User Guide

Arctera Mergel

Version 7.0.2604

CONTENTS

Document Version Control

This section includes:

April 06, 2026

The changes are represented in the table below:

Chapter/Section	Changes
Notifications > Webhook Push Notification	Added instructions for configuring Webhook Push Notifications.
Notifications > Event Subscriptions	Added guidance for managing notification type(s) via the Event Subscriptions section.
Job Monitoring	Outlined the new button for importer details.
Zoom Meetings	Added new notification events.
IceChat	Added an optional "Use corporate email" setting for internal users

March 02, 2026

The changes are represented in the table below:

Chapter/Section	Changes
Importers	Updated the section screenshots.
Importer Settings > Processing	Added a new functionality to the section.
Citrix Workspace & ShareFile	Added new notification events.
Zoom Chat	Added new notification events.
Box	Added new notification events.
Audio Video	Added a new configuration option to the Source.
Text-Delimited	Added a new configuration option to the Source.

Dashboard	Added a new widget to the section.

February 02, 2026

The changes are represented in the table below:

Chapter/Section	Changes
FX Connect	Added new notification events.
Cisco Webex Teams	Added new notification events.
Dropbox Business	Added new notification events.
SharePoint	Added a new configuration option to the Source.
ChatGPT	Added a new configuration option to the Source.
Database Configuration	Added a note.
Notifications	Added a new functionality to the section. Updated the entire section.

January 05, 2026

The changes are represented in the table below:

Chapter/Section	Changes
Component Descriptions	Added a new description section.
ChatGPT	Added a new collector.
Google Messages	Added a new collector.
Bloomberg	Added a new configuration section to the Source.
IceChat	Added a new configuration section to the Source.
Dubber Speik Recordings	Added three new notification events.
Dubber Speik SMS	Added three new notification events.
OneDrive for Business	Added three new notification events.
File-Based collectors	Added three new notification events.
SharePoint	Added three new notification events.
Azure Storage Source	Added a new configuration field.
Amazon S3 Target	Added a new configuration field.
Azure Blob Target	Added a new configuration field.

December 01, 2025

The changes are represented in the table below:

Chapter/Section	Changes
Copilot	Added notes to the Activities Captured section.
IceChat	Added a new checkbox to the Source configuration.
Bloomberg	Added a new captured activity.
Zoom Chat	Added a new captured activity.
Cisco Webex Teams	Updated the permission scopes required for application creation.
AmazonS3 Source	Added a new configuration field.
Job Monitoring	Added new metadata to the Job Monitoring Executions Information tab.
Notifications	Updated the Notification Preferences section.
All collectors	Added a new Supported Notifications section to all collectors.

November 03, 2025

The changes are represented in the table below:

Chapter/Section	Changes
FX Connect (File-Based)	Added a new collector.
Verba	Added a new configuration field.
Copilot	Added a new configuration section.
Zoom Phone	Added a new configuration section.
IceChat	Added a new configuration section.

October 06, 2025

The changes are represented in the table below:

Chapter/Section	Changes
Zoom Phone	Added a new collector.
Copilot	Updated the section.
Reporting & Message Tracking	Updated the section.

September 01, 2025

The changes are represented in the table below:

Chapter/Section	Changes
Zoom Chat	Added a new captured activity.

Dubber Speik Recordings	Added a new configuration section.
Microsoft Teams via Export API	Added an important note to the collector configuration.
File-Based Collectors	Added a note regarding volume and size limits of downloaded files.

August 04, 2025

The changes are represented in the table below:

Chapter/Section	Changes
Microsoft Teams via Export API	Added footnotes highlighting two known issues related to captured activities.
Microsoft Teams via Export API	Added a new checkbox to the Source configuration.
Zoom Chat	Added new captured activities.
Dashboard	Added a new performance metric to the Importer Jobs widget within the Dashboard.
Job Monitoring	Added status indicators to the Executions tab to reflect job completion states.

July 07, 2025

The changes are represented in the table below:

Chapter/Section	Changes
Cloud9	Added a new collector.
Verba	Added a new collector.
Viva Engage (Yammer)	Updated the Microsoft Entra ID application creation section.
SMTP Target	Added a new configuration field.
Zoom Chat	Added new captured activities.

June 02, 2025

The changes are represented in the table below:

Chapter/Section	Changes
Dashboard | Importer Jobs	Added a new column to the Importer Jobs widget.
Microsoft Teams via Export API	Added a new drop-down list to the Source Configuration Wizard.
Zoom Chat | Activities Captured	Added a new captured activity.
Zoom Chat | Creating a Zoom App	Added a new scope.

May 05, 2025

The changes are represented in the table below:

Chapter/Section	Changes
Text-Delimited	Added a new checkbox.

CHAPTER 1

Welcome to Merge1

This chapter represents:

- General Overview
- Component Descriptions
- System Requirements

General Overview

Merge1 aids financial service firms in complying with Sec Rule 17a-4, 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. Merge1 offers compatibility with Microsoft Exchange, Microsoft Office 365, and many other applications.

Merge1 is an internal cloud computing environment that is deployed and administered within a private network. Internal cloud environments can be utilized anywhere within the same network by several people on multiple machines simultaneously while demanding very few system resources.

Note

Merge1 collectors are designed for scheduled collection runs. While they can be used to discover older data, they are not suitable for large data migration tasks. The platform is not designed to be a migration tool with long-term migration tasks and monitoring/reconciliation/reporting features. Running tasks for extended periods of time increases the risk of unsuccessful completion.

Component Descriptions

Merge1 Portal

The **Merge1 Portal** is a web-based unified management interface that provides administrators with total visibility into the communication archive process. From this centralized console, users can configure source collectors, manage global settings, and monitor the real-time status of all active data capture jobs.

Key Responsibilities:

- **Source Configuration:** Setting up collectors (e.g.. Slack eDiscovery, OneDrive for Business, Copilot) by inputting API keys and credentials.
- **User Management:** Assigning roles (Administrator vs. Reviewer) and defining which users' data should be captured.
- **Filter Management:** Refining the data stream by applying criteria such as data size limits, file types, and keyword exclusions to ensure only relevant content is archived.
- **Target Configuration:** Mapping captured data to its final destination, such as EWS Server, Google Vault, or an SMTP endpoint, to ensure secure and compliant ingestion.
- **Performance Visualization:** Providing real-time visibility into whether data sources are capturing data successfully or if any tasks are failing.

Merge1 Agent

The **Merge1 Agent** is the **distributed execution engine** of the system, functioning as a dedicated service that manages the operational data lifecycle initiated by the Portal. Serving as the system's processing layer, the Agent executes the resource-intensive data capture, transformation, and delivery tasks defined within the centralized administrative console.

Key Responsibilities:

- **Data Extraction:** Establishing secure connections to content source APIs (e.g.. Slack, Teams) to retrieve raw communication data.
- **Data Transformation:** Structuring and converting raw metadata into standardized, archive-ready formats (such as EML files).
- **Data Delivery (Ingestion):** Transferring processed datasets to the configured target repository for final archival.
- **Operational Scalability:** Supporting high-volume environments through the deployment of Agent Pools to facilitate load-balancing and high availability.

System Requirements

Minimum Hardware Requirements

- 2.4 GHz 64-bit quad-core processor
- 16 GB RAM
- 1 GB hard-disk space

Having more processor cores will ensure adequate performance.

Software Requirements

For Merge1 Web Servers:

- Internet Information Services 8.0 or higher
- SQL Server 2016 or higher
- .NET Framework 4.8

For Merge1 Agent Servers:

- .NET 8.0 Runtime
- ASP.NET Core 8.0 Runtime

Consult the latest version of the Merge1 Compatibility Chart for information on all supported components including OS and SQL available at https://www.veritas.com/support/en_US/doc/Merge1_7.0_CompatibilityCharts.

Important

- Merge1 Web Services and Agent VM must be in the same time zone.
- Any path used for Merge1 should be visible to the Agent.
- The SQL server should be accessible from the Agent server.

CHAPTER 2

Getting Started

This chapter represents:

- Preinstallation Checklist
- Preinstallation Steps
- Installation

Preinstallation Checklist

Merge1 uses port 443 on the host machine for network distribution as well as OAuth pull calls to ensure that it is not occupied by another application. The default ports used for SSH key authentication by Bloomberg is 30206 and for IceChat and Redtail Speak is 22. The default FTP port for any Source is 21. Microsoft Internet Explorer versions 8 and below will not properly display some elements of the user interface and should not be used. Merge1 will never prompt you to update your browser.

Ensure that all the hardware and software requirements are met:

- 2.4 GHz or faster quad-core processor with at least 16 GB RAM and 1 GB hard-disk space
- Windows Server 2016 or later, x64-based
- Internet Information Services 8.0 or higher (see **Installing Internet Information Services**)
- SQL Server 2016 or later
- .NET Framework 4.8 (see **Verifying .Net Framework Requirements**)
- .NET 8.0 Runtime for Merge1 Agent servers
- ASP.NET Core 8.0 Runtime for Merge1 Agent servers

Consult the latest version of the Merge1 Compatibility List, available at https://www.veritas.com/support/en_US/doc/Merge1_7.0_CompatibilityCharts, for information on all supported components, including OS and SQL.

Ensure that all relevant Target requirements are met:

- Arctera Enterprise Vault 12.1 up to 15.0
- Enterprise Vault API Runtime 12 or 15 (on the Merge1 host)
- Microsoft Exchange Server 2007 SP1, 2010 (GA – SP3), 2013, 2016, and 2019
- Microsoft Exchange Server 2003, 2007, 2010, 2013, 2016, and 2019

SQL Configuration

If the Database Administrator wants to specify the location for **Database Log** and **Data files**, they can prepare the database in advance by following these steps:

1. Create a new database where the files will be stored.
2. Inside the newly created database, add a **Data File Group** named **`LargeDataFileGroup`**. This ensures that the Merge1 Database Initialization script detects the existence of a file group with this name and uses it instead of creating a new one.

By setting up the **`LargeDataFileGroup`** in advance, you can control the location of the database files and align with your organization's storage policies.

Note

- You can acquire the username and password of the administrator account on the host machine.
- Make a note of the address and authentication parameters of the SQL server that will host Merge1's databases.
- Acquire an SSL certificate (see **Preinstallation Steps**).
- All processes, services, and folder paths (the installation path and paths specified in the collector settings) related to Merge1 should be added to the antivirus software's exclusion list if one is installed on the machine.

- To enable support for long file paths in Windows servers, add the following in Windows Registry:
    - Path: `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem`
    - Key: `LongPathsEnabled`
    - DWORD Value: `1`

Service Account Permissions

The service account used to run Merge1 should have the following permissions on the Merge1 server:

- Local Administrator (must be a member of the Administrators' group)
- Log on as Service rights
- Log on as a batch job right

Preinstallation Steps

Installing Internet Information Services

To install **Internet Information Services** on Windows Server 2016 and later versions:

1. Click **Start > Administrative Tools > Server Manager**.
2. On the left panel of the **Server Manager** dialog box, click **Roles**.

Option A: If IIS has not been enabled:

- Click **Add Roles** on the **Roles Summary** panel.
- Click **Next** and enable **Web Server (IIS)** on the list.
- Click **Next** and select **Role Services** on the left panel.

Option B: If IIS is already enabled, but not all required components have been enabled:

- Click **Add Role Services** in the **Web Server (IIS)** panel on the right.

3. On the **Select Role Services** dialog box, verify that the web server components listed below are enabled:

- Common HTTP Features
  - Default Document
  - Static Content
- Security
  - Basic Authentication
  - Request Filtering
  - Windows Authentication
- Application Development
  - All .NET Extensibility Components
  - All ASP.NET Components
  - ISAPI Extensions
  - ISAPI Filters
- Web Management Tools
  - IIS Management Console
  - IIS 6 Management Compatibility
  - Metabase and IIS 6 Configuration Compatibility
  - IIS Management Scripts and Tools
  - IIS Management Service

4. After enabling the required IIS components, click **Next > Install**.

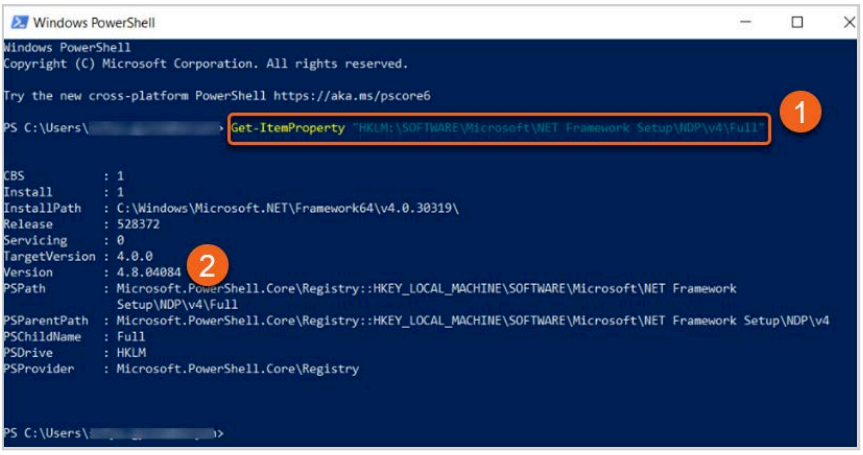
To enable **Internet Information Services**:

1. Open the **Control Panel** and click **Programs and Features > Turn Windows features on or off**.
2. Enable **Internet Information Services**.
3. Expand the **Internet Information Services** feature to verify the web server components listed below are enabled and click **OK**.

Verifying .Net Framework Requirements

Internet Information Services must be installed before installing .NET Framework 4.8 for all the necessary framework components.

To verify the .NET Framework version 4.8 open Windows PowerShell and enter the following command: `Get-ItemProperty "HKLM:\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full"`.

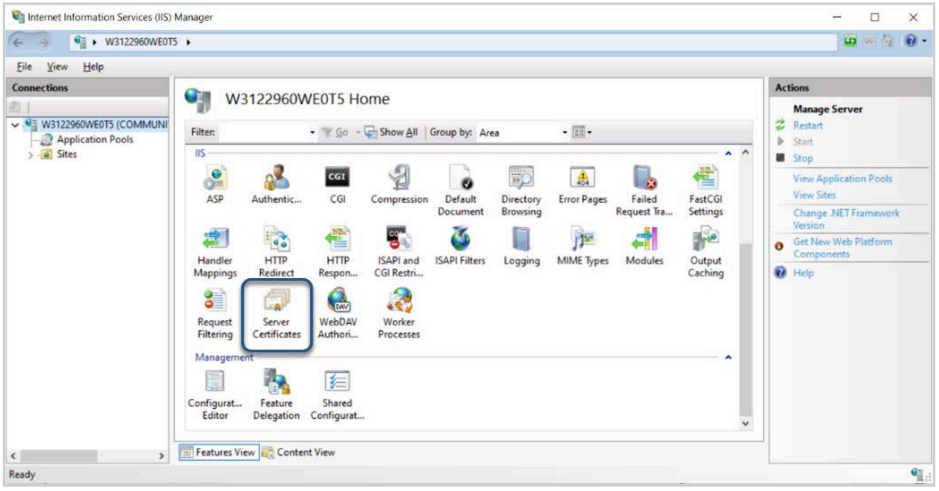


Application pools can be viewed in IIS Manager. If the .NET v4.8 and .NET v4.8 Classic application pools do not appear on the list, please reinstall or repair .NET Framework 4.8 after installing Internet Information Services.

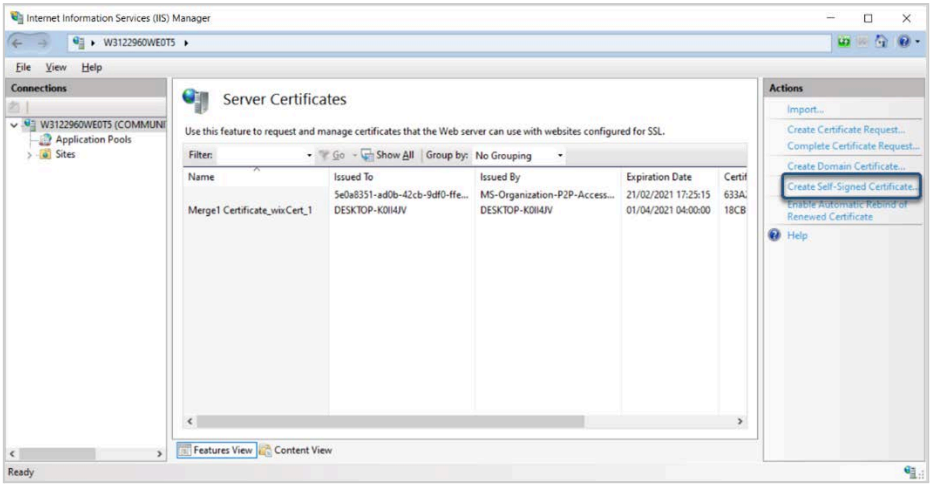
Creating a Self-Signed Certificate Using IIS

To create a self-signed certificate:

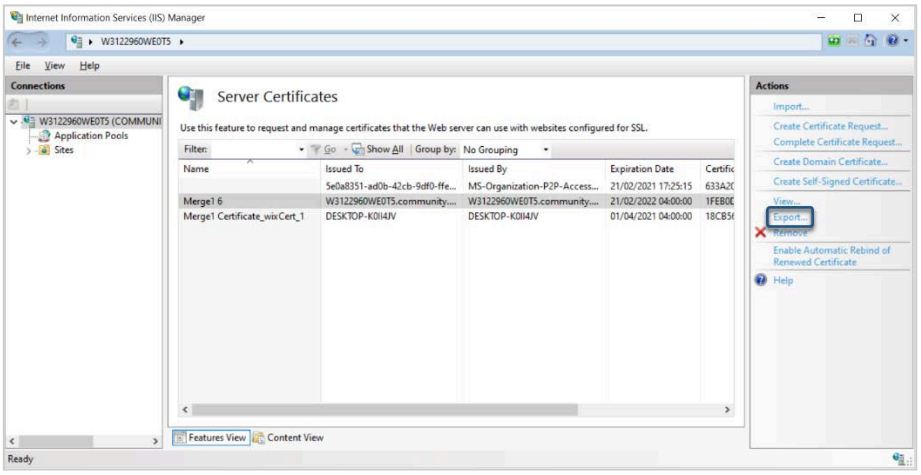
1. In **Internet Information Services (IIS) Manager**, click the name of the host machine in the **Connections** pane on the left, then double-click **Server Certificates**.



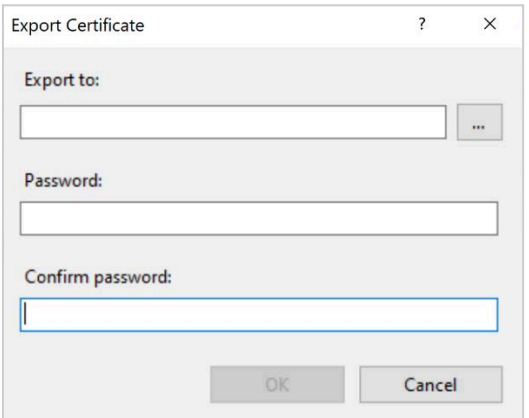
2. In the **Actions** column to the right, click **Create Self-Signed Certificate**.



3. Specify a name and click **OK** and on the next window, select your certificate from the list and click **Export** in the **Actions** column to the right.



4. Specify an export location and password, then click **OK**.



The certificate location and password must be provided when installing Merge1.

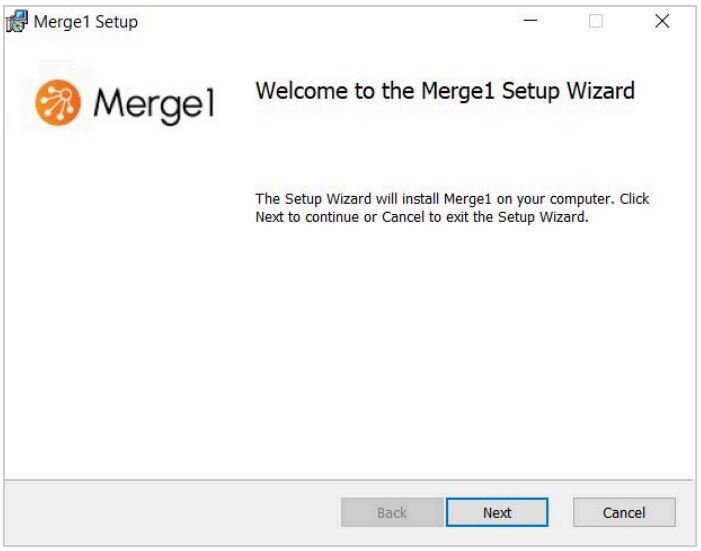
Installation

Starting with version 7.0, Merge1 has two installers - **Merge1 7.0 Setup** and **Merge1.Agent Setup** MSIs. Note that both should have the same version.

Merge1 Setup

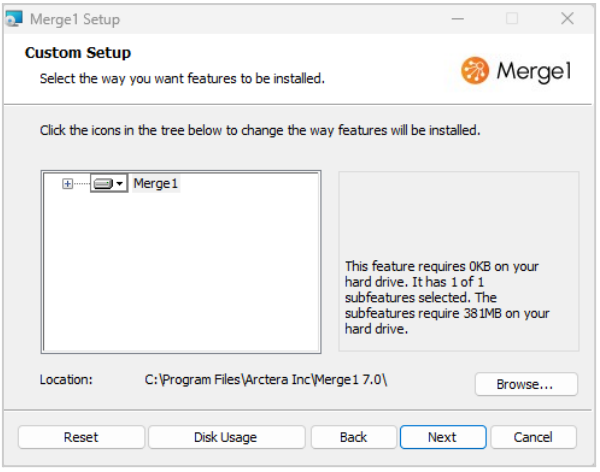
To install Merge1:

1. Run the **Merge1 7.0 Setup** installer with administrator permissions and click **Next**.

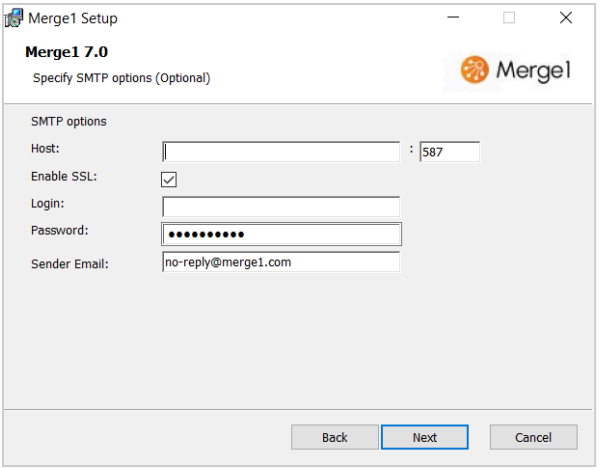


2. Read the **End-User License Agreement** and click **Accept**, which will activate once you scroll down.

3. Select the feature and click **Next**.

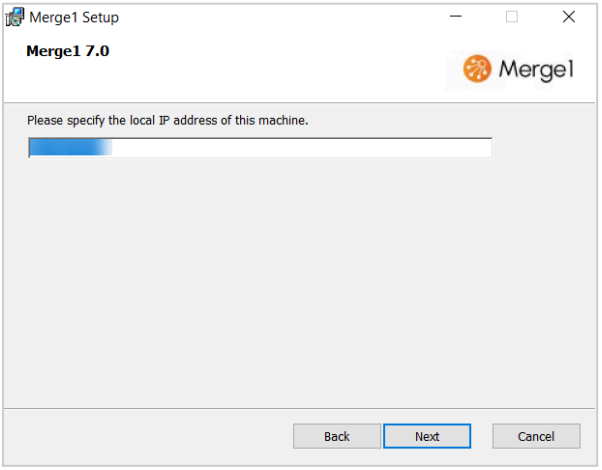


4. Specify the SMTP host and click **Next**.

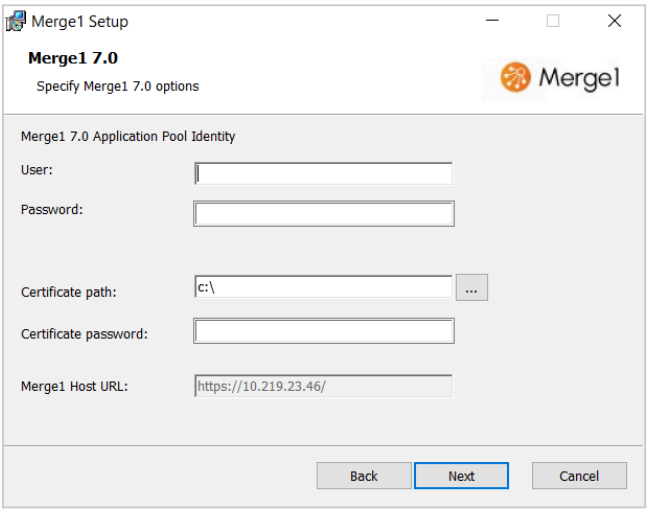


The **Sender Email** will appear in the **From** field when a confirmation email is sent to new users or when passwords are reset.

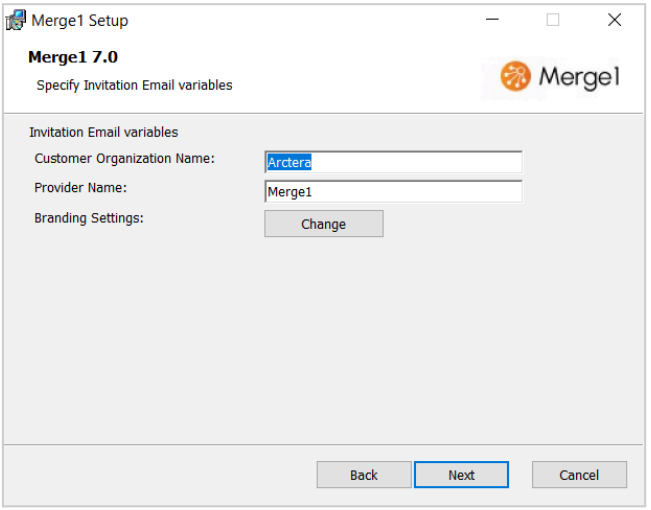
5. Click **Next.** Merge1 will automatically fetch the **Host IP**.



6. Enter the **Username** and **Password** of the administrator account of the host machine and specify the SSL certificate path and password. Save the **Host URL** - this UR is needed to access the Merge1 platform, then click **Next**.

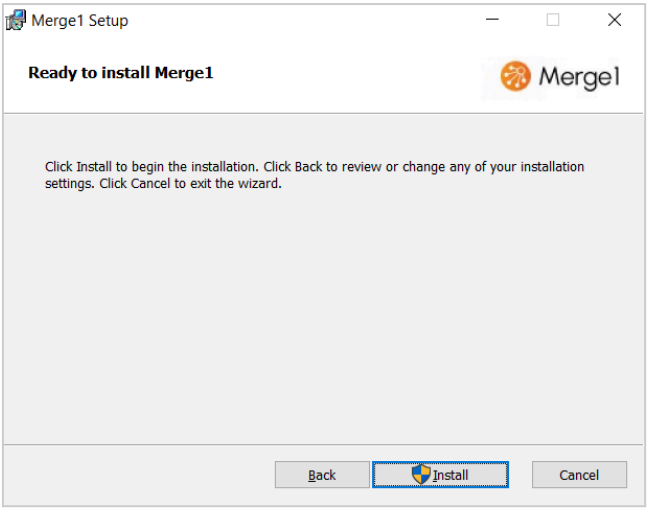


7. Enter the name of your organization and click **Next**.

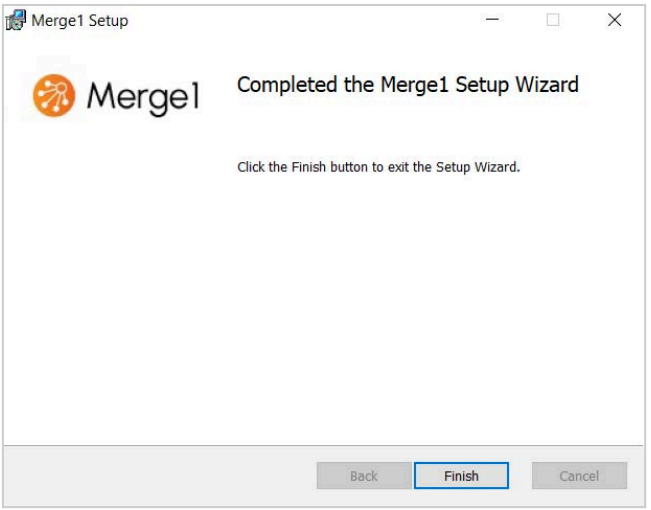


The **Provider Name** may be changed to assign a unique name to an environment (useful when multiple environments are deployed within the same network, i.e., Merge1 HR, Merge1 PR, etc.

8. Click **Install** to begin the installation. The installation window will open.



9. Click **Finish** to close the **Merge1 Setup** window.



You will have a 30-day free trial license period after the installation. Then, contact us to prolong the license.

After Merge1 installation, it is recommended to reset the IIS via PowerShell as an administrator.

Merge1 Upgrade

Before installing version 7.0 or later of Merge1, uninstall all previous versions released prior to version 6.21.2203.

Before the installation of a newer version:

- **In case your Merge1 version is earlier than 6.17.1129**:
    1. Uninstall it and install Merge1 v. 6.21.2203.
    2. Update the database.
    3. Upgrade the Merge1 version to 7.0.
- **In case your Merge1 version is between 6.17.1129 and 6.21.2202**:
    4. Upgrade Merge1 to 6.21.2203.

5. Update the database.
6. Upgrade the Merge1 version to 7.0.

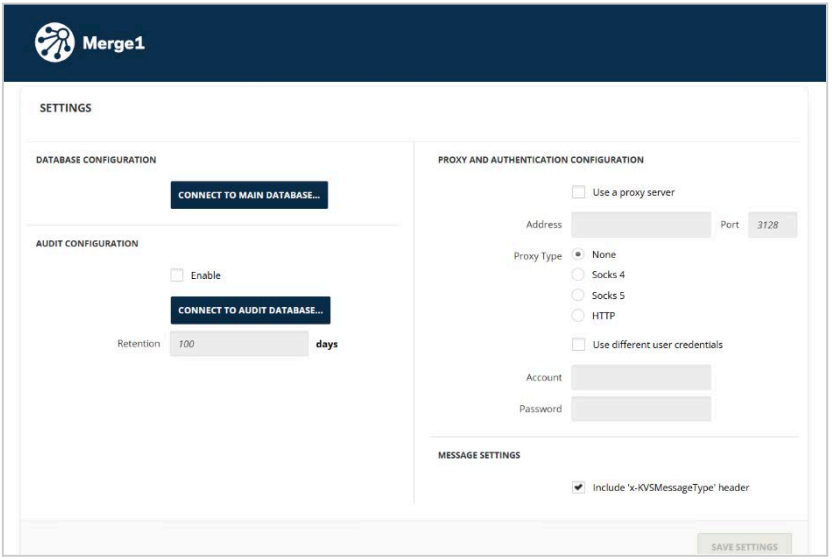
Merge1 Web Services Upgrade

To upgrade Merge1 Web Services:

1. Stop all collectors that are in progress. If they are importing, wait for them to finish the import and then stop them.
2. Take a backup of the Merge1 DB.
3. Take a snapshot from the Merge1 hosting VM.
4. Run the **Merge1 Installer** file.
5. Connect the same database if asked.

Database Configuration

To access the Merge1 portal, use the shortcut in the Start Menu or use the **Merge1 Host URL** from the installation wizard using a web browser of your choice. Merge1's configuration settings will appear.



Note

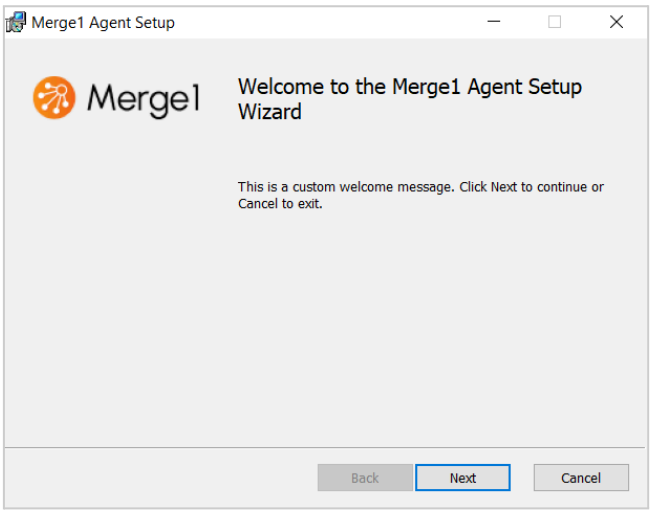
Never attempt to access or administer Merge1 using localhost as the URL because callback functions will not work properly, and critical errors may occur.

To manage database configuration, see **SETTINGS**.

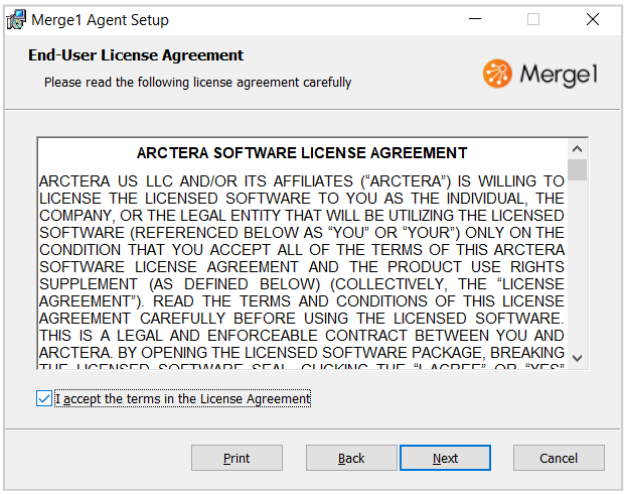
Merge1 Agent Setup

To install Merge1 Agent:

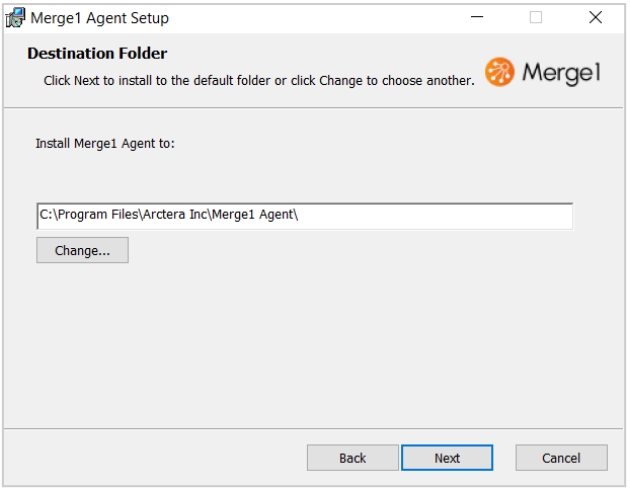
1. Run the Merge1 Agent installer and click **Next**.



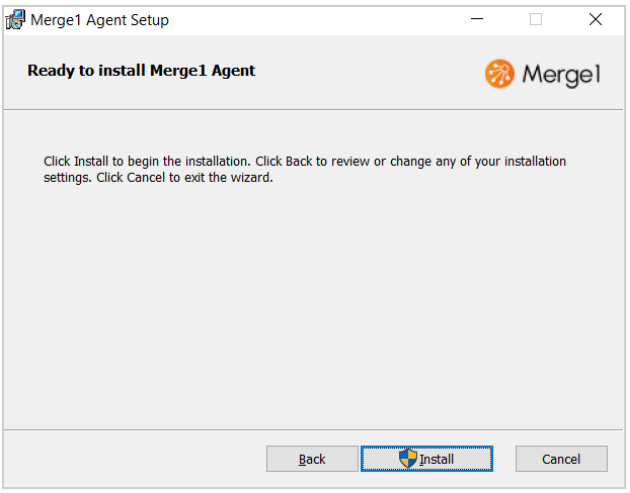
2. Read and accept the Arctera Software License Agreement by selecting *I accept the terms in the License Agreement*. Click **Next**.



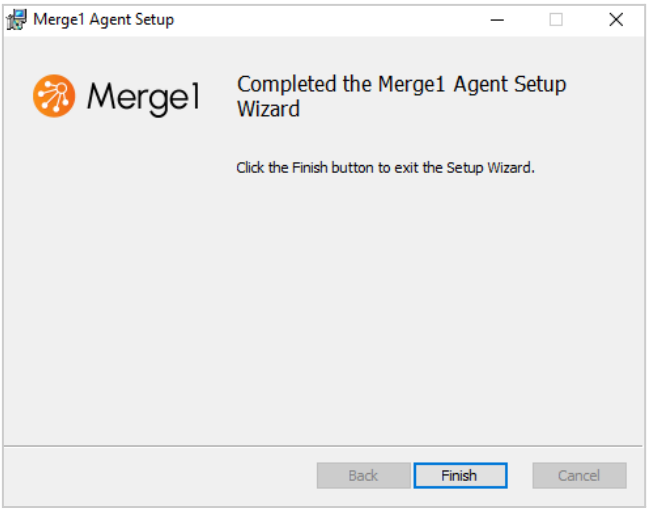
3. Click **Next** to install to the mentioned folder, or click **Change** to select a destination folder, then click **Next**.



4. Click **Install** to begin the installation. The installation window will open.



5. Click **Finish** to close the **Merge1 Agent Setup** window.

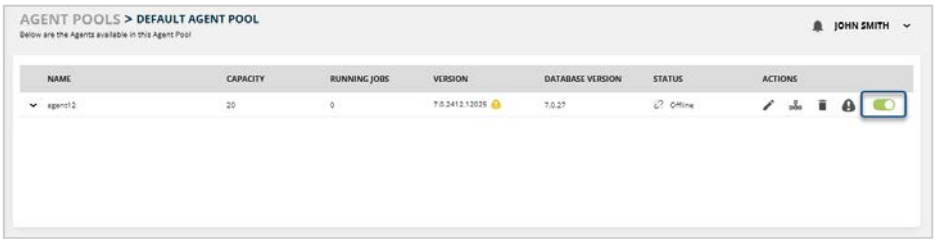


When the installation is completed, the Merge1 Agent folder will be in `C:\Program Files\Arctera Inc`.

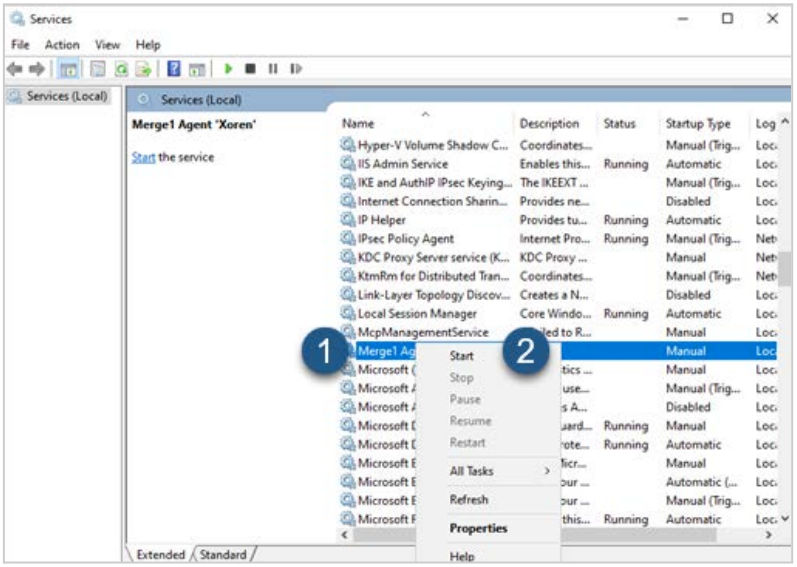
Merge1 Agent Upgrade

To upgrade Merge1 Agent:

1. Disable the agent.



2. Run the new Merge1 Agent installer.
3. Go to **Services** and turn on Merge1 Agent.



In case the database is not updated, the user will have to create a new database for Merge1 version 7.0.

