Notifications

The importer supports the following notification types:

- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users (N/A)
- Filters
- Targets
- Importer Settings

EML

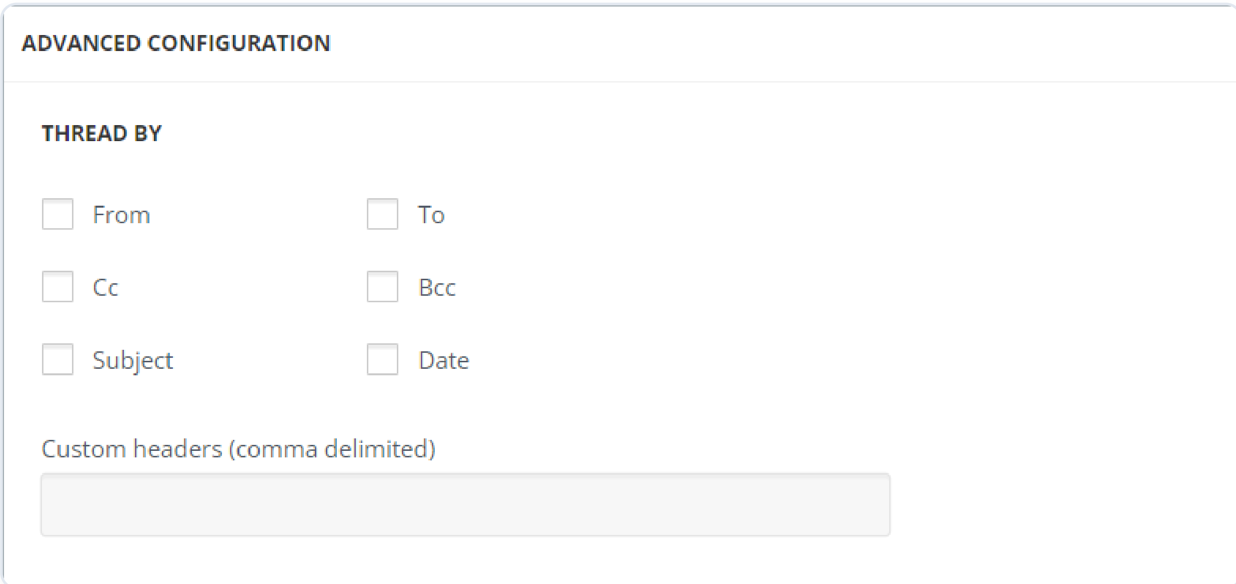
The EML collector is used for importing EML data from Symphony. EML format is widely used by various compliance and archiving solutions and helps the organization avoid the need to develop a specific-source parser. The collector is used for importing EML data from Symphony. Files with the MD5 extension should be excluded from the import, as content from Symphony is exported in a single ZIP file containing EML files for each active conversation. There are some drawbacks in using EML instead of the Symphony collector for processing files from Symphony. They include:

- EML does not have a subject line to do conversation threading when searching.
- EML has poorer look (XML to HTML looks better than EML).
- EML misses information about room created, when joined, etc..

Advanced Configuration

This section allows threading based on:

- **From**
- **Cc**
- **Subject**
- **To**
- **BCC**
- **Date**



You can also specify a custom header (comma-delimited) in the corresponding field.

Source Configuration

For information on how to configure the following sections of the **Source** tab, see:

- File Source Configuration
- PGP Configurations
- Quarantine Location
- Miscellaneous Settings

Timestamp Formatting

In addition to the primary stamp, a second timestamp can be enabled with its time zone. From the drop-down menu you can choose the time zone of the timestamp. The format of the timestamp in the output message can also be specified from the six options in the **Date Time Format** drop-down list.

Supported Notifications

The importer supports the following notification types:

- **Quarantine file**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Failed to quarantine file**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**

- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users (N/A)
- Filters
- Targets
- Importer Settings

EWS

Exchange Web Services (EWS) is an application program interface (API) that allows programmers to access Microsoft Exchange items such as calendars, contacts, and email. EWS, which first became available in Exchange Server 2007, provides administrators with the flexibility to store, retrieve, move, and modify email and related data for a single user, a group of users or an entire Exchange Server organization on an Exchange server. EWS can be useful for migrating Exchange data on-premises or to a third-party host in the cloud.

Arctera Capture retrieves data from Exchange servers via EWS.

Activities Captured

- Messages
- Meeting requests
- Meeting cancellations
- Appointments

Providing Necessary Permissions to the Account

To provide necessary permissions:

1. Go to **Admin Portal**.
2. Log into your account if you are not logged in yet.
3. Open Exchange admin center and go to permissions.
4. Double click Discovery Management to open its settings.

5. Click **+** under the **Roles** section to add roles.
6. Add ApplicationImpersonation, Mailbox Import Export, and Mailbox Search to select the administrator roles that correspond to the Exchange features and services that members of this role group should have permissions to manage and click **OK**.

> **Note:** Impersonator user must haveMailbox Searchpermission if on the **Monitored users** tab ALL is selected.

7. Click **+** under **Members** section to select the members of that role group.
8. Click **Save** in Discovery Management settings.

Setting Up Security and Compliance for Microsoft 365

To set up Microsoft 365 Security and Compliance:

1. Navigate to Information Governance website in the Microsoft Compliance center.
2. Click **+New retention policy** to start the setup wizard.
3. Add a **Name** and a **Description** for the policy and click **Next**.
4. Choose the applications to apply the retention policy to. You can either select Apply policy only to content in Exchange email, public folders, Office 365 groups, OneDrive, and SharePoint documents.
5. Once you choose the locations where the retention policy applies, click **Next**.
6. Set the retention period of the messages along with other options. Configure the settings so that they meet your compliance requirements and click **Next**. Review the settings that you have chosen. If everything is correct, click **Submit**.

> **Note:** It would take up to 1 day to apply the retention policy to the locations you chose.

Microsoft Entra ID App Creation

To authenticate via OAuth during the collector configuration, you need to create a Microsoft Entra ID Application.

To create an app:

1. Create an O365 account and open Azure Portal using the same credentials as for O365 (Global Admin).

2. Click **Microsoft Entra ID** at the top of the page and select **App Registration** from the left-side navigation pane.
3. Click the **+New registration** button.
4. Enter a **Name** for the application and click **Register**.
5. Find and make a note your **Application (client) ID** and **Directory(tenant) ID** as this is needed for configuring the collector in Arctera Capture.
6. In the navigation pane to the left, go to **Certificates & secrets**.
7. Click the **Upload certificate** button.
8. Select a certificate (public key) with one of the following file types: .cer,.pem, .crt, and click **Add**. For more information on how to create a certificate, see Creating a Certificate (Private and Public Keys).

Microsoft Entra ID Permissions

For permissions:

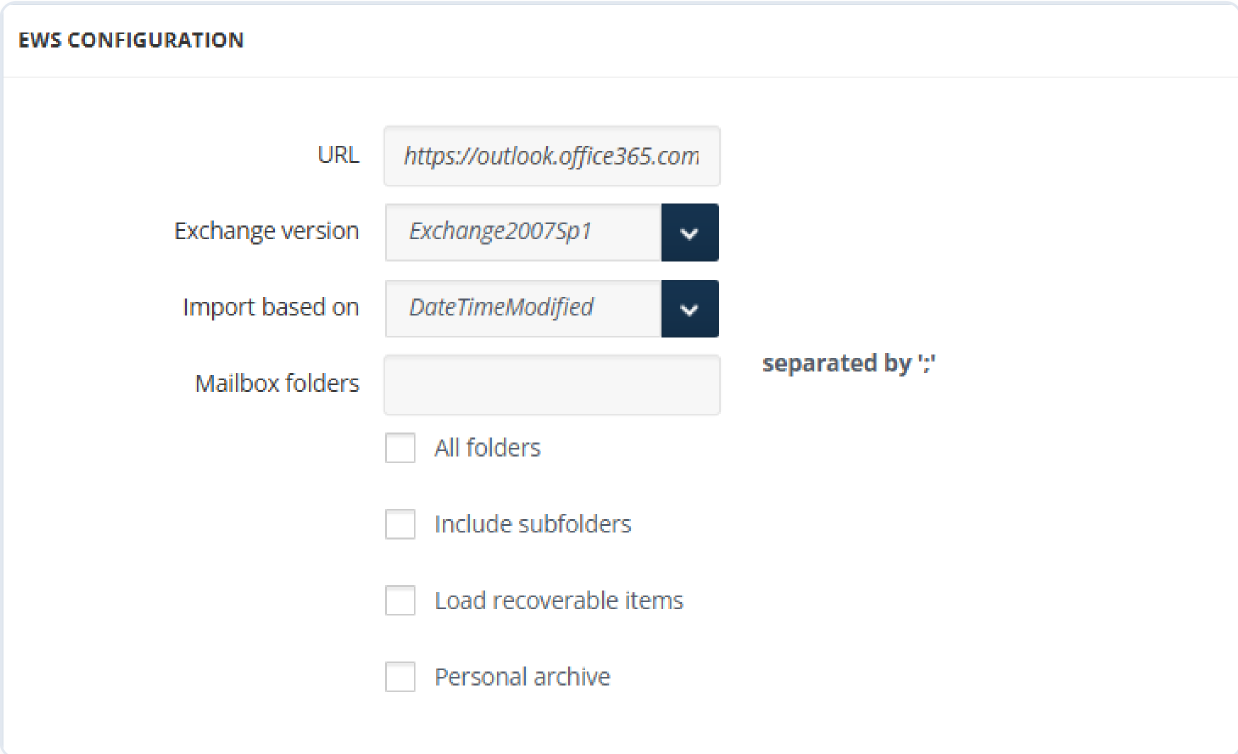
1. In the navigation pane to the left, click **API permissions**.
2. Click Microsoft Graph, and in the opened pane select **Application permissions**.
3. Add the following permissions:
   - User: User.Read.All
4. Add the Office 365 Exchange Online permissions (previously Exchange) - full_access_as_app, MailboxSettings: MailboxSettings.Read.
5. Grant all the above-mentioned permissions.

Source Configuration

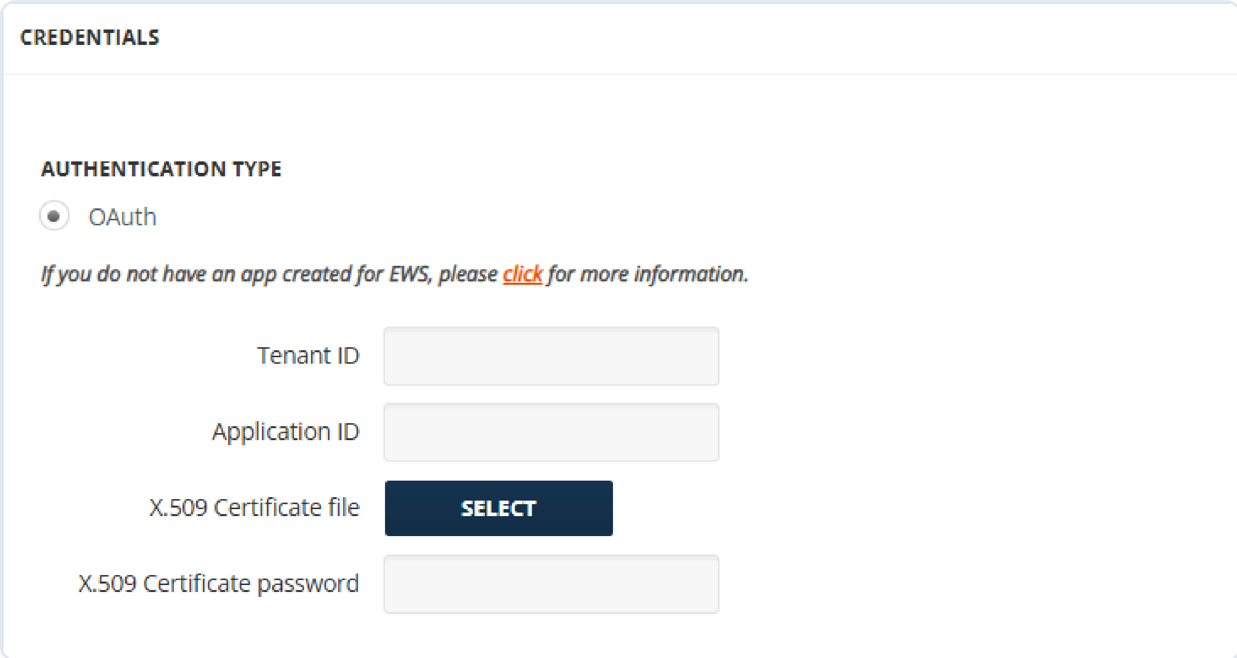
To configure the EWS collector:

1. Specify the **URL** for the EWS collector.
2. Select the required `Exchange version` from the drop-down list.
3. Choose if the import should be done by last modification date (DateTimeModified) or by creation date (OriginalDateTime). The cut-off date options change accordingly.
4. Fill in the **Mailbox Folder** from where the data should be imported. If you have more than one Mailbox Folder, separate each name with a semicolon.
5. To process data within all the folders, check **All folders**.

6. To process data within the subfolders of the specified mailboxes, check **Include subfolders**.
7. To search for the mentioned mailbox folders in the recovery route folders, check `Load recoverable items` if the Exchange Version is not Exchange2007 Sp1.
8. Enable **Personal archive** to process only the archived information.

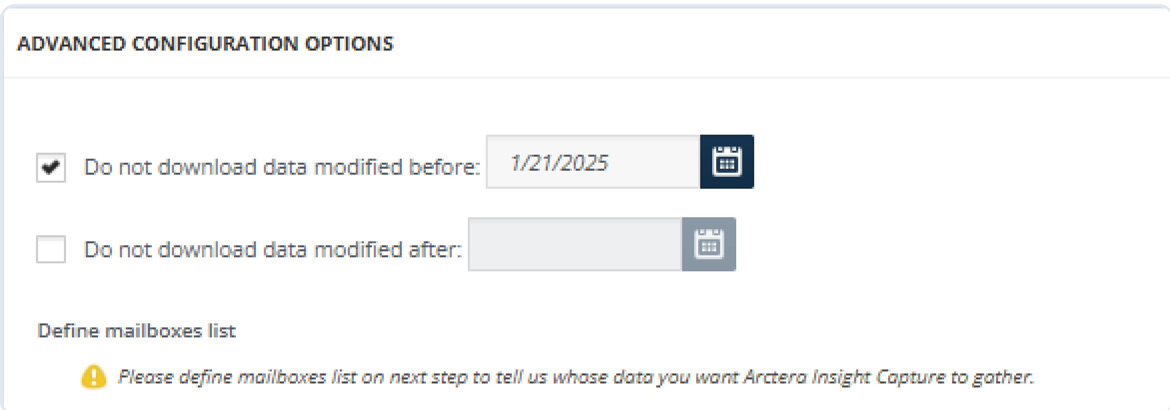


9. Provide **Application ID** and **Tenant ID**.
10. Select the **X.509 Certificate** file.
11. Enter the **X.509 Certificate password**. The **Certificate thumbprint** field will be auto populated in case the collector was previously configured by uploading a certificate.



> **Note:** For step-by-step instructions on how to get Application ID and Tenant ID, see Microsoft Entra ID App Creation.

12. For Advanced Configuration Options, **Do Not Download Data Modified/Created Before** and **Do Not Download Data Modified/Created After**, allow cutting off data outside the set date range. If the before date is set to 08/17/2021 and the after date is set to 08/25/2021, only the data between these two dates will be downloaded. Data outside that time frame will be ignored. Note that both options can be used independently as well.

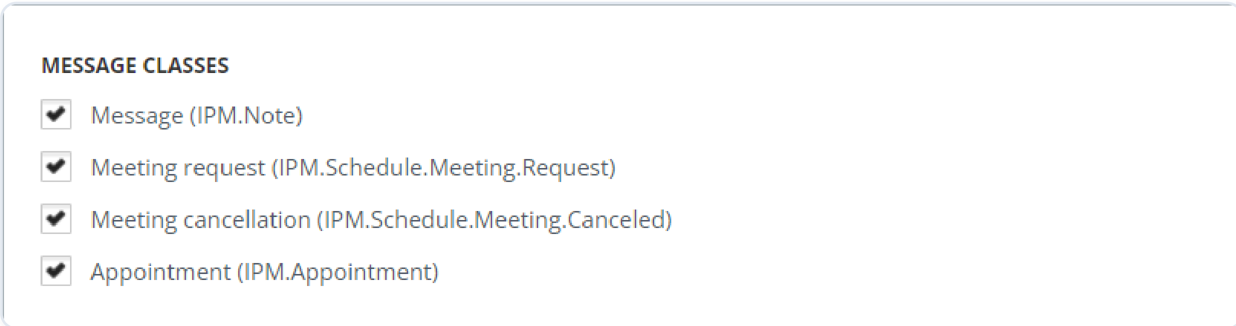


13. Select the **Message Class** you would like Arctera Capture to import and then click **Save**.

A Message Class is an internal identifier that Microsoft Outlook and Microsoft Exchange utilize to locate and activate forms. There are the following Message Class types that can be imported from Exchange:

- Message (IPM.Note)

- Meeting Request (IPM. Schedule.Meeting.Request)
- Meeting Cancellation (IPM.Schedule.Meeting.Canceled)
- Appointment (IPM.Appointment)



To include messages irrespective of their Message Class, select all of them.

History Tracking

Based on the provided information, there is a chance to monitor a certain time frame but get a message with a timestamp that is out of the specified frame. This case is applicable when import is based on DateTimeModified.

Supported Notifications

The importer supports the following notification types:

- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users
- Filters
- Targets
- Importer Settings

Exchange Graph API

Microsoft Exchange is a business-class email app which gives you a focused inbox that prioritizes important messages and adapts to your work style, so you can get more done - faster. Arctera Capture retrieves data from Exchange servers via Graph API.

Activities Captured

- Messages
- Appointments
- Meeting requests
- Meeting cancellations

Microsoft Entra ID App Creation

To authenticate for the collector configuration, you need to create a Microsoft Entra ID Application.

To create an app:

1. Create an O365 account and open Azure Portal using the same credentials as for O365 (Global Admin).
2. Click **Microsoft Entra ID Directory** at the top of the page and select **App Registration** from the left-side navigation pane.
3. Click the **+New registration** button.
4. Enter a **Name** for the application and click **Register**.
5. Find and make a note your **Application (client) ID** and **Directory(tenant) ID** as this is needed for configuring the collector.
6. In the navigation pane to the left, go to **Certificates & secrets**.
7. Click the **Upload certificate** button.

8. Select a certificate (public key) with one of the following file types: .cer,.pem, .crt, and click **Add**. For more information on how to create a certificate, see Creating a Certificate (Private and Public Keys).

Microsoft Entra ID Permissions

For permissions:

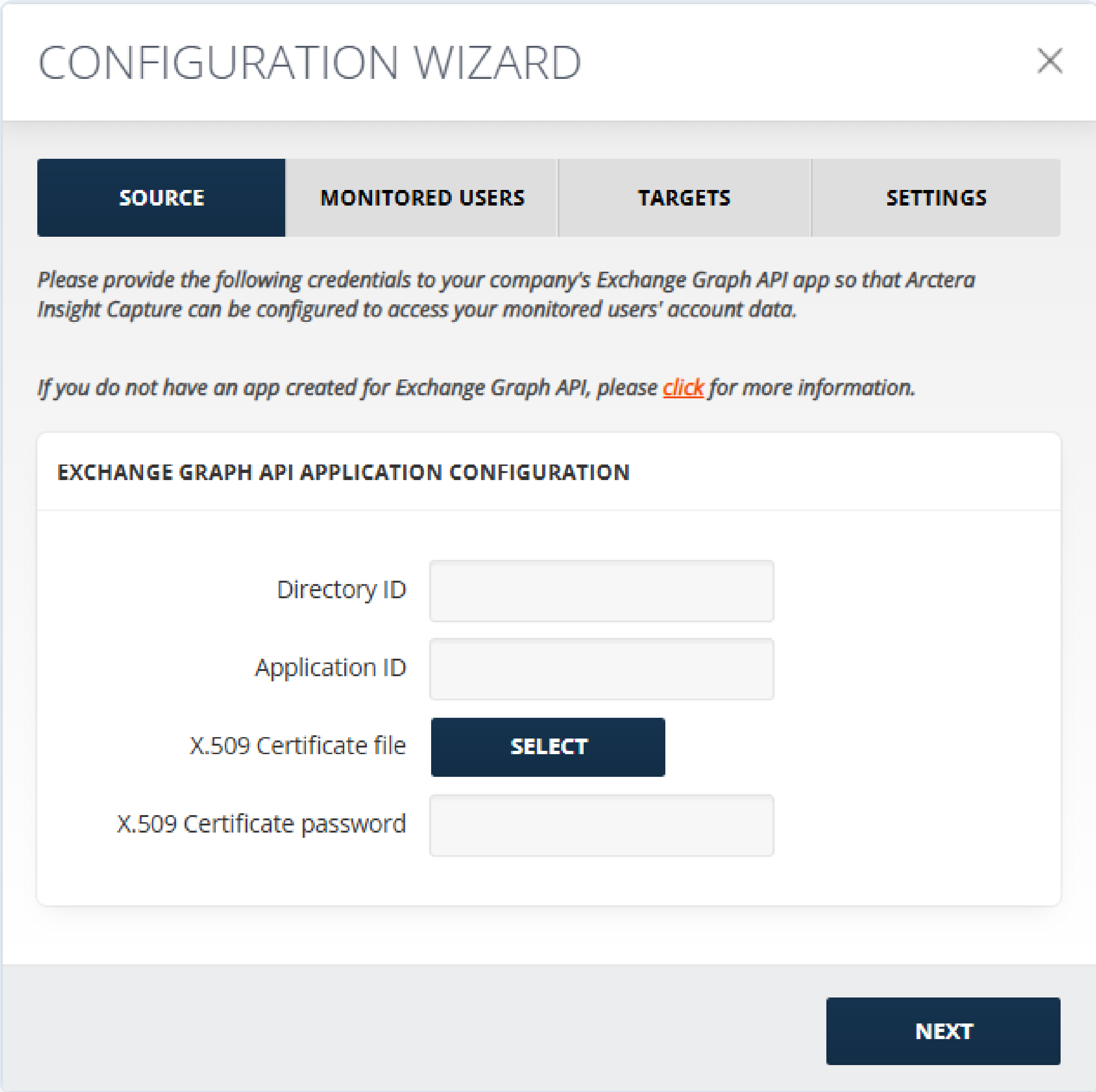
1. In the navigation pane to the left, click **API permissions**.
2. Click Microsoft Graph, and in the opened pane select **Application permissions**.
3. Add the following permissions:
   - User: User.Read.All
   - Mail: Mail.ReadBasic.All
   - Mail: Mail.Read
   - Calendars: Calendars.Read
   - MailboxItem: MailboxItem.Read.All
4. Grant all the above-mentioned permissions.

Source Configuration

To configure the Exchange Graph API collector:

1. In the new window opened, add **Application ID**, and **Application Secret/Key**.
2. Select the **X.509 Certificate** file and enter the **X.509 Certificate password**. The **Certificate thumbprint** field will be auto populated in case the collector was previously configured by uploading a certificate.

> **Note:** You can copy the Application ID from the Microsoft Entra ID > App Registrations> \<your app name\> section.



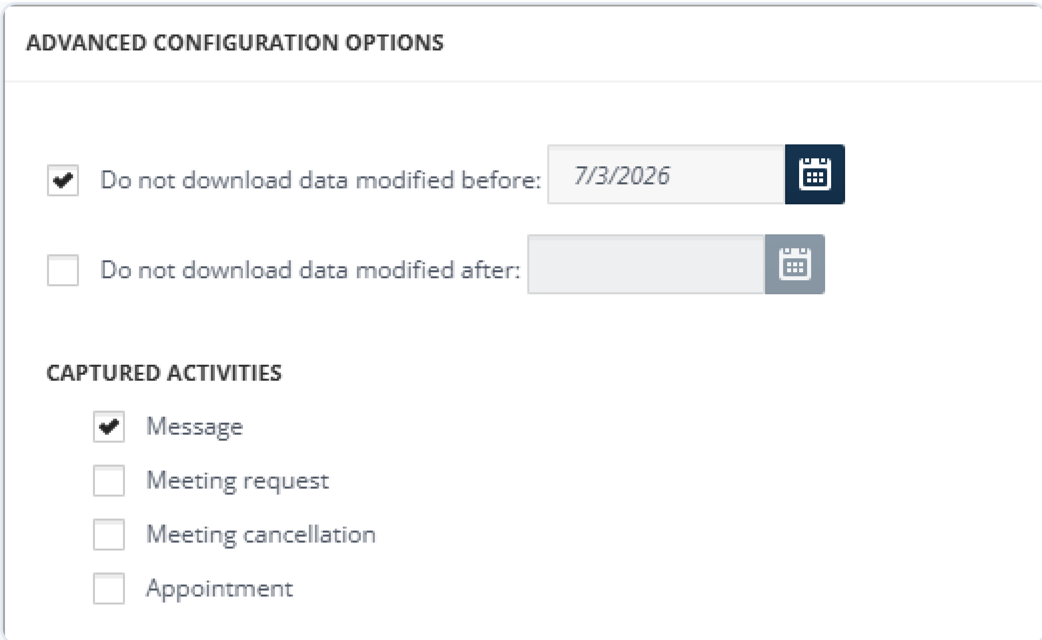
3. On the next screen, choose whether the import should be done by the last modification date (DateTimeModified) or by the creation date (OriginalDateTime). The cut-off date options change accordingly.
4. Fill in the **Mailbox Folder** from where the data should be imported. If you have more than one Mailbox Folders, separate each name with a semicolon (";").
5. Check **All folders** to process data within all the folders.
6. To process data within the subfolders of the specified mailboxes, check **Include subfolders**.
7. To search for the mentioned mailbox folders in the recovery route folders, check **Load recoverable items**.
8. For Advanced Configuration Options, **Do Not Download Data Modified/Created Before** and **Do Not Download Data Modified/Created After**, allow cutting off data outside the set date range. If the before date is set to 08/17/2024 and the after date is set to 08/25/2024, only the

data between these two dates will be downloaded. Data outside that range will be ignored. Note that both options can be used independently as well.

9. Select the **Captured Activity** type you would like to import and then click **Save**. There are the following activities that can be imported:

    - Message
    - Meeting request
    - Meeting cancellation
    - Appointment

    > **Note:** To include messages irrespective of their type, select all of them.



Supported Notifications

The importer supports the following notification types:

- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**

- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users
- Filters
- Targets
- Importer Settings

FX Connect

FX Connect is a market-leading FX execution venue that helps firms efficiently manage multiple portfolios, connect with brokers, and streamline global operations. It provides users with tools to manage pre- and post-trade workflows electronically, while also offering tools designed to help clients carry out their compliance obligations.

> **Note:** Message participants by default are imported in FX Connect User ID format. If you want to map them to the users' email addresses, each email address and corresponding FX Connect User ID should be added in User Mappings section of collector set up.

> The collector automatically merges messages with the same session ID into one output message.

Activities Captured

- Messages

Captured messages can contain:

- Session ID
- Trade participants
- Message body
- Activity datetime

Source Configuration

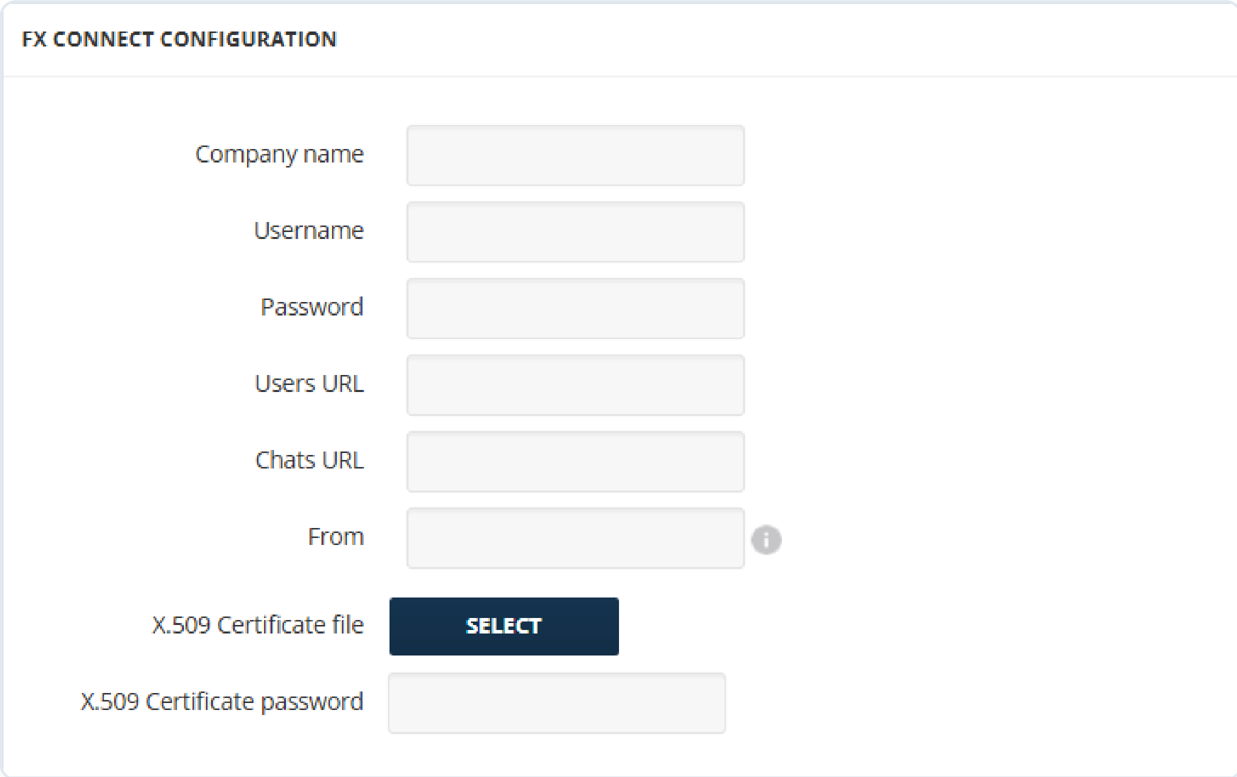
To configure the FX Connect source, complete the **FX Connect Configuration**, **Threading and Formatting**, and **Message Body** sections.

> **Note:** Message participants are imported in FX Connect User ID format by default. If you want to map them to the users' email addresses, add each email address and its corresponding FX Connect User ID in the **User Mappings** section of the collector setup.

FX Connect Configuration

To configure the source:

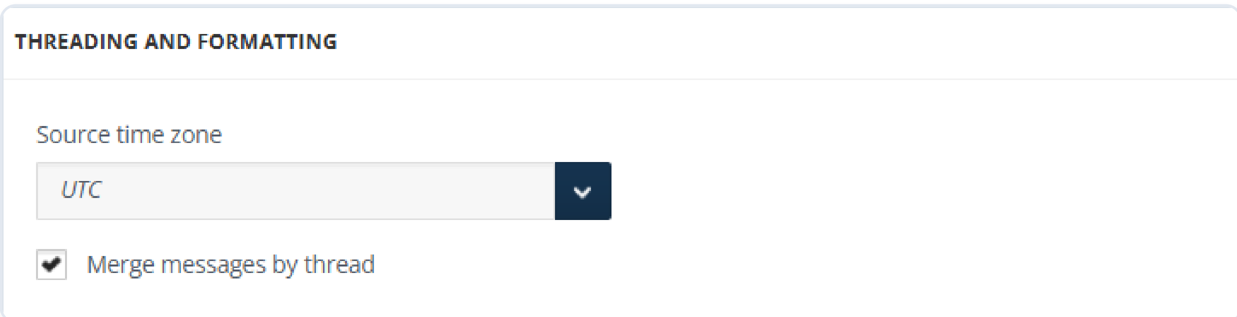
1. Fill out the following fields:
    - **Company name** - the company name provided to FX Connect
    - **Username** - the username provided to FX Connect
    - **Password** - the user's password
    - **Users URL** - the user link
    - **Chats URL** - the chat link
    - **From** - a dummy email address is being added in case the email of the event is missing
2. Provide **X.509 Certificate Thumbprint**.



Threading and Formatting

To configure the section:

1. Select **Source time zone**. The messages in the source file are of the set time zone, the dates in the messages are processed to the UTC time zone. By default, Capture sets the Source Time Zone as UTC.
2. Enable the **Merge messages by thread** option to combine all messages from a session into a single message.

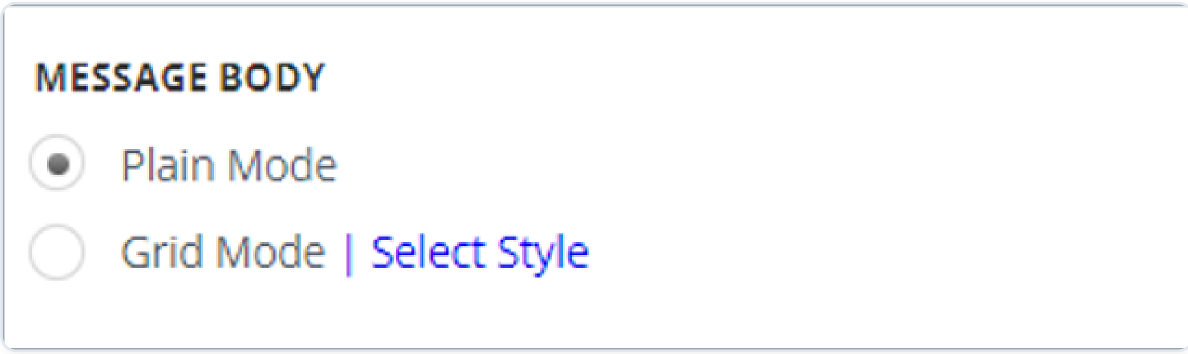


Message Body

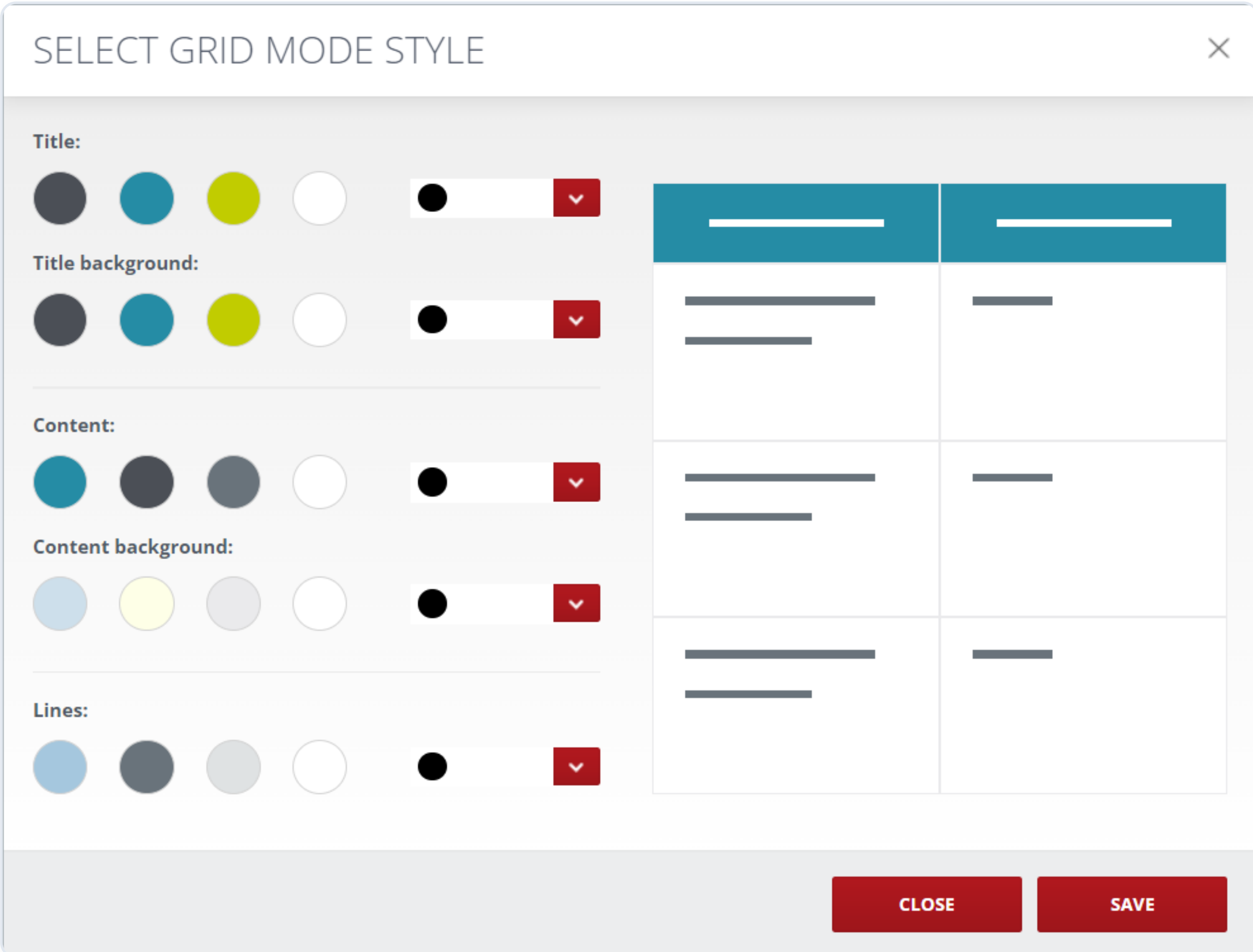
There are the following output message body options:

- **Plain** - this mode displays the message as a simple text.
- **Grid mode** - this mode allows you to see the information in the following columns:

- Message creator
- Message timestamp
- Message



It is possible to change the color scheme of the grid mode by clicking the **Select Style** link.



Reconciliation

Select **Enable Capture reconciliation** to reconcile the number of messages that Arctera Capture processes against the message count reported by the source. For FX Connect, the reconciliation file is delivered through file transfer together with the data files in the same run.

Supported Notifications

The importer supports the following notification types:

- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users (N/A)
- Filters
- Targets
- Importer Settings

Google Drive

G Suite's Business and Enterprise editions provide flexible storage options so there will always be enough space for the files. With centralized administration, data loss prevention, and Vault for Drive, users and file-sharing can be easily managed to help meet data compliance needs.

In enterprise applications a user's data might need to be accessed without any manual authorization on their part. In G Suite domains, the domain administrator can grant third-party applications with domain-wide access to its users' data - this is referred as domain-wide delegation of authority. To delegate authority this way, domain administrators can use service accounts with OAuth 2.0.

Activities Captured

- Shared files
- Conversations and comments around shared documents

Service Account Creation

First a service account and its credentials need to be created. During this procedure information that will be used later for the G Suite domain-wide delegation of authority and in the code to authorize with the service account needs to be gathered. The following items required later are service account's:

- Client ID
- Private key file
- Email address.

To create a Service Account:

1. Open the **Service accounts** page: https://console.developers.google.com/iam-admin/serviceaccounts. If prompted, select a project.
2. Click **Create service account**.
3. In the Create service account window, type a name for the service account.

> **Note:** The next two steps are optional.

4. Once the service account is created, click it to open its settings. Open the **Show Domain-wide Delegation** menu, check **Enable Google Workspace Domain-Wide Delegation** and click **Save**.
5. In the same window, copy the **Email** and the **Unique ID** of the service account.
6. Go to **KEYS** and click **ADD KEY**, then select **Create new key**, to create a private key for the service account.
7. Select the key type **JSON** and click **Create**.
8. Your new public/private key pair is generated and downloaded to your machine; it serves as the only copy of this key. Keep it in a secure location.

Domain-Wide Authority Delegation to the Service Account

The created service account needs to be granted access to the G Suite domain's user data that should be accessed.

The following must be performed by an administrator of the G Suite domain:

1. Go to your G Suite domain's Admin console https://admin.google.com/, click **Security** > **API controls**.
2. Scroll down to **Domain wide delegation** section and click **Manage Domain Wide Delegation**.
3. Click **Add New**.
4. Open the key file that you saved in the above section, copy the value of client_id, then paste it in the **Client ID** field. Enter the following scopes that your application should be granted access toin **OAuth scopes** fields and click **Authorize**:
   - `https://www.googleapis.com/auth/admin.directory.user.readonly`
   - `https://www.googleapis.com/auth/drive.readonly`
   - `https://www.googleapis.com/auth/drive.activity.readonly`
   - `https://www.googleapis.com/auth/drive.activity.readonly`

Your service account now has domain-wide access to the Google Admin SDK Directory API for all the users of your domain. Now you can use Admin SDK Directory service object on behalf of your G Suite domain's users.

> **Note:** Only users with access to the Admin APIs can access the Admin SDK Directory API, therefore your service account needs to impersonate one of those users to access the Admin

SDK Directory API. Additionally, the user must have logged in at least once and accepted the G Suite Terms of Service.

Creating Administrative Role for the User Manager Service Account

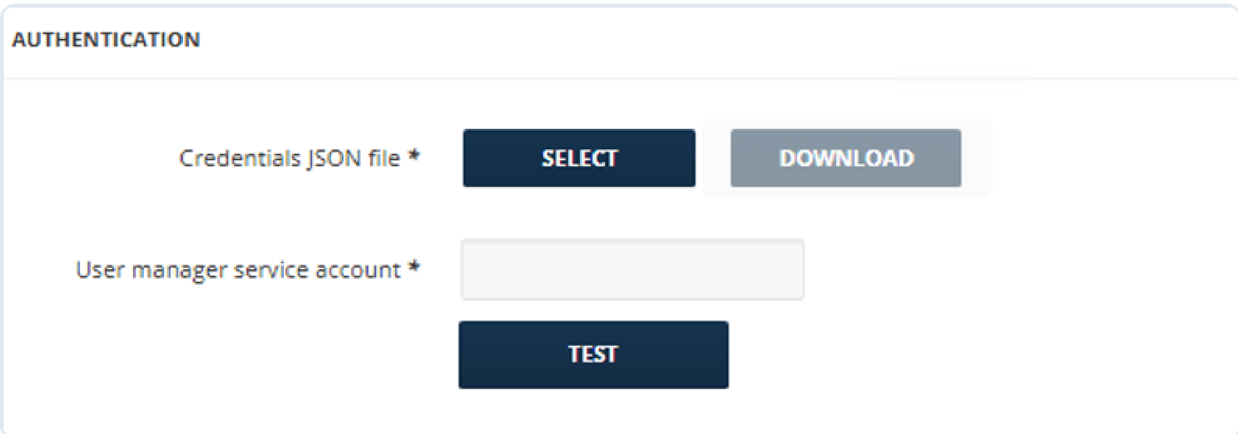
To create the account:

1. Go to https://admin.google.com and click **Account** > **Admin roles**.
2. Click **CREATE A NEW ROLE**.
3. Name the new role and click **CONTINUE**.
4. Expand **Users**, select **Read** and click **CONTINUE**.
5. Review the privileges and click **CREATE ROLE**.
6. To assign the role to a user, go to https://admin.google.com and click **Users**, then click the user that you want to assign the role to.
7. Select **Admin roles and privileges**.
8. Click the **Edit** button, assign a role, and click **Save**.
9. Go to https://console.developers.google.com/ and click **ENABLE APIS AND SERVICES**. API Library will be open.
10. Search and enable Admin SDK and Google Drive APIs.

Source Configuration

To authenticate the collector:

1. Upload the JSON of the public key saved to your device.
2. Enter the email address of the user created in the previous section.



> **Note:** The **Download** button is activated when there is a JSON file uploaded.

Timestamp Formatting

In addition to the primary stamp, a second timestamp can be enabled with its time zone. From the drop-down menu you can choose the time zone of the timestamp. The format of the timestamp in the output message can also be specified from the six options in the **Date Time Format** drop-down list.

Advanced Configuration Options

To configure advanced options:

1. Specify the **Subject Prefix** in the subject line of imported emails. This is useful for organizing imported data, i.e., when multiple sources share a common target.

   > **Note:** Not applicable to the EV Folder target.

2. Specify **Do not download data modified before** and **Do not download data modified after** to allow cutting off data outside the set date range. If the before date is set to 08/17/2024 and the after date is set to 08/25/2024, only the data between these two dates will be downloaded. Data outside that range will be ignored. Note that both options can be used independently.

Supported Notifications

The importer supports the following notification types:

- **Import job stopped**

- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users
- Filters
- Targets
- Importer Settings

Google Messages

Google Messages is a messaging app developed by Google for Android devices. It supports SMS, MMS, and RCS, allowing users to send text messages, images, videos, and more.

The Google Messages collector allows for the capture of communications that occur within Google Messages.

Following the successful onboarding of your devices on Sausalito Labs, please proceed with configuring your importer.

Activities Captured

- Text messages (Plain text, emojis)
- Message replies

> **Note:** Replies are captured as new messages prefixed with "Parent message".

- Documents (MS Word, MS Excel, PDF, PPT)
- Images
- Videos
- GIFs
- Stickers
- Links
- Audio messages (Recordings and voice notes)
- Apps from Play Store (App links)
- Reactions to messages
- Locations
- Contacts

File Formats Supported by the Collector

- .json

Source Configuration

For information on how to configure the following sections of the **Source** tab, see:

- File Source Configuration
- PGP Configurations
- Quarantine Location
- Miscellaneous Settings

Advanced Configuration Options

If **Include original data as attachment** is enabled, the XML file will be attached to the output message.

Supported Notifications

The importer supports the following notification types:

- **Quarantine file**

- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Failed to quarantine file**
- **Import job completed with failure**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users (N/A)
- Filters
- Targets
- Importer Settings

IceChat

IceChat messaging system offers collaboration with other market participants. It offers diverse setup options that can be tailored to support user's compliance requirements. With IceChat users can react to trade opportunities in real-time with features including quote and trade recognition logic, blast messages and a marketplace directory connecting over 80,000 market participants.

Activities Captured

- Room ID
- Start time
- Message content
- Participants
- Participants entered

- Message date

File Formats Supported by the Collector

- .xml

Source Configuration

For information on how to configure the following sections of the **Source** tab, see:

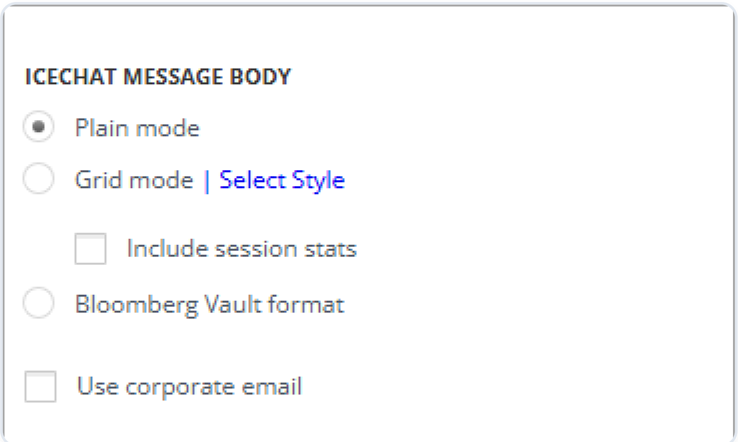
- File Source Configuration
- PGP Configurations
- Quarantine Location
- Miscellaneous Settings

IceChat Message Body

This setting specifies how the imported message will be displayed in the target. There are the following options:

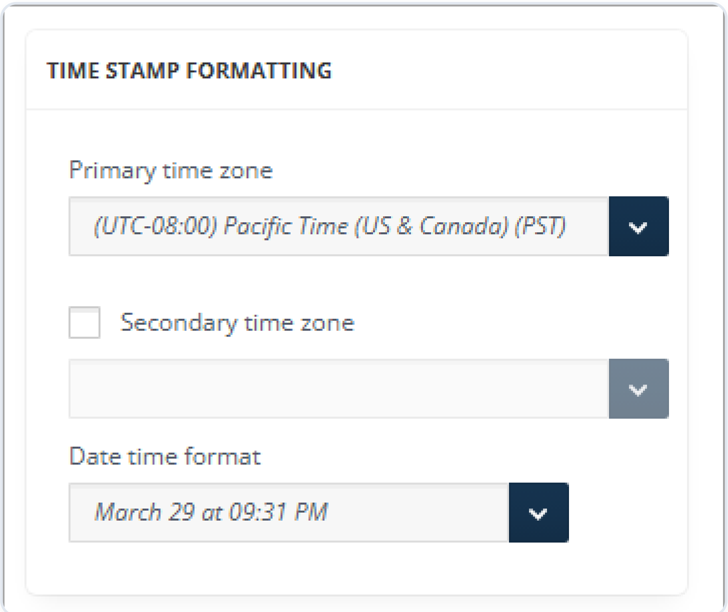
- **Plain mode** - displays the interactions below each other in their basic form.
- **Grid mode** - displays the information in a grid layout. You can change the color scheme by clicking the **Select Style** link. Enable **Include session stats** to include the session statistics in the message.
- **Bloomberg Vault format** - when enabled, the imported messages are displayed in Bloomberg Vault format.

Enable **Use corporate email** to use the corporate email addresses of the participants in the generated messages.



Time Stamp Formatting

In addition to the primary stamp, a second timestamp can be enabled with its time zone. From the drop-down menu, you can choose the time zone of the timestamp. The format of the timestamp in the output message can also be specified from the six options in the **Date Time Format** drop-down list.



Supported Notifications

The importer supports the following notification types:

- **Quarantine file**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Failed to quarantine file**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**

- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users (N/A)
- Filters
- Targets
- Importer Settings

iMessage

iMessage is a messaging service developed by Apple Inc. It allows users to send text messages, photos, videos, documents, and more to other Apple devices over the internet.

The Arctera Capture iMessage collector enables organizations to seamlessly integrate iMessage data into their communication management systems, ensuring comprehensive data collection and compliance.

Following the successful onboarding of your devices on Sausalito Labs, proceed with configuring your importer.

Activities Captured

- Text messages (iMessage, SMS)
- Edits

  > **Note:** Edited messages are captured as new messages prefixed with "Edited to".

- Replies
- Undo sent messages
- Deleted messages

  > **Note:** Deletes are not captured as separate events.

- Documents (MS Word, MS Excel, PDF, PPT)
- Images
- Videos
- Audio messages (recordings, voice notes)

> **Note:** Audio messages with user action "Keep" are captured.

- Emojis/Stickers/GIFs

> **Note:** Emojis, stickers, and GIFs are captured as separate messages.

- Links
- Apps from Store
- Pinned locations

File Formats Supported by the Collector

- .json

Source Configuration

For information on how to configure the following sections of the **Source** tab, see:

- File Source Configuration
- PGP Configurations
- Quarantine Location
- Miscellaneous Settings

Advanced Configuration Options

If **Include original data as attachment** is enabled, the XML file will be attached to the output message.

Supported Notifications

The importer supports the following notification types:

- **Quarantine file**

- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Failed to quarantine file**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users (N/A)
- Filters
- Targets
- Importer Settings

JSON

JSON collector allows our customers to rapidly transform JSON files using JSON template files to a predefined format. Once JSON is transformed, Capture processes the JSON file by generating the required mapping fields and creating the configured output format (EML, JSON, etc.). The mapping varies from source to source. Contact Arctera Support to get the template corresponding to the source and the signature file you are going to use it for.

Activities Captured

- Messages

Captured messages can contain:

- Message subject
- Message headers
- Participants: From, To, CC, and BCC
- Activity datetime
- Message body
- Attachments

File Formats Supported by the Collector

- .json

Source Configuration

For information on how to configure the following sections of the **Source** tab, see:

- File Source Configuration
- Quarantine Location
- Miscellaneous Settings
- PGP Configurations

JSON Collector Options

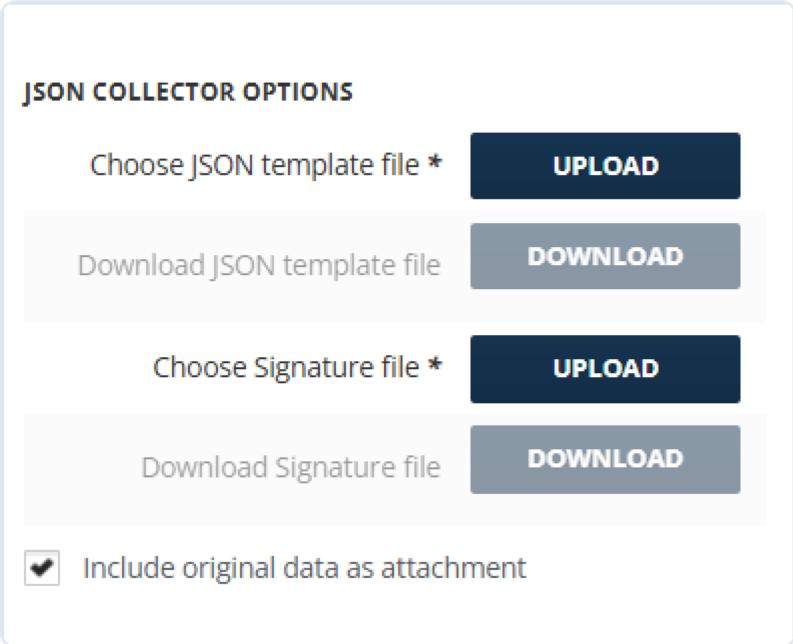
Upload the JSON template provided separately for each source which is used to rapidly transform .JSON files to a predefined format.

To configure the section:

1. Upload the JSON template.
2. Upload the Signature file.

> **Note:** Templates must be reviewed and cryptographically signed by Arctera.

3. Enable **Include original data as attachment** in case you want to include original data as an attachment in the output message.



Supported Notifications

The importer supports the following notification types:

- **Quarantine file**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Failed to quarantine file**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users (N/A)
- Filters
- Targets
- Importer Settings

LeapXpert

LeapXpert is a secure enterprise communications platform that enables compliant business conversations across consumer messaging channels, including WhatsApp, Signal, Telegram, iMessage, SMS, WeCome, and its own governed communications (Governed).

The Arctera Capture LeapXpert collector ingests archived conversations from LeapXpert compliance data and converts them into a normalized Arctera Capture JSON message format for compliant archiving and supervision.

Activities Captured

The LeapXpert collector captures conversations from the following sources:

- iMessage
- SMS
- Telegram
- WeCome
- WhatsApp
- Governed

Source Configuration

Provide your LeapXpert configuration data so that Arctera Capture can access your LeapXpert data.

For information on how to configure the following sections of the **Source** tab, see:

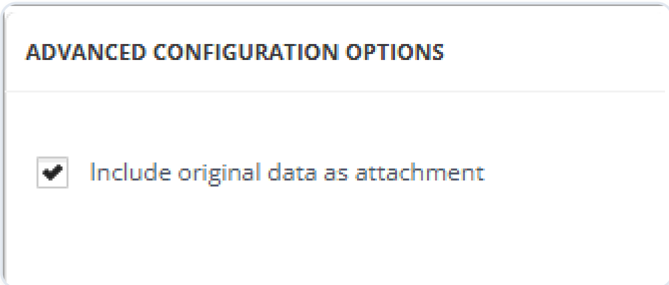
- File Source Configuration
- PGP Configurations

- Quarantine Location
- Miscellaneous Settings

Advanced Configuration Options

For this section:

- The **Include original data as attachment** feature allows including/excluding the original data as an attachment by enabling/disabling the corresponding checkbox. When enabled, the original data is attached to the output message.



Supported Notifications

The importer supports the following notification types:

- **Quarantine file**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Failed to quarantine file**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users (N/A)
- Filters
- Targets
- Importer Settings

LSEG (Refinitiv)

LSEG (Refinitiv) brings a user the latest news from around the world, covering breaking news in markets, the business, politics, entertainment, technology, video. LSEG (Refinitiv) collector processes data from Eikon Messenger and SI Dealing.

Eikon Messenger is captured and delivered to clients either via a daily XML posted to FTP (External Feed) or hosted archiving (Global Relay). The Eikon Messenger instant messaging network is based on an individual's user ID + firm name and is captured/recognized as such.

Contact our support at Arctera Support for more details on the mapping corresponding to the source, you are going to use for LSEG(Refinitiv) collector.

Activities Captured

- Person to person messages
- Group chats
- Attachments
- Disclaimers

> **Note:** To process current schema files, the file filter should be configured with the following extensions: messages.zip | attachments.zip | *.csv. **Note:** Quarantine sources column on the Dashboard shows the number of the files moved to the quarantine folder while processing source files with the below listed configured formats. All other files have initially been considered unwanted files and have been moved to the quarantine folder.

File Formats Supported by the Collector

- .csv

- .xml

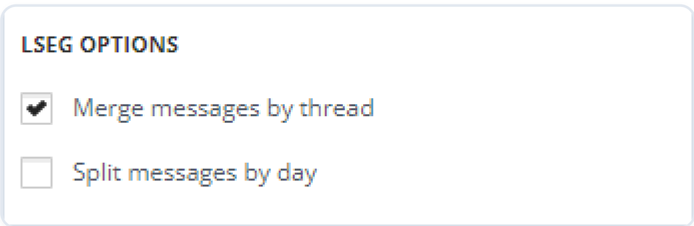
Source Configuration

For information on how to configure the following sections of the **Source** tab, see:

- File Source Configuration
- PGP Configurations
- Quarantine Location
- Attachment Validation
- Miscellaneous Settings

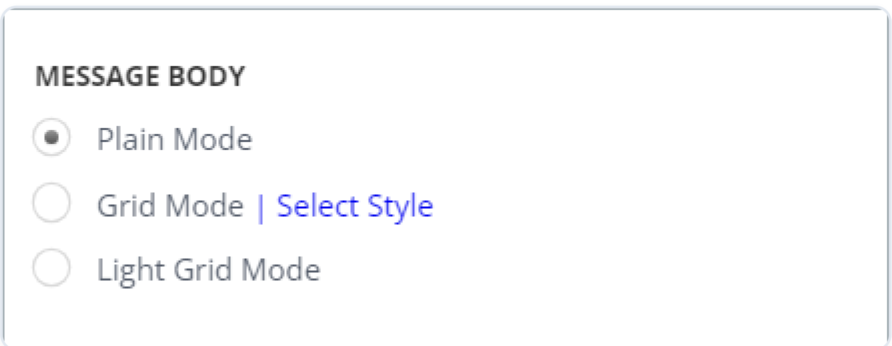
Advanced Configuration Options

The option **Split by Day** merges the messages from the same day into one email message. The time zone by which the messages are split can be selected from the drop-down menu. This option can be selected only if **Merge Messages by Thread** is selected.



Message Body

In the LSEG (Refinitiv) collector, you can choose between three IB message body options, which specify how the imported message will be displayed in the target.



- When you select the **Plain Mode** option, you will see the interactions below each other.
- When you select the **Light Grid Mode**, the data is two-toned, easy to be viewed with limited metadata.

If you enable the **Grid Mode** option, you will see the information in the five following columns:

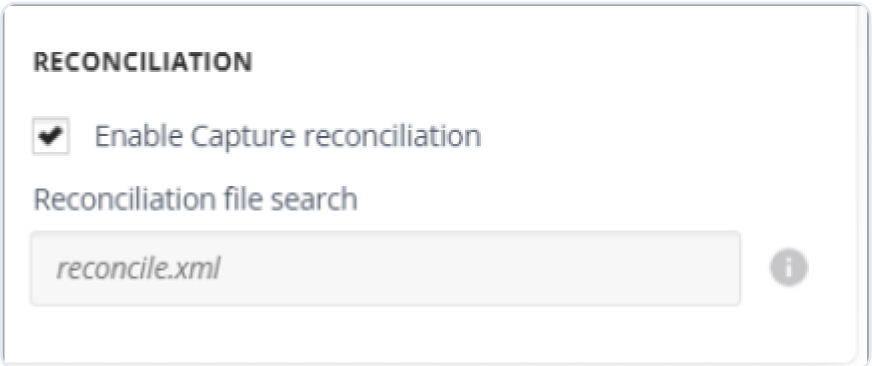
- UTC Time Stamp, which includes the date of the sent message
- Content
- Event Type, what kind of an event the activity is (joining the chat, sending a message, etc.)
- Message ID
- Attachment.

> **Note:** You can also change the color scheme of the grid mode by clicking the **Select Style** link.

Reconciliation

Select **Enable Capture reconciliation** to reconcile the number of messages that Arctera Capture processes against the message count reported by the source.

In the **Reconciliation file search** field, specify the pattern that Arctera Capture uses to identify the reconciliation file, for example, `reconcile.xml`. For LSEG (Refinitiv), the reconciliation file is delivered together with the data files.



Supported Notifications

The importer supports the following notification types:

- **Quarantine file**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**

- **Failed to quarantine file**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users (N/A)
- Filters
- Targets
- Importer Settings

LSEG Messenger

LSEG Messenger is a secure messaging and collaboration platform by the London Stock Exchange Group (LSEG) designed for the financial services industry. It facilitates professional networking and real-time data sharing, with compliance export feeds delivered via the LSEG Data Platform.

The Arctera Capture LSEG Messenger collector retrieves archived LSEG Messenger conversations from the LSEG compliance export service and converts them into a normalized message format for compliant archiving and supervision.

Activities Captured

- One-to-one conversations
- Group conversations

Captured activities can contain:

- Emojis

Note: The Capture import process uses the UTC date calculated at the time the job runs. Because Amazon S3 export files are generated on a fixed UTC schedule, the calculated import range may not align with the export boundaries, which can result in records near the time boundary being skipped. To ensure complete data import, use a wider import time range that overlaps consecutive import windows.

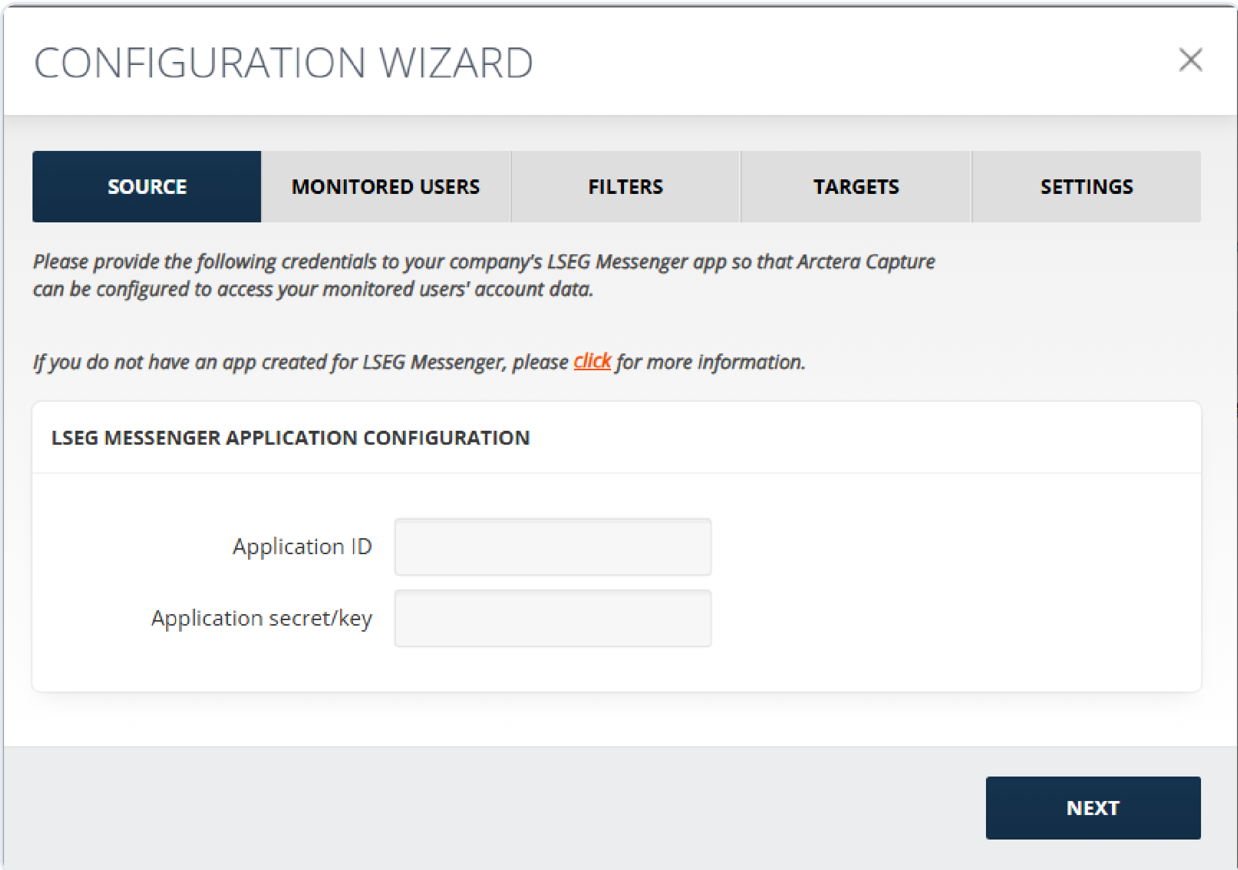
Source Configuration

Provide the following credentials to your company's LSEG Messenger app so that Arctera Capture can be configured to access your monitored users' account data.

Note: Please contact your LSEG representative directly to request and acquire these credentials.

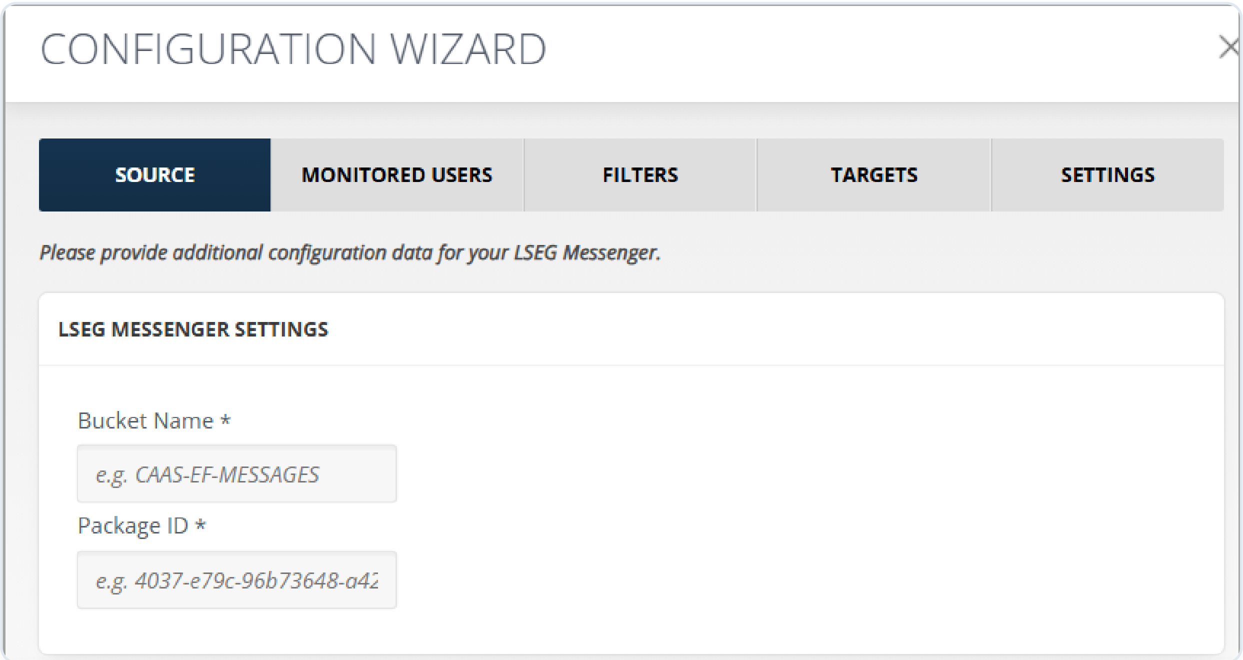
To configure the LSEG Messenger application:

1. Enter the **Application ID**.
2. Enter the **Application secret/key**, and then click **Next**.



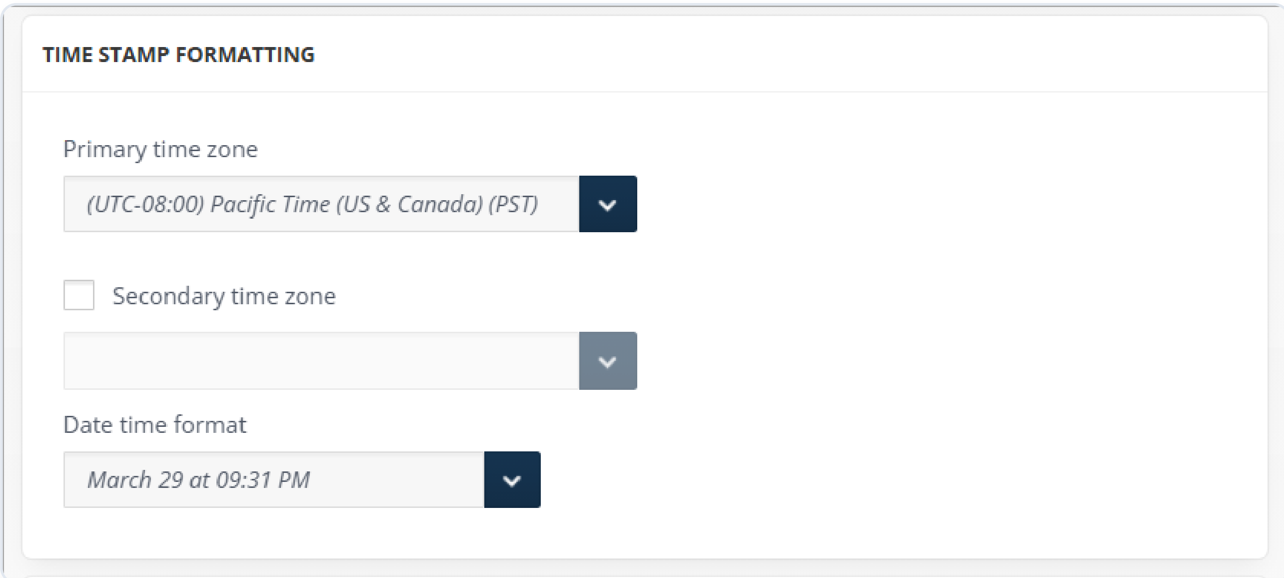
To configure the source, provide the following LSEG Messenger Settings:

- **Bucket Name**: The name of the LSEG compliance export feed bucket that stores the data to be captured (for example, CAAS-EF-MESSAGES).
- **Package ID**: The identifier of the LSEG compliance export package to be captured.



Timestamp Formatting

In addition to the primary stamp, a second timestamp can be enabled with its time zone. From the drop-down menu, you can choose the time zone of the timestamp. The format of the timestamp in the output message can also be specified from the six options in the **Date Time Format** drop-down list.



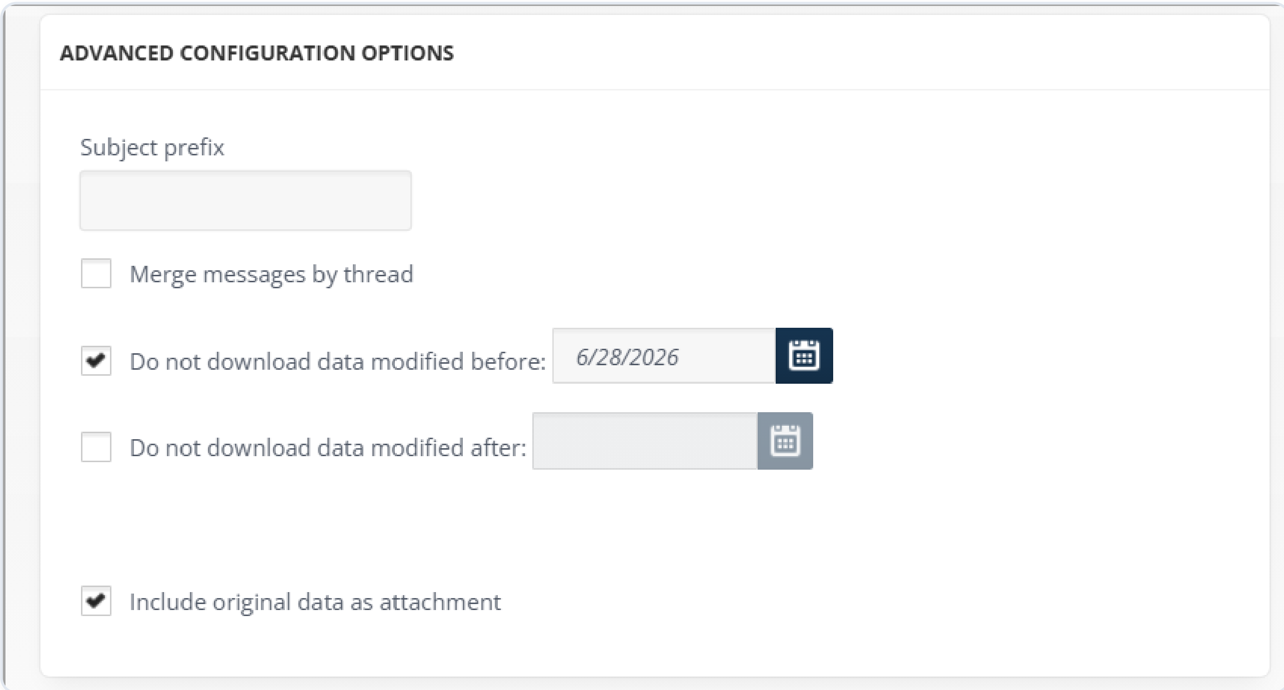
Advanced Configuration Options

There are the following advanced options:

- The **Subject Prefix** feature will add a prefix before the message subject to facilitate the search in the target.
- Enable the **Merge messages by thread** option to combine all messages from the same thread into a single message.
- Options **Do not download data modified before** and **Do not download data modified after** allow cutting off data outside the set date range. If the before date is set to 08/17/2023 and the after date is set to 08/25/2022, only the data between these dates will be downloaded. Data outside that time frame will be ignored.