Note

If the Merge1 Agent version is 7.0.2412 and below, before upgrading, ensure you:

1. Unregister all registered agents (see **Deleting/Unregistering an Agent**).
2. Uninstall the Merge1 Agent program.
3. Install the new version.
4. Register new agent(s) (see **Configuring an Agent via agentConfiguratorGUI.exe**).

CHAPTER 3

Navigating to Merge1

This chapter represents:

- Signing In
- Configuring the SSO Authentication
- Navigation Pane
- Account Settings

Signing In

The starting screen of Merge1 is the **Sign In** page. It serves as a gateway to viewing and modifying the data in the application.

To sign in to Merge1:

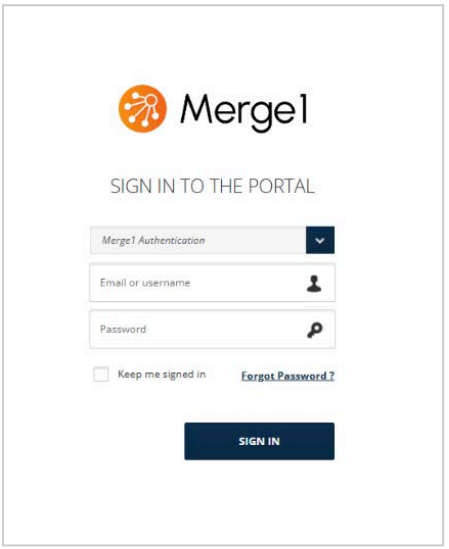
1. Navigate to the **Start Menu** shortcut to access the Merge1 portal.
   For enhanced security, it is recommended to disable spell-checking (also known as Writing Assistance in Microsoft Edge) in your web browser.
2. Select the **Authentication Method** from the drop-down list:
   - Merge1 Authentication
   - Windows Authentication
   - Single Sign-On with SAML 2.0

By default, only the **Merge1 Authentication** and **Windows Authentication** options are available as **Authentication Types** to select at the time of login. The Single Sign On (SSO) option will become visible in the drop-down list after **CONFIGURING THE SSO AUTHENTICATION**.

For **Merge1 Authentication**, sign in using the following credentials:

- Email: admin@merge1.com
- Password: a

The password should be changed after entering the temporary password.



For **Windows Authentication**, add an account from the domain where Merge1 is hosted. In the **Username** field, use the SAM account name.

- Username: exampledomain.com\admin
- Password: <user's password>.

To log in with Windows Authentication, you should have already selected an AD user. For more information, see **Select an AD User Account (Recommended per industry best practice)**.

The AD user must have login access to the Merge1 Server, to login into the Merge1 Portal using the Windows Authentication mode.

Windows authentication will be phased out on July 01, 2026. Before then, we recommend switching to Merge1 or SSO authentication.

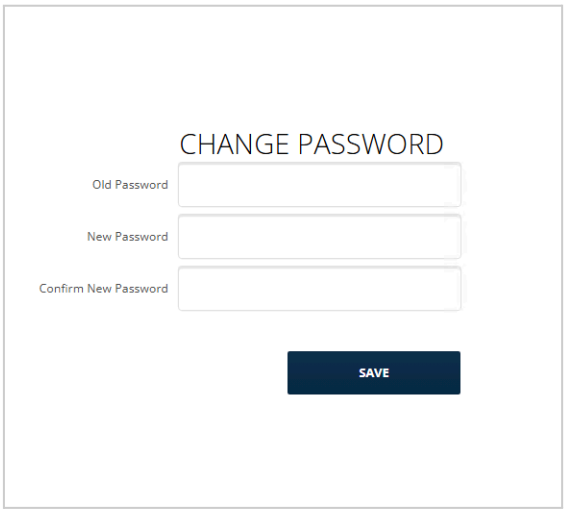
For **Single Sign-On with SAML 2.0**, see **CONFIGURING THE SSO AUTHENTICATION**.

Password Recovery

The system is designed to provide the functionality of retrieving user passwords in case of forgetting or for some other reason. Passwords are retrieved through the identification link sent to the user's email address in the user profile. When a user clicks the link in the email, the user identity will be verified, and an opportunity for defining a new password will be provided. Note that you CANNOT recover the password of admin@merge1.com.

To recover the user password:

1. Click the **Forgot Password** link in the **Sign-in** window.
2. Provide the email for signing in to the Merge1 account so that the recovery link is sent to this address.



3. Check your email and click the recovery link.
4. Provide a new password and re-enter it for verification.

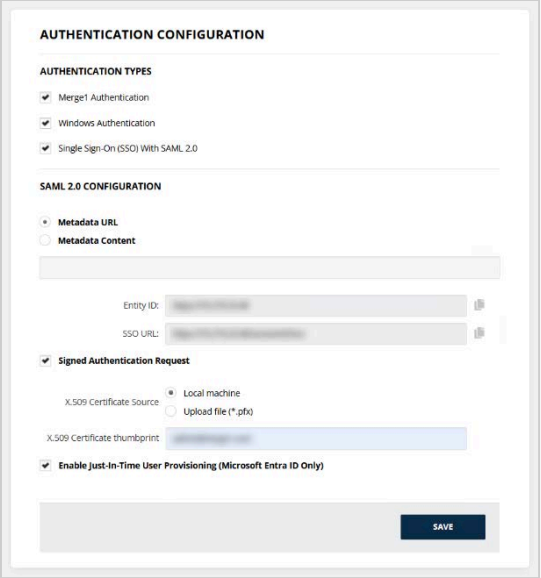
Password requirements:

- Minimum length of 12 characters.
- Combination of upper and lowercase letters, numbers, and symbols.

Upon logging in for the first time, navigate to the **Licensing** section for licensing (see **LICENSING**).

Configuring the SSO Authentication

This section describes managing Merge1 authentication types.



Below are all the steps for configuring Okta (IDP) and Microsoft Entra ID Application, but you can use any Identity provider's service that supports SAML 2.0.

Configuring SSO Authentication via Microsoft Entra ID Application

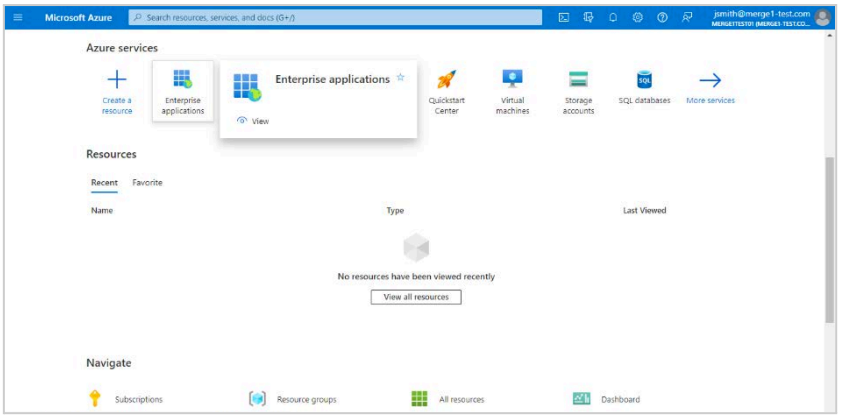
To configure the SSO authentication via Microsoft Entra ID, the admin should:

1. Create an enterprise application.
2. Assign the application to a user.
3. Obtain the **Metadata URL value**.
   Or,
4. Obtain the **Metadata Content Value**.

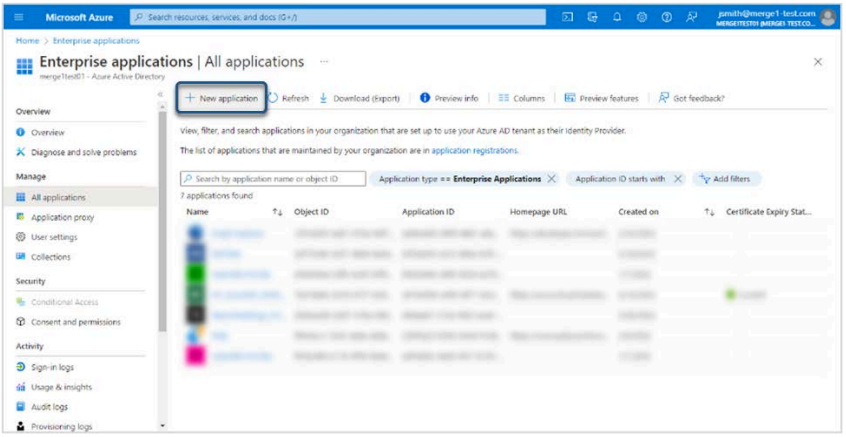
Creating an Enterprise Application

To use Single Sign-On as an Authentication method, an Enterprise Application on Microsoft Entra ID should be created.

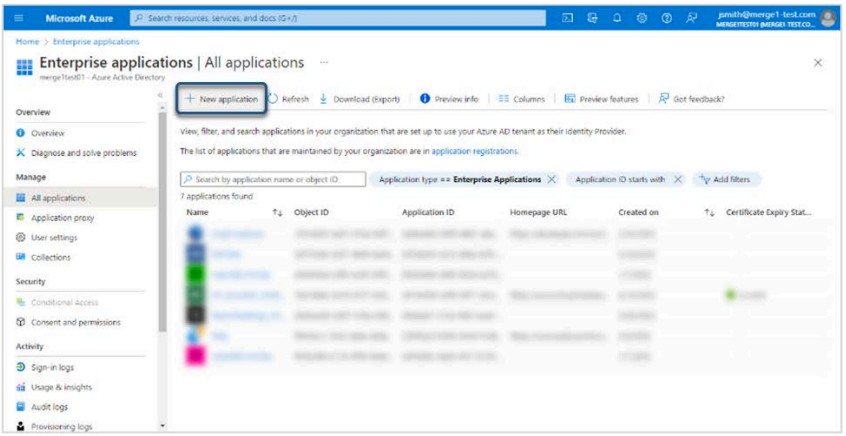
1. Go to Azure Portal using admin role credentials.
2. Click **Enterprise applications** under **Azure services**.



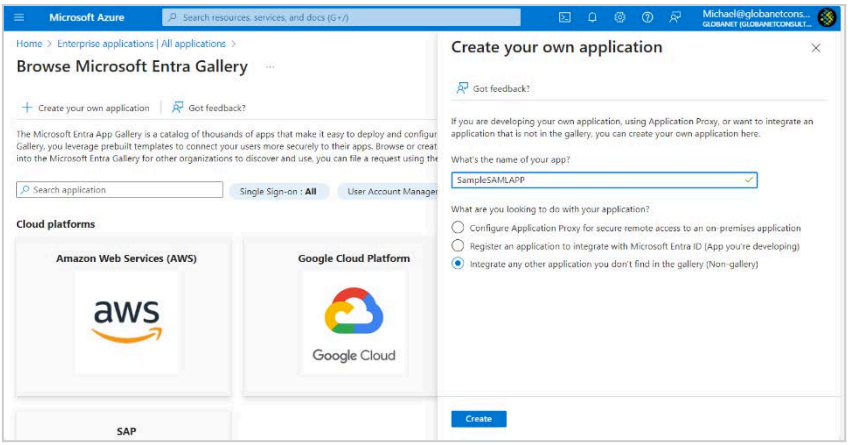
3. Click **New registration**.



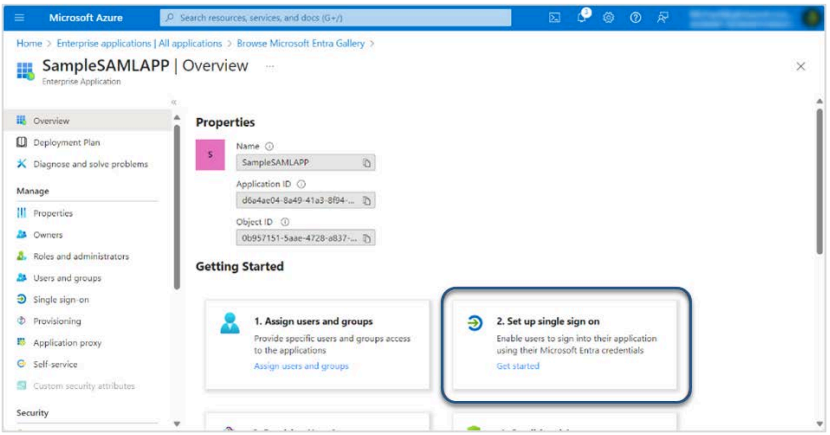
4. Click **Create your own application**.



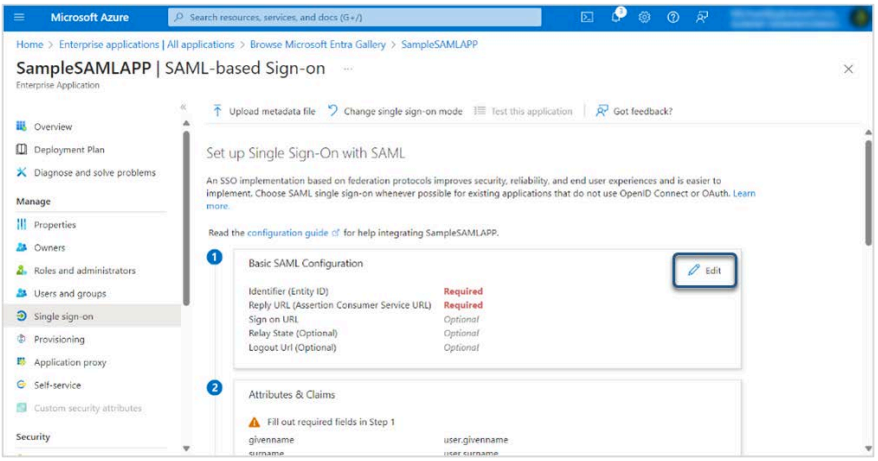
5. Enter a **Name** for the application and click **Create**.



6. Under **Getting Started**, select **Set up single sign-on**.



7. Click **Edit** to add the **Identifier (Entity ID)** and **Reply URL** (Assertion Consumer Service URL) from the Mergel portal Authentication section.



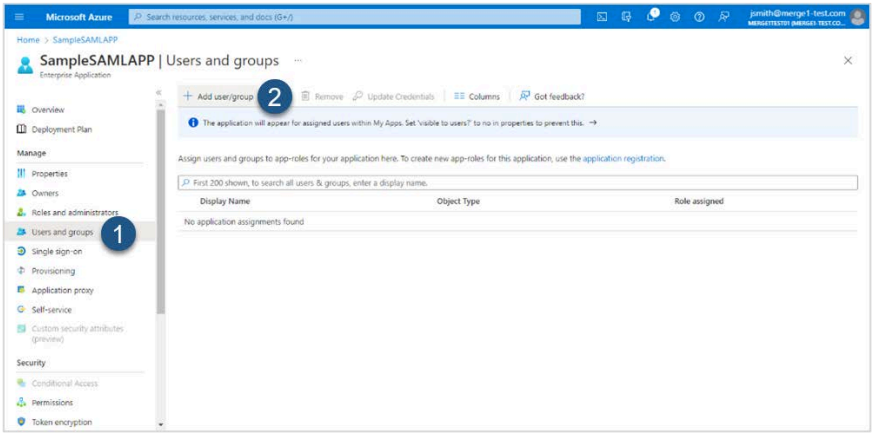
8. Go to Mergel Authentication and enable the **Single Sign-On (SSO) With SAML 2.0** checkbox. The **SAML 2.0 Configuration** section opens.
9. Under the **Metadata URL** option in the Mergel Authentication section:
    9.1. Copy the value of **Entity ID** and provide it as an **Identifier (Entity ID)** in the Microsoft Entra ID application.

9.2. Copy the value of **SSO URL** and provide it as a **Reply URL (Assertion Consumer Service URL)** in the Microsoft Entra ID application.

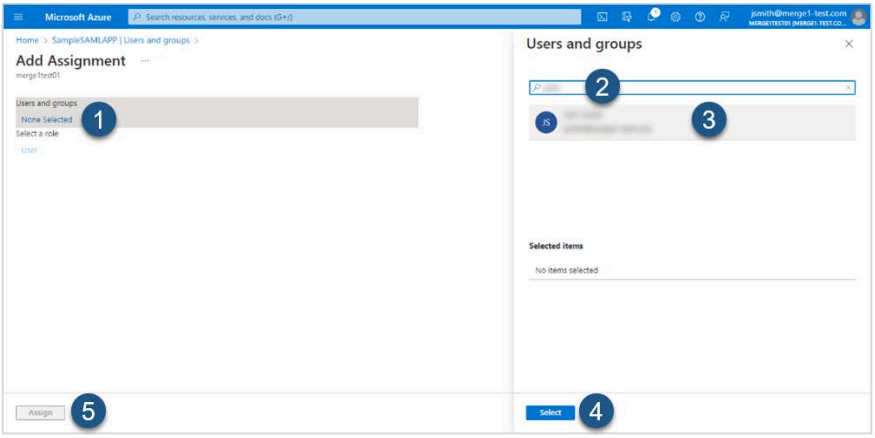
10. Click **Save**.

Assigning the Application to a User

1. Go to Users and groups and select **+Add user/group**.



2. Click **None Selected** under **Users and groups**, select the user, and click **Assign**.

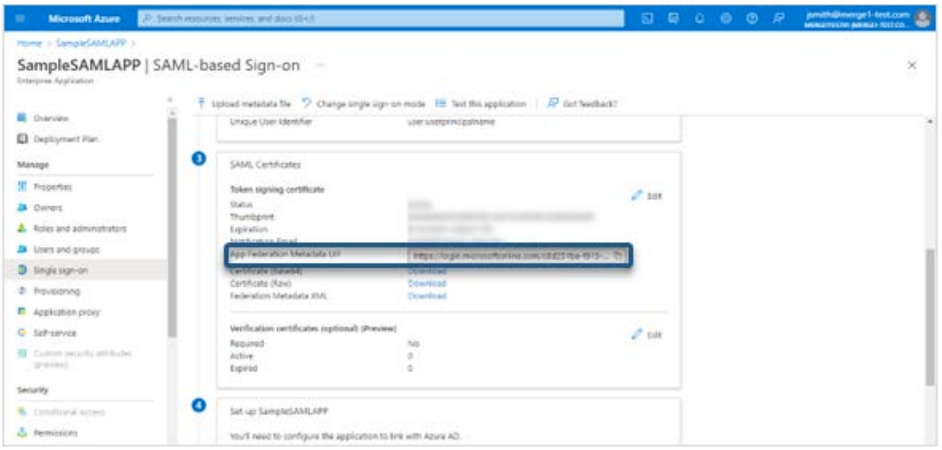


The assigned user details will appear on the **Users and groups** page.

3. Make sure the user is also created in Merge1.

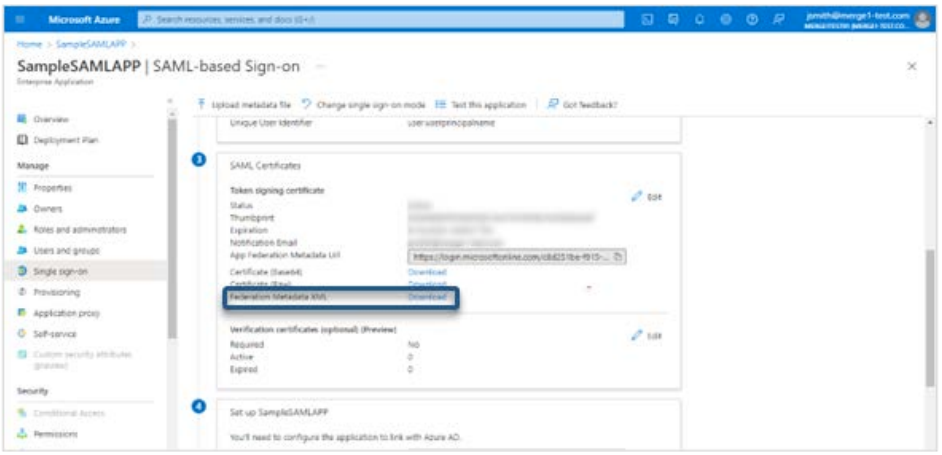
Obtaining the Metadata URL Value

1. Scroll down to **SAML Certificates** on the same Single sign-on page.
2. Copy the **App Federation Metadata URL** and provide it to Merge1 in case of configuring the SSO by Metadata URL.



Obtaining the Metadata Content Value

1. Scroll down to **SAML Certificates** on the same Single sign-on page.
2. Download the **Federation Metadata XML**. Copy the XML file content and provide it to Merge1 in case of configuring the SSO by Metadata Content.



Configuring the SSO Authentication via OKTA

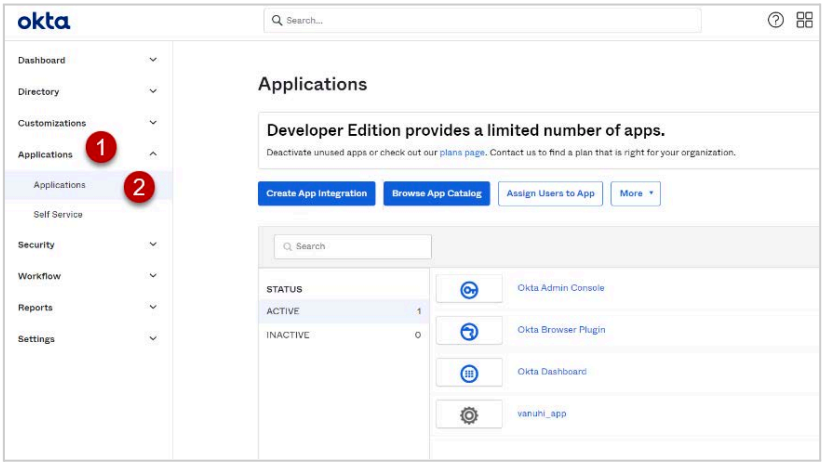
To configure the SSO authentication via OKTA, the admin should:

1. Create application integration.
2. Assign the application to people.
3. Obtain the **Metadata URL** value.
   Or,
4. Obtain the **Metadata Content** value.

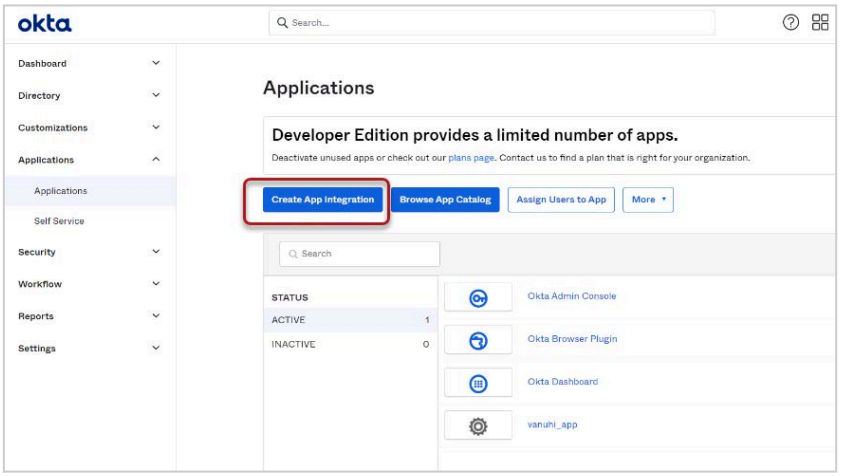
Creating an Application Integration

To use Single Sign-On as an authentication method an Application Integration on Okta (IDP) should be created.

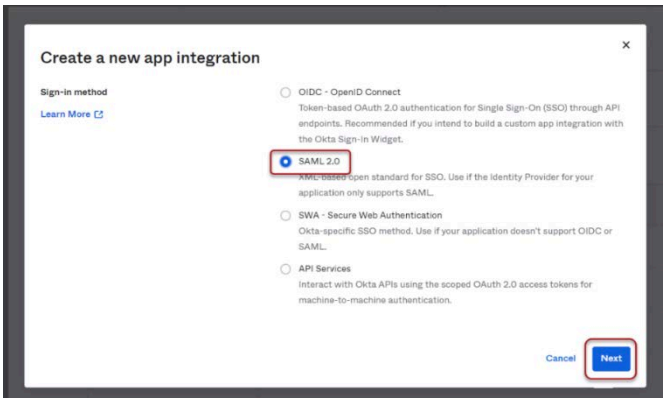
1. Login in with your business account and select **Applications > Applications** from the left-side Navigation Pane.



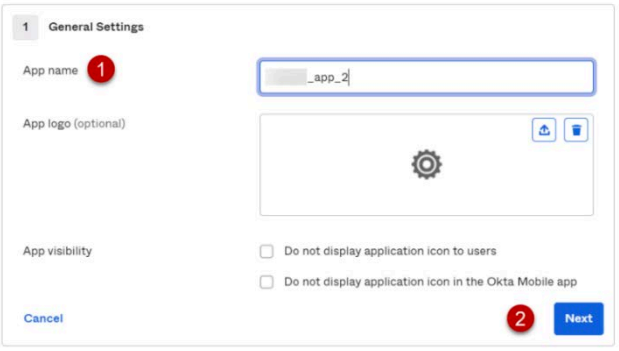
2. Click **Create App Integration**.



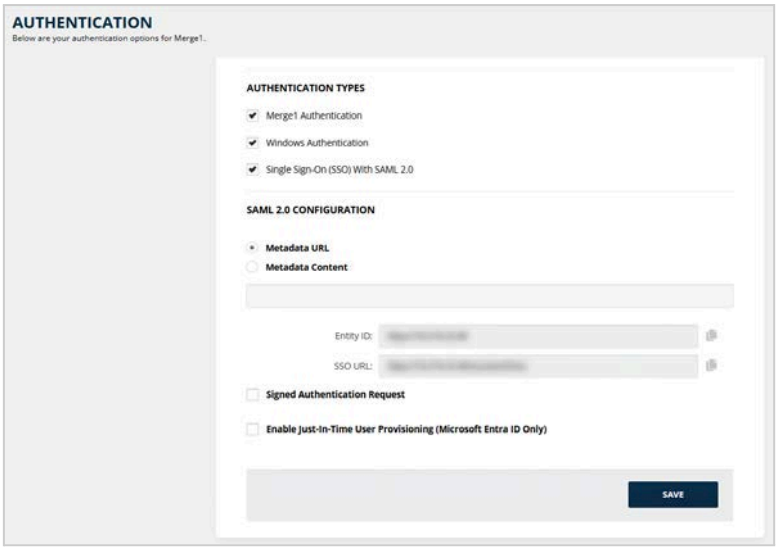
3. Select **SAML 2.0** and click **Next**.



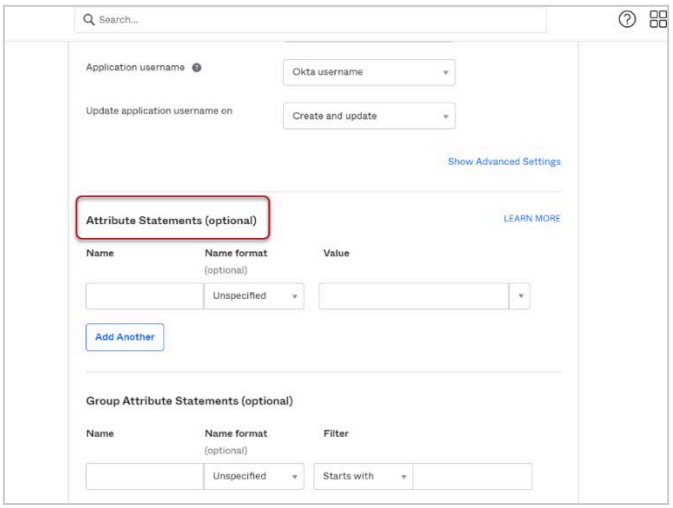
4. Provide an **App name** and click **Next**.



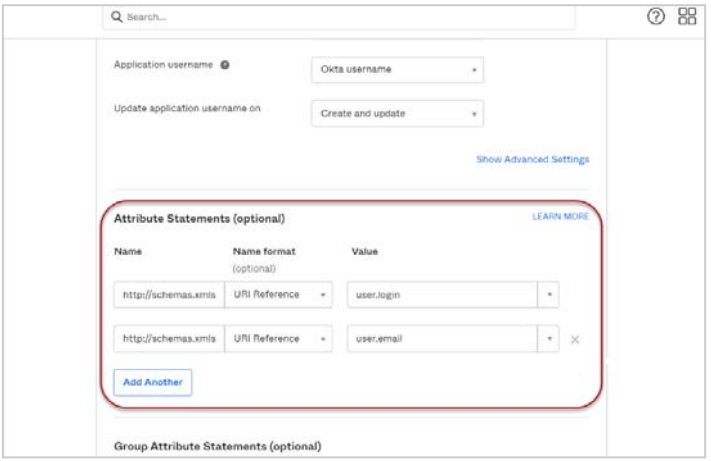
5. Go to **Merge1 > Authentication**.



6. Copy the value of the **SSO URL** and paste it as a **Single sign-on URL** in the **Okta** application.
7. Copy the value of **Entity ID** and paste it as **Audience URI (SP Entity ID)** in the **Okta** application.
8. In the **Okta** application, scroll down to **Attribute Statement (optional)**.



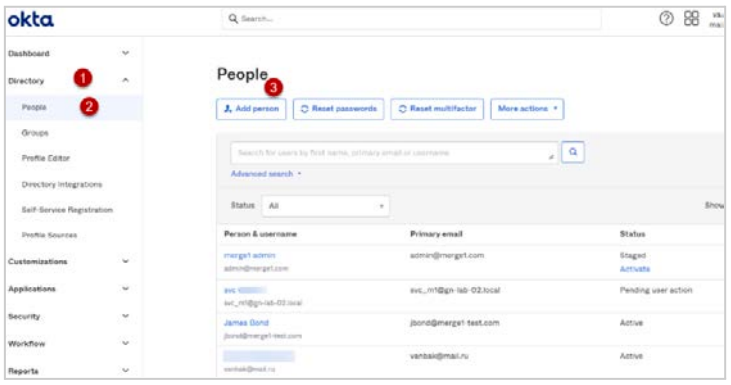
9. Provide the `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name` URI for **Name**, select **URI Reference** as a **Name format**, and `user.login` as a **Value**.
10. Click **Add Another** and provide `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress` for **Name**, select **URI Reference** as a **Name format** and `user.email` as a **Value**.



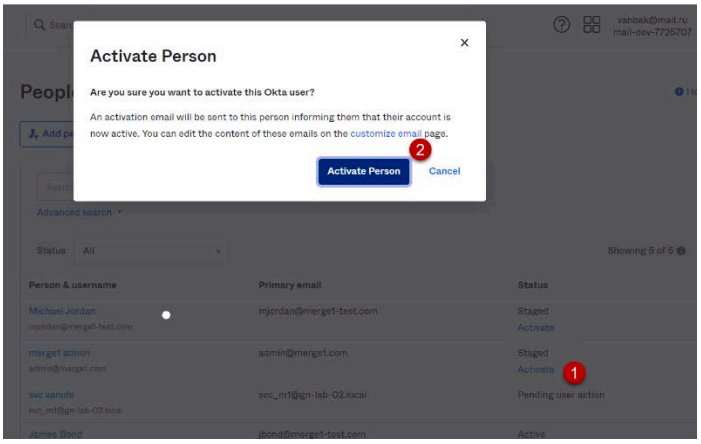
11. Click **Next**, select **I'm a Software vendor**, and then click **Finish**.

Assigning the Application to People

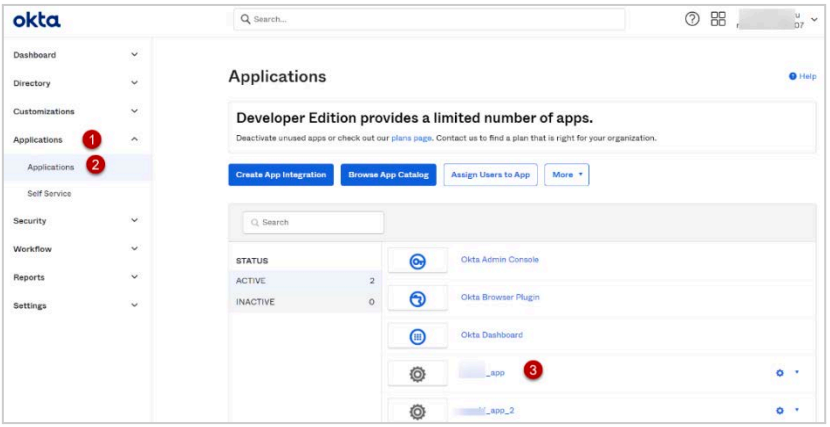
1. Go to **Directory > People** and select **Add person**.



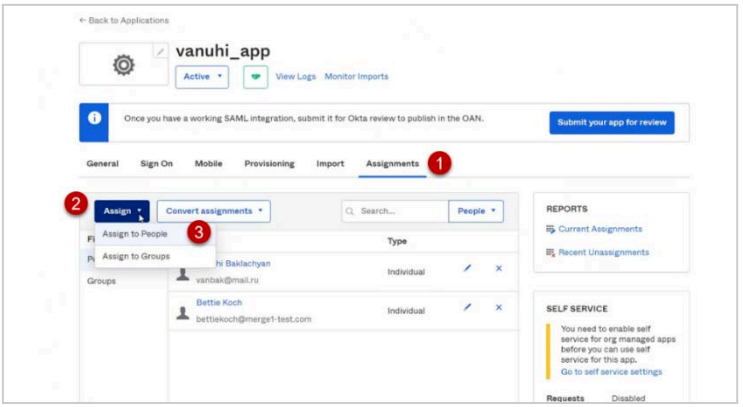
2. Provide **First name**, **Last name**, and **Username**, and click **Save**.
3. Click **Activate Person** and go by the link sent to the email for confirmation.



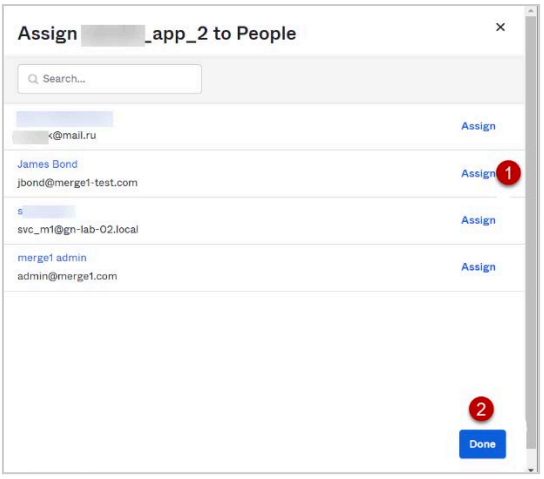
4. Go to **Applications > Applications** and select the application that was created.



5. Go to **Assignments > Assign > Assign to People**.

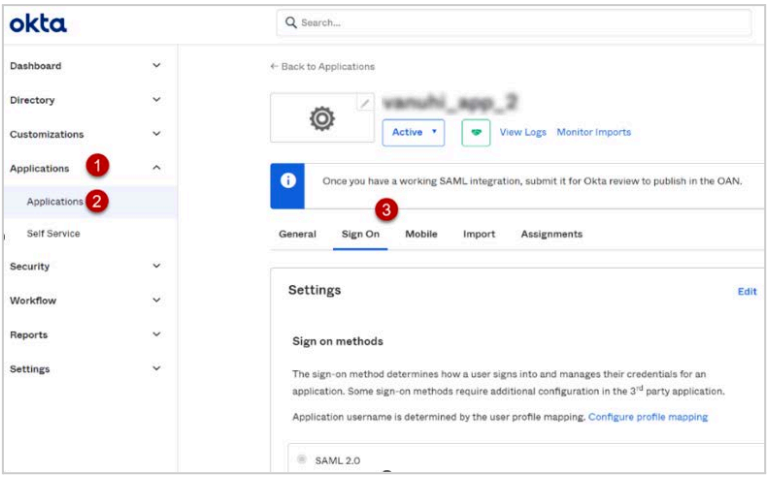


6. Select the user and click **Done**.

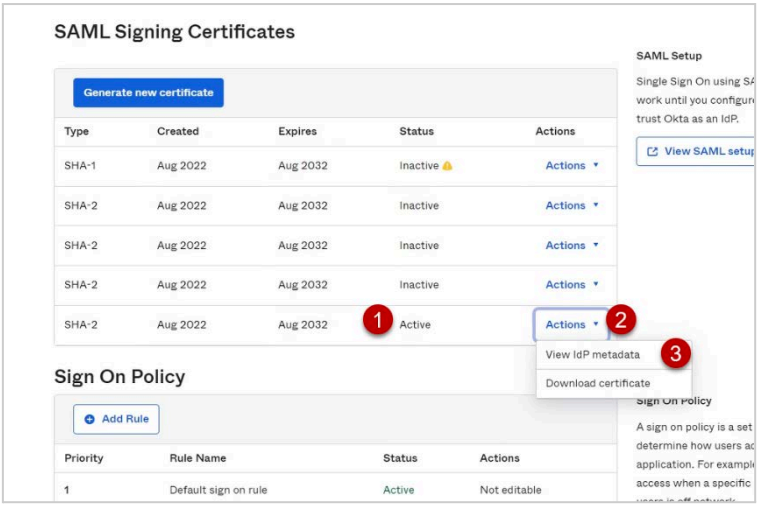


Obtaining the Metadata URL Value

1. Go to **Applications > Applications** and select **Sign On**.



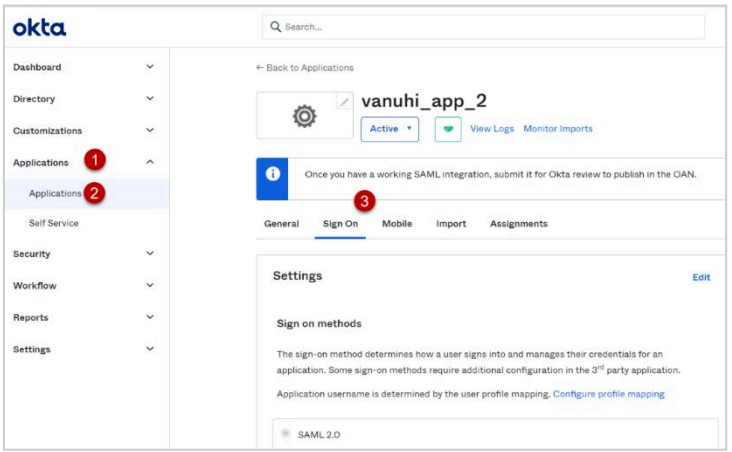
2. Scroll down to **SAML Signing Certificates**.
3. Find the certificate with an active status.
4. Click **Actions > View IDP metadata**.