> **Note:** Both options can be used independently as well.

- The **Include original data as attachment** feature allows including/excluding original data as attachment by enabling/disabling the corresponding checkbox.

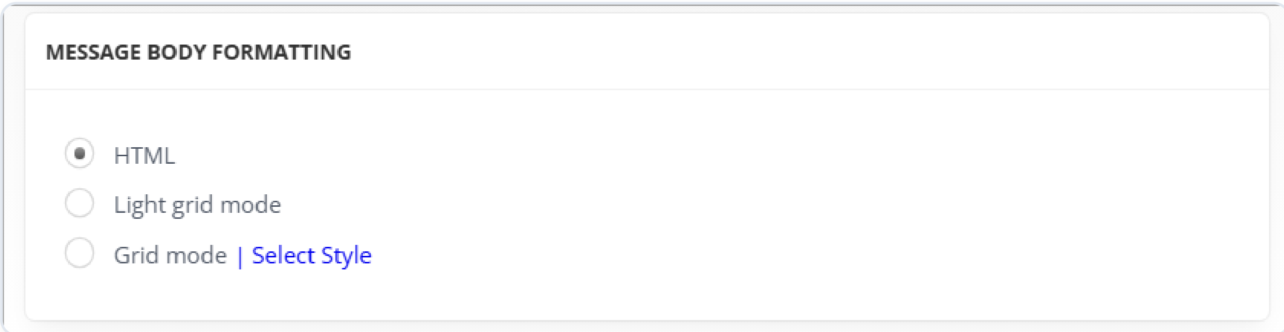


Message Body

This setting specifies how the imported message will be displayed in the target. There are the following output message body options:

- **HTML** - the message in the output will be displayed in the HTML format.
- **Light grid mode** - the message will be displayed in a light grid mode with limited metadata.
- **Grid mode** - the message will be displayed in a grid layout with the information organized in columns.

> **Note:** You can also change the color scheme of the grid mode by clicking the **Select Style** link.



Supported Notifications

The importer supports the following notification types:

- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users (N/A)
- Filters

- Targets
- Importer Settings

Microsoft Teams

Microsoft Teams is a chat-based workspace in Office 365 that integrates with the apps and services teams use to get work done together. It provides the enterprise security and compliance features you expect from Office365, including broad support for compliance standards, and eDiscovery and legal hold for channels, chats, and files.

Activities Captured

- Chat messages
  - Create
  - Edit

    > **Note:** If the **Capture retained messages (edits)** checkbox is selected, all versions of edited messages will be captured.

  - Delete
- Channel messages

  > **Note:** The team owner should be included in the monitored users list to capture data from shared channels.

  - Create
  - Edit

    > **Note:** If the **Capture retained messages (edits)** checkbox is selected, all versions of edited messages will be captured.

    > **Note:** Only the latest version of the message is captured for Private Channels due to an API limitation.

  - Delete

> **Note:** The team owner should be included in the monitored users list to capture data from shared channels.

Captured messages can contain:

- Chat/Channel info
- Attachments

  > **Note:** Only the latest version of a replaced attachment in a message is captured due to an API limitation. This limitation also applies to hosted content.

  > **Note:** It is recommended to run/capture the required data before deleting teams and/or channels.

- Loop components
- Video clips
- Voice messages
- Reactions

  > **Note:** Reactions of already captured messages are not captured.

- Emojis
- Praises
- Approvals
- Mentions
- System-generated events (members added/removed/joined/left)

  > **Warning:** The deduplication feature is available for Microsoft Teams chat messages. It is a process that eliminates duplicated copies of data and significantly decreases storage capacity requirements. To use the feature, enable the **Use Graph's chat deduplication (cost reduction)** checkbox from the **Advanced Configuration Options** on the **Source** tab. Note that due to the Graph API limitations, when this feature is enabled, the chat

> messages of guests and deleted users are not captured. To use this feature all users in the tenant should be monitored and have the E5 licenses.

> **Note:** In case of having an error with a '404 not found' message for a user when processing messages from Microsoft Teams, the collector will skip that user, and a warning will be logged for later troubleshooting.

Notes

Due to the API issues, we have the following limitations:

- Hosted content in one-on-one chats from external users is not captured.
- Hosted contents of deleted teams are not captured.
- Deleted messages are available for capture only 21 days from the time of deletion.
- Hosted contents (including voice messages) of deleted messages are not captured.

Microsoft Entra ID App Creation

To authenticate via OAuth during the collector configuration, you need to create a Microsoft Entra ID Application.

To create an app:

1. Create an O365 account and open Azure Portal using the same credentials as for O365 (Global Admin).
2. Click **Microsoft Entra ID** at the top of the page and select **App Registration** from the left-side navigation pane.
3. Click the **+New registration** button.
4. Enter a **Name** for the application and click **Register**.
5. Find and make a note your **Application (client) ID** and **Directory(tenant) ID** as this is needed for configuring the collector in Arctera Capture.
6. In the navigation pane to the left, go to **Certificates & secrets**.
7. Click the **Upload certificate** button.
8. Select a certificate (public key) with one of the following file types: .cer,.pem, .crt, and click **Add**. For more information on how to create a certificate, see Creating a Certificate (Private and Public Keys).

Microsoft Entra Permissions

For permissions:

1. In the navigation pane to the left, click **API permissions**.
2. Click **Microsoft Graph**, and in the opened pane select **Application permissions**.
3. Add the following permissions:
    - Channel:Channel.ReadBasic.All
    - ChannelMember: ChannelMember.Read.All
    - ChannelMessage: ChannelMessage.Read.All
    - Chat: Chat.Read.All
    - Chat: Chat.ReadBasic.All
    - ChatMember: ChatMember.Read.All
    - ChatMessage: ChatMessage.Read.All
    - Files: Files.Read.All
    - Group: Group.Read.All
    - Team: Team.ReadBasic.All
    - User: User.Read.All
4. Get back to **API permissions** section, click **+ Add a permission**, select **SharePoint** and then **Application permissions**. These are the permissions you need to grant:
    - Sites: Sites.Read.All
    - TermStore: TermStore.Read.All
    - User: User.Read.All
5. Grant all the above-mentioned permissions.

License Info

Creating a subscription in Microsoft Graph requires one of the following licenses:

- Microsoft 365 E5/A5/G5
- Microsoft 365 E5/A5/G5 Compliance
- Microsoft 365 E5/A5/G5/F5 Security
- Microsoft 365 E5/A5/G5 Information Protection and Governance

For pricing and licensing different subscriptions are required:

- In evaluation mode, seeded capacity is shared across all APIs
- Model A is for E5 customers

Note: the E5 IPG (Information Protection Governance) license can be added on E3 licenses.

In case of detecting a user with an improper licensing or other payment issues, the Microsoft Teams API call fails to fetch the data. Hence, conversations will be captured when at least one of the participants has the proper Microsoft 365 licensing and has no payment issues. For additional information about Teams API Pricing and licensing models, see Licensing and payment requirements - Microsoft Graph | Microsoft Docs.

Enabling Billing for Microsoft Teams APIs in Microsoft Graph

Existing applications that used these metered APIs must now set up an active Azure billing subscription by June 30th, 2023, to avoid service disruptions. All other applications, including new applications since March 1st, 2023, are already subject to these requirements.

Microsoft has deprecated support for Teams GCC/GCC High and it is no longer supported.

Note: Customers using GCC or GCC High tenants for Microsoft Teams data collection should plan migration to a supported environment.

Applications without an active Azure subscription will get error "HTTP 402 Payment required" when trying to access the metered APIs using model=A. Applications using Evaluation Mode will also get error "HTTP 402 Payment required" when the seeded capacity limit is exceeded.

To avoid service disruptions to your application(s), take the following actions if you have not done so yet:

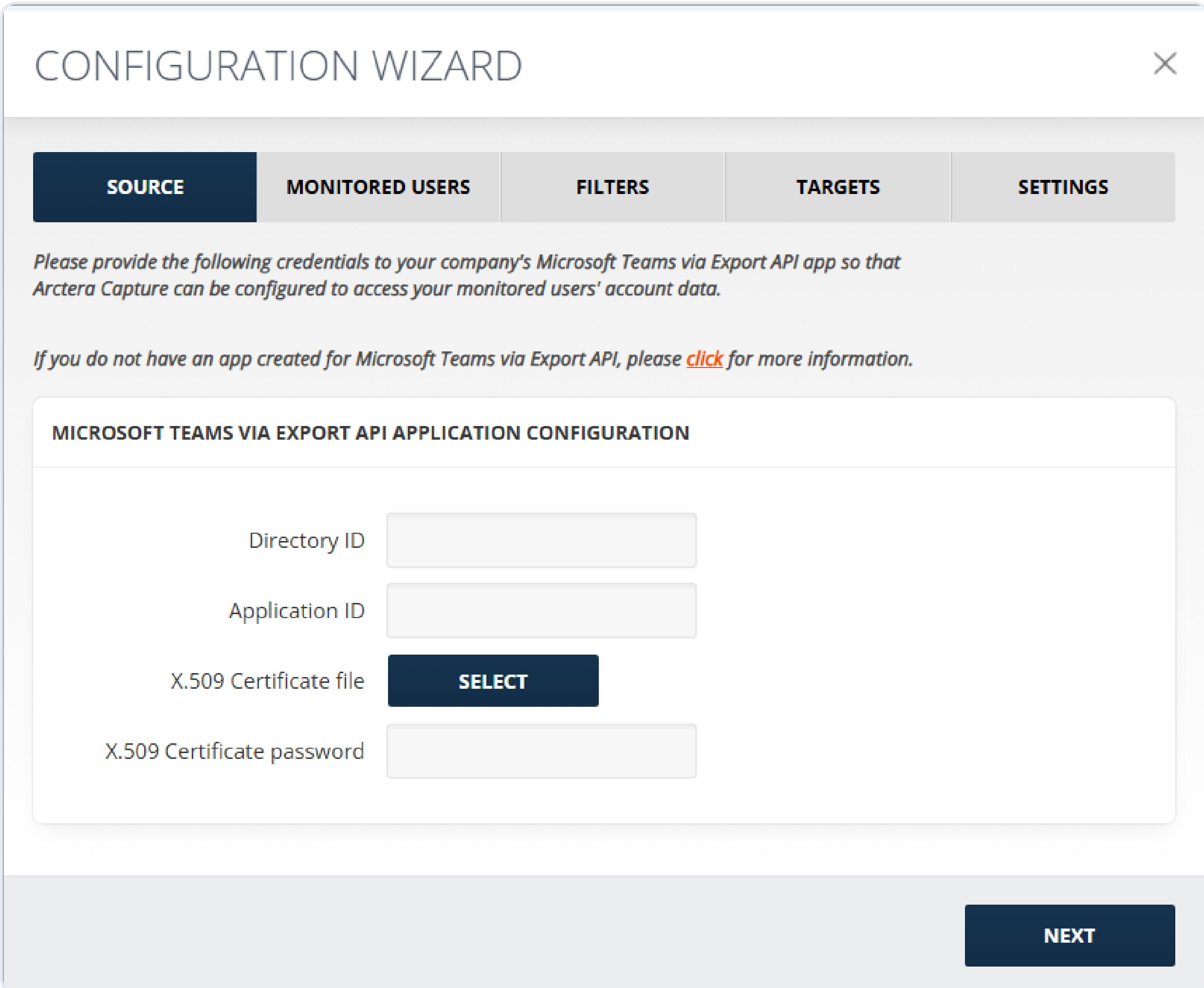
1. Set up an Azure billing subscription for each application.
2. Set up a payment model (model=A) for each API request of a metered API.
3. If your app is using model=A, ensure that your users have the proper E5 licenses and that DLP is enabled.

Note: If you have previously provided a subscription ID in the Protected API form, for the subscription to be properly configured, you still need to follow the instructions above to finish the setup.

Source Configuration

To configure the source:

1. Add **Directory (tenant) Id** and **Application Id**.
2. Select the **X.509 Certificate** file.
3. Enter the **X.509 Certificate password**.

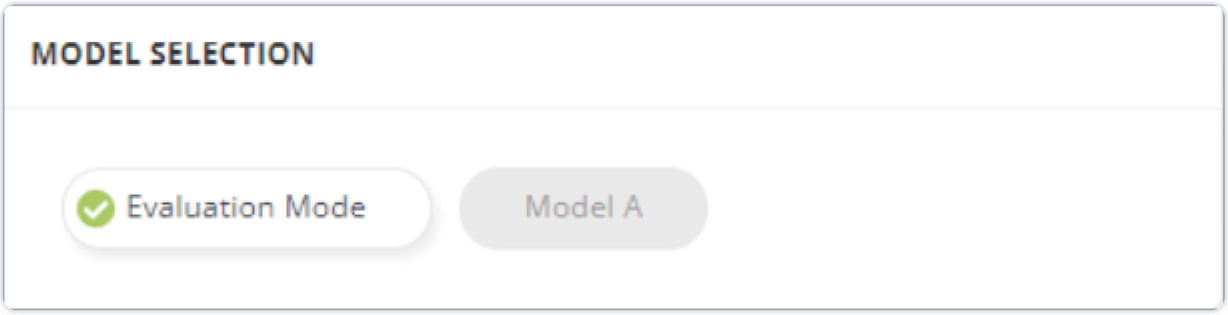


Model Selection

Here the user can make a **Model Selection** which allows selecting licensing and payment options for Microsoft Teams APIs:

- **Evaluation mode** - enables access to APIs with limited usage per requesting an application for evaluation purposes.

A - is restricted to applications performing a security or compliance function and requires a supported license.

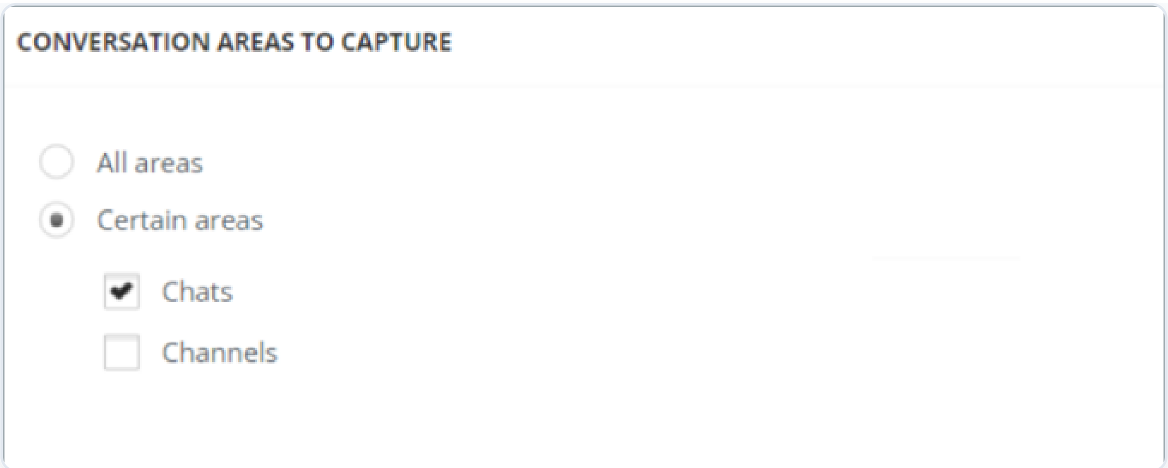


Conversation Areas to Capture

Specify the activities to be captured by the collector.

1. Enable **All areas** to capture data from chats and channels.
2. Enable **Certain areas** in case either Chats or Channels data needs to be collected.

> **Note:** The shared channels' membership type is printed in the output message as "UnknownFutureValue" due to API limitation.



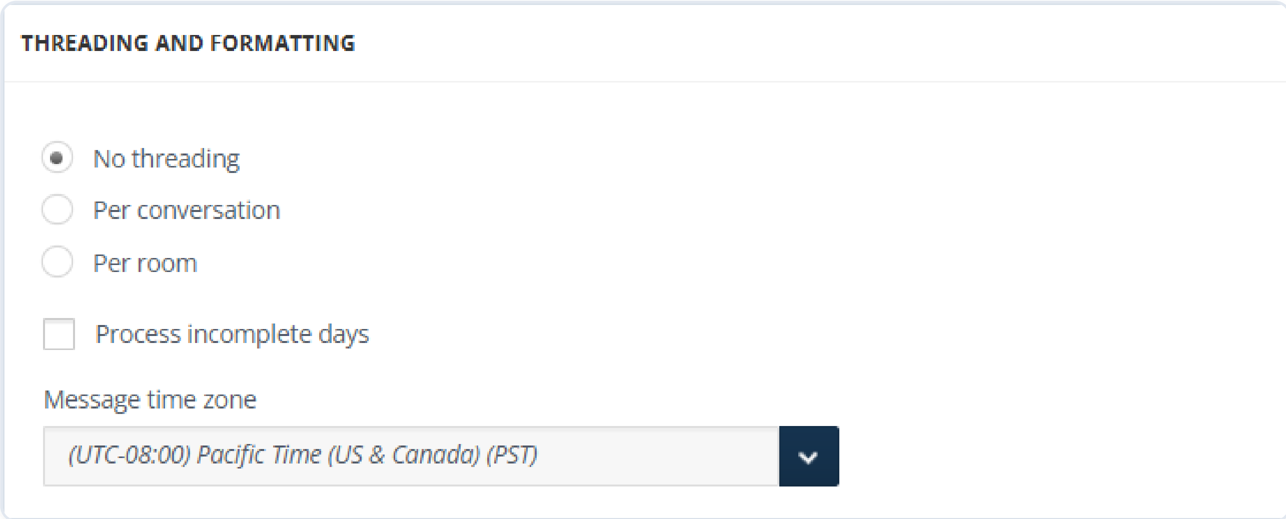
Threading and Formatting

> **Note:** This section is applicable to the EV Folder target partially.

> For Threading and Formatting:

- When the **Process incomplete days** option is enabled, the messages of the days that have not yet ended will be imported in a separate email.

Select the **Message time zone** by which the messages the drop-down menu.



Note: When font-family Segoe UI is present in the output message (HTML tags), and Heading 1,2,3, etc., Bold, and Italic formatting styles are applied, the Segoe UI font is not respected by Outlook. However, it is respected in HTML online editor. Also, when Monospaced formatting style is applied, the HTML editor does not respect the given font-family, and so does the Outlook.

Timestamp Formatting

In addition to the primary stamp, a second timestamp can be enabled with its time zone. From the drop-down menu you can choose the time zone of the timestamp. The format of the timestamp in the output message can also be specified from the six options in the **Date Time Format** drop-down list.

Advanced Configuration Options

There are following advanced options:

- The **Subject Prefix** feature will add a prefix before the message subject to facilitate the search in the target.

> **Note:** Not applicable to the EV Folder target.

- Options **Do not download data modified before** and **Do not download data modified after** allow cutting off data outside the set date range. If the before date is set to 08/17/2023 and the after date is set to 08/25/2023, only the data between these two dates will be downloaded. Data outside that time frame will be ignored. Note that both options can be used independently as well.

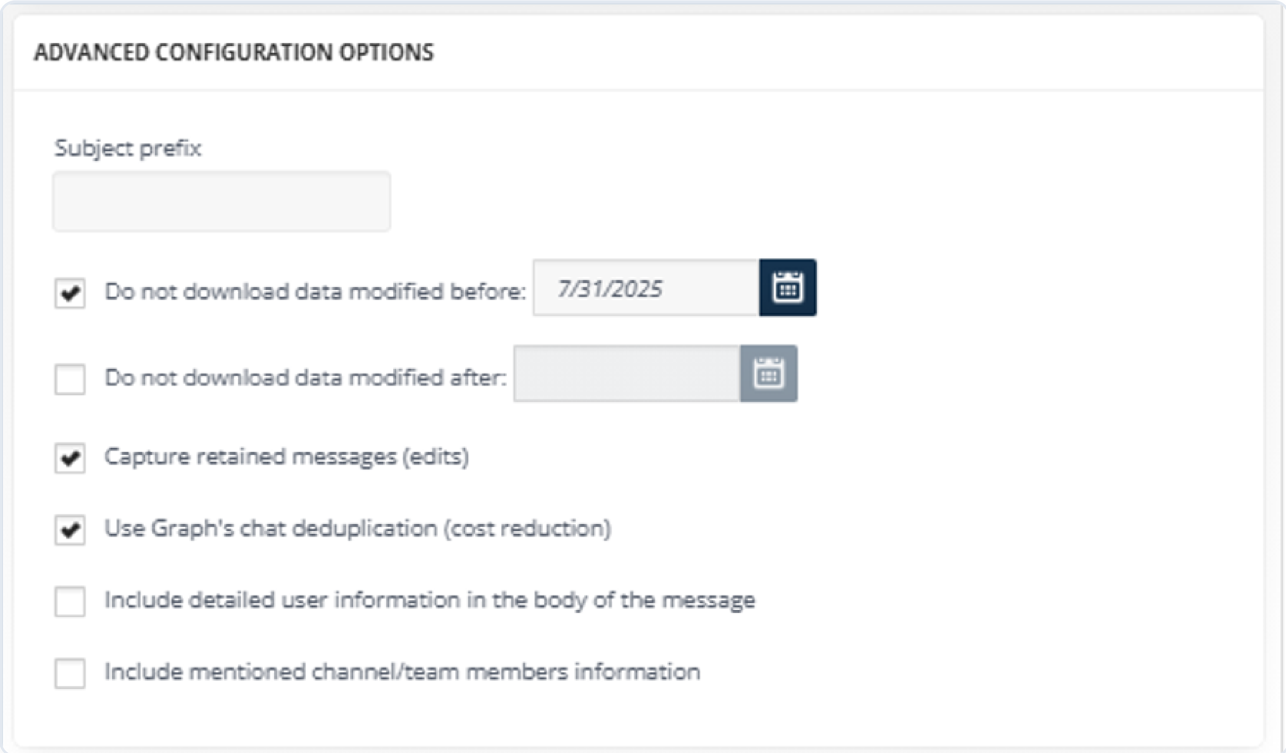
> **Note:** Due to the changes in the history tracking mechanism, it is required to set the date value for 'Do not download data modified after' to the previous day of the upgrade and run the collector on the new version only once. For daily import processes, it is required to clone the collector after the upgrade and on the cloned collector, set the date value for 'Do not download data modified before' to the day of the upgrade. Ignoring this recommendation can possibly cause duplicates during the first processing after the upgrade.

- **Capture retained messages (edits)**: When enabled, collects all versions of edited messages.

> **Note:** Before enabling this feature, review your retention policies and refer toMicrosoft documentationto ensure it is supported in your environment. Enabling this feature may result in additional Microsoft Graph API usage costs.

- **Use Graph chat deduplication (cost reduction)**: When enabled, captures only sent messages from monitored users.
- The **Include detailed user information in the body of the message** feature searches Entra ID for user principal name and then adds user display name and mail address from the Entra ID Directory.

Include mentioned channel/team members information allows getting the information of the mentioned members in channels/teams by enabling/disabling the corresponding checkbox.



Attachments Configuration

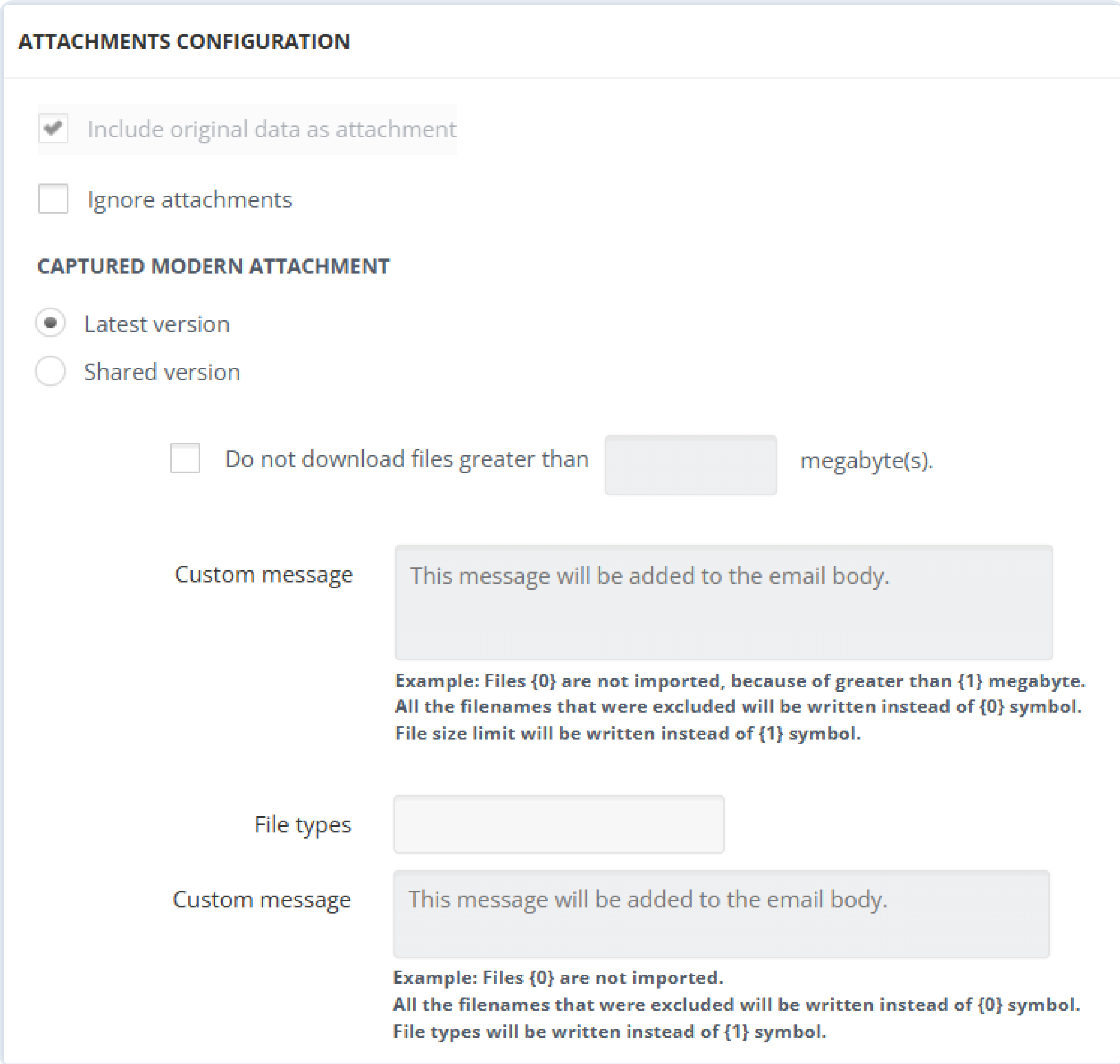
To configure te attachments:

1. Enable **Include original data as attachment** to include/exclude original data as attachment.
2. Enable **Ignore Attachments** to exclude all the attachments from the message. Each message will contain only information and the link of the excluded attachment. This will enhance the collector performance.
3. For **Captured Modern Attachments**,select:

- **Latest version** - to capture the latest saved version of shared document available at collector run time with the message.
- **Shared version** - to capture the saved version of the document at the time of sharing in Microsoft Teams with the message.

> **Note:** To respect the fidelity of the shared document timestamp, it is recommended to disable the **Edit** feature in Microsoft Teams.

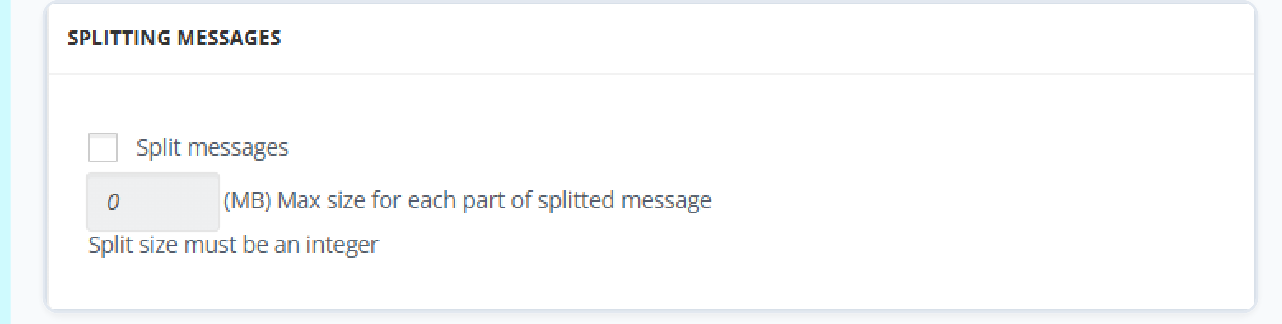
- When **Do not download files greater than X megabyte(s)** is selected, the files bigger than the filled-in number of megabytes, are not downloaded. In **Custom Message** field, a text for those excluded files can be specified. E.g.,"Files {0} are not imported, because they are greater than {1) megabytes". {0} is used to add the name of the file and {1} is used to add the number of megabytes specified above.
- In the **File Types** field, the types of files that should not be downloaded can be specified in the following format: e.g., .txt | .xml. The vertical bar is used to separate the file types.



Splitting Messages

This option allows splitting large files. In the field the size of a split part of the message can be specified so that each part does not exceed the set size. For example, if the **Max Size** for each part of split message is set to 25MB, and the original message is 65 MB, it will be split into 3 messages, each not exceeding 25MB.

> **Note:** Not applicable to the EV Folder target.



Supported Notifications

The importer supports the following notification types:

- **Monitored users skipped**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users
- Filters
- Targets
- Importer Settings

Microsoft Teams for Audio and Video

Nuclei is a third-party service that specializes in call recording and metadata management. It enables seamless capture, storage, and delivery of call recordings in formats compatible with enterprise systems. As part of its collaboration with Arctera, it places recordings and JSON metadata into locations like SFTP, Azure Blob, or Amazon S3.

The Arctera Capture Microsoft Teams for Audio and Video collector facilitates the integration of Nuclei data into organizational communication management systems. It ensures efficient acquisition of call recordings and metadata, performs data enrichment, and processes the collected data to make it accessible for compliance, analysis, and archiving.

Activities Captured

- Direct calls
- Group calls
- Meetings
- Calendar meetings

Source Configuration

For information on how to configure the following sections of the **Source** tab, see:

- File Source Configuration
- PGP Configurations
- Quarantine Location
- Miscellaneous Settings

Advanced Configuration Options

If **Include original data as attachment** is enabled, the XML file will be attached to the output message.

Supported Notifications

The importer supports the following notification types:

- **Quarantine file**
- **Import job stopped**
- **No data captured**

- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Failed to quarantine file**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users (N/A)
- Filters
- Targets
- Importer Settings

NTR-X

NTR-X is a cloud-ready omnichannel compliance recording solution which allows for recording all your regulated employee communications - traditional, unified, mobile - and ensuring compliance with all global regulations.

Activities Captured

- Calls

Captured messages can contain:

- Participants: From, To
- Call start time (as a timestamp)

- Call duration
- Audio attachment files in MP3 format

File Formats Supported by the Collector

- .xml

Source Configuration

For information on how to configure the following sections of the **Source** tab, see:

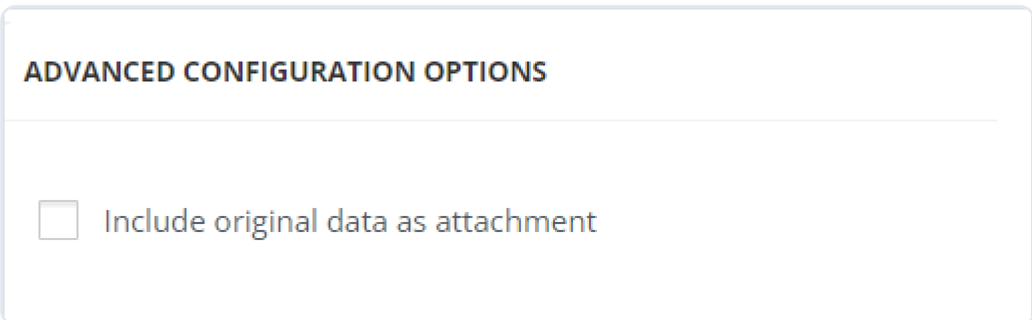
- File Source Configuration
- PGP Configurations
- Quarantine Location

Notes

- The source file group should contain an MP3 file and an XML file with the same GUID as a file name.
- When configuring the SFTP source, the **Download subdirectory recursively** option should be enabled as the expected file group (an MP3 file and an XML file) is nested with NTR-X structure.
- Ensure not to exceed the Windows limitation for file names when processing ZIP files as they may not be processed due to the file name length of the file group.

Advanced Configuration Options

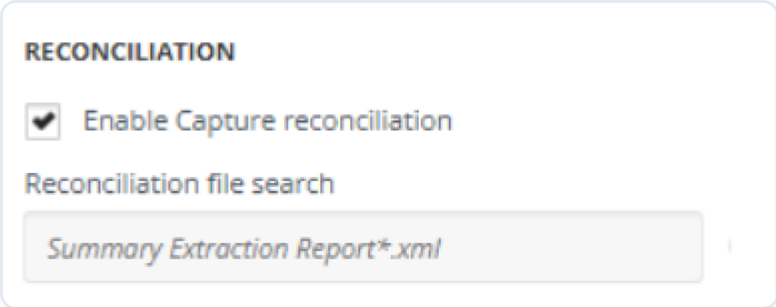
If **Include original data as attachment** is checked, the XML file will be attached to the output message.



Reconciliation

Select **Enable Capture reconciliation** to reconcile the number of messages that Arctera Capture processes against the message count reported by the source.

In the **Reconciliation file search** field, specify the pattern that Arctera Capture uses to identify the reconciliation file, for example, `Summary Extraction Report*.xml`. Arctera Capture reads the source message count from the matching summary extraction report and reconciles it against the processed messages.



Supported Notifications

The importer supports the following notification types:

- **Quarantine file**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Failed to quarantine file**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users (N/A)
- Filters
- Targets
- Importer Settings

OneDrive for Business

OneDrive is a file-hosting service operated by Microsoft as part of its suite of online services which allows you to store, share and synchronize work files.

The OneDrive for Business collector features include Monitored Users management, i.e., it is possible to specify which users accounts of Microsoft OneDrive should be captured.

OneDrive metadata is used to create a Arctera Capture email file. The metadata includes document creator (author in the Arctera Capture email file), the file name (subject), Modified date (sent date), item id, name, CreatedBy, CreatedDateTime, LastModifiedBy, LastModifiedDateTime, webUrl, size, parentReference, folderId and any other tags listed in the message body are added to the email file body.

Activities Captured

- Uploaded files
- Renamed files
- Delete event without the file

> **Note:** Delete events are not captured during the first run and immediately after the deletion.

> **Note:** Hard deleted items, i.e., items that have been deleted from Recycle bin as well, are not captured.

- New created documents via browser with the file

> **Note:** If there are multiple activities performed in the same file, only the most recent one will be recorded.

> **Note:** Microsoft OneNote files (where users' notes, drawings, screen clippings, and audio commentaries are gathered) are captured.

Activities Not Captured

- 'Move to' events with the file
- Download
- Preview
- Preview in the browser
- All folder activities (create, delete, rename, move, or copy)
- Flow activities

Microsoft Entra ID App Creation

To authenticate for the collector configuration, you need to create a Microsoft Entra ID Application.

To create an app:

1. Create an O365 account and open Azure Portal using the same credentials as for O365 (Global Admin).
2. Click **Microsoft Entra ID** at the top of the page and select **App Registration** from the left-side navigation pane.
3. Click the **+New registration** button.
4. Enter a **Name** for the application and click **Register**.
5. Find and make a note your **Application (client) ID** and **Directory(tenant) ID** as this is needed for configuring the collector in Arctera Capture.
6. In the navigation pane to the left, go to **Certificates & secrets**.
7. Click the **Upload certificate** button.
8. Select a certificate (public key) with one of the following file types: .cer,.pem, .crt, and click **Add**. For more information on how to create a certificate, see Creating a Certificate (Private and Public Keys).

Microsoft Entra ID Permissions

For permissions:

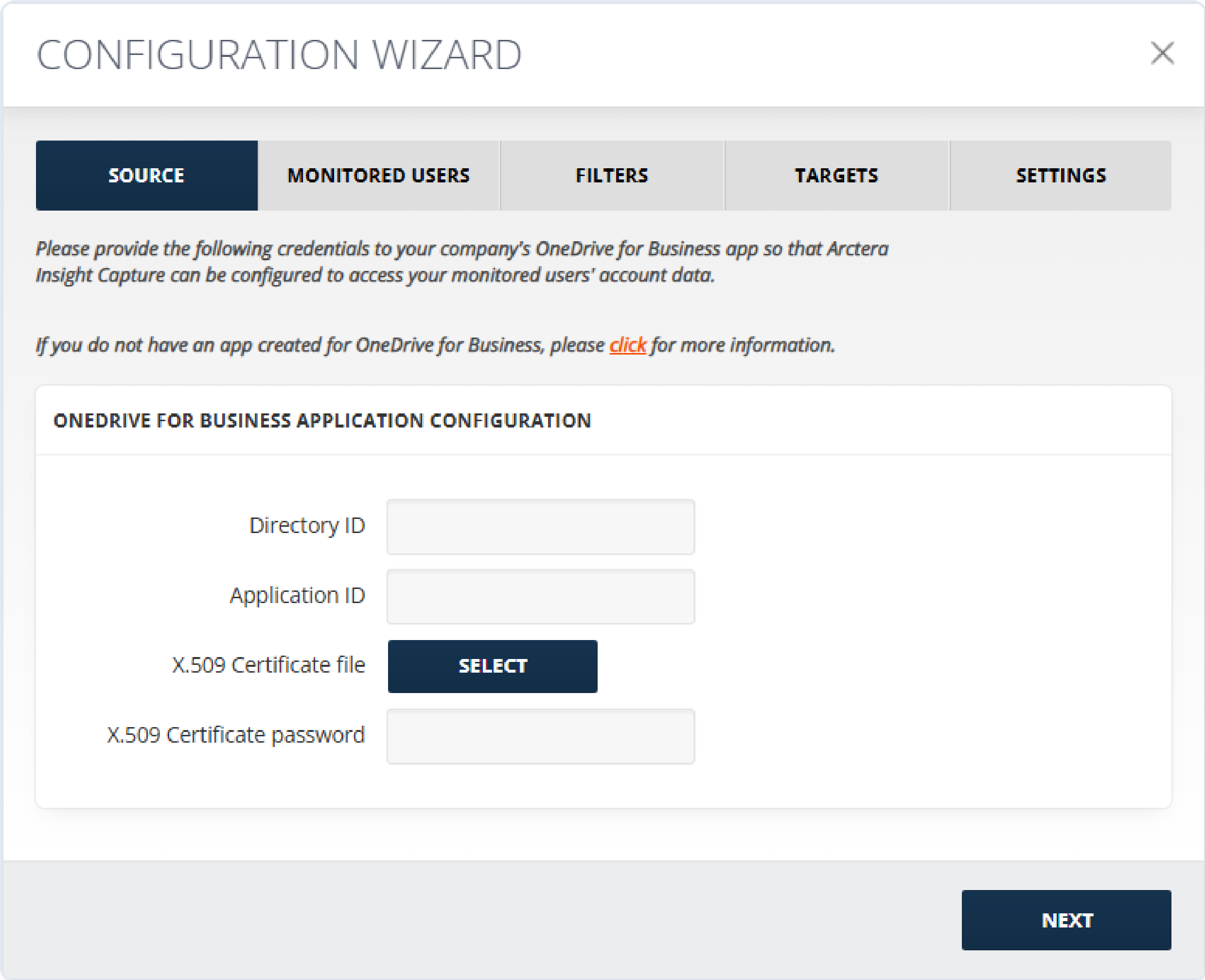
1. In the navigation pane to the left, click **API permissions**.

2. Click **Microsoft Graph**, and in the opened pane select **Application permissions**.
3. Add the following permissions:
    - Files: Files.Read.All
    - Directory: Directory.Read.All
    - User: User.Read.All
4. Once you have selected all check boxes, click **Add Permissions**.
5. Get back to the **API permissions** section, click **+ Add a permission** and select **SharePoint API** with **Application permissions**. These are the permissions you need to grant:
    - Sites: Sites.FullControl.All; Sites.Read.All
    - User: User.Read.All
    - TermStore: TermStore.Read.All
6. Click **Add Permissions**.
7. Grant all the above-mentioned permissions.

Source Configuration

To configure the source:

1. Add **Application ID** from the Entra ID Directory > App Registrations > \<your app name\> section.
2. Select the **X.509 Certificate** file.
3. Enter the **X.509 Certificate password**. The **Certificate thumbprint** field will be auto populated in case the collector was previously configured by uploading a certificate.
4. After clicking **Next**, a pop-up window should appear where you can provide the O365 Global Admin user credentials (note that usually the pop-up is being blocked by the browser, so pay attention to the top right corner of the browser if the popup is not appearing). In the next window, click **Accept** to grant the permissions.



Attachments Configuration

nd add a --- layout: doc title: "Attachments Configuration" source_url: "https://www.veritas.com/content/support/en_US/doc/161740922-161863400-0/v161735038-161863400"

When the **Ignore Attachments** checkbox is checked, all the attachments are being excluded from the message which will enhance the collector performance. Each message will contain only information and the link of the excluded attachment.

- **Include original data as attachment**: If checked, the message original data is attached to the output file.

> **Note:** Not applicable to the EV Folder target.

- When **Do not download files greater than X megabyte(s)** is selected, the files bigger than the filled-in number of megabytes are not downloaded. In the **Custom Message** field, a text for those excluded files can be specified. For example, "Files {0} are not imported, because they are greater than {1} megabytes". {0} is used to add the name of the file and {1} is used to add the number of megabytes specified above.

- In the **File Types** field, the types of files that should not be downloaded can be specified in the following format: e.g., .txt | .xml. The vertical bar is used to separate the file types.

Timestamp Formatting

In addition to the primary stamp, a second timestamp can be enabled with its time zone. From the drop-down menu you can choose the time zone of the timestamp. The format of the timestamp in the output message can also be specified from the six options in the **Date Time Format** drop-down list.

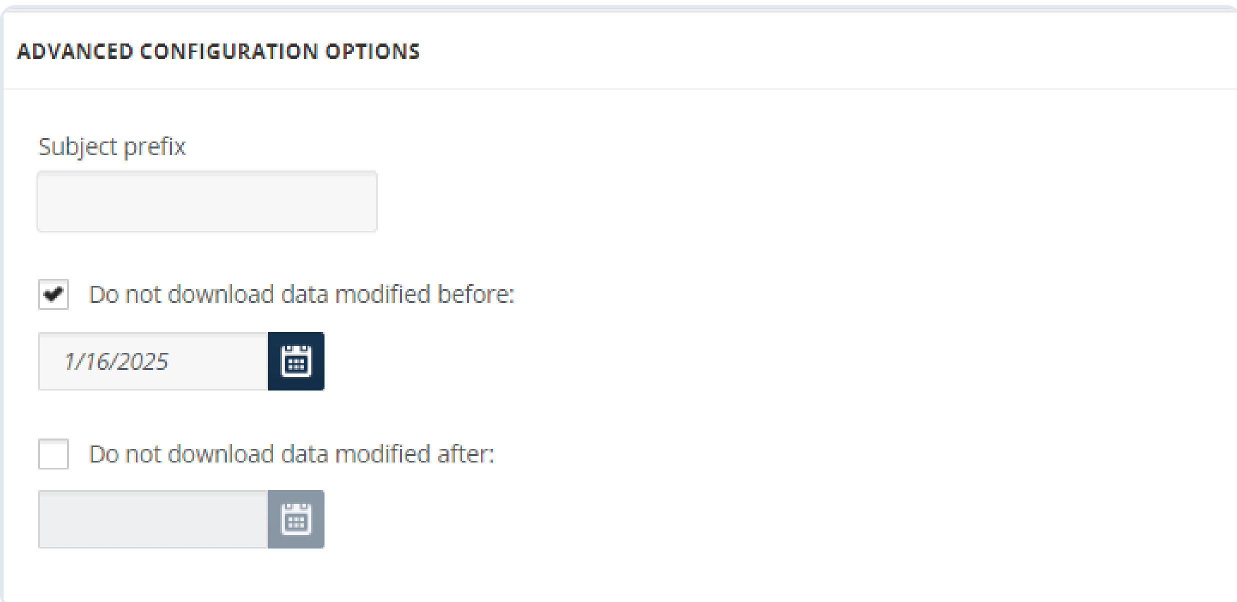
Advanced Configuration Options

To configure advanced options:

1. Specify the **Subject Prefix** in the subject line of imported emails. This is useful for organizing imported data, i.e., when multiple sources share a common target.

   > **Note:** Not applicable to the EV Folder target.

2. Specify **Do not download data modified before** and **Do not download data modified after** to allow cutting off data outside the set date range. If the before date is set to 08/17/2023 and the after date is set to 08/25/2023, only the data between these two dates will be downloaded. Data outside that range will be ignored. Note that both options can be used independently as well.



Supported Notifications

The importer supports the following notification types:

- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users
- Filters
- Targets
- Importer Settings

Pivot

Pivot is an instant messaging platform that allows collaboration with financial market participants over its secure and fast network.

Activities Captured

- Participant entered:
    - Date time

  - Internal flag
  - Corporate email ID
- Message:
  - Date time
  - Messages
- Participant left:
  - Date time
  - Corporate email ID

File Formats Supported by the Collector

- .xml

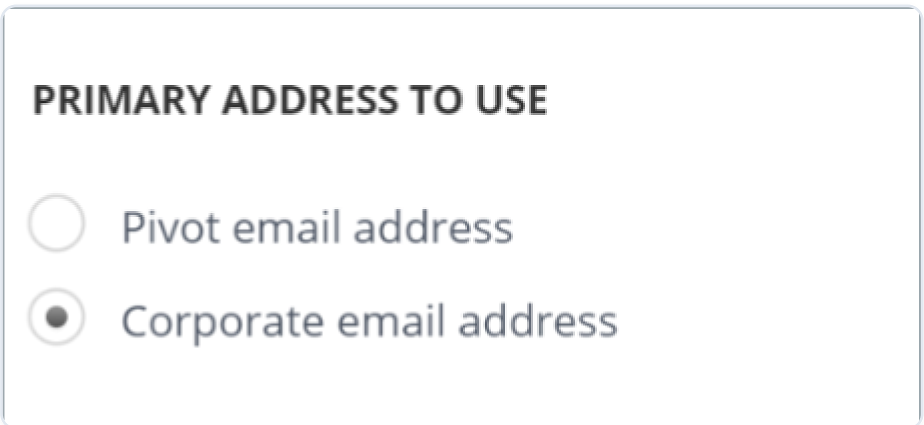
Source Configuration

For information on how to configure the following sections of the **Source** tab, see:

- File Source Configuration
- PGP Configurations
- Quarantine Location
- Miscellaneous Settings

Primary Address to Use

Choose the email address type you would like Arctera Capture to prioritize when processing data from users that have both Pivot email address and Corporate email address.



Supported Notifications

The importer supports the following notification types:

- **Quarantine file**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Failed to quarantine file**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users (N/A)
- Filters
- Targets
- Importer Settings

Progress ShareFile

Progress ShareFile provides secure file sharing, storage, sync and more - all built for business. The Progress ShareFile collector does not capture ShareFile activities for clients. The collector requires a service account to create the API.

Activities Captured

- Files - uploaded/deleted/archived/downloaded/viewed (Audio_Listen and Video_View for MP3/MP4 file types accordingly)/shared (including encrypted messages)/moved/checked in/out
- Folders - created/moved (currently, only the activity is captured)/shared/deleted
- Login info
- Share file requests
- Text-only messages
- Share file request message
- Revoked messages

> **Note:** We recommend using the owner account for authentication. Note that activities performed by the user of the Org. Owner account are not captured.

Notes

- We can upload several files with the same name in File Box. The generated report contains only path info for the uploaded files, which is the same for all the items having the same name. Hence, Arctera Capture attaches the same file (the latest among the ones with the same name) to all the generated messages.
- If files having the same name are downloaded, in all the generated messages we will have the same file attached. The reason for this issue is the same, as for the File upload. If the file is permanently deleted/archived, the activity is not captured.
- In case files are sent via Outlook and the shared information is not recorded in the ShareFile environment, the captured message will have an empty body.

Creating Progress ShareFile App

To create an app:

1. Navigate to https://api.sharefile.com/.
2. Log into your Progress ShareFile account.

> **Note:** The account should be a Service Account.

3. Click **Get an API Key**.

4. Fill in the **Application Name** field.
5. In the **Redirect URI** field, add the redirect URL address.

> **Note:** This can be found in the click information of the Source configuration.

6. Click **Generate API Key**.
7. Copy the generated **Client Id** and **Client Secret** and save it in a secure location.

Granting Permissions

To be able to capture data, Org Owner must give the Access other users' File Boxes and Sent Items specific permission.

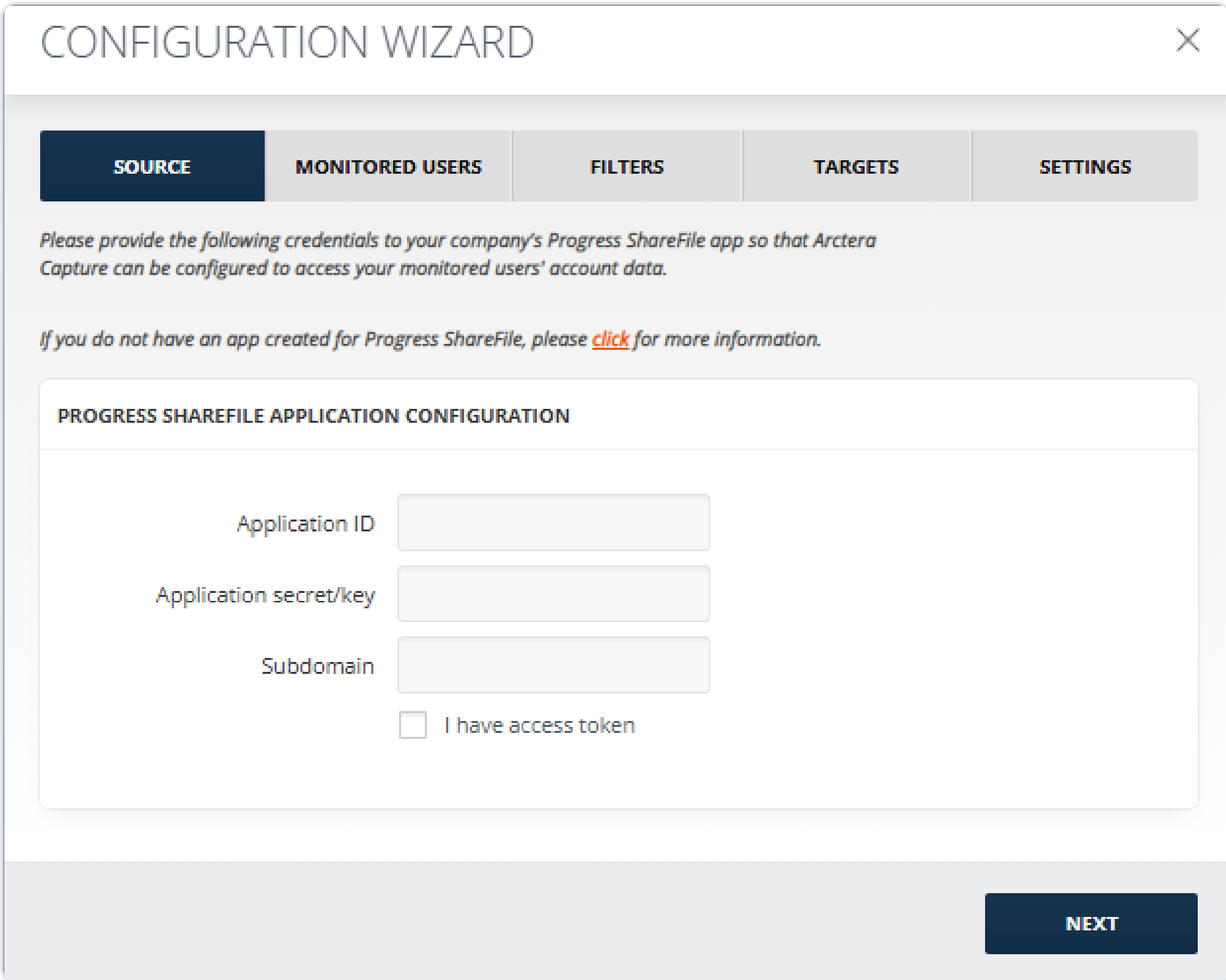
To grant the permission:

1. Navigate to your ShareFile instance.
2. Log into your Progress ShareFile Org Owner account.
3. Go to **People** > **Browse Employees**.
4. Select the employee to which the permission must be granted.
5. Scroll down to **Employee User Settings** and click **User Access**.
6. In the **Files and Folder** sub-section, enable the **Access other users' File Boxes and Sent Items** checkbox.
7. 7\. Scroll down and click **Save Changes**.

Source Configuration

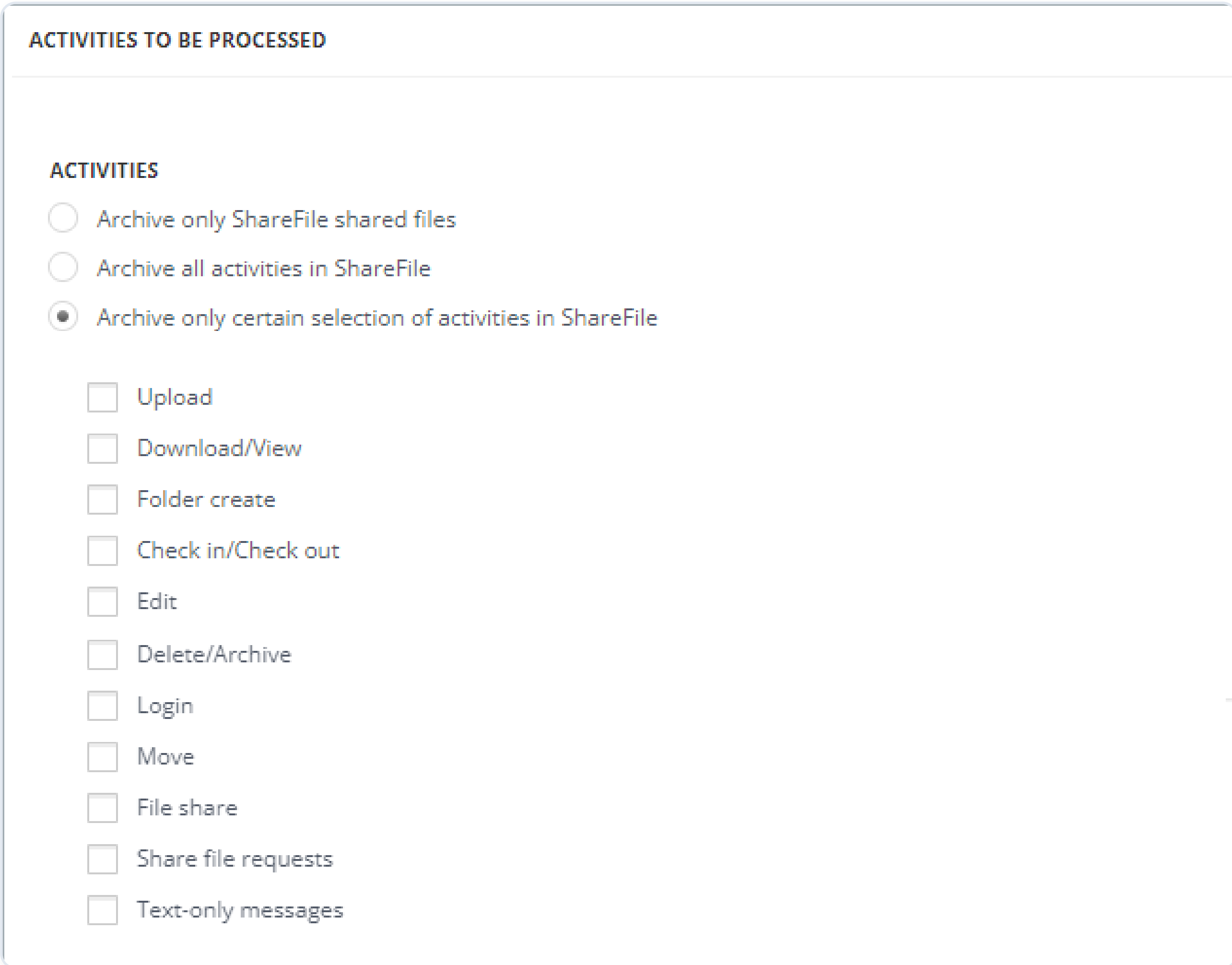
To configure the collector:

1. In the **Application ID** field, fill in the copied Client Id.
2. In the **Application Secret/Key** field, fill in the copied Client Secret.
3. Add subdomain of the ShareFile workspace into the **SubDomain** field. (SubDomain is located under **Admin settings** > **Company info** > **Edit company Branding**).



Activities to Be Processed

You can choose which activities are processed from Progress ShareFile.

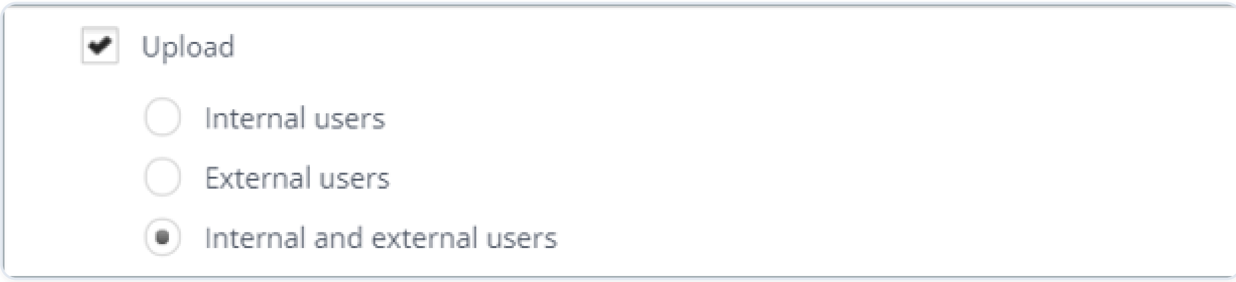


- **Archive only ShareFile shared files** - Only shared files are imported.
- **Archive all activities in ShareFile** - All activities are captured and imported.
- **Archive only certain selection of activities in ShareFile** - Activities to be captured and imported can be selected separately from the list below:
  - **Upload**
  - **Download/View**
  - **Folder create**
  - **Check in/Check out**
  - **Edit**
  - **Delete/Archive**
  - **Login**
  - **Move**
  - **File share**
  - **Share file requests**

  - **Text-only messages**

In case Upload activity is activated, the following options become available:

- **Internal users** - when enabled, only the upload activity of internal users will be captured
- **External users** - when enabled, only the upload activity of external users will be captured
- **Internal and external users** - when enabled, the upload activity of both the internal and external user will be captured.



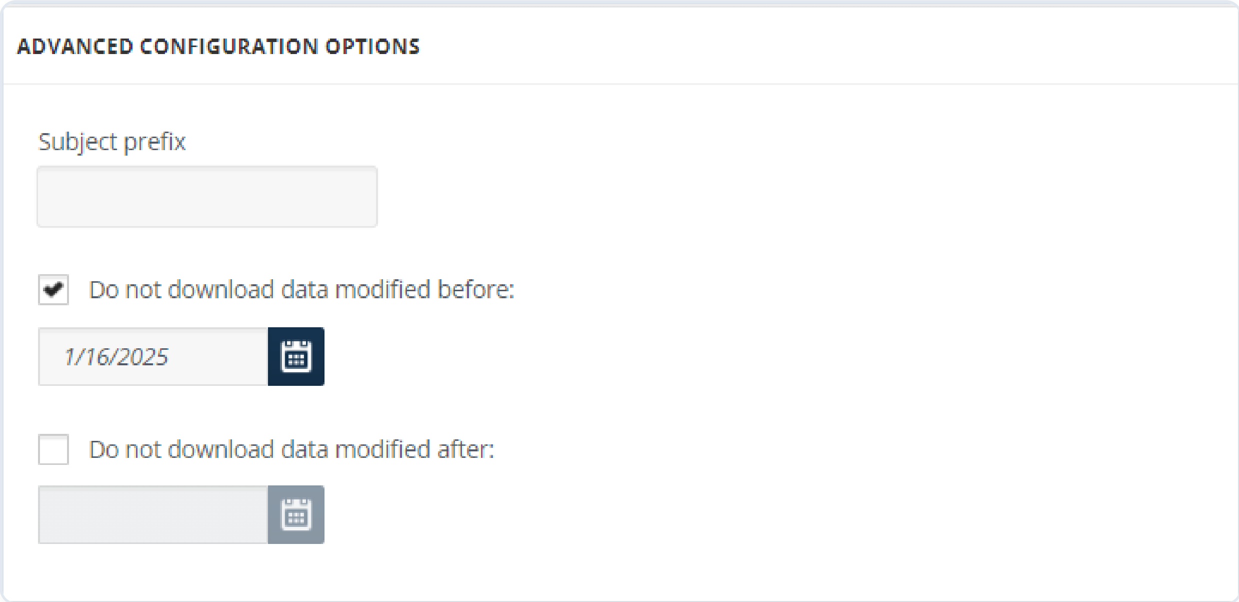
Advanced Configuration Options

To configure advanced options:

1. Specify the **Subject Prefix** in the subject line of imported emails. This is useful for organizing imported data, i.e., when multiple sources share a common target.

   > **Note:** Not applicable to the EV Folder target.

2. Specify **Do not download data modified before** and **Do not download data modified after** to allow cutting off data outside the set date range. If the before date is set to 08/17/2021 and the after date is set to 08/25/2021, only the data between these two dates will be downloaded. Data outside that time frame will be ignored. Note that both options can be used independently as well.



Attachments Configuration

- **Include original data as attachment**: If checked, the message original data is attached to the output file.

> **Note:** Not applicable to the EV Folder target.

- **Ignore attachments**: If checked, all the attachments are excluded from the message enhancing the collector performance. Each message will contain info and the link to the excluded attachment.
- When **Do not download files greater than X megabyte(s)** is selected, the files bigger than the filled-in number of megabytes are not downloaded. In the **Custom Message** field, a text for those excluded files can be specified. For example, "Files {0} are not imported, because they are greater than {1} megabytes". {0} is used to add the name of the file and {1} is used to add the number of megabytes specified above.
- In the **File Types** field, the types of files that should not be downloaded can be specified in the following format: e.g., .txt | .xml. The vertical bar is used to separate the file types.

Supported Notifications

The importer supports the following notification types:

- **Import job stopped**
- **No data captured**
- **Component deleted**

- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users
- Filters
- Targets
- Importer Settings

Redtail Speak

Redtail is a CRM system that focuses on financial advisor/client relationships. The Speak feature is an add-on model that allows advisors to communicate with their clients, team members, and the overall company. Through its Speak platform, Redtail can send text messages to communicate with the clients and recognizes the need for compliance.

Arctera Capture collects Redtail Speak messages from the Redtail Speak SMTP server. For setting up an SMTP server, contact Arctera Support.

Activities Captured

- One-on-one chats with team members
- Public/private group conversations

File Formats Supported by the Collector

- .eml

Source Configuration

For information on how to configure the following sections of the **Source** tab, see:

- File Source Configuration
- PGP Configurations
- Quarantine Location
- Miscellaneous Settings

Supported Notifications

The importer supports the following notification types:

- **Quarantine file**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Failed to quarantine file**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users (N/A)
- Filters
- Targets
- Importer Settings

RingCentral

RingCentral Team Messaging is a team collaboration solution that helps organize and centralize team communication. RingCentral provides a compliance API that will be used to download messages and meeting-based content.

Activities Captured

- Chats
- Tasks
- Notes
- Events
- SMS chats

> **Note:** The outgoing SMS chats of internal users and incoming SMS chats of external users are captured.

- Attachments

> **Note:** Attachment downloading is available only for files uploaded from a local computer. For third-party applications, such as Dropbox, Google Drive, Box, the downloadUrl is not returned, and a message is constructed without an attachment.

Compliance Exports

Compliance Exports is a special capability specifically built for companies and regulated industries, such as financial services, with compliance requirements for using electronic communication in the workplace. This feature is also a fail-safe way of preserving business communications for legal discovery or internal review.

When you download a compliance export, you will receive a .zip file that contains a number of files and folders that contain all of the data associated with your data export. For more information, see Team Messaging Compliance Export File Structure.

> **Note:** Only the content and items that fall within the specified period for the archive are included in the downloaded/compliance export file. Therefore, data outside that time range is not captured.

Creating a RingCentral Application

To create the application:

1. Sign in to the RingCentral Developer Console.
2. You will be navigated to the Apps console where all your apps are listed and can be managed. Click **Create App** at the upper right corner of All applications.

   > **Note:** If you see the **Create App** button, but it is disabled, then your account lacks the permission required to create an app. Contact your account administrator to request this permission.

3. Select your app type and click **Next**.
4. In the next opened window, enter **App Name** and **Description**.
5. Select **No** for Do you intend to promote this app in the RingCentral App Gallery? (For internal-use only).
6. In the **Auth** section, make sure **3-legged OAuth flow authorization code** is enabled and select **Server-side web app (most common)**.
7. In the **OAuth Redirect URI** field, enter the URL of your local environment.

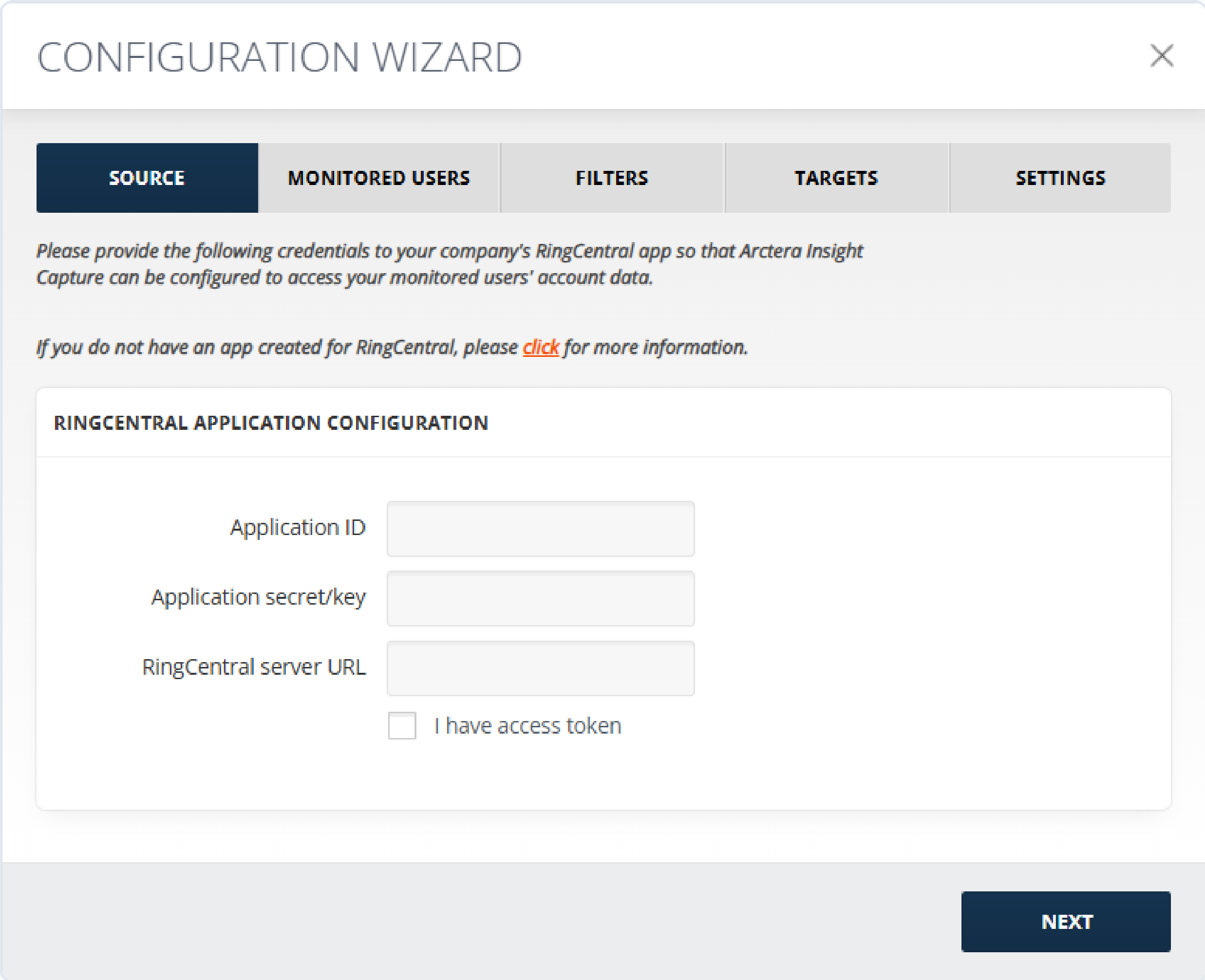
   > **Note:** The **Redirect URI** can be found in the Click information of the collector source configuration.

8. In the **Security** section, select **Read Accounts** and **Team Messaging** from the **App Permissions** drop-down list. Click **Create**.
9. In the opened window, you will find your application details, including Client ID, Client Secret, and RingCentral Server URL. Copy and save them for later using during Source configuration.

Source Configuration

To set up the collector:

- In the **Application ID** field, enter Client ID copied previously, in **Application secret/key**, enter the copied Client Secret, enter the API server URL in the **RingCentral server URL** field, and then click **Next**.



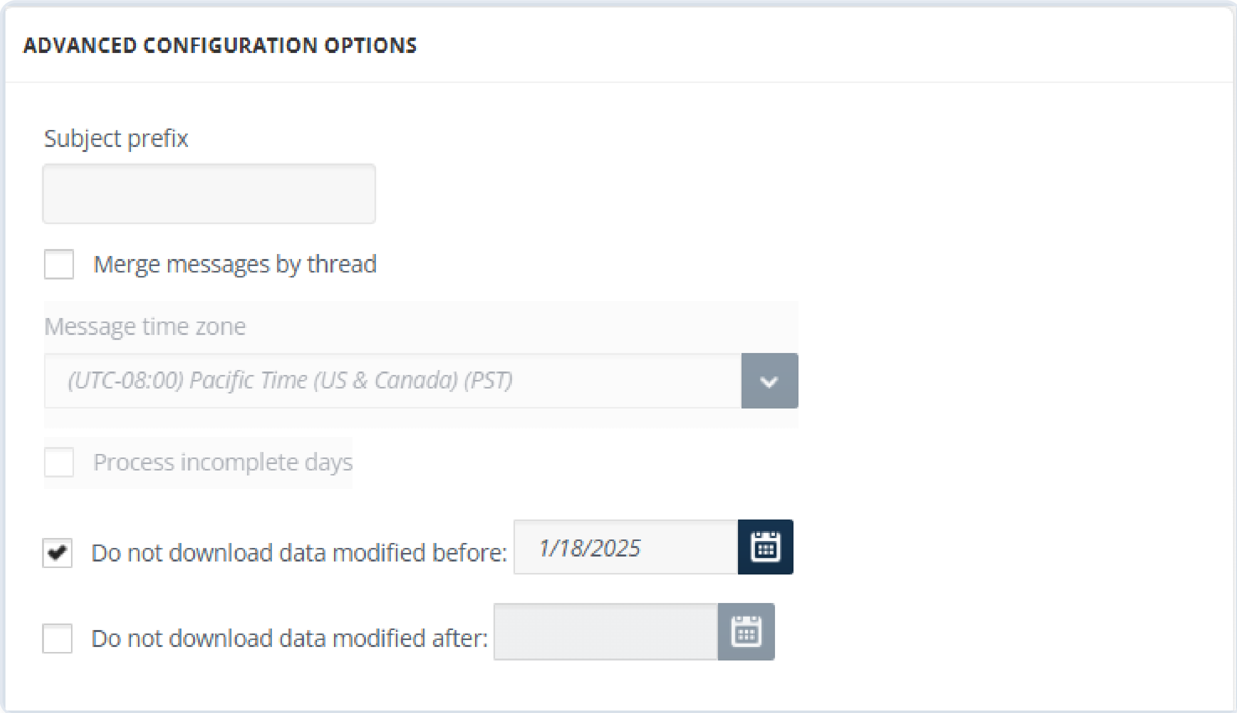
Timestamp Formatting

In addition to the primary stamp, a second timestamp can be enabled with its time zone. From the drop-down menu you can choose the time zone of the timestamp. The format of the timestamp in the output message can also be specified from the six options in the **Date Time Format** drop-down list.

Advanced Configuration Options

There are following advanced options:

- The **Subject Prefix** feature will add a prefix before the message subject to facilitate the search in the target.
- The **Merge message by thread** if checked combines messages by threads rather than sending them one by one.
- Select the **Message time zone** from the drop-down menu. When the **Process incomplete days** option is enabled, the messages of the days that have not yet ended will be imported in a separate email. This option can be selected only if **Merge messages by thread** is selected.
- Options **Do not download data modified before** and **Do not download data modified after** allow cutting off data outside the set date range. If the before date is set to 08/17/2022 and the after date is set to 08/25/2022, only the data between these two dates will be downloaded. Data outside that time frame will be ignored. Note that both options can be used independently as well.

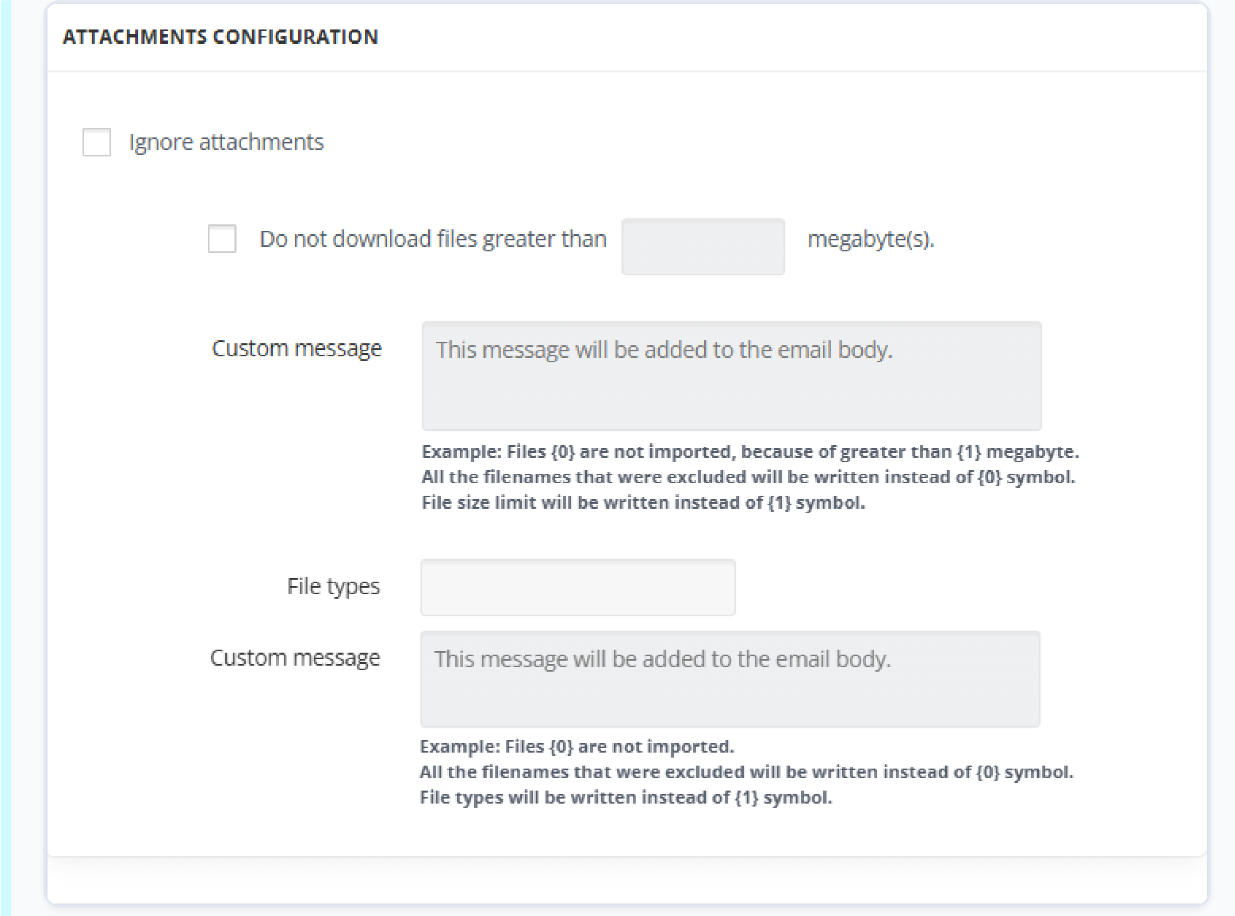


Attachments Configuration

There are the following configuration options:

- When the **Ignore Attachments** checkbox is checked, all the attachments are being excluded from the message which will enhance the collector performance. Each message will contain only information and the link of the excluded attachment.
- When **Do not download files greater than X megabyte(s)** is selected, the files bigger than the filled-in number of megabytes, are not downloaded. In **Custom Message** field, a text for those excluded files can be specified. E.g.,"Files {0} are not imported, because they are greater than {1) megabytes". {0} is used to add the name of the file and {1} is used to add the number of megabytes specified above.
- In the **File Types** field, the types of files that should not be downloaded can be specified in the following format: e.g., .txt | .xml. The vertical bar is used to separate the file types.

> **Note:** In case of using file filtering by size and by type, we recommend using custom messages.



Supported Notifications

The importer supports the following notification types:

- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users
- Filters
- Targets
- Importer Settings

ServiceNow

ServiceNow is a customizable service management platform that facilitates requests for support items such as hardware, software requests. The platform has ability for partners to develop solutions and add to the ServiceNow app library.

Activities Captured

- Live messages with comments and attachments created in My Feed
- Live messages with comments and attachments created in Company Feed
- Live messages with comments and attachments created in Group feed (Public/Private)
- Conversations with comments and attachments (one-on-one, group)
- Deletes
- Polls with choices and votes
- Like counts
- Links
- Mentions
- Emojis

> **Note:** When the group is deleted, the messages are not captured.

Activities not Captured

- Record feed
- Tasks with comments

- Incidents with comments
- Requests with comments
- Requested items with comments
- Problem with comments
- Change request
- Change task

Creating a ServiceNow Application

The administrator of your organization must perform the following steps:

1. Log in to ServiceNow instance and navigate to **System OAuth** > **Application Registry**.
2. Click the **Application Registry** and the applications list will open. Click **New**.
3. Select the **Create an OAuth API endpoint for external clients** option.
4. Enter a name for the application.
5. Unlock the **Redirect_URI** field and enter the URL of your local environment and click the **Submit** button.

   > **Note:** The **Redirect URI** can be found in the Click information of the collector source configuration.

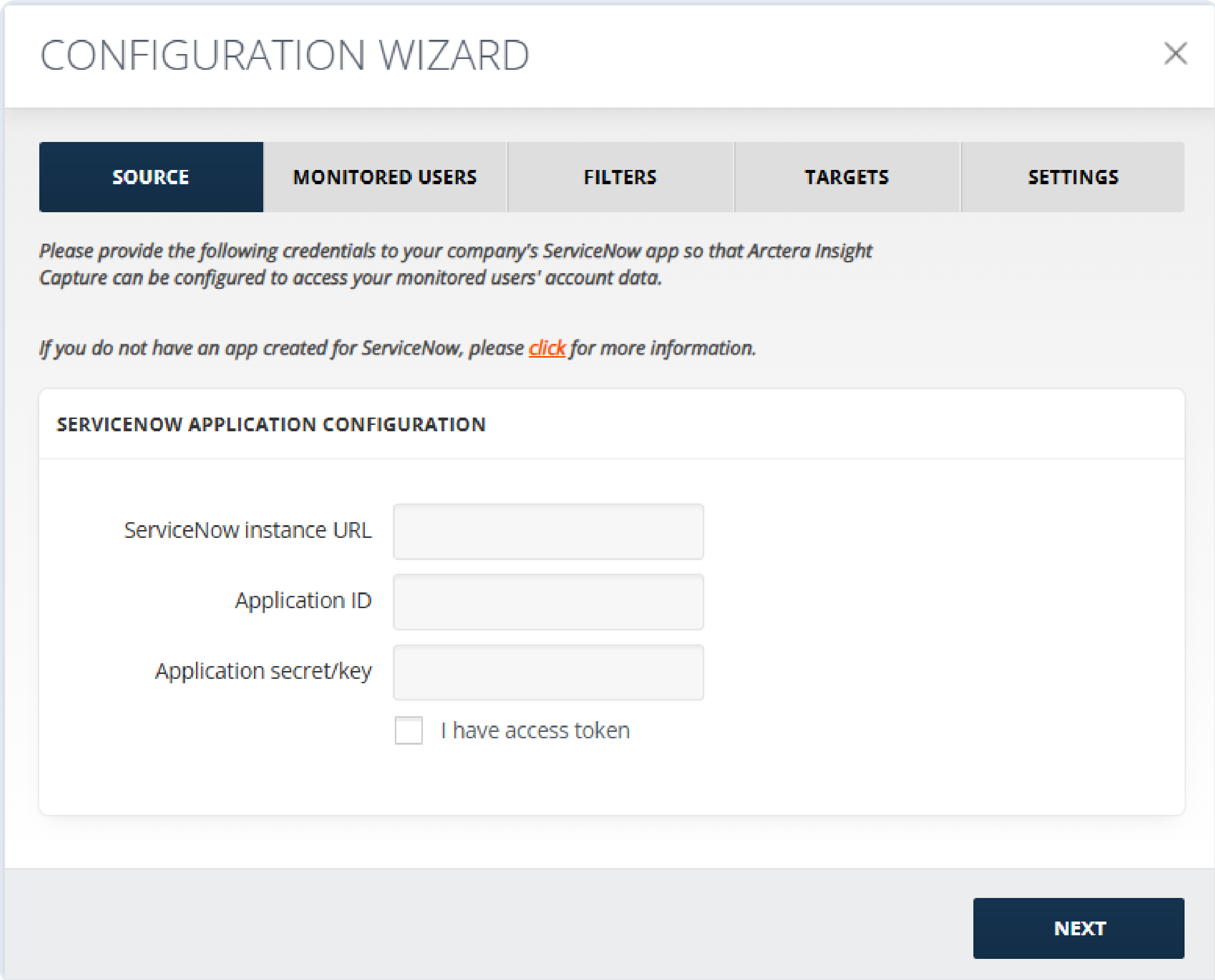
6. After executing the provided steps, on the Application Registry page you will find the application you have just created.

Click your application, and in the opened window, you will find your application details, including Client ID and Client Secret. Copy and save the Client ID and Secret to later provide them to Arctera Capture as part of ServiceNow configuration.

Source Configuration

To set up the collector:

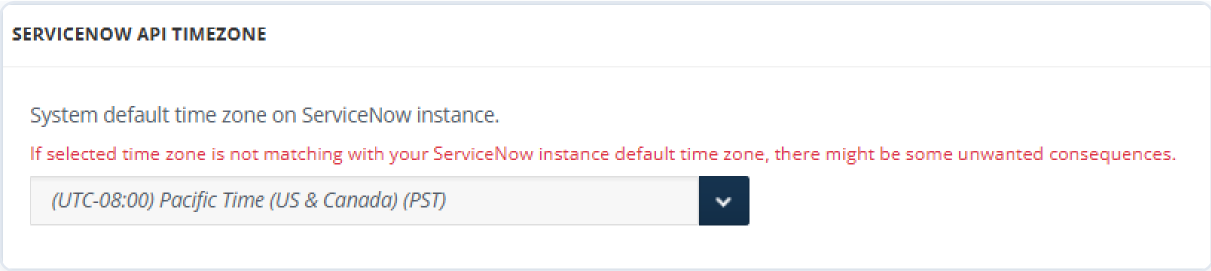
1. Add your **ServiceNow Instance URL**.
2. Add the App Key copied previously in the **Application ID** field.
3. In **Application Secret/Key**, enter copied Secret, and then click **NEXT**.



Timestamp Formatting

In addition to the primary stamp, a second timestamp can be enabled with its time zone. From the drop-down menu you can choose the time zone of the timestamp. The format of the timestamp in the output message can also be specified from the six options in the **Date Time Format** drop-down list.

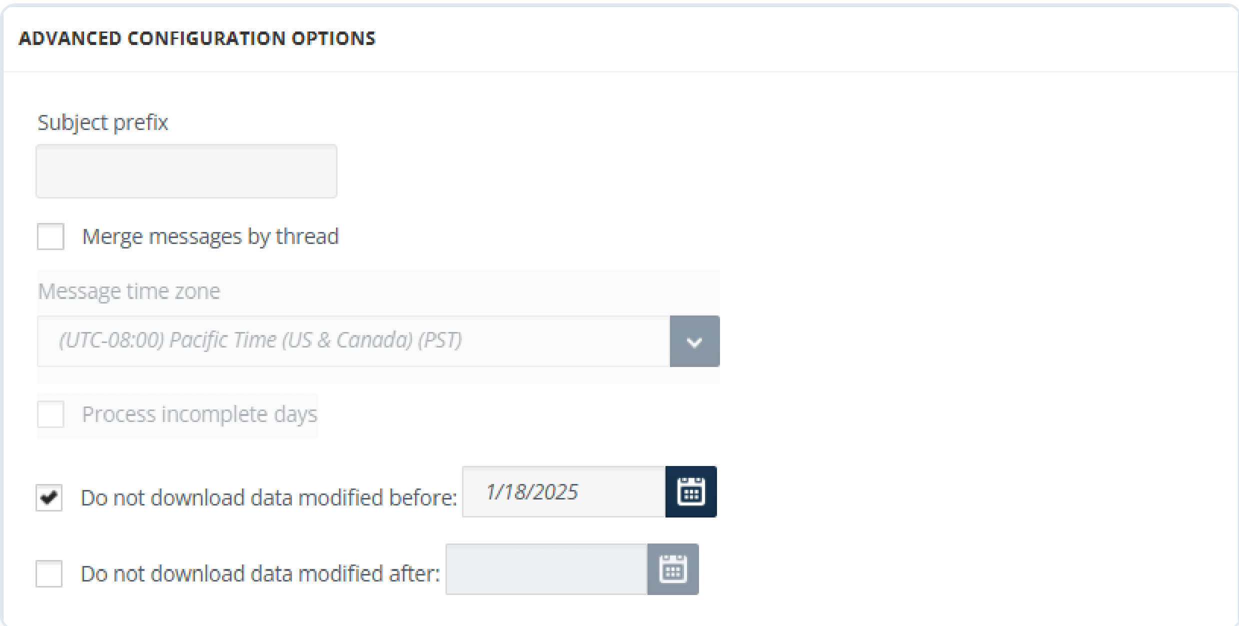
Note: If the selected time zone is not matching with your ServiceNow instance default time zone there might be some unwanted consequences.



Advanced Configuration Options

To configure advanced options:

1. Specify the **Subject Prefix** in the subject line of imported emails. This is useful for organizing imported data, i.e., when multiple sources share a common target.
2. Specify **Do not download data modified before** and **Do not download data modified after** to allow cutting off data outside the set date range. If the before date is set to 08/17/2023 and the after date is set to 08/25/2023, only the data between these two dates will be downloaded. Data outside that range will be ignored. Note that both options can be used independently as well.



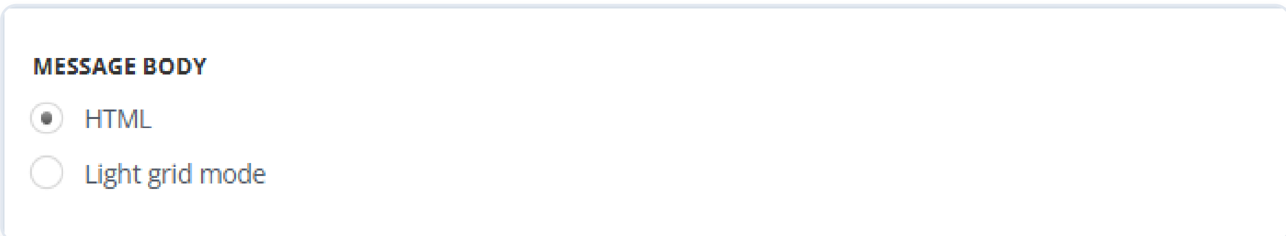
Attachments Configuration

- When **Do not download files greater than X megabyte(s)** is selected, the files bigger than the filled-in number of megabytes, are not downloaded. In **Custom Message** field, a text for those excluded files can be specified. E.g.,"Files {0} are not imported, because they are greater than {1) megabytes". {0} is used to add the name of the file and {1} is used to add the number of megabytes specified above.

- In the **File Types** field, the types of files that should not be downloaded can be specified in the following format: e.g., .txt | .xml. The vertical bar is used to separate the file types.

Message Body

This specifies how the imported message will be displayed in the target. The **Basic HTML** mode organizes the data in a simple way and data displayed in a **Light Grid Mode** is two-toned, easy to be viewed with limited metadata.



Supported Notifications

The importer supports the following notification types:

- **Import job stopped**

- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users
- Filters
- Targets
- Importer Settings

SharePoint

SharePoint is a web-based collaborative platform that integrates with Microsoft Office. Launched in 2001, SharePoint is primarily sold as a document management and storage system, but the product is highly configurable, and the usage varies substantially among organizations.

SharePoint can refer to one or more SharePoint products or technologies, including:

- SharePoint Online
- SharePoint Server
- SharePoint Foundation
- SharePoint Designer 2013
- OneDrive for Business sync

The Arctera Capture SharePoint collector captures data from SharePoint Online.

Activities Captured

- Newsfeed/Document library/ Picture library posts
- Newsfeed /Document library/ Picture library comments
- Custom lists
- Custom lists comments
- Site page comments

> **Note:** The SharePoint CSOM API provides two identical versions of the same data with a different version numbering and for the storage and visibility sack, only one version is kept.

Microsoft Entra ID App Creation

To authenticate for the collector configuration, you need to create a Microsoft Entra IDApplication.

To create an app:

1. Create an O365 account and open Azure Portal using the same credentials as for O365 (Global Admin).
2. Click **Microsoft Entra ID** at the top of the page and select **App Registration** from the left-side navigation pane.
3. Click the **+New registration** button.
4. Enter a **Name** for the application and click **Register**.
5. Find and make a note your **Application (client) ID** and **Directory(tenant) ID** as this is needed for configuring the collector in Arctera Capture.
6. In the navigation pane to the left, go to **Certificates & secrets**.
7. Click the **Upload certificate** button.
8. Select a certificate (public key) with one of the following file types: .cer,.pem, .crt, and click **Add**. For more information on how to create a certificate, see Creating a Certificate (Private and Public Keys).

Microsoft Entra ID Permissions

For permissions:

1. In the navigation pane to the left, click **API permissions**.
2. Click **Microsoft Graph**, and in the opened pane select **Application permissions**.
3. Add the following permissions:
   - Sites: Sites.Read.All
   - Files: Files.Read.All
   - Directory: Directory.Read.All
   - User: User.Read.All
4. Click **Add permissions**.
5. Get back to **API permissions** section, click **+ Add a permission** and select **SharePoint API with Application permissions**. These are the permissions you need to grant:
   - Sites: Sites.Read.All
   - User: User.Read.All
   - TermStore: TermStore.Read.All
6. Click **Add permissions**.
7. Grant all the above-mentioned permissions.

Setting Up Security and Compliance for Microsoft 365

To set up Microsoft 365 Security and Compliance:

1. Navigate to Information Governance website in the Microsoft Compliance center.
2. Click **+New retention policy** to start the setup wizard.
3. Add a **Name** and a **Description** for the policy and click **Next**.
4. Choose the applications to apply the retention policy to. You can either select **Apply policy only to content in Exchange email, public folders, Office 365 groups, OneDrive, and SharePoint documents**.
5. Once you choose the locations where the retention policy applies, click **Next**.
6. Set the retention period of the messages along with other options. Configure the settings so that they meet your compliance requirements and click **Next**. Review the settings that you have chosen. If everything is correct, click **Submit**.

> **Note:** Note that it would take up to 1 day to apply the retention policy to the locations you chose.

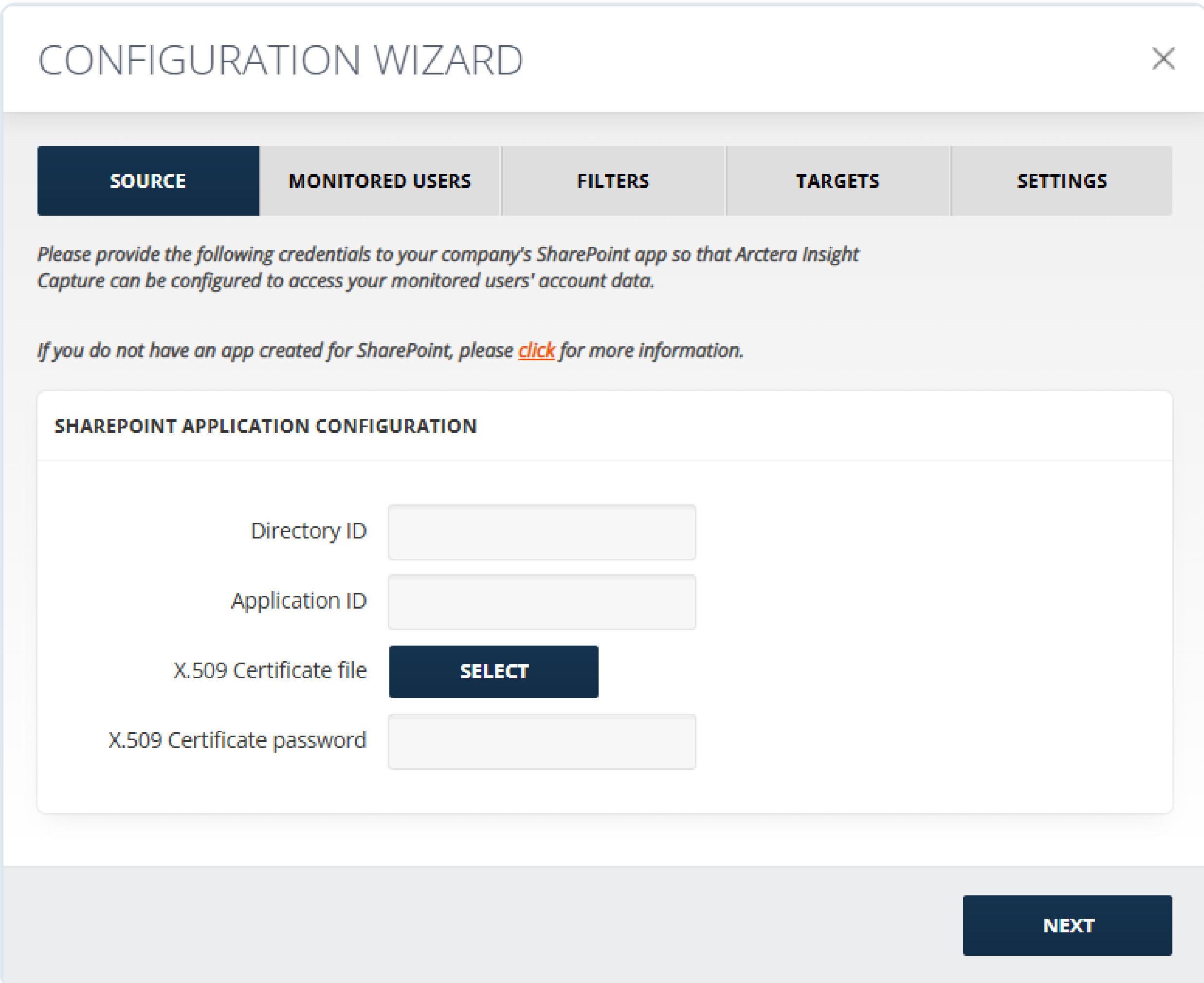
Source Configuration

To set up the collector:

1. Provide **Directory ID**.

You can copy the **Application ID** from the Entra ID > App Registrations > \<your app name\> section.

1. Select the **X.509 Certificate** file.
2. Enter the **X.509 Certificate password**. The **Certificate thumbprint** field will be auto populated in case the collector was previously configured by uploading a certificate.



For attachments configuration:

- **Include original data as attachment**: If checked, the message original data is attached to the output file.

> **Note:** Not applicable to the EV Folder target.

- **Ignore attachments**: If checked, all the attachments are excluded from the message enhancing the collector performance. Each message will contain info and the link to the excluded attachment.
- When **Do not download files greater than X megabyte(s)** is selected, the files bigger than the filled-in number of megabytes are not downloaded. In the **Custom Message** field, a text for those excluded files can be specified. For example, "Files {0} are not imported, because they are greater than {1} megabytes". {0} is used to add the name of the file and {1} is used to add the number of megabytes specified above.
- In the **File Types** field, the types of files that should not be downloaded can be specified in the following format: e.g., .txt | .xml. The vertical bar is used to separate the file types.

SharePoint Activities

For SharePoint activities:

1. Activate **Monitor all sites** in case all SharePoint sites should be monitored. In this case, file upload and download options will be inactive.
2. Activate **Monitor certain sites** in case only certain SharePoint sites/sub-sites should be monitored.
3. Upload the CSV file that includes:
   - The site/sub-site URL which can be found by clicking the **Copy** button from the right-side opened **Page Details** window.

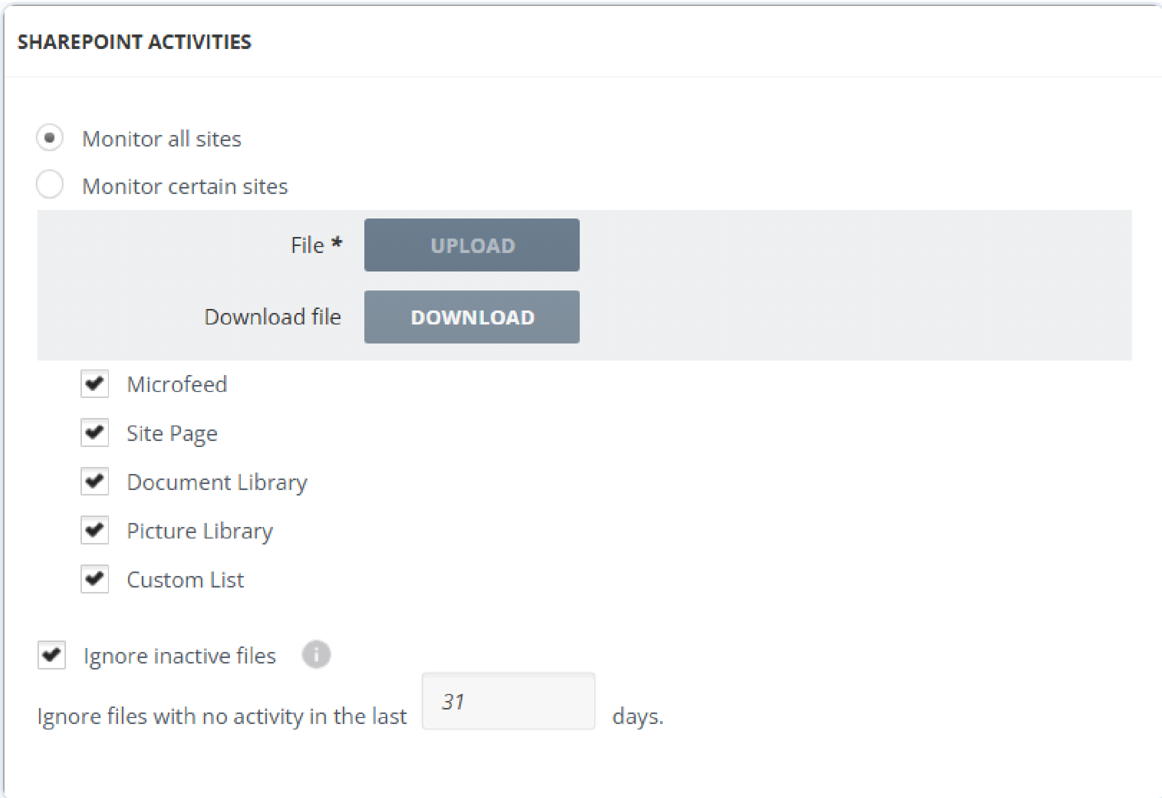
- TRUE or FALSE options which will specify whether the sub-sites should or should not be monitored accordingly. If not specified, the default value will be FALSE, i.e., sub-sites will not be monitored.

4. In case you need to make changes in the CSV, download the already uploaded file, make the necessary changes, and upload it again.

The following activities can be captured:

- Microfeed
- Site page
- Document library
- Picture library
- Custom list

> **Note:** If the file names contain the "#" and "%" symbols, they will not be downloaded.



By enabling the **Ignore inactive files** checkbox and specifying the **Ignore files with no activity in the last X days**, only the files with their comments modified within the specified days will be captured.

Timestamp Formatting

In addition to the primary stamp, a second timestamp can be enabled with its time zone. From the drop-down menu you can choose the time zone of the timestamp. The format of the timestamp in the output message can also be specified from the six options in the **Date Time Format** drop-down list.

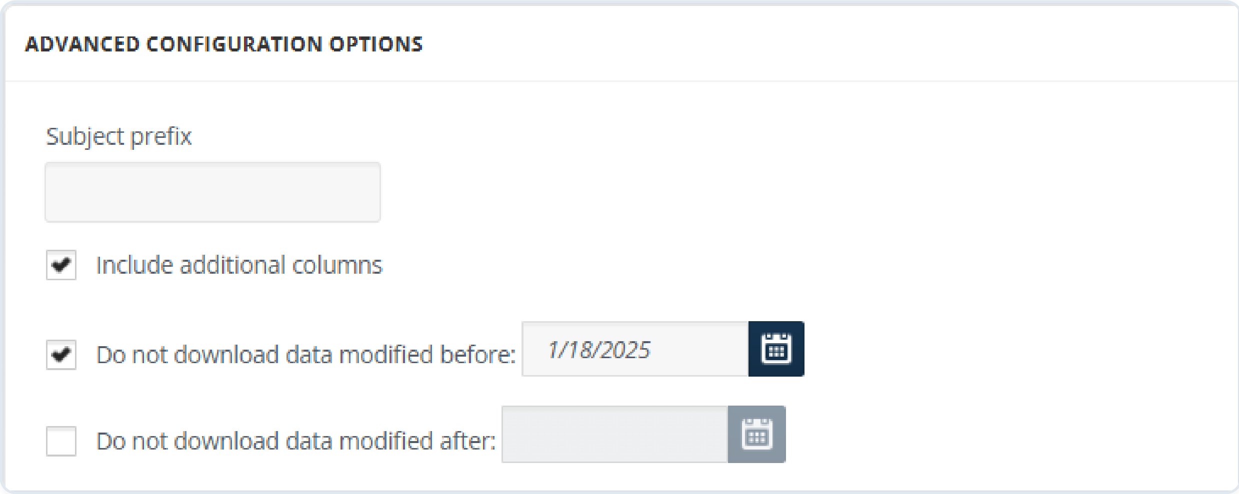
Advanced Configuration Options

To configure advanced options:

1. Specify the **Subject Prefix** in the subject line of imported emails. This is useful for organizing imported data, i.e., when multiple sources share a common target.

   > **Note:** Not applicable to the EV Folder target.

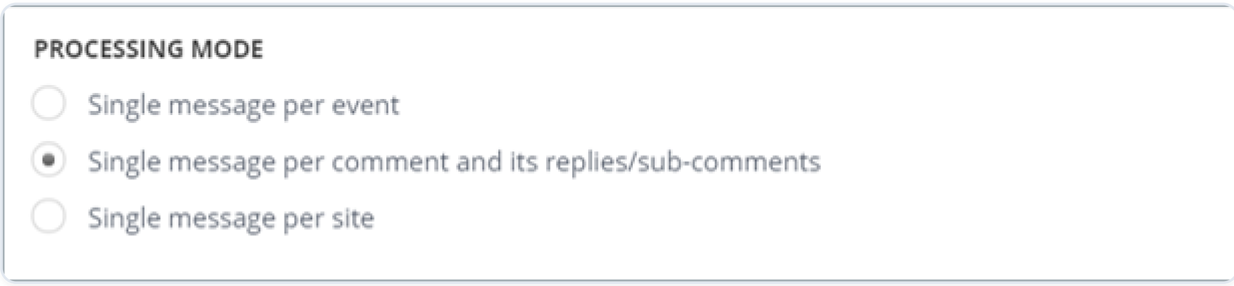
2. Enable **Include additional columns** to include more columns in the output message.
3. Specify **Do not download data modified before** and **Do not download data modified after** to allow cutting off data outside the set date range. If the before date is set to 08/17/2023 and the after date is set to 08/25/2023, only the data between these two dates will be downloaded. Data outside that range will be ignored. Note that both options can be used independently as well.



Processing Mode

There are the following options:

- The **Single message per event** captures each event (post, comment, reply) in one message.
- The **Single message per comment and its replies/sub-comments** captures a message and all replies and comments related to it in one output message.
- The **Single message per site** captures all messages and their replies and comments in one combined message.



If any event has been changed after a single Arctera Capture run, when it is run the next time, the updated version of the event will be imported. The processing modes apply both to the Newsfeed and to the Site Page comments.

Supported Notifications

The importer supports the following notification types:

- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**

- **Import job running threshold exceeded**
- **Importer data deleted**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users
- Filters
- Targets
- Importer Settings

Slack eDiscovery

The Slack eDiscovery collector allows retrieving data from Slack Enterprise account workspaces, consolidate it into one archive or mail for eDiscovery. Enterprise Grid is a "network" of two or more Slack workspace instances. Each Slack workspace has its team ID, its directory of members, its channels, conversations, and files.

To set up the Slack eDiscovery collector, contact Slack at exports@slack.com and ask to enable Discovery API for your organization before finishing the collector set up.

Activities Captured

- Activities from all workspaces
- Direct messages
- Canvases

> **Note:** The canvas download activities of the admin account are not captured.

- Canvas activities

> **Note:** Deleted canvases and canvas items are not captured.

Canvas comments

Canvas content

> **Note:** The latest version in the canvas content is captured in case of multiple edits. **Note:** Reauthentication is required for to capture canvases.

- Multi-participant direct messages
- Channel conversations/messages
- Attachments (the attachment itself is included in the generated message as an attachment)
- Attachments shared using third-party integrations such as OneDrive (only the link is included in the body of the generated message)
- Emojis (as texts)
- GIFs
- Deletes (including the deleted message and the event itself)
- Edits (including the message before and after it is edited)
- Guest conversations
- Message reactions
- Shared channel events (channels shared with external organizations)
- Channel join event
- Set channel purpose event
- Files delete event
- Emails sent from supported email services

> **Note:** Capturing the edit and delete activities depend on the retention policy of your Slack Enterprise account. You can set message retention to "Keep all messages and keep edit and deletion logs" from https://my.slack.com/admin/settings#data_retention. This will work for public channels. If you need to capture all edit and deletion logs for private channels

> and direct messages as well, please check the Retention Policy of your Slack Enterprise account.

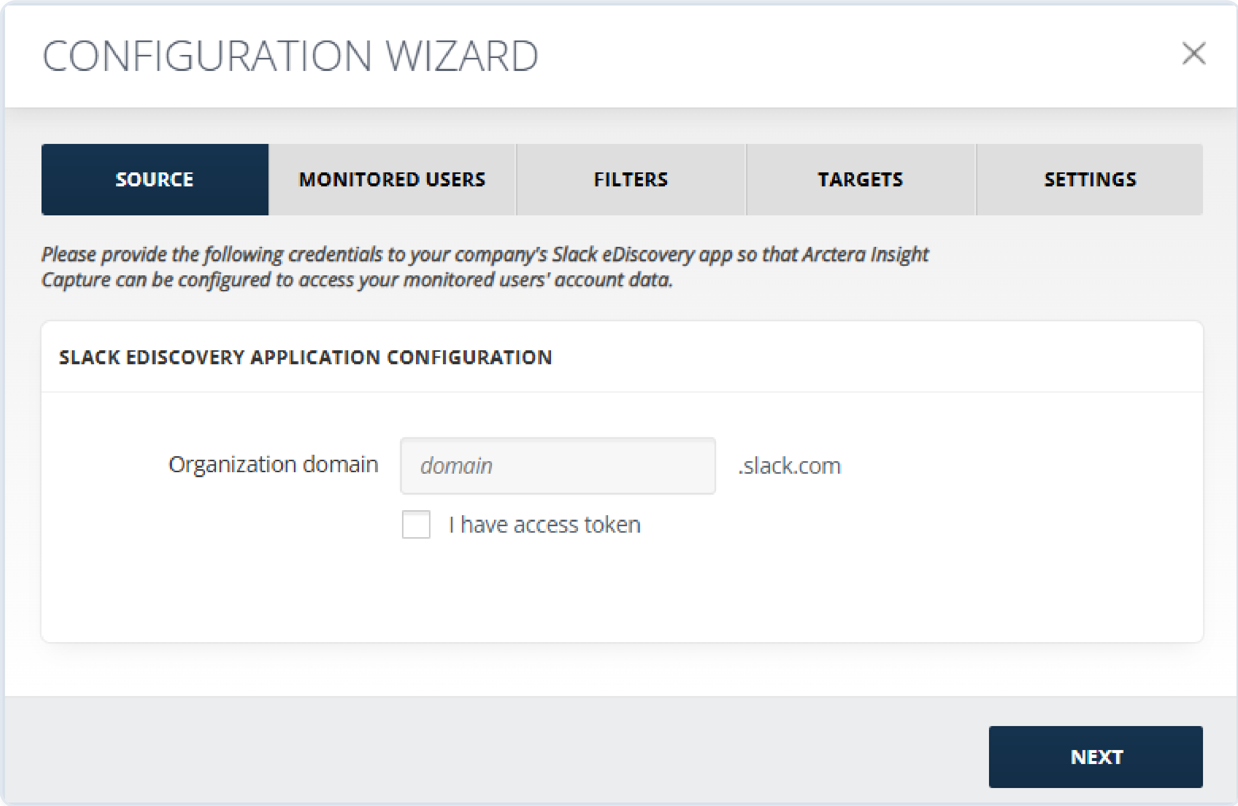
Source Configuration

To set up the Slack eDiscovery collector:

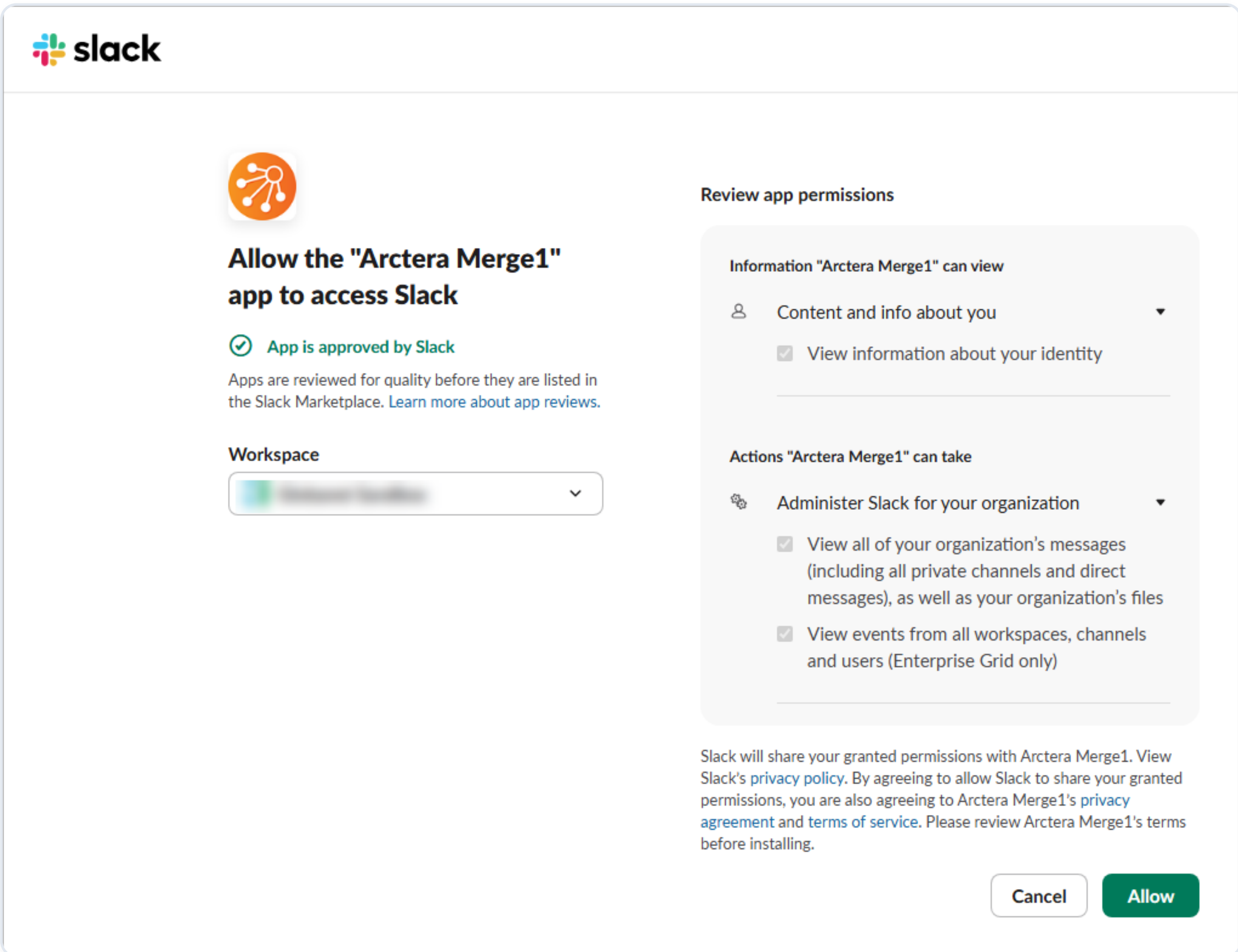
1. Log into your Slack Enterprise workspace using the organization URL. You should stay logged into your account when adding a Arctera Capture collector.
2. Click **Manage Organization** on the upper right corner.
3. Enter the necessary workspace.
4. Confirm that the account used for configuring the collector has the necessary permissions, i.e., is either an Org. Owner or a Primary Org. Owner.

   > **Note:** Org. Owner controls the highest-level security and administrative settings, but only thePrimary Org. Owner(usually the person who created the workspace) can delete it.

5. Leave the window open.
6. Go to Arctera Capture and add click **Add Importer**.
7. Add a **Name** to the importer and a **Description** and select the collector from the collectors list.
8. After receiving a confirmation from us, contact exports@slack.com and ask to enable Discovery API for your organization.
9. Add your Slack eDiscovery Organization URL in the **Organization Domain** field. If the organization domain has enterprise subdomain in it, it should be omitted from the field. For example, the domain `Arctera.enterprise.slack.com` should be filled in as `Arctera.slack.com`.
10. Click **NEXT**, to initialize the connection after the Discovery API is enabled. Discovery API allows using approved third-party apps (in this case Arctera Capture) to export, archive, or meet other security and compliance obligations for any organization content.



11. Authorize the connection between Slack eDiscovery and Arctera Capture.



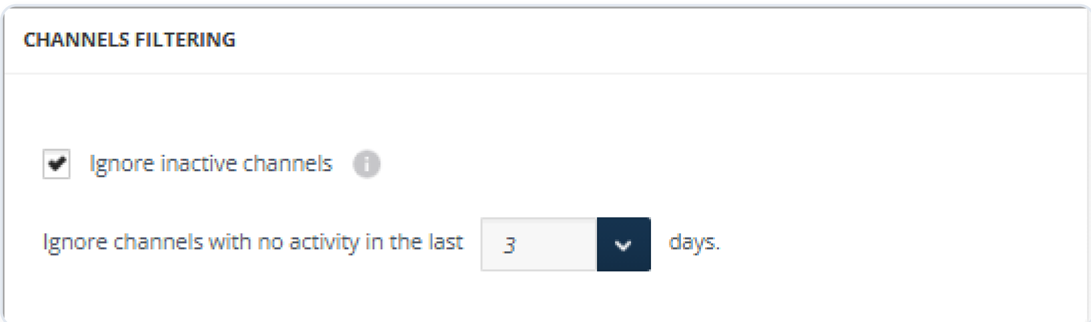
Timestamp Formatting

In addition to the primary stamp, a second timestamp can be enabled with its time zone. From the drop-down menu you can choose the time zone of the timestamp. The format of the timestamp in the output message can also be specified from the six options in the **Date Time Format** drop-down list.

Channels Filtering

In the **Channels Filtering** section:

- Enable **Ignore inactive channels** to exclude channels that have had no activity within the specified period.
- In the **Ignore channels with no activity in the last** field, specify the number of days of inactivity after which a channel is skipped.

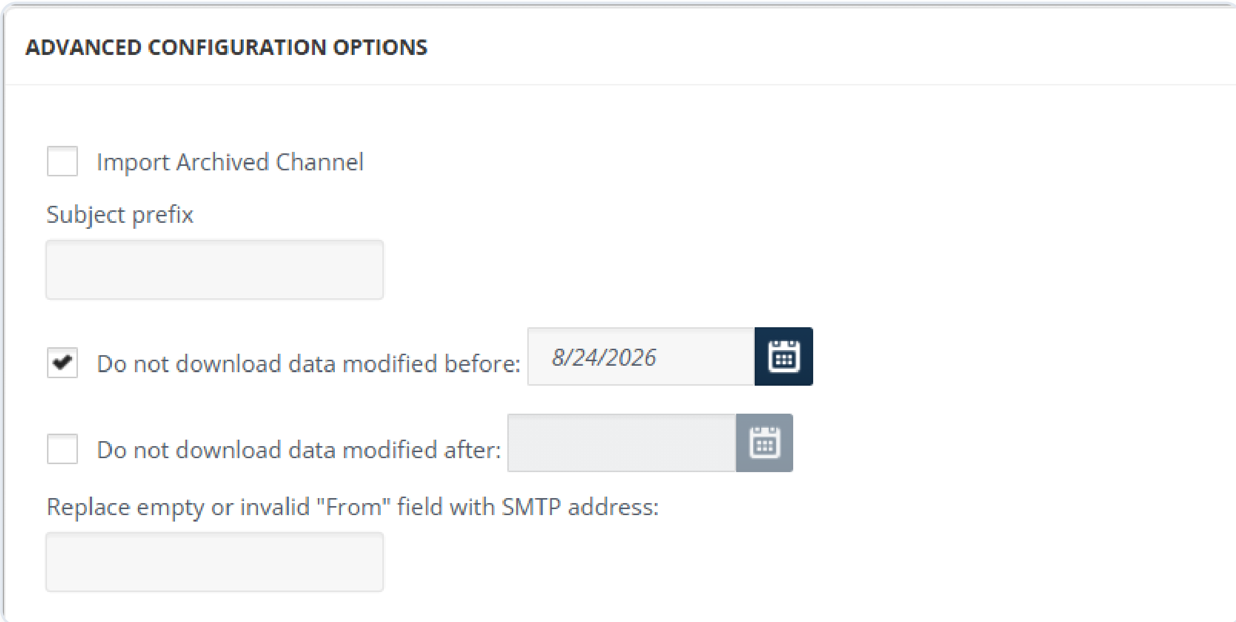


Advanced Configuration Options

There are the following advanced options when configuring the collector:

- **Import Archived Channel** - when this option is selected, Merge1 imports the data from archive channels in Slack.

- The **Subject prefix** is added to the subject line of imported emails. For example, if entered subject prefix is "Slack". This is useful for organizing imported data, i.e., when multiple sources share a common target.
- **Do not download data modified before** and **Do not download data modified after** - these options allow cutting off data outside the set date range. If the before date is set to 08/17/2022 and the after date is set to 08/25/2022, only the data between these two dates will be downloaded. Data outside that timeframe will be ignored. Note that both options can be used independently as well.
- **Replace empty or invalid "From" field with SMTP address** - the specified SMTP address is used in the **From** field when the original message has an empty or invalid sender.



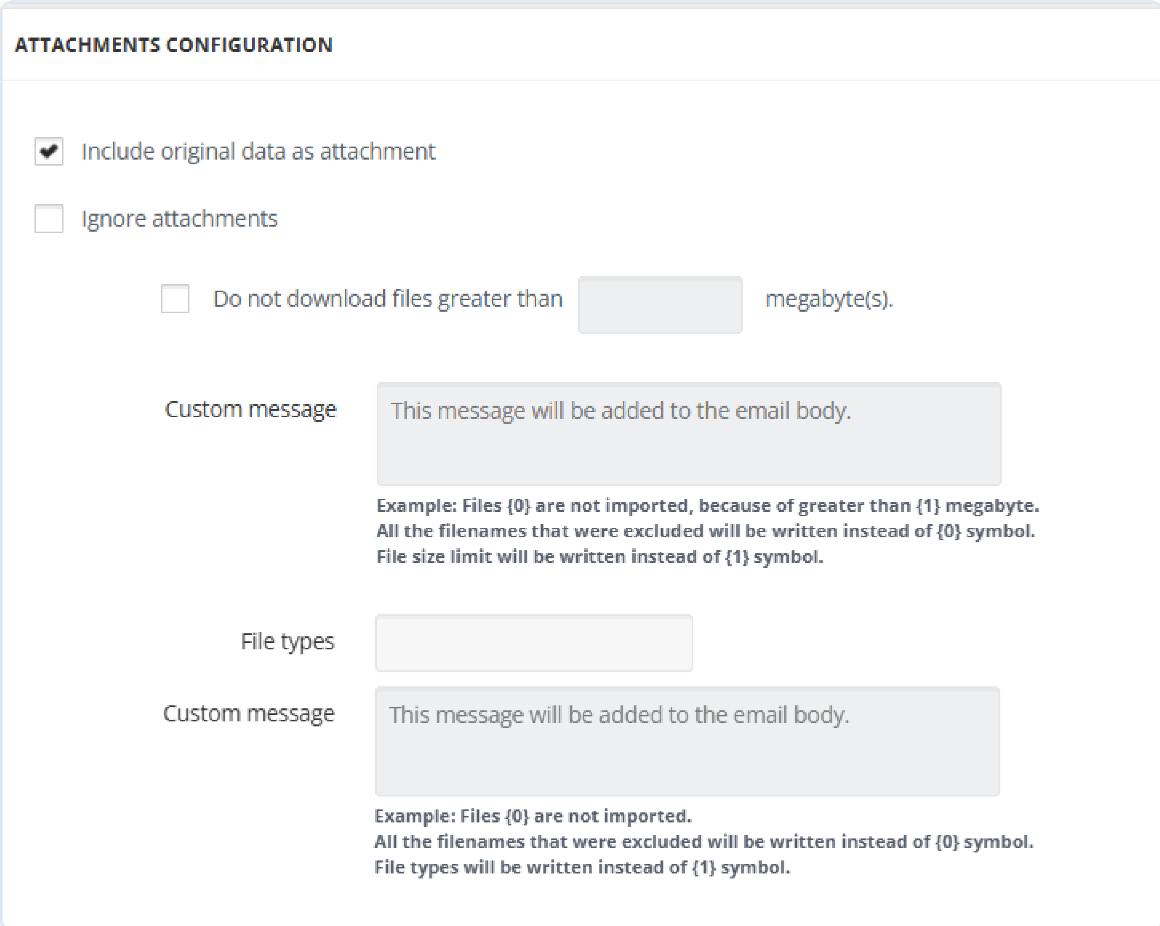
Attachments Configuration

There are the following options:

- The **Include original data as attachment** feature allows including/excluding original data as attachment by enabling/disabling the corresponding checkbox.
- When the **Ignore Attachments** checkbox is checked, all the attachments are being excluded from the message which will enhance the collector performance. Each message will contain only information and the link of the excluded attachment.
- When **Do not download files greater than X megabyte(s)** is selected, the files bigger than the filled-in number of megabytes, are not downloaded. In **Custom Message** field, a text for those excluded files can be specified. E.g.,"Files {0} are not imported, because they are greater than {1) megabytes". {0} is used to add the name of the file and {1} is used to add the number of megabytes specified above.

- In the **File Types** field, the types of files that should not be downloaded can be specified in the following format: e.g., .txt | .xml. The vertical bar is used to separate the file types.

> **Note:** In case of using file filtering by size and by type, we recommend using custom messages.



Message Body

There are the following output message body options:

- **HTML** - the message in the output will be displayed in the HTML format.
- **Light grid mode** - the message will be displayed in a light grid mode with limited metadata.
- **Grid mode** - this mode allows you to see the information in the five following columns:
  - UTC Time Stamp
  - Content Event Type
  - Message ID
  - Attachment

- **Pure body** - the messages will be displayed without any formatting.

> **Note:** Light grid modebecomes active if the **Merge messages by thread** is activated andPure bodyis activated in case **Merge messages by thread** is disabled.

Supported Notifications

The importer supports the following notification types:

- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users
- Filters
- Targets
- Importer Settings

Symphony

Symphony provides secure enterprise collaboration. Users can communicate with internal and external teams, securely share documents and content, conduct meetings with conferencing and screen-sharing, leverage open APIs in the growing app ecosystem to streamline and automate work flows.

The Symphony collector works with XML format only. Make sure that the files are in the correct format. There are following mappings of XML tags to emails:

- \<initiator\> = From
- \<sentTo\> = To
- \<readBy\> = CC

> **Note:** The Symphony collector can process only zipped XML files.

Activities Captured

- Post date
- From
- Message content
- Record type
- Message ID
- Attachment
- Downloaded by
- Event action
- Read by

File Formats Supported by the Collector

- .xml

Source Configuration

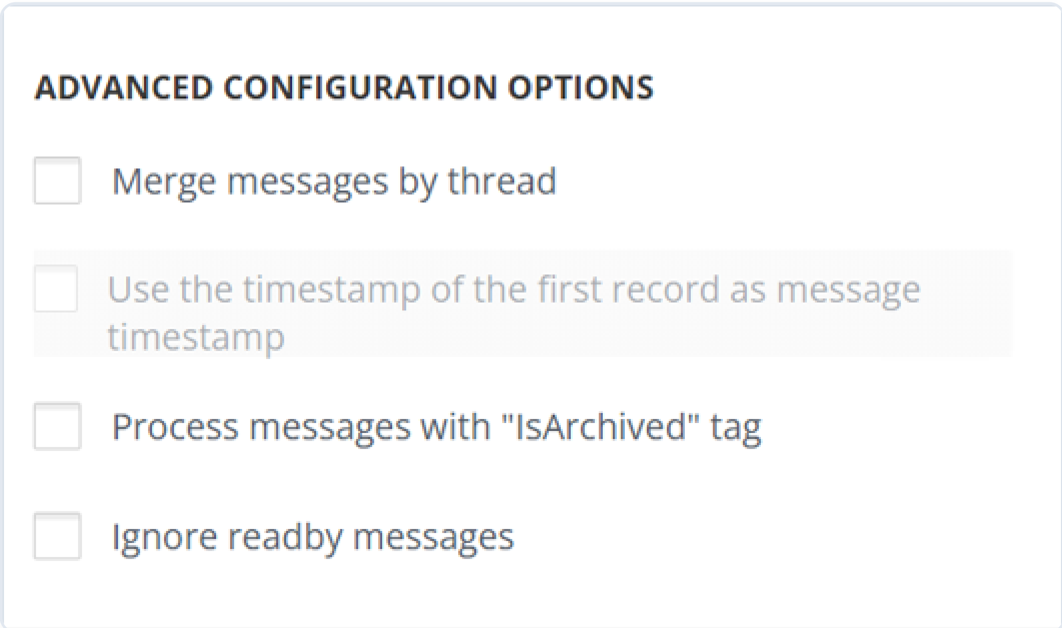
For information on how to configure the following sections of the **Source** tab, see:

- File Source Configuration
- PGP Configurations
- Quarantine Location
- Miscellaneous Settings
- Attachment Validation

Advanced Configuration Options

For this section:

- **Merge Messages by Thread** - when selected, messages with identical thread IDs are grouped into individual emails (as opposed to receiving a separate email per message). It is possible to select additional fields (**Downloaded By** and **Read By**) to be added to the merged message.
- **Use the timestamp of the first record as message timestamp** - selected only when **Merge Messages by Thread** is selected. When enabled, it uses the timestamp of the first Symphony message as a message timestamp, instead of the one of the last messages.
- **Process messages with "IsArchived" tag** - when checked, messages that have the 'IsArchived' tag are processed as well.
- **Ignore readby messages** when checked, messages with ReadBy field in them will be ignored.

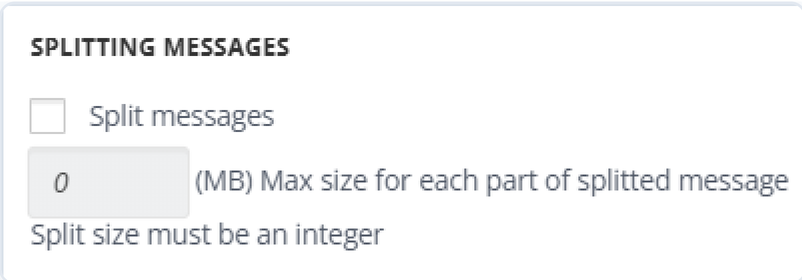


Split Messages

Splitting Messages option allows splitting big files. In the field the size of a split part of the message can be specified so that each part does not exceed the set size. For example, if the **Max Size for each part of split message** is set to 25MB, and the original message is 65 MB, it will be split into 3 messages, each not exceeding 25MB.

In case you have a limitation of 25 MB on your server, you must split your message max to 17MB as the server also must have space for some encryption and decryption tasks that are being carried out by Arctera Capture.

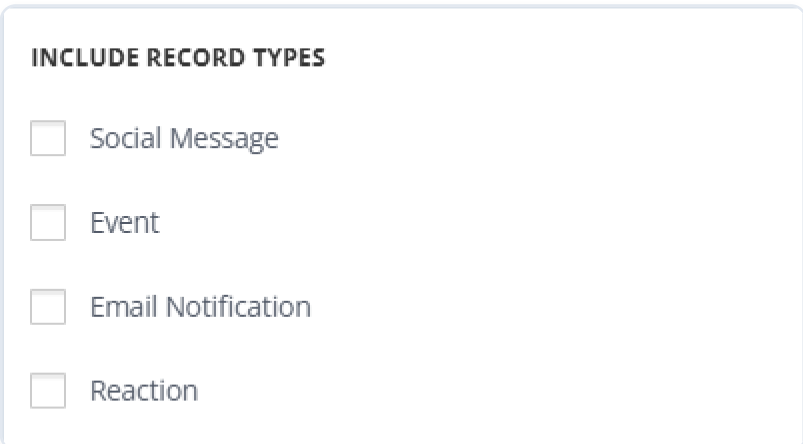
> **Note:** Not applicable to the EV Folder target.



Include Record Type

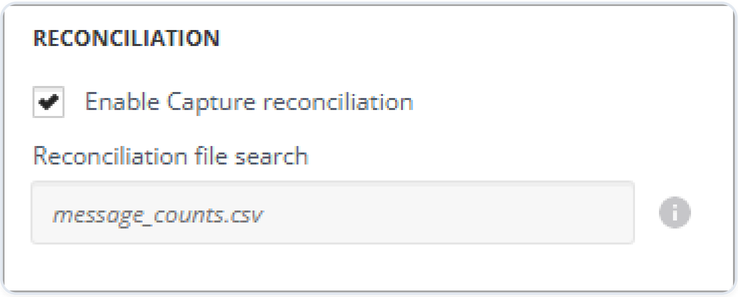
In this section the types of records that should be processed from Symphony can be specified. At least one type should be selected. There are three types of records from Symphony that can be selected:

- **Social Message**
- **Event**
- **Email Notification**
- **Reaction**



Reconciliation

Enable **Capture reconciliation** when reconciliation is supported for the collector. When enabled, specify the **Reconciliation file search** value that Arctera Capture uses to identify the applicable reconciliation file. The reconciliation workflow and the source of the reconciliation data may vary depending on the collector.

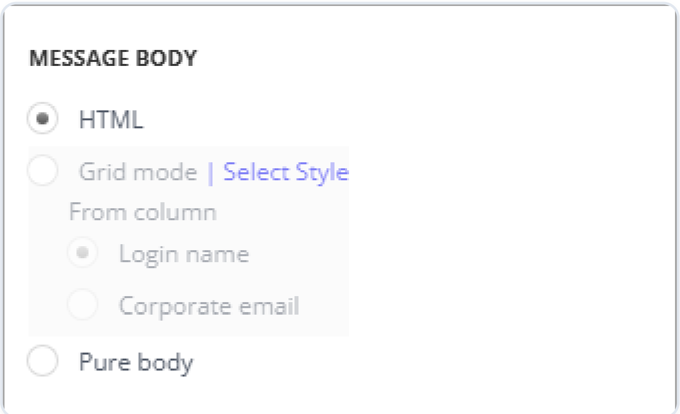


Message Body

This setting specifies how the imported message will be displayed in the target. There are the following output message body options:

- **HTML** - the message in the output will be displayed in the HTML format.
- **Light grid mode** - the message will be displayed in a light grid mode with limited metadata.
- **Grid mode** - the message will be displayed in a grid layout with the information organized in columns.

> **Note:** You can also change the color scheme of the grid mode by clicking the **Select Style** link.



Supported Notifications

The importer supports the following notification types:

- **Quarantine file**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Failed to quarantine file**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users (N/A)
- Filters
- Targets
- Importer Settings

Text-Delimited

Text- Delimited is designed to allow rapidly developing text- delimited file processing. The objective of the collector is to map the text- delimited fields to email required format. The mapping is done based on the uploaded XML template. It varies from source to source; it must be written separately. For more details on the mapping, corresponding to the source, you are going to use it for, contact our support at Arctera Support.

Activities Captured

- Messages

Captured messages can contain:

- Message subject
- Message headers
- Participants: From, To, CC, and BCC
- Activity datetime
- Message body

> **Note:** To process the files properly, the files and attachments that are going to be processed, should have the same name. **Note:** To process the attachments, add the full path to the attachment in the CSV document. To prevent files with similar names, we recommend creating attachments with folder structure to avoid clash of files with similar names shared on different days and in different conversations.

File Formats Supported by the Collector

- .txt
- .csv

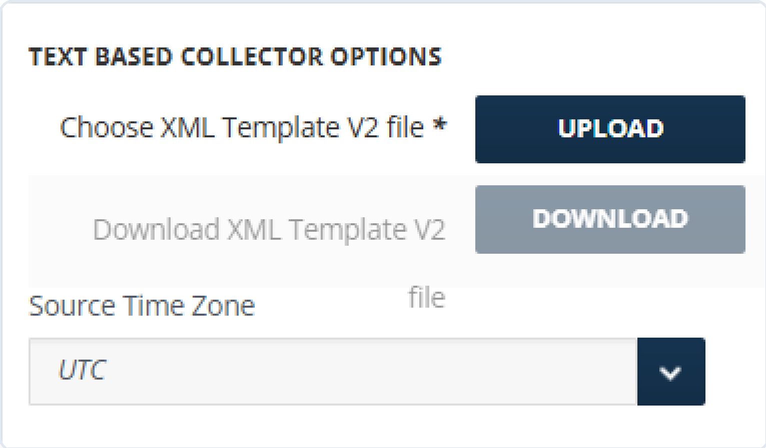
Source Configuration

For information on how to configure the following sections of the **Source** tab, see:

- File Source Configuration
- PGP Configurations
- Quarantine Location
- Miscellaneous Settings

Collector Options

Upload an XML template and select the relevant time zone. Arctera Capture will attempt to retrieve the correct time zone from the source automatically.



The XML file should contain the information about the file itself. It should specify if the file contains headers, the number of columns, delimiter type and the text qualifier. Next part of the XML file should assign column names, identify data types, and indicate if the columns are optional. Lastly, it should map the columns to the expected data fields: Sender, Participants, Title, ActivityDateTime, and Content.

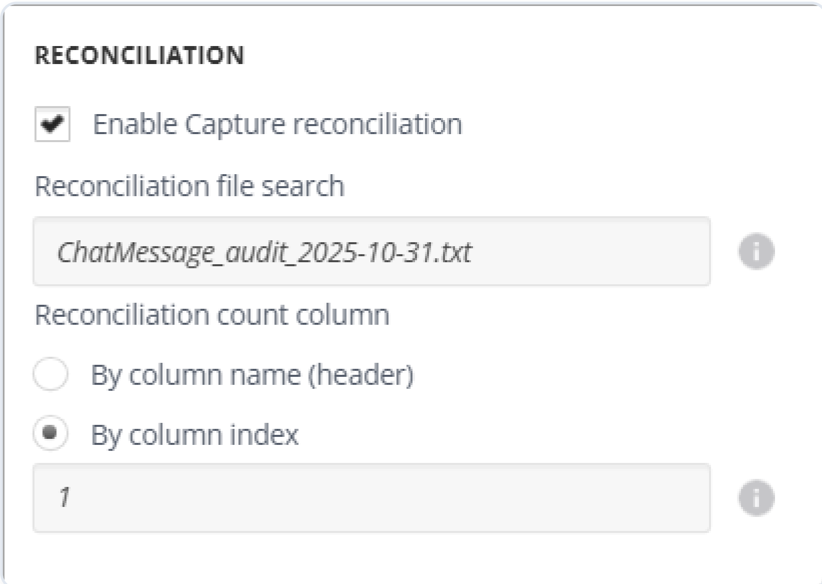
If you want to manually set up the **Source Time Zone**, select the relevant one from the drop-down list. The Source Time zone setting will attempt to retrieve the time zone from the data itself automatically.

Reconciliation

Select **Enable Capture reconciliation** to reconcile the number of messages that Arctera Capture processes against the message count reported by the source.

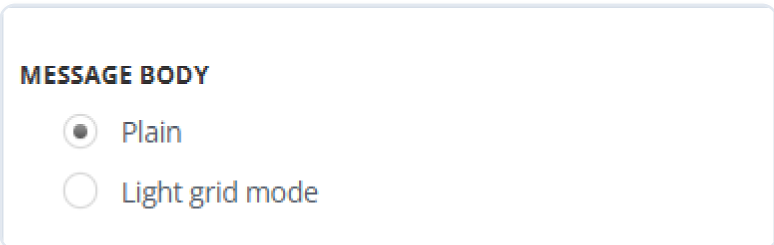
1. In the **Reconciliation file search** field, specify the pattern that Arctera Capture uses to identify the reconciliation file, for example, `ChatMessage_audit_2025-10-31.txt`.
2. Under **Reconciliation count column**, select how Arctera Capture locates the count in the reconciliation file:
   - **By column name (header)**: Identify the count column by its header name.
   - **By column index**: Identify the count column by its position, then enter the column number.

   > **Note:** For `.txt` reconciliation files, if you select *By column index*, set the column index to *1*. Arctera Capture treats `.txt` files as a single-column file.



Message Body

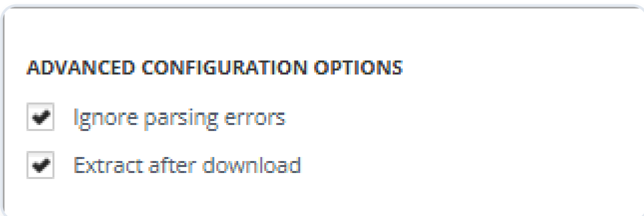
This specifies how the imported message will be displayed in the target. The **Plain Text** mode organizes the data in a simple way and data displayed in a **Light Grid** Mode is two-toned, easy to be viewed with limited metadata.



Advanced Configuration Options

To configure advanced options:

1. Enable **Ignore parsing errors** to skip files that cannot be parsed and continue the import instead of failing the job.
2. Enable **Extract after download** to extract the contents of downloaded archive files before they are processed.



XML Template Configuration Guideline

To configure XML Template sample:

1. Configure the information about the file itself: if the file contains headers, number of columns, text qualifier and attachment method.

```
<?xml version="1.0" encoding="UTF-8"?>

<configuration> <version>AV_2.0</version>

<options>

<containsHeader>Yes</containsHeader>

<maxCols>8</maxCols>

<delimiter>","</delimiter>

<text_qualifier>"</text_qualifier>

<content_type>PlainText</content_type>

<attachmentMethod>Archive</attachmentMethod>

</options>
```

1. Assign column names, identify data type, and indicate if columns are optional.

```
<columns>

<column>

<order>1</order>

<name>FileName</name>

<datatype>StringList</datatype>

<datatype_options>

<delimiter>";"</delimiter>

<append>""</append>

</datatype_options>

</column>

<column>
```

`<order>3</order>`

`<name>Start Date</name>`

`<datatype>DateTime</datatype>`

`<datatype_options> <format>XX/DD/YYYY HH:MM:SS</format> </datatype_options>`

`</column>`

> **Note:** In the DateTime `<format>`, each letter represents a part of the source value: `Y` (year), `X` (month), `D` (day), `H` (hour), `M` (minute), `S` (second), `F` (millisecond), and `Z` (time zone). To parse 12-hour times, add the `TT` token for the AM/PM designator. When `TT` is present, the time is converted to 24-hour format automatically. For example, the format `XX/DD/YYYY HH:MM:SS TT` parses `5/10/2013 3:59:27 PM` as `2013-05-10 15:59:27` and `5/10/2013 12:00:00 AM` as `2013-05-10 00:00:00`.

> `<column>`

`<order>5</order>`

`<name>Username</name>`

`<datatype>String</datatype>`

`</column>`

`<column>`

`<order>6</order>`

`<name>User Email</name>`

`<datatype>String</datatype>`

`</column>`

`<column>`

`<order>7</order>`

`<name>Participant Name</name>`

```
<datatype>StringList</datatype>

<datatype_options>

<delimiter>";"</delimiter>

<append>""</append>

</datatype_options>

</column>

<column>

<order>8</order>

<name>Participant Email</name>

<datatype>String</datatype>

</column>

</columns>
```

1. The last part of the XML file maps the columns to the expected data fields: Sender, Participants, Title, ActivityDateTime, and Body and Threading:

```
<mappings>

<mapping can_be_empty = "Yes">

<property>Sender</property>

<items>

<item>User Email</item>

</items>

</mapping>

<mapping can_be_empty = "Yes">

<property>SenderName</property>

<items>
```

```
<item>Username</item>

</items>

</mapping>

<mapping can_be_empty = "Yes">

<property>Participants</property>

<items>

<item Role="To">Participant Email

</item>

</items>

</mapping>

<mapping can_be_empty = "Yes">

<property>ParticipantNames</property>

<items>

<item Role="To">Participant Name</item>

</items>

</mapping>

<mapping can_be_empty = "Yes">

<property>Title</property>

<items>

<item>Call Id</item>

<string>" "</string>

</items>

</mapping>

<mapping can_be_empty = "Yes">
```

`<property>Content</property>`

`<items>`

`<string>"Call Id: "</string>`

`<item>Call Id</item>`

`<string>" "</string>`

`<string>"Start Date UTC: "</string>`

`<item>Start Date</item>`

`<string>"`

`"</string>`

`<string>"End Date UTC: "</string>`

`<item>End Date</item>`

`<string>"`

`"</string>`

`</items>`

`</mapping>`

`<mapping can_be_empty = "Yes">`

`<property>ActivityDateTime</property>`

`<items>`

`<item>Start Date</item>`

`</items>`

`</mapping>`

`<mapping can_be_empty = "Yes">`

`<property>Attachments</property>`

`<items>`

```
<item>FileName</item>

</items>

</mapping>

<mapping can_be_empty = "Yes">

<property>X-KVS-MessageType</property>

<items> <string>"Telemessage"</string>

</items>

</mapping>

</mappings>

<threading disabled = "No">

<case_sensitive>No</case_sensitive>

<date_sort_direction>Ascending</date_sort_direction>

<items> <item>From Email</item>

<item>To Email</item>

</items>

</threading>

</configuration>
```

> **Note:** Threading is configured if it is required.

Supported Notifications

The importer supports the following notification types:

- **Quarantine file**
- **Import job stopped**
- **No data captured**

- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Failed to quarantine file**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users (N/A)
- Filters
- Targets
- Importer Settings

UBS

UBS provides financial advice and solutions to private, institutional, and corporate clients worldwide.