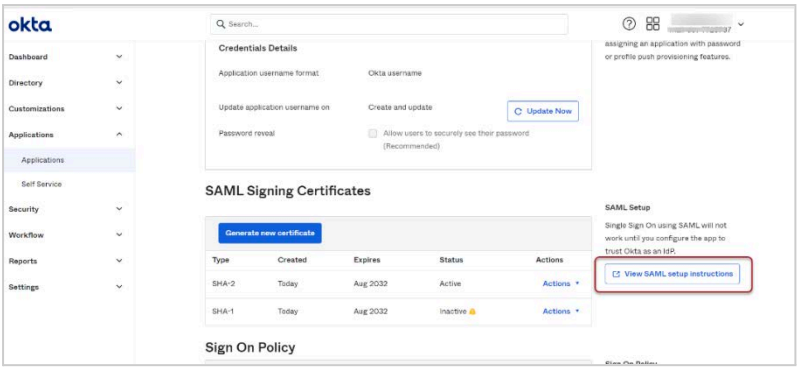
5. The metadata URL will be opened in a new tab. Copy and save it for later use in case of configuring SSO via Metadata URL.

Obtaining the Metadata Content Value

1. Go to **Applications > Applications** and select **Sign On**.



2. Scroll down and click **View SAML Setup Instructions**.



3. Copy the **IDP metadata** and save it for later use in case of configuring SSO via Metadata Content.

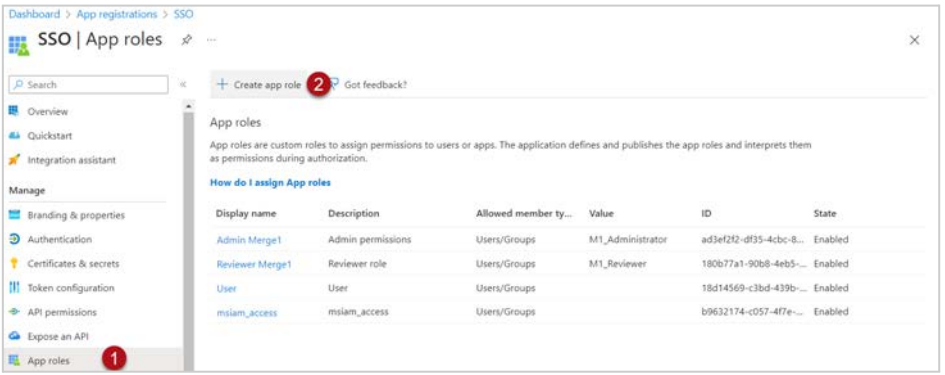
Just-In-Time Provisioning (JIT)

Just-in-time user provisioning (JIT provisioning) allows users to be created and updated automatically when they log in through SAML SSO.

Creating an App Role for JIT User Provisioning

Before enabling **Just-In-Time User Provisioning** in the Merge1 portal, a role must be created in Azure and assigned to the given user by following the steps below.

1. Find your **SAML/SSO App** in **Microsoft Entra ID App Registrations** and click **App roles**.
2. Click **Create app role**.



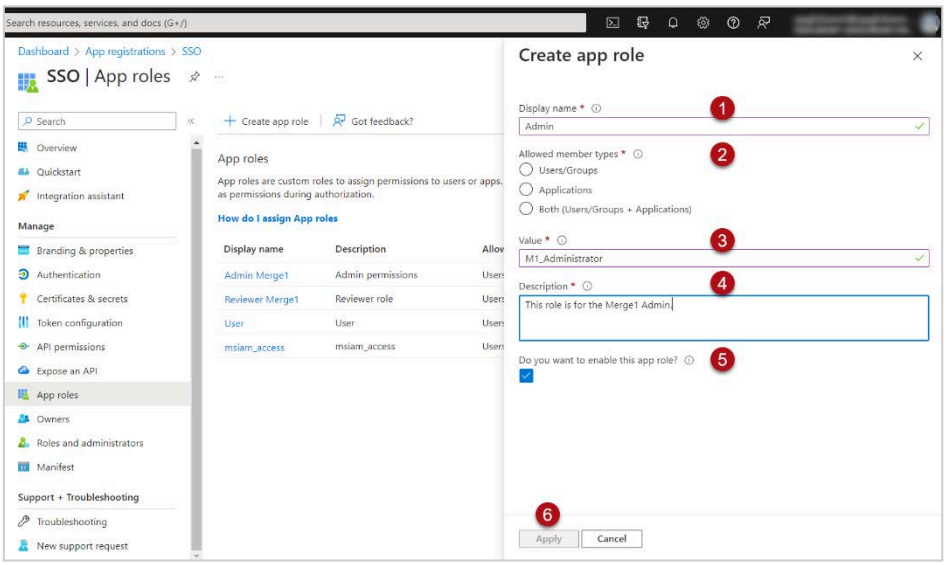
3. Populate the following fields:
   - **3.1. Display name**.
   - 3.2. **Allowed member types**: Users/Groups.
4. **Value**: Enter `M1_Administrator` for the Merge1 Admin role and `M1_Reviewer` for the Merge1 Reviewer role.

> **Note**
>
> Only M1_Administrator and M1_Reviewer values are supported for the Merge1 SSO in case Enable Just-In-Time User Provisioning (Microsoft Entra ID Only) is activated.

4.1. **Description**.

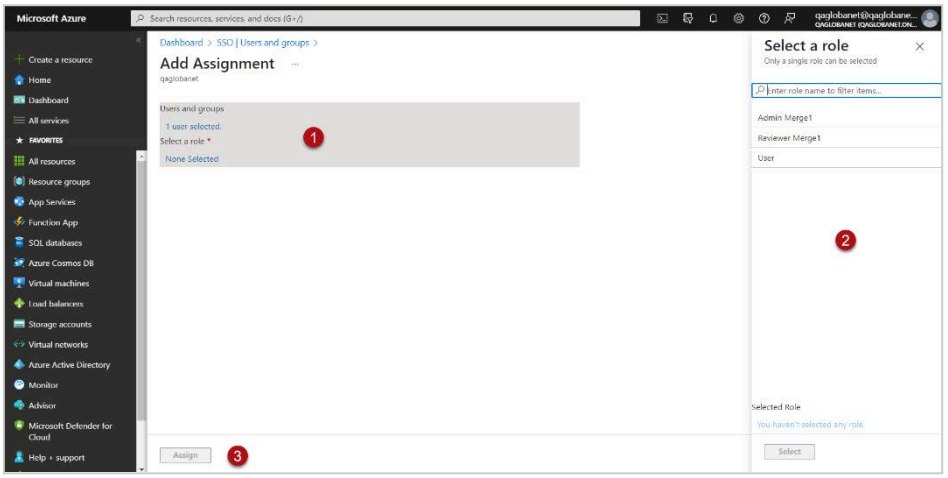
4.2. Keep the **Do you want to enable this app role** box checked.

5. Click **Apply**.



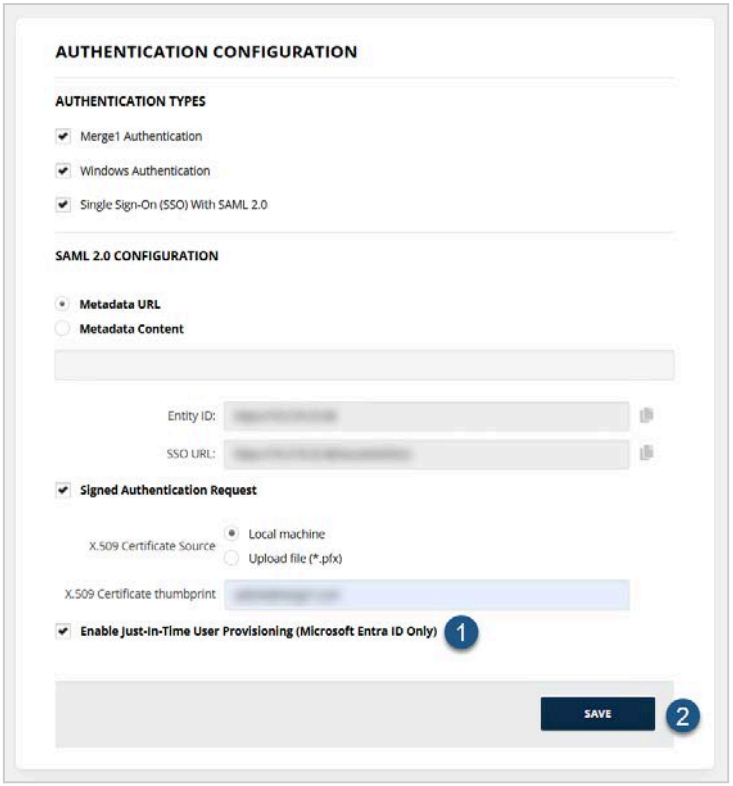
Assigning a Role to the User

1. Navigate to the **Enterprise Applications** page to assign the role to the user.
2. Click **Add user/group**.
3. Select the **User** or **Group** for the respective role to the user/group and click **Assign**.



Enabling JIT User Provisioning

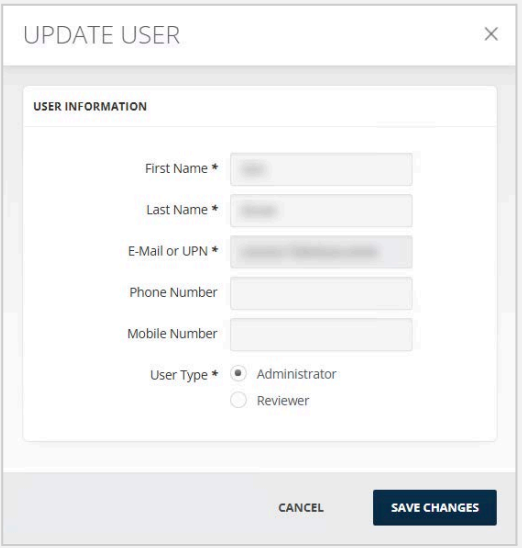
1. Navigate to the **Merge1 Authentication** section, check **Enable Just-In-Time User Provisioning (Microsoft Entra ID Only)** and click **Save**.



2. Sign in with SSO on the login page, authenticate with the user assigned to the Azure app, and the user will be automatically created in the **Users and Groups** section with a role that you have provided in Azure.

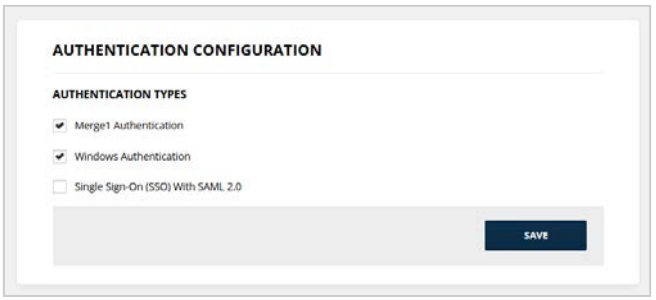
Note

The role cannot be changed from Mergel. If you want to change the role for the JIT user, you need to change it in Azure. Next time, when the user is signed in to Mergel, the role will be already changed. You can check it by navigating to the Mergel **Users & Groups** section and clicking the **Edit** button next to the user.



Configuring SSO Authentication in Merge1

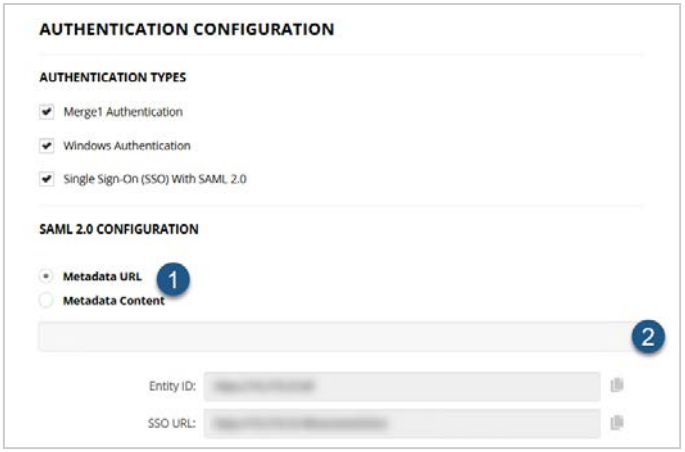
Open the **Authentication** section from **Navigation Pane**.



When enabling **Single Sign-On (SSO) with SAML 2.0**, the SAML 2.0 Configuration opens. The user can select configuring SSO either via **Metadata URL** or **Metadata Content**.

To configure the SSO via Metadata URL:

1. Select **Metadata URL** under **SAML 2.0 Configuration**.
2. Enter the copied Metadata URL in the **Metadata URL** field in case of using an Okta Application for SSO.
   Or,
3. Enter the copied Metadata URL in the **Metadata URL** field in case of using a Microsoft Entra ID Application for SSO.



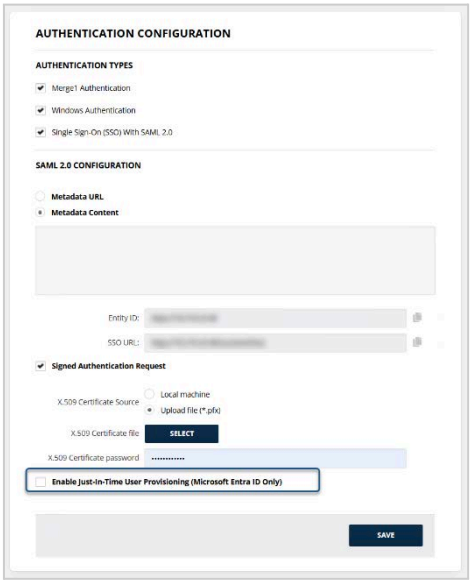
4. Click **Save**. The **Single Sign-On (SSO)** option will appear in the **Authentication method** drop-down list.

To configure SSO via Metadata Content:

1. Select **Metadata Content** under **SAML 2.0 Configuration**.
2. Provide the copied **IDP metadata** in the **Metadata Content** field in case of using an Okta Application for SSO.
   Or,
3. Provide the copied **IDP metadata** in the **Metadata Content** field in case of using a Microsoft Entra ID Application for SSO.

4. Enable **Signed Authentication Request** to sign in using the X.509 Certificate.
5. Provide an **X.509 Certificate Thumbprint** in case you activate the **Local machine** radio button as the X.509 Certificate source.

6. In case you activate **Upload file (*.pfx)**, click the **Select** button to upload the certificate and provide **X.509 Certificate password**.
   The **Certificate thumbprint** field will be auto populated in case the collector was previously configured by uploading a certificate.
7. Check **Enable Just-In-Time User Provisioning (Microsoft Entra ID Only)**. For more information see **Just-In-Time Provisioning (JIT)**.



8. Click **Save**. The **Single Sign-On (SSO)** option will become visible in the **Authentication method** drop-down list.

Navigation Pane

The GUI of Merge1 consists of two parts: The **Main Screen** and the **Navigation Pane**. You can easily switch between the different sub-sections of the software through the Pane. Merge1 **Navigation Pane** consists of the following shortcuts:

DASHBOARD

Here you can view all the statistical and logistical information about your Merge1 activities.

IMPORTERS

Here you can connect or remove company-relevant Importers, configure targets, and set filters.

NOTIFICATIONS

Here you can see notifications and manage the preferences.

USERS & GROUPS

Here you can view the basic information of all the users and groups who can log in to the company's Merge1 account.

REPORTS

Here you can export reports of each collector in a PDF or CSV format.

SETTINGS

Here you can view and/or customize the database, audit, proxy, and authentication configurations, as well as manage message settings.

BRANDING SETTINGS

Here you can make Merge1 on your own.

LICENSING

Here you can activate a license and view the version of your Merge1. Here you can activate a license and view the version of your Merge1.

API CLIENTS

Here client applications can have access to the Merge1 API.

AGENT POOLS

Here Agent Pools are available for running Importers.

AUTHENTICATION

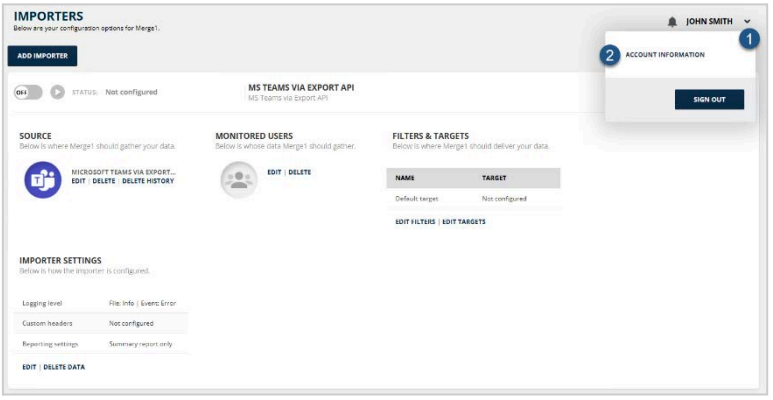
Here Merge1 authentication types can be configured.

JOB MONITORING

Here Merge1 import jobs can be monitored.

Account Settings

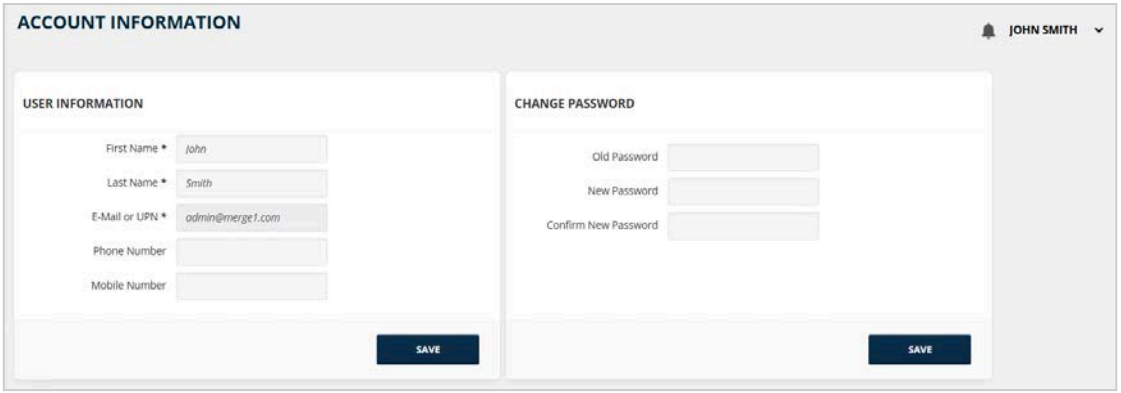
On the top right corner of the Main Screen, you can find your **Account Settings** which allows modifying your account default settings.



To view your user **Account Settings,** click ⌄ next to your username. A pop-up window will open. Click **ACCOUNT INFORMATION**.

On the **Account Information** page, you can modify your default User Information and change your password. The following settings refer solely to your account and have no connection with general Merge1 Settings.

The **Account Information** section consists of two parts: **User Information** and **Change Password**.



User Information

To edit the user information:

1. Update your account **First Name** and **Last Name** fields.
2. Update phone/mobile number.
3. Click **SAVE**.

Note that the **E-Mail** or **UPN** fields are not editable.

Logging Out

To log out from your Merge1 Account, click ⌄ next to your username and then click **SIGN OUT**.

Changing the Password

To change the password:

1. Enter the current password in the **Old Password** field.
2. Enter the new password in the **New Password** field.
3. Re-enter the new password in the **Re-type** field.
4. Click the **SAVE** under the **Change Password** section.

Once you have made all the relevant changes, click **SAVE**.

Your account information will be visible to everyone on your company's Merge1 account.

CHAPTER 4

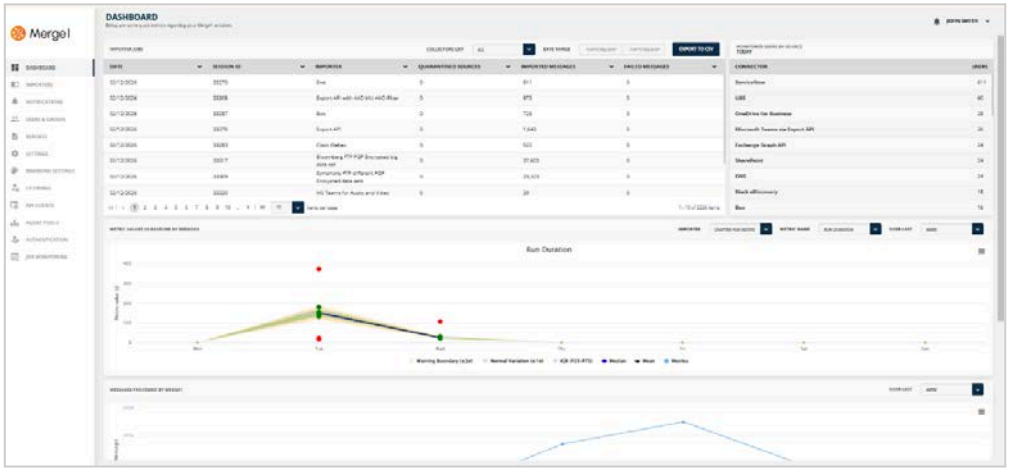
Dashboard

This chapter represents:

- Overview
- Importer Jobs
- Monitored Users by Source
- Metric Values vs Baseline by Weekday
- Messages Processed by Merge1
- Number of Messages by Importer
- Timeframe Filtering
- Viewing and Exporting Reports

Overview

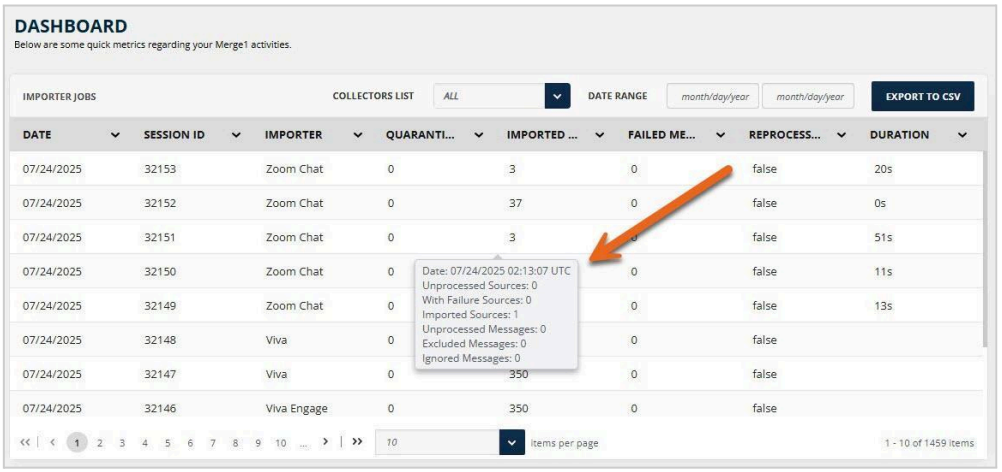
The Mergel **Dashboard** offers interactive visual modules that provide insights into your Mergel activity, including statistical trends and compliance-related data.



Mergel Dashboard consists of four widgets:

1. **Importer Jobs**
2. **Monitored Users by Source**
3. **Metric Values vs Baseline by Weekday**
4. **Messages Processed by Mergel**
5. **Number of Messages by Importer**

Hover over a job to access detailed information, including the date, sources, message statuses, and message counts.



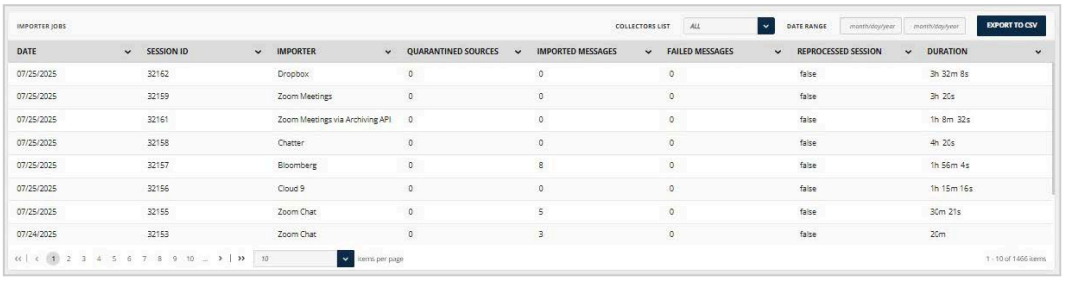
Importer Jobs

The **Importer Jobs** dashboard displays statistical information about the following activities:

- **Date**
- **Session ID**
- **Importer**

- **Quarantined Sources**
- **Imported Messages**
- **Failed Messages**
- **Reprocessed Session**
- **Duration** [1]

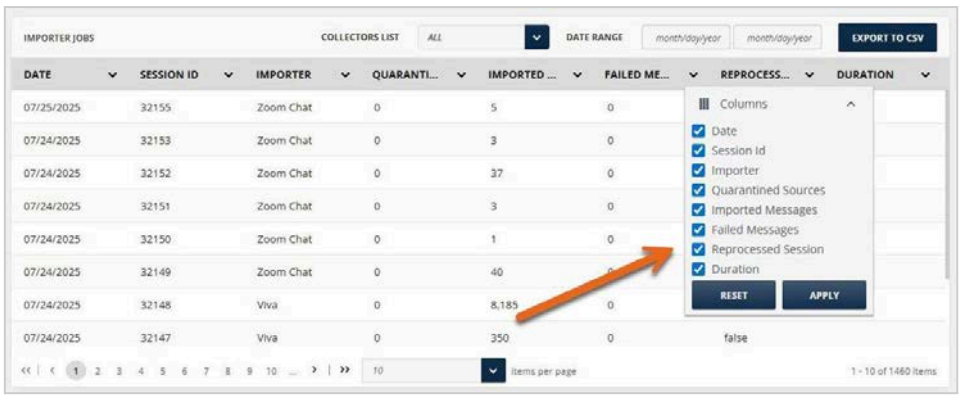
You can drag and rearrange items to modify their order in the Merge1 GUI.



Customizing the Columns of Importer Jobs

The columns of the **Importer Jobs** dashboard are customizable in a way to:

1. Dynamically resize the width of columns.
2. Rearrange the order of columns by dragging them to their new location within the spreadsheet.
3. Control the visibility of columns, such as hiding and showing them. This can be done by the following steps:
    3.1. Click the *expand* icon next to the column title.
    3.2. Click the *expand* icon next to the opened **Columns** title.
    3.3. Enable or disable the columns to show or hide them according to your preference.
    3.4. Click **Apply** to apply the changes.



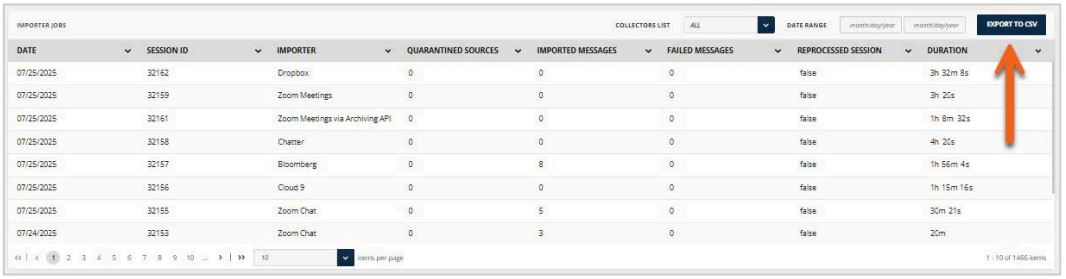
Exporting to CSV

You can export importer jobs as a CSV file for:

- A specific importer by selecting a collector from the **Collectors List** drop-down menu.

[1] The importer's duration will not be displayed if the job is interrupted or stopped before completion.

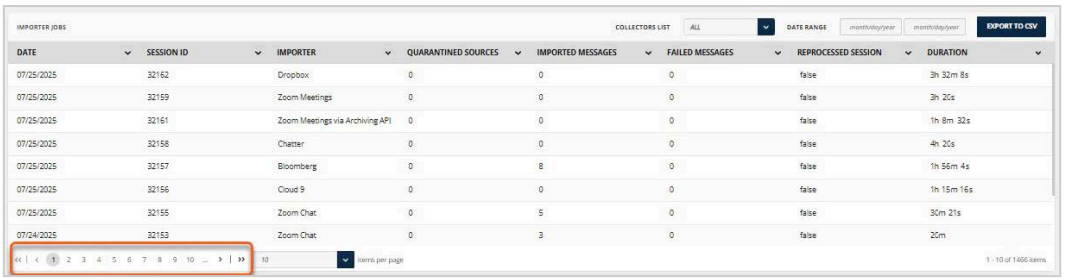
- A defined date range by choosing FROM and TO dates in the calendar.



> **Note**
>
> All columns of the **Importer Jobs** will be exported, regardless of any applied filters.

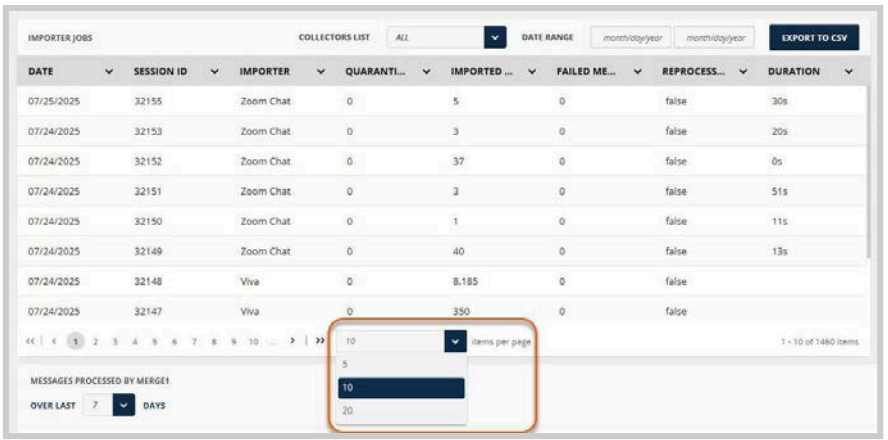
Browsing Importer Jobs

The list of items is divided into pages for easy navigation. Use pagination to browse through and view all available items.



Adjusting the Number of Items per Page

By default, each page displays 10 items to optimize loading speed. However, you can adjust this setting to show more or fewer items per page based on your preference.



Monitored Users by Source

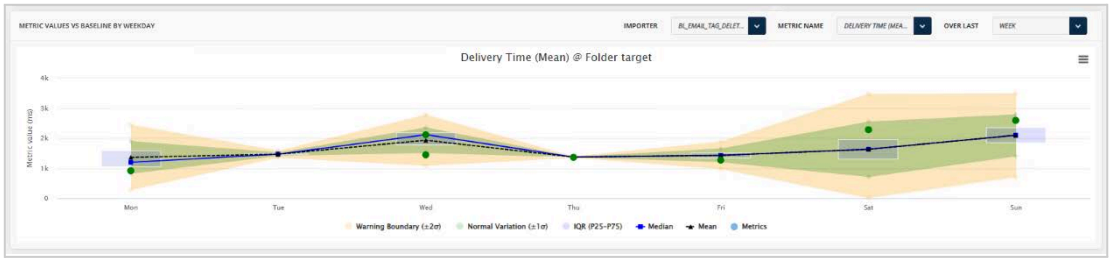
The **Monitored Users by Source** widget displays the number of monitored users per source for the current day.

MONITORED USERS BY SOURCE
TODAY

CONNECTOR	USERS
EWS	24
Skype for Business	21
Microsoft Teams via Export API	1
Viva Engage	1
Twitter	1

Metric Values vs Baseline by Weekday

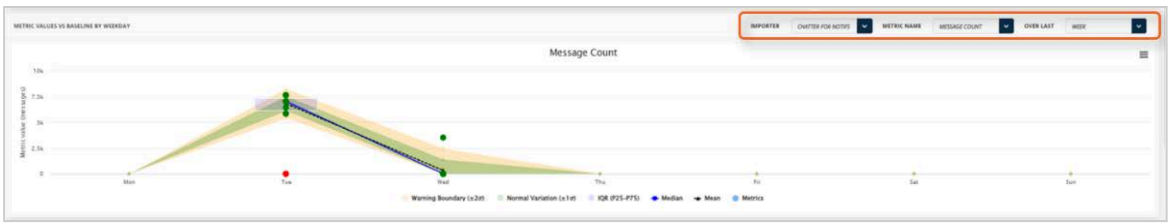
The **Metric Values vs Baseline by Weekday** widget provides a comparative analysis of importer performance metrics against historical averages.



Customizing and Exporting Data

The **Metric Values vs Baseline by Weekday** 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):** See **Timeframe Filtering**.
- **Viewing and Exporting Reports:** See **Viewing and Exporting Reports**.

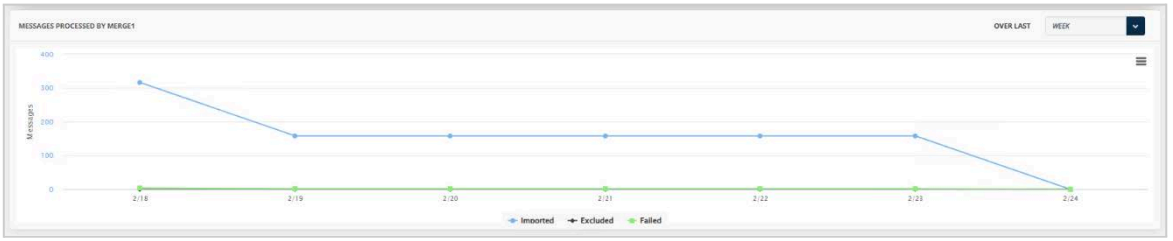


Messages Processed by Merge1

The **Messages Processed by Merge1** 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**.

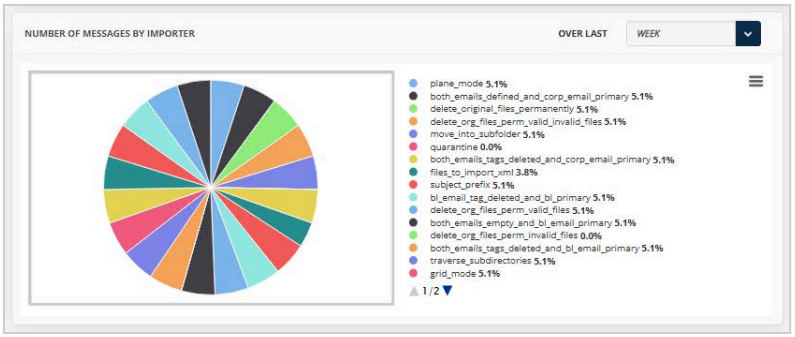


Number of Messages by Importer

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**.

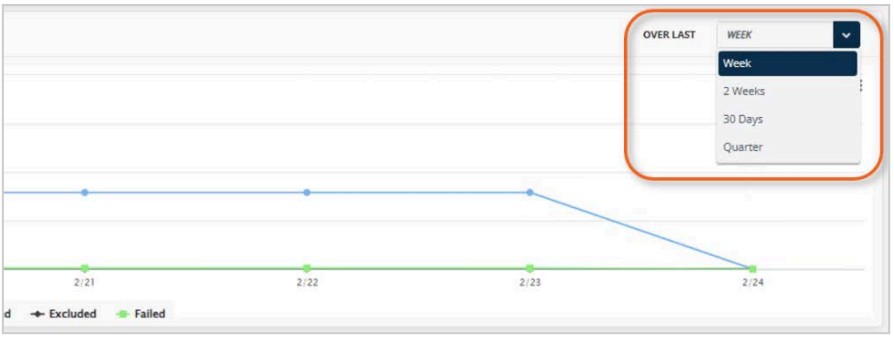


Timeframe Filtering

The **Over Last** dropdown 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**.

CHAPTER 5

Importers

This chapter represents:

- Overview
- API-Based Collector Options
- File-Based Collector Options
- Importers
- Monitored Users
- Filters
- Targets
- Importer Settings

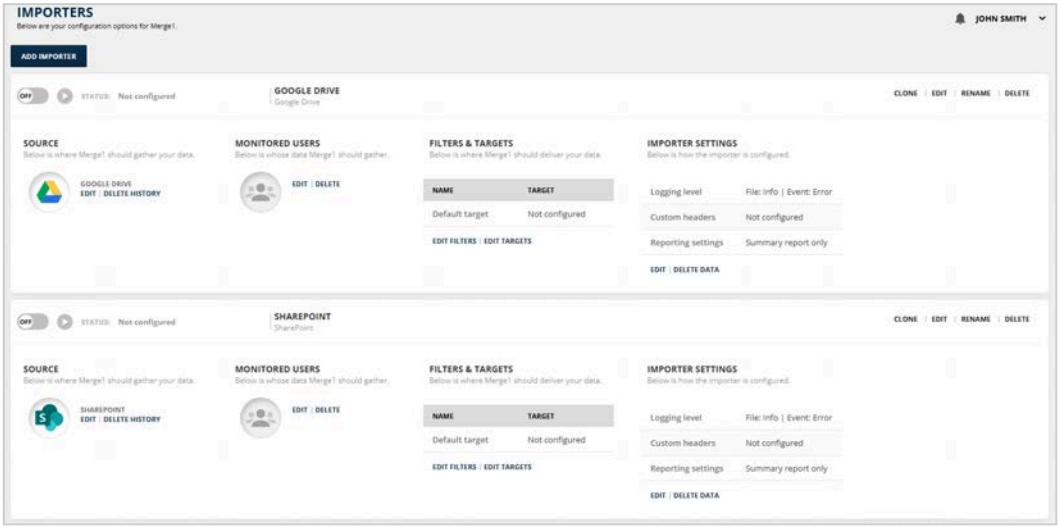
Overview

Merge1 collects data from an array of e-communication media. The collectors are designed to be used for ongoing archiving with steady-state scheduled runs doing deltas. This is done by configuring a collector with an open-ended date and scheduling it to run, usually nightly.

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

New sources are frequently added. Feel free to contact Arctera Support for new additions or requests.

The **Importers** section allows you to add, connect or remove company relevant importers, configure targets, and set filters.

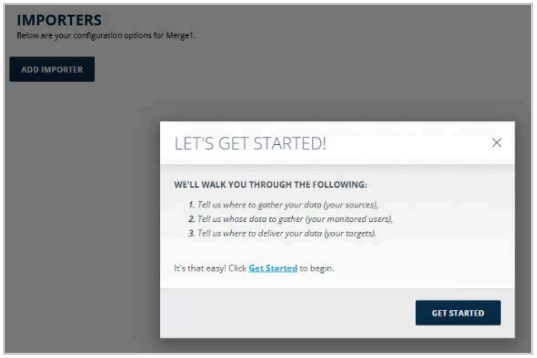


Each importer has its own configuration options:

- Clone, edit, rename, and delete importers
- Schedule, start/stop imports
- Add and edit collectors/monitored users/filters/targets
- Retry failed items
- Delete data
- Rename components

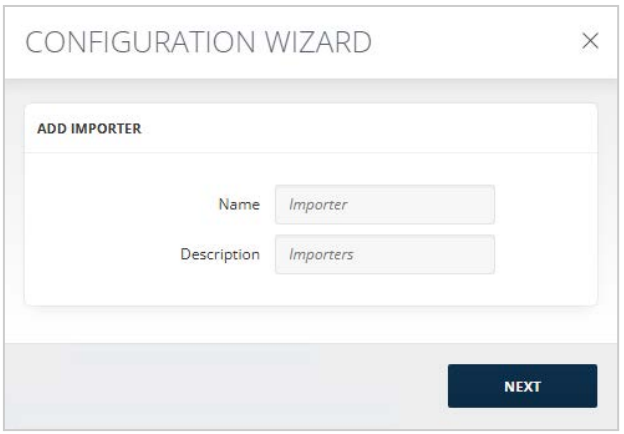
Adding a New Importer

As a first-time user, you will see a blank page to get started.