Activities Captured

- Datetime
- First name
- Last name
- Company name
- Says

- Content
- Participant's full name
- Email
- User ID

File Formats Supported by the Collector

- .xml

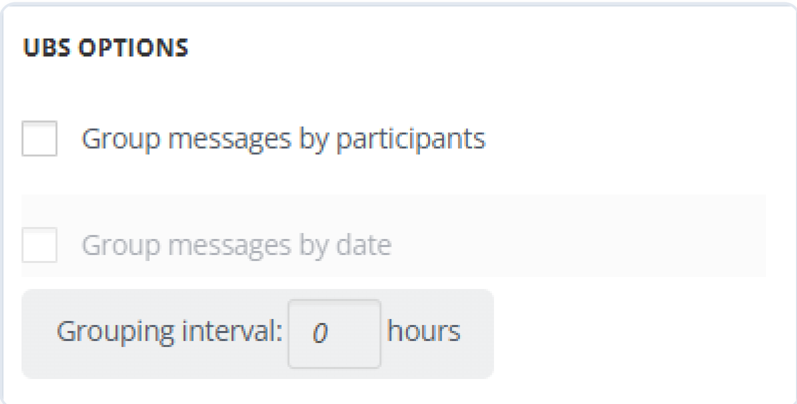
Source Configuration

For information on how to configure the following sections of the **Source** tab, see:

- File Source Configuration
- PGP Configurations
- Quarantine Location
- Miscellaneous Settings

UBS Options

Arctera Capture enables you to validate the UBS attachments. You can either group all messages based on participants or you can group messages by date.



You can also set grouping interval. The time is calculated in hours.

Supported Notifications

The importer supports the following notification types:

- **Quarantine file**
- **Import job stopped**
- **No data captured**

- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Failed to quarantine file**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users (N/A)
- Filters
- Targets
- Importer Settings

Verba

Verba is a call recording and communications compliance solution, typically used for recording, monitoring, and analyzing voice, video, and messaging interactions in corporate or regulated environments. The collector acquires and processes files exported from Verba. It supports ingestion of paired files which include a CSV file and its corresponding media file.

Activities Captured

- Calls

Captured activities can contain:

- Verba call ID

- Platform call ID
- Call start date time
- Call end date time
- Call duration
- Storage target
- Attachments

File Formats Supported by the Collector

- .csv

Source Configuration

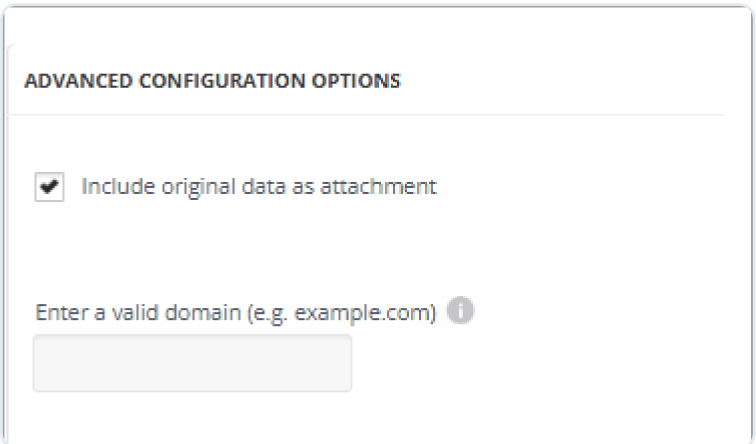
For information on how to configure the following sections of the **Source** tab, see:

- File Source Configuration
- PGP Configurations
- Quarantine Location
- Miscellaneous Settings

Advanced Configuration Options

If **Include original data as attachment** is enabled, the XML file will be attached to the output message.

In the **Enter a valid domain** field, specify a domain (e.g. `example.com`) that is used to construct a valid email address for participants who do not have one.



Supported Notifications

The importer supports the following notification types:

- **Quarantine file**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Failed to quarantine file**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users (N/A)
- Filters
- Targets
- Importer Settings

Verint

Verint recording is a full-time compliance recording solution that can be deployed on-premises or in hybrid cloud environments. It lets you capture, ingest, aggregate, and manage interaction data across all voice and digital channels.

The Arctera Capture Verint collector is a file-based collector to parse Avaya and Cisco call XML and JSON formatted interaction file sources.

Activities Captured

- Recorded calls

Captured messages can contain:

- Call start time (as a timestamp)
- Call duration
- Audio attachment files in WAV format
- Subject
- Participants
- Message body

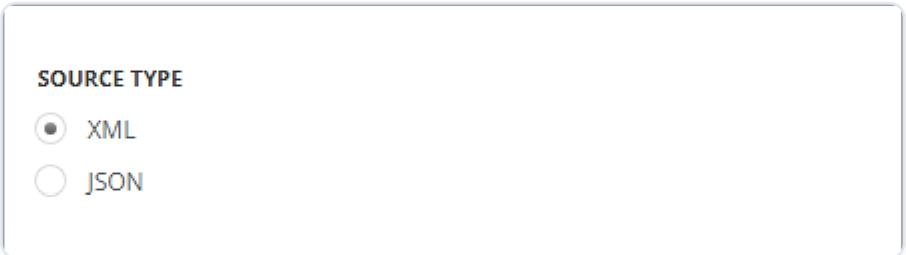
File Formats Supported by the Collector

- .xml
- .json

Source Configuration

For **Source Type**, select the format of the source data that the collector processes:

- **XML**
- **JSON**

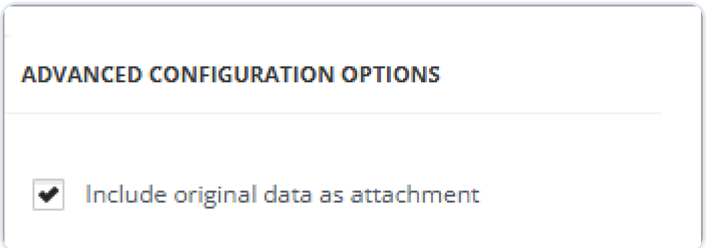


For information on how to configure the following sections of the **Source** tab, see:

- File Source Configuration
- PGP Configurations
- Quarantine Location
- Miscellaneous Settings

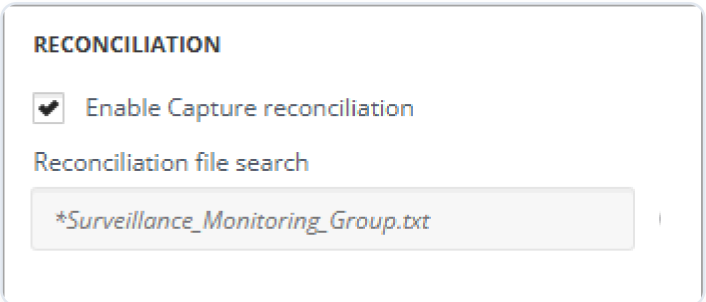
Advanced Configuration Options

If **Include original data as attachment** is enabled, the XML or JSON file will be attached to the output message.



Reconciliation

Enable **Capture reconciliation** when reconciliation is supported for the collector. When enabled, specify the **Reconciliation file search** value that Arctera Capture uses to identify the applicable reconciliation file. The reconciliation workflow and the source of the reconciliation data may vary depending on the collector.



Supported Notifications

The importer supports the following notification types:

- **Quarantine file**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Failed to quarantine file**
- **Import job completed with failure**
- **Import job finished with fatal error**

- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users (N/A)
- Filters
- Targets
- Importer Settings

Viva Engage (Yammer)

Viva Engage (Yammer) is a collaboration tool that helps users and their teams to stay on top of it all. They can start conversations, work together on files, and organize around projects. The collector securely captures and delivers data for seamless archiving, regulatory compliance, and structured communication management, helping organizations maintain transparency while preserving valuable insights.

Activities Captured

- Posts in public and private groups
- Comments and replies of posts in public and private groups
- Private messages

> **Note:** Unless the conversation has been started by an external user.

- Attachments (including SharePoint files)
- Edit activities of posts/comments/replies/private messages
- Polls

> **Note:** Votes are not captured.

> **Note:** The poll options for deleted polls are displayed on the same line.

- Praise (the text of the praise and the replies)
- Announcements (the text of the announcement and replies)
- Deleted private messages, posts, and comments (including attachments)

> **Note:** The delete event of the message/post will be captured in case there is a create/edit activity before the Arctera Capture run.

Notes

- Attachments are not captured in the following cases:
  - If the shared file has restrictions such as an expired link, password protection, or access limitations.
  - If the file was shared and then deleted.
  - If a file's link was shared but the site where the file is located has undergone changes.
- If messages are GDPR hard deleted, the attachments (if it has any) cannot be captured due to the source limitation.
- A dummy SMTP address is created for a deleted message which is missing the deleted_by_id field.
- GDPR hard deleted and soft deleted messages are captured as deleted. Legal Hold should be enabled so the attachments are not deleted from the SharePoint site.
- When sharing an already existing file from SharePoint, the attachment will not be captured - only the URL of that attachment will be retrieved.
- The created message does not say it was deleted from Viva Engage (Yammer). To capture the deletes, the data retention setting needs to be set to Delete. See instructions at Manage Viva Engage (Yammer) Data Compliance.
- Events of former members are not captured due to limited permissions of admin-generated token.
- A separate **Import folder path** should be provisioned on the **Source Configuration** tab for each Viva Engage (Yammer) collector when running 2 or more collectors simultaneously.

- Enabling the **Merge messages by thread** feature may impact the performance of the collector processing.
- If a message is created with an attachment and later edited to remove only the attachment, the deletion event will not be captured due to source limitations.
- Microsoft APIs do not support SharePoint link-sharing activities, including file protection features (passwords, expiration dates, download restrictions, and specific permissions) or cases where the file is deleted or the site becomes inaccessible during the run process.

Microsoft Entra ID App Creation

To authenticate via OAuth during the collector configuration, you need to create a Microsoft Entra ID Application.

To create an app:

1. Create an O365 account and open Azure Portal using the same credentials as for O365 (Global Admin).
2. Click **Microsoft Entra ID** at the top of the page and select **App Registration** from the left-side navigation pane.
3. Click the **+New registration** button.
4. Enter a **Name** for the application and click **Register**.
5. Enter the enter the URL of your local Arctera Capture environment.

> **Note:** The **Redirect URI** can be found in the Click information of the collector source configuration.

6. Find and make a note your **Application (client) ID** and **Directory(tenant) ID** as this is needed for configuring the collector in Arctera Capture.
7. In the navigation pane to the left, go to **Certificates & secrets**.
8. Click the **Upload certificate** button.
9. Select a certificate (public key) with one of the following file types: .cer,.pem, .crt, and click **Add**. For more information on how to create a certificate, see Creating a Certificate (Private and Public Keys).

To add a client secret:

1. In the left-hand navigation pane, go to **Manage** > **Certificates & secrets**.

2. Go to **Client secrets** and click **New client secret**.
3. Enter a **Description**, specify a **Duration**. Click **Add**.
4. Locate and save the new client secret value for configuring the collector.

Microsoft Entra ID Permissions

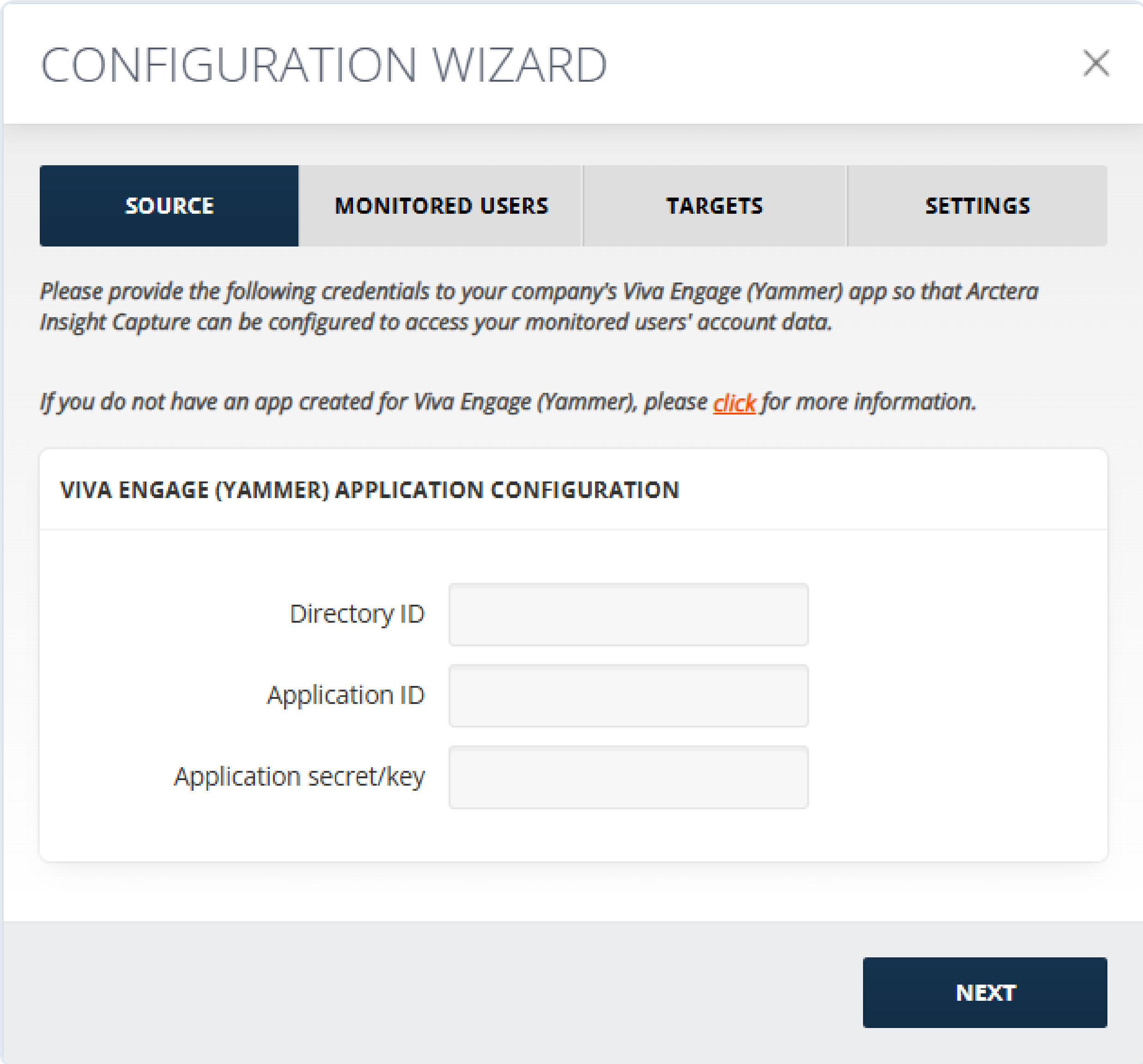
For permissions:

1. In the navigation pane to the left, click **API permissions**.
2. In the opened pane, select the **Yammer API**.
3. Click **Delegated permissions**, add the following permission: Other permissions: user_impersonation, and click **Add permissions**.
4. Click \+ **Add a permission** and select **SharePoint API** with **Application permissions**. Add the Sites:Sites.Read.All permission and click **Add permission**:
5. Grant all the above-mentioned permissions.

Source Configuration

To configure the Viva Engage (Yammer) application:

1. Add the saved Directory (tenant) ID and Application (client) ID in the **Directory ID** and **Application ID** fields, respectively.
2. Add the saved client secret value in the **Application secret/key** field and click **Next**.



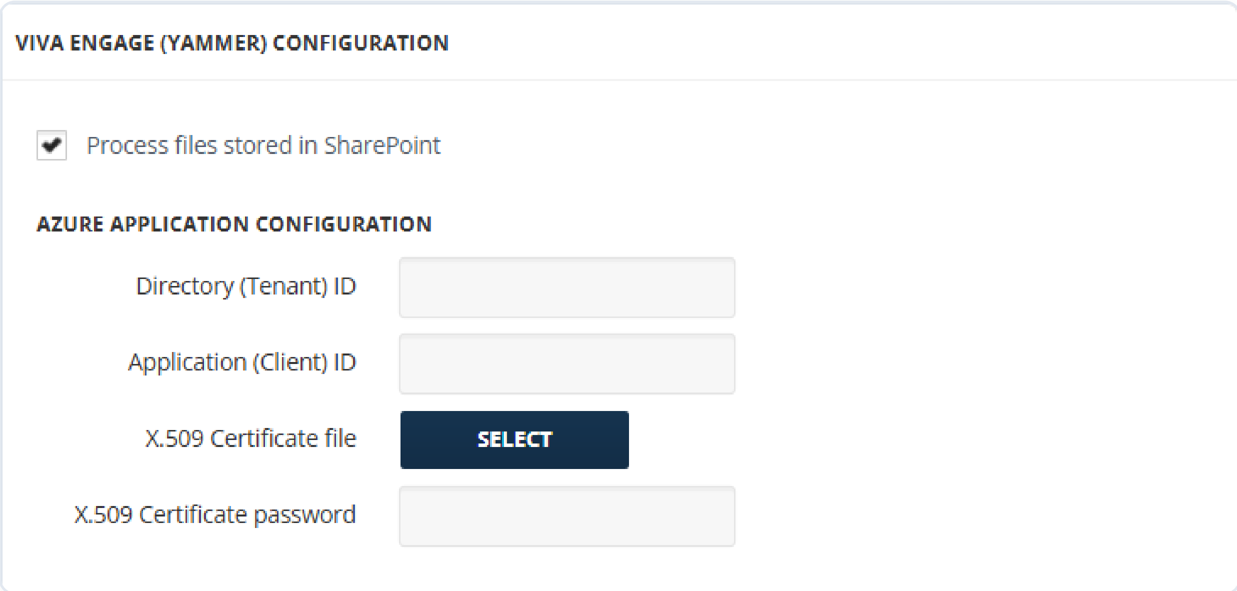
3. A pop-up window will open (ensure that the pop-ups are not disabled in the browser window). Click **Accept** to let the app access the specified resources for all users in the organization.

> **Note:** To authenticate with Arctera Capture, the user must have the Global Administrator role assigned in the Azure Portal. In addition, to use Arctera Capture, the user must be a Yammer Administrator in the Azure Portal and a Verified Admin in the Yammer Admin Portal. Note that these permissions must remain active while being in use by Arctera Capture. Removing or restricting them may cause authentication issues or importer run failures.

To configure the source:

1. For Viva Engage (Yammer) Application configuration, enter **Application ID** and **Application secret/key**.

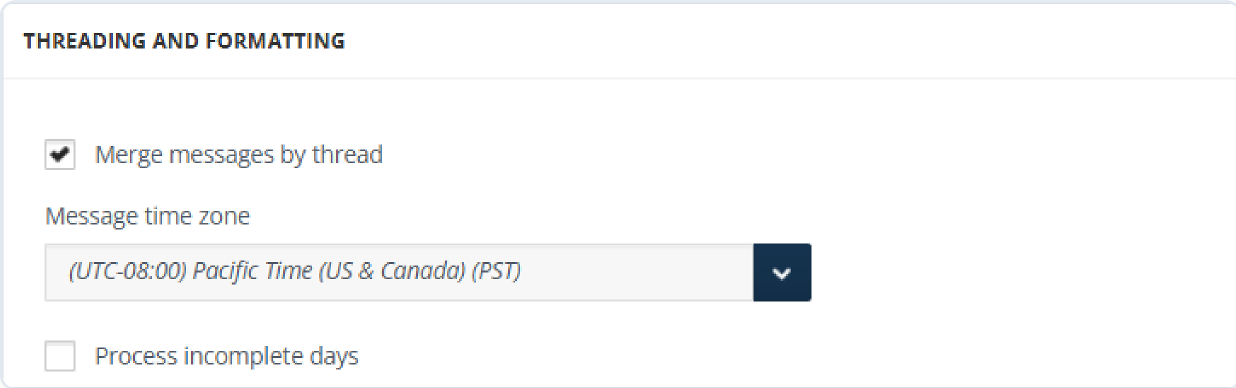
2. To capture SharePoint files, enable the **Process files stored in SharePoint** checkbox. The following Azure application credentials are required to capture the content:
    - **Directory (Tenant) ID**
    - **Application (Client) ID**
3. Select the **X.509 Certificate** file.
4. Enter the **X.509 Certificate password**. The **Certificate thumbprint** field will be auto populated in case the collector was previously configured by uploading a certificate.



Threading and Formatting

For Threading and Formatting:

- **Merge messages by thread** - this combines all messages in a thread into a single message. Only a single post, message, poll, announcement, or praise with its comments and replies is threaded into a single output message.
- Select the **Message time zone** from the drop-down menu. When the **Process Incomplete Days** option is enabled, the messages for days that have not yet ended will be imported in a separate email.

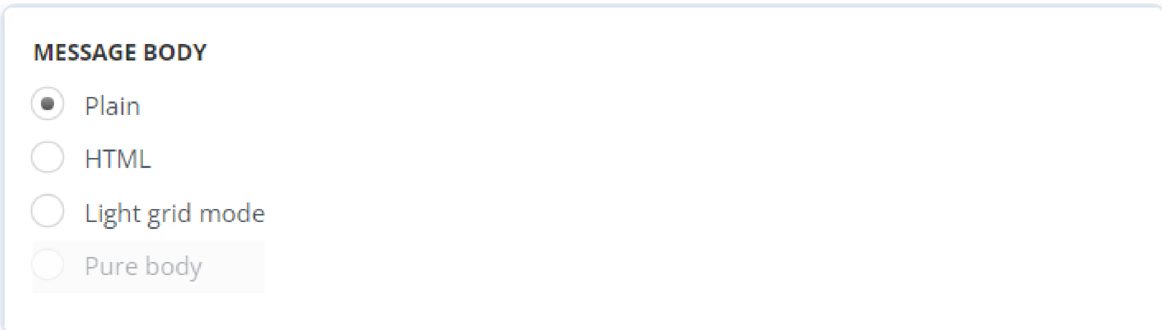


Message Body

There are the following output message body options:

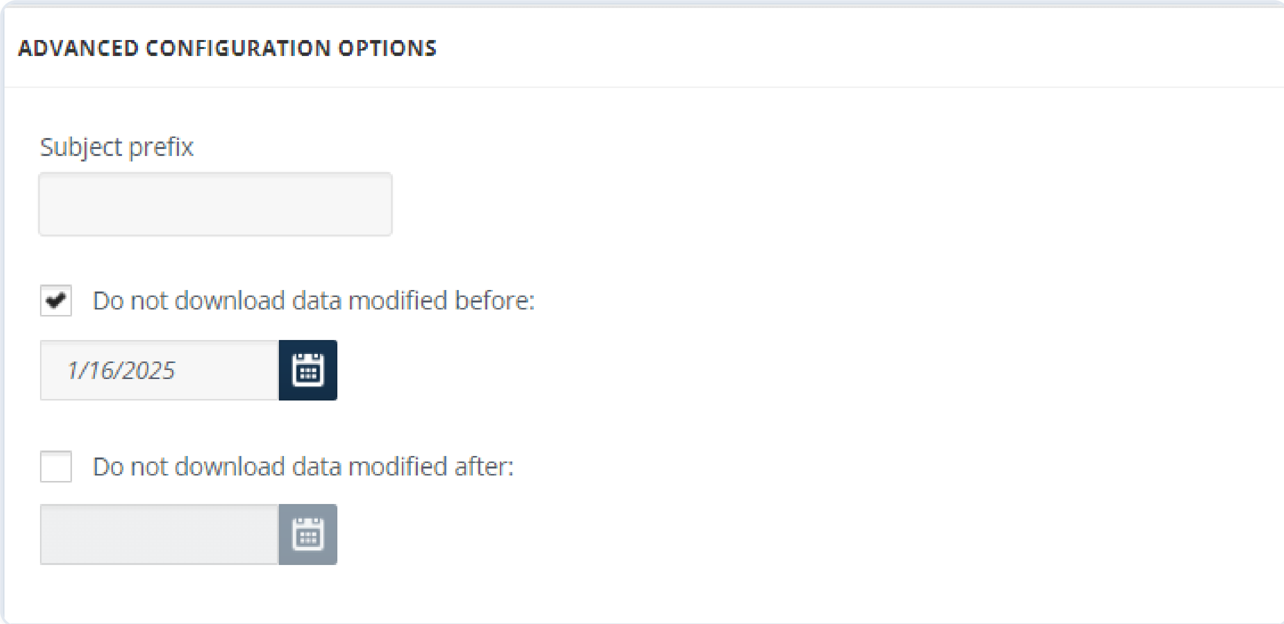
- **Plain** - this mode displays the message as simple text.
- **HTML** - the message in the output will be displayed in the HTML format.
- **Light grid mode** - the message will be displayed in a light grid mode with limited metadata.
- **Pure body** - the messages will be displayed without any formatting.

> **Note: Light grid mode** becomes active if the **Merge messages by thread** is activated and **Pure body** is activated in case **Merge messages by thread** is disabled.



Advanced Configuration Options

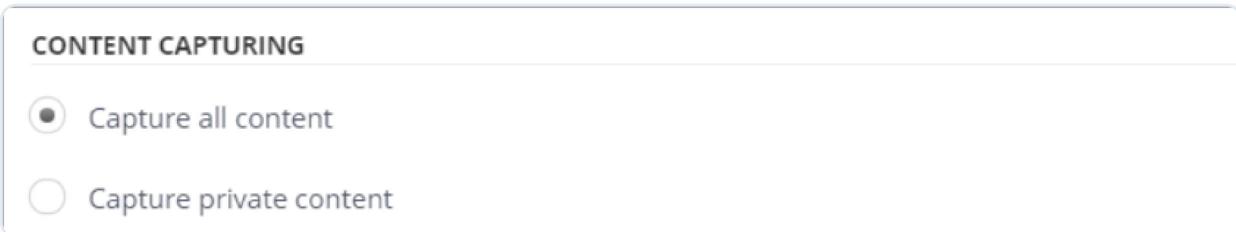
There are the following advanced options when configuring the Viva Engage (Yammer) collector:



- **Subject prefix**- this is added to the subject line of imported emails and is useful for organizing imported data, i.e., when multiple sources share a common target.

> **Note:** Not applicable to the EV Folder target.

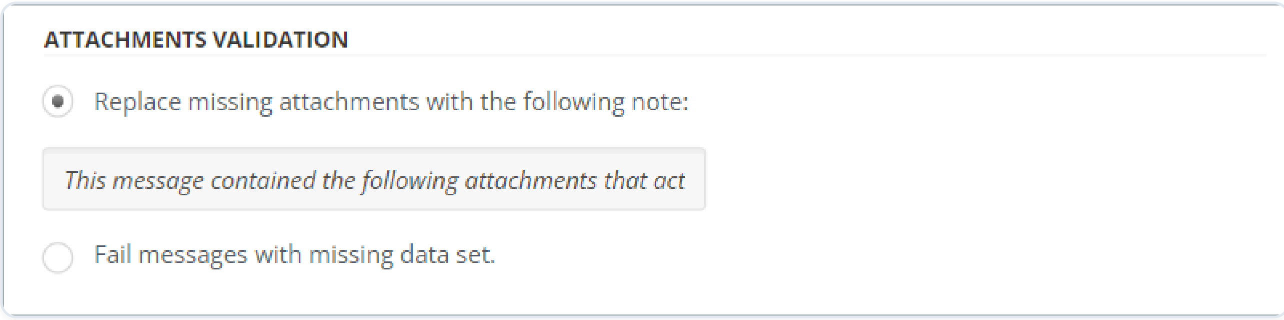
- Options **Do not download data modified before** and **Do not download data modified after** allow cutting off data outside the set date range. If the before date is set to 08/17/2021 and the after date is set to 08/25/2021, only the data between these two dates will be downloaded. Data outside that time frame will be ignored. Note that both options can be used independently as well.
- In the Content capturing section, you can choose either capturing all content or only private content by enabling the corresponding radio button.



Attachments Validation

Arctera Capture enables you to develop customized notes for attachments validation. In case **Fail Messages with missing data set** is selected, the messages that do not have data set are failed.

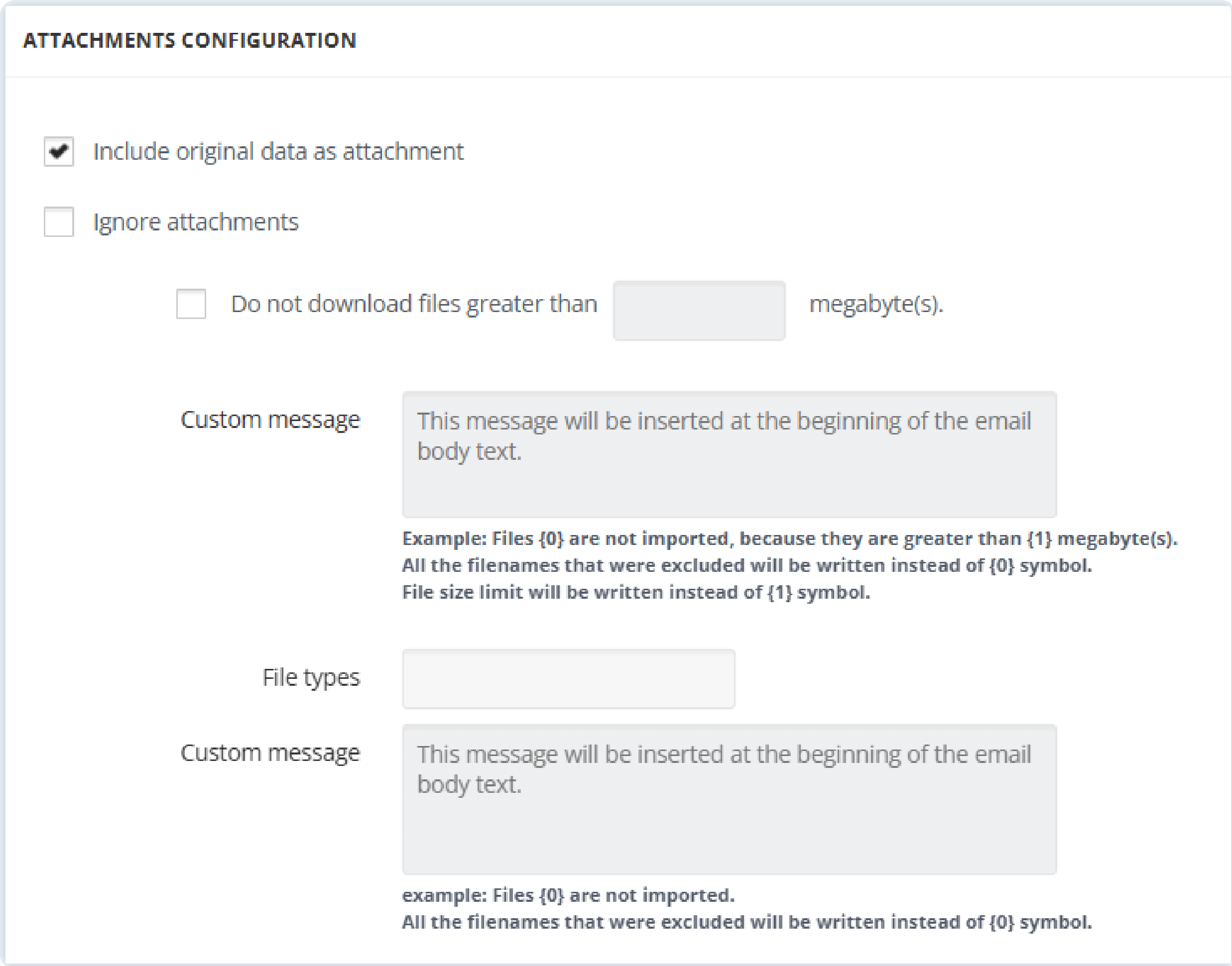
If you select the **Replace missing attachments with the following note** and input your custom note, all the missing attachments of the messages will not be processed, and you will see only the custom message that you have entered.



Attachments Configuration

There are the following configuration options:

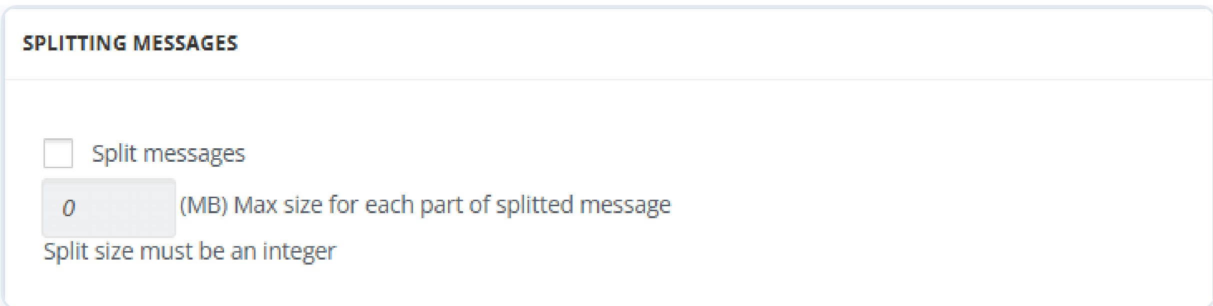
- The **Include original data as attachment** feature allows including/excluding original data as attachment by enabling/disabling the corresponding checkbox.
- When the **Ignore Attachments** checkbox is enabled, all the attachments are excluded from the message which will enhance the collector performance. Each message will contain only information and the link of the excluded attachment.
- When **Do not download files greater than X megabyte(s)** is selected, the files bigger than the filled-in number of megabytes, are not downloaded. In **Custom Message** field, a text for those excluded files can be specified. E.g.,"Files {0} are not imported, because they are greater than {1) megabytes". {0} is used to add the name of the file and {1} is used to add the number of megabytes specified above.
- In the **File Types** field, the types of files that should not be downloaded can be specified in the following format: e.g., .txt | .xml. The vertical bar is used to separate the file types.



Splitting Messages

This option allows splitting large files. In the field the size of a split part of the message can be specified so that each part does not exceed the set size. For example, if the **Max Size for each part of split message** is set to 25MB, and the original message is 65 MB, it will be split into 3 messages, each not exceeding 25MB.

> **Note:** Not applicable to the EV Folder target.



Reconciliation

Viva Engage (Yammer) data is collected through the API, and the source does not provide a reconciliation file. As a result, a source reconciliation count is not available for this collector.

Supported Notifications

The importer supports the following notification types:

- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users
- Filters
- Targets
- Importer Settings

Web Page Capture

The Web Page Capture collector captures the web pages. It captures a specific web page and the links on the page at a configurable through the collector UI level by the provided URL, retrieves its appearance and imports it in PDF, PNG, and custom formats, that can be specified in a JSON file.

Activities Captured

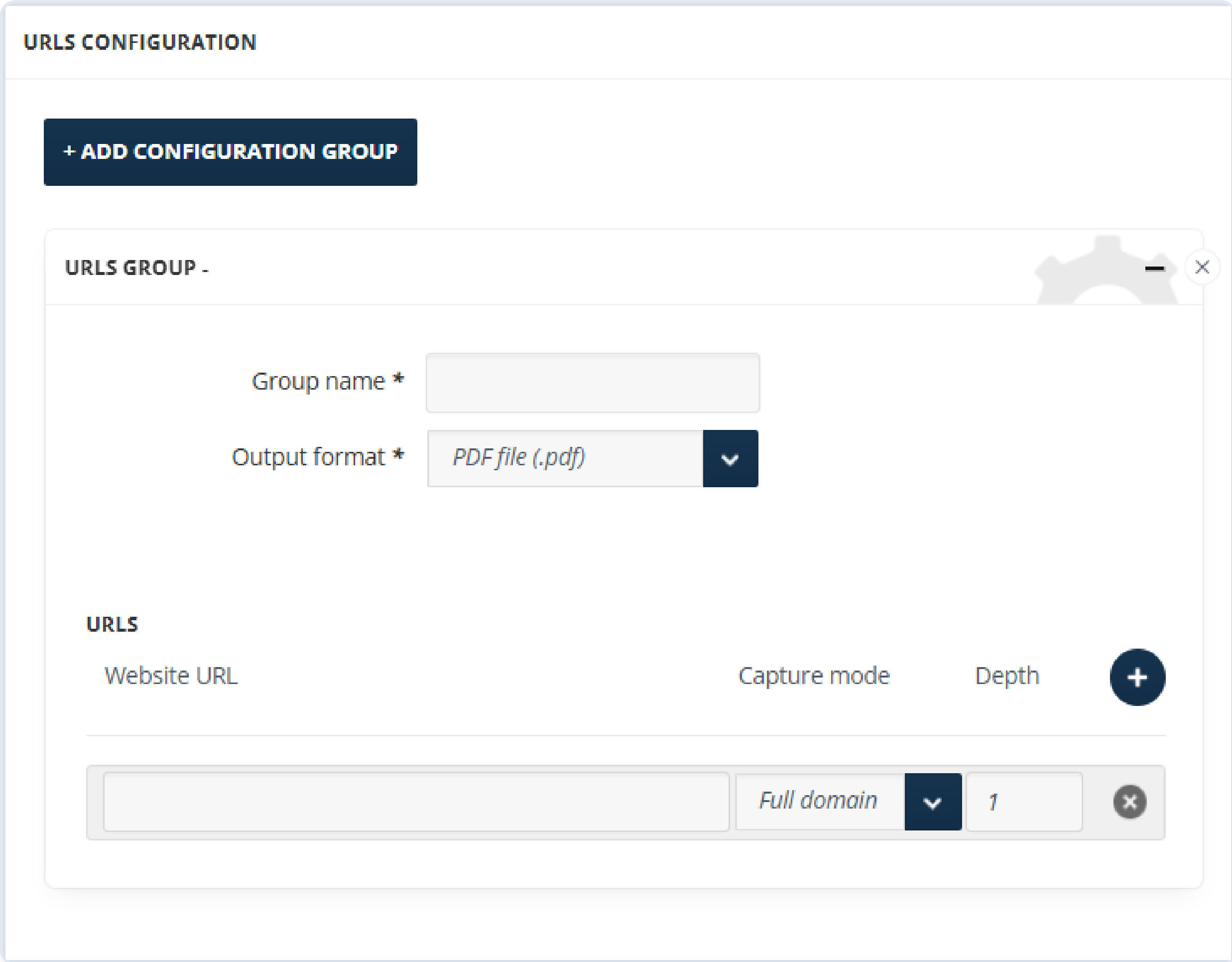
- Web page in PDF
- Web page in PNG
- Web page in custom formats

> **Note:** Heavy pages with the depth of capture more than 1 may be captured not fully, as all the pages may not be loaded completely by the time of the capture.

URLs Configuration

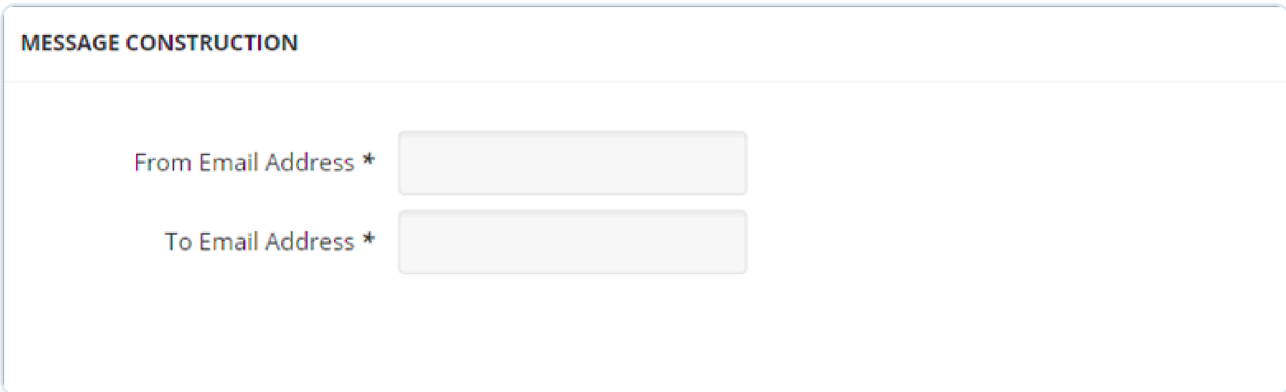
To configure URLs:

1. Click **+Add Configuration Group**.
2. Enter the **Group Name** for the output files of the captured URL.
3. Select the **Output Format**. It can be a PDF, PNG, or custom format file. For the custom format, contact our support at Arctera Support.
4. Enter the website URL from which the capture should start.
5. Choose the capture mode: **Full Domain** or **One Page**. One Page captures only the entered URL. Full Domain captures the mentioned URL and the pages that open from it with the same domain on the mentioned depth.
6. The depth is the level of the pages on the site map that should be captured. It includes the main website URL given in the configuration and the site pages below it on the site map. For Example, if the depth is 1, the Web Capture collector captures the filled in website URL and all the pages that open from that URL and have the same URL in their URLs.



Message Construction

As the messages generated by the Web Page Capture collector do not have senders or recipients, from and to email addresses need to be entered manually for the output email files to be generated. It is recommended to use existing email address in the **From Email Address** field, to avoid it being sent to the SPAM folder if the target of the collector is a mailbox.

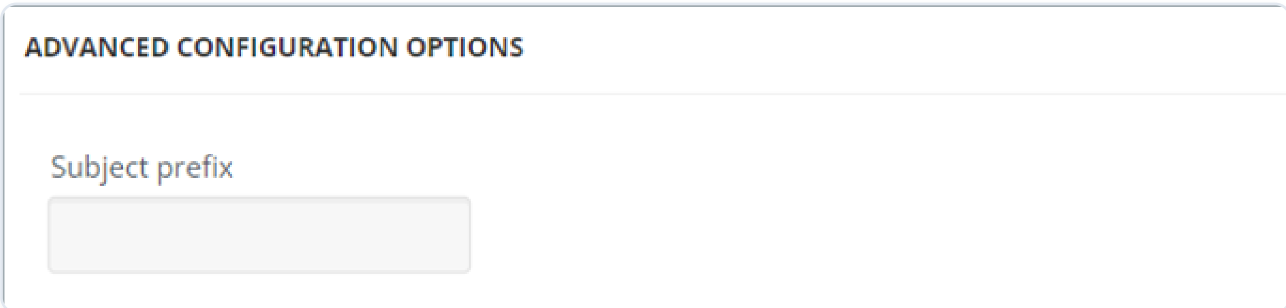


Time Stamp Formatting

In addition to the primary stamp, a second timestamp can be enabled with its time zone. From the drop-down menu you can choose the time zone of the timestamp. The format of the timestamp in the output message can also be specified from the six options in the **Date Time Format** drop-down list.

Advanced Configuration Options

The **Subject Prefix** feature will add a prefix before the message subject to facilitate the search in the target.



Supported Notifications

The importer supports the following notification types:

- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**

- **Importer data deleted**
- **Import job completed with failure**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users (N/A)
- Filters
- Targets
- Importer Settings

WhatsApp

WhatsApp is a communication app developed by Meta Platforms. It enables users to send messages, voice notes, photos, videos, documents, and more to other devices via the internet.

The Arctera Capture WhatsApp collector allows organizations to seamlessly integrate WhatsApp data into their comprehensive communication management systems.

Following the successful onboarding of your devices on Sausalito Labs, please proceed with configuring your importer.

Activities Captured

- Text messages
- Edits

> **Note:** Only the last version of edited messages is captured.

- Emojis
- Replies
- Deleted messages for everyone

> **Note:** Only the events are captured; the content of the message is not captured.

- Mentions
- Documents (MS Word, MS Excel, PDF, PPT)
- Images
- Videos
- Emojis
- GIFs
- Links
- Music
- Apps from Store (App link)
- Drawing

File Formats Supported by the Collector

- .json
- AI Imagine
- Stickers

> **Note:** Unknown sticker types are not captured.

- Audio messages
- Reaction to message by emoji
- Messages with image
- Messages with video

Source Configuration

For information on how to configure the following sections of the **Source** tab, see:

- File Source Configuration
- PGP Configurations
- Quarantine Location
- Miscellaneous Settings

Advanced Configuration Options

If **Include original data as attachment** is enabled, the XML file will be attached to the output message.

Supported Notifications

The importer supports the following notification types:

- **Quarantine file**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Failed to quarantine file**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users (N/A)
- Filters
- Targets
- Importer Settings

Workplace from Facebook

Workplace is an enterprise connectivity platform developed by Facebook, Inc. and featuring tools like groups, instant messaging, and News Feed. Workplace allows third parties to fetch data from its APIs for Compliance and eDiscovery purposes - this is achieved by using Custom Integrations.

Custom Integrations are not available in the free Workplace plans, customers who need to meet Compliance and eDiscovery must have a Premium plan.

Activities Captured

Chats:

- One-on-one chats
- Group chats
- Attachments in chats
- Deleted messages and attachments in chats (if only one chat participant has deleted the message)
- "Add" events in group chats

Posts:

- Group posts (except multi-company groups, and main posts of buy & sell groups)
- Attachments

  > **Note:** Workplace side internal server error occurs in case of having 80+ attachments.

- Polls (without attachments)
- GIFs Emojis GIF posts (mp4 format only)
- Likes & reactions to posts
- Comments and replies

  > **Note:** Specify the number of previous days (maximum 31) prior to the current run for Capture to scan for edits and new comments of a post.

- Photos
- Posts in MD format (without formatting)

- "Create" events (only images)
- Create doc posts in TXT format (without image)
- Live videos
- Latest versions of posts (except attachments)

Activities not Captured

Chats:

- Polls
- Reply to
- Reactions

Group posts:

- Timeline activities
- Deleted group posts
- Tagging coworkers
- Check-ins
- Feeling/Activity
- Comments deleted
- Created events
- Hidden chats
- Posts created on someone's timeline
- Previous versions of posts

Custom Integration Creation in Workplace

Workplace from Facebook allows third parties to fetch data from its APIs for Compliance and eDiscovery purposes - this is achieved by using Custom Integrations.

> **Note:** Custom Integrations are not available in free Workplace plans, so customers who need to meet Compliance and eDiscovery must have a Premium plan.

> To create a custom integration:

1. Login to workplace using a System Administrator account.
2. Navigate to https://my.workplace.com/work/admin/apps/.
3. Sign in if prompted to.
4. Click **Create Custom Integration**.
5. Enter a name for the Integration and click **Create**.
6. Copy **App ID** and **App Secret**.
7. Click **Create Access Token** and copy the generated token.
8. If **Discoverable** is set to **Yes**, change it to **No**. This is not required but it is best practice to make sure the users are not aware of existence of the application.
9. Under **Integration Permissions**, enable the following permissions:
    - **Read group content**
    - **Read user timeline**
    - **Read all messages**
    - **Read user email**
    - **Read group membership**
    - **Message any member**
        - **Allow this integration to work in group chats**
10. To make sure the permissions remain available for the collector, disable **Automatically remove unused permissions**. This is not required; you can leave it on for better security, but you might need to come back to this page and re-add the permissions.

    > **Note:** Facebook allows you to scope the App's permissions to specific groups. This is recommended if you only need to monitor users of the certain groups.

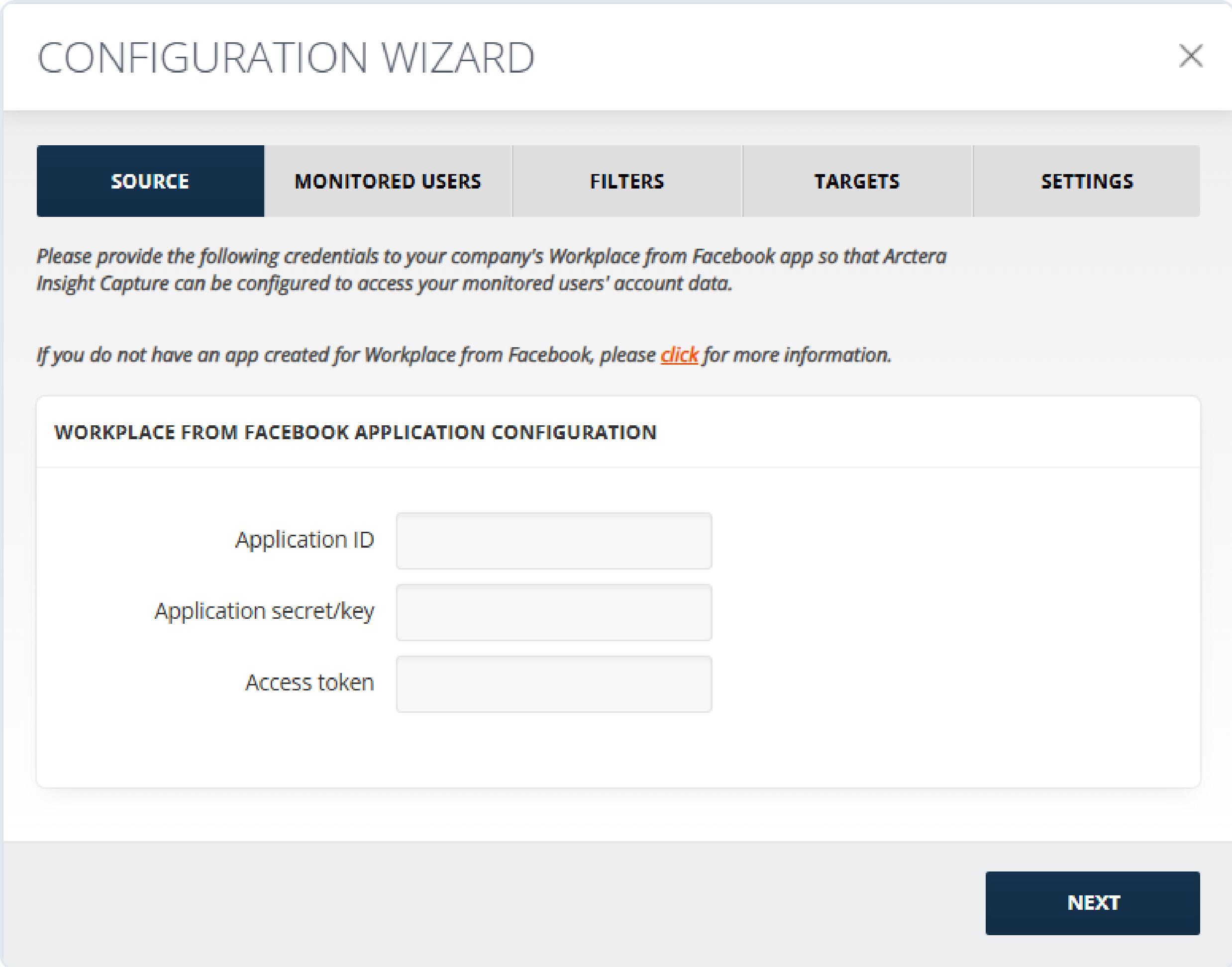
11. Enable **Require App Secret Proof** and allow list the public IP addresses of your Arctera Capture server(s), gateways and/or proxy server(s).

Source Configuration

To configure the collector:

1. Enter the App ID copied in the Step 6 of the previous section in the **Application ID** field.
2. Enter App Secret in the **Application Secret/Key** field.

3. Enter Access Token in the **Access Token** field.

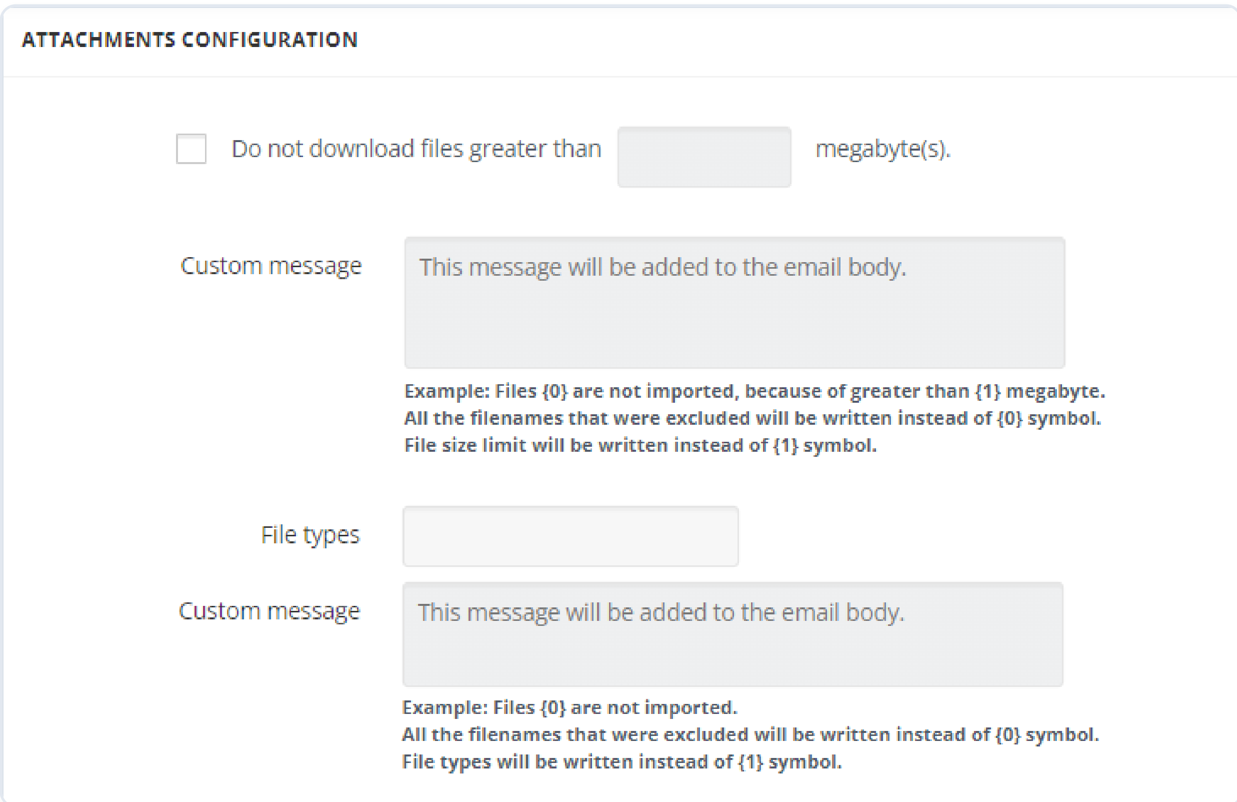


Timestamp Formatting

In addition to the primary stamp, a second timestamp can be enabled with its time zone. From the drop-down menu you can choose the time zone of the timestamp. The format of the timestamp in the output message can also be specified from the six options in the **Date Time Format** drop-down list.

Attachments Configuration

- When **Do not download files greater than X megabyte(s)** is selected, the files bigger than the filled-in number of megabytes, are not downloaded. In **Custom Message** field, a text for those excluded files can be specified. E.g.,"Files {0} are not imported, because they are greater than {1) megabytes". {0} is used to add the name of the file and {1} is used to add the number of megabytes specified above.
- In the **File Types** field, the types of files that should not be downloaded can be specified in the following format: e.g., .txt | .xml. The vertical bar is used to separate the file types.



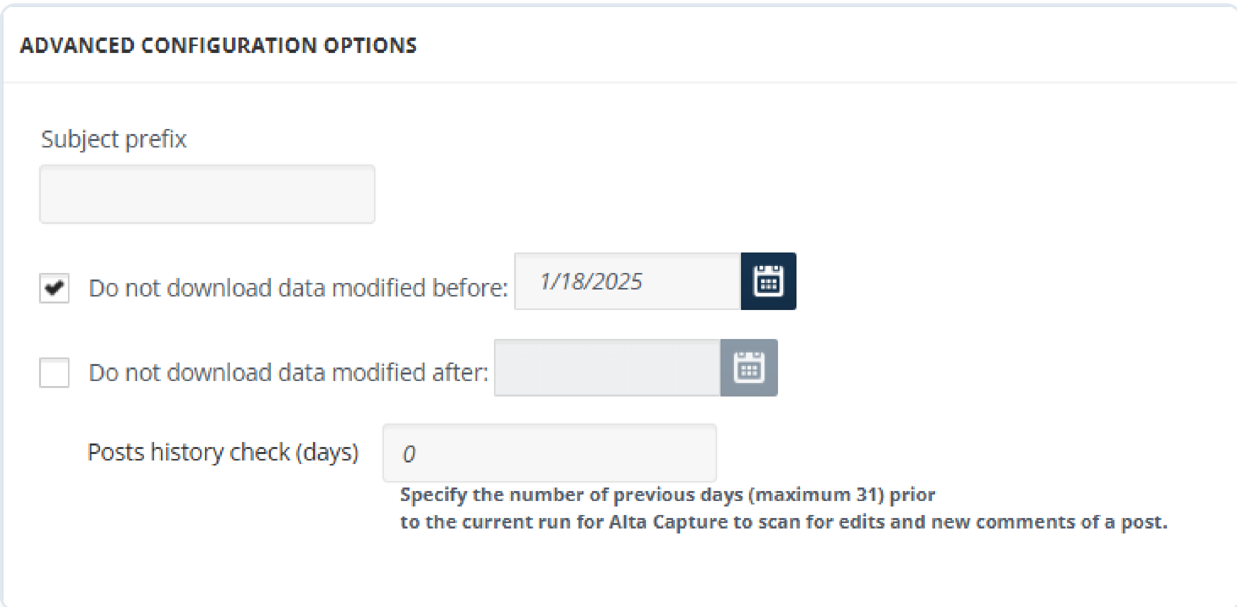
Advanced Configuration Option

To configure advanced options:

1. Specify the **Subject Prefix** in the subject line of imported emails. This is useful for organizing imported data, i.e., when multiple sources share a common target.

   > **Note:** Not applicable to the EV Folder target.

2. Specify **Do not download data modified before** and **Do not download data modified after** to allow cutting off data outside the set date range. If the before date is set to 08/17/2023 and the after date is set to 08/25/2023, only the data between these two dates will be downloaded. Data outside that range will be ignored. Note that both options can be used independently as well.
3. Specify the number of the previous days (0-31) prior to the current run so that Capture can scan for edits and new comments of a post.



Supported Notifications

The importer supports the following notification types:

- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**

- **Import job running threshold exceeded**
- **Importer data deleted**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users
- Filters
- Targets
- Importer Settings

X (Twitter)

X (Twitter) is an online news and social networking site where people communicate in short messages called tweets. The X (Twitter) collector does not work with a proxy server.

> **Note:** X (Twitter) business/professional accounts are not supported.

Activities Captured

- GIFs captured as links
- GIF post texts
- Attachments captured as links
- Comments
- Retweets
- Quote tweets
- Emojis
- Tweets to time lines

- Poll post note (poll options are not captured)

> **Note:** Follows and direct messages are not captured.

Creating an X (Twitter) Application

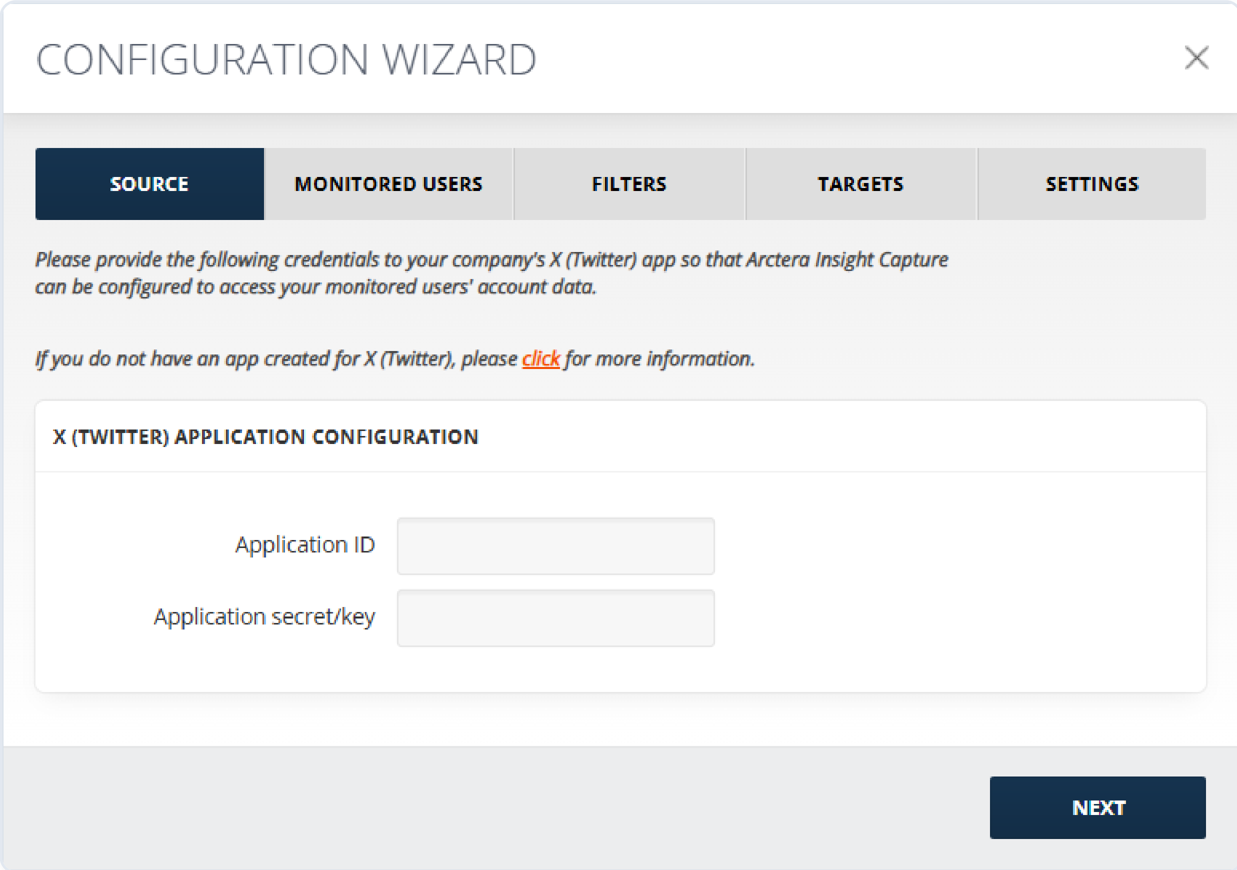
To create an X (Twitter) app:

1. Log in to https://developer.twitter.com/apps.
2. Click **Create New App**.
3. Complete the form by:
    - Providing a name for the application, i.e.," Capture X (Twitter) App".
    - Entering the URL of your organization's website.
    - Entering the URL of your local environment with the following format: `/ArcteraCapture_instance/Configuration/OAuthCallback.`
    - Agreeing to the terms of service.
4. Click **Create**.
5. Open the **Keys and Tokens** tab, to view the OAuth 2.0 **Client ID** and **Client Secret**.

Source Configuration

To set up the collector:

1. Provide your X (Twitter) **Application ID**.
2. Enter the **Application Secret/Key**.
3. Click **Save**.



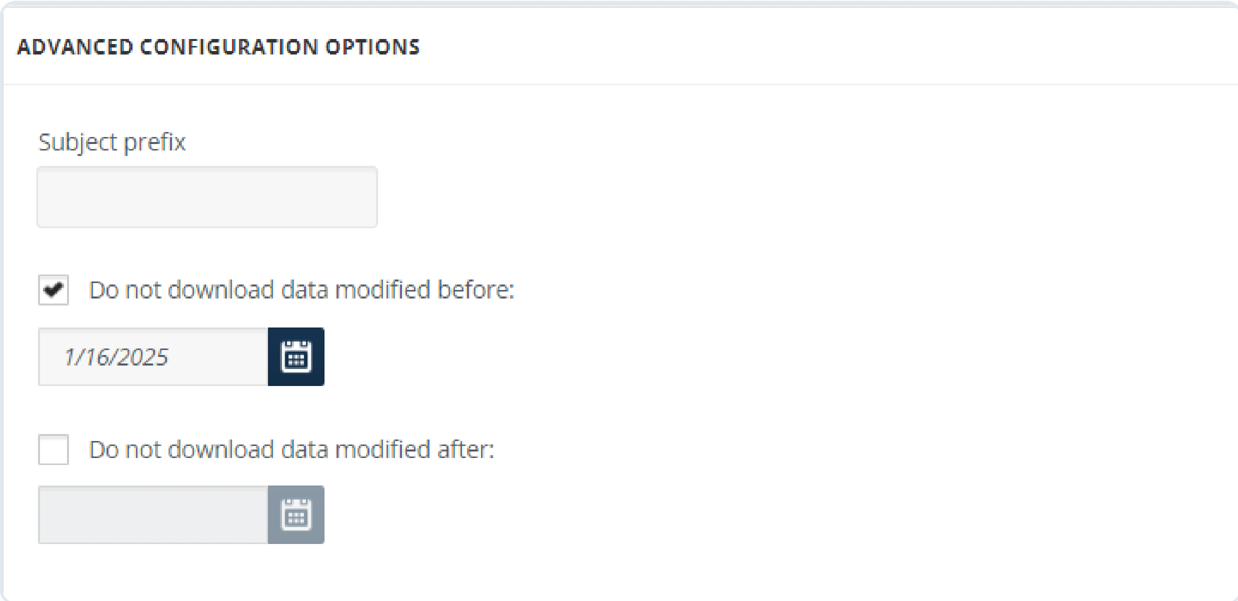
Timestamp Formatting

In addition to the primary stamp, a second timestamp can be enabled with its time zone. From the drop-down menu you can choose the time zone of the timestamp. The format of the timestamp in the output message can also be specified from the six options in the **Date Time Format** drop-down list.

Advanced Configuration Options

To configure advanced options:

1. Specify the **Subject Prefix** in the subject line of imported emails. This is useful for organizing imported data, i.e., when multiple sources share a common target.
2. Specify **Do not download data modified before** and **Do not download data modified after** to allow cutting off data outside the set date range. If the before date is set to 08/17/2023 and the after date is set to 08/25/2023, only the data between these two dates will be downloaded. Data outside that range will be ignored. Note that both options can be used independently as well.



Supported Notifications

The importer supports the following notification types:

- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**

- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users for Twitter
- Filters
- Targets
- Importer Settings

XIP

Greenwich Associates is the leading global provider of market intelligence and advisory services to the financial services industry. They specialize in providing fact-based insights and practical recommendations to improve business results.

Activities Captured

File Formats Supported by the Collector

- .csv

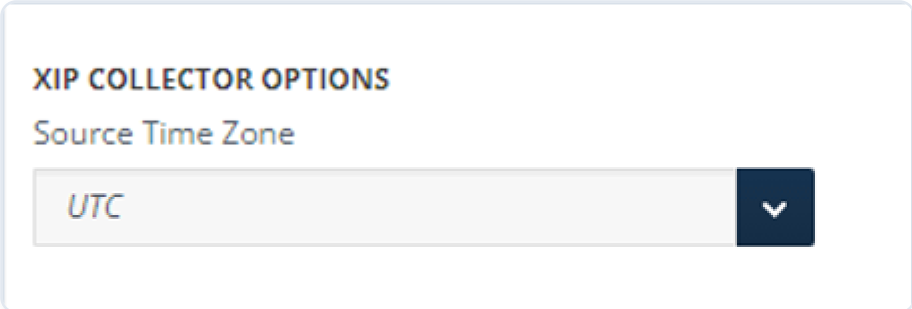
Source Configuration

For information on how to configure the following sections of the **Source** tab, see:

- File Source Configuration
- PGP Configurations
- Quarantine Location
- Miscellaneous Settings

XIP Collector Options

If you want to manually set up the **Source Time Zone**, select the relevant one from the drop-down list.



Arctera Capture assumes that the messages in the source file are of the set time zone and based on that data the dates in the messages are processed to UTC time zone. By default, Source Time Zone is set as the Local Time Zone.

Supported Notifications

The importer supports the following notification types:

- **Quarantine file**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Failed to quarantine file**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users (N/A)

- Filters
- Targets
- Importer Settings

XSLT/XML

Arctera Capture XSLT/XML collector allows our customers to rapidly transform XML file using XSLT to a predefined format. Once XML is transformed, the XML can be processed by generating the required mapping "From" "To" "Subject" "Date" "body" fields to appropriate elements of the XML file. The mapping varies from source to source, and it must be written separately. Contact Arctera Support to get the template and the signature file corresponding to the source you are going to use it for.

Activities Captured

- Messages

Captured messages can contain:

- Message subject
- Message headers
- Participants: From, To, CC, and BCC
- Activity datetime
- Message body

File Formats Supported by the Collector

- .xml

Source Configuration

For information on how to configure the following sections of the **Source** tab, see:

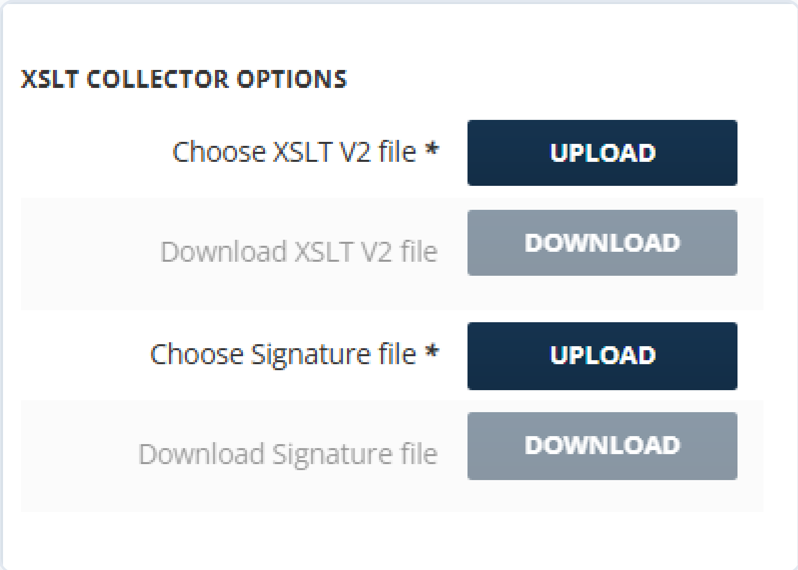
- File Source Configuration
- PGP Configurations
- Quarantine Location
- Miscellaneous Settings

XSLT Collector Options

To configure the section:

1. Upload the signed XSLT template.
2. Upload the Signature file.

> **Note:** Templates must be reviewed and cryptographically signed by Arctera.



Supported Notifications

The importer supports the following notification types:

- **Quarantine file**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Failed to quarantine file**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**

- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users (N/A)
- Filters
- Targets
- Importer Settings

Yieldbroker

Yieldbroker is the leading Tier 1 licensed electronic trading platform for Australian and New Zealand debt securities and derivatives. It is a dynamic collector that brings Banks, Portfolio Managers, Treasuries and Risk Managers together in a trusted trading environment with unrivalled liquidity and coverage of the AUD and NZD debt capital markets. The Yieldbroker collector processes data from Yieldbroker messages.

Activities Captured

- Participant names and email addresses in the To, From, CC, and BCC fields
- Messages in the body of the output message
- Sender and Recipient company names in the body along with messages
- Thread ID in the message subject

File Formats Supported by the Collector

- .csv

Source Configuration

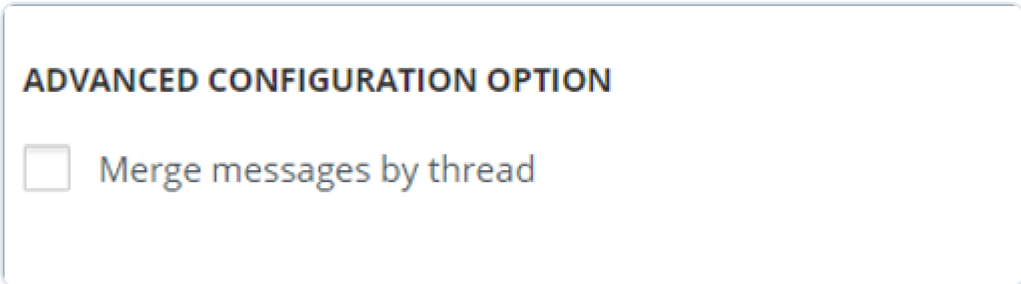
For information on how to configure the following sections of the **Source** tab, see:

- File Source Configuration
- PGP Configurations

- Quarantine Location
- Attachment Validation
- Miscellaneous Settings

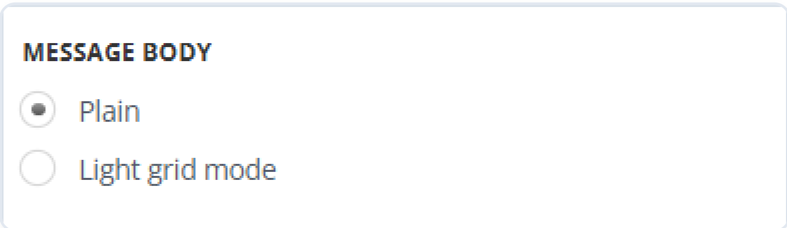
Advanced Configuration Options

The **Merge messages by thread** option combines all messages in a thread into a single message.



Message Body

This specifies how the imported message will be displayed in the target. The **Plain text** mode organizes the data in a simple way and data displayed in a **Light grid** mode is two-toned, easy to be viewed with limited metadata.



Supported Notifications

The importer supports the following notification types:

- **Quarantine file**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Failed to quarantine file**
- **Import job completed with failure**

- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users (N/A)
- Filters
- Targets
- Importer Settings

YouTube

YouTube is an online video sharing and social media platform owned by Google. It acts as a social network by allowing users with a Google account to watch and upload their videos, comment on videos, rate and respond to comments, like or dislike videos, etc.

Activities Captured

- Comments/replies of channel discussions
- Comments/replies of videos on channel playlists
- Comments/replies of uploaded videos
- Edits of comments/replies (only the latest version)
- Likes count
- Video view counts

> **Note:** Deleted comments and replies are not captured due to the YouTube API limitations.

Creating a YouTube Application

To create a YouTube application, the user should:

- Create a new project
- Create credentials
- Manage domain-wide authority delegations.

To create a new project:

1. Sign in to Google Cloud Platform.
2. Click **Select a project**, then **NEW PROJECT**.
3. Enter a name for the project and click **CREATE**.
4. Once the project is created, click **SELECT PROJECT** from the Notifications and you are navigated to the Project page.
5. From the left side navigation menu, select **APIs & Services** > **Dashboard**.
6. Click **ENABLE APIS AND SERVICES**.
7. In the **Search for APIs & Services** search box, type `YouTube Data API v3`.
8. Click **YouTube Data API v3**.
9. Once you are in the Gmail API page, click **ENABLE**.

To create the credentials:

1. From the left side navigation menu, select **APIs & Services** > **Credentials**.
2. Click **CREATE CREDENTIALS** and select **OAuth client ID**.
3. From the **Application type** drop-down menu, select **Web application**.
4. Enter the name for the application.
5. In the **Authorized redirect URIs** section, click **ADD URI** and add the URL of your local Arctera Capture environment and click **CREATE**.

> **Note:** The **Redirect URI** can be found in the Click information of the collector source configuration.

6. Copy and save the **Client ID** and **Client ID** from the created OAuth client pop-up window.

To manage Domain-Wide Authority Delegation:

1. Sign in to Google Admin Console.
2. On the left side menu, click **Security** > **API controls**.

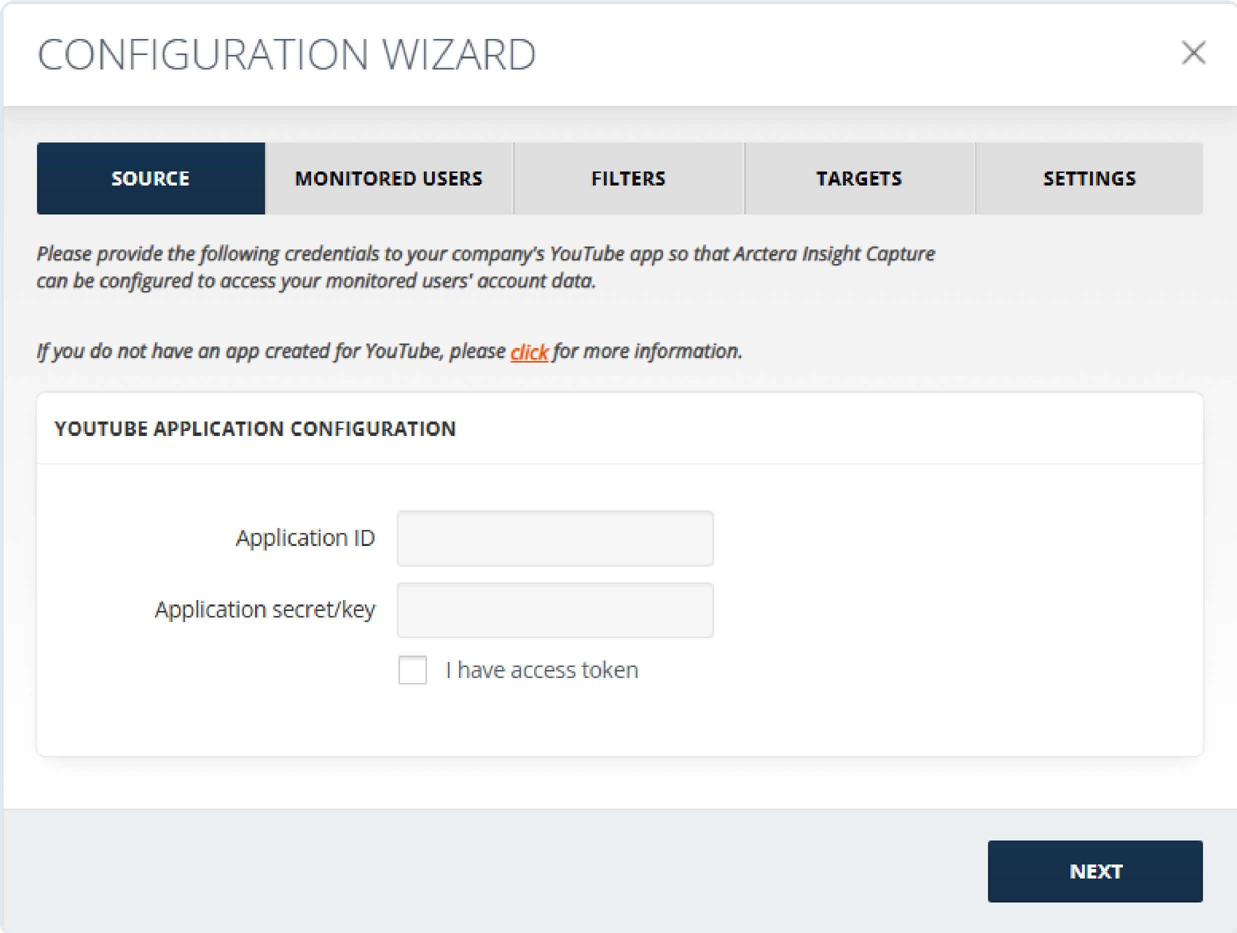
3. Scroll down to **Domain wide delegation** section and click **MANAGE DOMAIN WIDE DELEGATION**.
4. Click **Add new**.
5. Enter the above saved Client ID in the **Client ID** field, add the following scopes in the **OAuth scopes** fields:
   - `https://www.googleapis.com/auth/youtube`
   - `https://www.googleapis.com/auth/youtube.force-ssl`
   - `https://www.googleapis.com/auth/youtube.readonly`
   - `https://www.googleapis.com/auth/youtubepartner`
6. Click **AUTHORIZE**.

> **Note:** By using this importer, you are agreeing to the YouTube terms at https://www.youtube.com/t/terms,https://policies.google.com/privacy.

Source Configuration

To set up the collector:

1. In the **Application ID** field, enter Client ID copied previously.
2. In **Application secret/key**, enter the copied Client Secret and click **Next**.



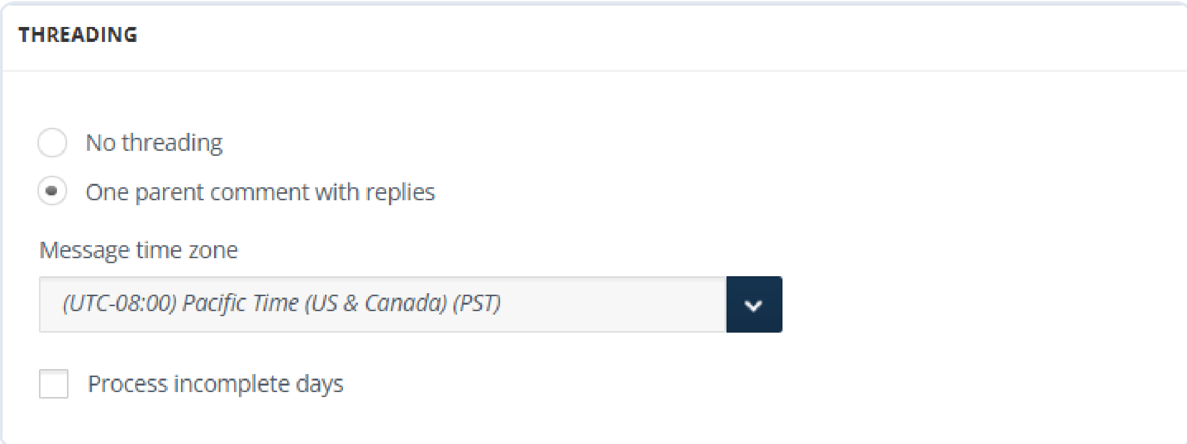
Timestamp Formatting

In addition to the primary stamp, a second timestamp can be enabled with its time zone. From the drop-down menu you can choose the time zone of the timestamp. The format of the timestamp in the output message can also be specified from the six options in the **Date Time Format** drop-down list.

Threading

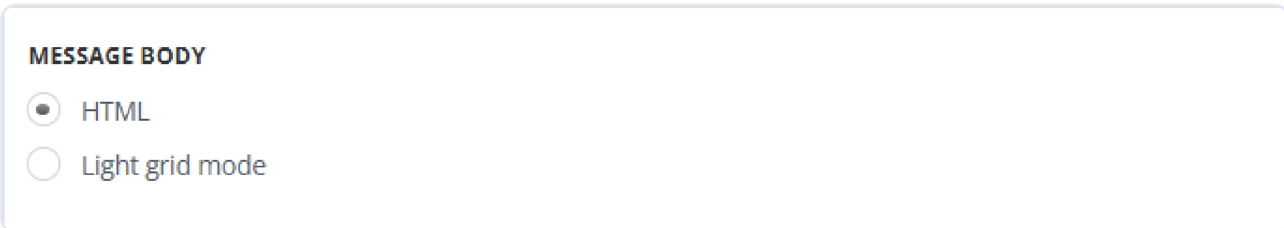
For Threading:

- If the **No threading** radio button is activated, only a single message is generated for a comment or reply.
- If **One parent comment with replies** is activated, then a threaded message is generated for comments and replies.
    - The **Message time zone** by which the messages are split based on the selected time zone from the drop-down menu. When **Process Incomplete Days** option is enabled, the messages of the days that have not yet ended will be imported in a separate email. This option can be selected only if **One parent comment with replies** is activated.



Message Body

This specifies how the imported message will be displayed in the target. The **HTML** mode organizes the data in a simple way and data displayed in a **Light grid** mode is two-toned, easy to be viewed with limited metadata.

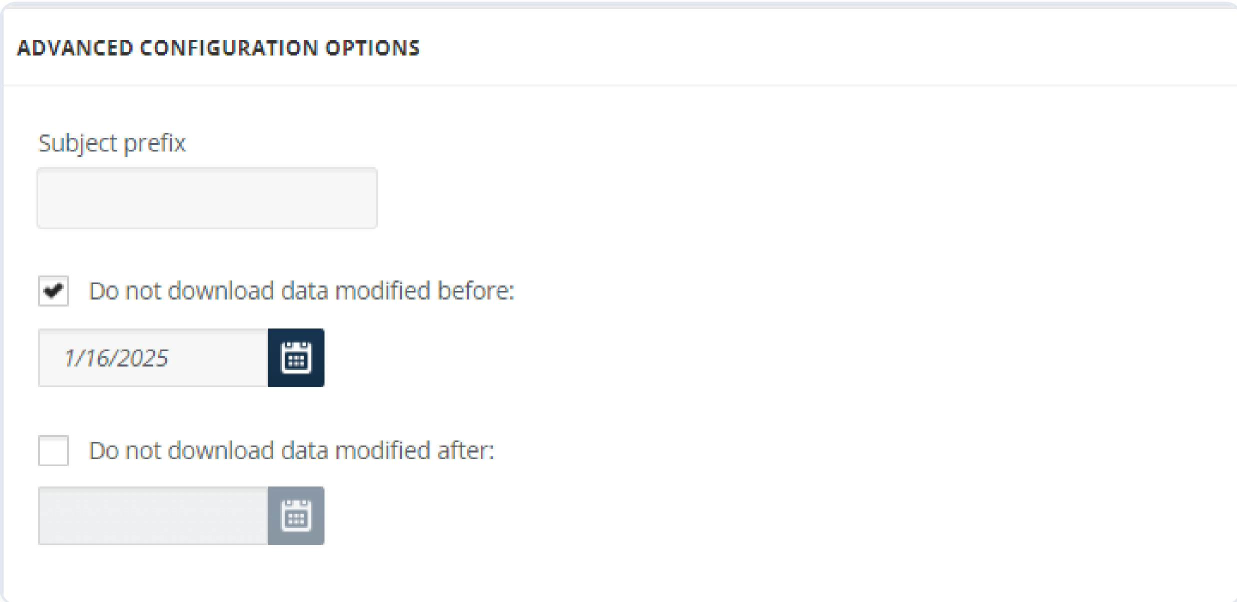


Advanced Configuration Options

To configure advanced options:

1. Specify the **Subject Prefix** in the subject line of imported emails. This is useful for organizing imported data, i.e., when multiple sources share a common target.

2. Specify **Do not download data modified before** and **Do not download data modified after** to allow cutting off data outside the set date range. If the before date is set to 08/17/2024 and the after date is set to 08/25/2024, only the data between these two dates will be downloaded. Data outside that time frame will be ignored. Note that both options can be used independently as well.



Supported Notifications

The importer supports the following notification types:

- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Import job completed with failure**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users (N/A)
- Filters
- Targets
- Importer Settings

Zoom Chat

Zoom is the leader in modern enterprise video communications, with an easy, reliable cloud platform for video and audio conferencing, chat, and webinars.

Zoom Team Chat is a messenger that allows users with free and paid accounts to facilitate communications between Zoom users. With Zoom Team Chat, you can send texts, audio, and video messages, as well as share files, emojis, screenshots, and so on.

> **Note:** The Zoom account used for the Zoom Chat collector needs to be on the Business or Enterprise plan to gain access to the API. Note that the Pro plan is not supported.

Activities Captured

- One-on-one chat messages
  - Create
  - Edit
  - Delete
- Group chat messages
  - Create
  - Edit
  - Delete
- Channel messages
  - Create
  - Edit
  - Delete
- Membership activities (joined/left)

Captured messages can contain:

- Links

> **Note:** Both inserted and regular links are captured.

- Emojis
- Attachments
- Forwarded messages

> **Note:** Deleted forwarded messages are not captured due to the API limitation.

- Voice messages
- Video messages
- Code snippets
- Hosted GIFs

> **Note:** The link of the GIFs only is captured due to the API limitation.

> **Note:** Chats only from the last 6 months can be captured.

> **Note:** Text formatting (rich text) is captured as plain text.

> **Note:** Message reactions are not captured due to the API limitation.

Creating a Zoom OAuth App

To create an oAuth application:

1. Sign in to Zoom Marketplace.
2. Select **Develop** > **Build App**.
3. Select **General App** and click **Create**.

4. A Client ID and Client secret will be generated. Use these credentials to configure the collector.
5. On the **Basic Information** page, under **Select how the app is managed**, choose **Admin-managed** and click **Save**.
6. Give an app name, choose **Account-level app**, disable **Publishing to Marketplace** and click **Create**.
7. Copy the Client ID and the Client Secret. They will be used later to configure the Zoom collector.
8. Under **OAuth Information** add the URL of your local environment in the following format: https://<your_instance\>/Configuration/OAuthCallback to the **OAuth Redirect URL**. Ensure that **OAuth Allow lists** field is filled with the same URL as well.

> **Note:** The **Redirect URI** can be found in the Click information of the collector source configuration.

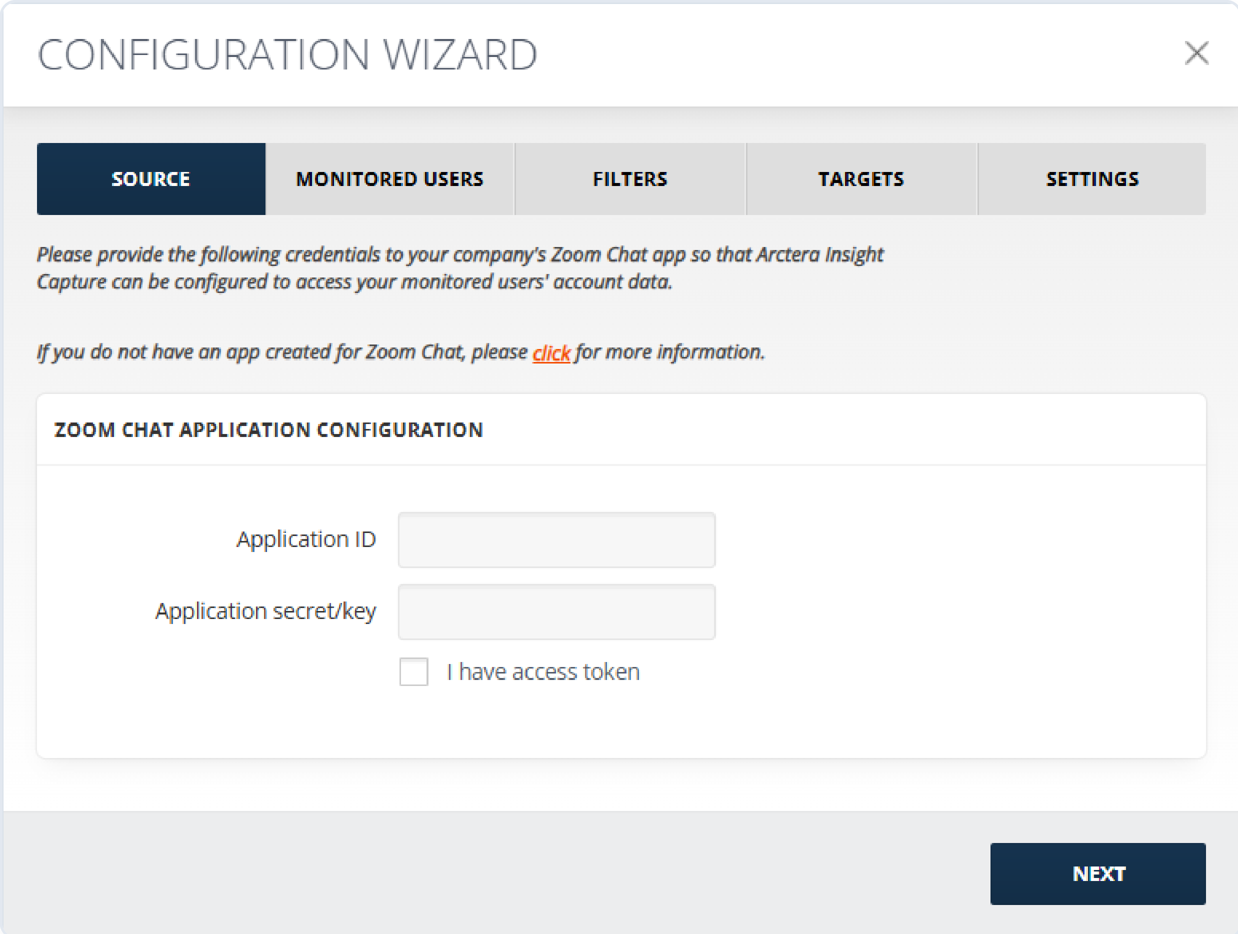
9. Click **Continue**.
10. Go to **Scopes** and click **Add Scopes**.
11. Add the following scopes to the application and click **Done**:
    - team_chat:read:list_user_channels:admin
    - team_chat:read:list_members:admin
    - team_chat:read:list_channel_activity_logs:admin
    - team_chat:read:user_message:admin
    - team_chat:read:message_emoji:admin
    - user:read:user:admin
    - user:read:list_users:admin
    - report:read:chat_session:admin
    - report:read:list_chat_sessions:admin
12. Click **Done**.

Source Configuration

To configure the collector:

1. Enter Client ID in the **Application ID** field.

2. Enter Client Secret in the **Application Secret/Key** field. Click **NEXT**.



3. In the opened pop-up, confirm the application connection. Make sure the pop-ups are not disabled in the browser window.

Timestamp Formatting

In addition to the primary stamp, a second timestamp can be enabled with its time zone. From the drop-down menu you can choose the time zone of the timestamp. The format of the timestamp in the output message can also be specified from the six options in the **Date Time Format** drop-down list.

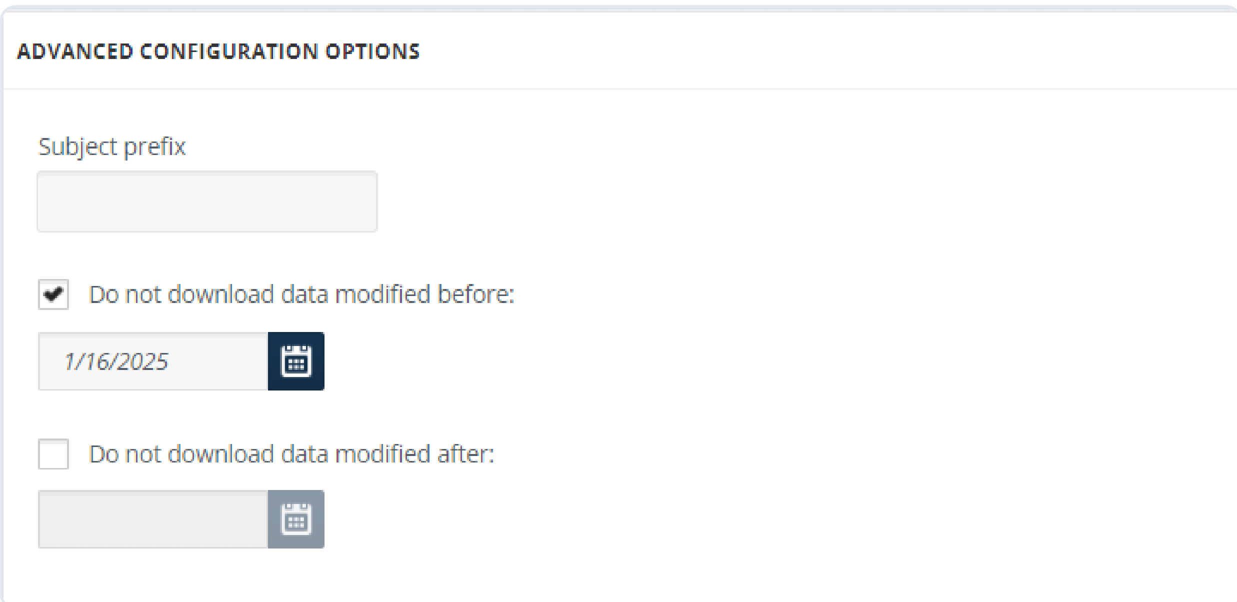
Advanced Configuration Options

To configure the advanced options:

1. Specify the **Subject Prefix** in the subject line of imported emails. This feature allows organizing imported data when multiple sources share a common target.

   > **Note:** Not applicable to the EV Folder target.

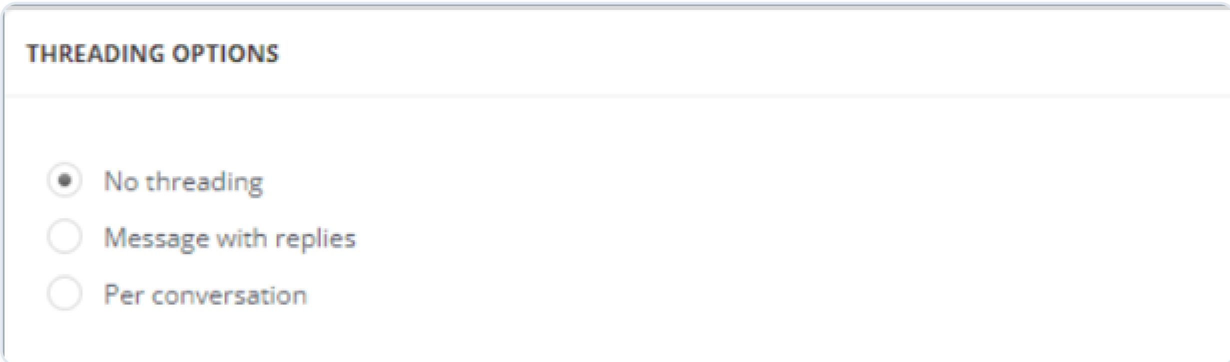
2. Specify **Do not download data modified before** and **Do not download data modified after** to allow cutting off data outside the set date range. If the before date is set to 08/17/2022 and the after date is set to 08/25/2022, only the data between these two dates will be downloaded. Data outside that time frame will be ignored. Note that both options can be used independently as well.



Threading Options

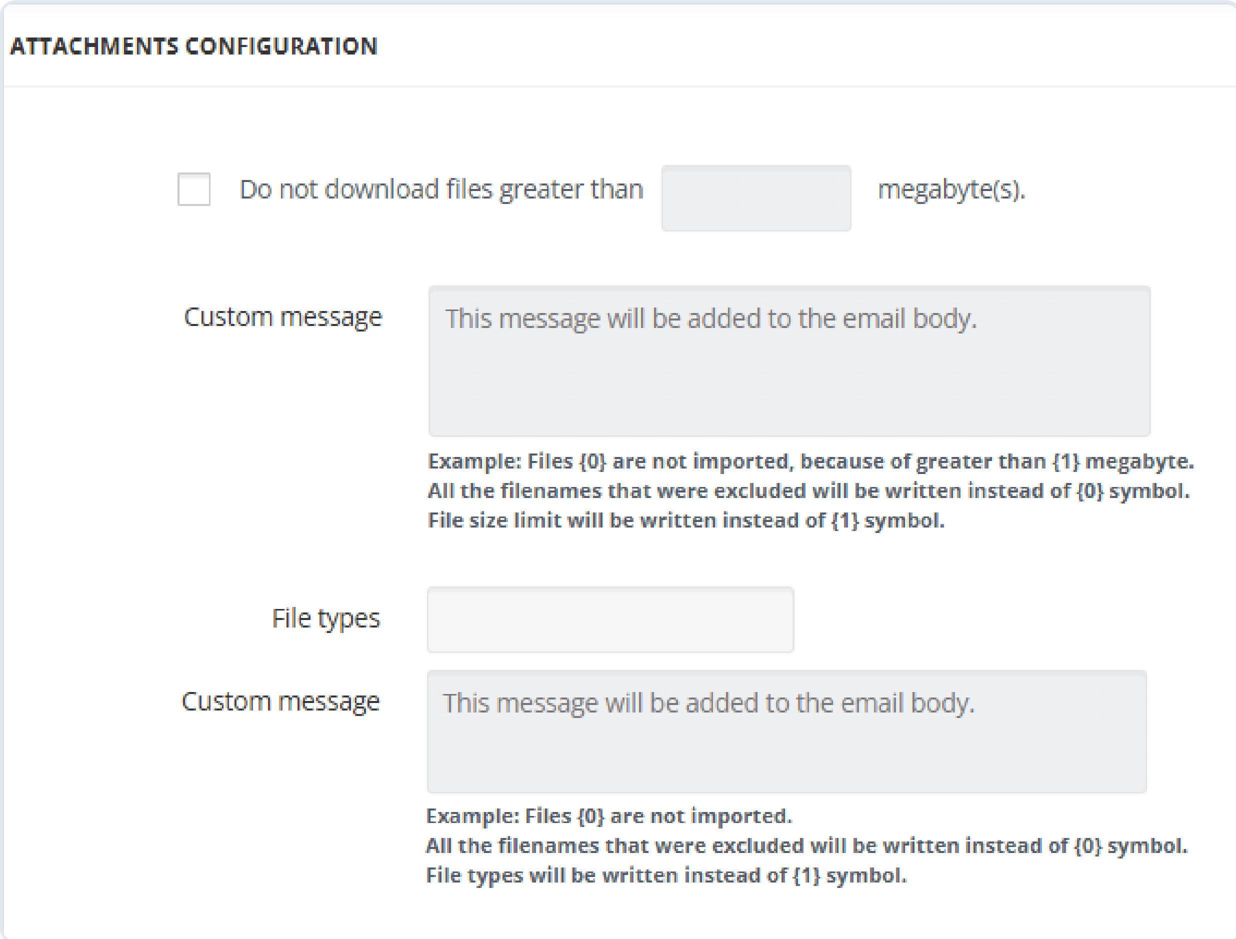
Enable one of the following options:

- **No threading** - If selected, only a single message will be generated for a message in the chat/ channel.
- **Message with replies** - If selected, chat/channel messages with all their replies will be generated.
- **Per conversation** - If selected, chat/channel messages per conversation will be generated.



Attachments Configuration

- When **Do not download files greater than X megabyte(s)** is selected, the files bigger than the filled-in number of megabytes, are not downloaded. In **Custom Message** field, a text for those excluded files can be specified. E.g.,"Files {0} are not imported, because they are greater than {1) megabytes". {0} is used to add the name of the file and {1} is used to add the number of megabytes specified above.
- In the **File Types** field, the types of files that should not be downloaded can be specified in the following format: e.g., .txt | .xml. The vertical bar is used to separate the file types.



Supported Notifications

The importer supports the following notification types:

- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users
- Filters
- Targets
- Importer Settings

Zoom Meetings

Zoom is the leader in modern enterprise video communications, with an easy, reliable cloud platform for video and audio conferencing, chat, and webinars.

> **Note:** The Zoom account used for the Zoom collector needs to be on Business or Enterprise plan to gain access to the API. Note that Pro plan is not supported.

Activities Captured

- Meeting metadata
- Meeting recording files:
  - Audio and video
  - Audio
  - Audio transcripts
- Meeting chats
  - Messages
  - Replies
  - Emojis

Notes

- Only meetings from the last 6 months can be captured. The option to select a longer cut-off date in the Arctera Capture UI, has also been disabled.

- Zoom does not support IP addresses as call back URLs.
- To capture the content, the meetings should be recorded. This applies to chats during meetings too. To enable automatic recording, go to My Settings - Zoom > **General** > **Automatic recording**.
- If a message was sent privately to one of the meeting participants, it is not added to the recording file, as the Zoom API does not provide that option. We recommend disabling the meeting chat direct messages from Account Settings - Zoom > **In Meeting (Basic)** > **Meeting chat - Direct messages** to be SEC-compliant.
- Attachments sent during a meeting are not captured. To prevent data loss, the option to send files via meeting chat should be disabled from Account Settings - Zoom > **In Meeting (Basic)** > **Send files via meeting chat**.
- In addition, the following features should be disabled for the hosts:
    - **General** > **Host can pause/stop the auto recording in the cloud**
    - **General** > **The host can delete cloud recordings**
    - **Notification** > **Delete cloud recordings and transcripts after a specified number of days**

Creating a Zoom OAuth App

To create an oAuth application:

1. Login to Zoom Marketplace in case of using Zoom Commercial.

   OR,
2. Login to Zoom for Government in case of using Zoom for Government.
3. Select **Develop** > **Build App**.
4. Select **General App** and click **Create**.
5. A Client ID and Client secret will be generated. Use these credentials to configure the collector.
6. On the **Basic Information** page, under **Select how the app is managed**, choose **Admin-managed** and click **Save**.
7. Under **OAuth Information** add the URL of your local environment in the following format: `https://<your_instance>/Configuration/OAuthCallback` to the **OAuth Redirect URL**. Ensure that **OAuth Allow lists** field is filled with the same URL as well.

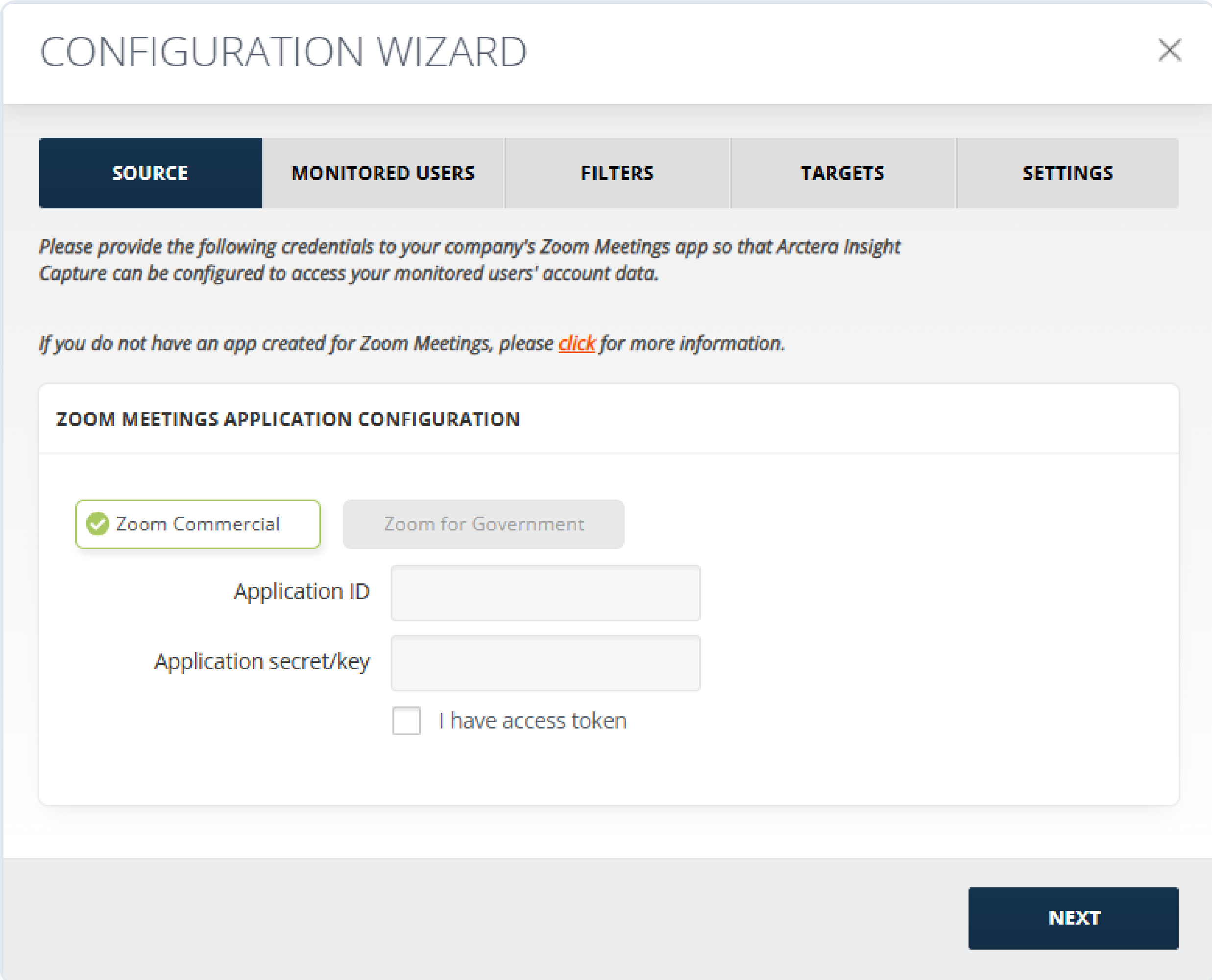
> **Note:** The **Redirect URI** can be found in the Click information of the collector source configuration.

8. Click **Continue**.
9. Go to **Scopes** and click **Add Scopes**.
    - `user:read:user:admin`
    - `user:read:list_users:admin`
    - `dashboard:read:list_meetings:admin`
    - `dashboard:read:list_meeting_participants:admin`
    - `cloud_recording:read:list_recording_files:admin`
    - `cloud_recording:read:list_recording_files:master`
10. Click **Done**.

Source Configuration

To configure the collector:

1. Enable **Zoom Commercial** or **Zoom for Government** and use the respective credentials of the applications.
2. Enter Client ID in the **Application ID** field.
3. Enter Client Secret in the **Application Secret/Key** field. Click **NEXT**.



4. In the opened pop-up, confirm the application connection. Make sure that the pop-ups are not disabled in the browser window.

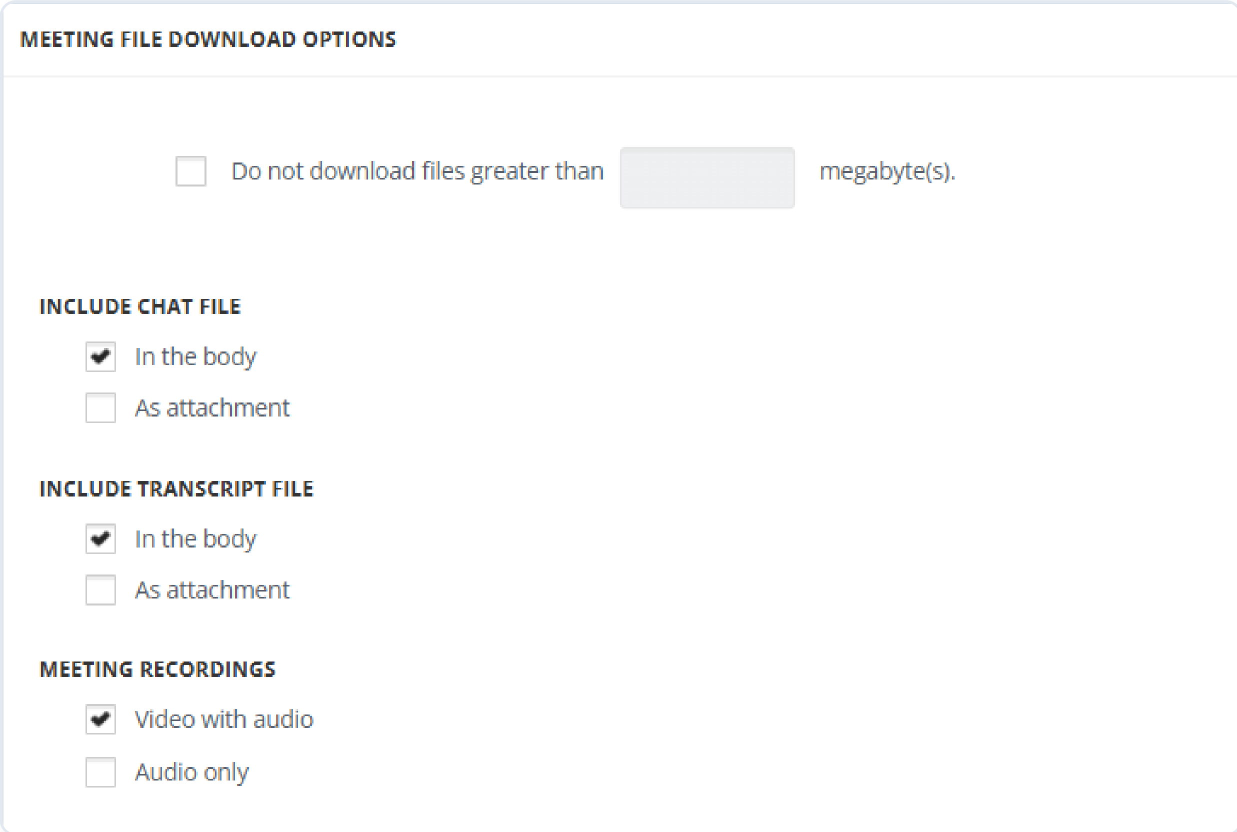
Timestamp Formatting

In addition to the primary stamp, a second timestamp can be enabled with its time zone. From the drop-down menu you can choose the time zone of the timestamp. The format of the timestamp in the output message can also be specified from the six options in the **Date Time Format** drop-down list.

Meeting File Download Options

This section includes the following:

- When **Do not download files greater than X megabyte(s)** is selected, the files, that are bigger than the filled-in number of megabytes, are not downloaded.
- **Include Chat File** specifies how the chat file is added to the imported message: in the body of the message or attached to the message as a separate file.
- **Include Transcript File** specifies how the transcript file is added to the imported message in the body of the message or attached to the message as a separate file.
- **Meeting Recordings** specifies whether video with audio or only audio is included in the imported message.



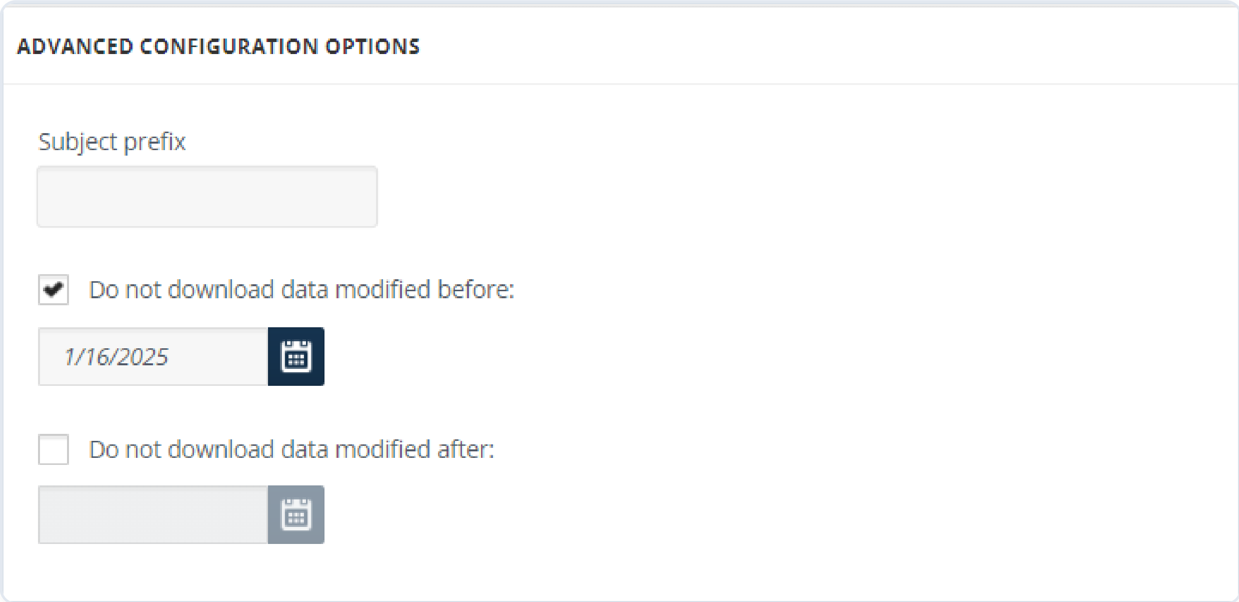
Advanced Configuration Options

To configure advanced options:

1. Specify the **Subject Prefix** in the subject line of imported emails. This is useful for organizing imported data, i.e., when multiple sources share a common target.

   > **Note:** Not applicable to the EV Folder target.

2. Specify **Do not download data modified before** and **Do not download data modified after** to allow cutting off data outside the set date range. If the before date is set to 08/17/2024 and the after date is set to 08/25/2024, only the data between these two dates will be downloaded. Data outside that time frame will be ignored. Note that both options can be used independently as well.



Supported Notifications

The importer supports the following notification types:

- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users
- Filters
- Targets

- Importer Settings

Zoom Meetings Chats

Zoom is the leader in modern enterprise video communications, with an easy, reliable cloud platform for video and audio conferencing, chat, and webinars.

Zoom's Meeting and Webinar Archiving solution allows account administrators to set up an automated mechanism to collect and archive meeting data to a 3rd party platform of their choice and hence, satisfy FINRA and/ or other compliance requirements. Only account administrators can manage what data is archived, what is displayed in the disclaimer, and enable archiving for specific groups as well. Arctera Capture uses this API to retrieve archived meeting or webinar chats.

> **Note:** The Zoom account used for the Zoom collector needs to be on the Business or Enterprise plan to gain access to the API. Note that the Pro plan is not supported. **Note:** The Meeting Archiving feature is enabled for your account byZoom Support.

Activities Captured

- Webinar/Meeting metadata
- Webinar/Meeting chats
- Polls in chats

Notes

- The maximum number of days of archiving is up to 60 days. The number of days can be specified from Account Settings - Zoom > **In Meeting (Advanced)** > **Set the retention for archiving content**.
- Attachments sent during a meeting are not captured. To prevent data loss, the option to send files via meeting chat should be disabled from the Account Settings - Zoom > **In Meeting (Basic)** > **Send files via meeting chat**.

Creating a Zoom OAuth App

To create an oAuth application:

1. Login to Zoom Marketplace in case of using Zoom Commercial.

   OR,

2. Login to Zoom for Government in case of using Zoom for Government.
3. Select **Develop** > **Build App**.
4. Select **General App** and click **Create**.
5. A Client ID and Client secret will be generated. Use these credentials to configure the collector.
6. On the **Basic Information** page, under **Select how the app is managed**, choose **Admin-managed** and click **Save**.
7. Under **OAuth Information** add the URL of your local environment in the following format: `https://<your_instance>/Configuration/OAuthCallback` to the **OAuth Redirect URL**. Ensure that **OAuth Allow lists** field is filled with the same URL as well.

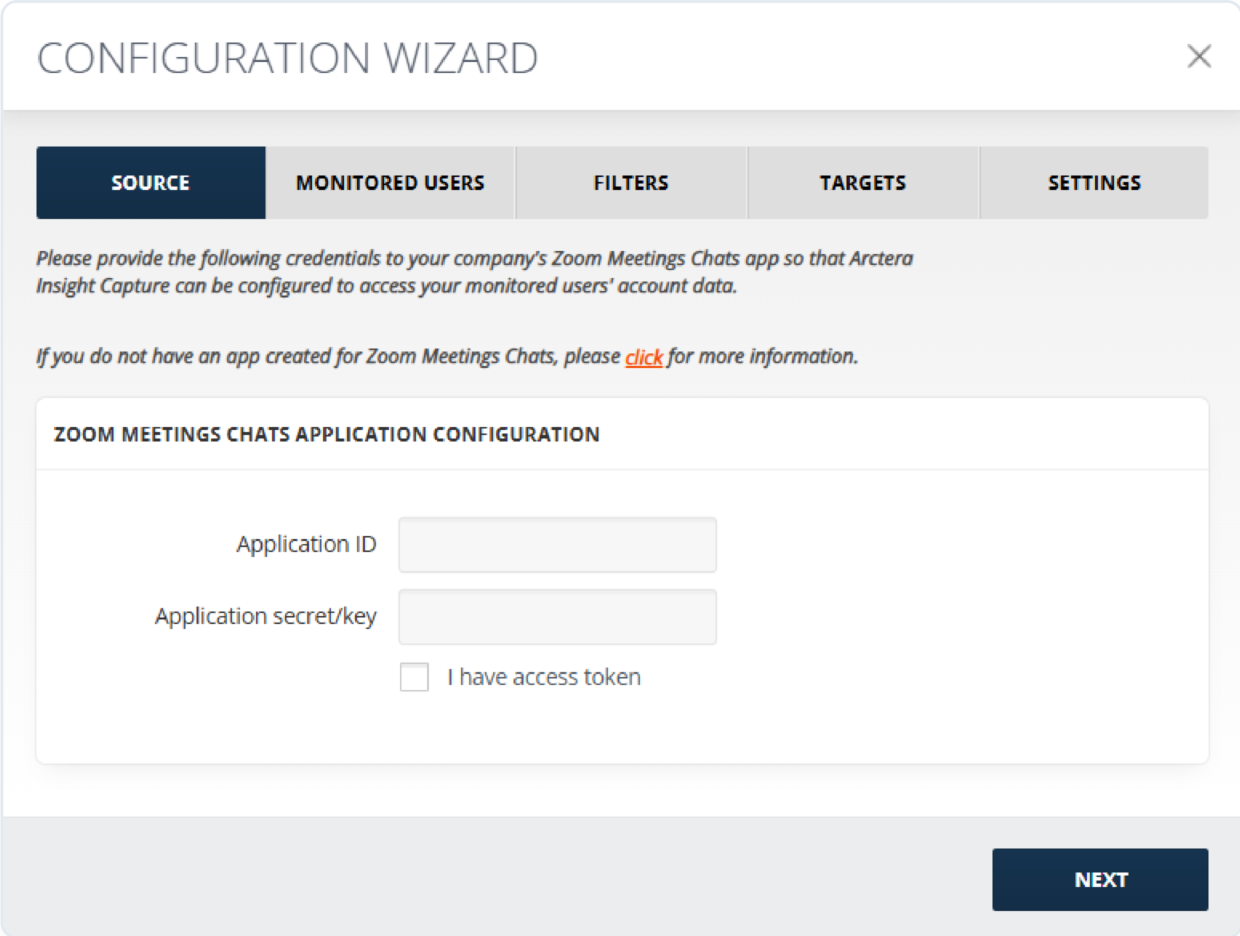
   > **Note:** The **Redirect URI** can be found in the Click information of the collector source configuration.

8. Click **Continue**.
9. Go to **Scopes** and click **Add Scopes**:
   - `user:read:user:admin`
   - `user:read:list_users:admin`
   - `archiving:read:list_archived_files:admin`
   - `archiving:read:list_archived_files:master`
   - `meeting:read:list_past_participants:admin`
   - `meeting:read:list_poll_results:admin`
10. Click **Done**.

Source Configuration

To configure the collector:

1. Enter Client ID in the **Application ID** field.
2. Enter Client Secret in the **Application Secret/Key** field. Click **NEXT**.



3. In the opened pop-up, confirm the application connection. Make sure that the pop-ups are not disabled in the browser window.

Timestamp Formatting

In addition to the primary stamp, a second timestamp can be enabled with its time zone. From the drop-down menu you can choose the time zone of the timestamp. The format of the timestamp in the output message can also be specified from the six options in the **Date Time Format** drop-down list.

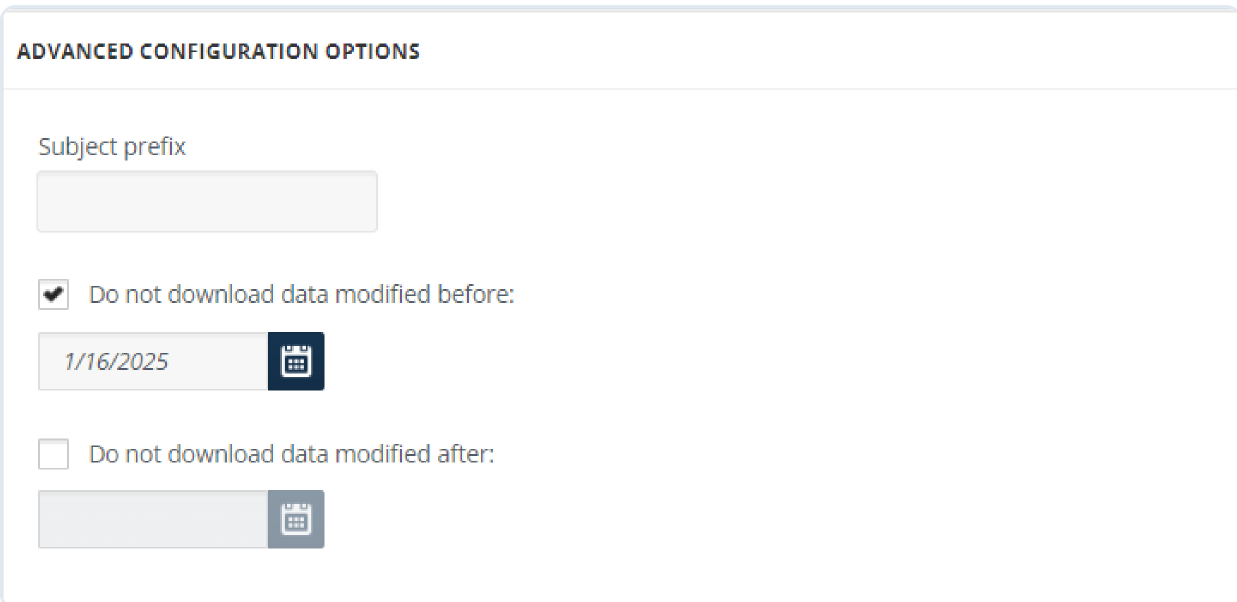
Advanced Configuration Options

To configure advanced options:

1. Specify the **Subject Prefix** in the subject line of imported emails. This is useful for organizing imported data, i.e., when multiple sources share a common target.

> **Note:** Not applicable to the EV Folder target.

2. Specify **Do not download data modified before** and **Do not download data modified after** to allow cutting off data outside the set date range. If the before date is set to 08/17/2023 and the after date is set to 08/25/2023, only the data between these two dates will be downloaded. Data outside that time frame will be ignored. Note that both options can be used independently as well.



Supported Notifications

The importer supports the following notification types:

- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users
- Filters
- Targets
- Importer Settings

Zoom Meetings via Archiving API

Zoom is the leader in modern enterprise video communications, with an easy, reliable cloud platform for video and audio conferencing, chat, and webinars.

Zoom's Meeting and Webinar Archiving solution allows account administrators to set up an automated mechanism to collect and archive meeting data to a 3rd party platform of their choice and hence, satisfy FINRA and/ or other compliance requirements. Only account administrators can manage what data is archived, what is displayed in the disclaimer, and enable archiving for specific groups as well.

Arctera Capture uses this API to retrieve archived meeting or webinar files of an account.

> **Note:** The Meeting Archiving feature is enabled for your account byZoom Support. **Note:** The Zoom account used for the Zoom collector needs to be on the Business or Enterprise plan to gain access to the API. Note that the Pro plan is not supported.

Activities Captured

- Webinars/Meeting metadata
- Webinars/Meeting recording files:
  - Audio and video
  - Audio
  - Closed captions (only if the option is enabled by the user from the Zoom Settings)
- Webinars/Meeting chats
- Recording files as attachments

  > **Note:** A token should be added to download files with the download URLs.

- Polls in chats

Notes

- The maximum number of days of archiving is up to 60 days. The number of days can be specified from Account Settings - Zoom > **In Meeting (Advanced)** > **Set the retention for archiving content**.
- Attachments sent during a meeting are not captured. To prevent data loss, the option to send files via meeting chat should be disabled from the Account Settings - Zoom >**In Meeting (Basic)** > **Send files via meeting chat**.
- In addition, the following features should be disabled for the hosts:
  - **General** > **Host can pause/stop the auto recording in the cloud**
  - **General** > **The host can delete cloud recordings**

- **Notification** > **Delete cloud recordings and transcripts after a specified number of days**

Creating a Zoom OAuth App

To create an oAuth application:

1. Login to Zoom Marketplace in case of using Zoom Commercial.

OR,

1. Login to Zoom for Government in case of using Zoom for Government.
2. Select **Develop** > **Build App**.
3. Select **General App** and click **Create**.
4. A Client ID and Client secret will be generated. Use these credentials to configure the collector.
5. On the **Basic Information** page, under **Select how the app is managed**, choose **Admin-managed** and click **Save**.
6. Under **OAuth Information** add the URL of your local environment in the following format: https://<your_instance\>/Configuration/OAuthCallback to the **OAuth Redirect URL**. Ensure that **OAuth Allow lists** field is filled with the same URL as well.

> **Note:** The **Redirect URI** can be found in the Click information of the collector source configuration.

7. Click **Continue**.
8. Go to **Scopes** and click **Add Scopes**.

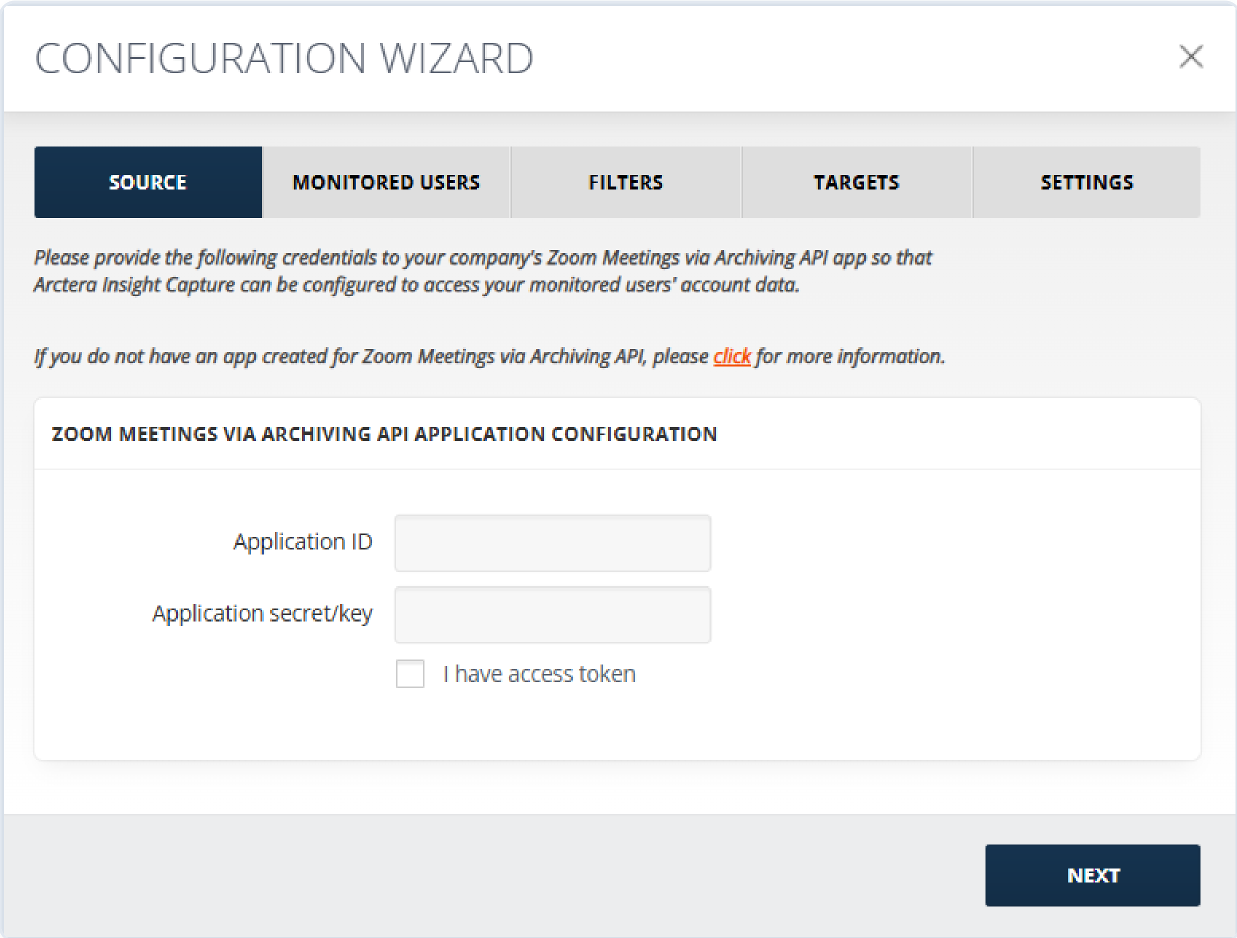
- meeting:read:list_past_participants:admin
- meeting:read:list_poll_results:admin
- archiving:read:archive_files:admin
- archiving:read:list_archived_files:admin
- user:read:user:admin
- user:read:list_users:admin
- webinar:read:list_past_polls:admin
- webinar:read:list_past_participants:admin

9. Click **Done**.

Source Configuration

To configure the collector:

1. Enter Client ID in the **Application ID** field.
2. Enter Client Secret in the **Application Secret/Key** field. Click **NEXT**.



3. In the opened pop-up, confirm the application connection. Make sure the pop-ups are not disabled in the browser window.

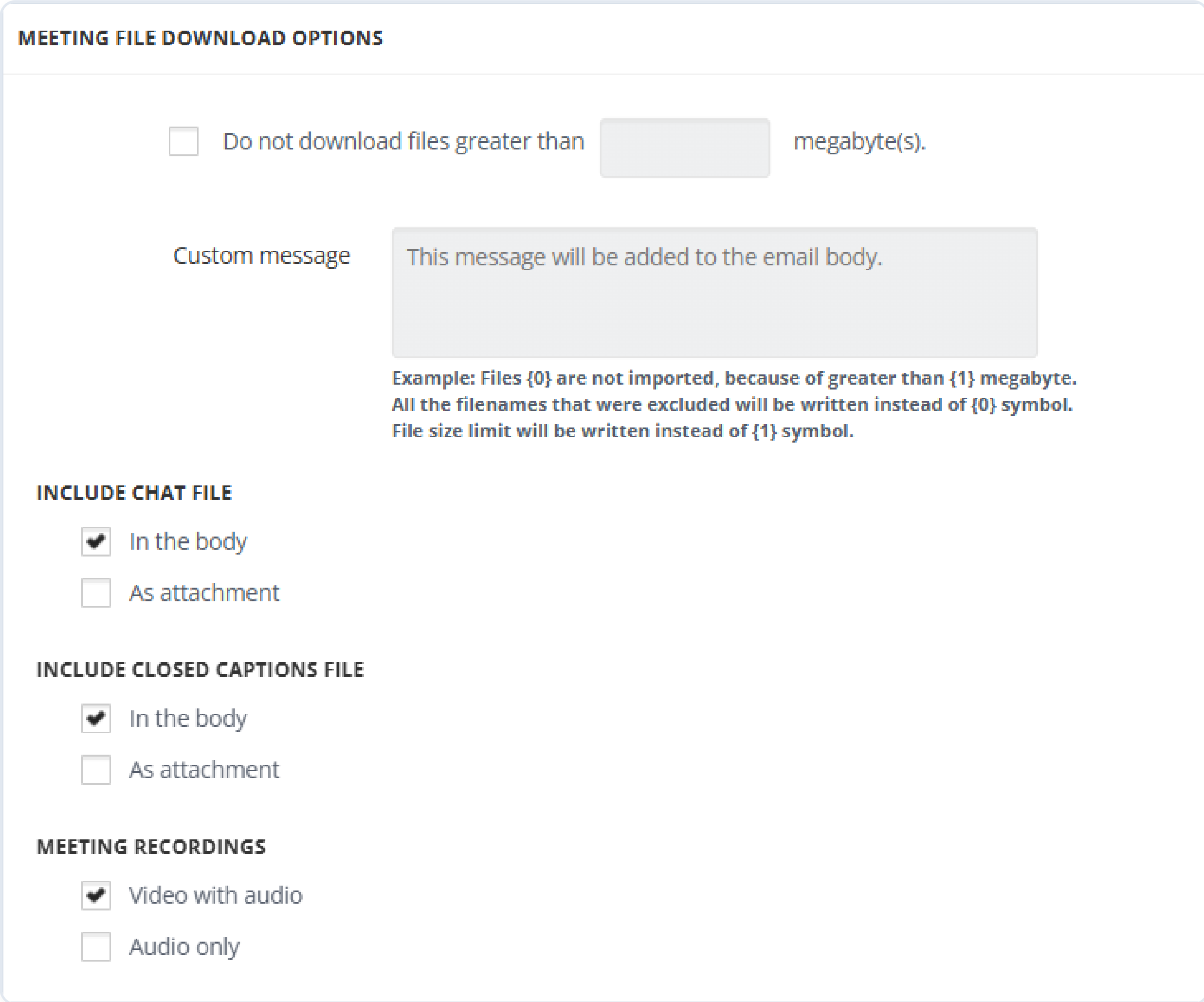
Timestamp Formatting

In addition to the primary stamp, a second timestamp can be enabled with its time zone. From the drop-down menu you can choose the time zone of the timestamp. The format of the timestamp in the output message can also be specified from the six options in the **Date Time Format** drop-down list.

Meeting File Download Options

This section includes the following:

- When **Do not download files greater than X megabyte(s)** is selected, the files, that are bigger than the filled-in number of megabytes, are not downloaded. In the **Custom Message** field, a text for those excluded files can be specified. For example: "Files {0} are not imported, because they are greater than {1) megabytes". {0} is used to add the name of the file and {1} is used to add the number of megabytes specified above.
- The **Include Chat File** option specifies how the chat file is added to the imported message - in the body of the message or attached to the message as a separate file.
- **Include Closed Captions File** option specifies how the closed captions are added to the imported message in the body of the message or attached to the message as a separate file.
- **Meeting Recordings** option specifies whether video with audio or only audio is included in the imported message.



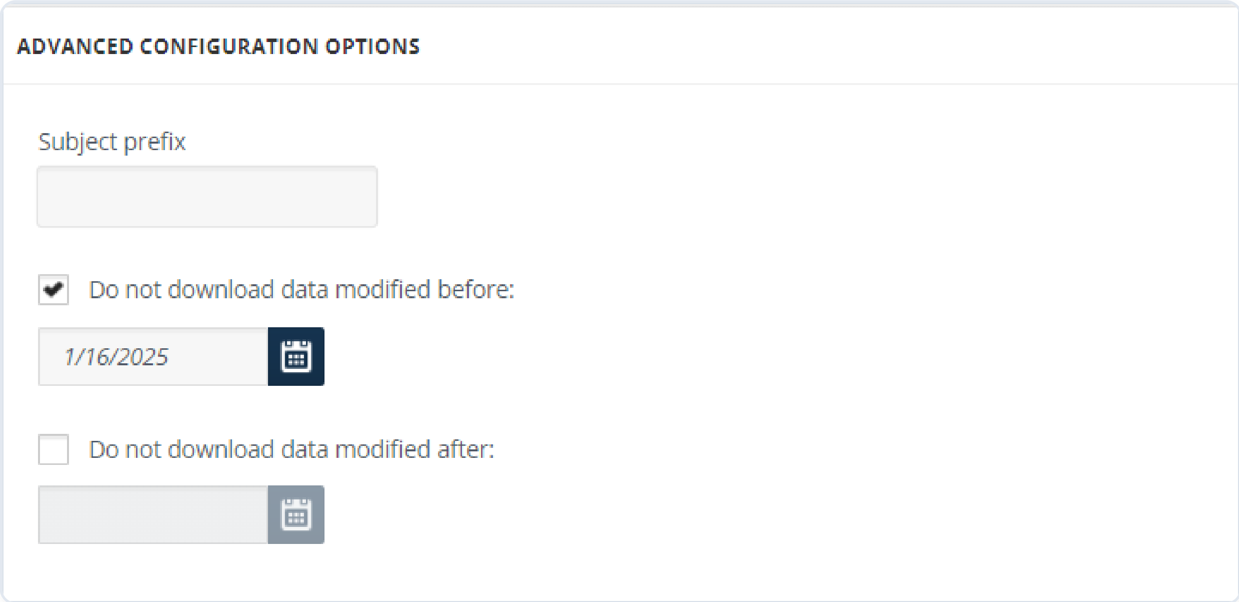
Advanced Configuration Options

To configure advanced options:

1. Specify the **Subject Prefix** in the subject line of imported emails. This is useful for organizing imported data, i.e., when multiple sources share a common target.

   > **Note:** Not applicable to the EV Folder target.

2. Specify **Do not download data modified before** and **Do not download data modified after** to allow cutting off data outside the set date range. If the before date is set to 08/17/2024 and the after date is set to 08/25/2024, only the data between these two dates will be downloaded. Data outside that time frame will be ignored. Note that both options can be used independently as well.



Supported Notifications

The importer supports the following notification types:

- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users

- Filters
- Targets
- Importer Settings

Zoom Phone

Zoom Phone is a cloud-based telephony solution integrated into the Zoom collaboration ecosystem, offering enterprise-grade voice communication through VoIP. It supports features such as call routing, voicemail, call recording, SMS, and integrations with contact centers and CRM platforms. The Zoom Phone collector focuses on capturing SMS messages, enabling secure ingestion of text communications for archiving, compliance, and oversight.

> **Note:** To use the collector, the Zoom account must be on a Business, Business Plus, or Enterprise plan; Pro plan access is not supported.

Activities Captured

> **Note:** As long as Zoom Phone's SMS/MMS features remain enabled on the user's side, activities will be captured.

- One-on-one SMS/MMS messages
- Group SMS/MMS messages

Captured activities can contain:

- Emojis
- GIFs
- Attachments

  > **Note:** The capture includes data from the past six months, which is the timeframe made available through the API.

Creating a Zoom OAuth App

To create an oAuth application:

1. Sign in to Zoom Marketplace.
2. Select **Develop** > **Build App**.
3. Select **General App** and click **Create**.
4. A Client ID and Client secret will be generated. Use these credentials to configure the collector.
5. On the **Basic Information** page, under **Select how the app is managed**, choose **Admin-managed** and click **Save**.
6. Give an app name, choose **Account-level app**, disable **Publishing to Marketplace** and click **Create**.
7. Copy the Client ID and the Client Secret. They will be used later to configure the Zoom collector.
8. Under **OAuth Information** add the URL of your local environment in the following format: https://<your_instance\>/Configuration/OAuthCallback to the **OAuth Redirect URL**. Ensure that **OAuth Allow lists** field is filled with the same URL as well.

   > **Note:** The **Redirect URI** can be found in the Click information of the collector source configuration.

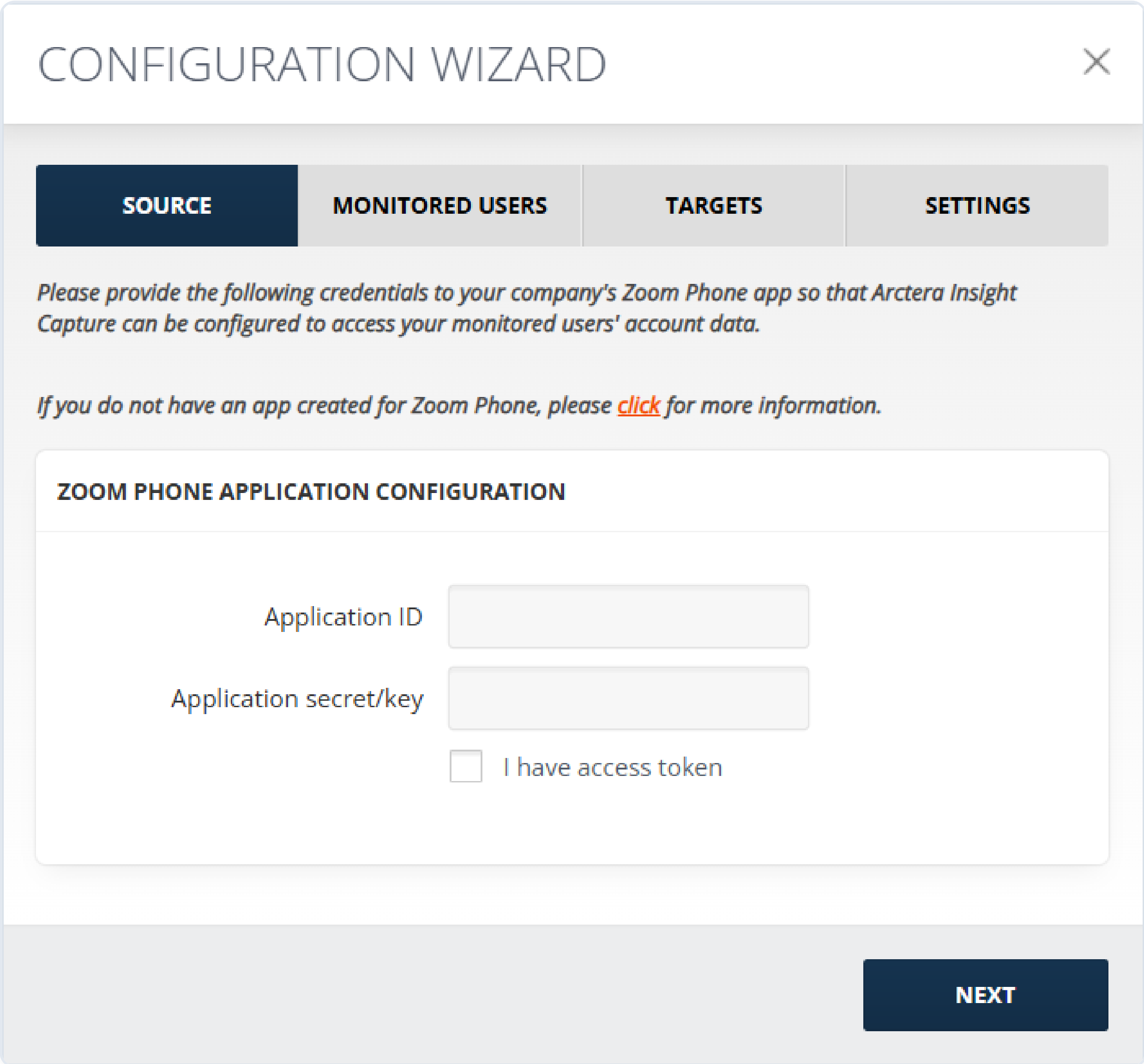
9. Click **Continue**.
10. Go to **Scopes** and click **Add Scopes**.
11. Add the following scopes to the application and click **Done**:
    - phone:read:user:admin
    - phone:read:list_users:admin
    - phone:read:sms_message:admin
    - phone:read:sms_session:admin
    - phone:read:list_sms_sessions:admin
12. Click **Done**.

Source Configuration

To configure the collector:

1. Enter the saved Client ID in the **Application ID** field and the Client Secret in the **Application secret/key** field. Then, click **NEXT** to continue.

2. A pop-up window will open (ensure that the pop-ups are not disabled in the browser window). Click **Allow** to let the app access the specified resources for all users in the organization.