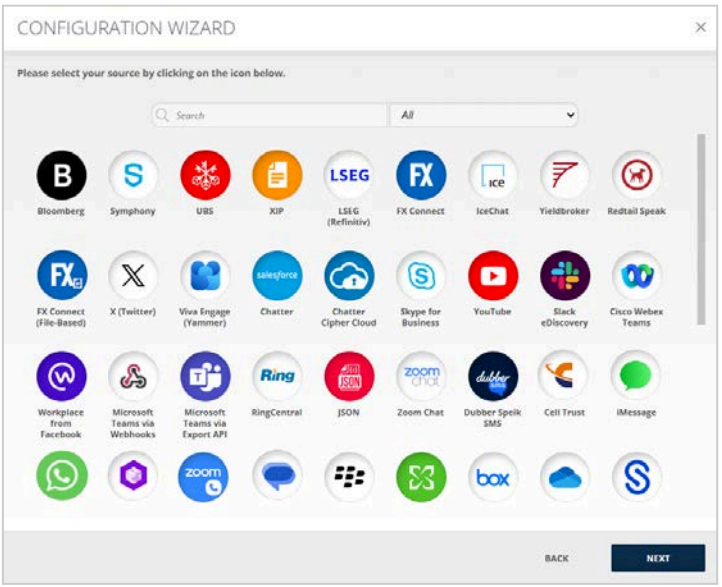


To add a new importer:

1. Click **Get Started**. A configuration wizard of adding a new importer will appear (the same wizard will open when clicking **Add Importer** on the top left corner.



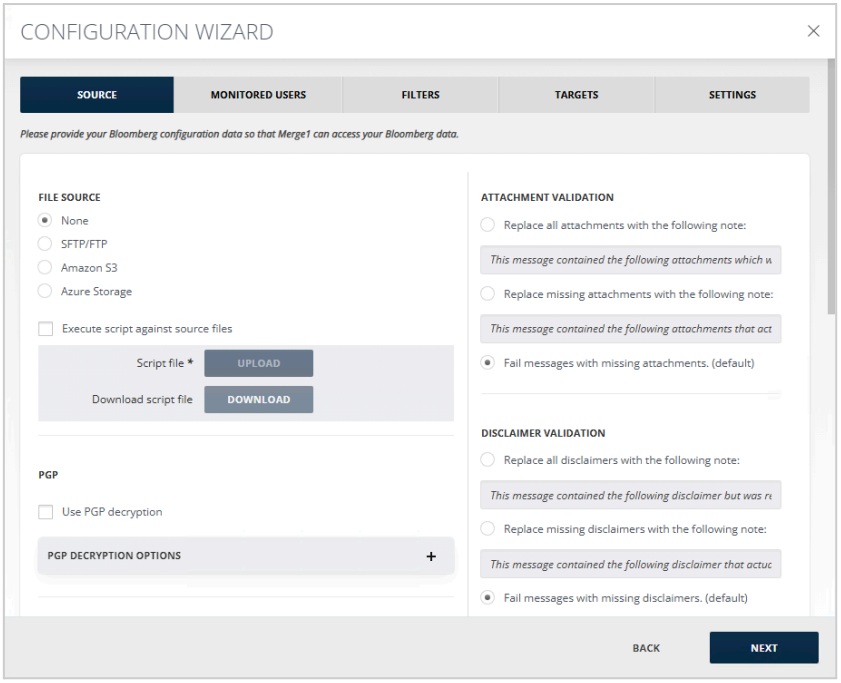
2. Fill in the **Name** and the **Description** fields and click **NEXT**. The next wizard will open where you can find all the sources provided by Merge1.



Here you can make use of:

- **Searching option.** Type the name of the source in the search box located above the sources.
- **Filtering option.** Select one of the following source types from the drop-down list above the sources:
    - Financial Platforms
    - Enterprise Social
    - Mobile
    - Enterprise Tools and File Sharing
    - Voice
    - Other

3. Select your source and click **NEXT**. The **Configuration Wizard** of the **Source** tab opens.



Note

From collector to collector the **Source** tab may vary.

Importer Panels

Merge1 importer panel is comprised of the following components:

- **Collectors (Sources)** - Contains general information about the collector and how to manage it.
- **Monitored Users -** Contains information about all the users of the collector and its configurations.
- **Targets -** Allows setting up where the collector information should be sent.
- **Importer Settings -** Helps to configure settings to load filtered data to the destination target.

You can also:

- Drag importer panels to re-arrange their order in the Merge1 GUI.
- Double-click the importer panel and the importer will collapse.

Managing an Importer

The options for managing the importers are:

- **Clone.** Allows copying the importer with all the previously configured settings.
- **Edit.** Allows editing the settings of the collector.
- **Rename.** Allows changing the name and the description of the importer.
- **Delete.** Deletes the importer with all the configured settings.

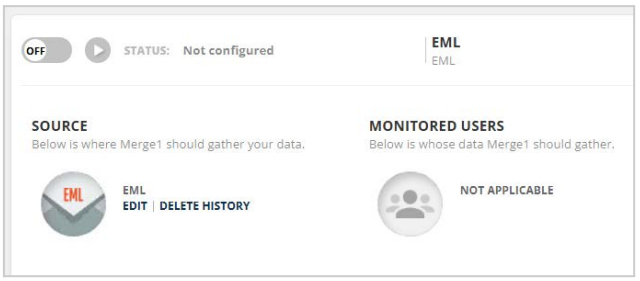
Note

If the importer is deleted, it will not be possible to recover it.

Running an Importer

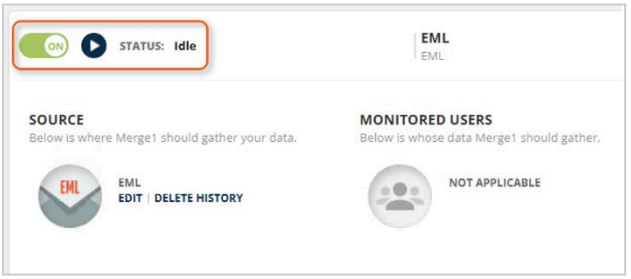
An importer can be run using:

- the **scheduler**
- the **start import** button



To run a job using the scheduler:

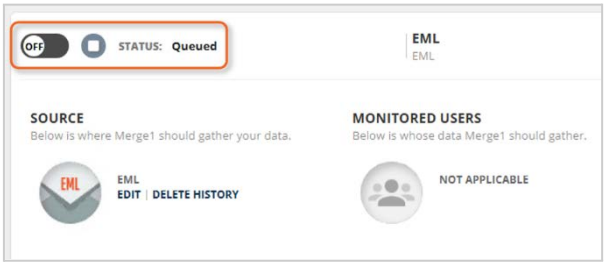
1. When enabling the **scheduler**, the running will remain **Idle** until the running time set by **Importer Schedule** (see Importer Schedule).



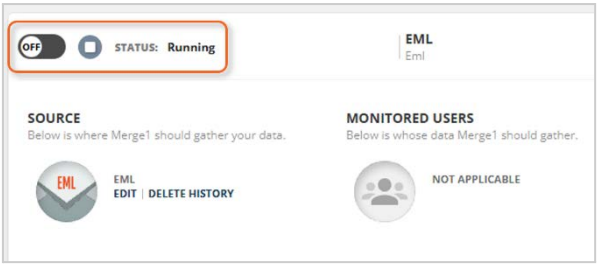
2. When the time is achieved and an agent is available, the running status will become **Queued**.
3. The status will be changed to **Running** within 30 seconds.

To run a job using the **start import** button:

1. If the **scheduler** is **off**, the job can be run by clicking the **start import** button. The status will change from **Idle** to **Queued**.



2. When an agent is available, the status will be changed to **Running** in 30 seconds.

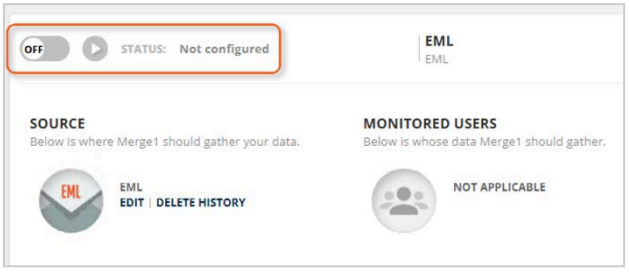


If the **scheduler** is enabled for an importer, and the **start import** button is set to **Queued** for the same importer, even if the running time is not set by **Importer Schedule**, the job will run (in case an agent is available).

Note

- When the **start import** button is set to **on** for a job, and a **scheduler** is enabled for another one, an available agent will run the job which was scheduled earlier.
- Even if the **Importer Schedule** is set, but the **scheduler** is not enabled, the job will not be queued.

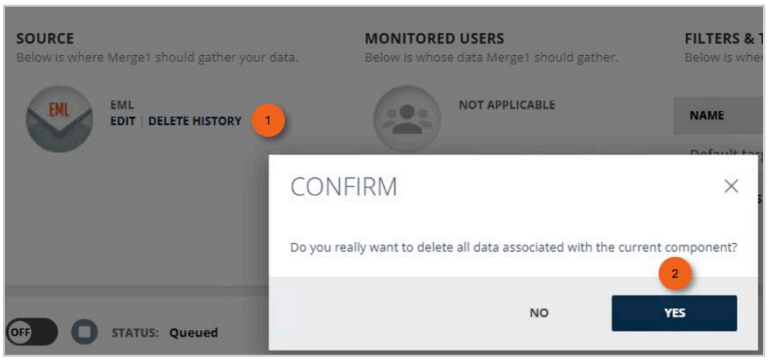
In case the collector is not configured, it cannot be run or scheduled for run from the Importer Settings.



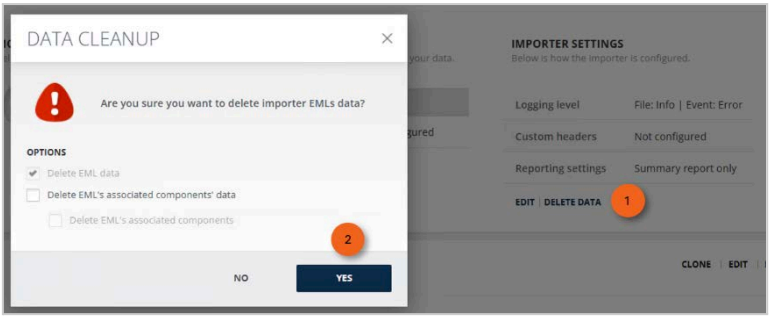
Collector History Deletion

There are two ways of deleting the collector's history.

The first one is to use the **Delete History** option under the **Source** section. This removes all collector data history from the previous runs and processed data.



The second way is to select **Delete** under **Importer Settings**. It also removes all collector data history from the previous runs.



If the **Delete <Collector Name>'s associated components' data** option is checked, all the failed messages and failed sessions are also deleted from the database.

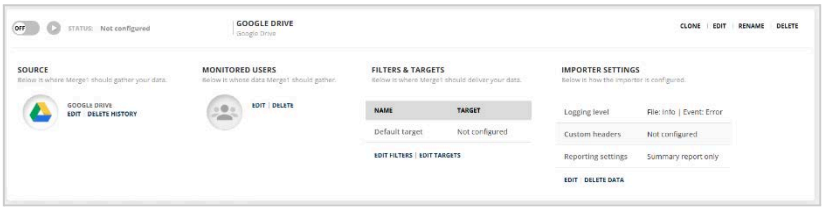
API-Based Collector Options

API-Based Collector Options

Progress Counter

The Progress counter to the right of the Status bar shows the progress of the collector in three stages:

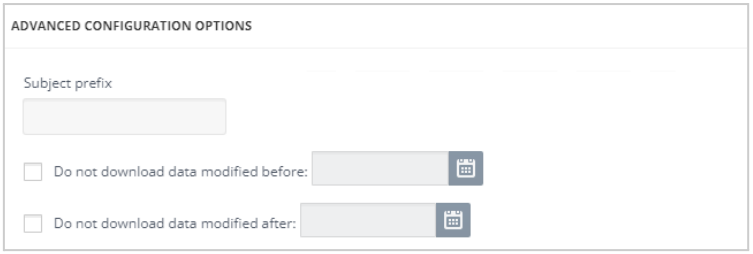
- Acquiring Monitored Users
- Scanning the Number of Users
- Processing the Users | Total Number of Messages Processed



Advanced Configuration Options

To configure advanced options:

- 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.
- 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 09/17/2024, only the data between these two dates will be downloaded. Data outside that timeframe will be ignored.



Attachments Configuration

To prevent large files from slowing down your system or consuming excessive storage, use the size limit setting:

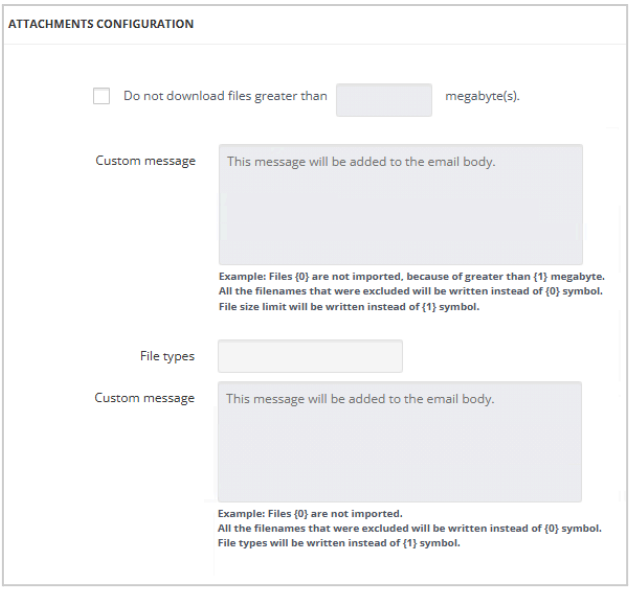
- **Do not download files greater than [X] megabyte(s):** Check this box and enter a numeric value. Any file exceeding this limit will not be downloaded.
    - **Custom message:** Define a custom message text for files excluded due to their size. If a file exceeds the limit, this message will be inserted into the output message body.

> **Tip**
>
> ***Example Message:*** Files {0} are not imported because they exceed the limit of {1} MB.
>
> - **{0}** is replaced by the name of the file.
> - **{1}** is replaced by the size limit you specified.

Use the filtering file type section to exclude specific file formats:

- **File types:** Enter the extensions you wish to exclude, separated by a comma (without space).
    - **Custom message:** Define a custom message text for files excluded due to their format. If a file is excluded, this message will be inserted into the output message body.

> **Tip**
>
> ***Example Message:*** Files {0} are not imported because the {1} file types are restricted.
>
> - **{0}** is replaced by the name of the file.
> - **{1}** is replaced by the size limit you specified.



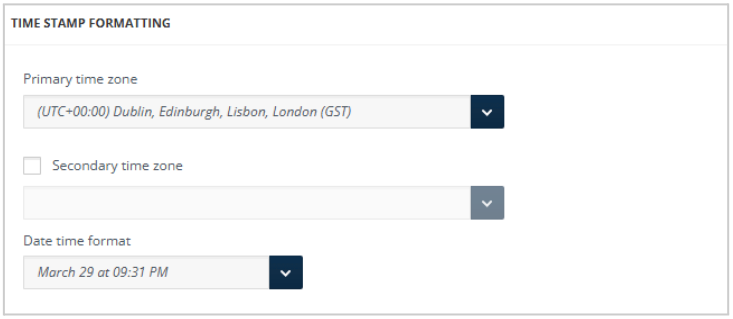
Info

In case of using file filtering by size and by type, we recommend using custom 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 options in the **Date time format** drop-down list.



File-Based Collector Options

File Source

For file collectors, there are the following options to configure the source [2]:

- **None**

[2] It is possible to configure the volume and size limits of the downloaded files. For further guidance, reach out to Arctera Support.

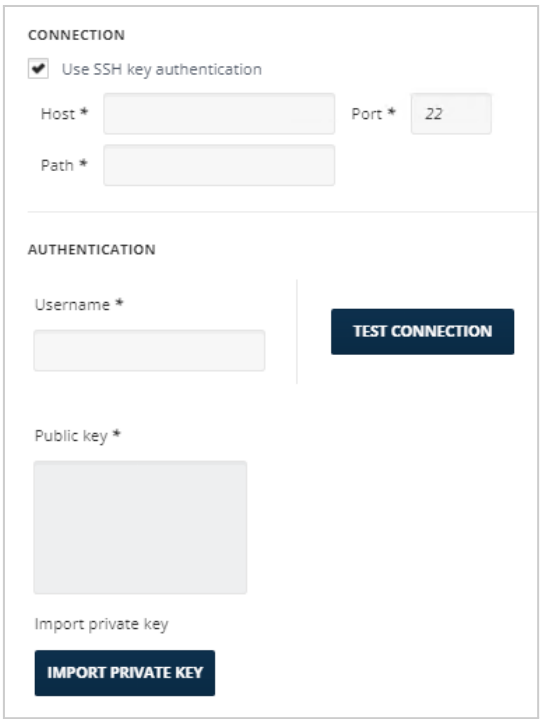
- **SFTP/FTP**
- **Amazon S3**
- **Azure Storage**

If **None** is selected, the files from the Import folder are processed.

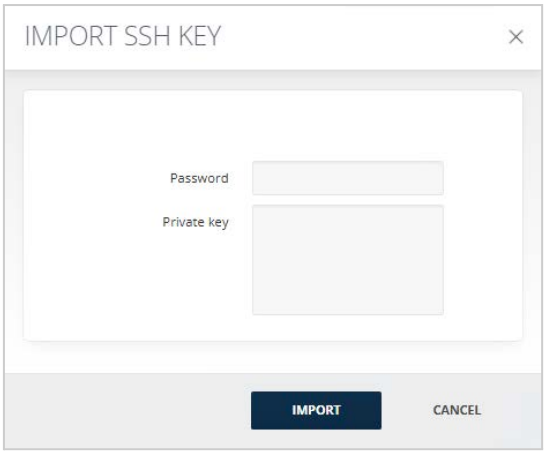
SFTP/FTP Configuration

To configure **SFTP/FTP:**

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 other source is 21.



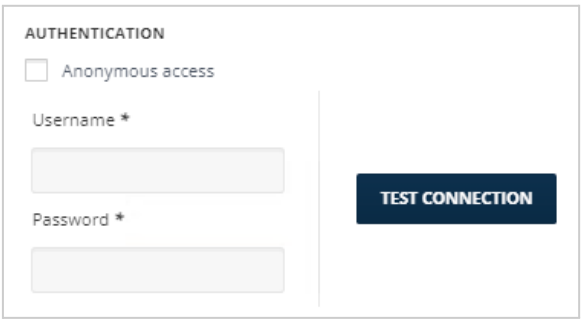
2. Make sure the connection settings match those of the SFTP server. Enter the **Path** to the required folder.
3. Enable **Use SSH key authentication** to open the configuration window. SSH key authentication is used for connecting to the source SFTP Server.
4. For Authentication, enter the **Username** provided by the source.
5. Click the **Import Private Key** button and **Import SSH Key** will open.
6. Enter the **Password** of the Private key, if it has a password.
7. Copy and paste the **Private Key**.



8. Click **Import** and the **Public Key** field will be populated automatically.

To Use security:

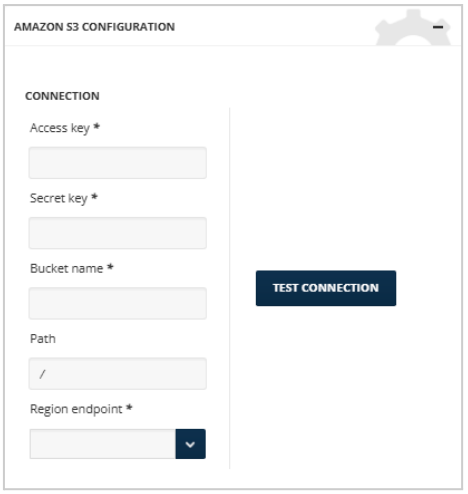
1. Choose **FTP connection type** from the **Connection Type** drop-down list. FTP can run in either passive or active mode. The information about the connection type should be provided by the FTP host. If you wish to use FTP over SSL, enable the **Use Security** checkbox and choose the connection method **Implicit SSL**, **Explicit SSL** or **SSH**.
2. Enter the **Username** and **Password** fields provided by the source.
3. Click **Test Connection**. If the connection is successful, a green check sign is displayed.
4. To enable anonymous FTP connections, enable the **Anonymous Access** checkbox which is the default setting.



Amazon S3 Configuration

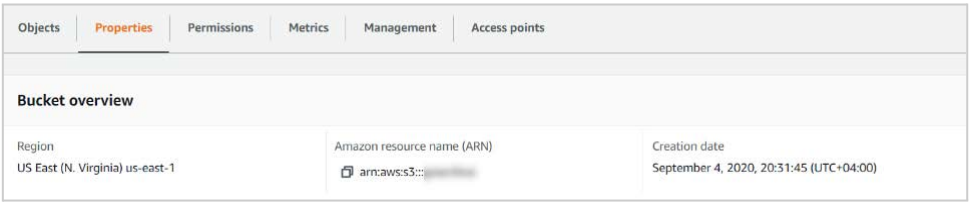
To capture data from **Amazon S3**, triggers and a Lambda function need to be created on the Amazon S3 site. The trigger is run when specific actions occur within a bucket and the source bucket items with their metadata are imported to the archive bucket. Merge1 will then capture the data from the archive bucket.

If the **Amazon S3** source is selected, the **Amazon S3 Configuration** window opens.



The following information is required:

- **Access key:** Enter the access key found under *Users* > *Security Credentials* in your Amazon S3 account. This field is required for authentication.
- **Secret key:** Enter the secret key obtained during the setup of *Security Credentials*. Save it securely, as this key is provided only once. If the secret key is incorrect, the connection will fail.
- **Bucket name:** Enter the name of the archive bucket where your data is stored. If the bucket name is invalid, data will not be retrieved.
- **Path:** If specified, data will be downloaded from the designated folder within the bucket. If left blank, all data from the bucket will be processed.
- **Region endpoint:** Enter the *Region Endpoint* located under *Bucket Overview* > *Properties* in your Amazon S3 bucket. Note that if the *Region Endpoint* is not set correctly, the archive content will not be captured or processed.



Azure Storage Configuration

To capture data stored from different sources in Azure Blob storage, Azure storage should be configured accordingly. For more information on how to configure Azure Storage, see **Configuring Azure Storage**.

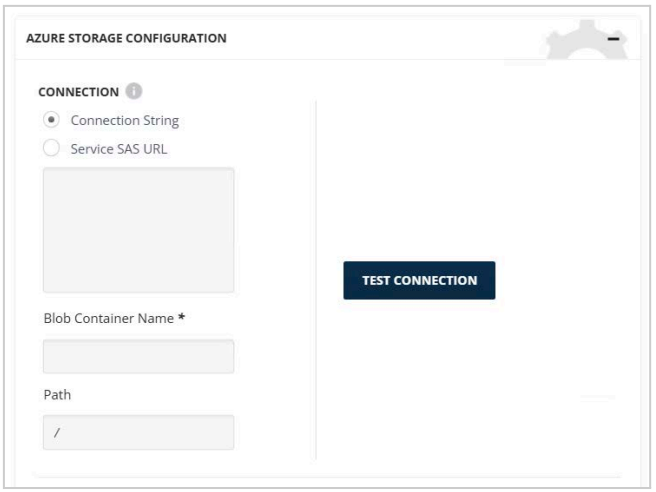
Using custom domains is not supported, the URL must point to one of the well-known Azure Storage endpoints listed below:

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

Merge1 will then capture the stored data from the storage.

To configure **Azure Storage**:

1. Enable **Connection String** and enter the **Connection String** copied in step 10.[3]
   Or,
2. Enable **Service SAS URL** and enter the Service SAS URL copied in step 10.[3]
3. Enter **Blob Container Name** from 11.
4. If the **Path** field is specified, data will be downloaded from the designated folder within the bucket. If left blank, all data from the bucket will be processed.

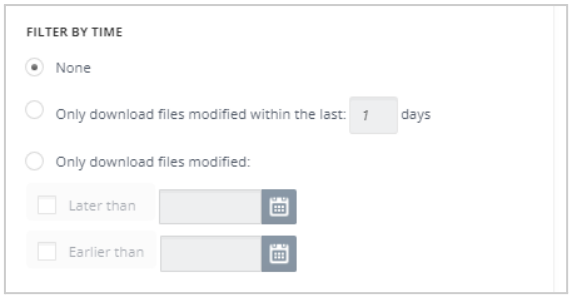


For **File Filter** a wildcard can be used to denote the file types to be included or excluded. Each type of filter is separated by the vertical pipe character |. For example: *.tar.gz | *.txt.

For Filter by Time:

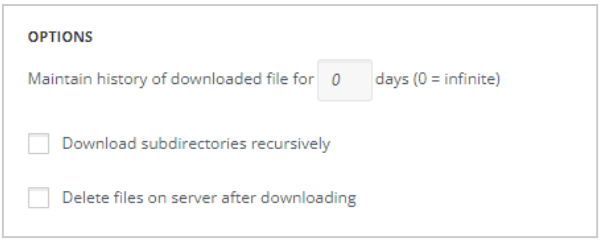
1. If **None** is selected, the data is not filtered by time.
2. When **Only download files modified within the last X days** is selected, only the data modified within the mentioned days will be downloaded.
3. When **Only download files modified earlier than/later than** is selected only the data modified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

[3] Only the Storage Account-level connection string and service SAS URL are supported.



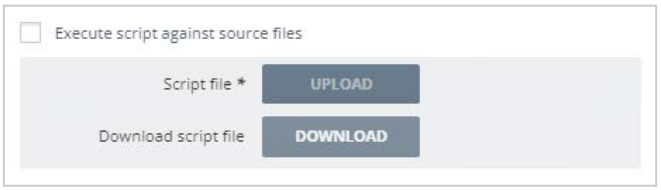
For Options:

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 the 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.



Execute Script Against Source Files

The following feature allows the user to modify the script manually before processing it.



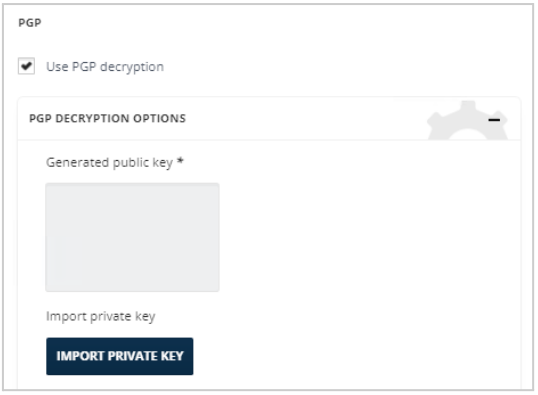
Note

The script file must be in either PS1 or BAT format and must not exceed the 100kb size limit.

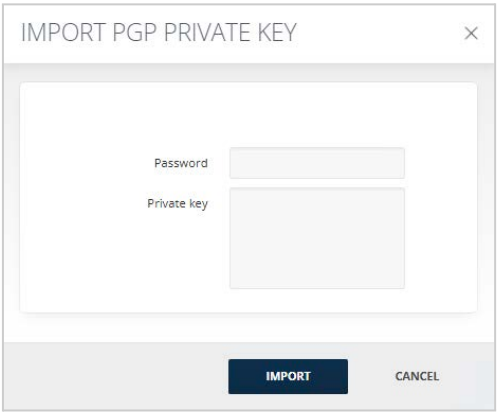
PGP Decryption

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**.



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.

Folders

Merge1 Folder is a required setting option. In case you miss to fill in the information, you will not be allowed to proceed to the next screen.

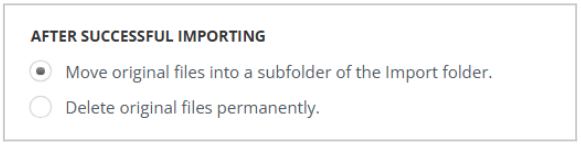
After successfully setting up the FTP/SFTP and PGP Configurations, you will have to change the folder configurations. In Merge1 you will have to specify the **Import folder**, where you can store the data after retrieving it from Amazon S3, as well as **Quarantine folder** where all the failed messages will be archived.

If you have subfolders under your **Import folder**, you can enable **Traverse subdirectories** to maintain the subfolder structure of imported data and include the data in your Yieldbroker Merge1.

After Successful Importing

Under **After Successful Importing** settings, you can provide Merge1 what to do with the original files. You can either **Move the original files in a subfolder within an Importer Folder** or you can **Delete the files**. Note that once deleted, the files cannot be recovered.

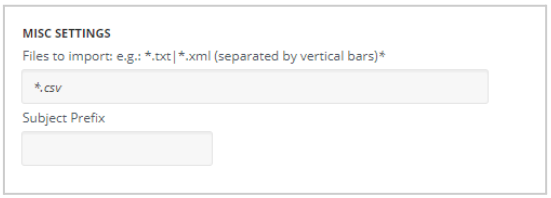
The files in Quarantine folder are not automatically reprocessed. During the next import, the same files from the FTP server or Import folder will be checked and, in case they are available, will be reprocessed.



Misc Settings

If you want to import specific files or file types, note them in the Files to import form. You can separate each file or filetype with a vertical bar I. Simply write the name of the file or use wildcards to import the whole filetype) (e.g., *.txt | *.xml). The default setting formats is *.csv as Amazon S3 parses messages with these source files.

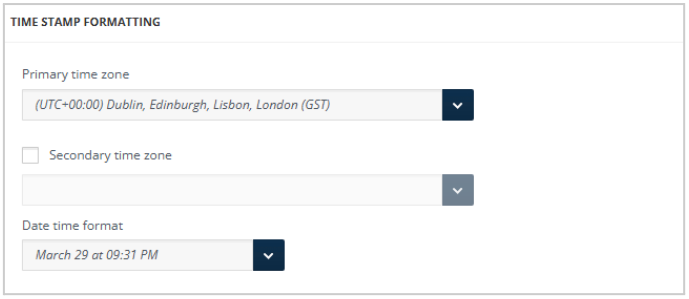
The **Subject Prefix** is added to the subject line of imported emails. This is useful for organizing imported data especially when multiple sources share a common target.



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.

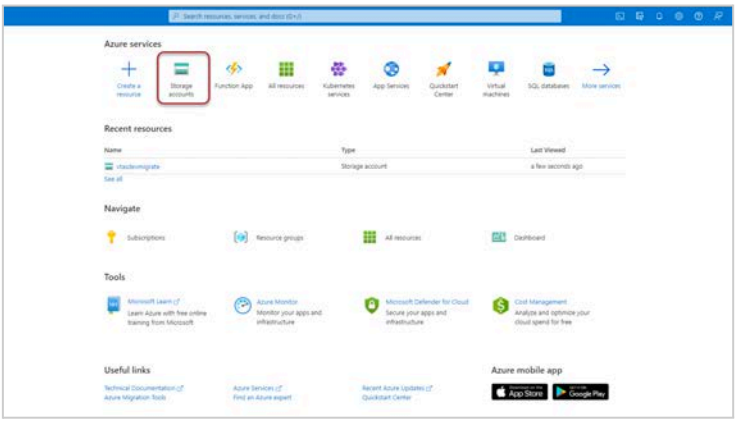
The format of the timestamp in the output message can also be specified from the six options in the **Date time Format** drop-down list.



Configuring Azure Storage

For Azure Blob storage:

1. Login to your Azure portal account.
2. Navigate to Storage Accounts.[4]



3. Click the account **Name**.

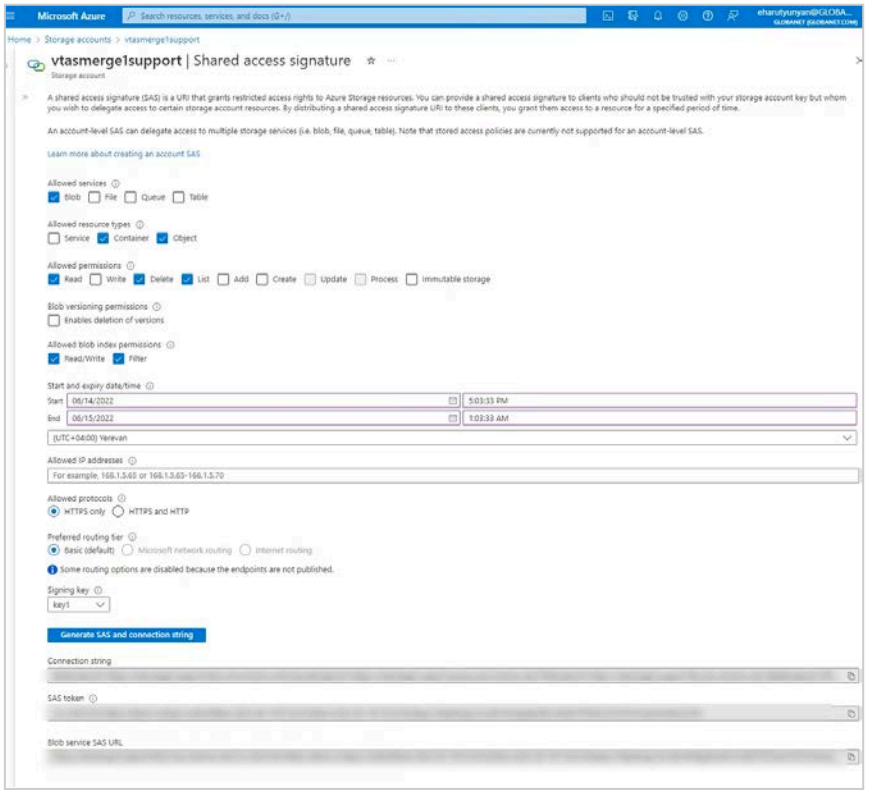
4. On the left side navigation pane, navigate to **Shared Access Signature**.
5. For **Allowed services**, enable **Blob**.
6. For **Allowed resource types**, enable **Container and Object**.
7. For **Allowed permissions**, enable:
   - Read
   - Delete[5]

[4] Only the Storage Account-level connection string and service SAS URL are supported.

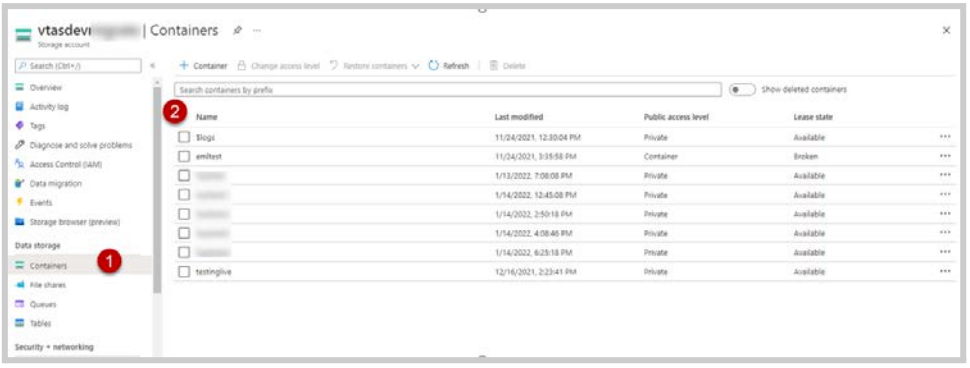
[5] This is needed in case the 6th step is enabled.

- 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** or **Blob service URL** for **Connection** configuration.



11. On the left side navigation pane, select **Containers** (1) and click the name of the container you want (2).



Amazon S3

Amazon S3 is a cloud-based object storage service developed by Amazon Web Services (AWS). It enables organizations to securely store, manage, and retrieve large volumes of data, offering high scalability, durability, and access control. Users can store documents, media files, and structured datasets while ensuring compliance with business and regulatory requirements.

The **Mergel Amazon S3 collector** integrates seamlessly with Amazon S3, allowing businesses to capture and archive content stored in S3 buckets. This ensures efficient data management, security, and accessibility for compliance and eDiscovery needs.

Activities Captured

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

For Mergel 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. The source bucket items with their metadata are imported to the archive bucket. Mergel will then capture the data from the archive bucket.

Collector Configuration

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

- **File Source**
- **Execute Script Against Source Files**
- **PGP Decryption**
- **Folders**
- **After Successful Importing**
- **Misc Settings**
- **Time Stamp Formatting**

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**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:

Supported Notifications

The importer supports the following notification preferences:

- **Quarantine file**
- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

Audio Video

The **Merge1 Audio Video collector** is designed to capture and process audio/video recording files. It parses metadata stored in CSV format and transforms source information to match the required output file structure. The collector applies predefined mapping based on an uploaded XML template, ensuring seamless data integration.

For more details on the mapping, corresponding to the source you will use it for, contact our support at Arctera Support.

Activities Captured [6]

- Messages

Captured activities can contain:

- 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.
- The CSV/TXT and the ZIP files should have the same name to process the files properly.

Collector Configuration

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

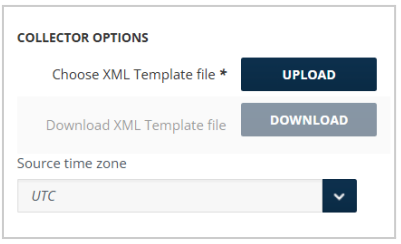
- **File Source**
- **Execute Script Against Source Files**
- **PGP Decryption**
- **Folders**
- **After Successful Importing**
- **Misc Settings**

Collector Options

Upload an XML template. The XML file should contain 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**.

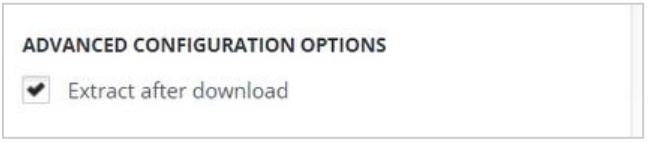
[6] In case the listed properties exist in the source file.

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. By default, Merge1 sets the **Source time zone** as **UTC**.



Advanced Configuration Options

When the **Extract after download** checkbox is enabled, the collector automatically unpacks ZIP archives that are not part of a paired file group (TXT+ZIP or CSV+ZIP). If the option is disabled, Merge1 will automatically quarantine the files.



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 [7].

```
<?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>
```

2. 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>
```

[7] Note that if you want attachments to be processed properly, they should be in the same zipped folder and have **attachments.zip** format.

```
            <delimiter>";"</delimiter>
            <append>""</append>
        </datatype_options>
    </column>
    <column>
        <order>2</order>
        <name>Call Id</name>
        <datatype>String</datatype>
    </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>
    <column>
        <order>4</order>
        <name>End Date</name>
        <datatype>DateTime</datatype>
        <datatype_options>
            <format>XX/DD/YYYY HH:MM:SS</format>
        </datatype_options>
    </column>
    <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>
```

3. 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>
```

Note

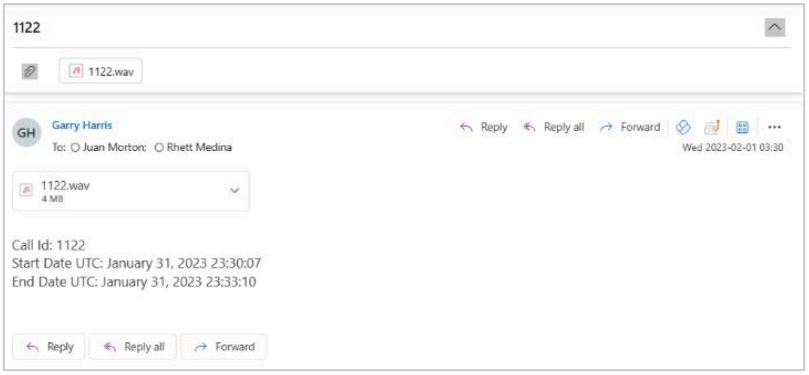
Valid nodes in the XML template are 'version', 'options', 'columns', and 'mappings'. In case there is a 'threading' node or any other node outside the mentioned valid list in the template, an error (example for threading: The `<configuration/threading>` tag is unrecognized) will be thrown and the processing will be stopped.

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**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Quarantine file**
- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

BlackBerry

BlackBerry was once a leading smartphone for enterprise communication, offering secure messaging and business-focused features.

The **Merge1 BlackBerry collector** allows organizations to capture and archive BlackBerry communications, integrating them into existing email archives - whether on-premise or in the cloud - to support compliance and data retention.

Activities Captured

- Pin-to-pin
- Messenger
- SMS/MMS

Collector Configuration

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

- **File Source**
- **Execute Script Against Source Files**
- **PGP Decryption**
- **Folders**
- **After Successful Importing**
- **Misc 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

If you want to manually set up the **Source time zone**, select the relevant one from the drop-down list. Merge1 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, Merge1 sets the **Source time zone** as **Local Timezone**.

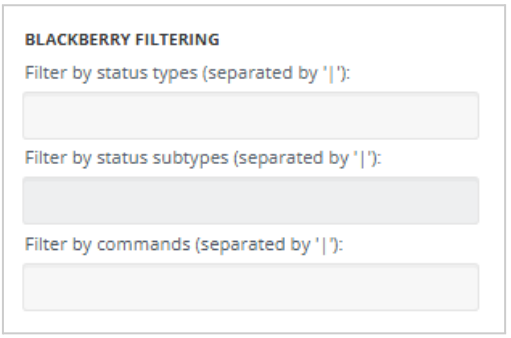
BlackBerry Filtering

Use **BlackBerry Filtering** configurations to determine which status types, subtypes, or commands are imported. Separate each name with the vertical bar (**|**). Note, that wildcards are NOT supported for the following field. Each source type has different filtering options.

Each source type has different filtering options:

- **P2P** type can be filtered with status types and commands.
- **SMS** sources can be filtered by all displayed options.
- **Messenger** type can be filtered only by commands.
- **VideoChat** type cannot be filtered at all.

If you want to process the whole data, leave all three fields blank.

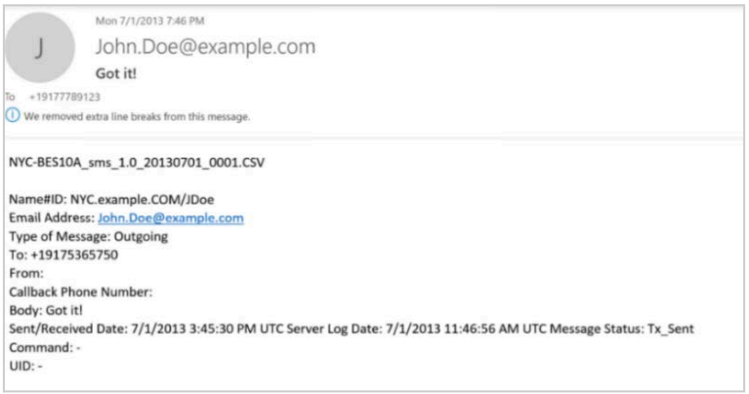


Next Steps

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

- Monitored Users (N/A)
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Quarantine file**
- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

Bloomberg

Bloomberg is a leading provider of financial news, market data, and analytics, offering real-time insights to businesses and investors worldwide.

The **Merge1 Bloomberg collector** processes Bloomberg-generated data in file sets, including emails, instant messages, attachments, and disclaimers.

Activities Captured

- Instant Bloomberg messages (`.ib`), invites (`.ib`), attachments (`.att`)
- Email messages (`.msg`), attachments (`.att`), disclaimers (`.dscl`)

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`.
- The 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.

Collector Configuration

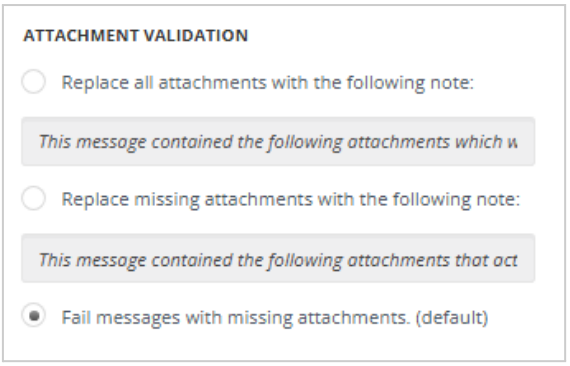
For information on how to configure the following sections of the **Source** tab, see:

- **File Source**
- **Execute Script Against Source Files**
- **PGP Decryption**
- **Folders**
- **After Successful Importing**
- **Misc Settings**

Attachment Validation

Merge1 enables you to develop customized notes for attachment validation.

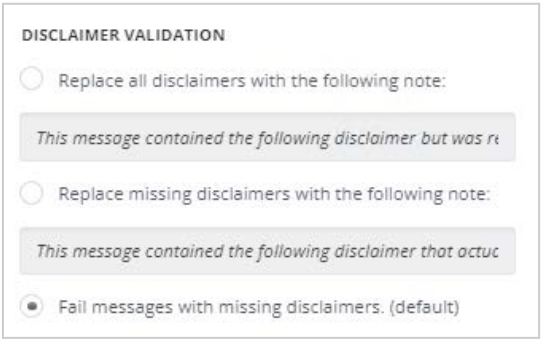
- If you select the **Replace all the attachments with the following note** and input your custom note, all the attachments to the messages will not be processed and in their place the input note will be added to the message.
- If you select the **Replace missing attachments with the following note**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



Disclaimer Validation

Merge1 enables you to develop customized notes for disclaimer validation.

- 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.
- The default setting is **Fail messages with missing disclaimers**, so the messages that do not have disclaimers are failed and can be viewed under the Reports. Note that **Advanced reprocessing** should not be selected for this to happen.

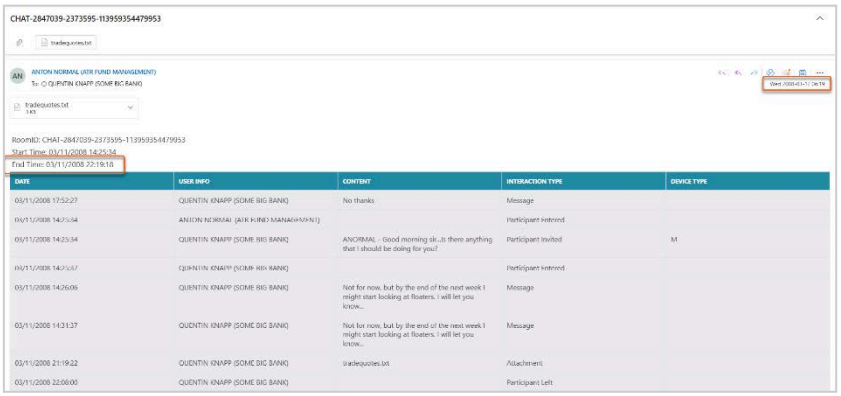


Bloomberg Options

There are the following Bloomberg options:

- **Advanced reprocessing**: For more details see **Advanced Reprocessing: Attachment Validation** and **Advanced Reprocessing: Disclaimer Validation**.
- **Use legacy Bloomberg importer style of date processing**: Merge1 will scan the date and time stamp of dump files and assume their time zones correspond with those of the device on which Merge1 is running (recommended for dump files created before March of 2009). If this option is not selected, Merge1 will assume 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).

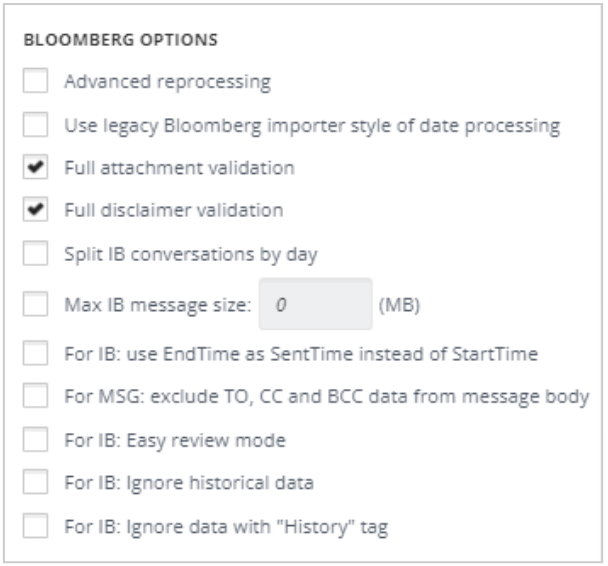
- **Full attachment validation**: If enabled, the entire source (file group) will be quarantined, in case the attachment of a message is missing or corrupted, i.e., the **Fail messages with missing attachments** under **Attachment validation** will be ignored. If disabled, the selection under **Attachment validation** will be applied to the messages that are missing attachments.
- **Full disclaimer validation**: If enabled, the entire source (file group) will be quarantined, in case the disclaimer of a message is missing or corrupted, i.e., the **Fail messages with missing disclaimers** under **Disclaimer validation** will be ignored. If disabled, the selection under **Disclaimer validation** will be applied to the messages that are missing disclaimers.
- **Split IB conversations by day**: If checked messages with the same UTC Day will be imported in one message. Note that if **Split IB conversations by day** is enabled, `DateTimeUTC` is prioritized.
- **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. See the examples below.



Note that in the above example the timestamps in the body message are UTC, while the SentTime of the generated output is UTC +4. The sent time of the message is adjusted to the time zone of the device it is opened on.

Also note that the mapping of sent time can be changed using the **For IB: use EndTime as SentTime instead of StartTime** checkbox.

- **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.



Advanced Reprocessing: Attachment Validation

Advanced reprocessing is for processing messages that failed because of either missing attachments or disclaimers.

If **Advanced reprocessing** and **Full attachment validation** is enabled and **Fail messages with missing attachments** is selected, the following happens: In case an attachment file is either missing or corrupted, Mergel starts processing the source files and quarantines them due to missing attachments. When running the next import, on the condition that the missing attachment is available now, Mergel successfully processes all the files. This way Mergel processes the messages previously quarantined just like any new complete file group.

If **Full attachment validation** is disabled: In case the attachment file is either missing or corrupted, Mergel starts processing the source files. The messages that have available attachments are processed and sent to the target. The messages that have reference to missing attachments are not delivered to the target, they are stored in the database and marked as failed. The record of these failed messages can be found in **Reports > Report Type** (Missing Attachment Failure). When running the next import, on the condition that the missing attachment is available now, Mergel reprocesses the failed messages.

Advanced Reprocessing: Disclaimer Validation

If **Advanced reprocessing** and **Full disclaimer validation** is enabled and **Fail messages with missing disclaimers** is selected, the following happens: In case disclaimer file is either missing or corrupted, Mergel starts processing the source files and quarantines them due to missing attachment. When running the next import, if the missing disclaimer is available now, Mergel successfully processes all the files. So, Mergel processes the messages previously quarantined just like any new complete file group.

If **Full disclaimer validation** is disabled: In case disclaimer file is either missing or corrupted, Mergel starts processing the source files. The messages with available disclaimers are processed and sent to the target. The messages that have reference to missing disclaimers are not delivered to the target, they are stored in the database and marked as failed. The record of these failed messages can be found in **Reports > Report Type** (Missing Disclaimer Failure). When running the next import, in case the missing disclaimer is available now, Mergel reprocesses the failed messages.

Processing Bloomberg Firm-Level Files

To process Bloomberg's firm-level files, set **Ignored** target as the default. Configure a filter to match segments for the necessary account numbers and route them to a secondary target, and likewise, another filter to match segments to unnecessary account numbers and route them to a **Failed** target. Use the reporting feature in **Importer Settings** to discover new account numbers (Reporting). Ensure **Unconditional hit default target** and **Process all filters** are disabled (Filtering). However, if you intend to set other targets for your importer, click the exact target type to view setup details.

Managing Quarantine Files

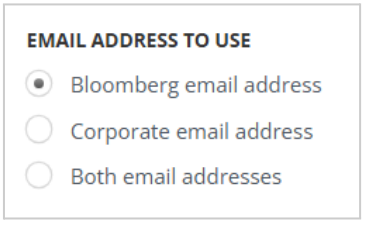
Files are quarantined for two main reasons: either the file format is incorrect and cannot be parsed, or an IB (instant messages) or MSG (message) file is missing attachments or disclaimers. To resolve this, the client requests Bloomberg to resend ATT (attachments) or DSCL (disclaimer) files. The corrected file, including the quarantined IB or MSG file, is then placed into the IMPORT folder (named during configuration). When the importer runs again, the data is reprocessed, provided **Full attachment/disclaimer validation** and **Advanced reprocessing** are not enabled.

An alternative is to process messages without attachments or disclaimers. To do this, **enable Full attachment/disclaimer validation** and set the default to **Replace missing attachments/disclaimers with the following note**. This option is used when only a reference to the missing file name is required, and the attachment or disclaimer itself is not needed. A reference for the missing attachment will then be included in the delivered messages.

Email Address to Use

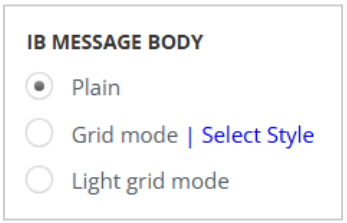
Select the email address type you would like Merge1 to use when processing data from users that have both their personal email address, and their corporate email address registered on Bloomberg.

By selecting **Both email addresses**, there will be the choice to set the Bloomberg or corporate email as a primary address.

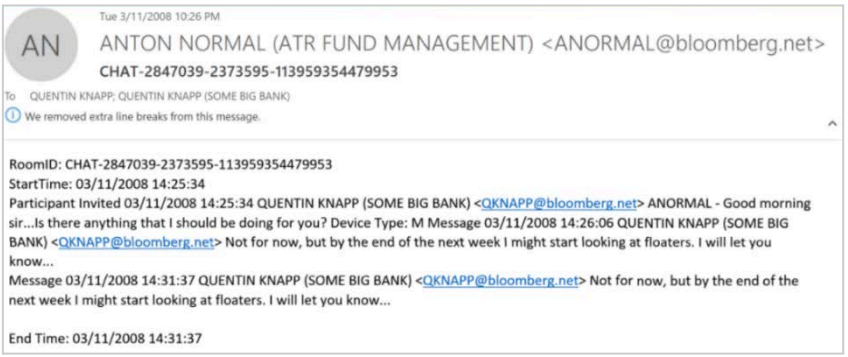


IB Message Body

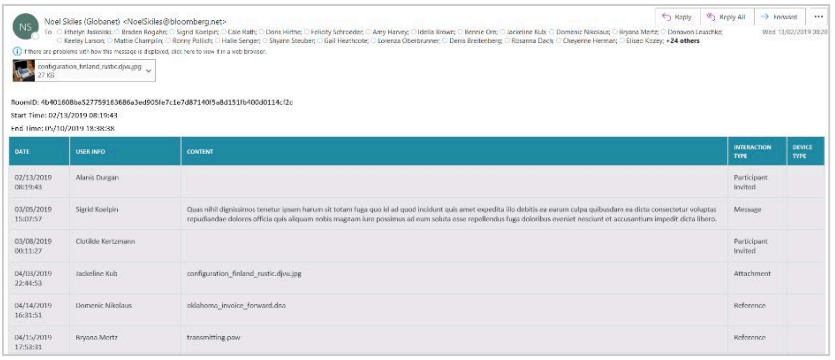
This setting determines how imported messages are displayed in the target. There are the following output message body options:



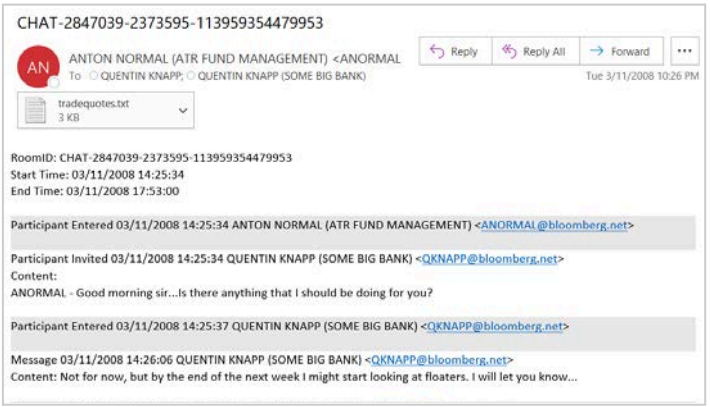
- **Plain**: Displays the message in a simple text format.



- **Grid mode**: Displays output message content in a compact grid format for structured and efficient viewing. The information is structured into the following columns:
    - *Date*: Shows the date and time the message was sent.
    - *User info*: The user's Full Name (Company Name) <Email Address>.
    - *Content*
    - *Interaction type*: Contains information about participants and messages, such as Participant Entered, Participant Left, Participant Invited, Message, and Attachment.
    - *Device type*: If the message was sent from a mobile device, it will be displayed as M in this field.

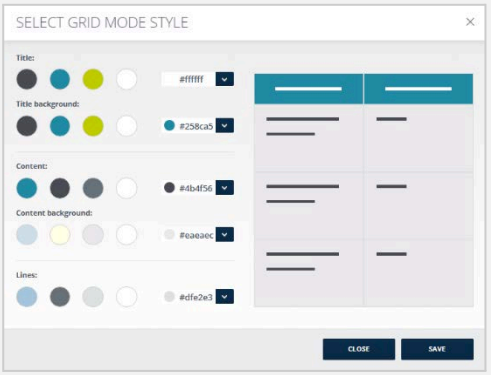


- **Light grid mode**: Displays data in a two-toned layout, making it visually distinct and easier to view while displaying limited metadata.



Tip

In **Grid mode**, the color scheme can be adjusted through the **Select Style** pop-up menu:



Time Stamp Formatting

For more details on how to configure timestamps, see **Time Stamp Formatting**.

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**

Supported Notifications

The importer supports the following notification preferences:

- **Quarantine file**
- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

Box

Box is a cloud content management platform that enables businesses to securely store, manage, and collaborate on their digital assets. Designed for flexibility and scalability, Box provides a suite of cloud-based content services that allow organizations to streamline workflows and enhance productivity.

The **Mergel Box collector** processes Box-generated content, capturing files and metadata for seamless integration into existing data management systems. By leveraging the Box Content API, organizations can efficiently archive and retain critical business information while ensuring compliance.

Activities Captured

- Uploads
- Downloads and task assignments[8]
- Comments
- Box quick notes (in Box generated special format)
- New version uploads (in the message subject, event type is displayed as edited)
- Tasks completed/rejected (displayed in the message body as task deleted)
- Comments deletion
- Move/Copy/Edits (only Box quick notes)/Preview/Rename activities
- Reports export

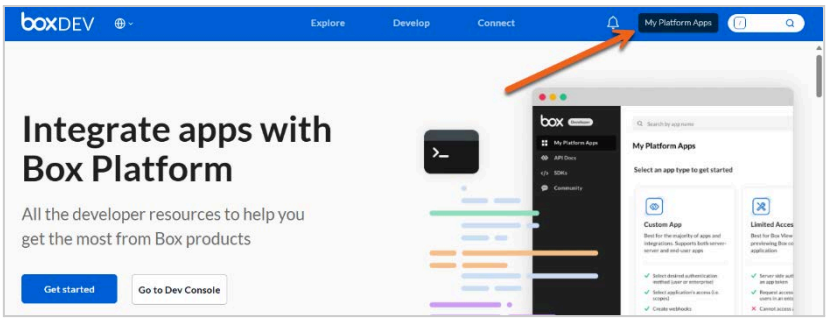
Note

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

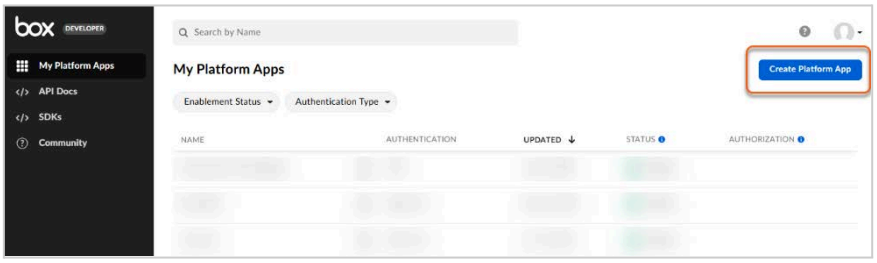
To create a Box application:

1. Sign in to Box Developer.
2. Go to **My Platform Apps**.
3. Click **Create Platform App**.

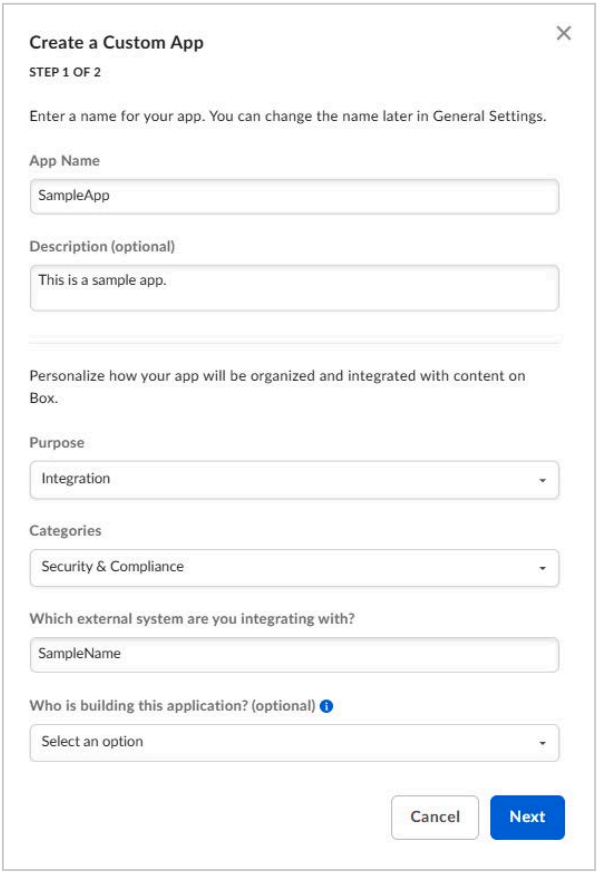


[8] During the first run, only the folder structure is retrieved.

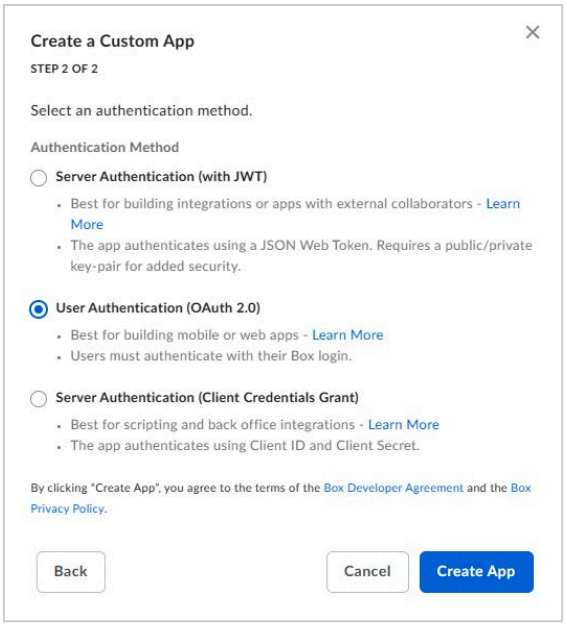
4. Choose **Custom App**.



5. On the opened window, enter the following details:
   5.1. **App Name**: Provide an app name.
   5.2. **Description**: Briefly describe the app.
   5.3. **Purpose**: Select the purpose of the app from the drop-down menu.
   5.4. **Categories**: Select applicable categories from the drop-down menu.
   5.5. **System Name**: Enter the system being integrated.
   5.6. Click **Next** to continue.

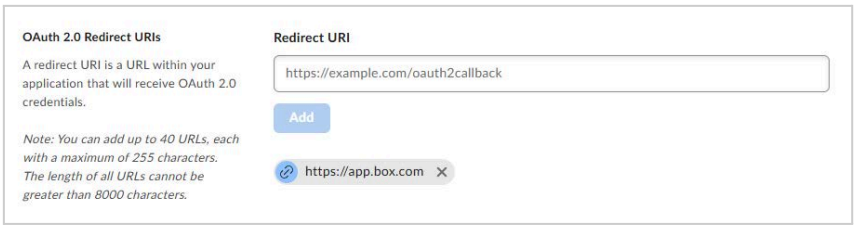


6. Select the **User Authentication (OAuth 2.0)** method and click **Create App**.



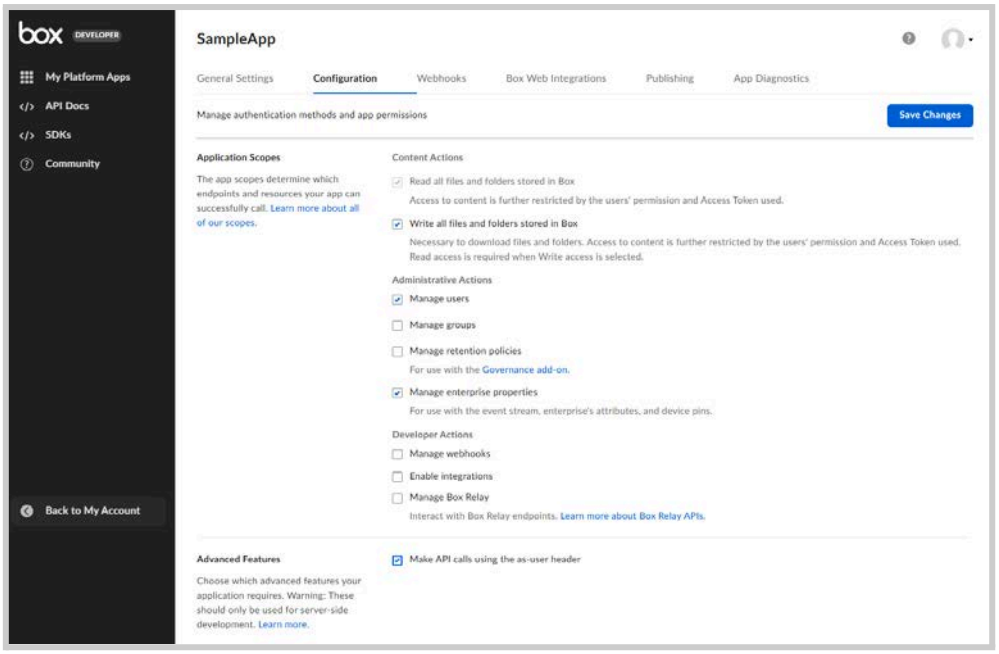
7. Go to **Configuration > OAuth 2.0 Credentials**, then copy and save the **Client ID** and **Client Secret**.

8. In the Redirect URIs field add the URL of your local Merge1 environment in the following format: `https://<merge1_instance>/Configuration/OAuthCallback`, click **Add**.



9. 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

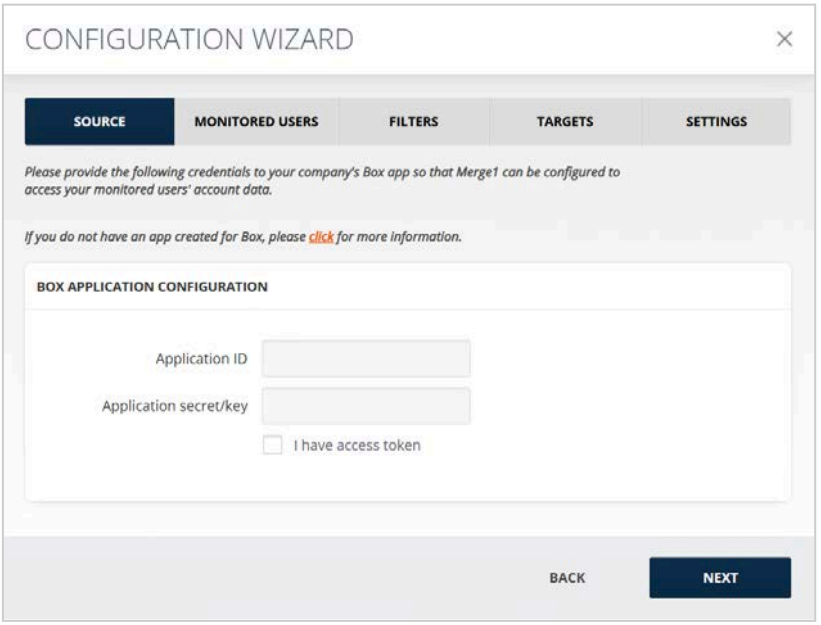


10. Click **Save Changes**.

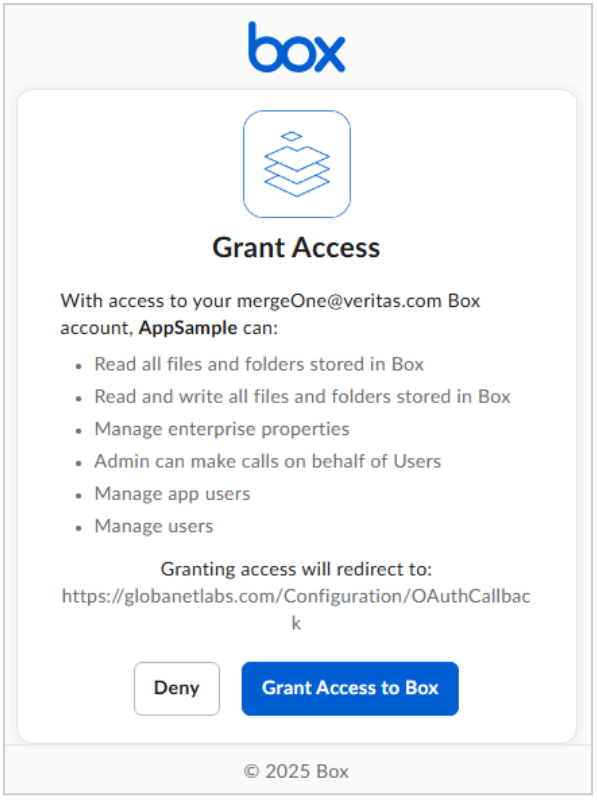
Collector Configuration

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.



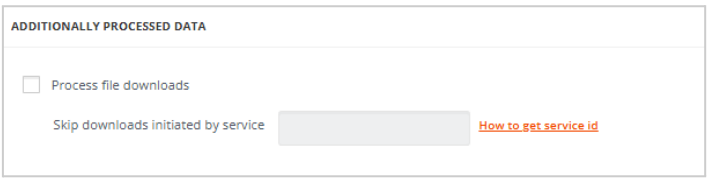
2. A pop-up window will open (ensure that the pop-ups are not disabled in the browser window). **Grant access to Box** to let the app access the specified resources for all users in the organization.



Additionally Processed Data

Once you set up the Box application, you can also configure a few optional settings.

- **Process file downloads**: If checked, it processes download file events from the events feed in Box. Merge1 downloads the files from Box, attaches them to messages, and records them as download events. With each cycle, the number of imported download events increases exponentially.
    - **Skip downloads initiated by service**: Enter the application ID of the downloading service. Downloads performed by this application (if connected to Merge1) will be ignored and not processed by Merge1. Follow these steps to retrieve the ID:
        1. Sign in to Box Developer.
        2. Go to **My Platform Apps**.
        3. Select your application to navigate to its details page.
        4. Copy the last numeric value from the URL, e.g., `https://<merge1_instance>.app.box.com/developers/console/app/{NUMERIC-VALUE}`.



Advanced Configuration Options

For more details on how to configure advanced configuration options, see **Advanced Configuration Options**.

Attachments Configuration

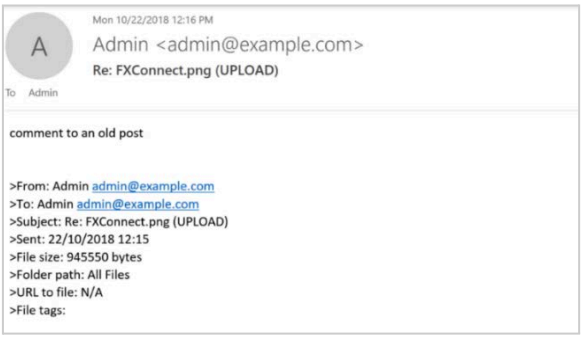
For more details on how to configure attachments, see **Attachments Configuration**.

Next steps

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

- **MONITORED USERS**
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

CellTrust

CellTrust is a trusted provider of secure and compliant mobile communication solutions for regulated industries. Its platform enables organizations to manage voice, text/SMS, and chat communications while integrating seamlessly with leading archiving and e-discovery providers.

The **Merge1 CellTrust collector** processes CellTrust-generated communications, capturing and archiving messages to support compliance and data retention across enterprise environments.

Activities Captured

- Messages

Captured activities can contain:

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

Collector Configuration

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

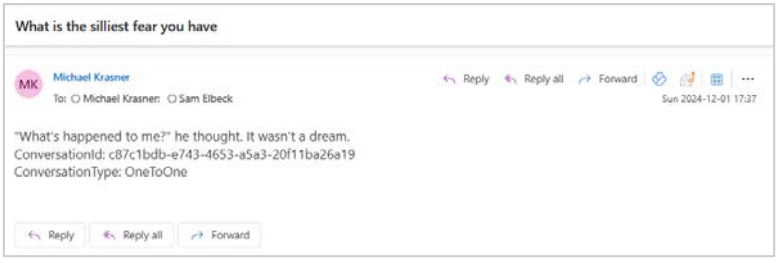
- **File Source**
- **Execute Script Against Source Files**
- **PGP Decryption**
- **Folders**
- **After Successful Importing**
- **Misc Settings**

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**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Quarantine file**
- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

ChatGPT

ChatGPT is a powerful 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 **Merge1 ChatGPT collector** captures communication that occurs between users and the AI assistant.

Activities Captured

- User prompts
- User uploaded files
- AI responses

> **Note**
>
> Due to current API limitations, the following are not captured:
> - User-uploaded expired files (Refer to Chat and File Retention Policies in ChatGPT for more details)
> - Files generated as an output of AI responses

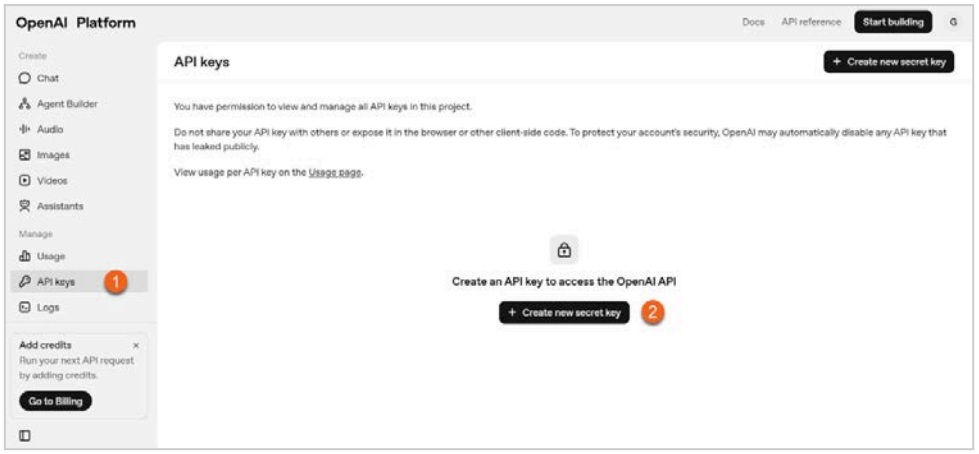
Acquiring an API Key and Workspace ID

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

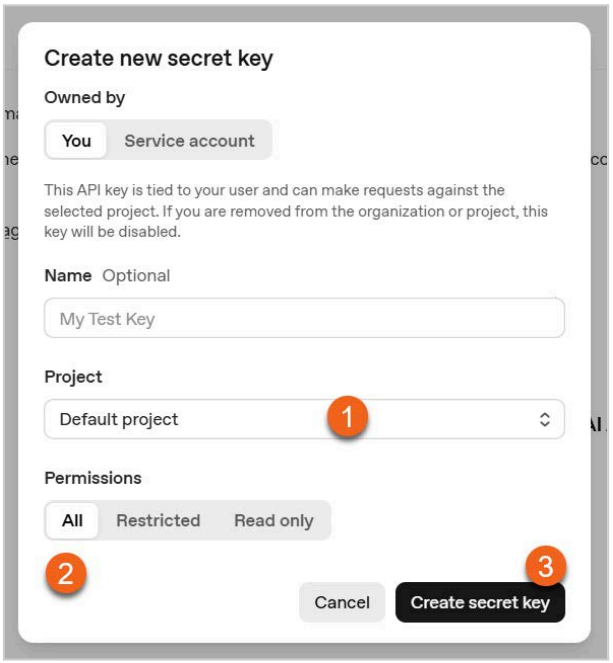
Generating an API Key

Creating a new API Key

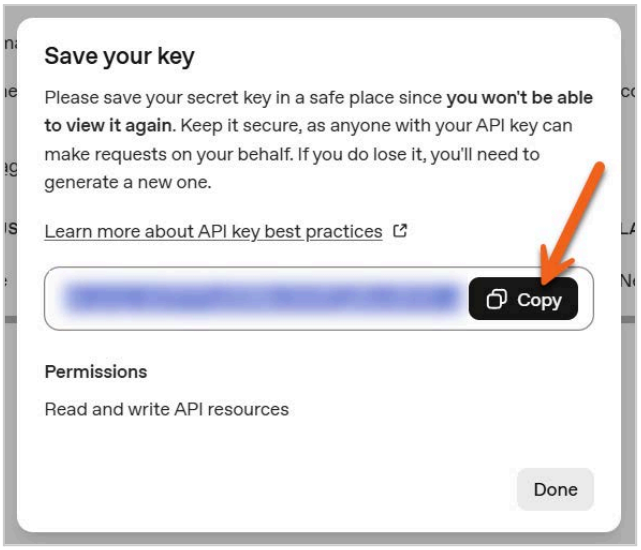
1. Navigate to the **OpenAI Platform** (https://platform.openai.com/api-keys) and log in. Verify that the correct organization is selected in the organization picker menu (usually found in the top right corner).
2. Click **Create new secret key**.



3. In the pop-up window:
   3.1. Leave **Project** set to **Default Project**.
   3.2. Leave **Permissions** set to **All**.
   3.3. Click **Create secret key**.