Timestamp Formatting

In addition to the primary stamp, a second timestamp can be enabled with its time zone. From the drop-down menu you can choose the time zone of the timestamp. The format of the timestamp in the output message can also be specified from the six options in the **Date Time Format** drop-down list.

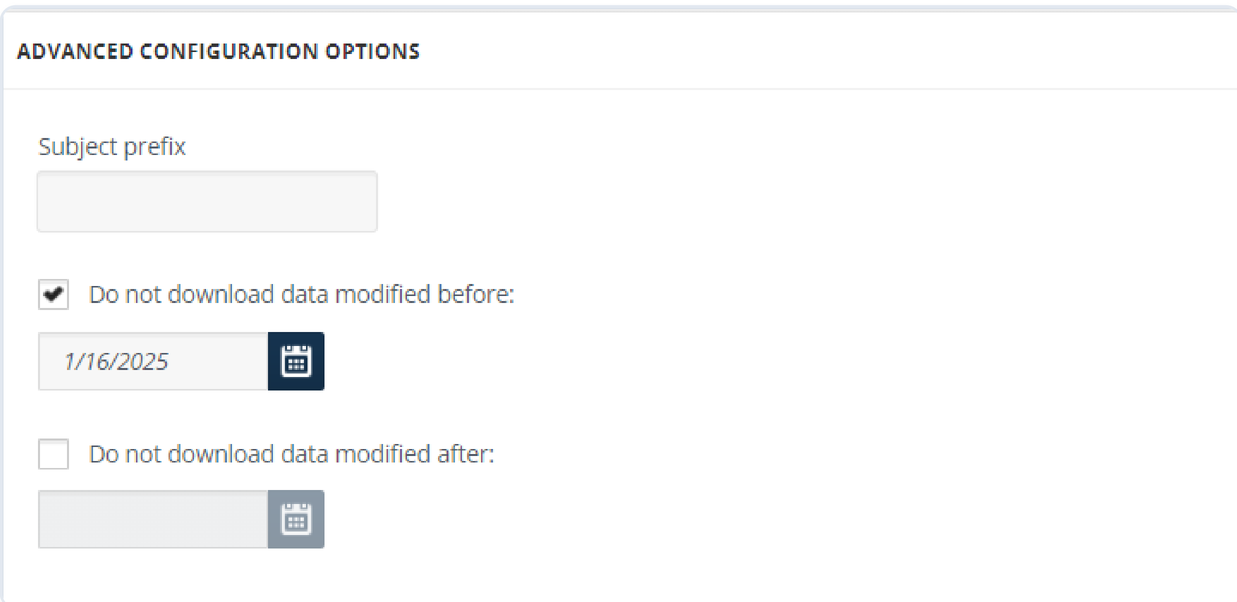
Advanced Configuration Options

To configure advanced options:

1. Specify the **Subject Prefix** in the subject line of imported emails. This is useful for organizing imported data, i.e., when multiple sources share a common target.

> **Note:** Not applicable to the EV Folder target.

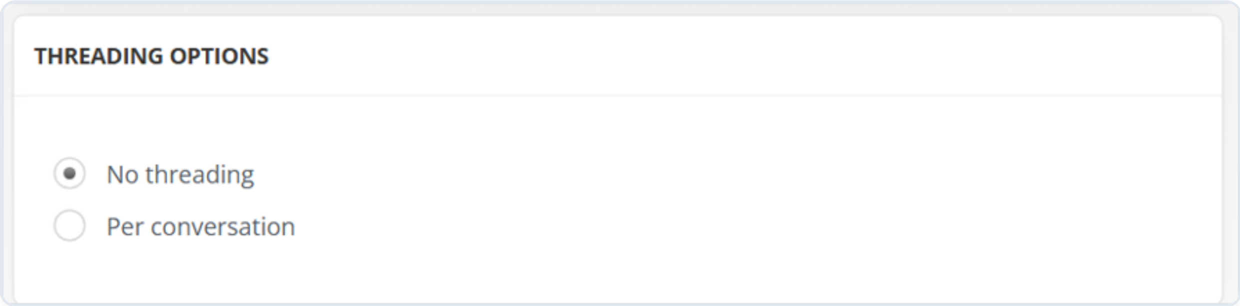
2. Specify **Do not download data modified before** and **Do not download data modified after** to allow cutting off data outside the set date range. If the before date is set to 08/17/2024 and the after date is set to 08/25/2024, only the data between these two dates will be downloaded. Data outside that time frame will be ignored. Note that both options can be used independently as well.



Threading Options

Enable one of the following options:

- **No threading**: If selected, only a single SMS/MMS message will be generated for a message in the group.
- **Per conversation**: If selected, group SMS/MMS messages per conversation will be generated.

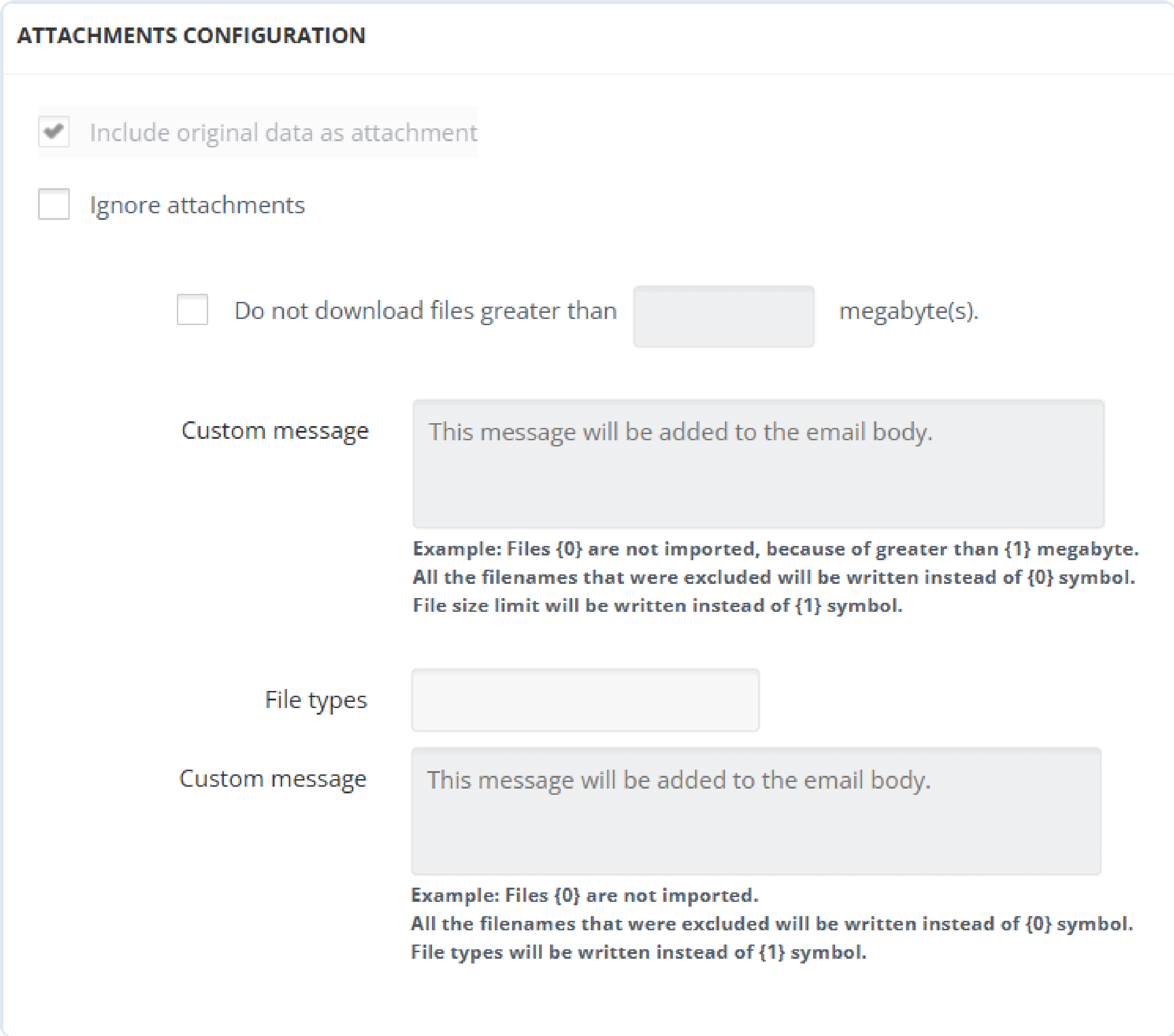


Attachments Configuration

- **Include original data as attachment**: If checked, the message original data is attached to the output file.

> **Note:** Not applicable to the EV Folder target.

- **Ignore attachments**: If checked, all the attachments are excluded from the message enhancing the collector performance. Each message will contain info and the link to the excluded attachment.
- When **Do not download files greater than X megabyte(s)** is selected, the files bigger than the filled-in number of megabytes, are not downloaded. In **Custom Message** field, a text for those excluded files can be specified. E.g.,"Files {0} are not imported, because they are greater than {1) megabytes". {0} is used to add the name of the file and {1} is used to add the number of megabytes specified above.
- In the **File Types** field, the types of files that should not be downloaded can be specified in the following format: e.g., .txt | .xml. The vertical bar is used to separate the file types.



Supported Notifications

The importer supports the following notification types:

- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Import job running threshold exceeded**
- **Importer data deleted**
- **Import job completed with failure**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**

- **Importer metric anomaly detected**
- **Importer metric deviation detected**

For more information, refer to Notification Preferences.

Next Steps

After setting up the collector, follow the links below to continue with the configuration of:

- Monitored Users
- Filters
- Targets
- Importer Settings

MONITORED USERS

This section includes the following topics:

Monitored Users

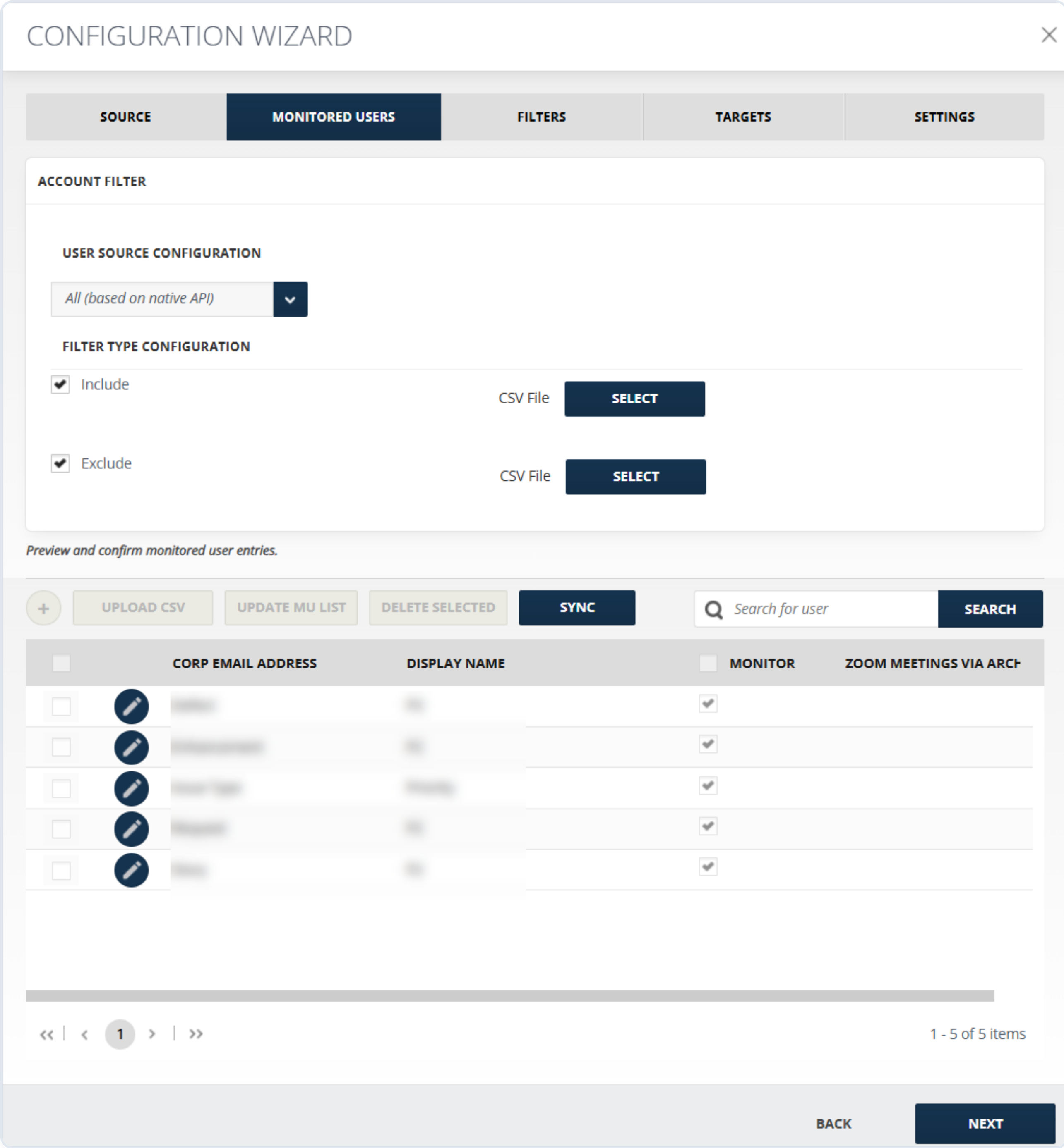
Monitored Users are individuals whose data is collected by Arctera Capture. There are the following User Sources from where Monitored Users can be added to the collector:

User Sources

1. **All (based on native API)**
2. **Manually maintain the list**
3. **Microsoft Entra ID**

All (Based on Native API)

This option automatically imports the users of the collector using its API. This works for sources that are connected to Arctera Capture by the API, like Slack eDiscovery, Zoom Meetings and Microsoft Teams, and so on.



The following options are available:

- **Include** is used for uploading a CSV file with a list of users that have not been retrieved via API but should be included in the Monitored Users.
- **Exclude** is used for uploading a CSV file with the users that should not be monitored.

When the monitored users' source type+ is set to **All (Based on native API)**, the **Sync** button is available for the following collectors:

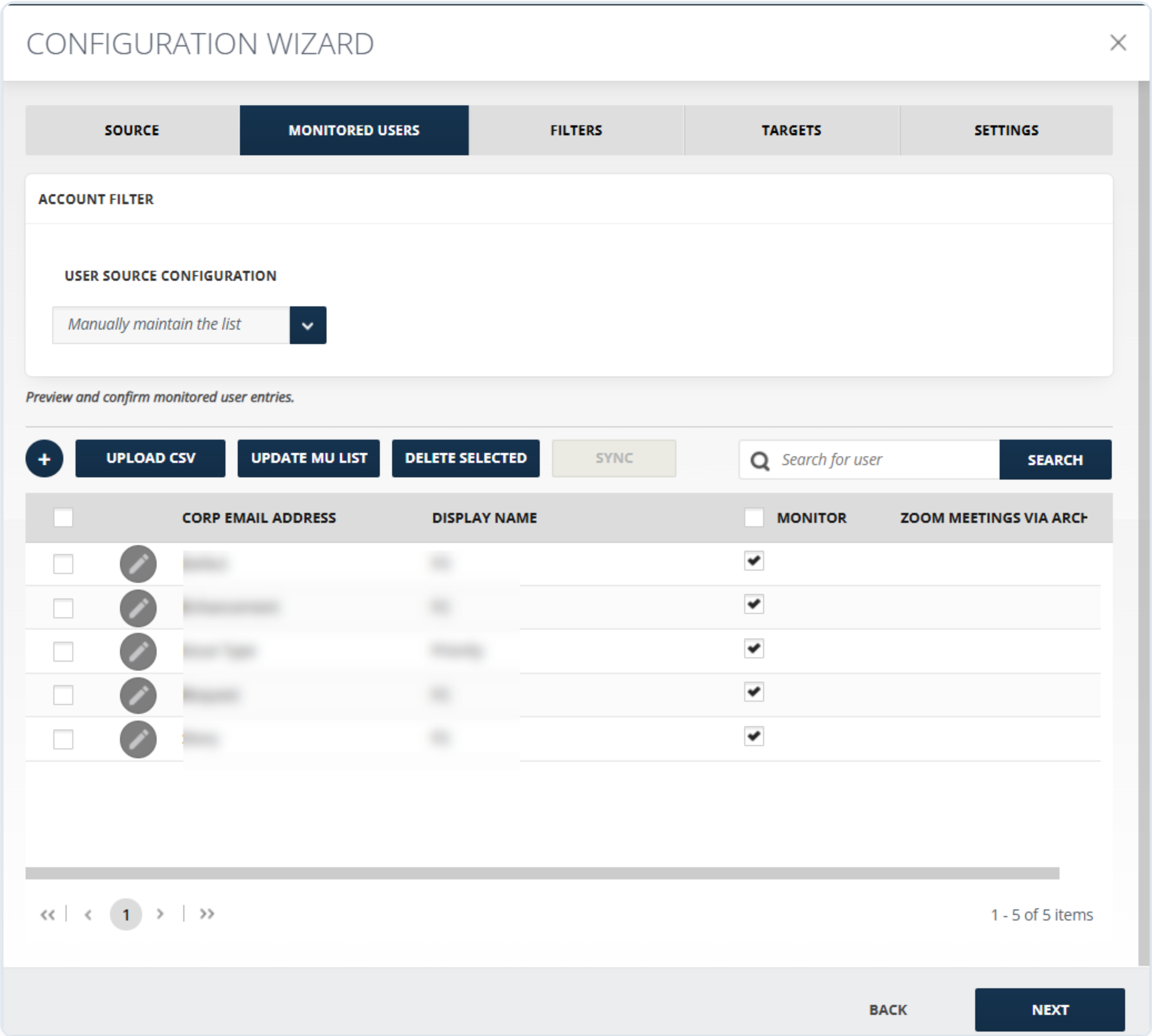
- Viva Engage (Yammer)
- Slack eDiscovery

- Chatter
- Chatter Cipher Cloud
- Microsoft Teams via Export API
- SharePoint
- Workplace from Facebook
- Dropbox Business
- OneDrive for Business
- Exchange Graph API
- Progress ShareFile
- Dropbox Business
- Google Drive
- RingCentral
- ServiceNow
- Zoom Meetings Chats
- Zoom Chat
- Cisco Webex Teams
- Zoom Meetings
- Zoom Meetings via Archiving API
- Box
- Zoom Phone
- ChatGPT
- Copilot
- Lseg Messenger
- Cloud9

> **Note:** To sync monitored users for the some of the collectors in the list (if the collectors already have history saved.), the Delete data action is required.

Manually Maintain the List

This option allows manually managing users.



After selecting **Manually maintain the list** from **User Source Configuration**, the below list of monitored list will become active.

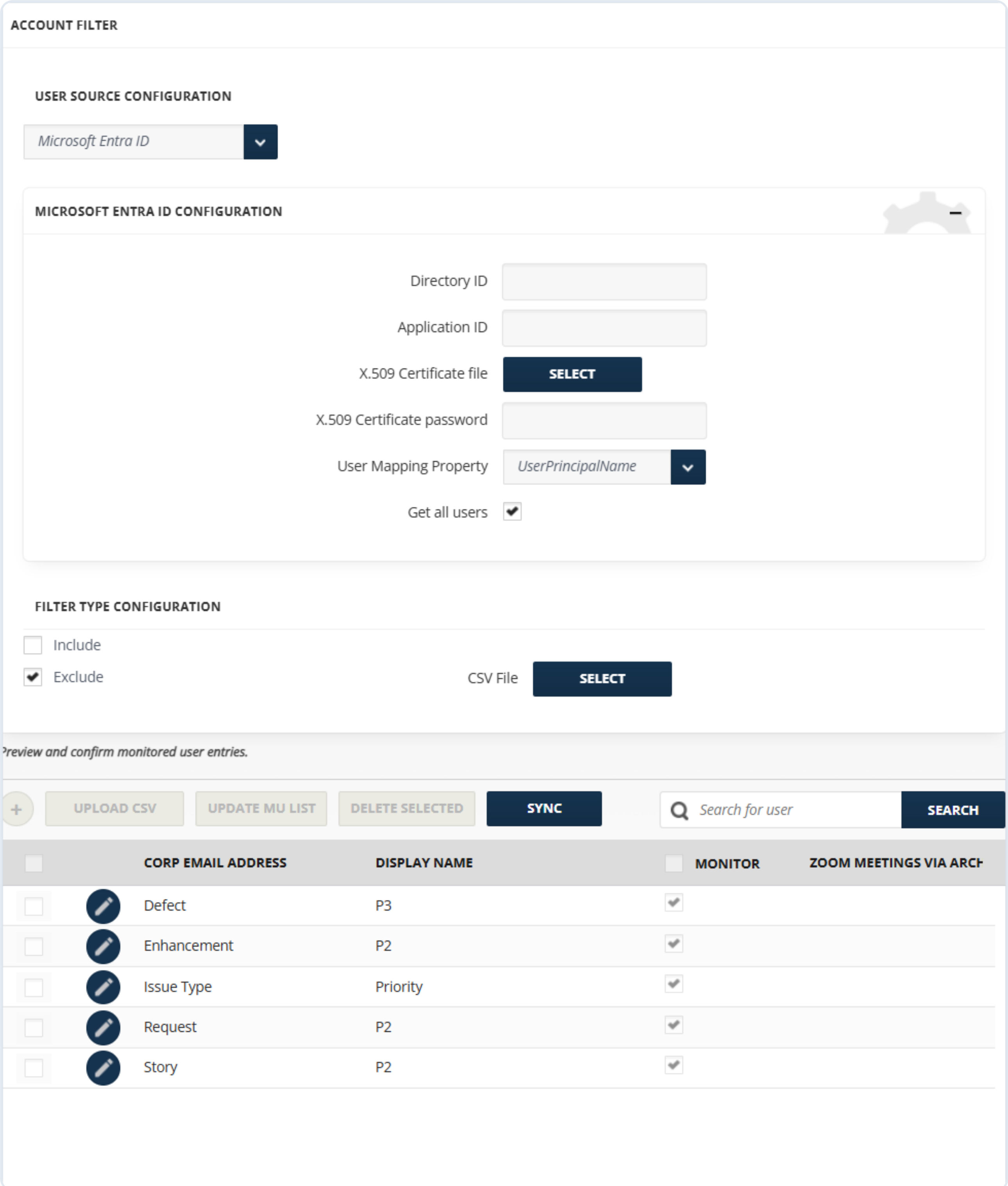
To configure Manually Maintain the List:

1. **+(Add monitored user)** opens a window where you can add details of a user to be monitored and fill in the required information. The same information can later be edited by clicking **Edit Monitored User** as described in point 8.
   - **Corp Email Address** is a required field for the corporate email address of the user.
   - **Display Name** is the name that will be displayed in the Monitored Users list.
   - **Collector Email/ID** is for the email or id of the user's Collector account.
   - If **Monitor this user** checked monitors the user and vice versa.
2. **Upload CSV** allows uploading a Monitored users' list as a CSV.

3. **Update MU list** allows updating the already selected list of monitored users.
4. **Delete Selected** removes selected users from the monitored list.
5. **Sync** allows synchronizing with the current data.
6. **Search** in the list of existing users.
7. Select the user and click **Delete Selected**. This will remove selected Monitored Users' list.
8. Edit the information about an existing user.
9. If **Monitor** is checked, the user is monitored, if not, the user is not monitored.

Microsoft Entra ID

This option automatically imports the users from the Microsoft Entra ID. By expanding **Microsoft Entra ID Configuration**, the following screen opens.



To configure the section:

1. Specify **Application ID** and **Directory ID**. For more details on how to create an app in Microsoft Entra ID and grant the permissions, see Microsoft Entra ID App Creation and Microsoft Entra ID App Permissions accordingly.
2. Activate **Upload file (*.pfx)**, click the **Select** button to upload the certificate and then provide **X.509 Certificate Password**.

3. Select **User Mapping Property** form the drop-down list. Note that **User Principal Name** always exists.

> **Note:** Only for the users that have the respective field.

4. Enable **Get all users** checkbox to process all users in a tenant or provide a group name to process only the specific group.

> **Note:** Both Security and Office 365 group are supported including Nested Groups.

The following Filter Type Configurations are available:

- **Include** is used for uploading a CSV file with a list of users that have not been retrieved via API but should be included in the Monitored Users.
- **Exclude** is used for uploading a CSV file with the users that should not be monitored.

Microsoft Entra ID App Creation

To authenticate via OAuth during the collector configuration, you need to create a Microsoft Entra ID Application.

To create an app:

1. Create an O365 account and open Azure Portal using the same credentials as for O365 (Global Admin).
2. Click **Microsoft Entra ID** at the top of the page and select **App Registration** from the left-side navigation pane.
3. Click the **+New registration** button.
4. Enter a **Name** for the application and click **Register**.
5. Find and make a note your **Application (client) ID** and **Directory (tenant) ID** as this is needed for configuring the collector in Arctera Capture.

Microsoft Entra ID Permissions

For permissions:

1. In the navigation pane to the left, click **API permissions**.
2. Click **Microsoft Graph**, and in the opened pane select **Application permissions**.

3. Add the following permissions:

    - Group.Read.All
    - GroupMember.Read.All
    - User.Read.All

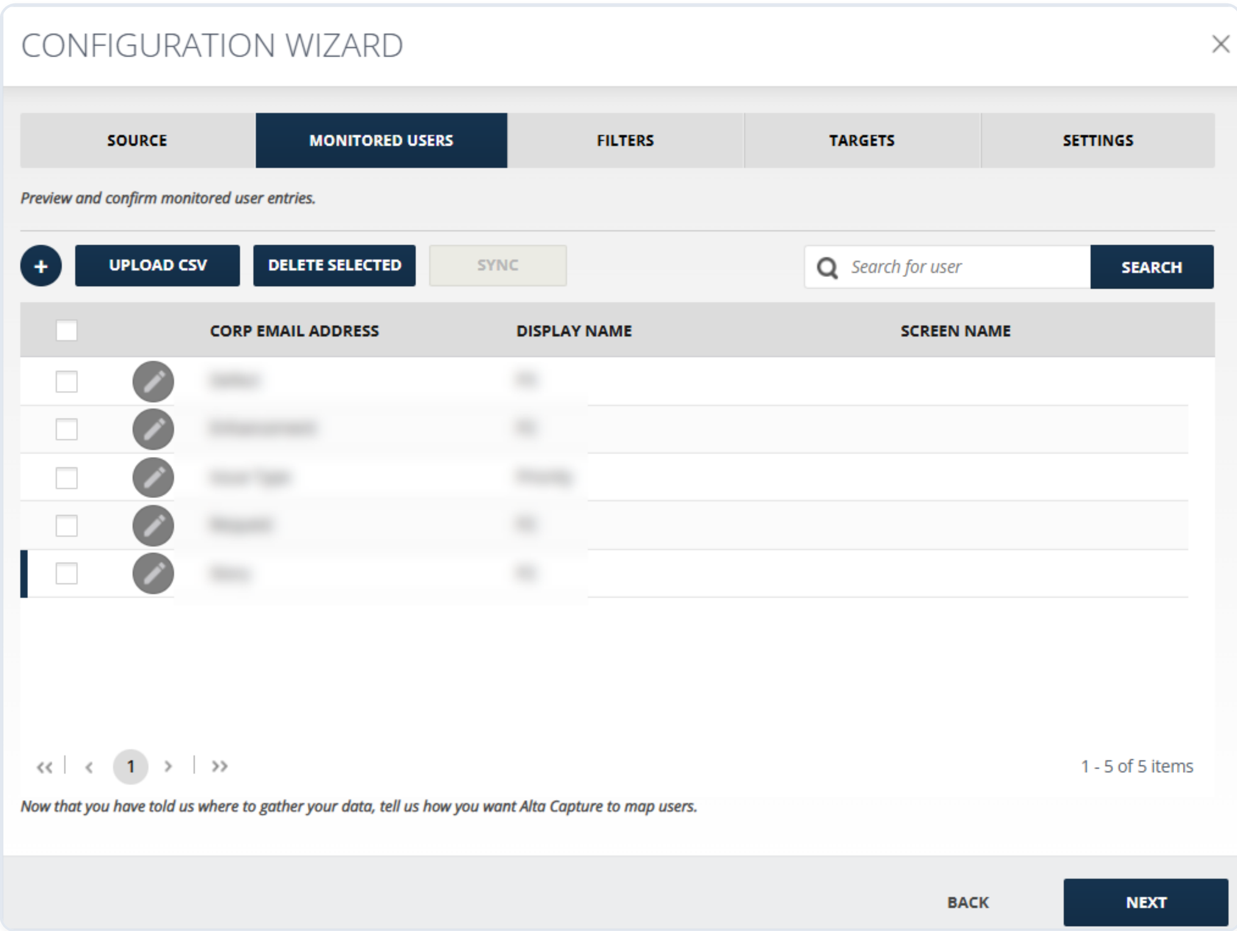
4. Grant all the above-mentioned permissions.

Monitored Users for Twitter

Here the user can add, edit, and delete the listed monitored users or browse among them by searching the users.

To configure the section:

1. When **\+ (Add Monitored User Manually)** is chosen, the following pop-up opens, where **Corporate email address** (email address of the Monitored User), **Display name** and the **Screen name** of the user should be entered.



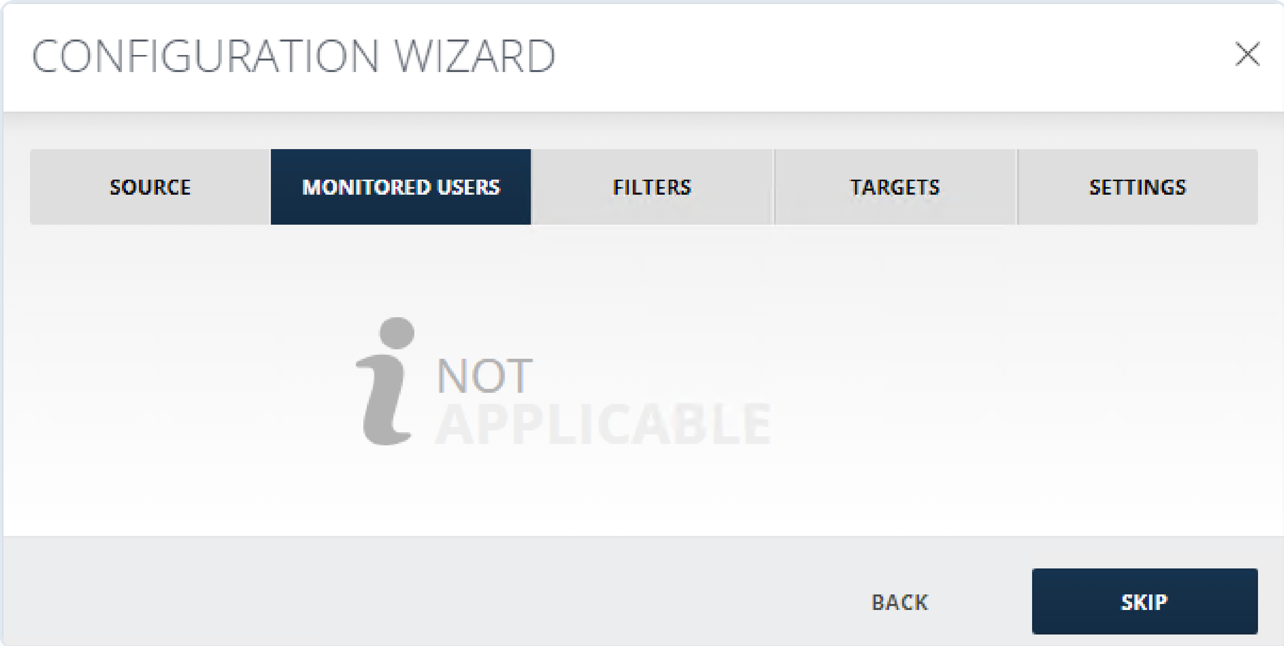
2. Click **Upload CSV** for uploading the Monitored users' list as a CSV.
3. Click **Delete selected** for deleting the below selected list of monitored users.

4. Click **SAVE CHANGES** or **CLOSE**.

Monitored Users (N/A)

Some of the collectors do not have users, therefore instead of seeing the user configuration options under the **Monitored Users** tab, you will see the following screen:

If you click **SKIP**, you will be redirected to the **Filters** tab.



Here is the list of collectors for which Monitored Users is not applicable:

- Amazon S3
- Audio Video
- Bloomberg
- BlackBerry
- CellTrust
- Dubber Speik Recordings
- Dubber Speik SMS
- EML
- FX Connect
- Google Messages
- IceChat
- iMessage

- JSON
- LeapXpert
- Microsoft Teams for Audio and Video
- NTR-X
- Redtail Speak
- Symphony
- Text-Delimited
- LSEG (Refinitiv)
- Yieldbroker
- Pivot
- UBS
- Verba
- Verint
- WhatsApp
- Webpage Capture
- XSLT/XML
- XIP
- YouTube

FILTERS

This section includes the following topics:

Filters

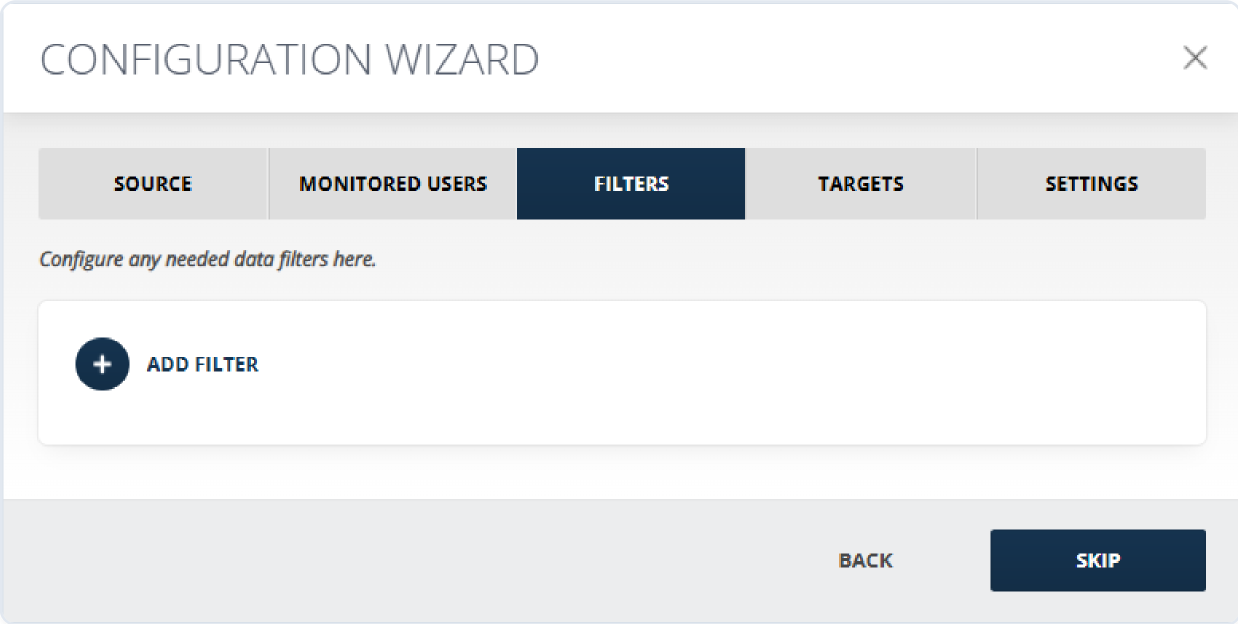
Filters are used to filter or separate data according to content. They can be configured to match specific email addresses, XML tags with specific values, or other information using LDAP queries.

Filters

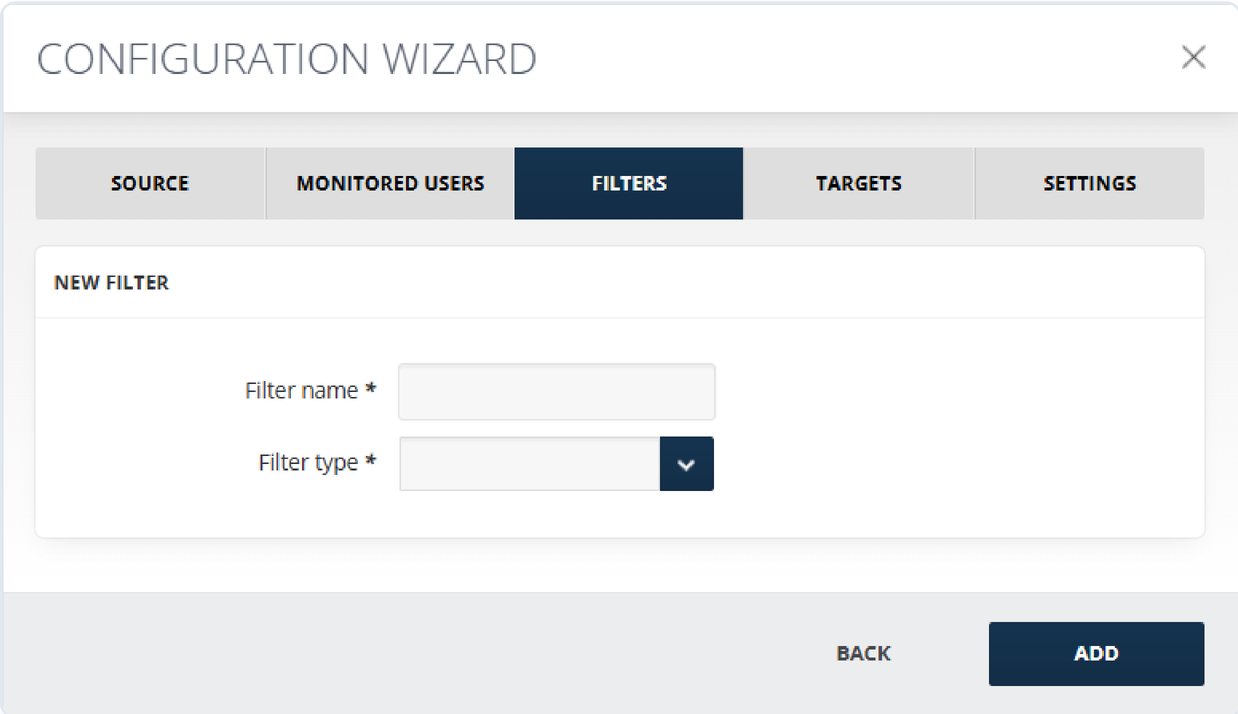
1. **Keyword Filter**
2. **Mail Filter**
3. **XML Filter**
4. **Message Size Filter**
5. **Time Stamp Filter**
6. **Participants Count Filter**

To configure the filters:

1. Click **Add Filter**.

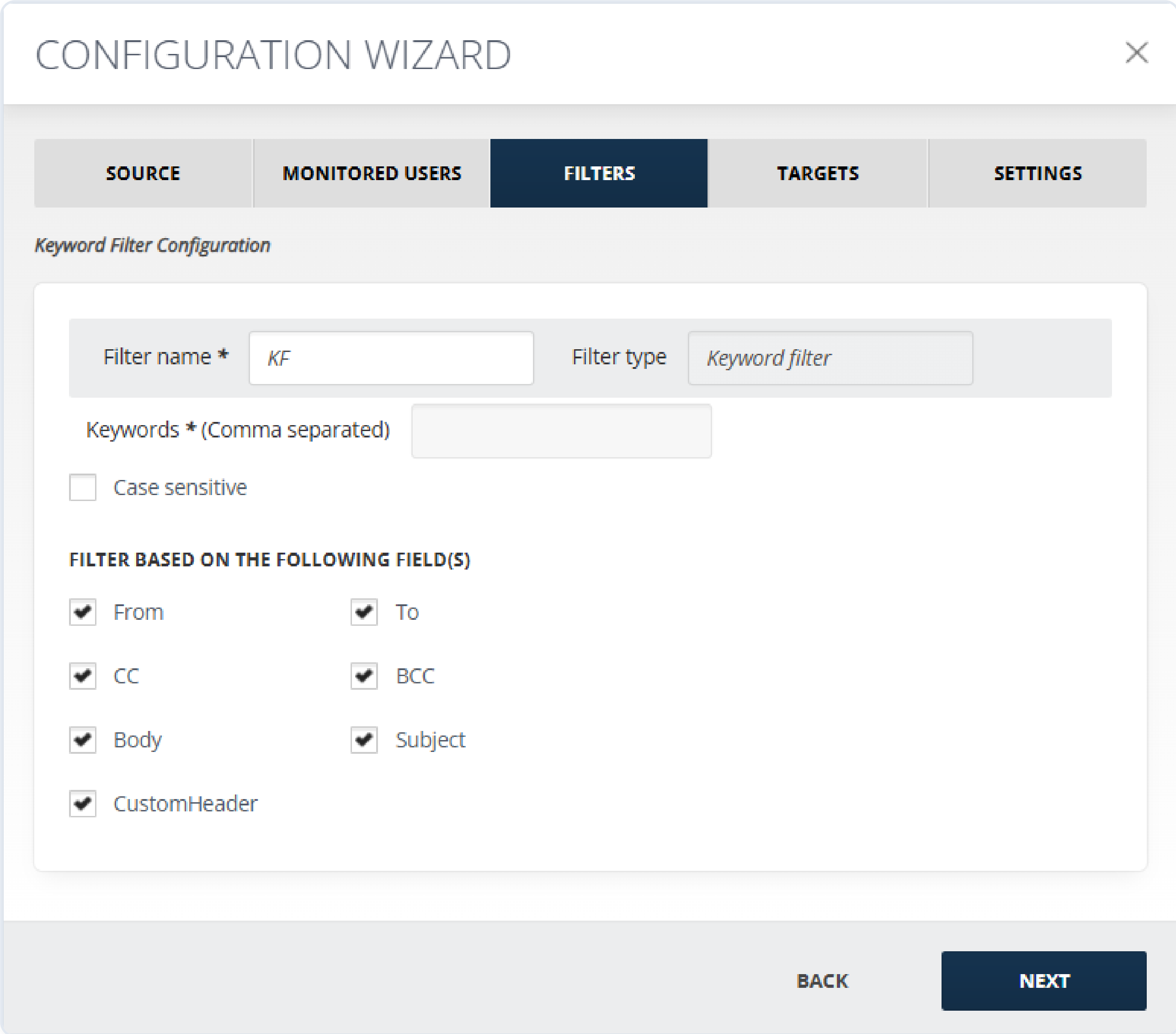


2. Enter **Filter Name** and select **Filter Type**.



Keyword Filter

Keyword filter allows you to retrieve and refine the data by mentioned keywords and collect it in the specified target.



To configure the filter:

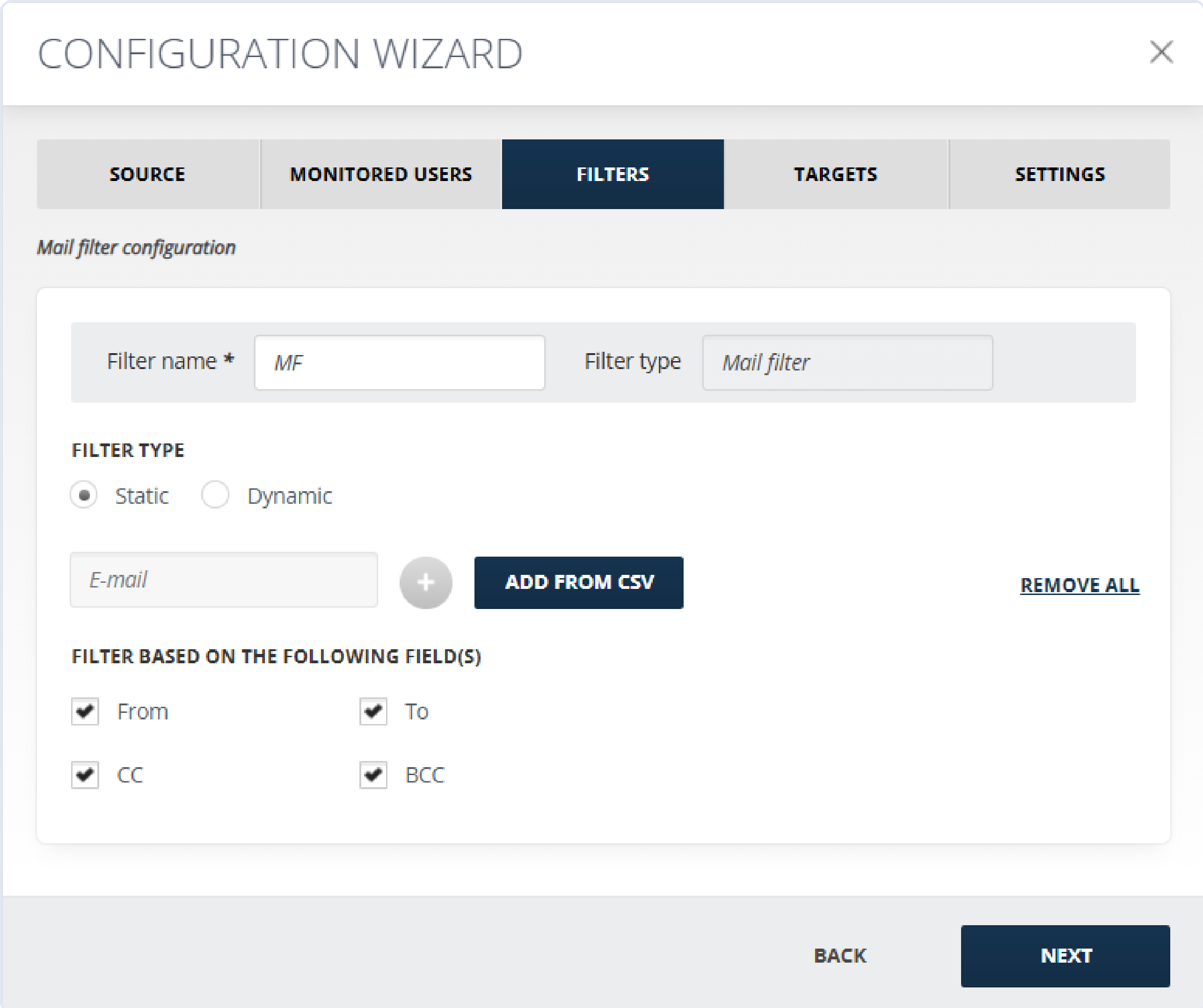
1. In the **Keywords (Comma separated)** field, the keywords, by which the data will be filtered, should be added. The keywords need to be separated by commas for the filtering to work. Keywords are searched for in the body of the message, as well as in its subject.
2. If **Case Sensitive** option is checked, only the words with the same case sensitivity as the input keyword will be filtered. E.g., if you input Direct, it will filter only messages with Direct in their subjects and/or bodies, the results with direct or DIRECT will not be filtered.
3. Filter can be done being based on the following field(s):
   - **From**
   - **CC**
   - **Body**
   - **To**
   - **BCC**

- **Subject**
- **Custom Header**

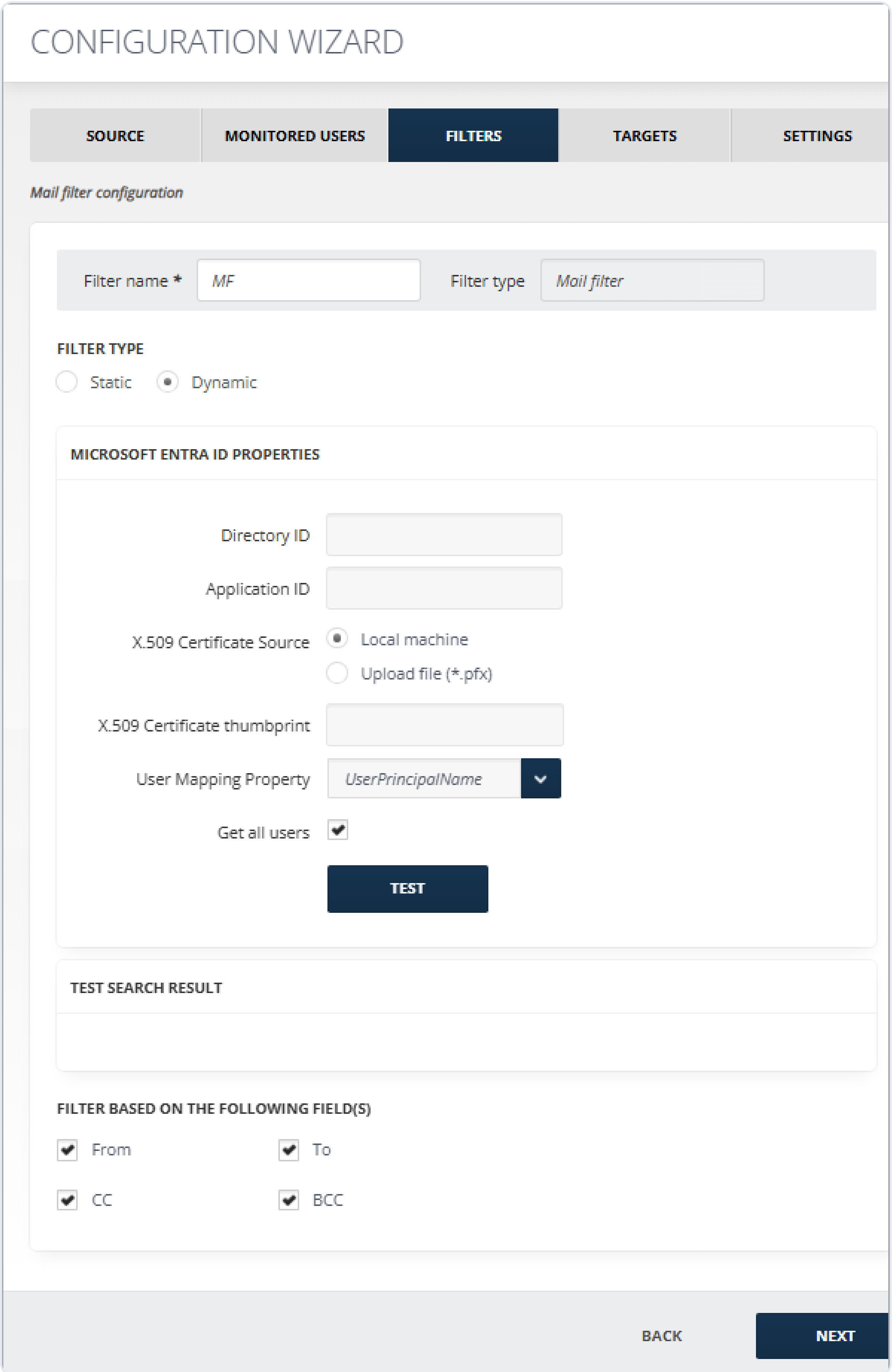
Mail Filter

Using Mail Filter, you can send the imported data to different targets based on the email addresses in the **TO**, **FROM**, **CC**, and **BCC** fields of the imported messages, depending on the fields you specify in the filter settings. The mail filtering in Arctera Capture can be static and dynamic.

Static Filter allows uploading a CSV file with email addresses that will be used for filtering. Click **Add from CSV** to browse for the necessary list for filtering. The CSV file should include only email addresses that should be used for filtering.



Dynamic Filter is used to specify email addresses dynamically from Entra ID. This means, that if any changes are applied to the user list in the server or in the CSV file, the filter settings are refreshed, and values are retrieved newly each time the Importer is run.



To configure the **Microsoft Entra ID** section:

1. Specify **Application ID** and **Directory ID**. For more details on how to create an app in Microsoft Entra and grant the permissions, see Microsoft Entra App Creation and Microsoft Entra App Permissions below.
2. Select the **X.509 Certificate Source** — **Local machine** or **Upload file (*.pfx)** — and enter the **X.509 Certificate thumbprint**.
3. Select **User Mapping Property** form the drop-down list.

> **Note:** User Principal Name always exists.

4. Enable **Get all users** checkbox to get all users.
5. Click **Test** to verify the Microsoft Entra ID connection.

Microsoft Entra ID App Creation

To authenticate via OAuth during the collector configuration, you need to create a Microsoft Entra Application.

To create an app:

1. Create an O365 account and open Azure Portal using the same credentials as for O365 (Global Admin).
2. Click **Microsoft Entra ID** at the top of the page and select **App Registration** from the left-side navigation pane.
3. Click the **+New registration** button.
4. Enter a **Name** for the application and click **Register**.
5. Find and make a note your **Application (client) ID** and **Directory(tenant) ID** as this is needed for configuring the collector in Arctera Capture.
6. In the navigation pane to the left, go to **Certificates & secrets**.
7. Click the **Upload certificate** button.
8. Select a certificate (public key) with one of the following file types: .cer,.pem, .crt, and click **Add**. For more information on how to create a certificate, see Creating a Certificate (Private and Public Keys).

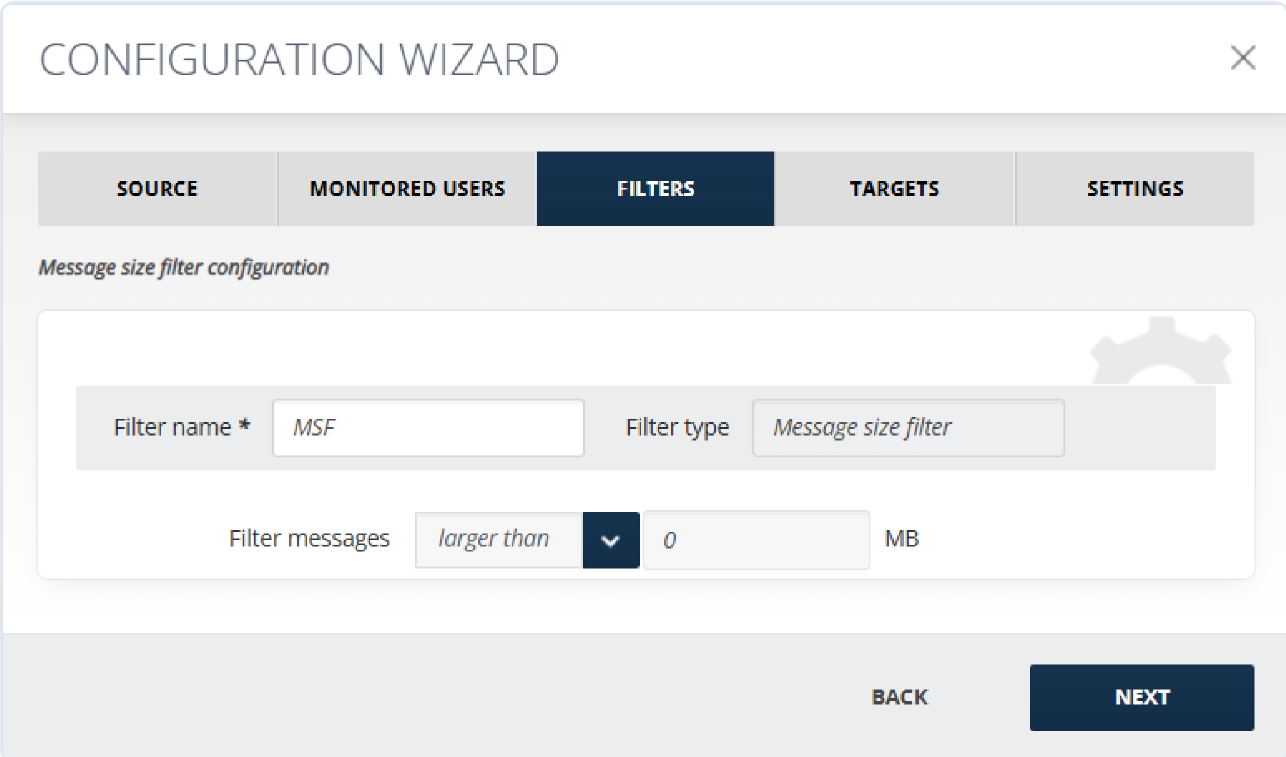
Microsoft Entra ID App Permissions

For permissions:

1. In the navigation pane to the left, click **API permissions**.
2. Click **Microsoft Graph**, and in the opened pane select **Application permissions**.
3. Add the following permissions:
    - Group.Read.All
    - GroupMember.Read.All
    - User.Read.All
4. Click **Yes** to grant consent, or **No** to discard changes.
5. Grant all the above-mentioned permissions.

Message Size Filter

This allows filtering messages to a different target based on their size.

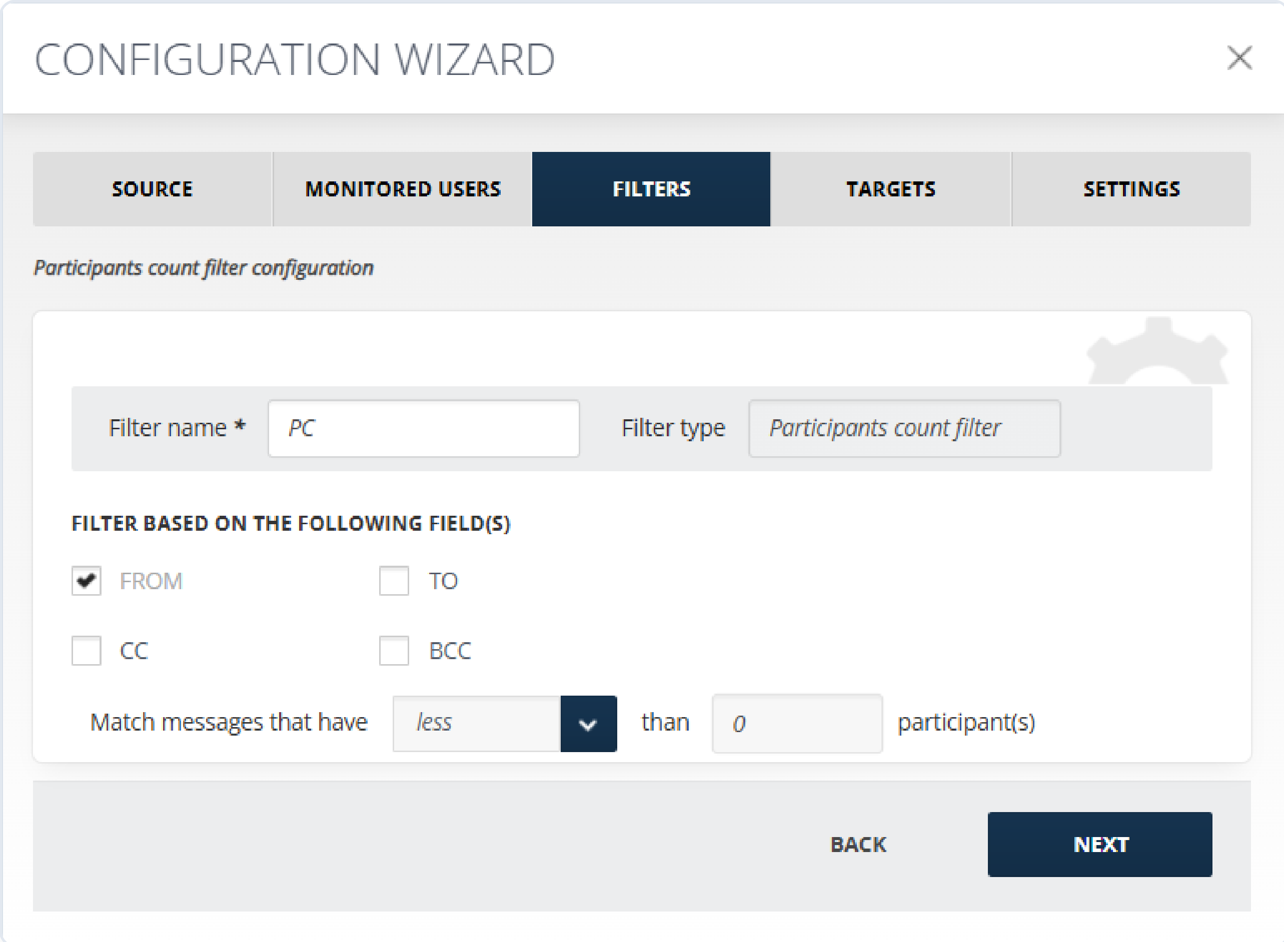


In the **Filter messages larger than/smaller than _ MB**, **larger than** or **smaller than** should be selected and the size of messages should be entered:

- If larger than is selected and the size of messages is entered, the messages that exceed that size will be filtered.
- If smaller than is selected and the size of messages is entered, the messages that are smaller than that size will be filtered.

Participants Count Filter

This allows filtering messages based on the number of participants.

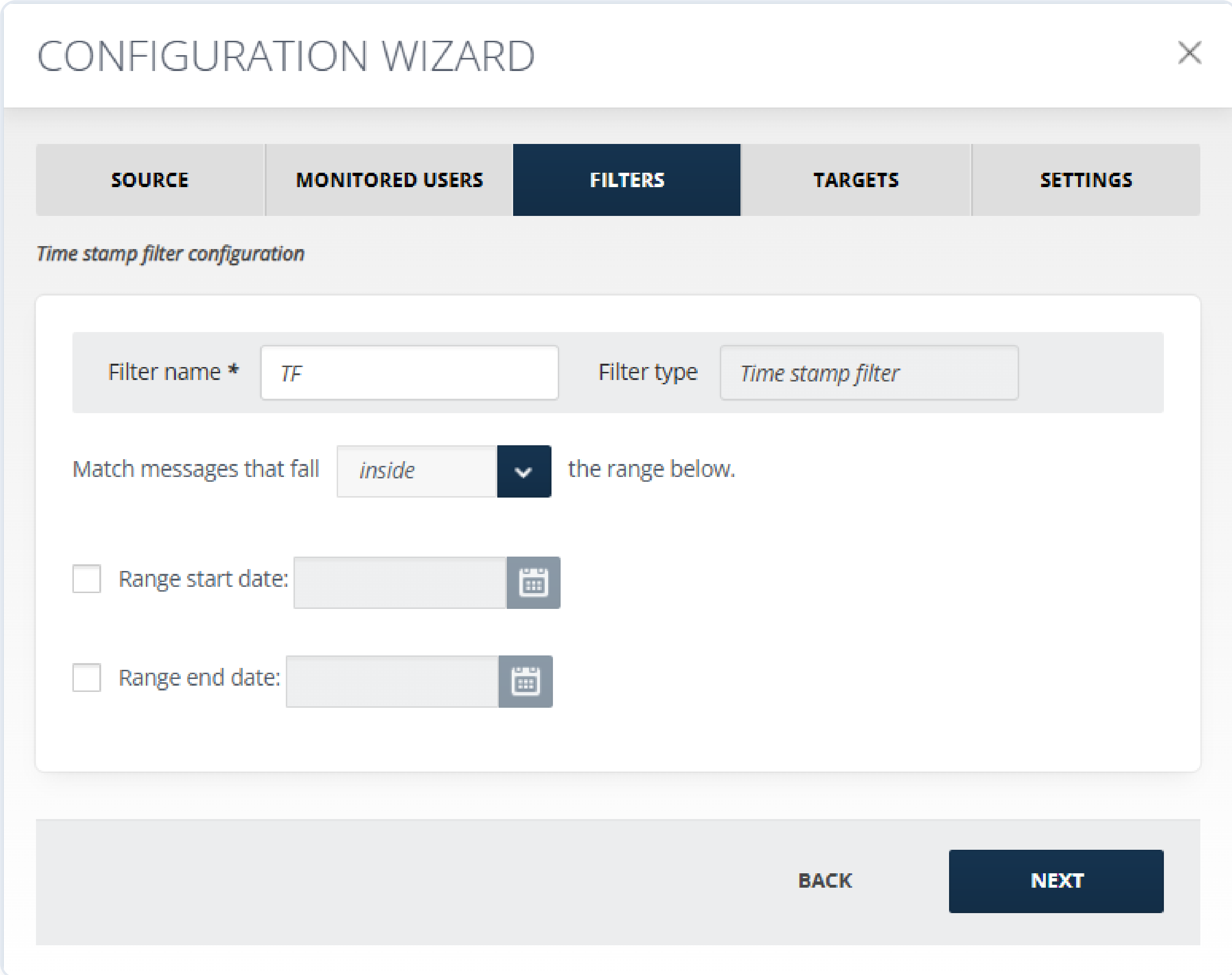


The filter is configured based on the **FROM**, **TO**, **CC**, and **BCC** check boxes. Note that the **FROM** field is always marked as checked and is not editable.

Match messages that have _ than X participant(s) is used to filter messages that have more/ less than the specified quantity of participants by choosing **less** or **more** from the drop-down list and inputting the needed quantity of participants.

Time Stamp Filter

Time Stamp filter allows filtering messages that are already constructed and ready to be sent based on the timestamp.



To configure the filter:

1. The **Match messages that fall inside/outside the range below** drop-down list allows you to include or exclude the specified period depending on the following cases:

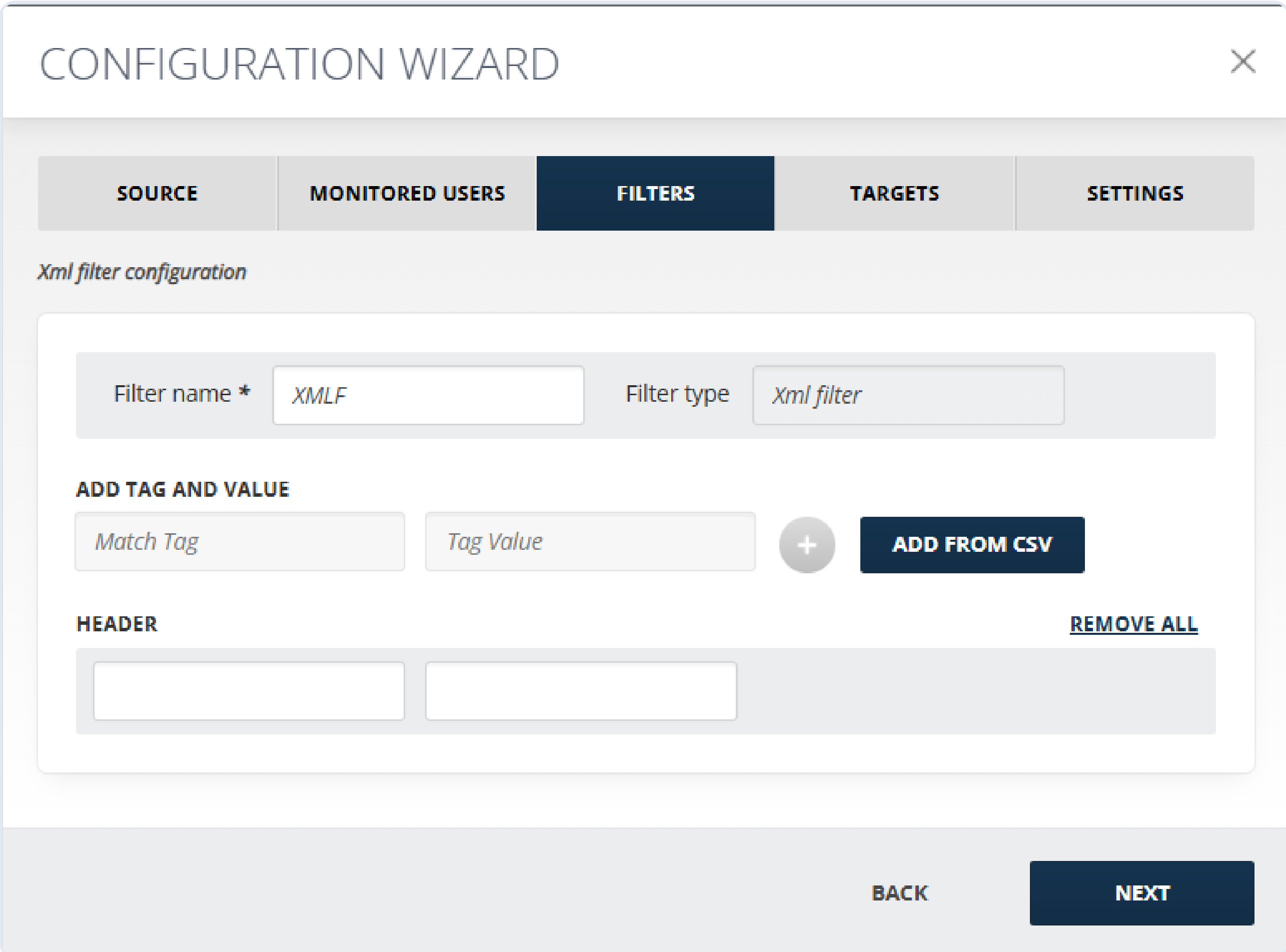
   - In case both the Range start date and the Range end date are specified, and the inside option is selected from the drop-down list, then the content between that cut-off dates and the specified dates included, is filtered.
   - In case both the Range start date and the Range end date are specified, and the outside option is selected from the drop-down list, then the content before and after the specified dates, is filtered.
   - In case only the Range start date is specified, and the inside option is selected from the drop-down list, then the content after that specified start date and the specified start date included, is filtered.
   - In case only the Range start date is specified, and the outside option is selected from the drop-down list, then the content before that specified start date is filtered.

- In case only the Range end date is specified, and the inside option is selected from the drop-down list, then the content before that specified end date and the specified end date included, is filtered.
- In case only the Range end date is specified, and the outside option is selected from the drop-down list, then the content after that specified end date is filtered.

2. The **Range start date** checkbox allows specifying a start date.
3. The **Range end date** checkbox allows specifying an end date.

XML Filter

XML filter allows filtering through XML source data with tags and their specific values.



To configure the filter:

1. In the **Add Tag and Value** field, an XML tag and corresponding to it value should be added. They will be searched for in the body of the message from XML Source and when matched, will be sent to the assigned target. You can add more than one XML tag and value. After adding one, click the activated **Plus** button.

2. If you do not want to input each tag and its value manually, upload a CSV file that includes tags and their values. Click **Add from CSV**, browse for the necessary file and upload it.
3. If the added tag and value are matched with a message, that message is sent to the corresponding target. In the **Header** section you can add a specific text to be added in the message header for facilitating future filtering. For example, you can add tags that match by country and if the tag is matched, the header can be "MessageOriginCountry - USA".

   > **Note:** Only one header can be added to a single filter, so for each country, in this case, a separate filter needs to be created.

This filter works only with XML sources:

- Bloomberg
- CellTrust
- Symphony
- XSLT/XML
- IceChat
- Pivot
- UBS

TARGETS

This section includes the following topics:

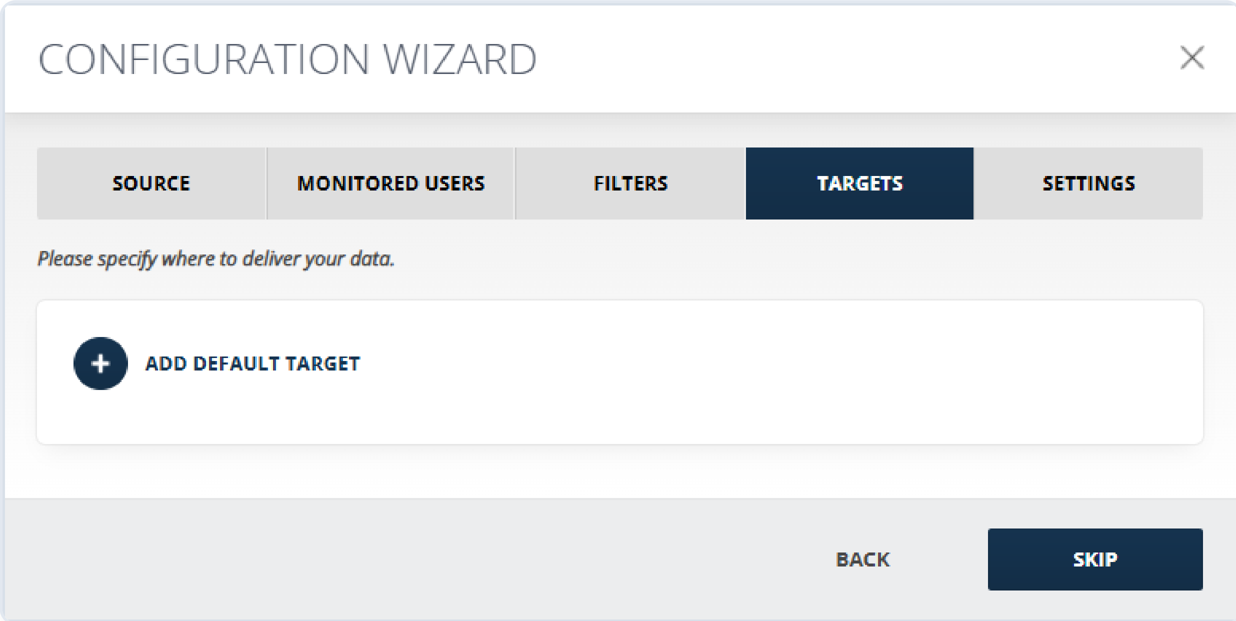
Targets

Here you can specify where you want to deliver your data.

> **Note:** Note that files and attachments, greater than 2 GB are not being processed.

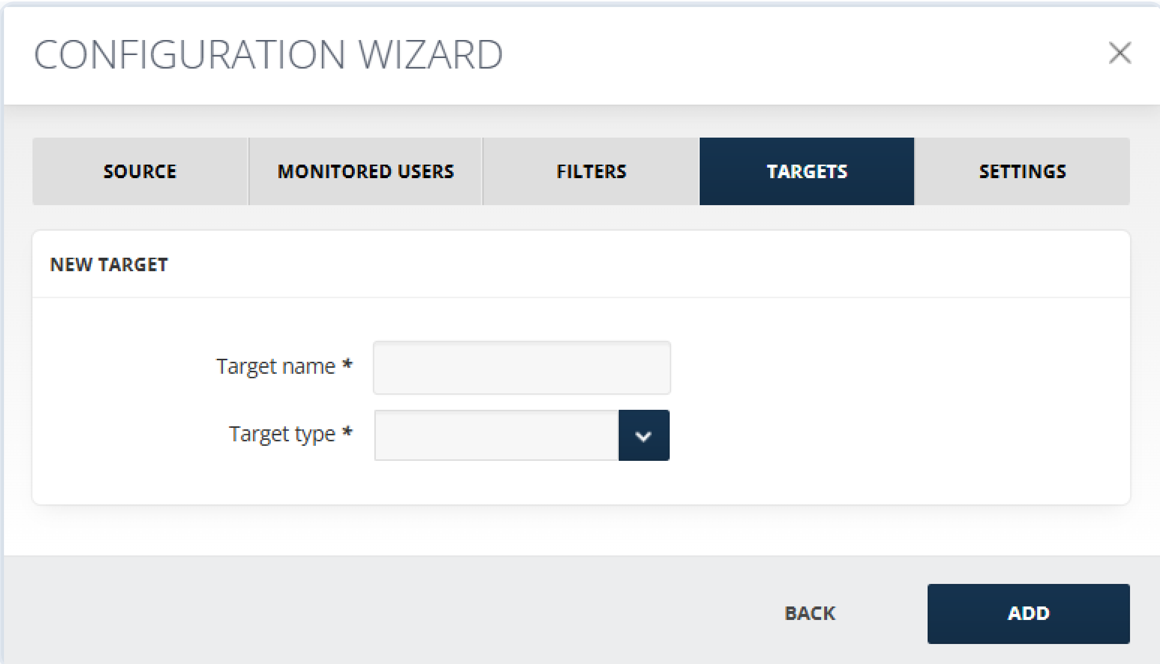
> To set up targets:

1. Click **Add Default Target**. You will be redirected to the **Targets** screen.



2. Fill in the **Target Name** and select **Target Type** from the drop-down menu.

> **Note:** These are mandatory fields.

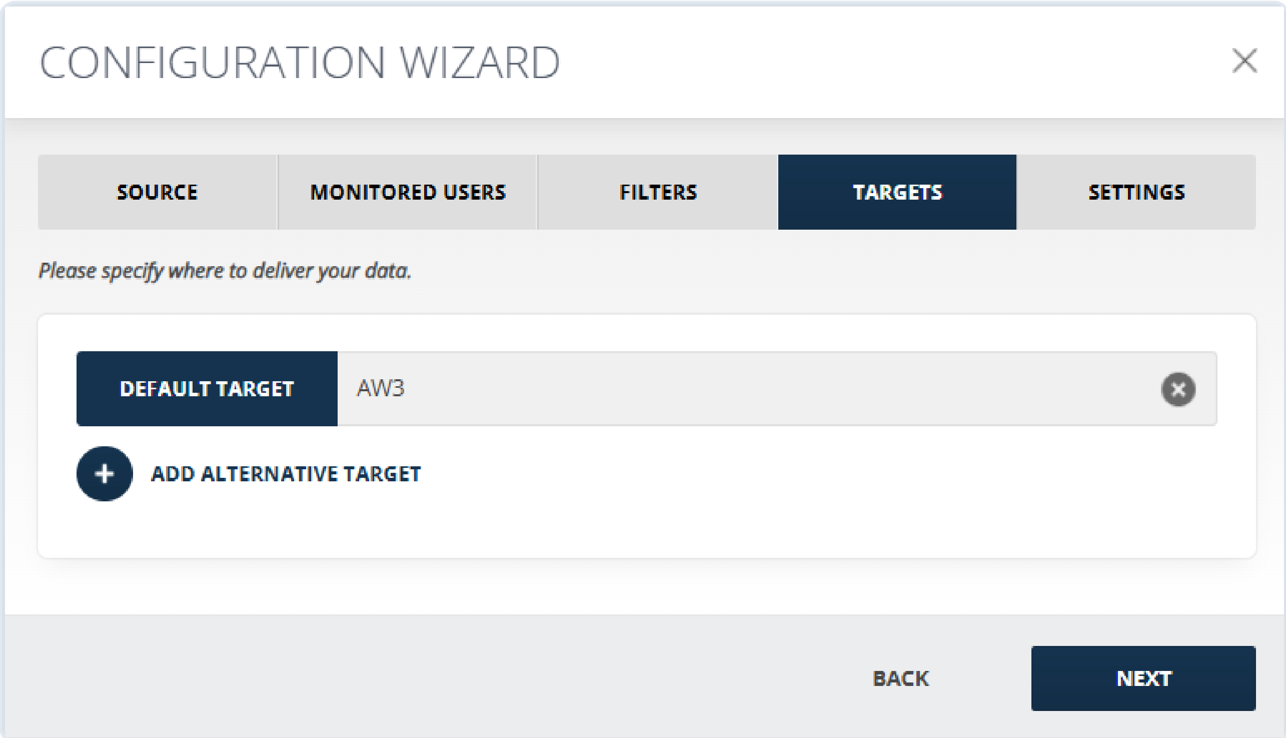


3. When you have selected the exact target, you wish to configure click **Next**. There are the following types of targets:

   - **Amazon S3** - Delivers data directly to the Amazon S3 storage.
   - **Azure Blob target** - Delivers data directly to the Azure Blob target.
   - **Direct SMTP target** - Delivers data to an SMTP server address directly from the server.
   - **EWS Server target** - Delivers data to an Exchange Web Services server.

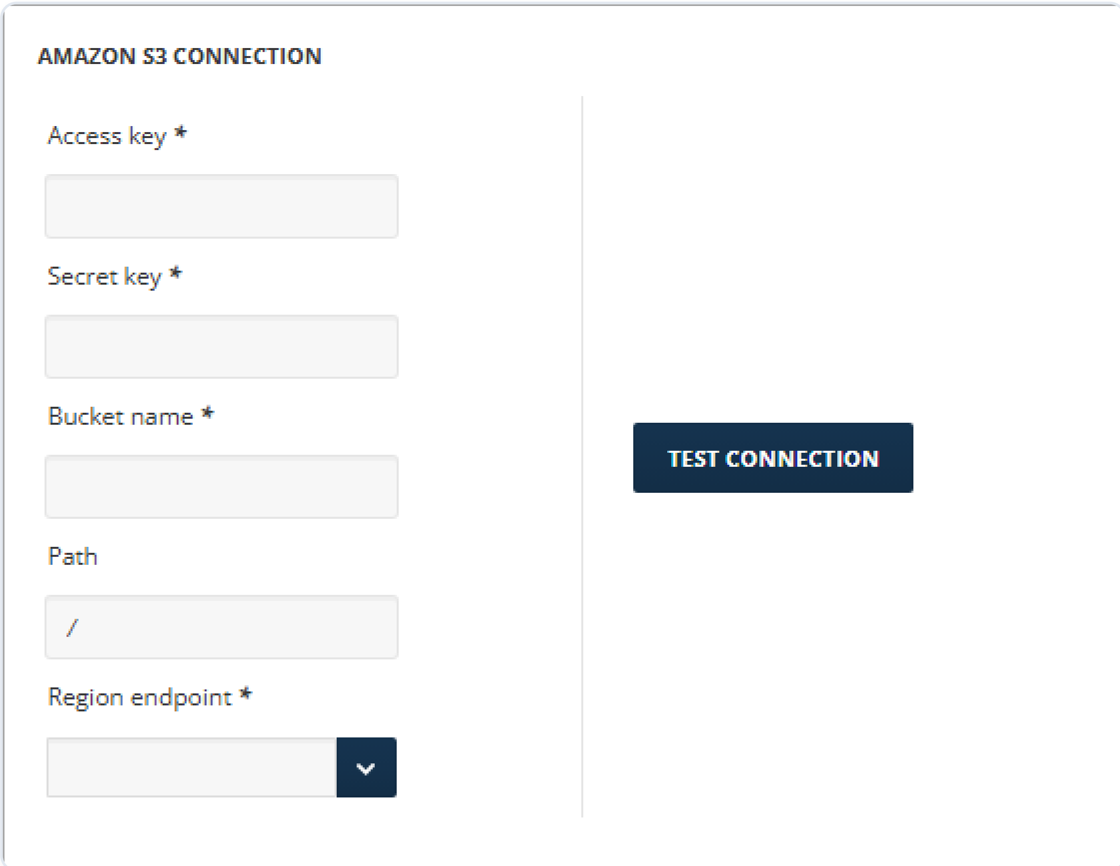
- **Failed target** - Lists all imports as failed delivery attempts.
- **Google Vault target** - Delivers data to Google Vault.
- **Ignored target**- Ignored target is used to mark all items sent to it as Ignored.
- **SFTP target**- Allows delivering data to an FTP/SFTP server address.
- **SMTP target** - Delivers data to an SMTP server address using a relay.

In addition to one default target, you can also have Alternative Targets. To make an Alternative target as the Default one next to the close button, you will see the **Default** button. Click it and your Alternative Target will become your default and it will be listed under the Alternative Targets.



Amazon S3 Target

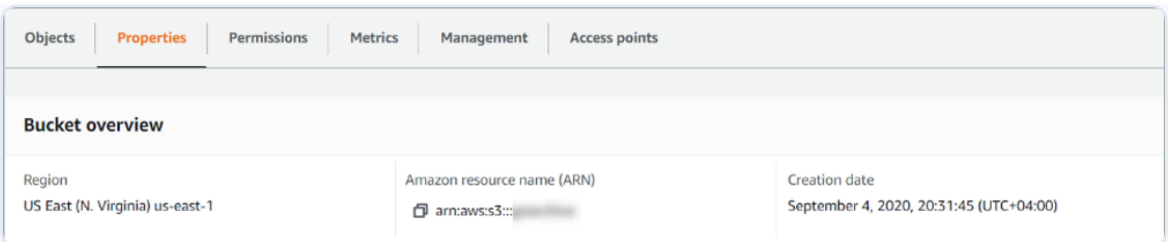
To deliver data collected from different sources to the Amazon S3 storage, the storage should be configured accordingly.



The following information is required:

- **Access Key** - enter the access key which you can find in the Users > Security Credentials of your Amazon S3 account.
- **Secret Key** - enter the secret key acquired while setting up the Security Credentials. Save it in a secure place as that secret key is provided only once.
- **Bucket Name** - enter the archive bucket name.
- **Path** - enter the path within the bucket where the data is delivered. The default is the bucket root (`/`).
- **Region Endpoint** - enter the Region Endpoint which you can find in the Bucket Overview > Properties of your Amazon S3 bucket.

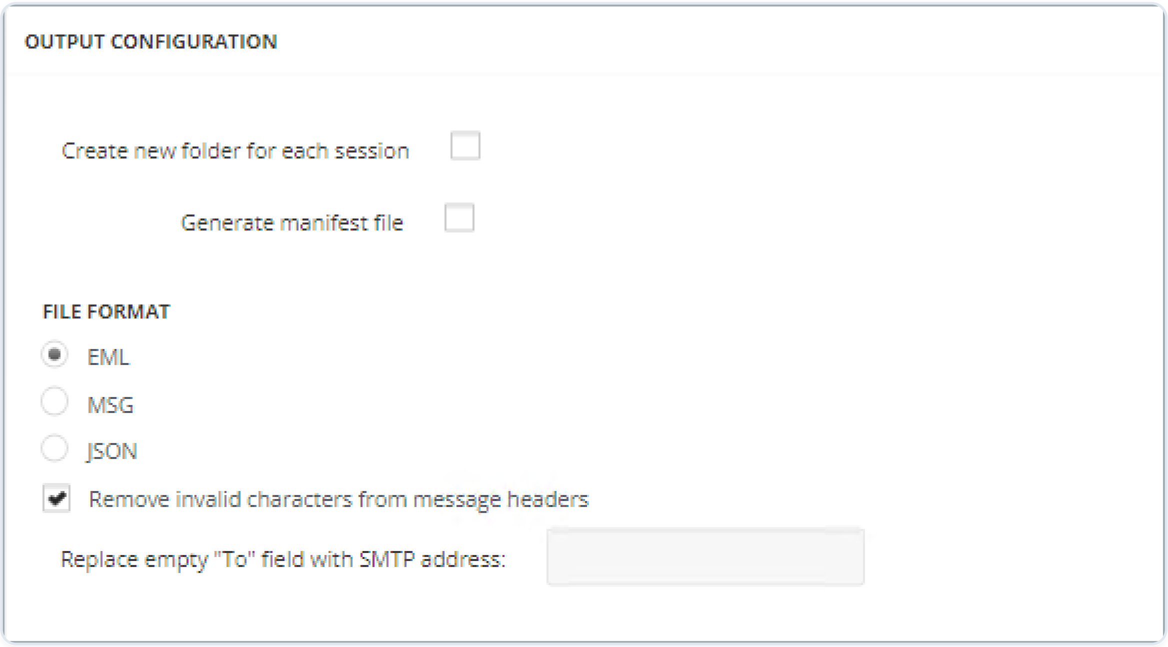
> **Note:** IfRegion Endpointis not set correctly, the archive content will not be delivered.



Output Configuration

To configure the output:

1. Enabled **Create New Folder Per Session** to create a separate folder for each time the Importer is run, named after the date and time of the run.



2. Enable **Generate manifest file** checkbox, to have a generated a CSV file that will contain the list of generated message files.
3. Specify the format of the exported message: EML, MSG or JSON.

You can easily convert your .msg file into an .eml file as there could be possibilities where you want to view an .msg file but you do not have MS Outlook to open it. The .msg files are client dependent because they are a proprietary message for Outlook, whereas .eml is a text - based file representing a message. Therefore, having single messages stored in .EML rather than an .msg file proves more beneficial for the users, due to its flexibility.

1. The **Remove invalid characters from message headers** checkbox is activated by default.
2. Enter the SMTP address in case you want to Replace the empty "To" with an SMTP address in the corresponding field.

The JSON file format is available in all the collectors' folder target but currently is supported only for the below listed collectors. For other collectors an error will be thrown.

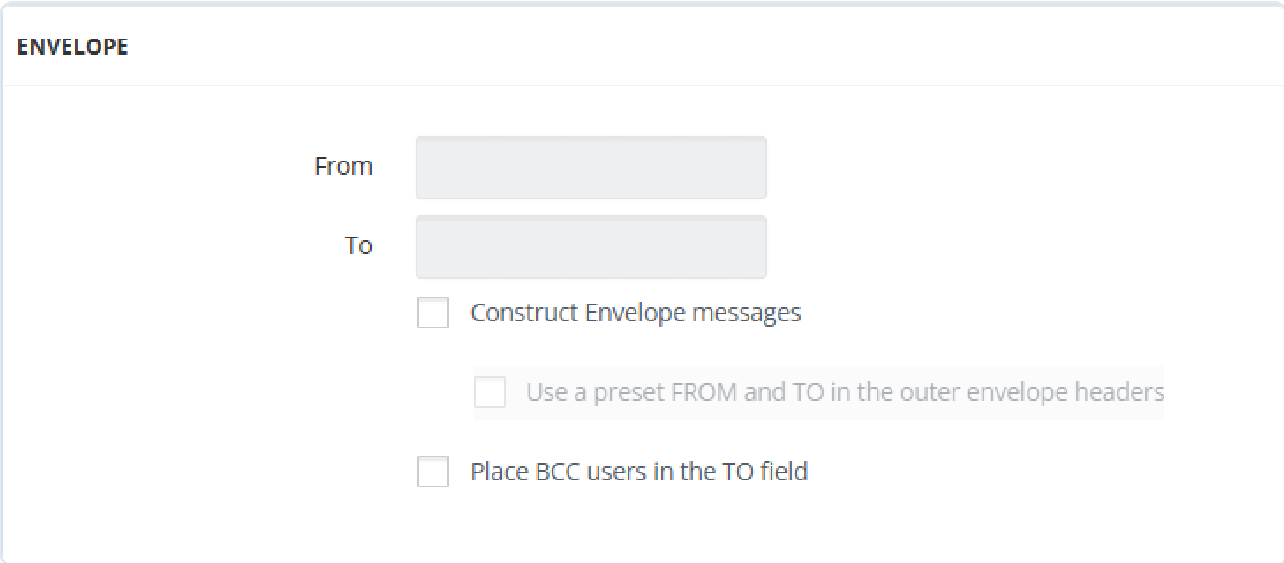
- Amazon S3
- Audio Video
- Box

- ChatGPT
- Chatter / Chatter Cipher Cloud
- Cloud9
- Copilot
- Dropbox Business
- Dubber Speik Recordings
- Dubber Speik SMS
- FX Connect
- iMessage
- JSON
- LSEG (Refinitiv)
- LSEG Messenger
- Microsoft Teams for Audio and Video
- Microsoft Teams via Export API
- NTR-X
- OneDrive for Business
- Pivot
- Redtail Speak
- RingCentral
- ServiceNow
- Slack eDiscovery
- Symphony
- Text- Delimited (newly created ones, not upgraded)
- Verba
- Verint
- X (Twitter)
- Web Page Capture
- WhatsApp
- Workplace from Facebook
- XIP

- XSLT/XML (newly created ones, not upgraded)
- Yieldbroker
- YouTube
- Zoom Phone
- Zoom Chat
- Zoom Meetings
- Zoom Meetings Chats
- Zoom Meetings via Archiving API

Envelope

The following options are available:



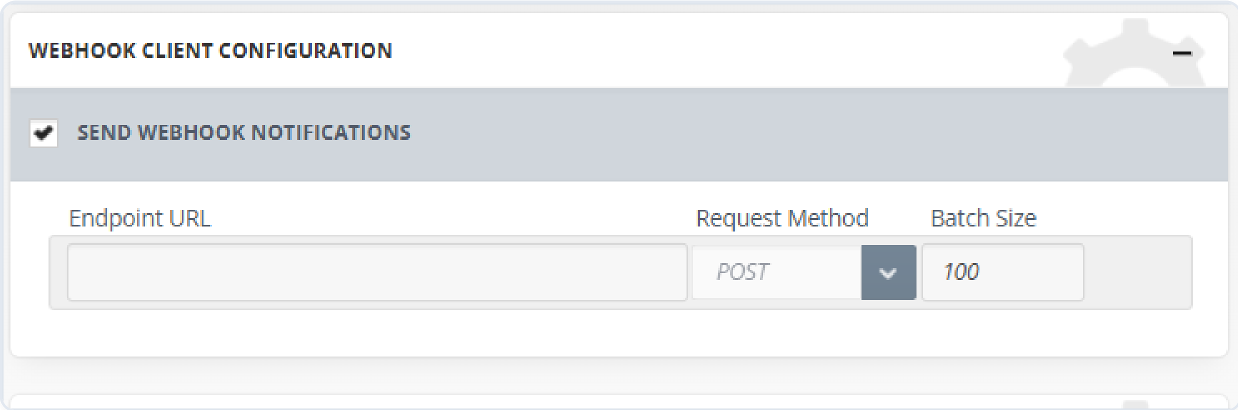
- The **Construct envelope messages** option when enabled envelopes the original output message in a new message with the From and To email addresses set in the corresponding fields.
- The **Use a preset FROM and TO in the outer envelope headers** option adds the From and To email addresses of the original output message in the header of the envelope.
- The **Place BCC users in the TO field** option adds the email addresses from the BCC field of the original output message to the TO field.

> **Note:** The service account that runs the service should have read/write permission for the specified folder.

Webhook Client Configuration

To configure the section:

1. Enable **Send Webhook Notifications**.



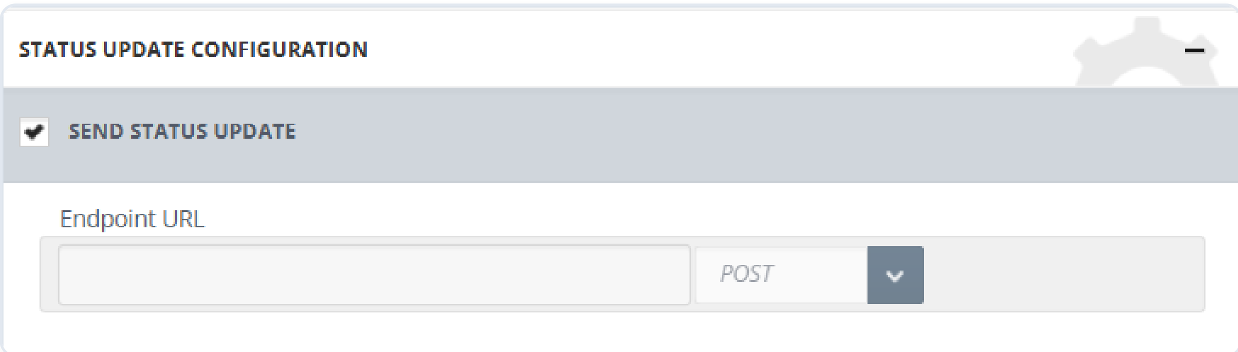
2. Specify **Endpoint URL**.
3. Specify **Batch Size**. The default size is 100.

> **Note:** The default value for **Request Method** is POST.

Status Update Configuration

To configure the section:

1. Enable **Send Status Update**.
2. Specify **Endpoint URL**.



> **Note:** The default value for **Request Method** is POST.

Azure Blob Target

To deliver data collected from different sources to the Azure Blob storage, Azure storage should be configured accordingly. For more information on how to configure Azure Storage, see the section called “Configuring Azure Storage”.

Using custom domains is not supported, the URL must point to one of the well-known Azure Storage endpoints listed below:

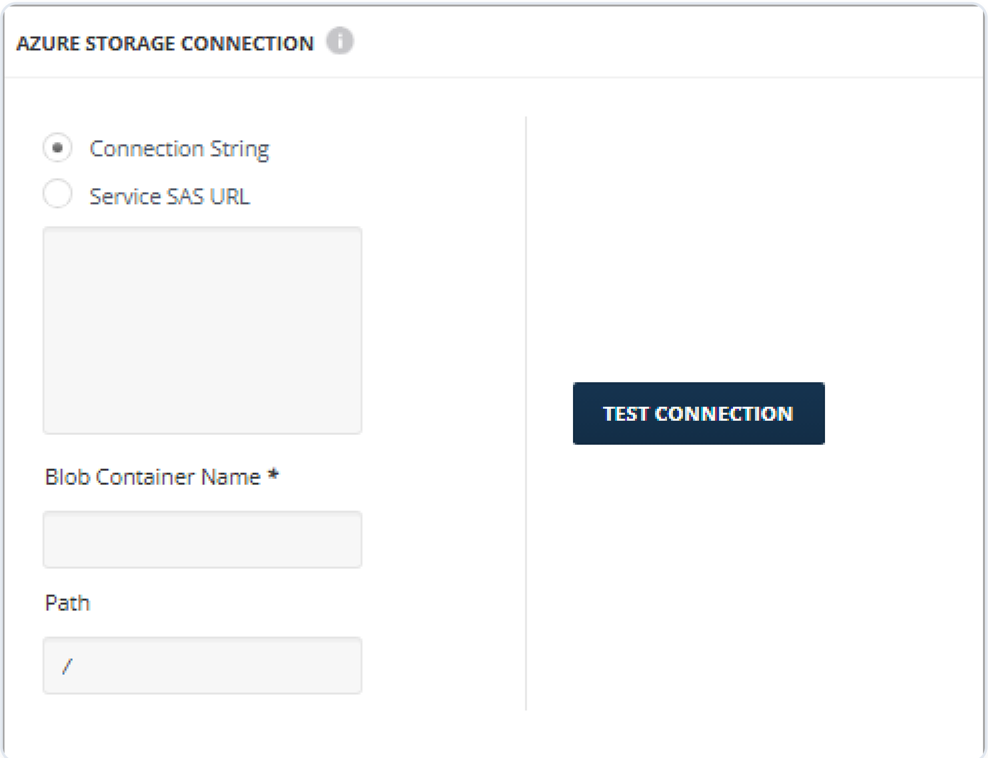
- blob.core.windows.net
- blob.core.usgovcloudapi.net
- blob.core.chinacloudapi.cn

To configure Azure Storage:

1. Enable **Connection String** and enter the Connection String copied in step 9.

Or,

1. Enable **Service SAS URL** and enter the Service SAS URL copied in step 9.
2. Enter **Blob Container Name** from step 10.
3. Enter the **Path** where the data is delivered within the Blob container.
4. Click **Test Connection** to verify that the configured Azure Storage connection is valid.



Configuring Azure Storage

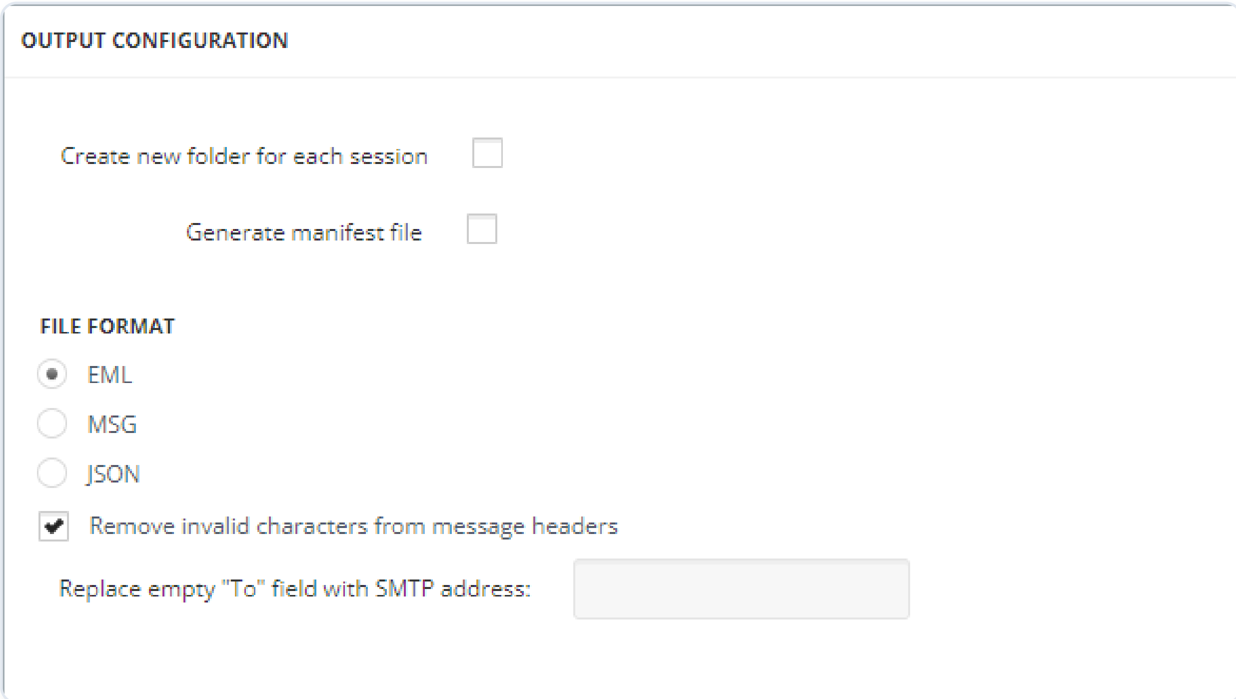
For Azure Blob storage:

1. Login to your Azure portal account.
2. Navigate to **Storage Accounts**.
3. Click the account Name.
4. On the left side navigation pane, navigate to **Shared Access Signature**.
5. For **Allowed services**, enable **Blob**.
6. For **Allowed resource types**, enable **Service**, **Container**, and **Object**.
7. For **Allowed permissions**, enable:
    - **Read**
    - **Write**
    - **Add**
    - **Create List**
8. Specify the Expiration start and end date and click **Generate SAS and connection string**.
9. Copy **Connection string** or **Blob service URL** for Connection configuration.
10. On the left side navigation pane, select **Containers** and click the name of the container you want and save the name for later use.

Output Folder Configuration

To configure the section:

1. If **Create New Folder Per Session** is enabled, a separate folder will be created for each time the Importer is run, named after the date and time of the run.
2. If the **Generate manifest file** checkbox is enabled, a CSV file is generated that will contain the list of generated message files.



3. Specify the format of the exported message, EML, MSG or JSON. See the difference between the file types in the table below.

> **Note:** You can easily convert your .MSG file into an .EML file as there could be possibilities where you want to view an .MSG file but you do not have MS Outlook to open it. .MSG files are client dependent because they are a proprietary message for Outlook, whereas .EML is a text - based file representing a message. Therefore, having single messages stored in .EML rather than an .MSG file proves more beneficial for the users, due to its flexibility.

> **Note:** JSON file format is available in all the collectors' folder target but currently is supported only for the below listed collectors. For other collectors an error will be thrown.

- Amazon S3
- Audio Video
- Box
- ChatGPT
- Chatter / Chatter Cipher Cloud
- Cloud9
- Copilot
- Dropbox Business

- Dubber Speik Recordings
- Dubber Speik SMS
- FX Connect
- iMessage
- JSON
- LSEG (Refinitiv)
- LSEG Messenger
- Microsoft Teams for Audio and Video
- Microsoft Teams via Export API
- NTR-X
- OneDrive for Business
- Pivot
- Redtail Speak
- RingCentral
- ServiceNow
- Slack eDiscovery
- Symphony
- Text- Delimited (newly created ones, not upgraded)
- Verba
- Verint
- X (Twitter)
- Web Page Capture
- WhatsApp
- Workplace from Facebook
- XIP
- XSLT/XML (newly created ones, not upgraded)
- Yieldbroker
- YouTube
- Zoom Chat
- Zoom Meetings

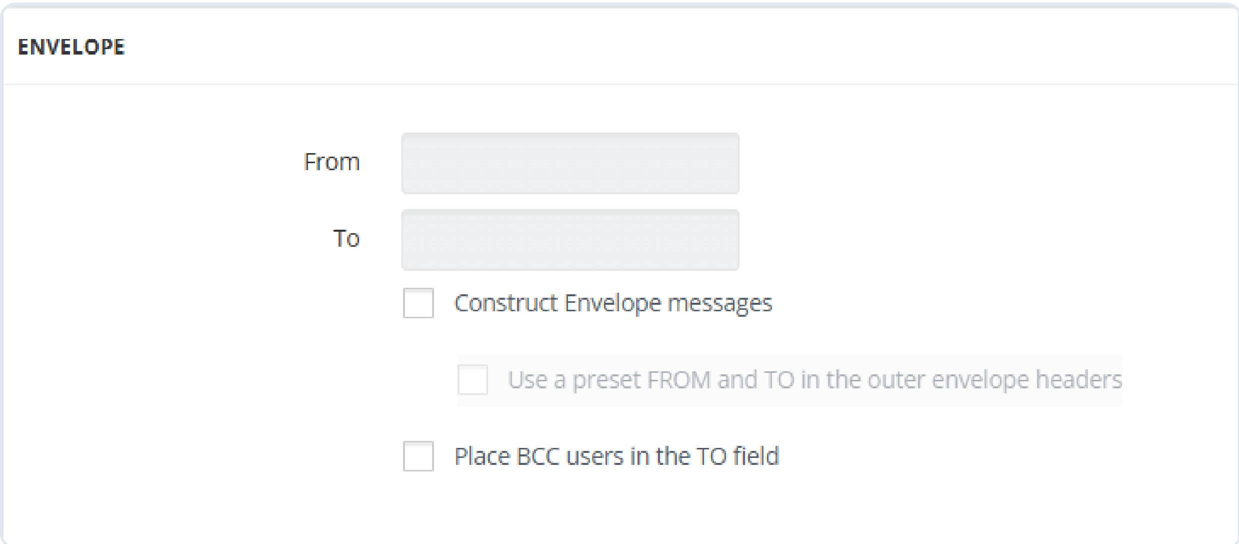
- Zoom Meetings Chats
- Zoom Meetings via Archiving API
- Zoom Phone

4. The **Remove invalid characters from message headers** checkbox is activated by default.
5. Enter the SMTP address in case you want to Replace the empty "To" with an SMTP address in the corresponding field.

Envelope

To configure the section:

1. The **Construct Envelope messages** option when enabled envelopes the original output message in a new message with the From and To email addresses set in the corresponding fields.
2. The **Use a preset FROM and TO in the outer envelope headers** option adds the From and To email addresses of the original output message in the header of the envelope.
3. The **Place BCC users in the TO field** option adds the email addresses from the BCC field of the original output message to the TO field.

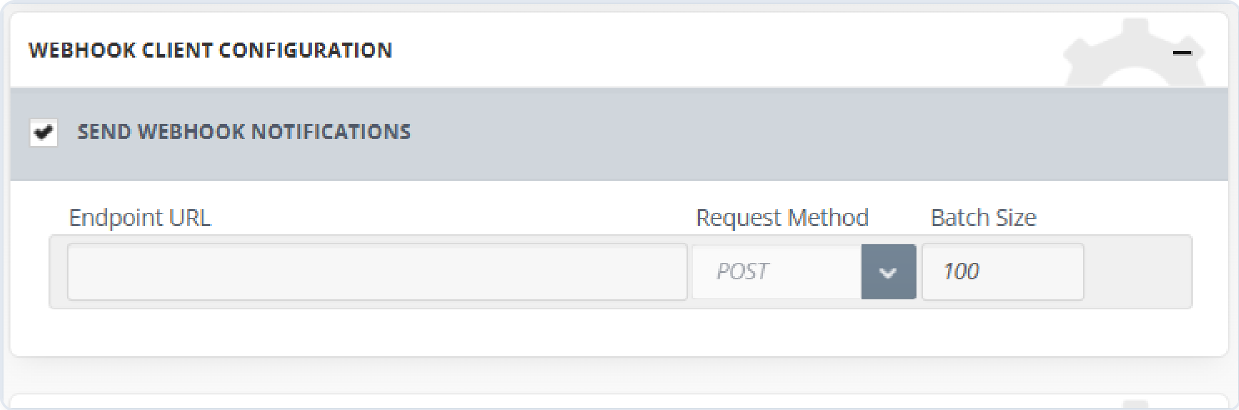


> **Note:** The service account that runs the service should have read/write permission for the specified folder.

Webhook Client Configuration

To configure the section:

1. Enable **Send Webhook Notifications**.



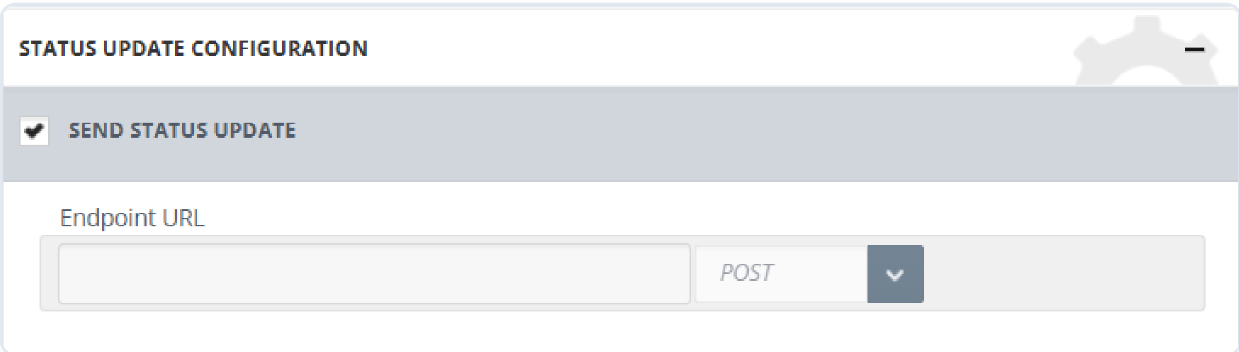
2. Specify **Endpoint URL**.
3. Specify **Batch Size**. The default size is 100.

> **Note:** The default value for **Request Method** is POST.

Status Update Configuration

To configure the section:

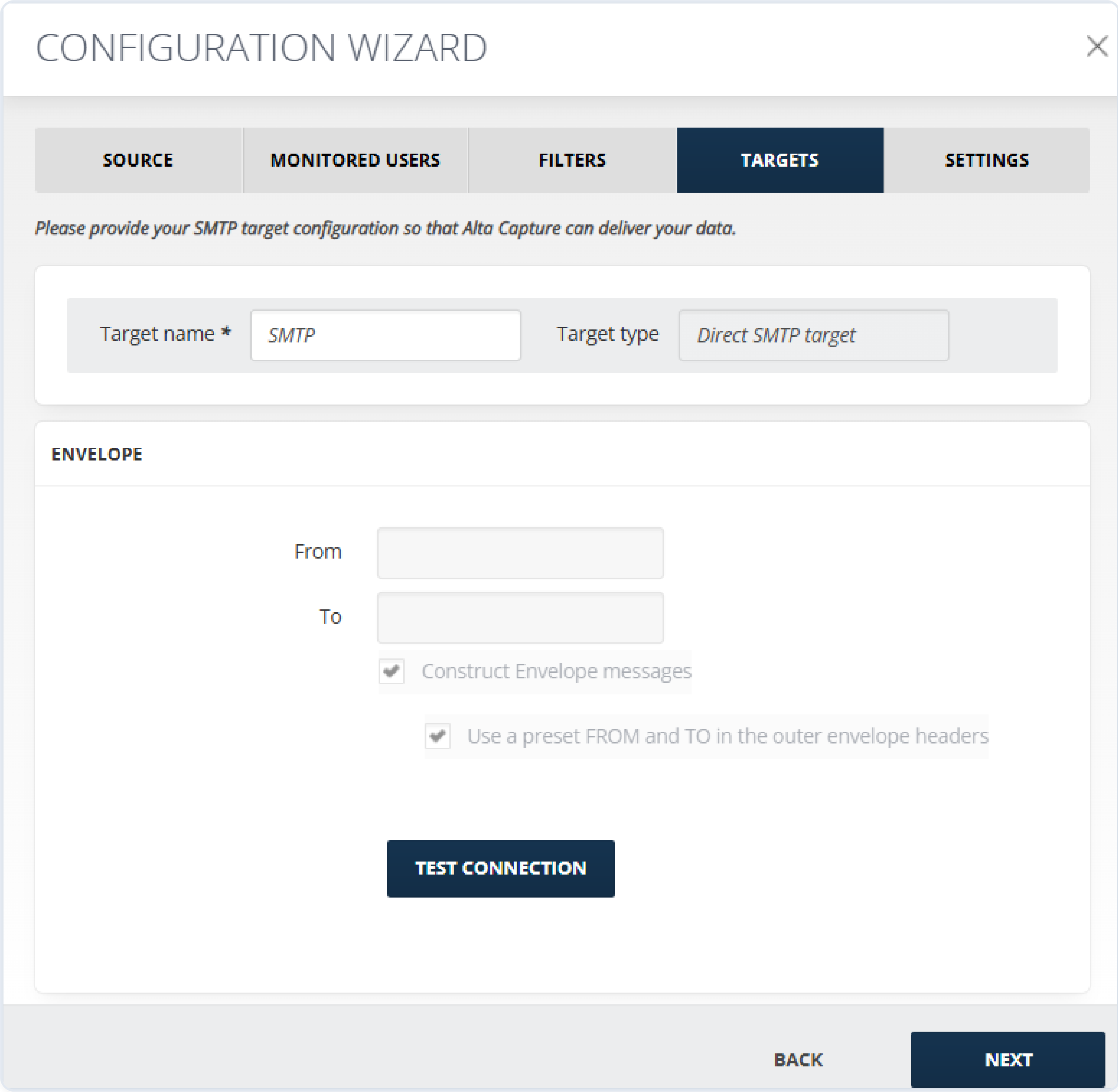
1. Enable **Send Status Update**.



2. Specify **Endpoint URL**.

Direct SMTP Target

Direct SMTP target allows delivering the processed messages directly to the recipients' SMTP server without requiring relaying through a secondary SMTP server like in the SMTP target.



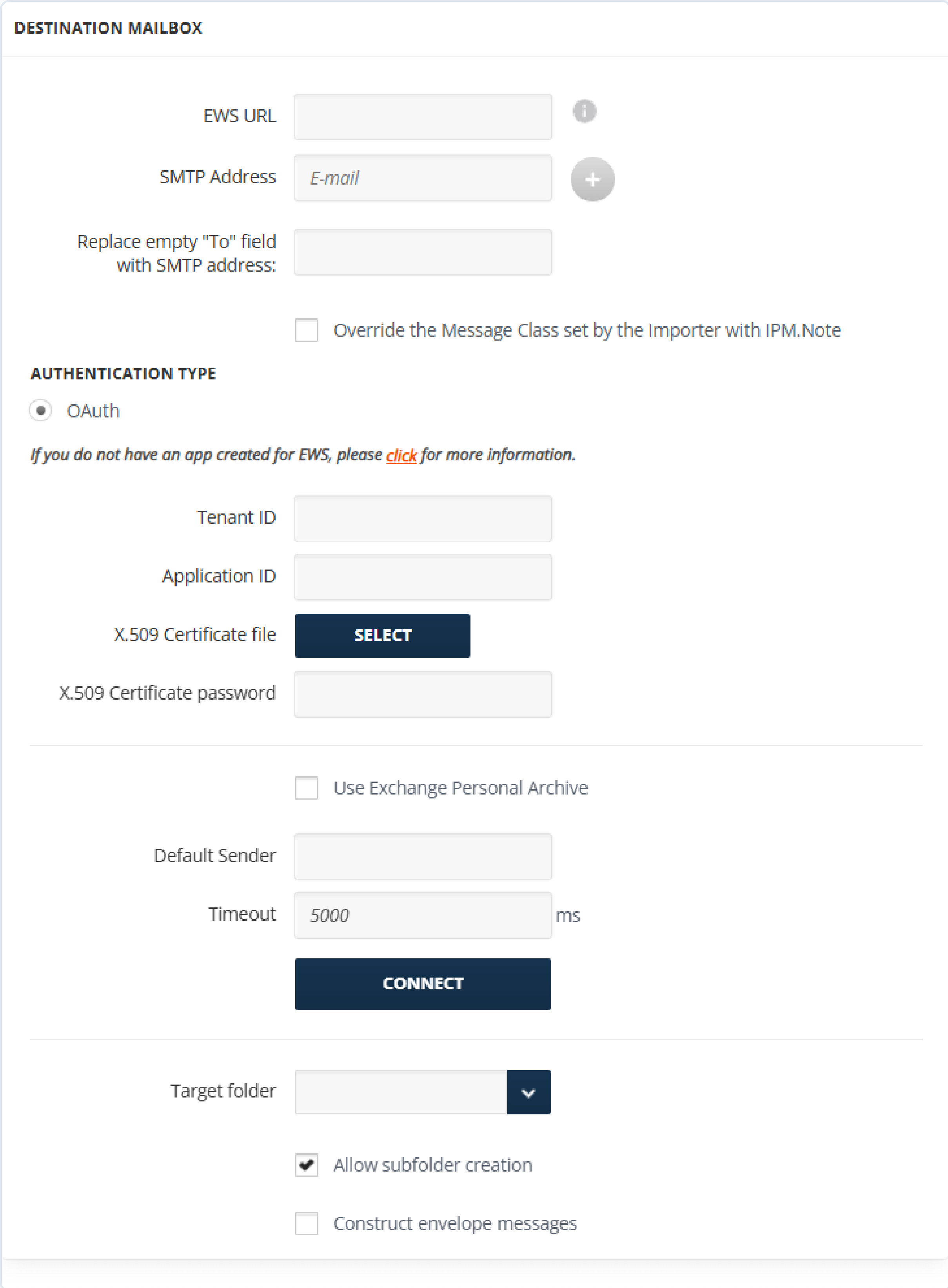
To set up the target:

1. Specify the sender SMTP address that you want to use in the **From** field. We recommend using an existing email address so the emails will not be sent to spam.
2. Specify a destination email address in the **To** field.
3. When you have filled in all the fields, click **Next**.
4. When the **Place BCC users in the TO field** is selected, the BCC emails of the message will be added to the TO field.

EWS Server Target

Capture delivers the data to the Exchange Web Services server you have chosen. The EWS server target can be used to connect to the on-prem and Microsoft Exchange Online servers.

Note: In case of connecting to the Microsoft Exchange Server Online, only Microsoft OAuth is supported.



To set up the target:

1. Enter **EWS URL**.
2. Enter the SMTP address in the relevant field.
3. Click **+** to add other SMTP addresses and click **Connect** in **Authentication Type**. In case the email address is valid, a check icon is displayed. Otherwise, information will be provided about the incorrect address. This feature allows for overcoming size and count limitations by distributing the messages across multiple locations instead of using a single one.
4. Enter an SMTP address for the **Replace empty "To" field with SMTP address** field.
5. Enable the **Override the Message Class set by the Importer with IPM.Note** checkbox to ensure items are delivered only with the message class IPM.Note. Leave it unchecked to ensure items are delivered with the message class IPM.Note.\<MessageClass\>.
6. Activate **OAuth**, provide **Application ID**, **Tenant ID**, and **Thumbprint** in case you select OAuth Authentication type. For step-by-step instructions on how to get Application ID, Tenant ID, and Thumbprint, see Microsoft Entra ID App Creationand Creating a Certificate (Private and Public Keys) accordingly.
7. Specify a **Default Sender** address for emails with empty FROM fields (EWS rejects such emails).
8. Click **Connect**, to get the folder list.
9. Specify a **Target folder** for imported data.

When you have filled in all the fields, click **Next**.

> **Note:** By checking **Use Exchange Personal Archive**, the import of data to the Personal Archive folder of the Target folder will be enabled. **Note:** By checking the **Construct Envelope Message**, the import of data in MS Exchange journal report format (the X-MS-journal-report header is also added) will be enabled.

SFTP Target

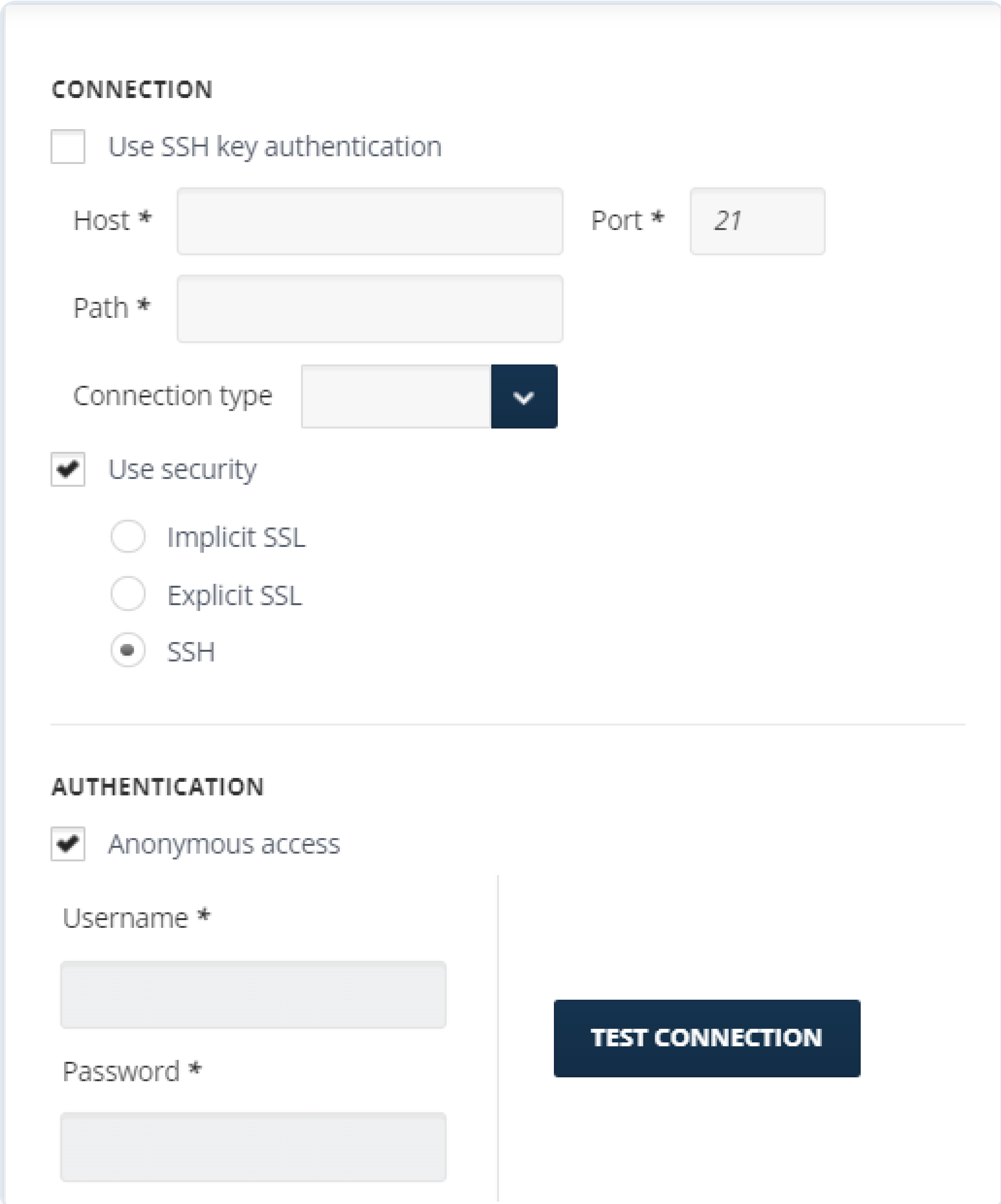
The SFTP target allows Arctera Capture to deliver data to an FTP/SFTP server address.

Below you can find information on how to setup the SFTP target for your collector.

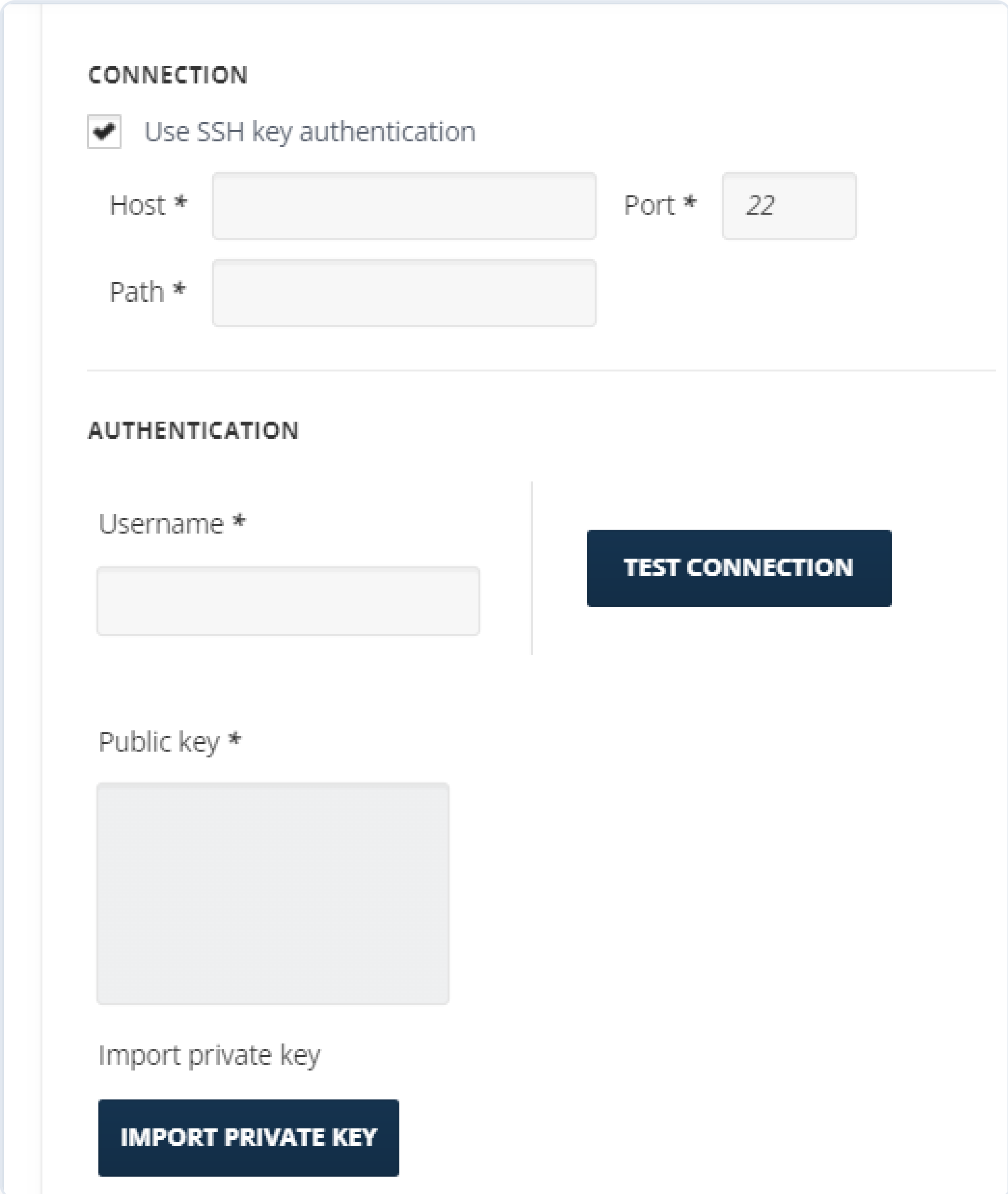
FTP/SFTP Connection

For Connection:

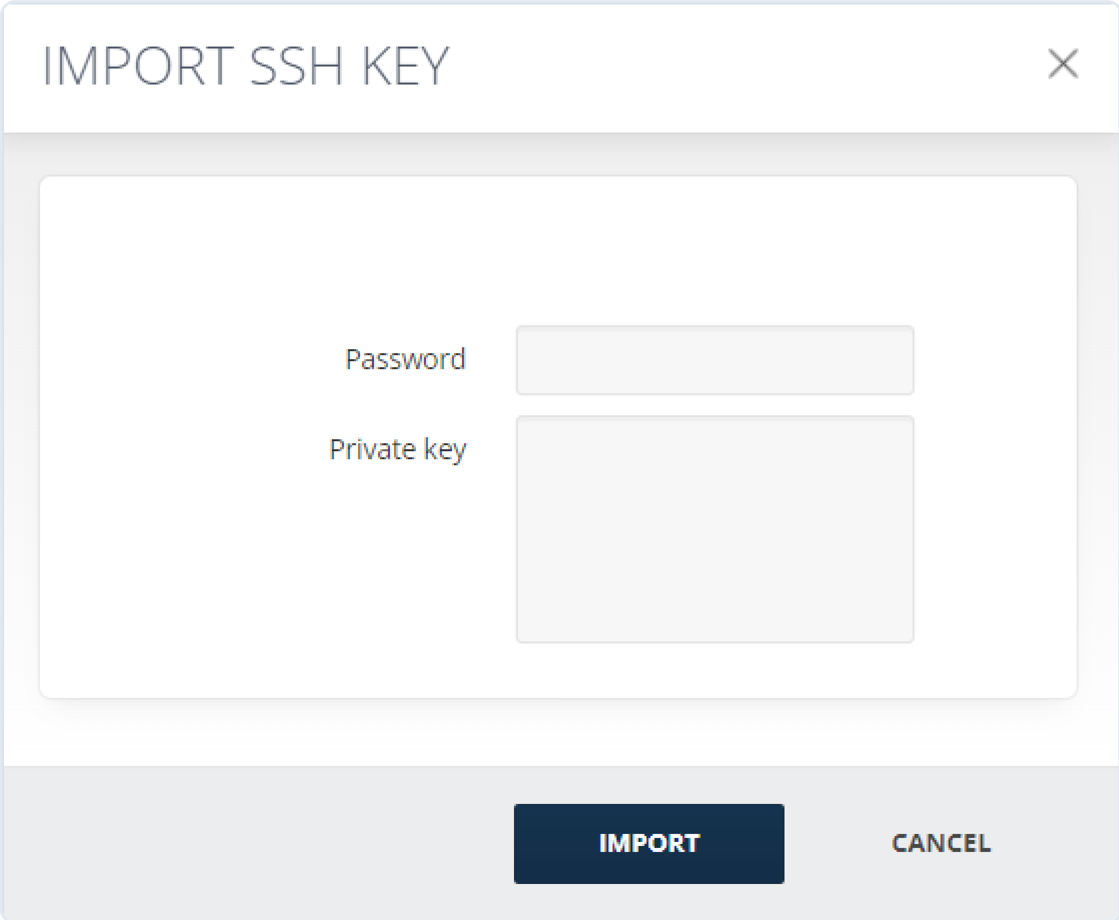
1. Enter the hostname of the remote FTP server and the folder path provided by the source in the **Host** and **Path** fields, respectively. The default FTP port is 21.



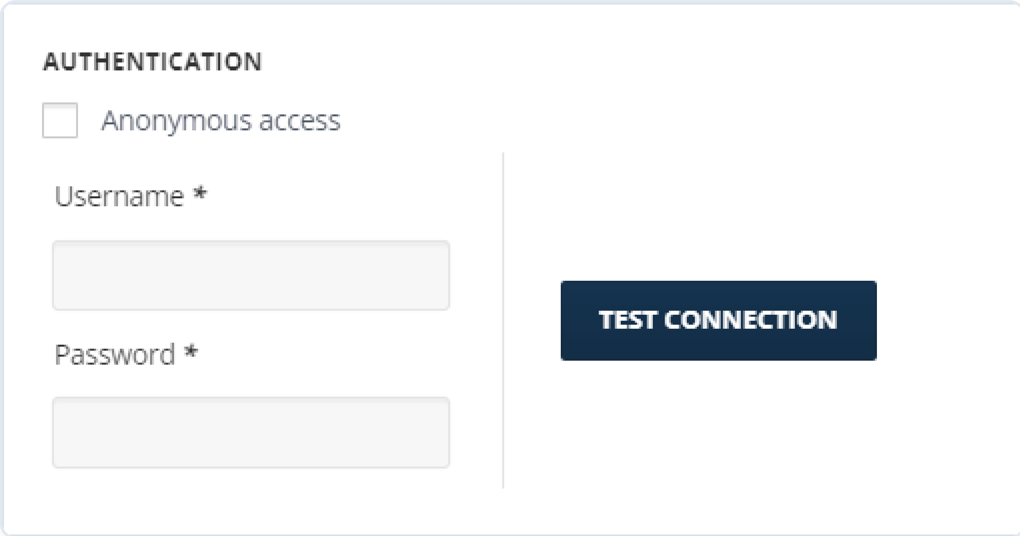
2. Make sure the connection settings match those of the SFTP server. Enter the **Path** to the required folder.
3. Enable **Use SSH Key Authentication** to open the configuration window. SSH Key Authentication is used for connecting to the source SFTP server.
4. For Authentication, enter the **Username** provided by the source.



5. Click the **Import Private Key** button and **Import SSH Key** will open.
6. Copy and paste the **Private Key**.



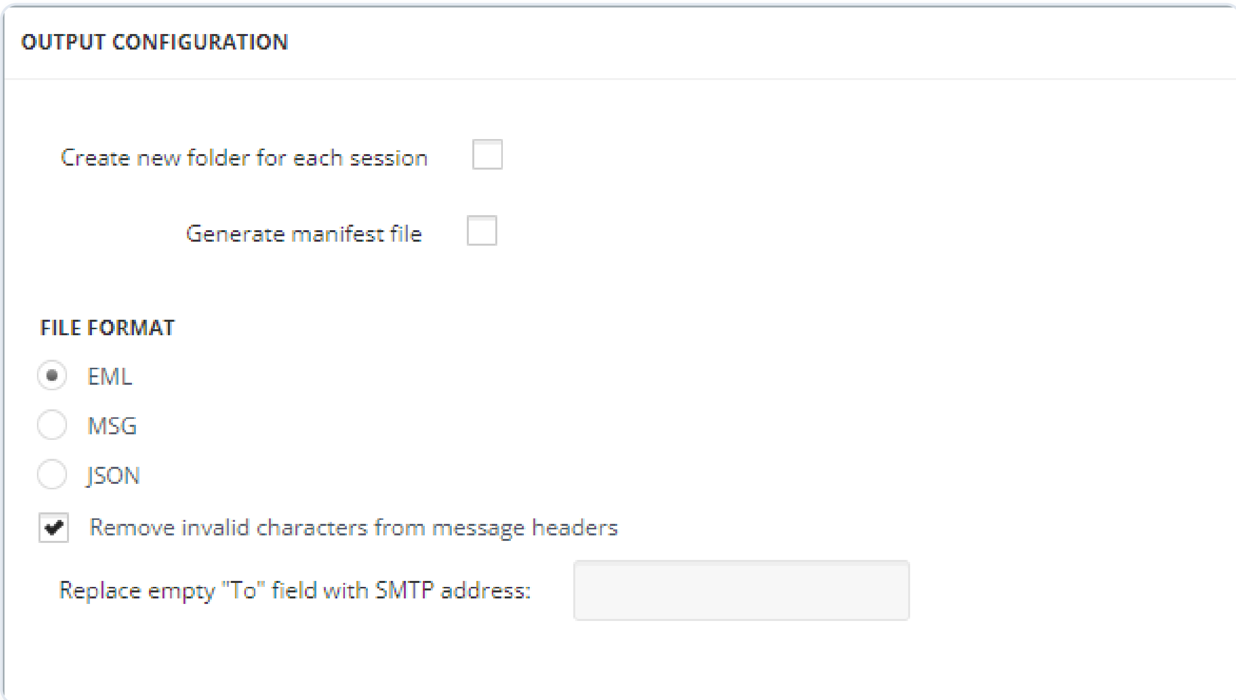
7. Enter **Password**.
8. Click **Import** and the **Public Key** field will be populated automatically.
9. In case you enable **Use Security**, select FTP connection type from the **Connection Type** drop-down list. FTP can run in either passive or active mode. The information about the connection type should be provided by the FTP host. If you wish to use FTP over SSL, enable the **Use Security** checkbox and choose the connection method **Implicit SSL**,**Explicit SSL** or **SSH**.
10. Enter the **Username** and **Password** fields provided by the source.
11. Click **Test Connection**. If the connection is successful, a green check sign is displayed.
12. To enable anonymous FTP connections, enable the **Anonymous Access** checkbox which is the default settings.



Output Folder Configuration

To configure the section:

1. If **Create New Folder Per Session** is enabled, a separate folder will be created for each time the Importer is run, named after the date and time of the run.
2. If the **Generate manifest file** checkbox is enabled, a CSV file is generated that will contain the list of generated message files.



3. Specify the format of the exported message, EML, MSG or JSON. See the difference between the file types in the table below.

> **Note:** You can easily convert your .MSG file into an .EML file as there could be possibilities where you want to view an .MSG file but you do not have MS Outlook to open it. .MSG files are client dependent because they are a proprietary message for Outlook, whereas .EML is a text - based file representing a message. Therefore, having single messages stored in .EML rather than an .MSG file proves more beneficial for the users, due to its flexibility.

> **Note:** JSON file format is available in all the collectors' folder target but currently is supported only for the below listed collectors. For other collectors an error will be thrown.

- Amazon S3
- Audio Video
- Box
- ChatGPT
- Chatter / Chatter Cipher Cloud
- Cloud9
- Copilot
- Dropbox Business
- Dubber Speik Recordings
- Dubber Speik SMS
- FX Connect
- iMessage
- JSON
- LSEG (Refinitiv)
- LSEG Messenger
- Microsoft Teams for Audio and Video
- Microsoft Teams via Export API
- NTR-X
- OneDrive for Business
- Pivot
- Redtail Speak

- RingCentral
- ServiceNow
- Slack eDiscovery
- Symphony
- Text- Delimited (newly created ones, not upgraded)
- Verba
- Verint
- X (Twitter)
- Web Page Capture
- WhatsApp
- Workplace from Facebook
- XIP
- XSLT/XML (newly created ones, not upgraded)
- Yieldbroker
- YouTube
- Zoom Chat
- Zoom Meetings
- Zoom Meetings Chats
- Zoom Meetings via Archiving API
- Zoom Phone

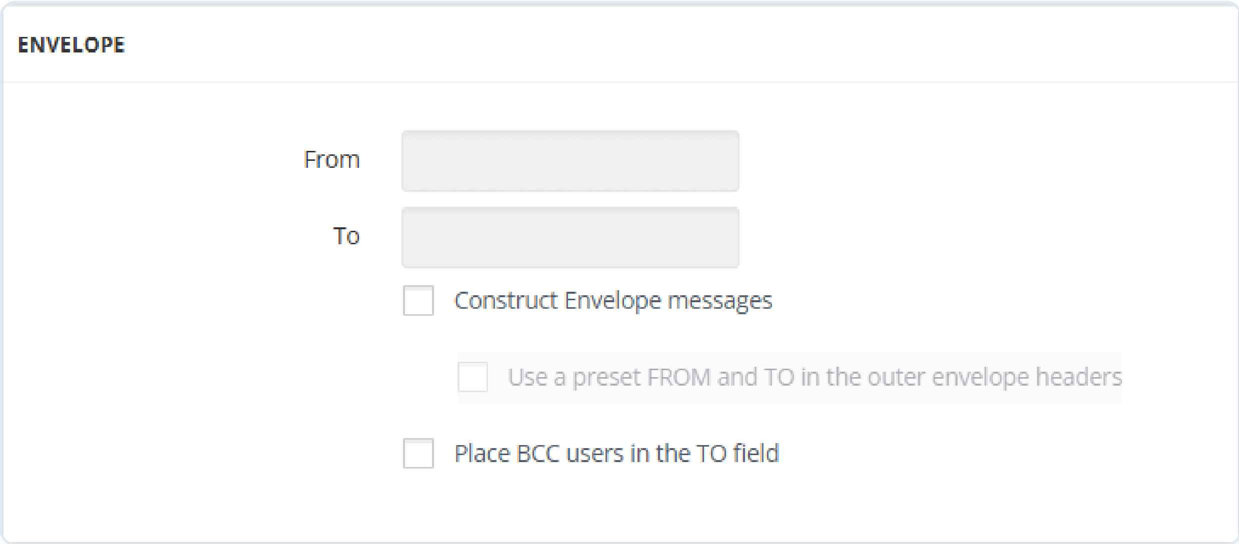
4. The **Remove invalid characters from message headers** checkbox is activated by default.
5. Enter the SMTP address in case you want to Replace the empty "To" with an SMTP address in the corresponding field.

Envelope

To configure the section:

1. The **Construct Envelope messages** option when enabled envelopes the original output message in a new message with the From and To email addresses set in the corresponding fields.
2. The **Use a preset FROM and TO in the outer envelope headers** option adds the From and To email addresses of the original output message in the header of the envelope.

3. The **Place BCC users in the TO field** option adds the email addresses from the BCC field of the original output message to the TO field.

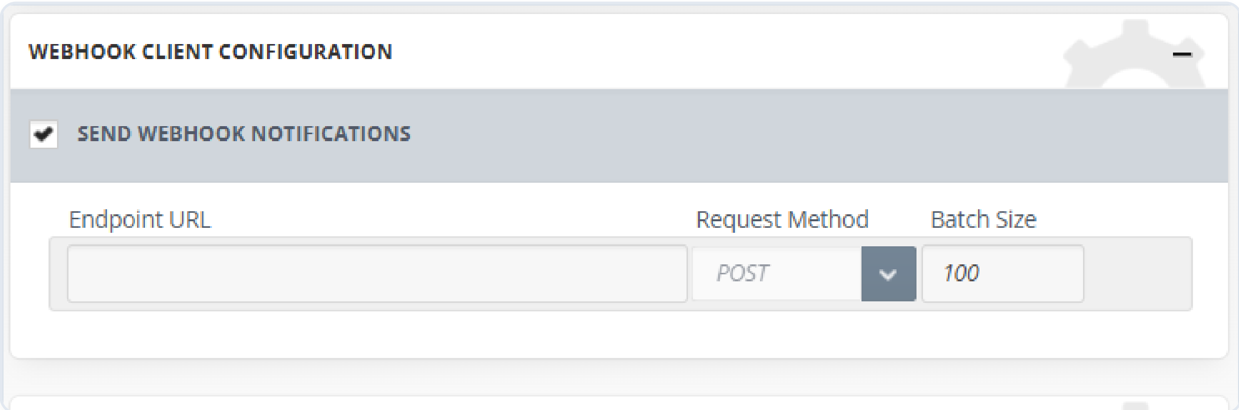


> **Note:** The service account that runs the service should have read/write permission for the specified folder.

Webhook Client Configuration

To configure the section:

1. Enable **Send Webhook Notifications**.



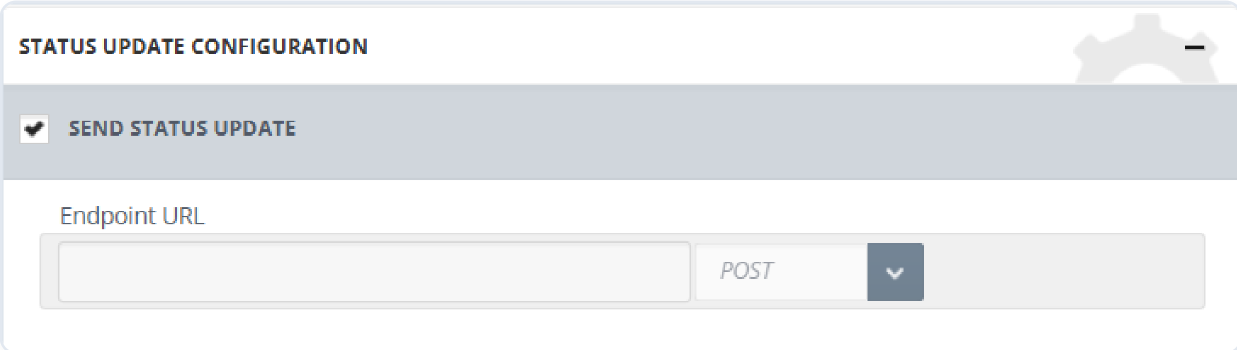
2. Specify **Endpoint URL**.
3. Specify **Batch Size**. The default size is 100.

> **Note:** The default value for **Request Method** is POST.

Status Update Configuration

To configure the section:

1. Enable **Send Status Update**.



2. Specify **Endpoint URL**.

SMTP Target

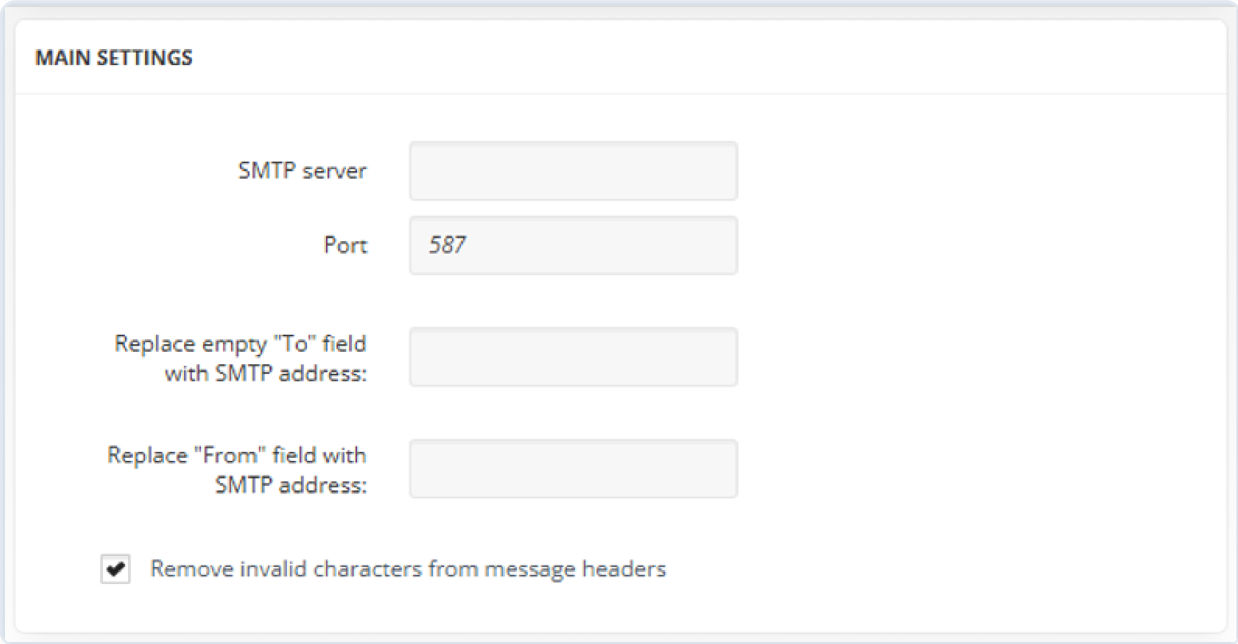
If you choose a SMTP Target, Arctera Capture will deliver the data to an SMTP server address you provide.