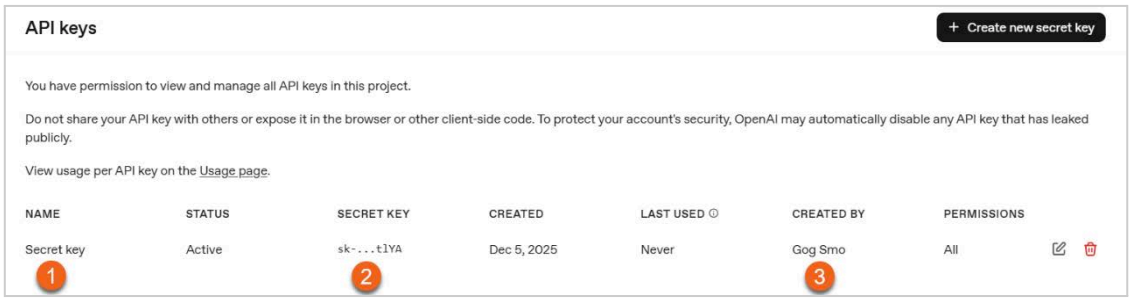
4. Copy the generated API key immediately and store it securely (it can only be viewed once).



API Key Verification and Scope Granting Request

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

1. Send an email to support@openai.com with the subject line, "API Key Verification and Scope Granting Request", including the following details in the body:
    1.1. The **Key Name**
    1.2. The **last 4 digits of the API Key**
    1.3. The **Created By** name
    1.4. **Requested scope**: **`read`**.

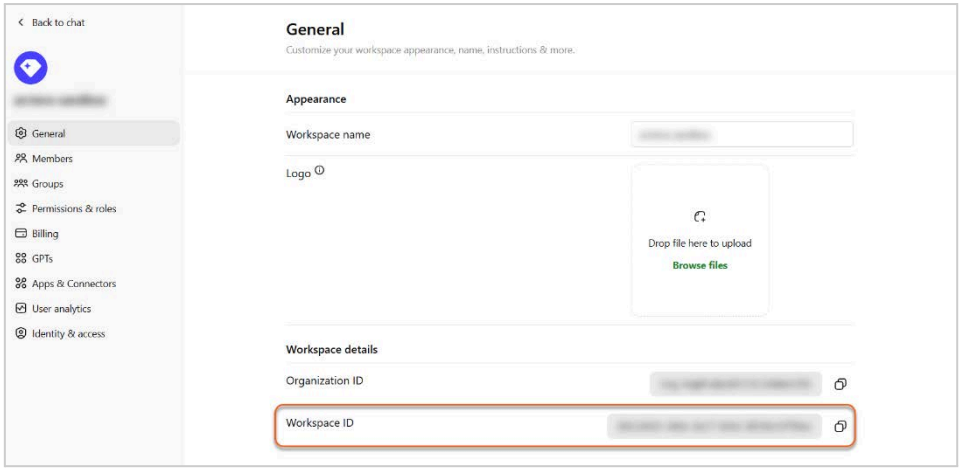


2. Wait for confirmation from OpenAI regarding the key verification and scope granting.

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.

Retrieving the Workspace ID

1. Navigate to the **ChatGPT Enterprise Admin Console** at https://chatgpt.com/admin.
2. Copy the **Workspace ID**. Use this credential to configure the collector.



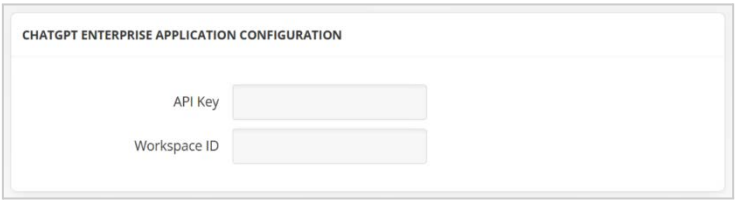
Configuring the Collector in Mergel

Adding the Importer

For details on adding the importer, see **Adding a New Importer**.

ChatGPT Enterprise Application Configuration

For configuring the **ChatGPT Enterprise** application add the previously saved **API Key** and **Workspace ID**.



Advanced Configuration Options

For more details on how to configure advanced configuration options, see **Advanced Configuration Options**.

Threading and Formatting

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

Choose how imported messages should be displayed in the target. The available output message body formats are:

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

Note

The **Pure body** mode is active ONLY if the **No threading** mode is checked.

Attachments Configuration

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

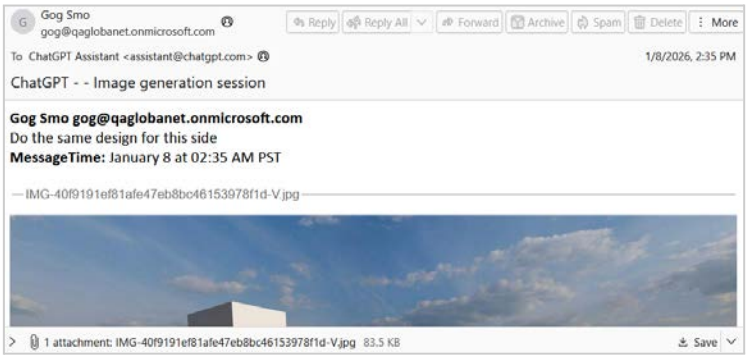
Otherwise, additional configurations will open for setup. See **Attachments Configuration**.

Next Steps

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

- MONITORED USERS
- FILTERS
- TARGETS
- IMPORTER SETTINGS

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

Chatter

Chatter is an enterprise collaboration platform from Salesforce, designed to enhance communication and information sharing within organizations. It enables teams to connect, collaborate, and exchange updates in a secure cloud-based environment.

The **Mergel Chatter collector** integrates Chatter communications into data management systems, ensuring comprehensive data capture and compliance. To import Chatter data, Mergel requires authentication via an Admin user's personal token and the publication of triggers on the Chatter site. These triggers generate posts in designated channels, allowing Mergel to capture updates, deletions, and edits. For more information on triggers, see **Installation Instructions** document listed in the **References**.

Mergel supports **Shield Platform Encryption** without additional configuration, ensuring encrypted data remains protected while being decrypted via the Salesforce API. For organizations with a host domain, Chatter Cipher Cloud can be utilized for secure data management.

Activities Captured

- Posts
- Files
- Comments
- Shares (including group posts)
- Comments of shared posts
- Deletes (requires triggers)
- Edits (requires triggers)
- Links
- Polls
- Private chats
- Group chats
- Feed poll choices (If *Modify all data* permission is enabled)
- New events/task contacts/opportunities/cases/leads
- All online communications, including attachments and deleted information (if the triggers are set)

Activities not Captured

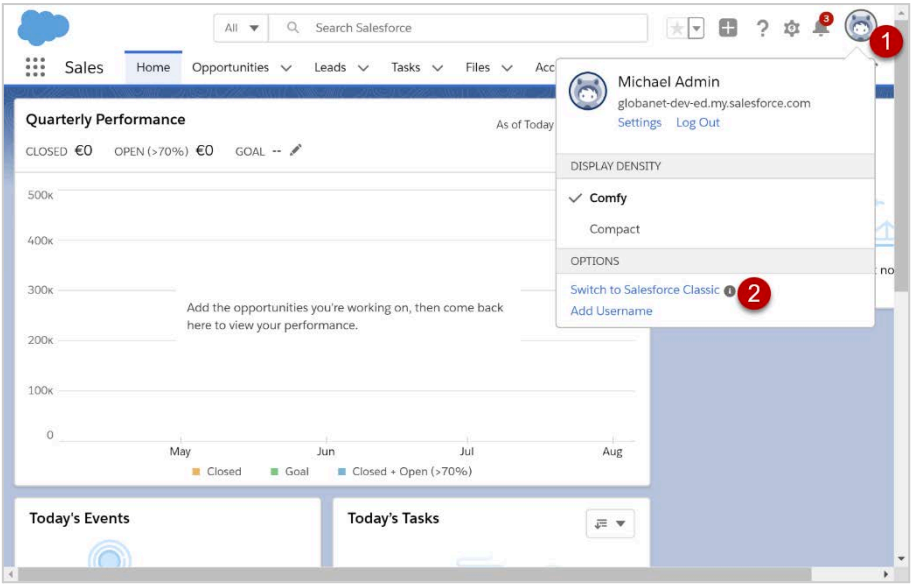
- Log a call
- Topics

Creating a Salesforce Application

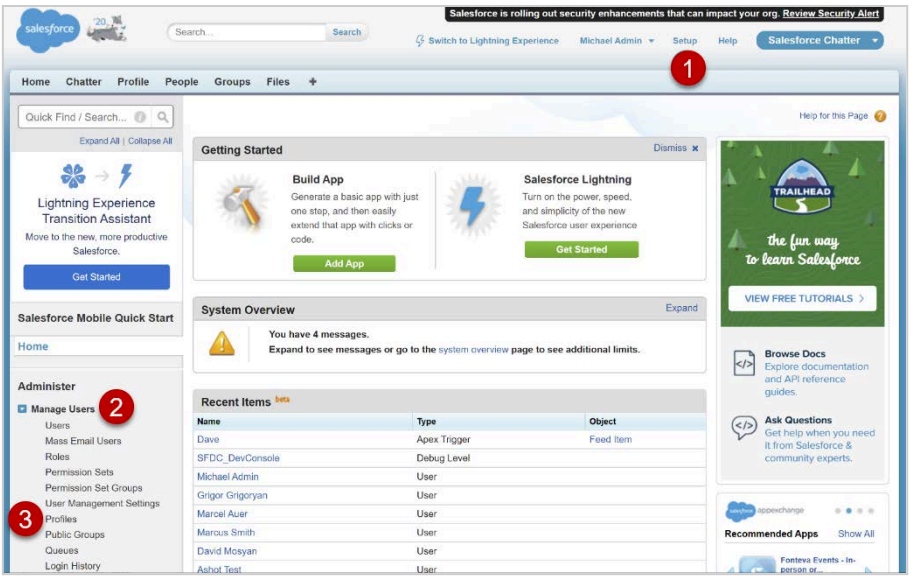
To perform the steps below you will need a Salesforce account with a System Administrator profile. If you do not have access to a System Administrator user, please contact your Salesforce admin and ask for permissions.

Step 1: Creating a profile

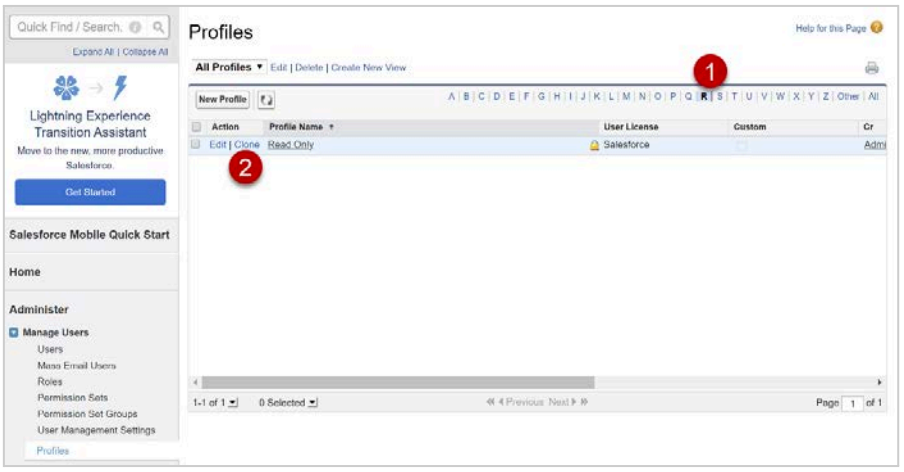
1. Login to Salesforce using an account that has the System Administrator profile and switch to **Salesforce Classic** (if you are using the Lightning Experience).



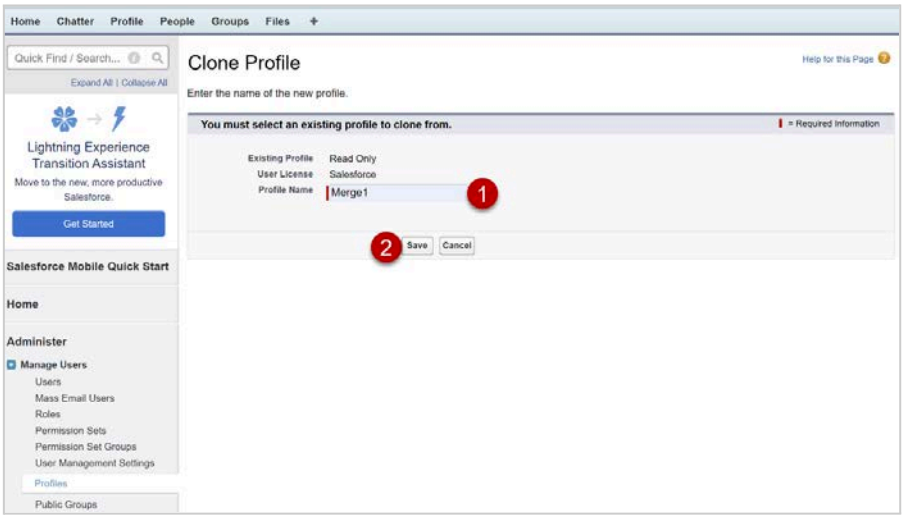
2. Click **Setup**, then expand **Manage Users** and click **Profiles**.



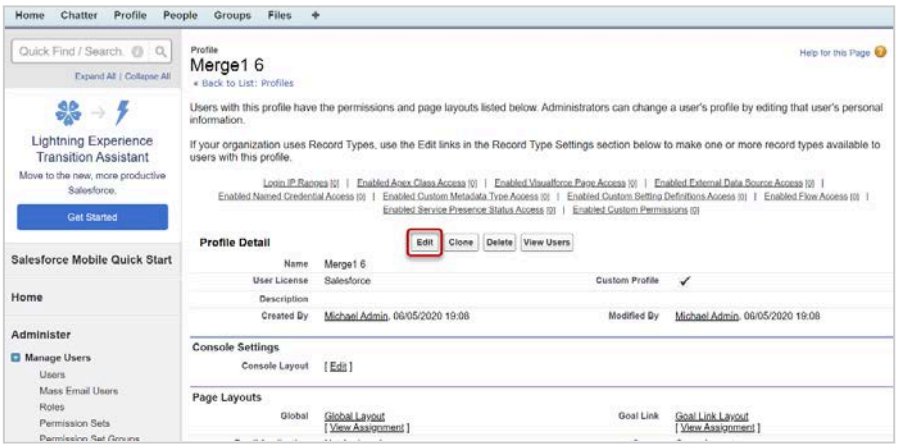
3. Find the **Read Only** profile and click the **Clone** button.



4. Enter a **Name** for in the **Profile Name** field and click the **Save** button.



5. Click **Edit**.



The required administrative permissions for Merge1 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).

6. Under **General User Permissions**, make sure the following checkboxes are enabled:

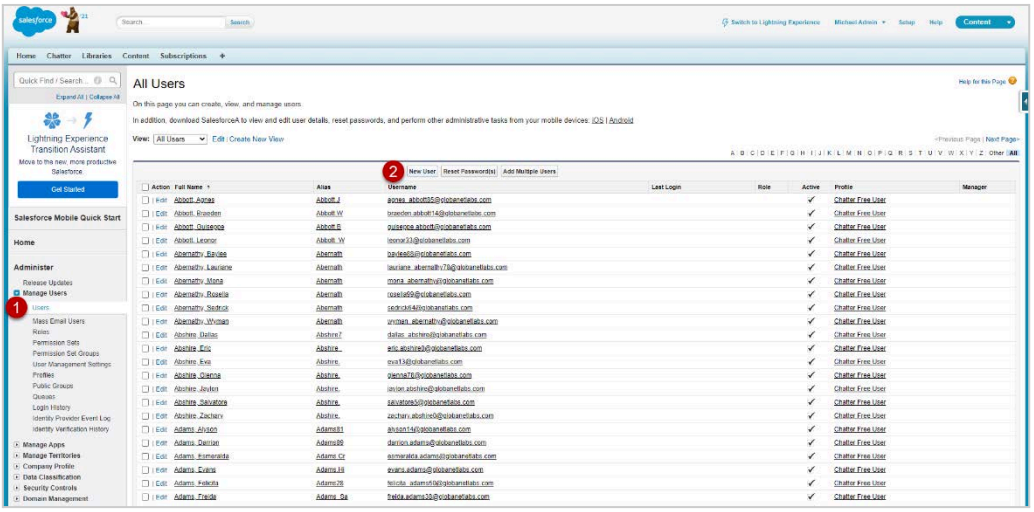
   - Access Activities
   - Allow View Knowledge
   - Knowledge One

7. Under **Standard Object Permissions**, disable all the **Create**, **Edit**, **Delete** and **Modify All** checkboxes. Only the **Read** and **View All** permissions should stay.

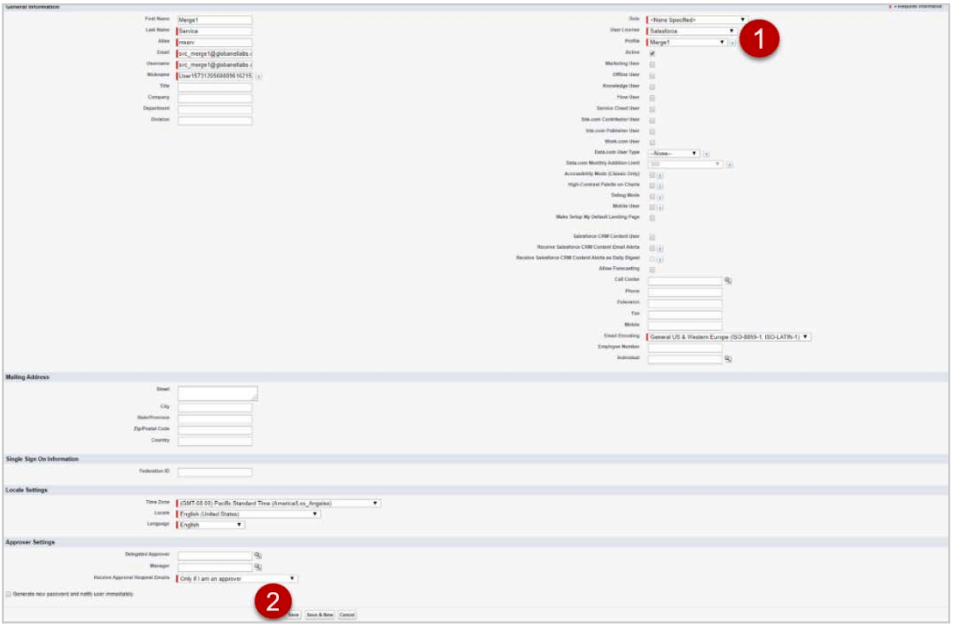
8. Scroll down and click **Save**.

Step 2: Creating a User (Service Account)

1. Go to the **Users** page and click **New User**.

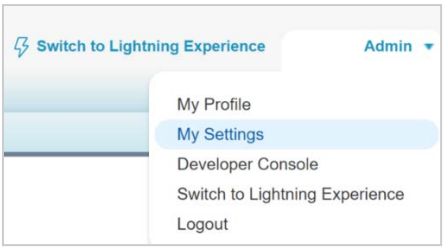


2. Populate the required fields, select **Salesforce** as **User License**, the profile created in step 1 from the **Profile** drop-down list, scroll down and click **Save**.

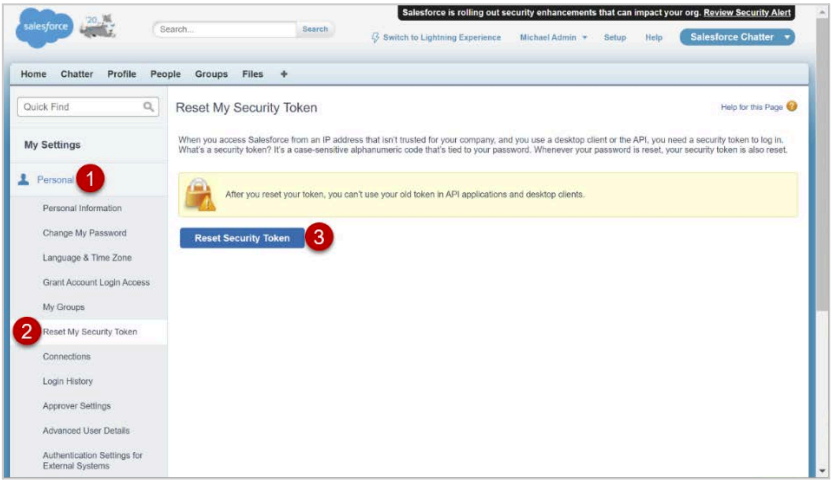


Step 3: Retrieving Access Token

1. Click your **Username** at the top right corner of the screen and select **My Settings**.

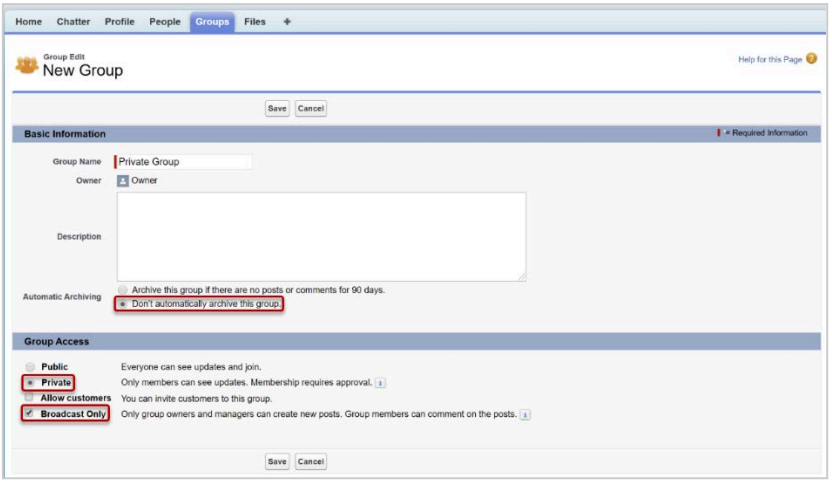


2. In the left-hand navigation pane, under the **Personal** section, choose **Reset My Security Token**, then click **Reset Security Token**. The new token will be sent to the email associated with your account.

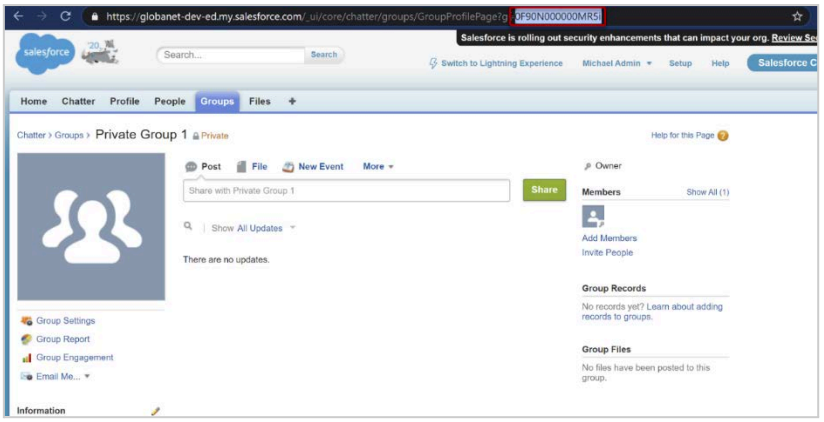


If you want to enable Merge1 to collect deleted or updated comments and posts in Chatter, ask your Salesforce administrator to perform the following steps in the Chatter UI:

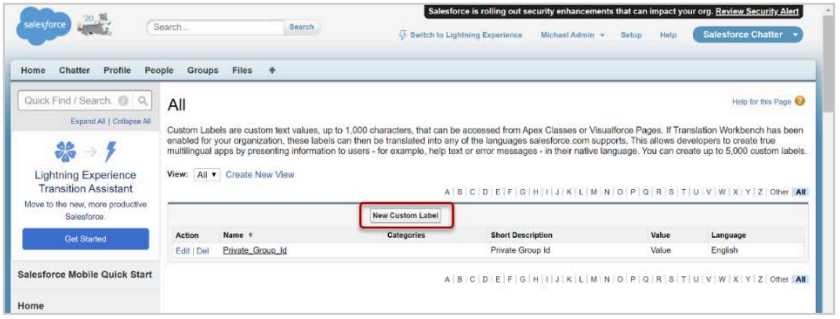
1. Create a new **Private Group** ensuring they do not automatically archive this group and the **Private** option and the **Broadcast Only** checkbox are selected.



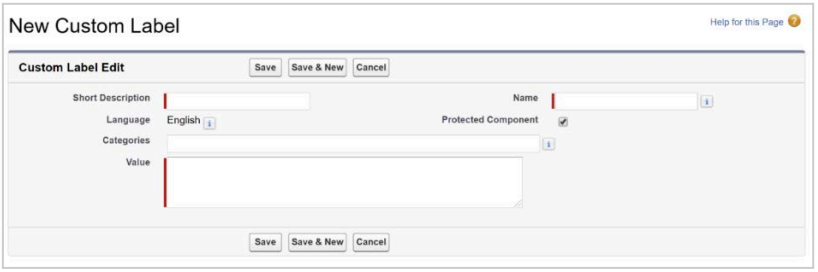
2. Locate and make a note of the **Group ID** in the page URL.



3. Create a new label **Private Group Id**.
   - Go to **Setup > Custom Labels**.
   - Click **New Custom Label**.



   - For Short Description - **Private Group Id**
   - For Name - **Private_Group_Id**
   - Value - Insert **Group Id** of Private group.

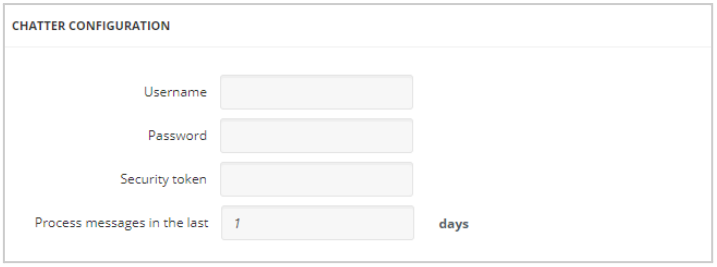


4. For further instructions on how to create apex triggers, refer to **Chatter Triggers** guide in the installation folder.

Collector 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

For more details on how to configure advanced configuration options, see **Advanced Configuration Options**.

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.

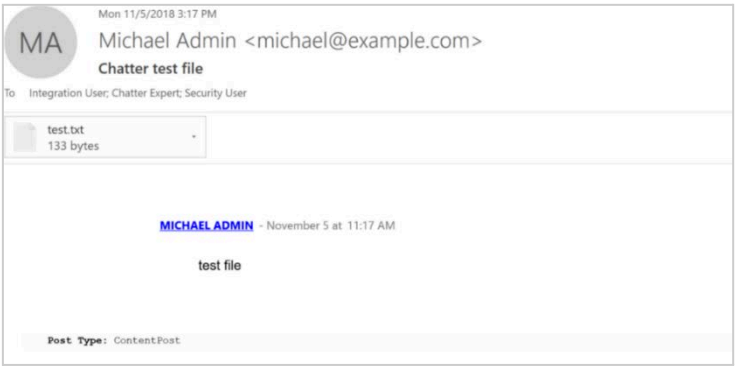
For more details on how to configure attachments, see **Attachments Configuration**.

Next Steps

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

- **MONITORED USERS**
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**

- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

Chatter Cipher Cloud

Chatter is an enterprise collaboration platform from Salesforce, designed to enhance communication and information sharing within organizations. It enables teams to connect, collaborate, and exchange updates in a secure cloud-based environment.

The **Mergel Chatter collector** integrates Chatter communications into data management systems, ensuring comprehensive data capture and compliance. To import Chatter data, Mergel requires authentication via an Admin user's personal token and the publication of triggers on the Chatter site. These triggers generate posts in designated channels, allowing Mergel to capture updates, deletions, and edits. For more information on triggers, see **Installation Instructions** document listed in the **References**.

Mergel supports **Shield Platform Encryption** without additional configuration, ensuring encrypted data remains protected while being decrypted via the Salesforce API. For organizations with a host domain, Chatter Cipher Cloud can be utilized for secure data management.

Activities Captured

- Posts
- Files
- Comments
- Shares (including group posts)
- Comments of shared posts
- Deletes (requires triggers)
- Edits (requires triggers)
- Links
- Polls
- Private chats
- Group chats
- Feed poll choices (If *Modify all data* permission is enabled)
- New events/task contacts/opportunities/cases/leads
- All online communications, including attachments and deleted information (if the triggers are set)

Activities not Captured

- Log a call
- Topics

Creating a Salesforce Application

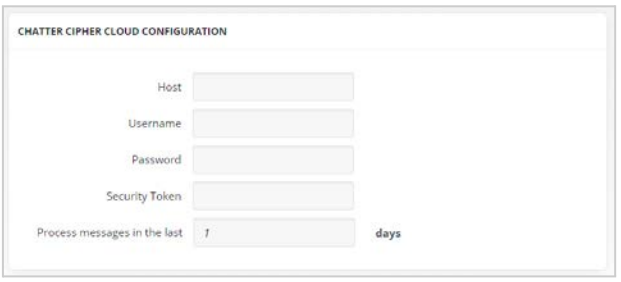
For more details on how to create Salesforce application and acquire a token see **Creating a Salesforce Application**.

Collector 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

For more details on how to configure advanced configuration options, see **Advanced Configuration Options**.

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.

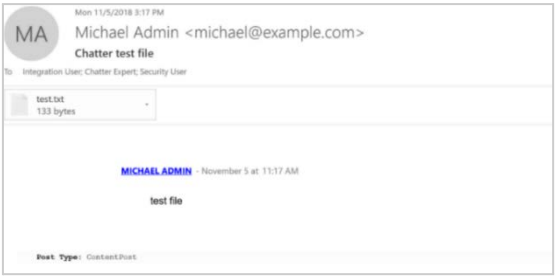
For more details on how to configure attachments, see **Attachments Configuration**.

Next Steps

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

- **MONITORED USERS**
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

Cisco Webex Teams

Cisco Webex Teams is a secure collaboration platform that enables people to meet, message, call, share files, and whiteboard in one place. Designed to support compliance and regulatory requirements, it helps organizations communicate and work together while maintaining security and control.

The **Mergel Cisco Webex Teams collector** captures messages, files, and metadata from Webex Teams, integrating this data into existing archiving and compliance systems. Using Webex Teams APIs, it ensures organizations can retain collaboration content and meet legal and business mandates.

Activities Captured

- Direct messages during a call
- Persistent chats and channels
- Group members in a group or persistent chat
- Attachments
- Emojis
- Edited messages
- Deleted messages
- Conversations related to all newly added users
- Message threading/post threading/group chats threading

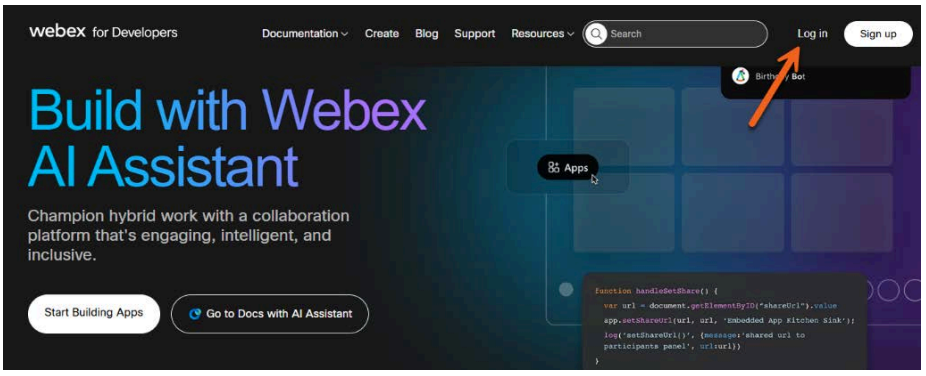
Note

- 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.
- Deleted attachments are not captured due to API temporary limitations.

Cisco Webex Teams App Creation

To create an app, follow the steps below:

1. Go to Webex for Developers and log into your account.

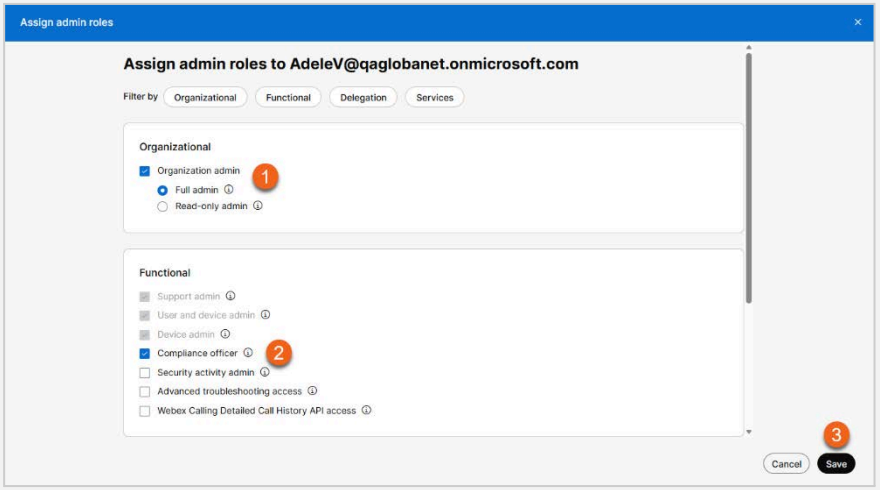


Note

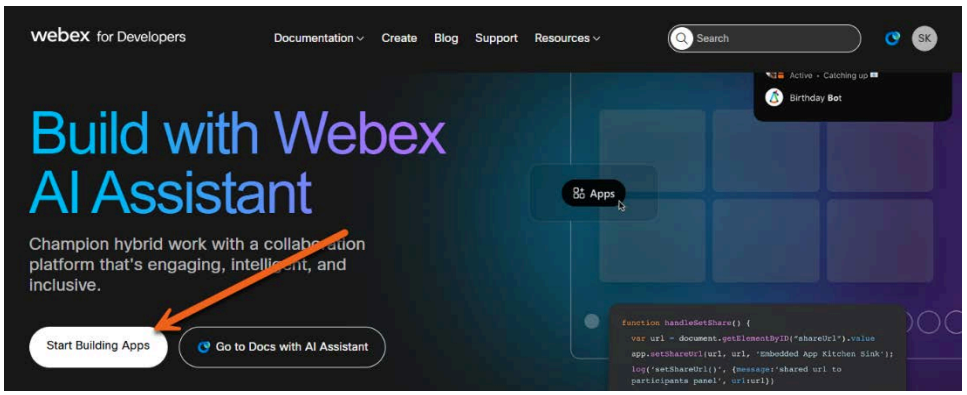
The account used for compliance-related tasks must have **Full admin** privileges and be assigned the **Compliance officer** role.

To verify or assign these permissions:

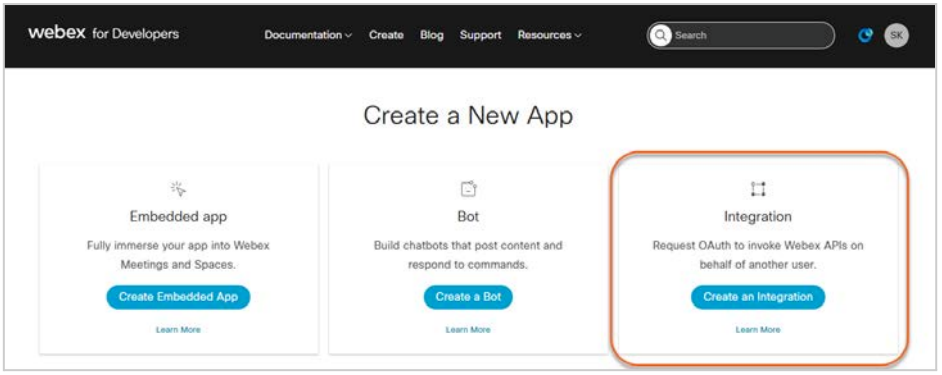
1. Navigate to [Webex Control Hub](#).
2. Go to **Users** and select the relevant user account.
3. In the **Assign admin roles** panel:
   3.1. Under **Organizational**, ensure **Organization admin** is checked and **Full admin** is selected.
   3.2. Under **Functional**, check **Compliance officer**.
4. Click **Save** to apply changes.



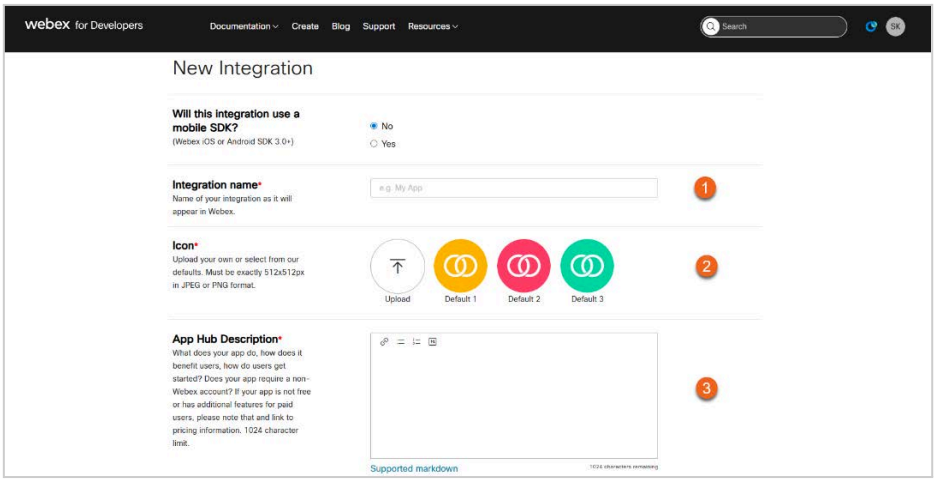
2. When you are logged in and permissions are set, click **Start Building Apps**.



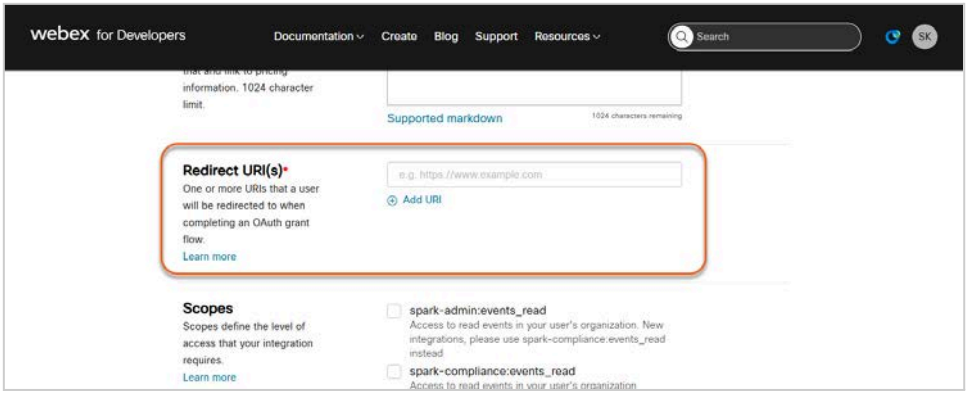
3. Choose **Create an Integration**.



4. Enter **Integration Name**, select or upload an **Icon**, and provide **App Hub Description**.



5. Add the **Redirect URI(s)** of your local Merge1 environment in the following format: `https://<merge1_instance>/Configuration/OAuthCallback`.



6. Select the following scopes:
   6.1. spark-compliance:events_read
   6.2. spark-compliance:messages_read
   6.3. spark-compliance:memberships_read
   6.4. spark-compliance:rooms_read
   6.5. spark-compliance:teams_read

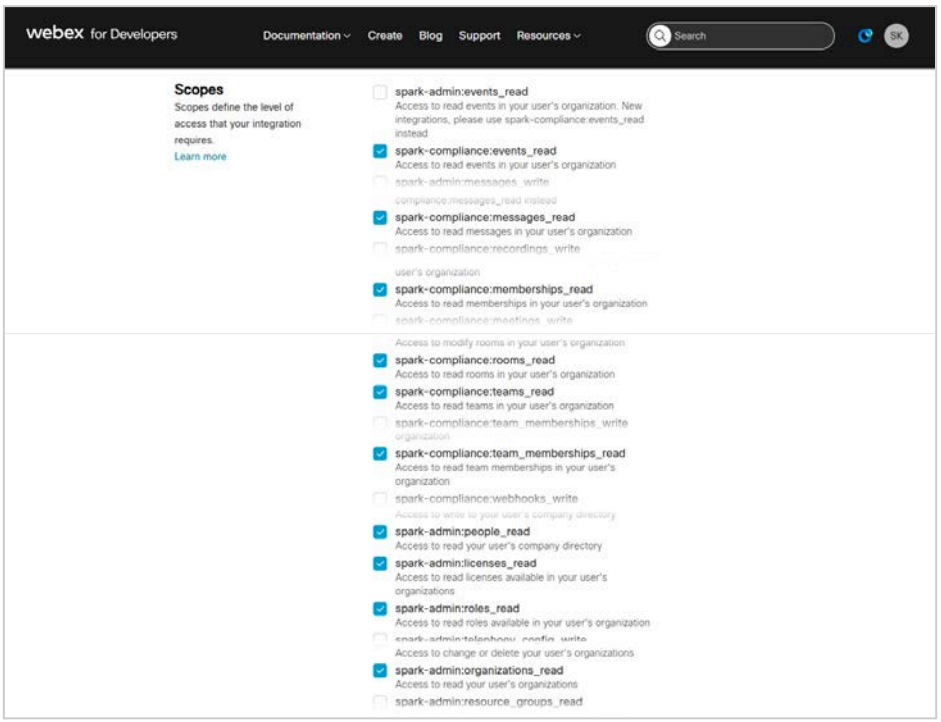
6.6. spark-compliance:team_memberships_read

6.7. spark-admin:people_read

6.8. spark-admin:licenses_read

6.9. spark-admin:roles_read

6.10. spark-admin:organizations_read



7. Click **Add Integration** at the bottom of the page.

8. A **Client ID** and **Client Secret** will be generated. Keep both for configuring the collector in Merge1.

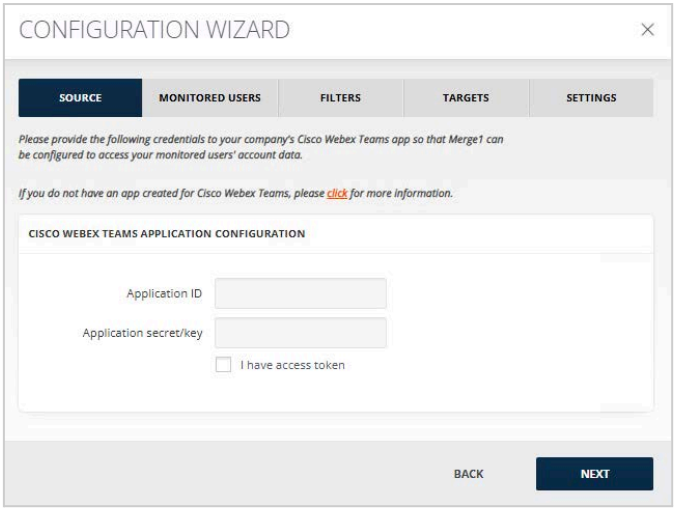
Collector Configuration

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**.



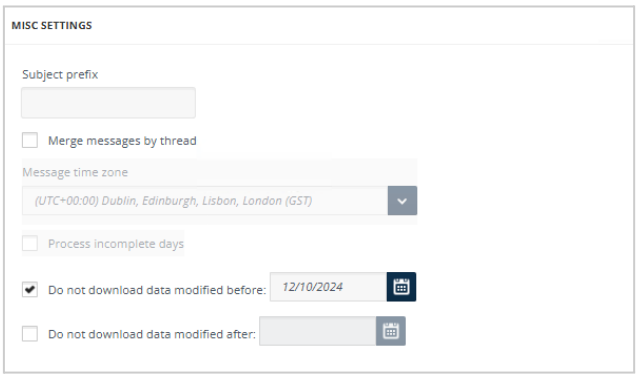
Time Stamp Formatting

For more details on how to configure timestamps, see **Time Stamp Formatting**.

Misc Settings

- **Subject prefix:** Specify a prefix to add in the subject line of imported emails. This is useful for organizing imported data, i.e., when multiple sources share a common target.
- **Merge messages by thread:** If checked, combines messages by thread rather than sending them one by one.
- **Message time zone:** The messages will be split by day with the specified time zone from the drop-down list.
- **Process incomplete days:** If checked, the messages of the days that have not ended yet will be imported in a separate email.

> **Note**
>
> *Message time zone* can be specified and/or the *Process incomplete days* checkbox can be enabled ONLY IF *Merge messages by thread* is checked.



- **Do not download data modified before**, **Do not download data modified after**: Specify dates to allow cutting off data outside the set date range.

  Example: If the before date is set to 08/17/2025 and the after date is set to 09/17/2025, only the data between these two dates will be downloaded: data outside that timeframe will be ignored.

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

Splitting Messages

Check the **Split 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

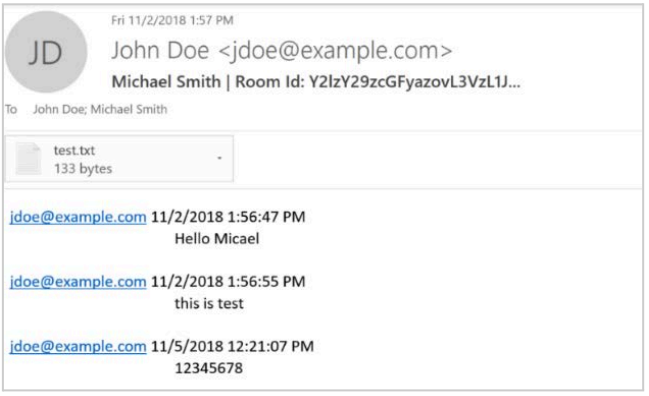
For more details on how to configure attachments, see **Attachments Configuration**.

Next Steps

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

- **MONITORED USERS**
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

Citrix Workspace & ShareFile

Citrix Workspace & ShareFile provides secure file sharing, storage, sync and more - all built for business. The collector requires a service account to create the API.

Activities Captured

- **Files** – uploaded, deleted[9], archived, renamed, downloaded, viewed[10], shared[11], moved, checked in/out
- **Folders** – created, moved[12], shared, deleted
- Login info
- Share file requests
- Text-only messages
- Share file request message
- Revoked messages

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 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, Merge1 attaches the same file (generally, the latest among the ones with the same name) to all the generated messages.
- If files with 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 Citrix environment, the captured message will have an empty body.
- Duplicate messages are captured for shared and then deleted files in case *Archive all activities in ShareFile* or from the *Archive only certain selection of activities in ShareFile*, *File share* and *Text-only messages* are enabled.

Citrix Workspace & ShareFile App Creation

To create an app:

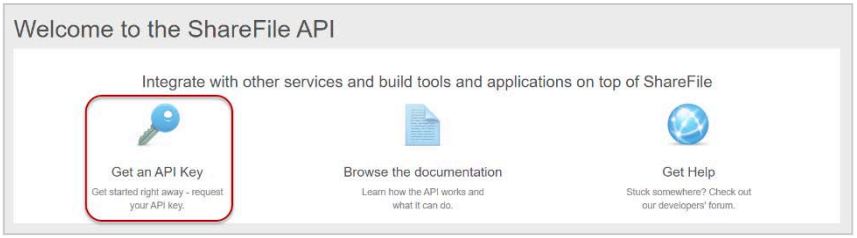
1. Navigate to https://api.sharefile.com/rest/.
2. Log into your Citrix ShareFile account. Note that the account should be a Service Account.
3. Click **Get an API Key**.

[9] Only the activity is captured.

[10] Audio_Listen and Video_View for MP3/MP4 file types accordingly.

[11] Including encrypted messages.

[12] Currently, only the activity is captured.



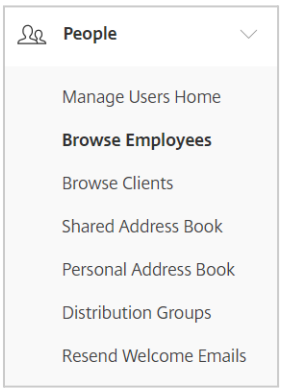
4. Fill in the **Application Name** field.
5. In the **Redirect URI** field add the URL of your local Merge1 environment with the following format: `https://<merge1_instance>/Configuration/OAuthCallback`.
6. Click **Generate API Key**.

7. Copy the generated **Client Id** and **Client Secret**.

Granting Permissions

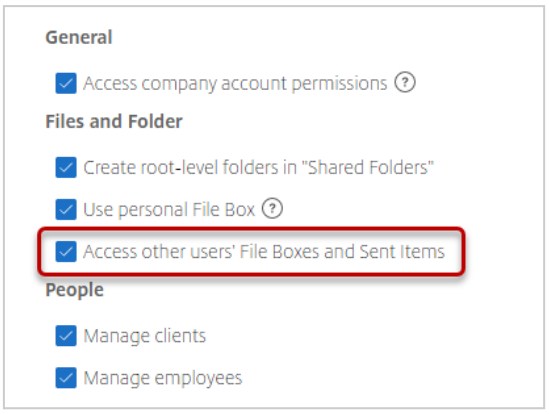
To be able to capture data, Org Owner must give the **Access other users' File Boxes and Sent Items** specific permission. To give the permission:

1. Navigate to your ShareFile instance.
2. Log into your Citrix 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.

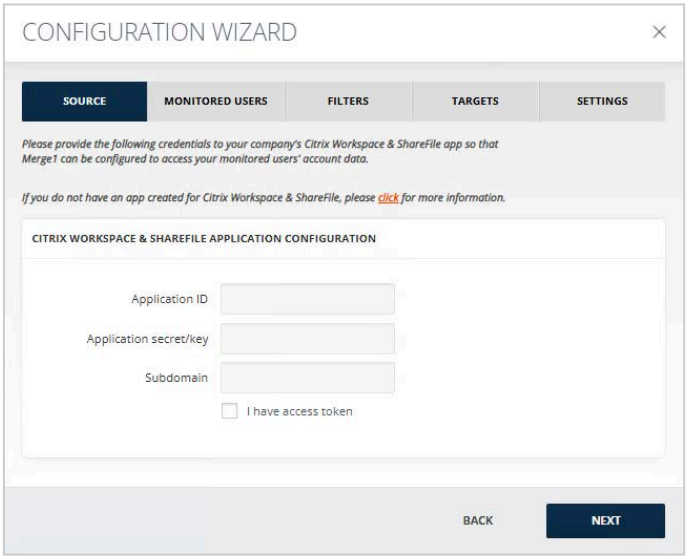


7. Scroll down and click **Save Changes**.

Collector 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).

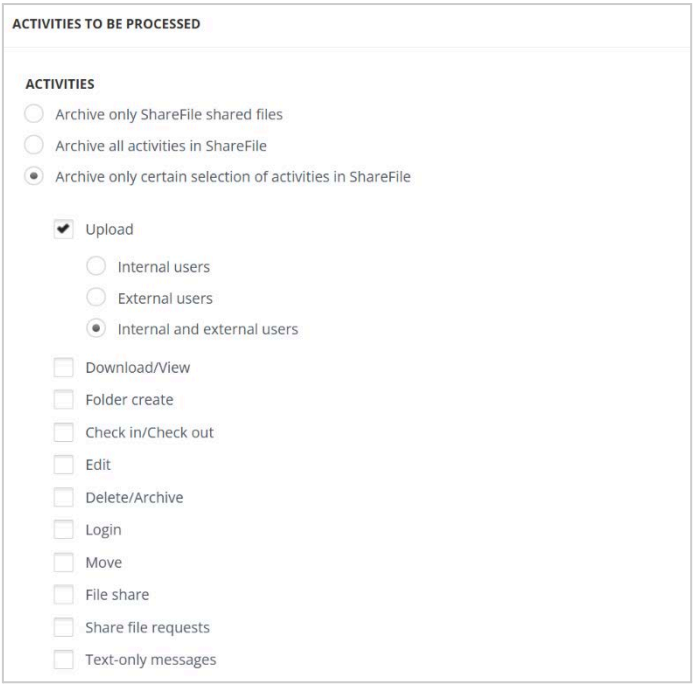


4. In the opened window, enter your accounts subdomain, and then sign into ShareFile account. Make sure that pop-ups are not blocked by the browser. This can be checked from the top right corner of the address field.

Activities to Be Processed

It is possible to choose which activities Merge1 processes from Citrix Workspace & 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**
        - *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.
    - **Download/View**
    - **Folder create**
    - **Check in/Check out**
    - **Edit**
    - **Delete/Archive**
    - **Login**
    - **Move**
    - **File share**
    - **Share file requests**
    - **Text-only messages**



Time Stamp Formatting

For more details on how to configure timestamps, see **Time Stamp Formatting**.

Advanced Configuration Options

For more details on how to configure advanced configuration options, see **Advanced Configuration Options**.

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.

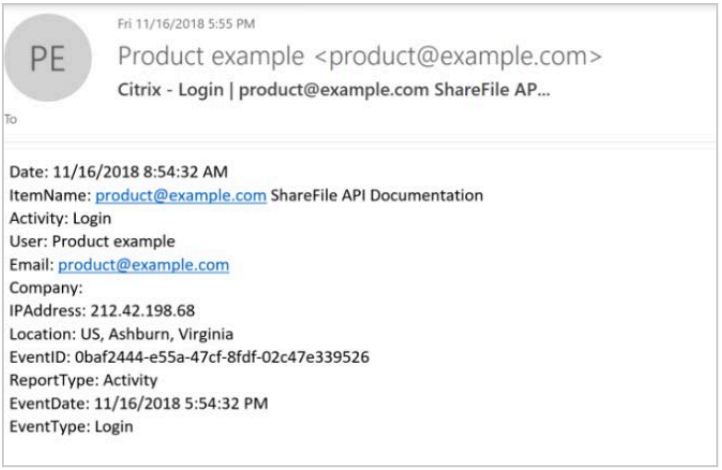
For more details on how to configure attachments, see **Attachments Configuration**.

Next Steps

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

- **MONITORED USERS**
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

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 **Mergel 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.

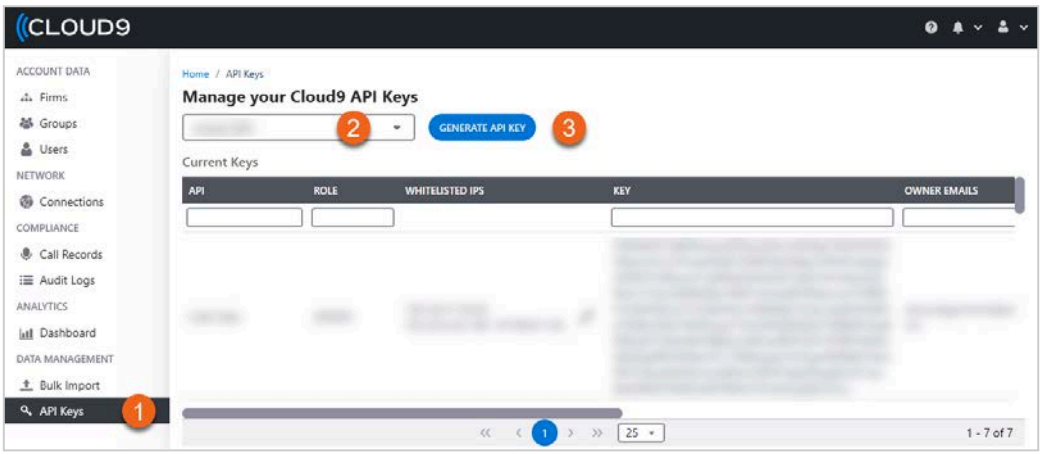
Activities Captured

- Calls

Generating an App Key and Secret

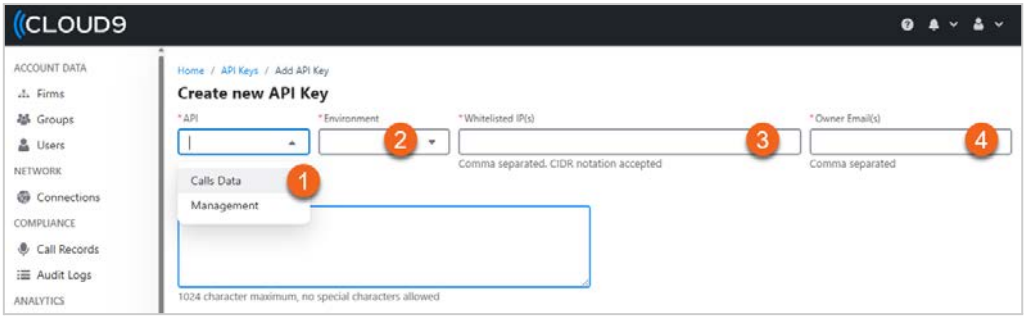
The Firm Admin of your organization must complete the following steps to generate an App Key and Secret in Cloud9.

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**.

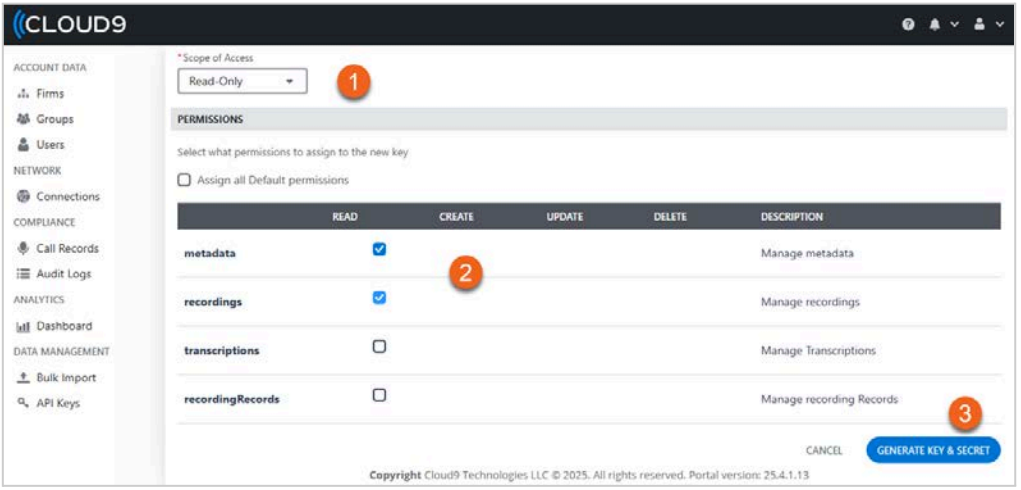


Generating a Call Data App Key and App Secret

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.
4. Enter the relevant email(s) under **Owner Email(s)**.



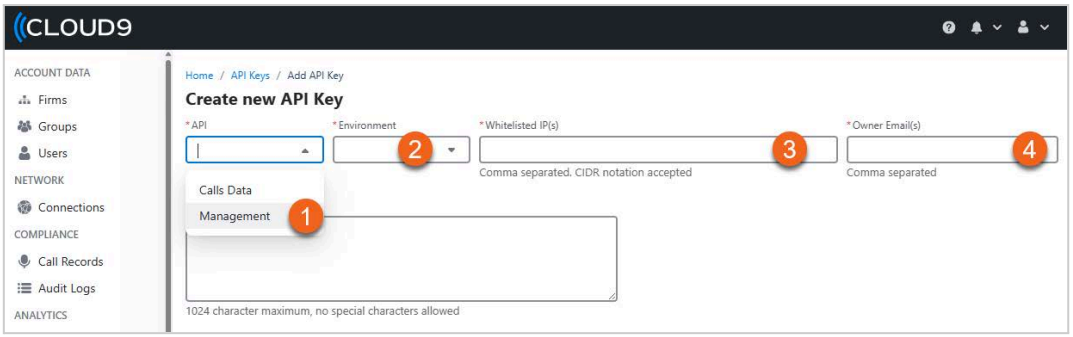
5. Under **Scope of Access**, select **Read-Only**, then choose the following permissions:
    - **metadata**
    - **recordings**
6. Click **Generate Key & Secret**.



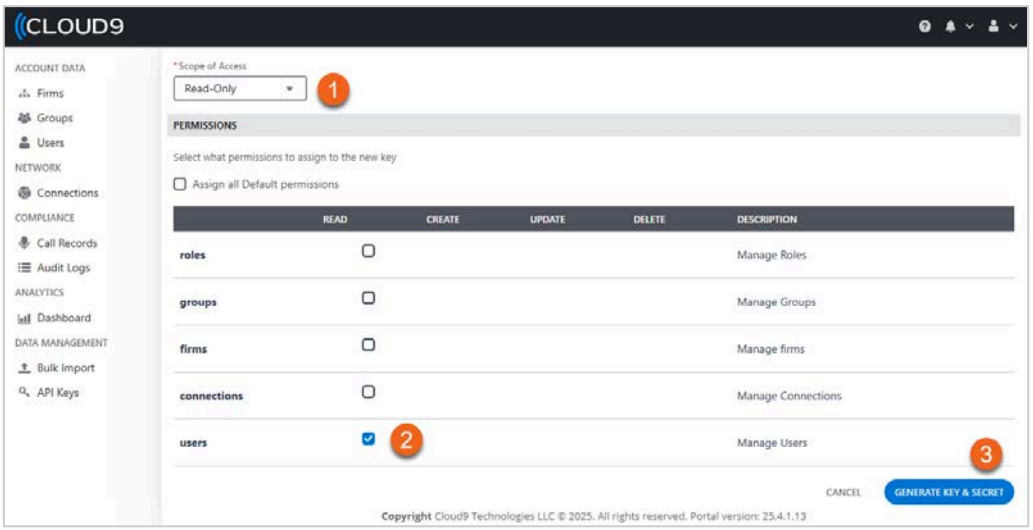
7. Copy and securely store the generated **Call Data API Key** and **Call Data Secret Key** for source configuration.

Generating 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.
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**.



7. Copy and securely store the generated **Management API Key** and **Management Secret Key** for source configuration.

Configuring the Collector in Merge1

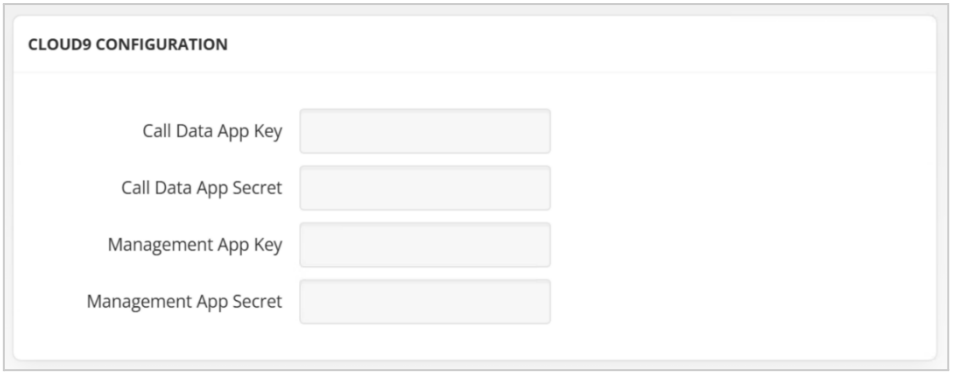
Adding the Importer

For details on adding the importer, see **Adding a New Importer**.

Cloud9 Configuration

For configuring the **Cloud9** application:

1. Enter the securely stored **Call Data API Key** and **Call Data Secret Key** to the **Call Data App Key** and **Call Data App Secret** fields, respectively.
2. Enter the securely stored **Management API Key** and **Management Secret Key** to the **Management App Key** and **Management App Secret** fields, respectively.

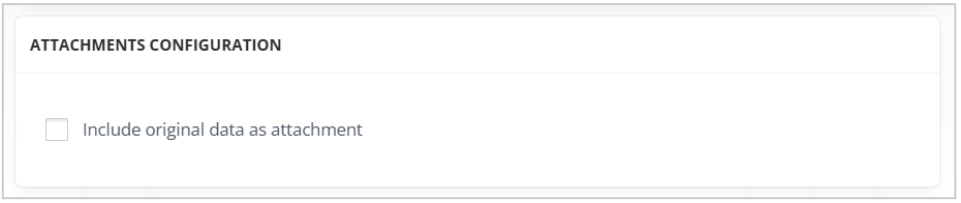


Advanced Configuration Options

For more details on how to configure advanced configuration options, see **Advanced Configuration Options**.

Attachments Configuration

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

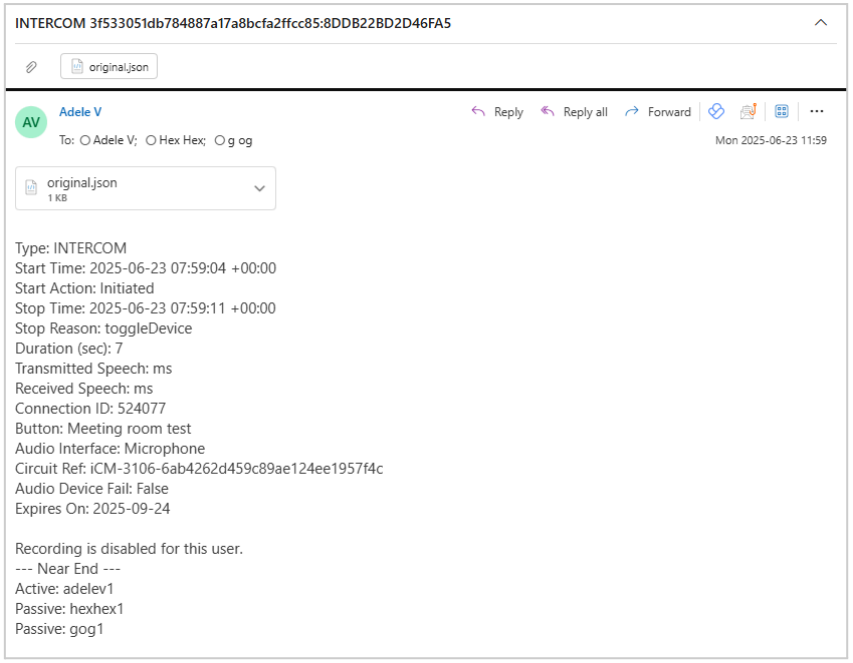


Next Steps

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

- **MONITORED USERS**
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

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 **Mergel 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

Due to current API limitations, the following constraints apply:

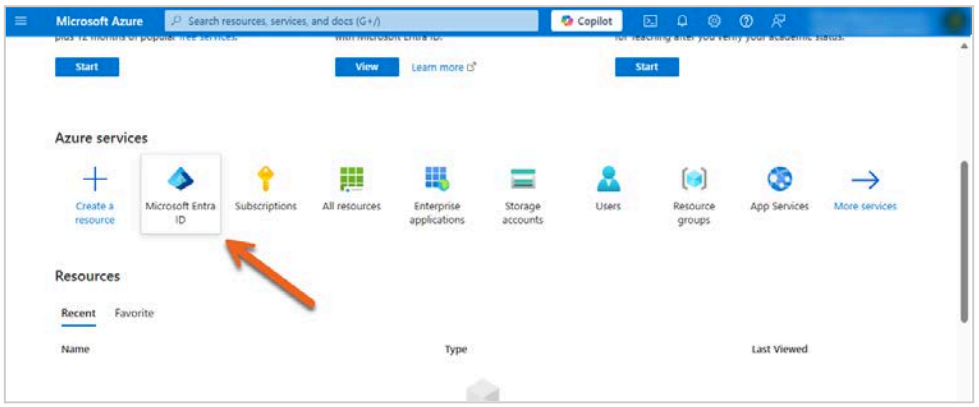
1. Captured data may contain auto-generated and progress reporting messages.
2. When Copilot is used directly within a Microsoft Word or Microsoft PowerPoint document, one AI response may include the attachment. All other AI responses and UI prompts will provide a URL to the attachment instead of including 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 (a Mergel limitation). For longer periods, multiple sessions are required.

Creating a Microsoft Entra ID Application

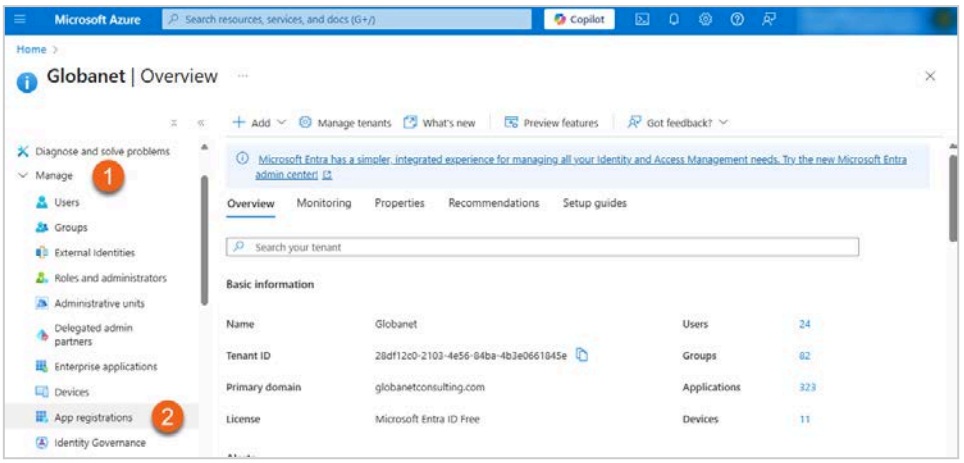
The Office 365 or Azure administrator in your organization must complete the steps detailed in the sections below.

Registering an Application

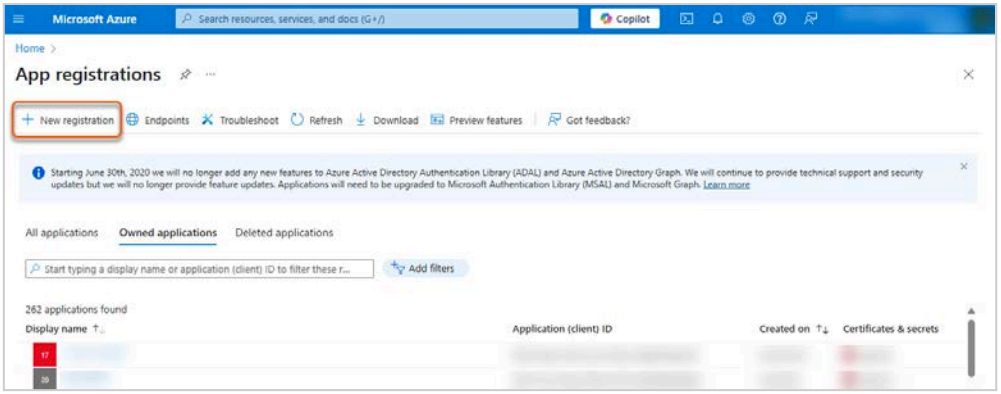
1. Sign in to Azure Portal.
2. Select **Microsoft Entra ID** under **Azure services**.



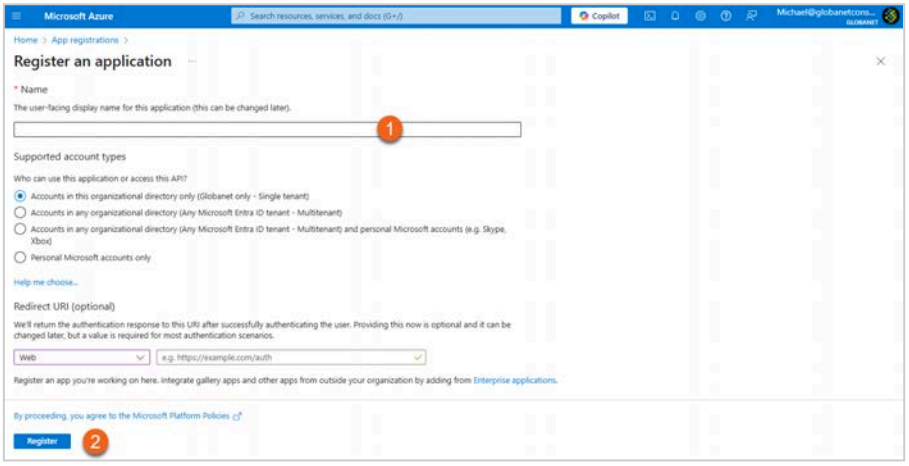
3. In the left-hand navigation pane, click **Manage > App registrations**.



4. Click **New registration**.



5. To register an application:
    5.1. Enter a **Name** for the application.
    5.2. Click **Register**.



An **Application (client) ID** and **Directory (tenant) ID** will be generated. Keep both for configuring the collector in Merge1.

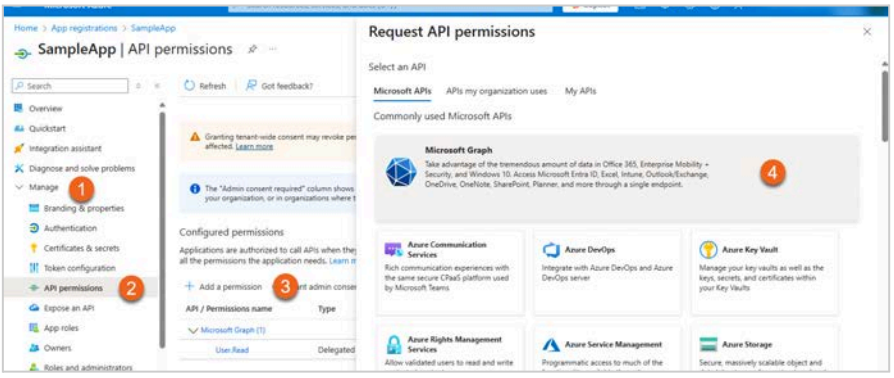
Granting Permissions

Adding Microsoft Graph API Permissions

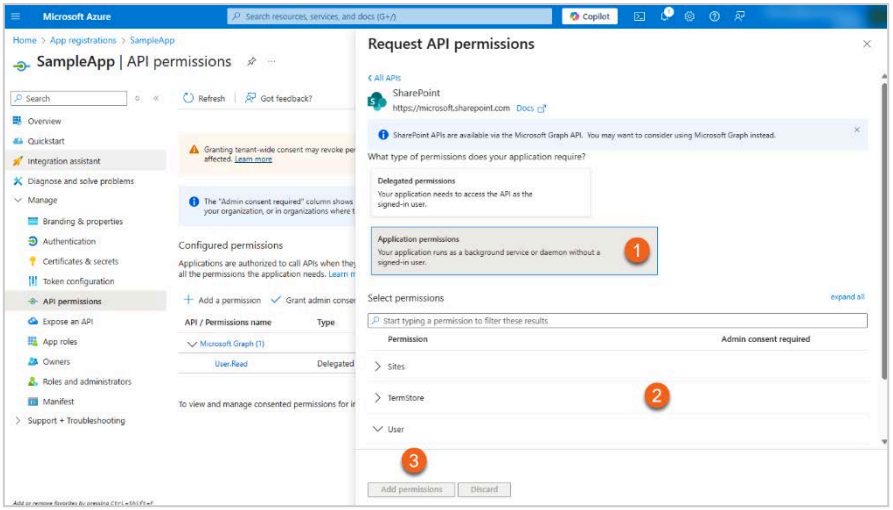
To add **Microsoft Graph** API permissions:

In the left-hand navigation pane, click **Manage > API permissions**.

1. Click **Add a permission**.
2. In the opened pane select the **Microsoft Graph** API.



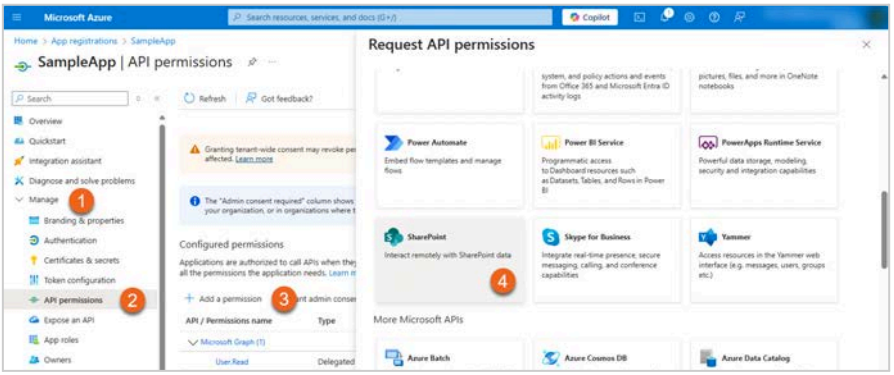
3. To add the necessary permission:
    3.1. Click **Application permissions**.
    3.2. Add the following permissions:
        3.2.1. **AiEnterpriseInteraction:** *AiEnterpriseInteraction.Read.All*
        3.2.2. **User:** *User.Read.All*
    3.3. Click **Add permissions**.



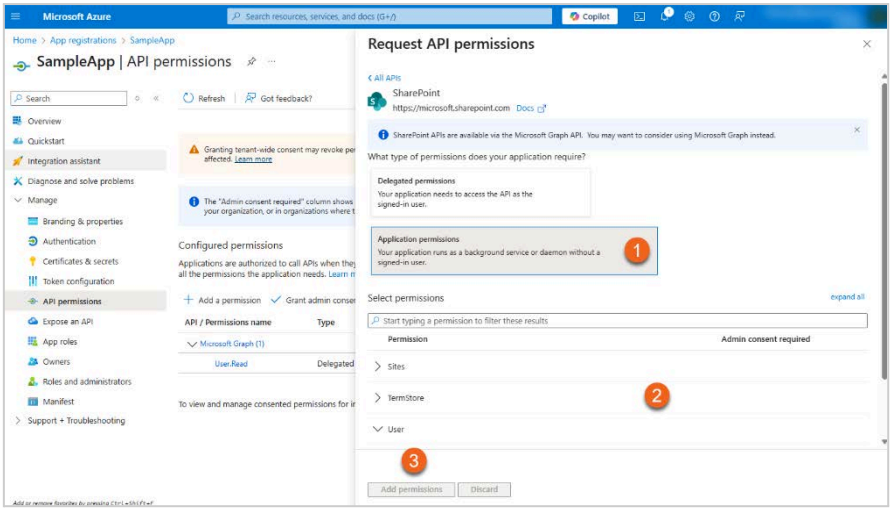
Adding SharePoint API Permissions

To add **SharePoint** API permissions:

1. In the left-hand navigation pane, click **Manage > API permissions**.
2. Click **Add a permission**.
3. In the opened pane select the **SharePoint** API.