To configure **Main Settings**:

1. Specify the **SMTP Server** and **Port** fields.

   > **Note:** The default is 587.

2. Enter an SMTP address for the **Replace empty "To" field with SMTP address** field. If needed, provide a fallback email address to be used when an outgoing message has an empty "To" field. This ensures the message is still processed and not rejected due to missing recipient data.
3. Enter a valid email address that will be used to replace the "From" address in outgoing emails.



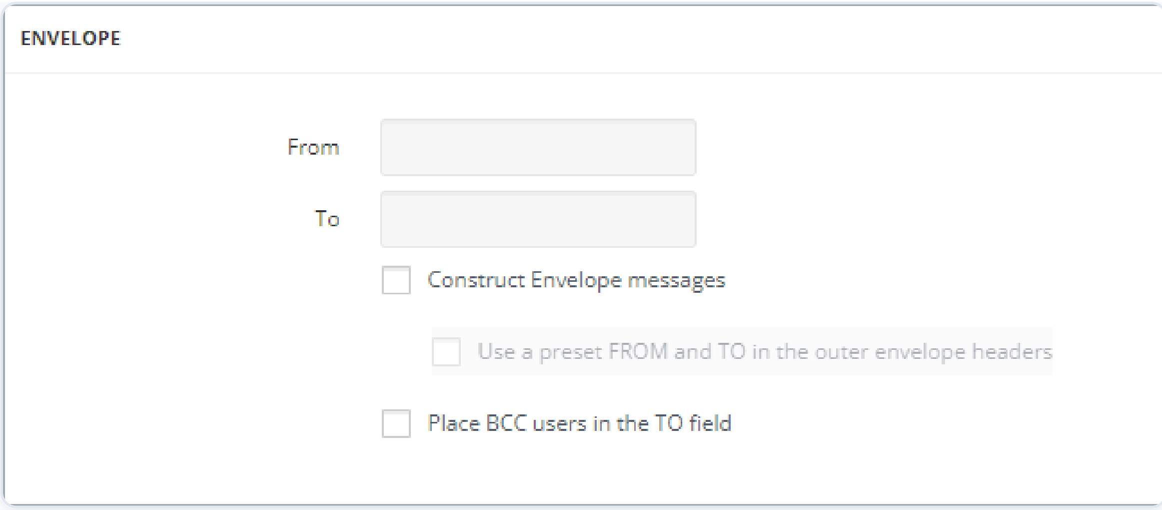
To configure the **Envelope** section:

1. Specify a destination email address in the **To** field and a return address in the **From** field.
2. Enable the **Construct Envelope messages** checkbox to envelope the original output message in a new message with the From and To email addresses set in the corresponding fields. The **Use a preset FROM and TO in the outer envelope headers** option adds the From and To email addresses of the original output message in the header of the envelope.

> **Note:** When enabling theConstruct Envelope Messagescheckbox, data in MS Exchange journal report format (the X-MS-journal header also be added) will be imported.

3. Enable **Place BCC users in the TO field** to add the email addresses from the BCC field of the original output message to the TO field.

> **Note:** When enabling the **Place BCC users in the TO field** checkbox, all BCC recipients will be moved to the TO field.

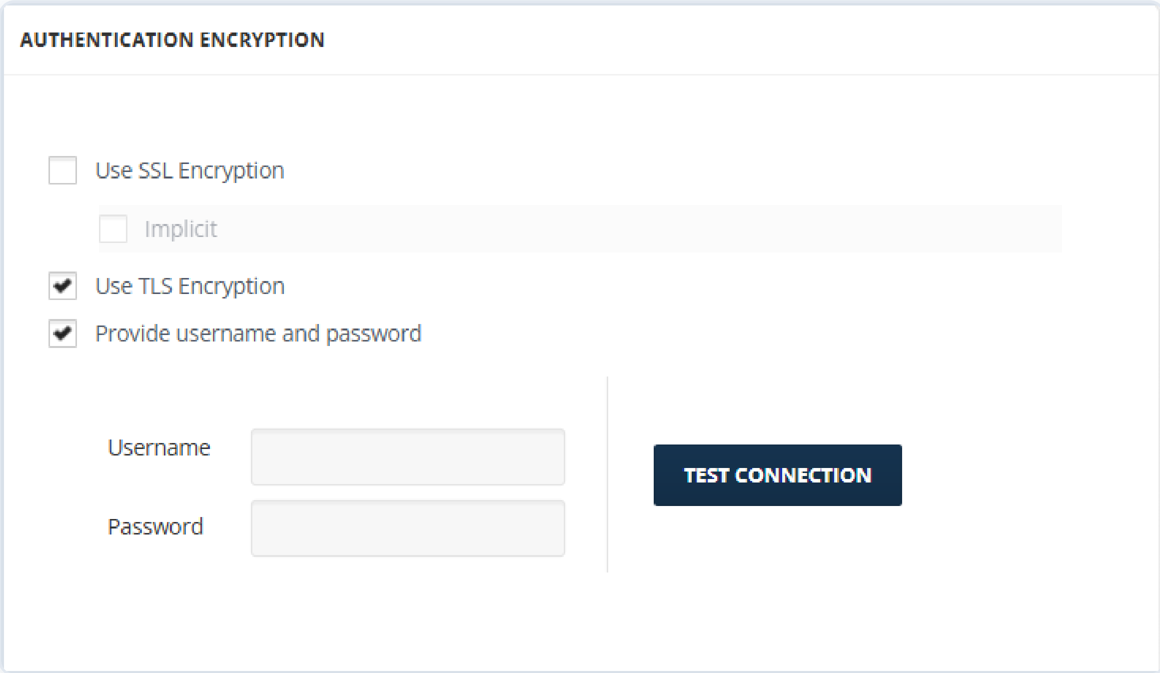


> **Note:** SMTP Target is not recommended for delivering messages to Exchange Online Mailboxes, due to various throttling policies set by Microsoft. Also, Exchange Online does not accept Journal Envelope messages which can result in loss of original message time stamps and other metadata.

To configure **Authentication Encryption**:

1. Enable **Use SSL encryption** if you want to use SSL encryption. When enabled you can also check the **Implicit** checkbox to encrypt the entire FTP connection from the start of the session.
2. Enable **Use TLS Encryption** if you want to encrypt using TLS.
3. Enable **Supply Username and password** to enter username and password.

> **Note:** For Encryption, SSL and TLS encryption settings should match those of the target SMTP server. Click **Test Connection** to check the connection and to ensure that your settings are accurate.



Google Vault Target

Before configuring the Google Vault Target in the Arctera Capture UI, the following configurations should be done in Google Admin Console.

- **Google Vault Configuration**
- **Google Vault Target Configuration**

Google Vault Configuration

To configure the section

1. Login to https://console.cloud.google.com/ using an Administrator account, click **Select a project**, then **NEW PROJECT**.
2. Enter a name for the project and click **CREATE**.
3. Once the project is created, and there are multiple projects, click **SELECT PROJECT** from the Notifications. You will be navigated to the created project dashboard.

> **Note:** If this is the first project created, you will automatically be navigated to the project dashboard.

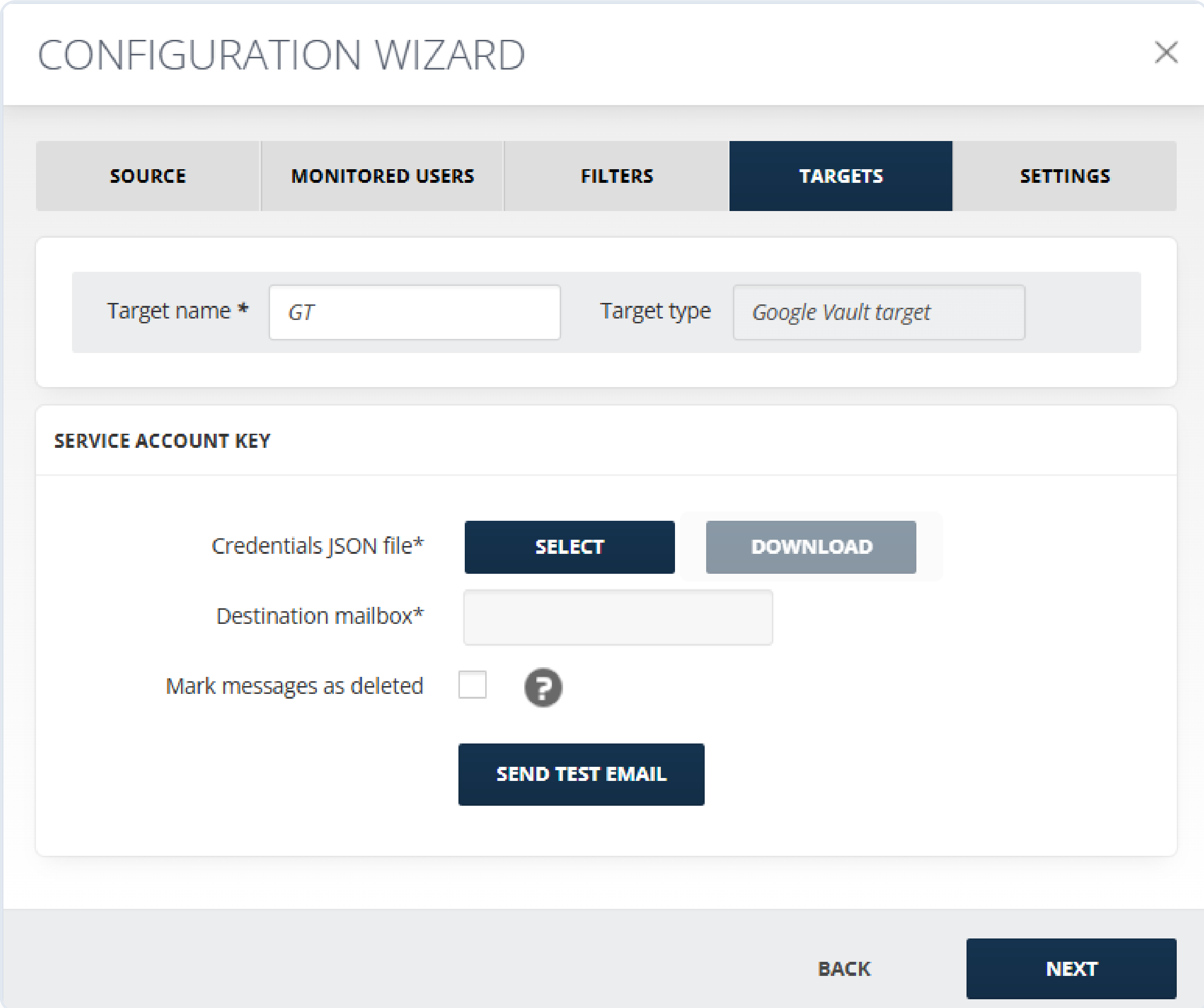
4. Hover **APIs & Services**, then select **Library**.
5. In the **Search for APIs & Services** search box, type Gmail.

6. Click **Gmail API**.
7. Once you are in the Gmail API page, click **ENABLE**.
8. Click **Credentials**.
9. Click **Manage service accounts**.
10. Click **\+ CREATE SERVICE ACCOUNT**.
11. Enter a name and a description for the service account and click **CREATE AND CONTINUE**.
12. Select **Owner** as a role and click **CONTINUE**, then click **DONE**.
13. You will be redirected to the Service Accounts page. Click the kebab icon and select **Manage keys**.
14. Select **ADD KEY** > **Create new key**.
15. Select **JSON** as a key type and click **CREATE**.
16. Once the key is created, you should get prompted to save the file on your computer, save it somewhere secure, you will need it when configuring the collector.
17. To grant permissions to the application, go to https://admin.google.com > **Security** > **API controls**.
18. Scroll down to **Domain wide delegation** section and click **MANAGE DOMAIN WIDE DELEGATION**.
19. Click **Add new**.
20. Open the key file that you saved as JSON above, copy the value of client_id, then paste it in the **Client ID** field. Enter `https://www.googleapis.com/auth/gmail.insert` in **OAuth scopes** field and click **AUTHORIZE**.

Google Vault Target

To set up the section:

1. Upload JSON file saved in the step 15 of the previous section by clicking **SELECT**.
2. Specify the mailbox, to which the imported messages should be delivered, in the **Destination mailbox** field.
3. When **Mark messages as deleted** option is checked, the imported messages are not visible in the All Mail section but are still available for compliance search.
4. Click **SEND TEST EMAIL** to test the connection to the target.

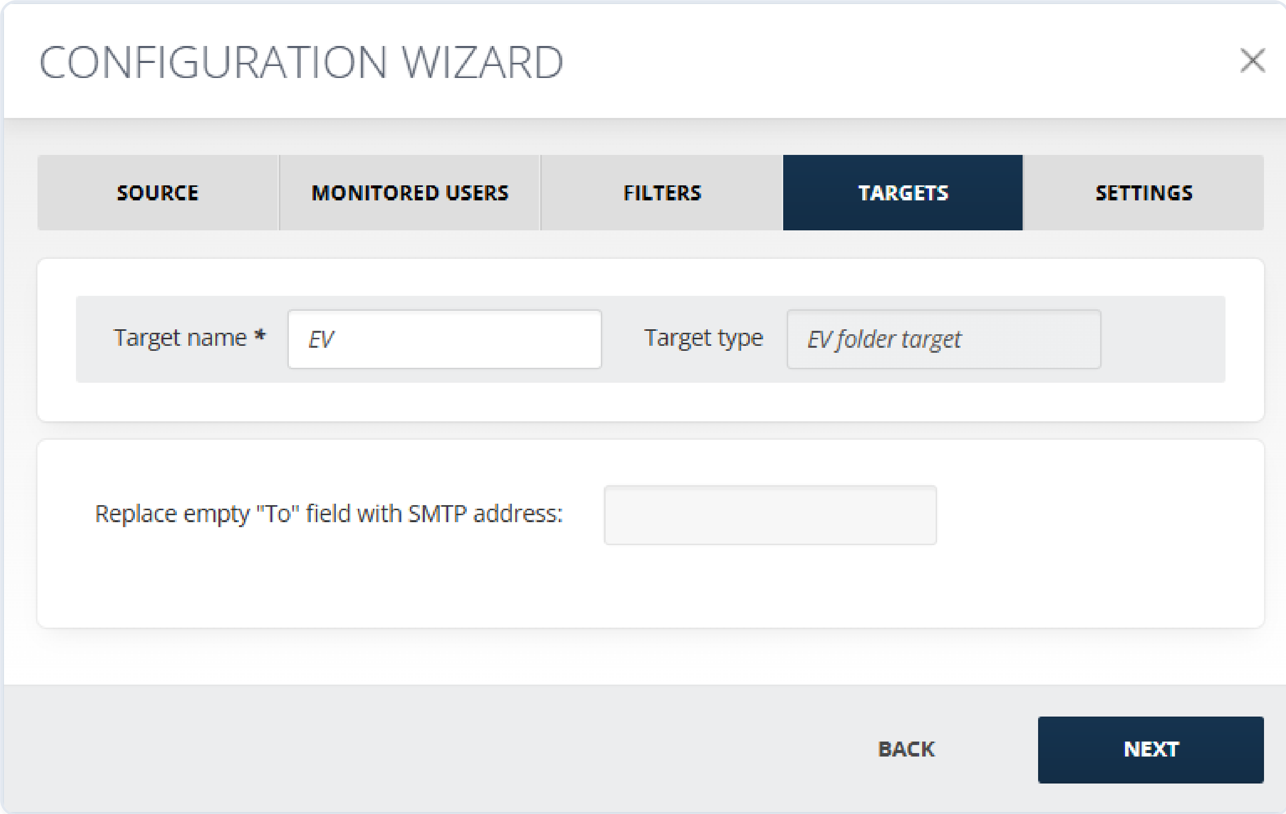


Note: You can download the uploaded JSON file by clicking **Download**. It is active only when there is a JSON file to download.

EV Folder Target

Note: The target is applicable only to Arctera View Compliance and Governance.

If the EV Folder target is configured for the importer, the original items will be directly delivered to that folder.


CONFIGURATION WIZARD
SOURCE
MONITORED USERS
FILTERS
TARGETS
SETTINGS
Target name *
EV
Target type
EV folder target
Replace empty "To" field with SMTP address:
BACK
NEXT

SETTINGS

This section includes the following topics:

- Importer Settings
- Reporting & Message Tracking
- Message Headers
- Logging
- Importer Schedule
- Filtering
- Processing
- Advanced Configuration Options

Importer Settings

The final step for the **Importer Configuration Wizard** is the Importer Settings. Under this tab, you can configure the following:

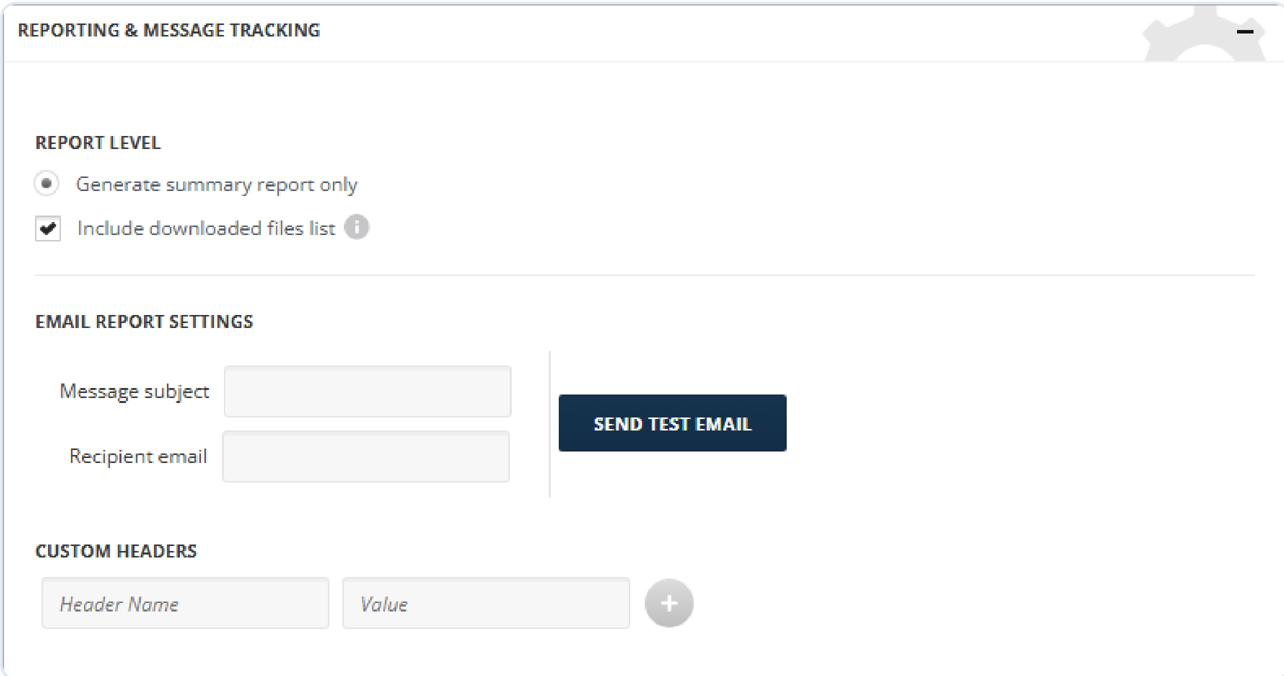
Importer Settings

1. **Reporting & Message Tracking**
2. **Message Header**
3. **Logging**
4. **Importer Schedule**
5. **Filtering**
6. **Processing**
7. **Advanced Configuration Options**

Reporting & Message Tracking

The following section of the **Importer Settings** refers to email reports, which may be used to deliver statistical information (also viewable on the **Dashboard**) via email.

Reports are different from collector to collector, based on the activities that can be captured from them.



To configure the section:

1. For **Report Level**, **Generate Summary Report Only** reports include Source Statistics and Message Statistics. Source Statistics includes the number of unprocessed, quarantined, failed, and imported sources. Message Statistics includes the number of unprocessed, failed, successful, excluded, and ignored messages.

   > **Note:** Detailed reports are longer and take more time to read. Reports exceeding 5 MB are shortened.

2. Select **Include downloaded files list** to include the names of the files that the collector processes during each run in the summary report, regardless of whether the run succeeds or fails. This option is selected by default.

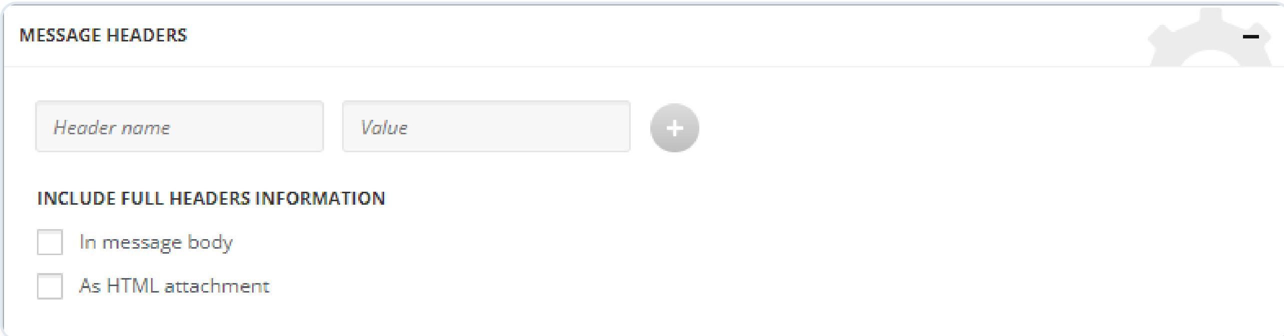
   > **Note:** This option applies only to file-based collectors that download source files (for example, EML, Bloomberg, and Audio/Video). It does not apply to API-based collectors that do not download source files.

   > If a run processes 100 files or fewer, the file names are listed in the report message body. If a run processes more than 100 files, the file names are included as a `.txt` attachment instead.

3. Enter **Message subject** for the report message.
4. Enter **Recipient email address** for delivering reports.
5. For **Custom Headers**, enter **Header Name** and **Value**.

Message Headers

Message headers are custom headers that are used for labeling and sorting messages.



> **Note:** Filters are not applied to headers generated by these settings.

> To configure the section:

1. Fill in the **Header name** and **Value** fields and click **+**.
2. Include the full header information either in the message body (with metadata separators in between) or as HTML attachment (as Metadata.HTML attachment).

   > **Note:** These settings do not apply to the EML source.

The existing custom headers can be overridden if the user specifies another Header name. The user cannot specify one of the following headers and the added header must meet RFC 5322 standard:

- Message-ID
- From
- To
- Cc
- Bcc
- Subject

- Date
- In-Reply-To

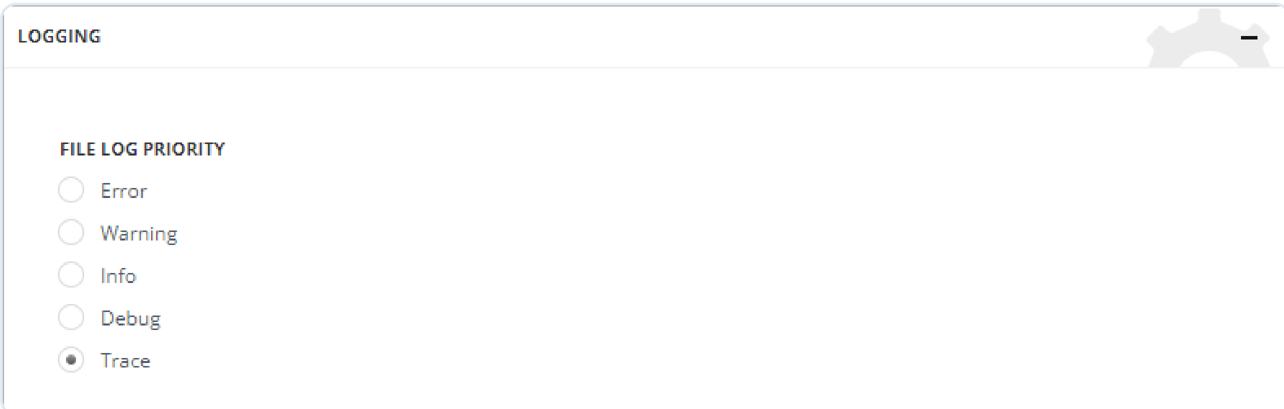
References

- MIME-Version
- Content-Type
- Content-Transfer-Encoding
- Received
- Return-Path
- Authentication-Results
- DKIM-Signature

Logging

Enter a file path in **file log folder** field. File logs are typically used for troubleshooting purposes. This field is required.

With **File Log Priority** the logs are saved in a separate log file and with **Event Log Priority** the event Logs are stored in the Windows Event Viewer and is used to avoid third-party tools in Windows. Also, the latter helps to customize logging process and facilitate monitoring based on requirements.



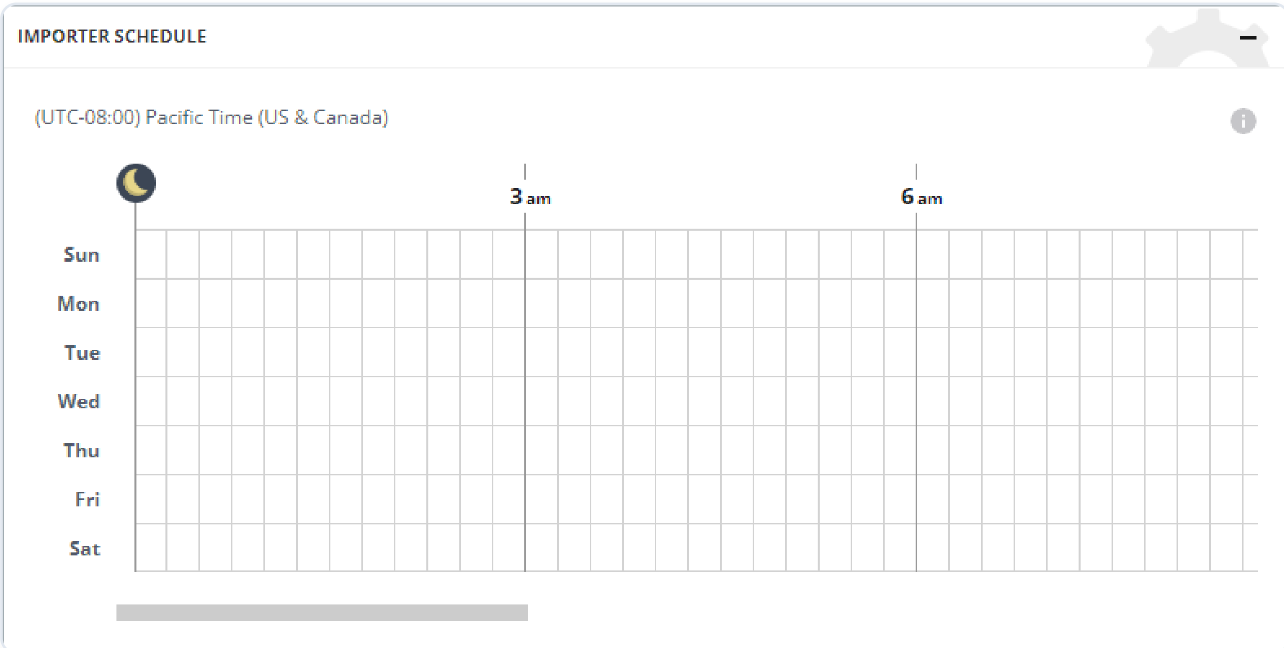
For File Log Priority:

- **Error**. Only errors are recorded in the log file. Example: ERROR Arctera Capture.Core.SenderThread - \<1\> Failed to send message #4, TargetError. Error: Failed to save message C:\Users\Desktop\Bloomberg Target\4.eml: Header name contains invalid characters.

- **Warning**. In addition to error logs, warning logs are also added. Example: WARN Arctera Capture.Core.Importer - The report won't be sent as no Email Address is provided.
- **Info**. This logging level gives information on performed actions. Example: INFO Arctera Capture.Core.Importer -Creating default Target.
- **Debug**. This logging level provides information on how an action was accomplished. It gives more detailed overview than the previous three levels. Example: DEBUG Arctera Capture.Core.Importer - new session for Importer: 1
- **Trace**. The trace level is the lowest logging level, e.g., is the most detailed one. TRACE Arctera Capture.Core.SenderThread - \<31\> Preparing message #820 for sending. When choosing Trace logging level, a warning message will appear notifying about possible security risks with this level of logging. Sensitive data can be stored in the log as plain text.

Importer Schedule

Here you have the option to choose the **Selected Times** importer schedule option. This enables you to set a weekly automated option. Increments are at 15-minute intervals.



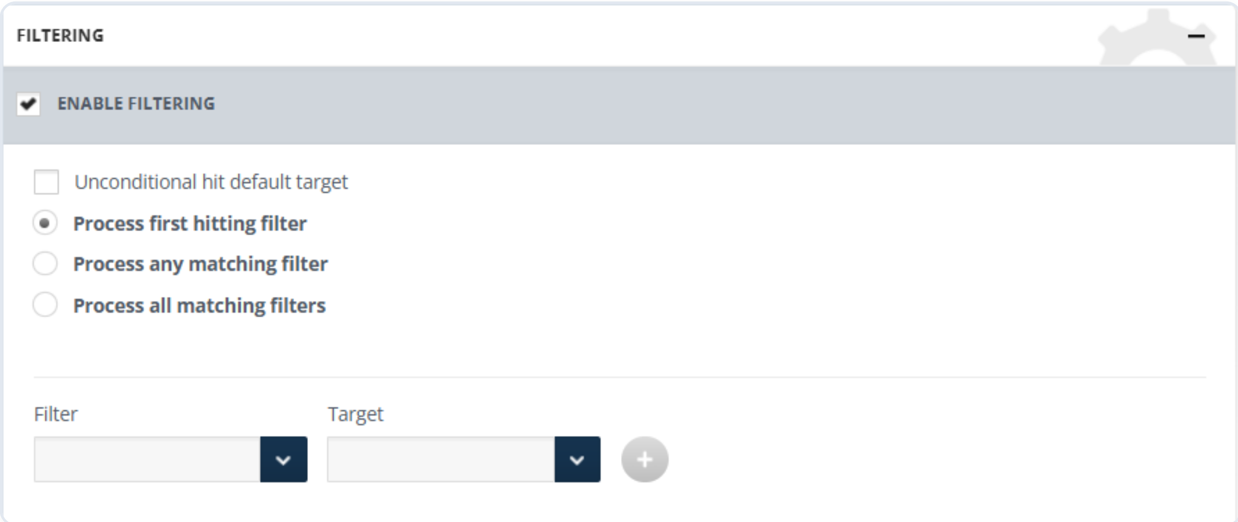
Even if the scheduler is enabled, but a time is not selected through Importer Schedule, the job will not be queued.

Filtering

Filters will not be applied unless filtering is enabled. enable the **Enable filtering** checkbox to configure their behavior.

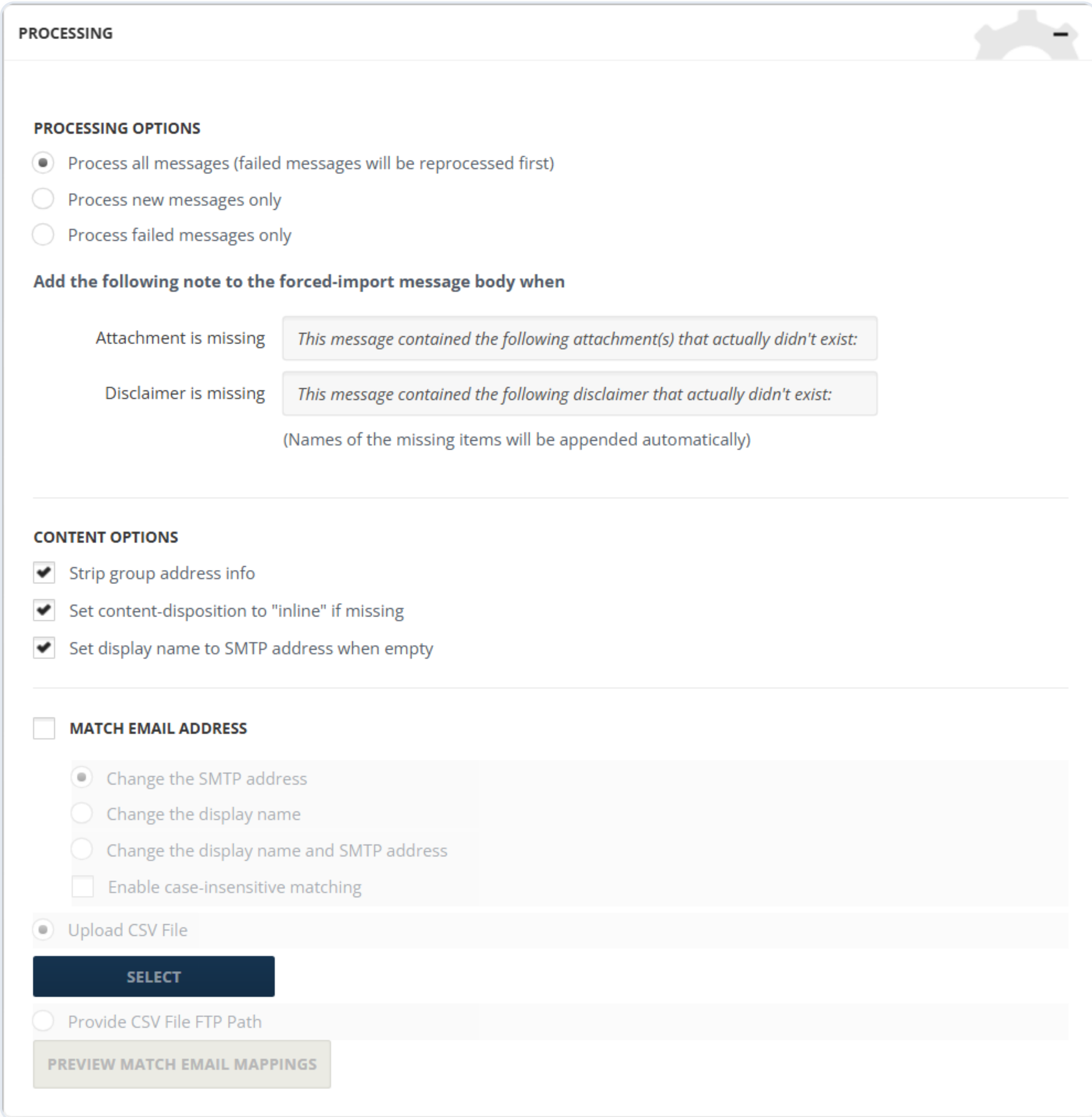
To configure the filter:

1. Enable the **Enable filtering** checkbox and select the corresponding option:
    - **Unconditional hit default target** - If selected, all data will be delivered to the default target, even if an alternative target is set.
    - **Process first hitting filter** - If enabled, a single message will be sent to the first Target which fulfills the filters condition.
    - **Process and matching filter** - If enabled, Filter and Target pairs will be configured, and a copy will be sent to the target for each filter fulfillment.
    - **Process all matching filters** - If enabled, only filters can be configured with a single target.
2. Select the filter name and choose the target from the drop-down menu where the corresponding messages should be sent.
3. Click the activated **+** button to add the filtering setting, otherwise it will not be saved.



Processing

The following options are available for Processing options:



- **Processing Options** is mostly used for the troubleshooting purpose.
- It is advised to use **Process Failed Messages Only** when there is a big number of failed messages.
- If there are problems with connection which lead to failed messages, **Process All Messages** is the preferred choice. If necessary, change this setting to process new segments or failed segments exclusively.
- **Attachment is missing** - This line is added to the first line of the reprocessed segments with references to missing attachments.
- **Disclaimer is missing** - This line is added to the first line of the reprocessed segments with references to missing disclaimers.

- **Strip Group Address Info** - This option is selected by default and applies to the EML collector. With this option, recipients in the header (To, CC and BCC) in an EML file will be removed upon conversion.
- **Set Content-Disposition to inline if missing** - This option applies only to the EML source. When processing EML files that have image attachments, Arctera Capture will insert any missing.
- Content Disposition header fields and set their disposition type to inline so that images will appear in the message body when they are viewed in applications such as Microsoft Outlook.
- **Set display name to SMTP address when empty** - Enter the SMTP address in the **Display Name** field.

Match Email Address - The Match Email Address option can match the existing ID or SMTP Address and replace:

- **SMTP Address**
- **Display Name**
- **Display Name and SMTP Address**

Select **Enable case-insensitive matching** to match email addresses regardless of letter case.

The CSV file should contain the following columns:

- Last Name (A)
- First Name (B)
- Company Name (C)
- Old Email (D)
- New Email (E)

You can provide the matching file from either of the following sources:

- **Upload CSV File** - Select and upload the CSV file directly.
- **Provide CSV File FTP Path** - Enter the FTP path to the location where the CSV file resides.

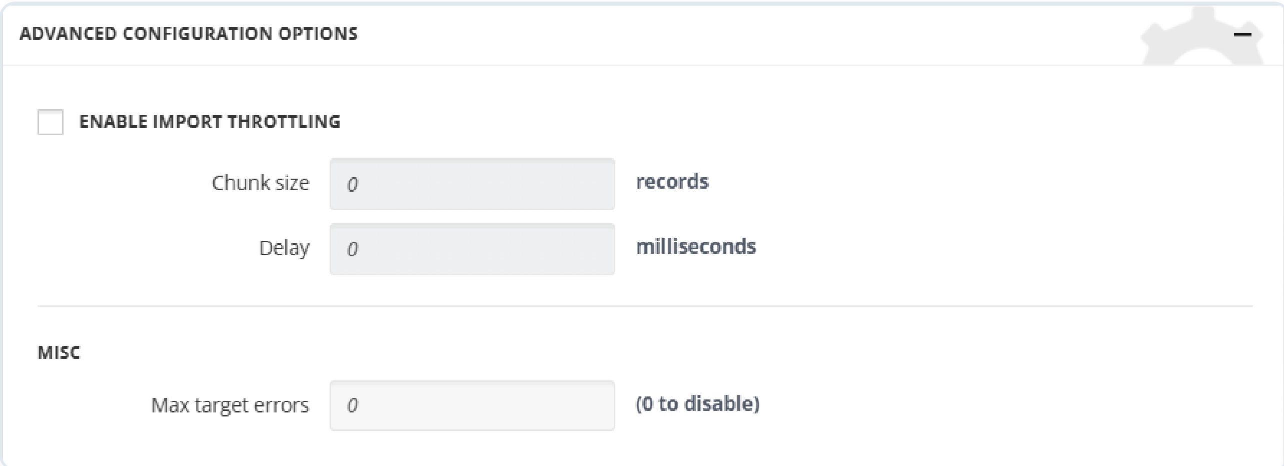
For both source types, Arctera Capture validates and previews the file so that you can confirm it is processed correctly. The validation and preview are performed on the Agent side during the import job.

Select **Preview** to view a sample of the matched records. The preview displays the first 10 records only, for preview purposes.

Note: The preview grid shows the first 10 records for preview purposes only.

Advanced Configuration Options

With the help of **Enable Import Throttling** you can reduce bandwidth consumption by breaking down the data transfer into chunks with delays in between.

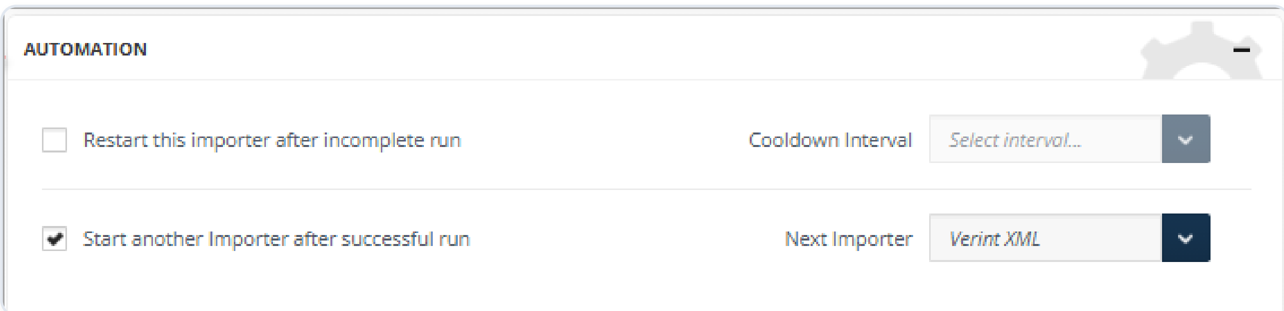


After you have filled in all the fields in the five tabs you will have to click **Save & Finish**. In case you want to make changes in the Wizard, click **back** and you will be redirected to **Importer Settings**.

Automation

The **Automation** section lets you automatically recover and chain importer runs.

- **Restart this importer after incomplete run**: When enabled, the importer automatically restarts after an incomplete run. Select the **Cooldown Interval** from the drop-down to set how long to wait before the importer restarts.
- **Start another Importer after successful run**: When enabled, another importer starts after this importer completes its run successfully. Select the importer to run from the **Next Importer** drop-down.



CAPTURE NOTIFICATIONS

This section includes the following topics:

Overview

The **Notifications** section provides visibility into the Arctera Capture importer lifecycle and the overall health of the import pipeline. It allows users to monitor operational events, delivery outcomes, configuration changes, and pipeline issues through in-app notifications and webhook push notifications.

To access the Capture Notifications, navigate to **Reports and Notifications** > **Notifications** and open the **Capture Notifications** tab.

Event Subscriptions

Event subscriptions allow users to define which events generate notifications and how those notifications are delivered. For each subscription, users can enable one or both of the following notification type to receive notification events:

- **Receive In-App Notification**: Displays the events in the Arctera Capture **Notification Center**.
- **Webhook Push Notification**: Sends the events to a configured webhook endpoint.

Notifications can also be delivered to a Microsoft Teams channel. For more information, see Configuring Microsoft Teams Notifications.

By creating specific subscriptions, users can monitor important event triggers in real time, ranging from successful data processing to critical pipeline interruptions.

Creating an Event Subscription

To create an event subscription:

1. Open the **Notifications** page.
2. In the **Event Subscriptions** section, click **New Subscription**.
3. In the **Create Event Subscription** window, select the event you want to monitor from the **Event** drop-down list.
4. Select the importer scope from the **Importer Type** drop-down list.
5. Select one or both of the available notification options:
    - **Receive In-App Notification**
    - **Webhook Push Notification**
6. Click **Create**.

> **Note:** The new subscription becomes active immediately and appears in the subscription list. The new subscription becomes active immediately and appears in the subscription list.

Configuring Webhook Push Notifications

Webhook notifications let you receive real-time updates about events that occur in your Merge1 instance. When a configured event occurs, Merge1 sends an HTTPS POST request to a URL that you specify. To use webhook push notifications, you must first configure the webhook settings.

To configure webhook push notifications:

1. In the **Event Subscriptions** section, click the gear icon.
2. In the **Configure Webhook Push Notification** window, specify the **Endpoint URI**.
3. Review the **Method** field. Webhook notifications are sent by using the POST method.
4. Optional: Add one or more **Custom Headers** by entering a header name and value.
5. Click **Save**.

Configuring Webhook Settings

Your listener endpoint must meet the following requirements:

- Use an HTTPS URL.
- Be able to receive HTTPS POST requests.
- Return a 2xx HTTPS status code to confirm that the notification was received successfully.

If Arctera Capture receives a non-2xx response, it may attempt to redeliver the notification.

Example in Node.js:


```
{
  "TenantId": "0380ca8e-9c66-4cb2-b4e1-a881cc4fc0c5",
  "CreatedDate": "2026-08-27T14:36:55.9031195Z",
  "SentTime": "2026-08-27T14:36:55.8774493Z",
  "Title": "Importer data deleted",
  "Body": "\"Yieldbroker 01.07\" importer data has been deleted by
\"admin@merge1_saas_tenant20.com | Admin\".\r\n ● Associated component
data has also been deleted.",
  "BodyType": 0,
  "Severity": 1,
  "Source": "Importer",
  "ImporterId": "789b9374-6fc0-4819-8d8a-4c20b7f3fcd4",
  "ImporterName": "Yieldbroker 01.07",
  "EventCode": 40014
}
```


The notification object sent to your listener endpoint may have the following structure:

- `TenantId`: A unique identifier (GUID) for the tenant that the event belongs to.
- `CreatedDate`: The date and time when the event was created.
- `SentTime`: The date and time when the notification was sent.
- `Title`: The event title.
- `Body`: A detailed description of the event. In this case, it explains that the importer data was deleted.
- `BodyType`: An integer that specifies the format of the Body. 0 represents PlainText.
- `Severity`: An integer that represents the severity level of the event.

- `Source` : The source that generated the event.
- `ImporterId` : A unique identifier (GUID) for the specific importer that generated the event.
- `ImporterName` : The name of the importer, which is "Yieldbroker 01.07" here.
- `EventCode` : A numerical code that represents the specific type of event. Indicates that 40014 corresponds to the "ImporterDataDeleted" event.

The list of error codes is represented in the below:

- 10000 — FileQuarantined: Quarantine file
- 10001 — FailedToQuarantineFile: Failed to quarantine file
- 10002 — MonitoredUsersSkipped: Monitored users skipped
- 40001 — ImportJobFinishedWithFatalError: Import job finished with fatal error
- 40002 — ImportJobFinishedWithTransientError: Import job finished with transient error
- 40003 — ImportJobStopped: Import job stopped
- 40004 — ImportJobSuccessfullyCompleted: Import job successfully completed
- 40005 — NoDataCaptured: No data captured
- 40006 — ComponentDeleted: Component deleted
- 40007 — ImporterDeleted: Importer deleted
- 40008 — ImporterMetricDeviationDetected: Importer metric deviation detected
- 40009 — ImporterMetricAnomalyDetected: Importer metric anomaly detected
- 40012 — ImportJobRunningTooLong: Import job running threshold exceeded
- 40013 — ImportJobCompletedWithFailure: Import job completed with failure
- 40014 — ImporterDataDeleted: Importer data deleted

Configuring Microsoft Teams Notifications

Microsoft Teams notifications let you deliver event notifications to a Microsoft Teams channel. Notifications are posted as Adaptive Cards through a Microsoft Power Automate (Workflows) endpoint, so you do not need to register an application in Microsoft Entra ID.

Creating the Teams workflow

Before configuring Arctera Capture, create a workflow in Microsoft Teams to generate the endpoint URL:

1. In Microsoft Teams, open the **Workflows** app.

2. Create a workflow that posts to a channel when a webhook request is received, and select the specific **Team** and **Channel** where notifications should be posted.
3. Copy the generated HTTP POST URL. This is the **Teams Workflow URL** used in the notification configuration.

> **Note:** As a best practice, create the workflow under a **service account** so that the notification stream continues to work if the employee who created it leaves the organization.

Configuring the notification in Arctera Capture

1. In the **Event Subscriptions** section, open the Microsoft Teams notification settings.
2. Paste the **Teams Workflow URL** into the dedicated field. The URL must originate from the `logic.azure.com` domain; other URLs are rejected.
3. Click **Test Connection** to send a **System Test** Adaptive Card to the configured channel and confirm that the connection works.
4. Save the configuration.

> **Note:** Anyone who has the Teams Workflow URL can post messages to the channel. Keep the URL confidential and rotate it if you suspect it has been compromised.

Managing the Subscriptions

To quickly find a specific subscription without scrolling:

1. Type a keyword related to the Event Type into the search bar.
2. Click **Search**. The list will filter to show only the Event subscriptions that match your keyword.

The table is organized into primary columns to help you identify the active subscriptions:

- **Event**: Displays the specific event (e.g. Import job finished with fatal error).
- **Importer Type**: Indicates the scope, showing either a specific Importer name or all the importers.
- **Receive In-App Notification**: Indicates whether in-app notification delivery is enabled for the subscription.
- **Webhook Push Notification**: Indicates whether webhook delivery is enabled for the subscription.

- **Actions**: Allows you to remove an event subscription. Click the Delete icon to open a confirmation pop-up window, then click **Yes** to finalize the removal.

If you have a large number of subscriptions, use the pagination tools located at the bottom of the section:

- Page navigation: Click the page numbers or arrows to move through multiple pages of events.
- Items per page: Use the drop-down menu to adjust how many subscriptions are displayed at once (5, 10, 20, or 50 items per page).

Audit Tracking

Changes to webhook push notification settings and subscription delivery methods are recorded in the **Reports** section under the **Audit** report type. This allows users to review configuration changes related to event subscriptions and notification delivery.

Notification Preferences

This section of the **Notification Center** displays the **Notification Preferences** page, where users can manage their in-app notifications for events.

The **Filtering** panel at the top allows users to search for specific event types using keywords.

Each event has a toggle switch, enabling users to turn notifications ON or OFF based on their preferences. Notifications will be received for the following events:

- Quarantine file: Triggered when a corrupt or incomplete file set is being quarantined.
- Failed to quarantine file: Triggered when the system is unable to quarantine a corrupt or incomplete file set.
- Monitored users skipped: Triggered when user/users is/are skipped due to thrown PaymentRequired or NotFound errors.
- Import job finished with fatal error: Triggered when an error causes the import pipeline to discontinue.
- Import job finished with transient error: Triggered when an error happens, but the import pipeline continues.
- Import job stopped: Triggered when the importer is stopped by a user. The user's name, email address and role are included in the event details.
- Import job successfully completed: Triggered when the importer processes all data successfully and delivers messages to the target without any errors.

- No data captured: Triggered when the importer does not capture any data. Even if any data is captured while it's not delivered to target, the notification will not be received.
- Component deleted: Triggered when the user deletes a component from the importer (source, filter, or target). The event details include the name and email address of the user who performed the deletion, as well as the names of the component and the importer.
- Importer deleted: Triggered when the importer is deleted. The event details include the name and email address of the user who performed the deletion, as well as the importer name, along with a list of all component names, if they were configured (source, filter(s), or target(s)). When an importer with configured component(s) is deleted, a Component deleted notification will be triggered separately for each deleted component as well.
- Importer metric deviation detected: Triggered when an importer metric deviates from its expected baseline value.
- Importer metric anomaly detected: Triggered when an anomaly is detected in an importer metric.
- Import job running threshold exceeded: Triggered when an import job has been running for more than the configured number of hours. The threshold (in hours) is configurable when enabling this notification, and only one notification is sent per period once the job exceeds the configured threshold.
- Import job completed with failure: Triggered when the system detects that the import job was stuck in an abnormal state and returns it to a normal state.
- Importer data deleted: Triggered when a user deletes importer data. The event details include the name and email address of the user who performed the action, the importer name, and whether the child components' data was also deleted.

Notifications

This screen shows the **Notifications** section of the **Notification Center** where users can view and manage their notifications displayed from newest to oldest.

Notifications are classified into the following severity types:

- Info: Indicates general status updates.
- Success: Indicates successful operations.
- Warning: Highlights non-critical issues that may require attention, such as skipped tasks or minor configuration problems.

- Failure: Marks critical issues or failures that require immediate intervention, such as system errors, file parsing issues, or connectivity problems.

The following actions can be performed:

1. **Mark as Read** for individual notifications by clicking the eye icon.
2. **Mark All as Read** for all notifications by clicking the corresponding button.
3. **Refresh Data** updates the notification list without refreshing the entire page.

There are filtering options, allowing users to narrow notifications by:

- **Type** – includes Read/Unread, Failure, Warning, Info and Success
- **Source** – includes System and Importer
- **Date Range** – before and after dates can be specified
- **Component** - includes Importers, Collectors, Filters, and Targets.

REPORTS

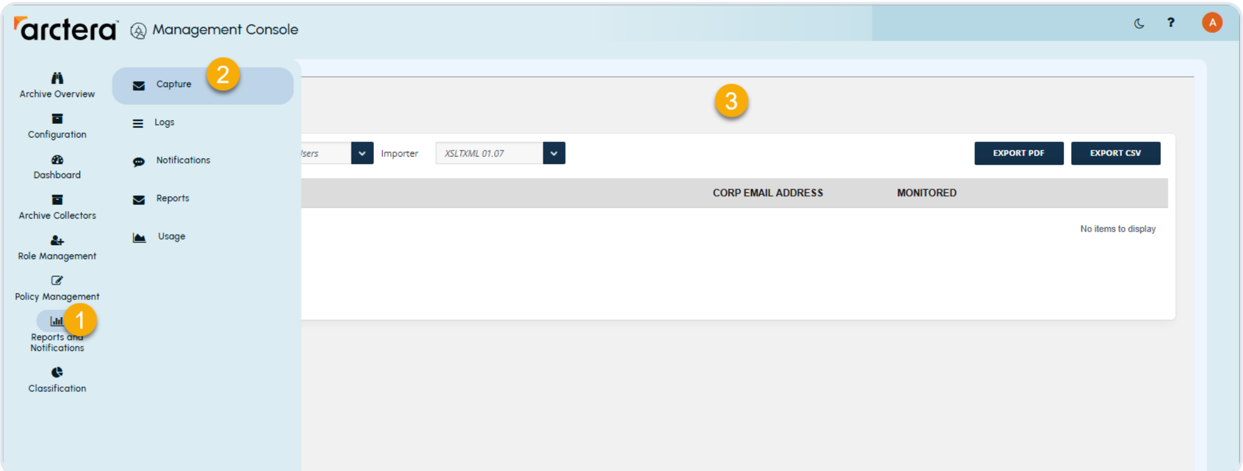
This section includes the following topics:

- Overview
- Managing Reports
- Audit
- Unprocessed Messages
- Target Delivery Failure
- Missing Attachment Failure
- Missing Disclaimer Failure
- Data Acquisition Failure
- Notes

Overview

To view and extract detailed information about the Capture user activity and delivery failures:

1. Go to **Reports and Notifications** in the Navigation pane(1).
2. Expand **Reports** and click **Capture**(2).



The following report types are available:

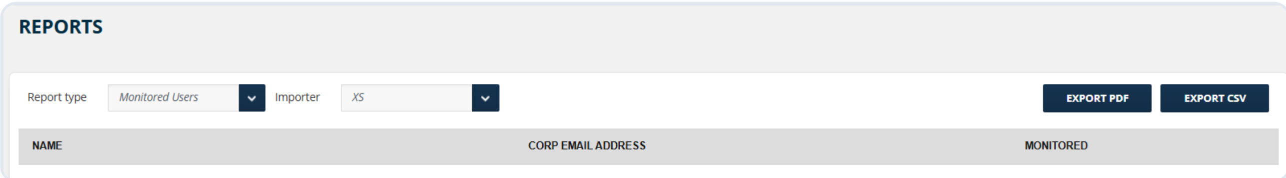
- **Audit**: View Arctera Capture user activity.
- **Monitored Users**: View monitored users by Capture.

- **Unprocessed Messages**: View unprocessed messages.
- **Target Delivery Failure**: View all failed attempts to deliver data.
- **Missing Attachment Failure**: View all failed messages with missing attachments.
- **Missing Disclaimer Failure**: View all failed messages with missing disclaimers.
- **Data Acquisition Failure**: View all failed messages with failed data acquisitions.

Managing Reports

After selecting the report type, choose the collector type and which reports you would like to review. You can export the report information either in a PDF or CSV format.

For **Audit** and **Monitored Users** reports data can be exported as a PDF or CSV file when clicking **Export PDF** or **Export CSV** correspondingly.



The **Target Delivery Failure**, **Missing Attachment Failure**, **Missing Disclaimer Failure**, and **Data Acquisition Failure** reports have actions.

There are the following **Reprocessing Options** when we click **Actions**:

- **Retry processing** - Retries failed messages processing when the importer is run.
- **Force processing** - Processes the failed messages when the importer is run and delivers them to the target without missing data.
- **Delete failed messages** - Deletes failed messages from DB.
- **Skip** - Does not process failed messages when the importer is running.

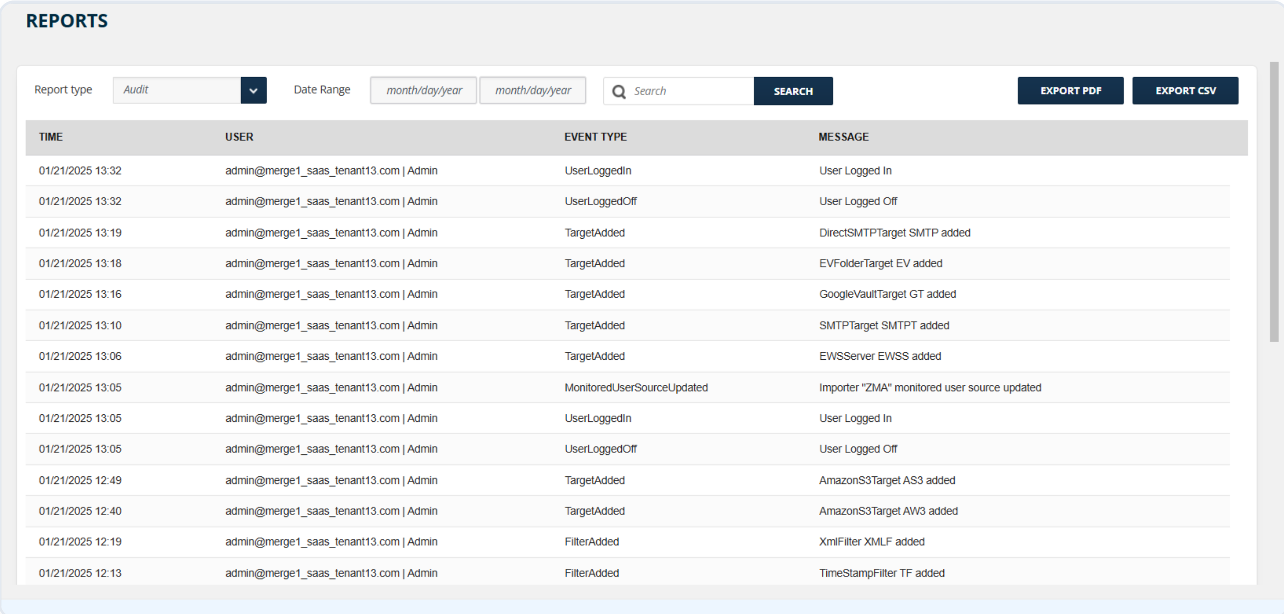
After selecting the reprocessing option, click **Apply**. The configuration will be applied to the data stored in DB. Click **OK** to close the pop-up window.

> **Warning:** The Reprocessing Options are applied in pairs with the **Importer Settings** > **Processing** > **Processing Options**, i.e., Processing Options should also be configured, so the Reprocessing Options configuration is applied properly.

> By default, the Reprocessing option is Retry processing: if not configured by the user, there will be retries with each session to process the failed messages until data reprocessing is succeeded.

Audit

Many important actions that users make such as logging in or configuring importers, are listed in Audit.



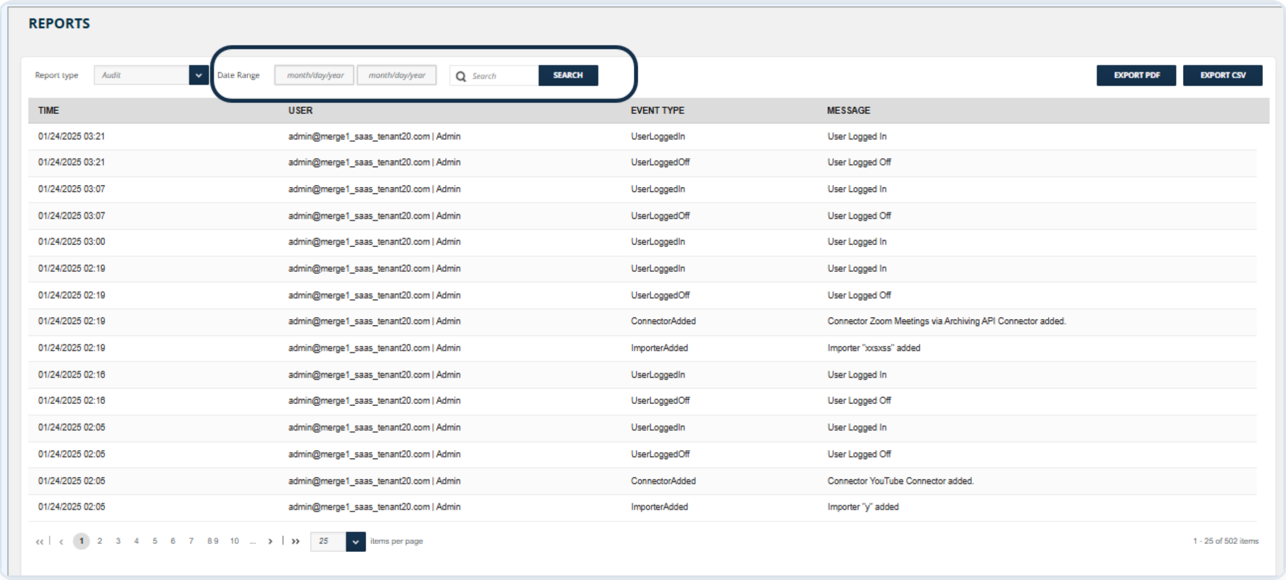
TIME	USER	EVENT TYPE	MESSAGE
01/21/2025 13:32	admin@merge1_saas_tenant13.com | Admin	UserLoggedIn	User Logged In
01/21/2025 13:32	admin@merge1_saas_tenant13.com | Admin	UserLoggedOff	User Logged Off
01/21/2025 13:19	admin@merge1_saas_tenant13.com | Admin	TargetAdded	DirectSMTPTarget SMTP added
01/21/2025 13:18	admin@merge1_saas_tenant13.com | Admin	TargetAdded	EVFolderTarget EV added
01/21/2025 13:16	admin@merge1_saas_tenant13.com | Admin	TargetAdded	GoogleVaultTarget GT added
01/21/2025 13:10	admin@merge1_saas_tenant13.com | Admin	TargetAdded	SMTPTarget SMTPT added
01/21/2025 13:06	admin@merge1_saas_tenant13.com | Admin	TargetAdded	EWSServer EWSS added
01/21/2025 13:05	admin@merge1_saas_tenant13.com | Admin	MonitoredUserSourceUpdated	Importer "ZMA" monitored user source updated
01/21/2025 13:05	admin@merge1_saas_tenant13.com | Admin	UserLoggedIn	User Logged In
01/21/2025 13:05	admin@merge1_saas_tenant13.com | Admin	UserLoggedOff	User Logged Off
01/21/2025 12:49	admin@merge1_saas_tenant13.com | Admin	TargetAdded	AmazonS3Target AS3 added
01/21/2025 12:40	admin@merge1_saas_tenant13.com | Admin	TargetAdded	AmazonS3Target AW3 added
01/21/2025 12:19	admin@merge1_saas_tenant13.com | Admin	FilterAdded	XmlFilter XMLF added
01/21/2025 12:13	admin@merge1_saas_tenant13.com | Admin	FilterAdded	TimeStampFilter TF added

The following event types are captured:

- UserLoggedIn
- UserLoggedOff
- UserUpdatedProfileInfo
- ImporterAdded
- ConnectorAdded
- FilterAdded
- TargetAdded
- ComponentSettingsModified
- ComponentRenamed
- ImporterRemoved
- ConnectorRemoved
- FilterRemoved

- TargetRemoved
- ImporterCloned
- ConnectorCloned
- FilterCloned
- TargetCloned
- MonitoredUserSourceUpdated
- ImportJobQueued
- ImportJobCanceled
- ImporterSchedulerEnabled
- ImporterSchedulerDisabled
- ImporterScheduledRunSkipped
- AutomationRestartTriggered
- AutomationChainTriggered
- TenantEventSubscriptionCreated
- TenantEventSubscriptionDeleted
- TenantEventSubscriptionNotificationTypeChanged
- TenantNotificationSettingsChanged

The filtering option allows filtering out the list of records from the section using the date range filter and the search functionality.



TIME	USER	EVENT TYPE	MESSAGE
01/24/2025 03:21	admin@merge1_saas_tenant20.com | Admin	UserLoggedIn	User Logged In
01/24/2025 03:21	admin@merge1_saas_tenant20.com | Admin	UserLoggedOff	User Logged Off
01/24/2025 03:07	admin@merge1_saas_tenant20.com | Admin	UserLoggedIn	User Logged In
01/24/2025 03:07	admin@merge1_saas_tenant20.com | Admin	UserLoggedOff	User Logged Off
01/24/2025 03:00	admin@merge1_saas_tenant20.com | Admin	UserLoggedIn	User Logged In
01/24/2025 02:19	admin@merge1_saas_tenant20.com | Admin	UserLoggedIn	User Logged In
01/24/2025 02:19	admin@merge1_saas_tenant20.com | Admin	UserLoggedOff	User Logged Off
01/24/2025 02:19	admin@merge1_saas_tenant20.com | Admin	ConnectorAdded	Connector Zoom Meetings via Archiving API Connector added.
01/24/2025 02:19	admin@merge1_saas_tenant20.com | Admin	ImporterAdded	Importer "xxsxss" added
01/24/2025 02:16	admin@merge1_saas_tenant20.com | Admin	UserLoggedIn	User Logged In
01/24/2025 02:16	admin@merge1_saas_tenant20.com | Admin	UserLoggedOff	User Logged Off
01/24/2025 02:05	admin@merge1_saas_tenant20.com | Admin	UserLoggedIn	User Logged In
01/24/2025 02:05	admin@merge1_saas_tenant20.com | Admin	UserLoggedOff	User Logged Off
01/24/2025 02:05	admin@merge1_saas_tenant20.com | Admin	ConnectorAdded	Connector YouTube Connector added.
01/24/2025 02:05	admin@merge1_saas_tenant20.com | Admin	ImporterAdded	Importer "y" added

Unprocessed Messages

The Unprocessed Messages report generates information on messages which have been constructed and stored in the database, but there hasn't been an attempt to be sent to the target. Unprocessed messages are reported when:

- A running importer is stopped.
- An importer is force killed before the messages are sent to the target.

> **Note:** To process the unprocessed messages, the **Processing Options** of **Importer Settings** should be configured.

Target Delivery Failure

This report type generates information on messages which are constructed and stored in the database - there is an attempt to send them to the target, but the attempt is failed. Target delivery failures are reported when:

- The target is configured with invalid credentials.
- The selected target has size limits and there has been an attempt to send larger sizes of messages. Specifically, the SMTP target has size limits and if the messages' size limits exceed the target specified limit, the delivery of the messages to the target will fail.
- A target has insufficient storage.
- A target is overloaded.
- A network connectivity issue occurs.
- A target delivery has failed for some other reasons.

Missing Attachment Failure

For collectors, such as Bloomberg or Symphony, there is an option to fail messages with missing attachments in the **Attachment Validation** sub-section when configuring **Source**.

Information on failed messages with missing attachments is reflected in the Missing Attachment Failure report.

Missing Disclaimer Failure

For collectors, such as Bloomberg, there is an option to fail messages with missing disclaimers in the **Disclaimer Validation** sub-section when configuring **Source**.

Information on failed messages with missing disclaimers is reflected in the Missing Disclaimer Failure report.

Data Acquisition Failure

When Arctera Capture captures data that is incomplete or damaged, information on the data will be reflected in the Data Acquisition Failure report in case a report is generated.

Initially, this report has been constructed for the Viva Engage (Yammer) collector. According to the configuration, the collector gets a date range, which is divided into chunks (a chunk is one hour) and starts exporting the chunks separately in ZIP files. The ZIP file may or may not contain data depending on the activity that occurred in the Viva Engage (Yammer) communication for the specific hour. Data processing in a chunk (the whole ZIP file export) are reported when:

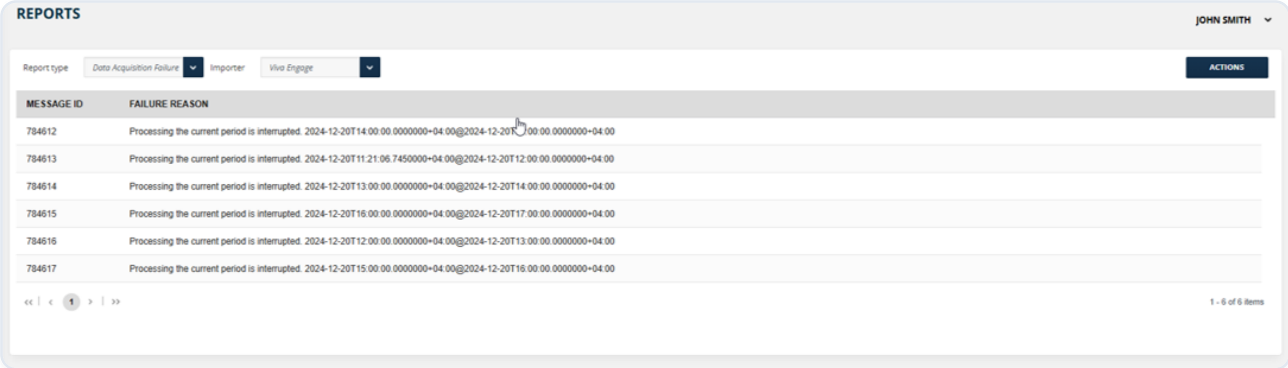
- The download fails, and data processing remains incomplete.
- The download is successful but there has been a column added in the CSV file while no updates have been made on our side.
- An attachment has been added to a file while it is not included in the ZIP file.

When the data processing failure occurs, an output message is constructed. The body of the message contains the start and end dates (separated with ":") of the processing data (chunk), and the failure type is mentioned as Data Acquisition Failure.

When the data processing failure occurs, an output message is constructed. The body of the message contains the start and end dates (separated with ":") of the processing data (chunk), and the failure type is mentioned as Data Acquisition Failure.

When Arctera Capture starts running next time and is set up to process the failed messages, the messages (chunks) will be queued to be partially processed (DoPartialProcess for the collector). The body is split into 2 parts - start and end date, by which a range (chunk) is created to reprocess.

The log file reflects information on generated data in the form of messages, while those messages are the chunks, which may or may not contain messages.



Notes

- In the RingCentral collector, data processing also occurs in ranges, however, when a range (chunk) is failed, it is not considered a Data Acquisition Failure: the information is only logged.
- In the Workplace from Facebook collector, the Data Acquisition Failure report information is generated differently. Specifically, Capture messages are generated from the data stream. When a message is not processed for some reasons (e.g., the message contains a new body type, the attachment is missing, or the participant list is absent) the data is stored in the Capture DB as a message with the available data (such as from, time, body, subject and more) and the status is specified as Data Acquisition Failure. In this case, the quantity of Data Acquisition Failure messages is equivalent to the number of Unprocessed Messages.
- Only the Viva Engage (Yammer) collector has a reprocessing functionality. Before reprocessing occurs, the failed range (chunk) is deleted from DB. When the range fails again, the record is created again and stored in DB.

APPENDIX

This section includes the following topics:

Creating a Certificate (Private and Public Keys)

For private key:

1. Go to the Start menu & click **Administrative Tools** > **Internet Information Services (IIS) Manager** and click the server's name in the Connections column on the left and double click **Server Certificates**.
2. Click **Create Self-Signed Certificate** in the Actions column on the right.
3. Type any meaningful name and then click **OK** to proceed.

Once that is complete, you should now see the SSL in the list of Self-Signed certificates. Now, you have IIS Self-Signed Certificate with 1 year validation.

1. Right-click on that certificate and click **Export**.

Specify the path, type the password, confirm the password, and click **OK**. Now, you have exported the Private key.

For public key:

1. Launch Microsoft Management Console. Press Win+R, type `mmc.exe` and click **OK**.
2. Click **File** and select the **Add/Remove Snap-in** option.
3. Click **Certificates** in the list of Available snap-ins and then click **Add**.
4. Select **Computer account** and click **Next**. Choose **Local Computer** and click **Finish**.
5. Click **OK** to add the certificate snap-in and get back to console.
6. Expand the Personal folder in the left-side menu and choose **Certificates**.
7. Right-click the certificate you want to export - **All Tasks** > **Export**.
8. On the prompt menu, click **Next**.
9. Click **No**. Do not export the private key.
10. Choose **Base-64 encoded X.509 (.CER)** and click **Next**.

11. Fill in the file path and click **Next**.
12. Click **Finish** and now you have the Public key.