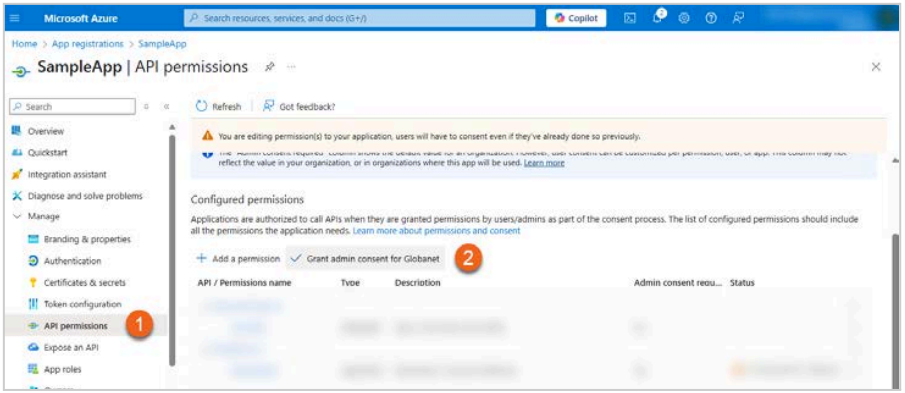


4. To add the necessary permission:
    4.1. Click **Application permissions**.
    4.2. Add the following permissions:
        4.2.1. **Sites:** *Sites.Read.All*
        4.2.2. **TermStore:** *TermStore.Read.All*
        4.2.3. **User:** *User.Read.All*
    4.3. Click **Add permissions**.



Granting Admin Consent

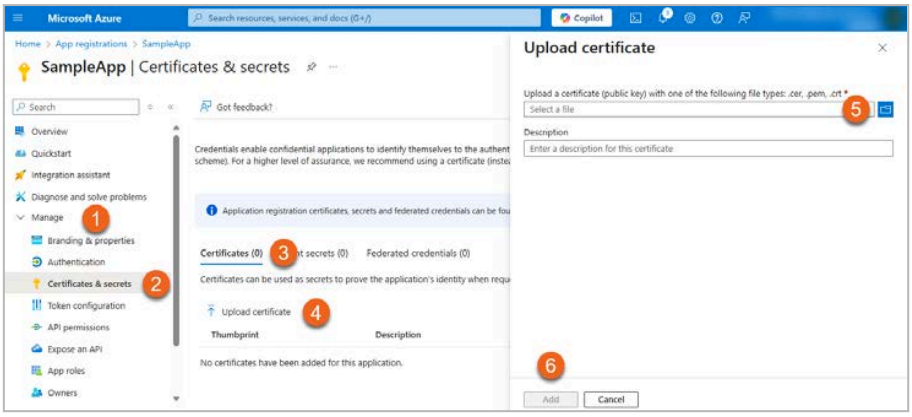
1. Go back to **API permissions**.
2. Click **Grant admin consent** for your company to grant the added permissions.



Uploading a Certificate

To upload a certificate:

1. In the left-hand navigation pane, go to **Manage > Certificates & secrets**.
2. Select **Certificates**.
3. Click **Upload certificate**.
4. Select a certificate (public key) with one of the following file types: `.cer`, `.pem`, `.crt`.
5. Click **Add**.



A certificate **thumbprint** will be generated. Keep the value for configuring the collector in Merge1.

For more information on how to create a certificate, see **Creating a Certificate (Private and Public Keys)**.

Configuring the Collector in Merge1

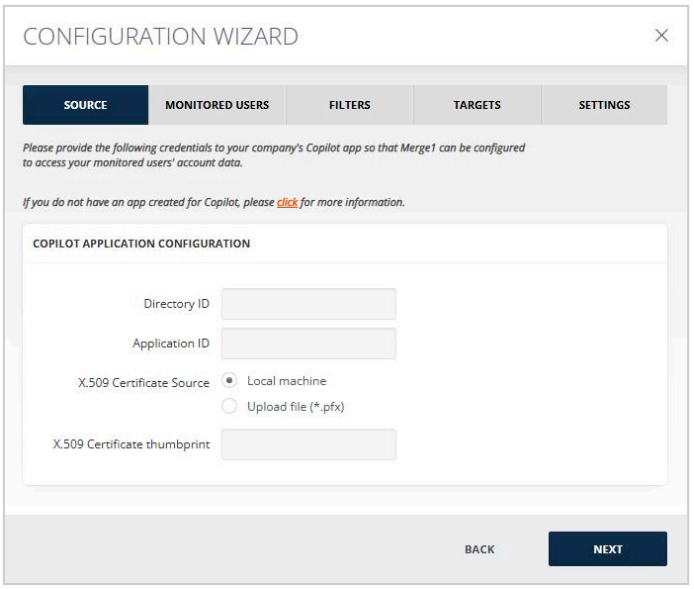
Adding the Importer

For details on adding the importer, see **Adding a New Importer**.

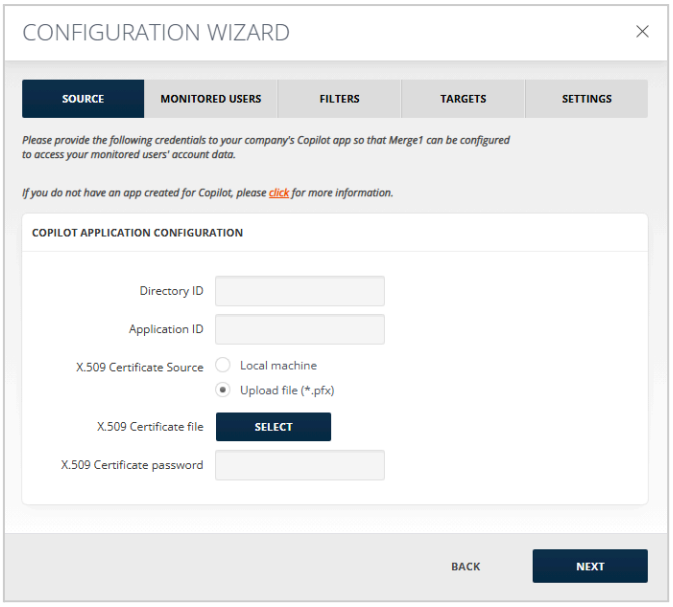
Source Configuration

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. Provide **X.509 Certificate Thumbprint** in case you activate the **Local machine** radio button as the X.509 Certificate source.



3. In case you activate **Upload file (*.pfx)**, click the **Select** button to upload the certificate and provide **X.509 Certificate password**.



The **Certificate thumbprint** field will be auto populated in case the collector was previously configured by uploading a certificate.

4. Click **Next**.

Time Stamp Formatting

For more details on how to configure timestamps, see **Time Stamp Formatting**.

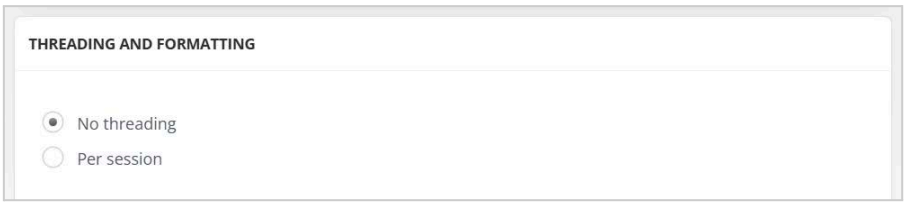
Advanced Configuration Options

For more details on how to configure advanced configuration options, see **Advanced Configuration Options**.

Threading and Formatting

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 session**: If selected, a threaded message will be generated for each Copilot conversation.



Message Body

Choose how imported messages should be displayed in the target. The available output message body formats are:

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

Note

The **Pure body** mode is active ONLY if the **No threading** mode is checked.

Attachments Configuration

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

Otherwise, additional configurations will open for setup. See **Attachments Configuration**.

Next Steps

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

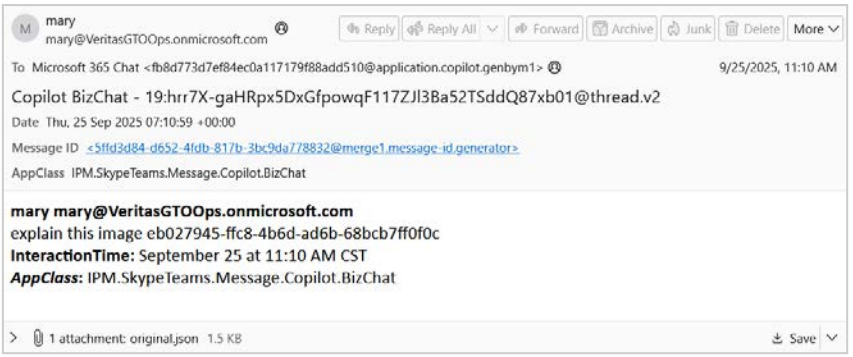
- MONITORED USERS

Note

Only users with an active Copilot license at the time of the request are included when retrieving interaction data. By default, data from users with revoked or expired licenses is excluded.

- FILTERS
- TARGETS
- IMPORTER SETTINGS

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

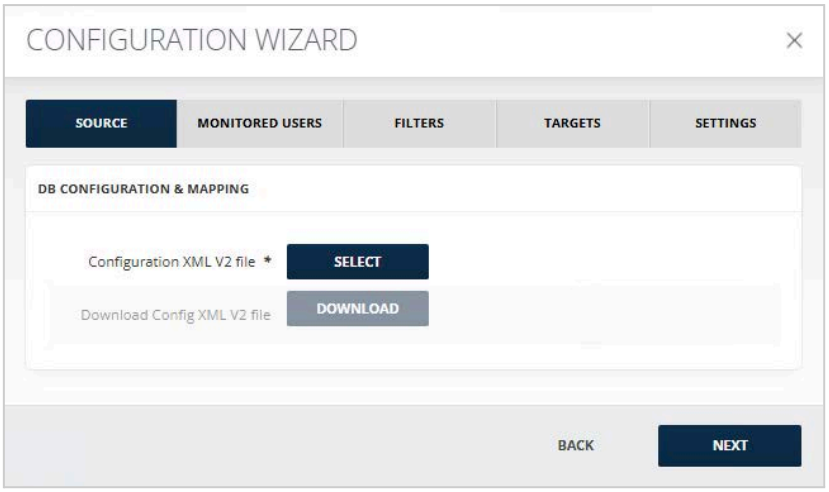
DB

Merge1 DB collector is designed as an open SDK platform to allow our customers to rapidly import a table or part of a table from an MS SQL or Oracle Database. With the DB source, you can collect and process data from any MS SQL database.

The collector's objective is to map the table's columns to the specific email field format required. We are looking to map the "Sender," "To," "Title," "ActivityDateTime," and "Content" fields to appropriate columns in the text-delimited file. Merge1 keeps a history of imported data to ensure that the same data is not re-imported (note that multiple columns could be added to the body of the email).

With the DB source, you can collect and process data from any database. To do so, use XML mapping (see **XML Mapping Sample**).

Upload the XML file containing your formatting preferences and click **Next**. Then, click the **Download** button in the collector configuration wizard to download a DB configuration and mapping XML file.



XML Mapping Sample

```
<?xml version="1.0" encoding="utf-16"?>
<DBCollector Mapping xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsdd="http://www.w3.org/2001/XMLSchema">
    <Version>2.0</Version>
    <ConnectionString> {Database Connection String}; Initial
Catalog=DB_Connect;Integrated Security=True; </ConnectionString>
    <DbProvider>MsSql</DbProvider>
    <TableName> {Source Table Name} </TableName>
    <Columns>
        <ColumnMetaInfo>
            <Name> {Column Name} </Name>
            <DataType> {Column Type} </DataType>
            <Nullable>{true/false} </Nullable>
        </ColumnMetaInfo>
        <ColumnMetaInfo>
            ……
        </ColumnMetaInfo>
        ……
```

```
    </Columns>
    <ColumnMaps>
        <ColumnMapping>
            <CanBeEmpty>{true/false} </CanBeEmpty>
            <MessagePropertyName> {Message Field Name}
</MessagePropertyName>
            <ColumnNames>
                <string> {Column Name from above} </string>
                <string>…</string>
            </ColumnNames>
        </ColumnMapping>
        <ColumnMapping>
            ……
        </ColumnMapping>
        ……
    </ColumnMaps>
</DBCollector Mapping>
```

To connect to the relevant database, use a sample code idea presented below:

```
<add name="NAME" connectionString="data source=.\SQLSERVER;Integrated
Security=SSPI;Initial Catalog=SOURCE_DB/>
```

For MS SQL Database:

```
    <ConnectionString>Data Source=.; Initial Catalog=MyDb;Integrated
Security=True;
    </ConnectionString>
```

For Oracle Database:

```
    <ConnectionString>Data
Source=(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=192.168.10.253)(PORT=1540))(
CONNECT_DATA=(SERVICE_NAME=TestDb))); User ID = <username>; Password =
<password>;
    </ConnectionString>
```

There can be as many `<ColumnMetaInfo>` tags as there are columns in the source table.

Note that there should not be any duplicates. Names are not case-sensitive.

There can be as many `<ColumnMapping>` tags as it is necessary. These columns can be reused in any way. `<ColumnName>` may contain multiple string tags only if the `<MessagePropertyName>` allows for multiple entries (see below). If multiple entries are present, the contents are sequenced in order with spaces.

Valid `<MessagePropertyName>` values are not case-sensitive and are as follows:

- Sender: One value, must be a valid SMTP email address.
- To: One or more values, each must be a valid SMTP email address.
- CC: One or more values, each must be a valid SMTP email address.

- BCC: One or more values, each must be a valid SMTP email address.
- Title: One or more values.
- ActivityDateTime: One value, must be a valid DateTime value.
- Content: One or more values.

Custom fields may be used with multiple values and are added to each message as custom properties. `<DataType>` and `<Nullable>` tags are semantic and are not mandatory.

Merge1 DB supports the following data type values that can be collected from the database: varchar, nvarchar, ntext, int, tinyint, longint, and datetime.

Sender, To, CC, and BCC fields are set to SMTP addresses only, thus imported messages will show up with empty fields.

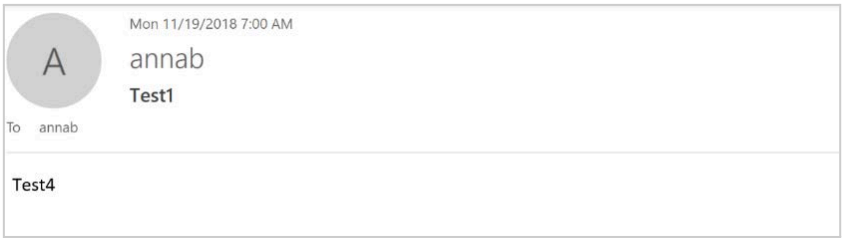
Select the **Set Display Name** to SMTP address when empty option in **Importer Settings** under **Processing** to avoid this.

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**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

Dropbox Business

Dropbox Business is a cloud-based file storage and collaboration platform, providing secure storage for tools, content, and teams while enhancing productivity across industries. Designed for flexibility and data security, Dropbox Business enables organizations to store, share, and sync files seamlessly, ensuring compliance with enterprise requirements.

The **Merge1 Dropbox Business collector** processes Dropbox-generated content, capturing files, metadata, and user activity for seamless integration into data management and compliance systems. By leveraging the Dropbox Business API, organizations can efficiently archive, retain, and analyze critical business files while ensuring security and regulatory compliance.

Activities Captured

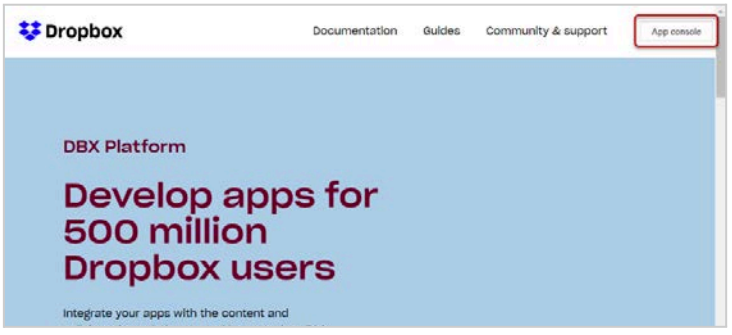
- **Files and file operations** – added, copied, deleted, downloaded, edited, moved, permanently deleted, renamed, restored, reverted, rolled back
- **Comments** – added, deleted, edited
- **Sharing:**
  - Shared content - add invitees, add members
  - Shared content - copy, view, unshare
  - Shared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

There are some cases, such as events generated by external (anonymous) users, which are not captured.

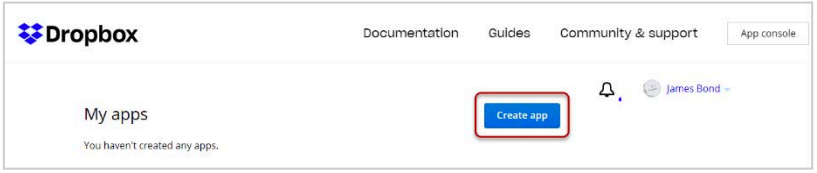
Creating a Dropbox Application

The owner of your organization's Dropbox folder must perform these steps to create a Dropbox application for use in Merge1.

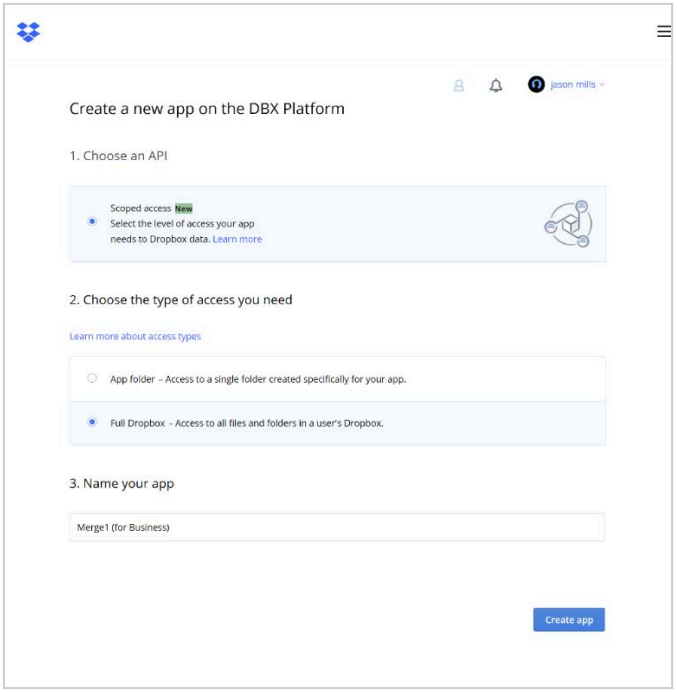
1. Log in to Dropbox and navigate to https://www.dropbox.com/developers.
2. At the top right corner, click **App console**.



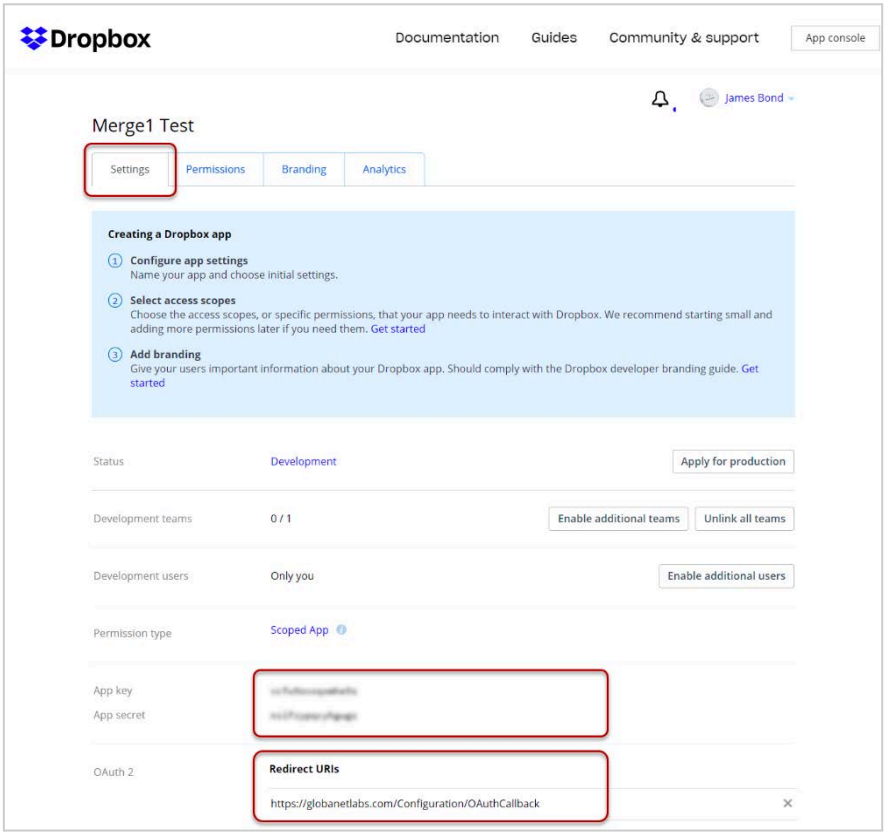
3. Click **Create app**.



4. Enable **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**.



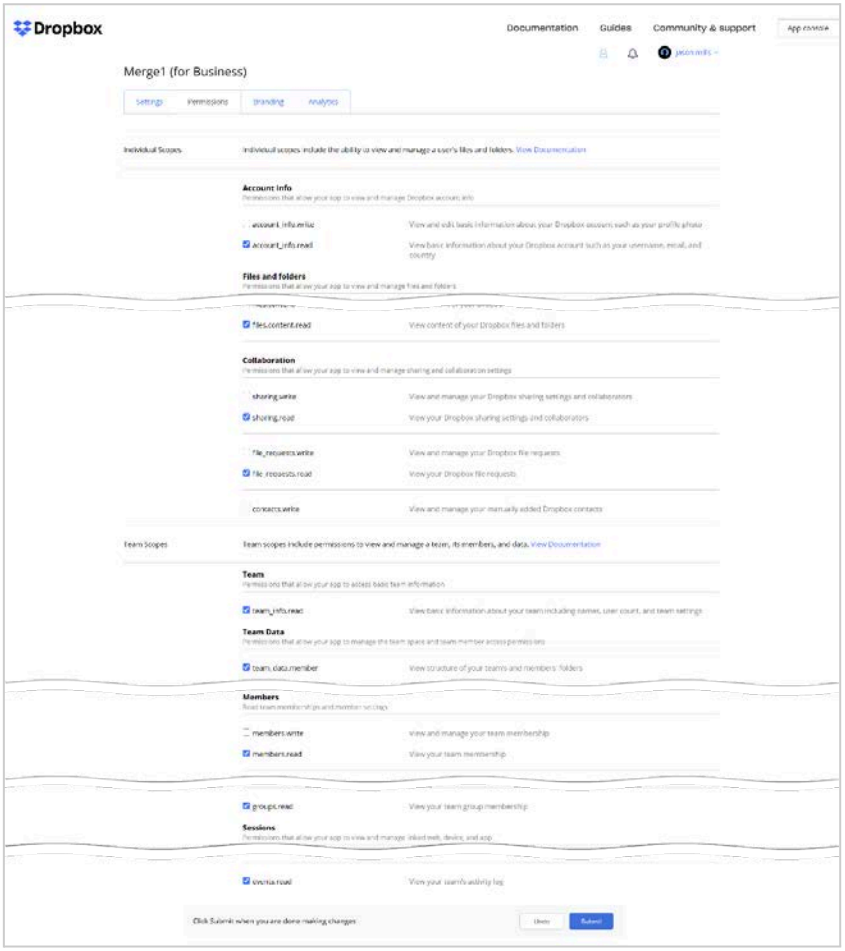
5. Name your app and click **Create app**.
6. On the opened **Settings** tab (1), copy and save the **App key** and **App secret** (2) and then in the **Redirect URIs** field, enter `https://merge1_instance/Configuration/OAuthCallback`.



Note that both the **App key** and **App secret** must be provided to Merge1 as a part of Dropbox Business configuration.

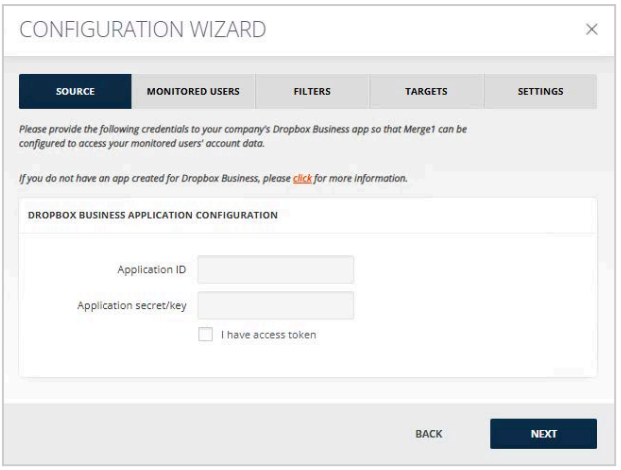
7. On the **Permissions** tab, select the following checkboxes and click **Submit**:

   - account_info.read: View basic information about your Dropbox account such as your username, email, and country.
   - files.metadata.read: View information about your Dropbox files and folders.
   - files.content.read: View content of your Dropbox files and folders.
   - sharing.read: View your Dropbox sharing settings and collaborators.
   - file_requests.read: View your Dropbox file requests.
   - team_info.read: View basic information about your team including names, user count, and team settings.
   - team_data.member: View structure of your team's and members' folders.
   - members.read: View your team membership.
   - groups.read: View your team group membership.
   - events.read: View your team's activity log.

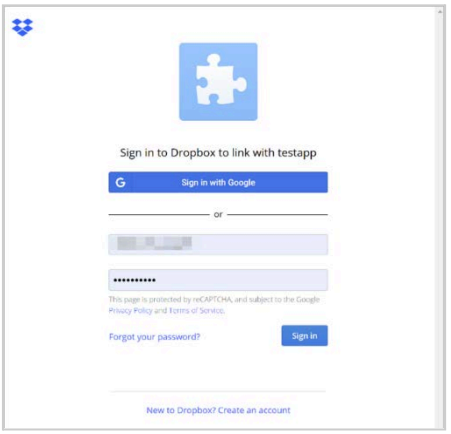


Collector Configuration

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.



Advanced Configuration Options

For more details on how to configure advanced configuration options, see **Advanced Configuration Options**.

Time Stamp Formatting

For more details on how to configure timestamps, see **Time Stamp Formatting**.

Attachments Configuration

For more details on how to configure attachments, see **Attachments Configuration**.

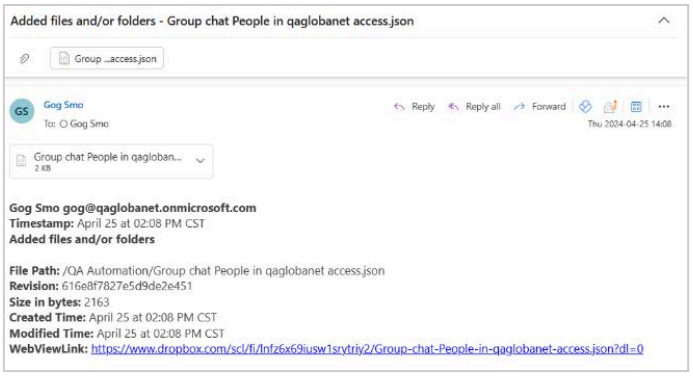
Next Steps

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

- **MONITORED USERS**
- **FILTERS**
- **TARGETS**

- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

Dubber Speik Recordings

Dubber Speik is a unified data capture and streaming engine that records conversation data from various sources, including video, chat, SMS, and voice communications. Built for compliance and intelligence, Dubber Speik ensures secure and scalable data processing across enterprise networks and OTT Unified Communications platforms.

The **Merge1 Dubber Speik Recordings collector** captures and archives audio and video communication data, providing businesses with real-time access, storage, and analytics for compliance, security, and business insights. By integrating with Dubber's recording infrastructure, organizations can effectively retain critical conversation records while ensuring regulatory adherence.

Info

Please reach out to your Dubber Speik representative to obtain your credentials.

Activities Captured

- Microsoft Teams calls
- Mobile phone calls

Note

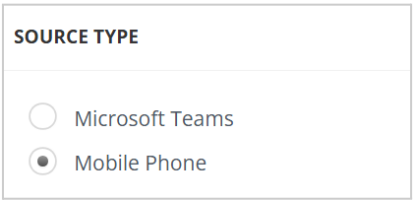
These activities must be recorded by Dubber Speik.

Collector Configuration

Source Type

For **Source Type** configuration:

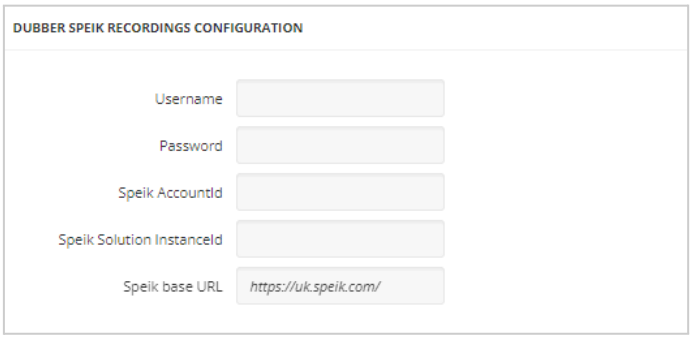
- Enable **Microsoft Teams** to collect recordings from Microsoft Teams.
- Enable **Mobile Phone** to collect recordings from mobile phone calls.



Dubber Speik Recordings Configuration

Enter the following credentials of the Dubber Speik account:

- **Username**
- **Password**
- **Speik AccountId**
- **Speik Solution InstanceId**
- **Speik base URL**.

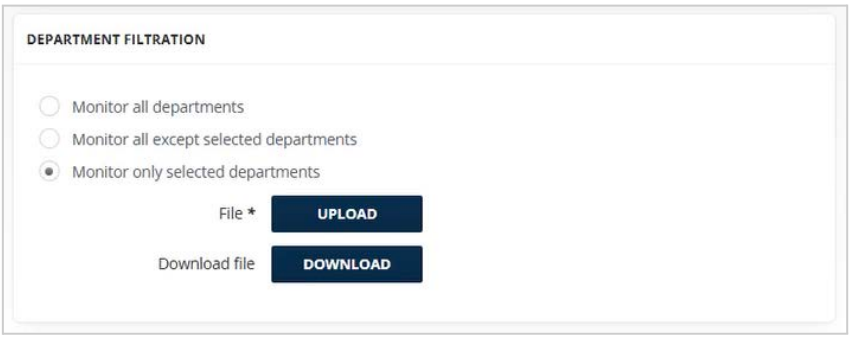


These credentials should be provided to configure the Dubber Speik Recordings collector. Please reach out to your Dubber/Speik representative to obtain your credentials.

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.



Tips on CSV Validation Rules

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

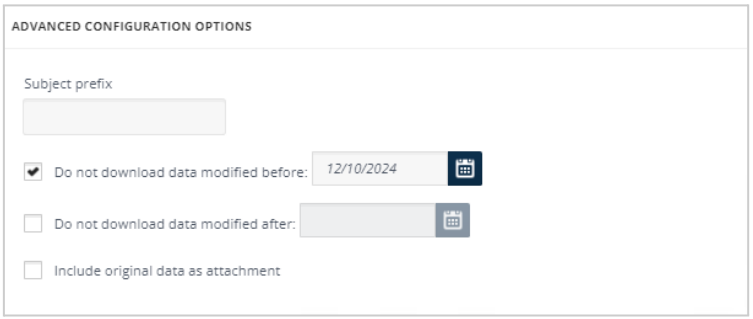
- **File Format:** Must be a CSV file.
- **File Size:** Must be greater than 0 KB. Empty files will be rejected.

- **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.
- 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 08/17/2024 and the *after date* is set to 09/17/2024, only the data between these two dates will be downloaded. Data outside that timeframe will be ignored.
- The **Include original data as attachment** feature allows including/excluding original data as attachment by enabling/disabling the corresponding checkbox.

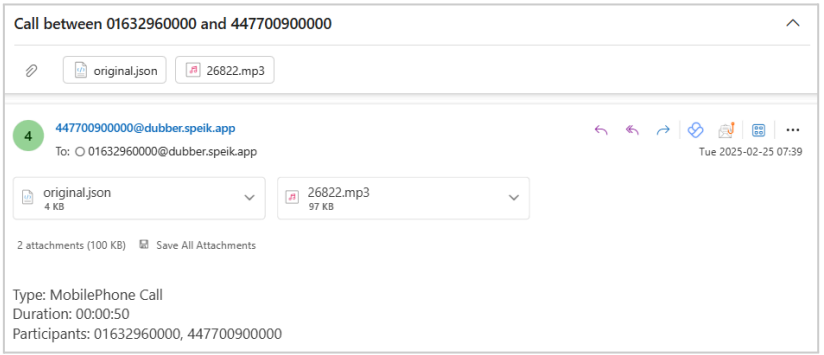


Next Steps

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

- Monitored Users (N/A)
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

Dubber Speik SMS

Dubber Speik is a unified data capture and streaming engine that records conversation data from various sources, including video, chat, SMS, and voice communications. Built for compliance and intelligence, Dubber Speik ensures secure and scalable data processing across enterprise networks and OTT Unified Communications platforms.

The **Mergel Dubber Speik SMS collector** captures and archives SMS data, providing organizations with real-time access, storage, and analytics for compliance, security, and regulatory adherence. By integrating with Dubber's recording infrastructure, businesses can efficiently retain critical SMS records while ensuring secure communication management.

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

Activities Captured

- SMSs

Collector Configuration

Enter the following credentials of the Dubber Speik account:

- **Dubber Speik Username**
- **Password**
- **Speik AccountId**
- **Speik Solution InstanceId**
- **Speik base URL**

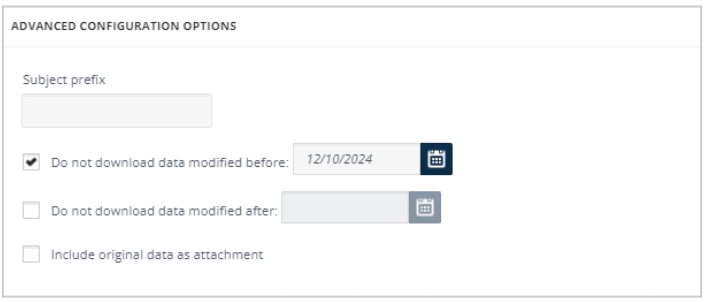
These credentials should be provided to configure the Dubber Speik SMS collector. Reach out to your Dubber/Speik representative to obtain your credentials.

Advanced Configuration Options

There are the following advanced options when configuring the collector with Mergel.

- The **Subject Prefix** feature will add a prefix before the message subject to facilitate the search in the 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 08/17/2024 and the *after date* is set to 09/17/2024, only the data between these two dates will be downloaded. Data outside that timeframe will be ignored.
- The **Include original data as attachment** feature allows including/excluding original data as attachment by enabling/disabling the corresponding checkbox.

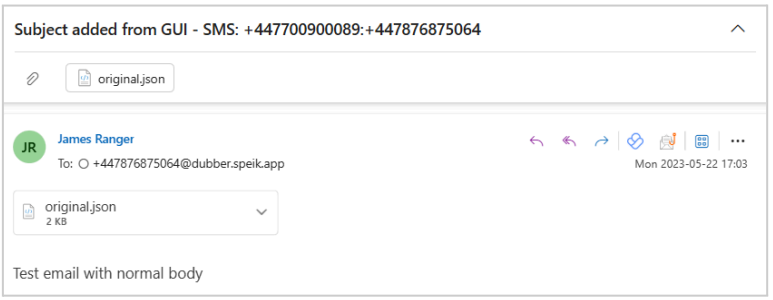


Next Steps

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

- Monitored Users (N/A)
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**

- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

EML

The EML collector is used for importing EML data from Symphony. EML format is widely used by various compliance and archiving solutions and may help the organization avoid the need to develop a specific source parser. The EML 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 to 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 a poorer look (XML to HTML looks better than EML).
- EML misses information about the room created, when joined, etc.

Collector Configuration

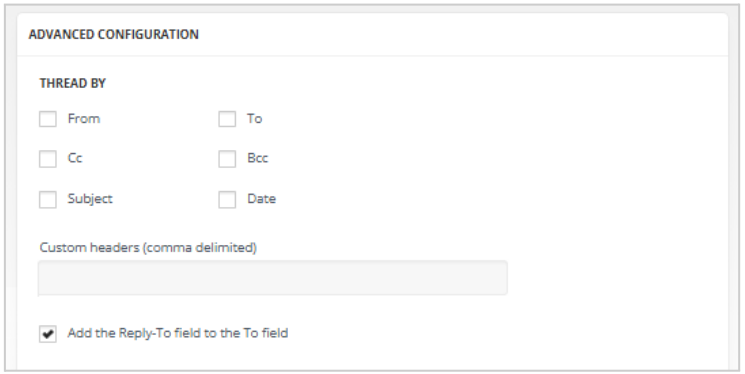
Advanced Configuration

Thread By

This section allows threading a message based on:

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

- **Custom headers (comma-delimited):** Specify the headers you wish to include, using commas as delimiters.
- **Add the Reply-To field to the To field:** If checked, the **Reply-To** field value will be added to the **To** field value.



Timestamp Formatting

For more details on how to configure timestamps, see **Time Stamp Formatting**.

Other Configurations

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

- **File Source**
- **Execute Script Against Source Files**
- **PGP Decryption**
- **Folders**
- **After Successful Importing**
- **Misc Settings**

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**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:

Supported Notifications

The importer supports the following notification preferences:

- **Quarantine file**
- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

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.

Mergel retrieves data from Exchange servers via EWS.

Activities Captured

From Exchange:

- Messages
- Meeting requests
- Meeting cancellations
- Appointments

When to Turn File Transfer Off

There is a situation where you would want to turn **File Transfer off** and leave it off - when you must maintain a regulatory compliance standard.

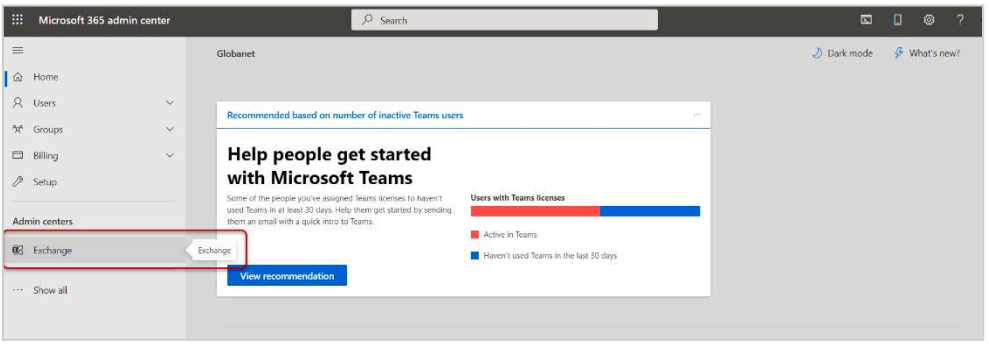
In Skype for Business Online, file transfers within Instant Messaging are considered a "non-archived feature." That means the feature is not captured when you have an **In-Place Hold** set up in Exchange. Thus, the data you would send via file transfer does not get recorded, which can jeopardize compliance. (Shared OneNote pages and PowerPoint annotations are also non-archived features.)

This option is controlled at the user level. In the Skype for Business Admin Center, under **Users**, you will find the option for turning off non-archived features. You are supposed to select this option if you are legally required to preserve electronically stored information.

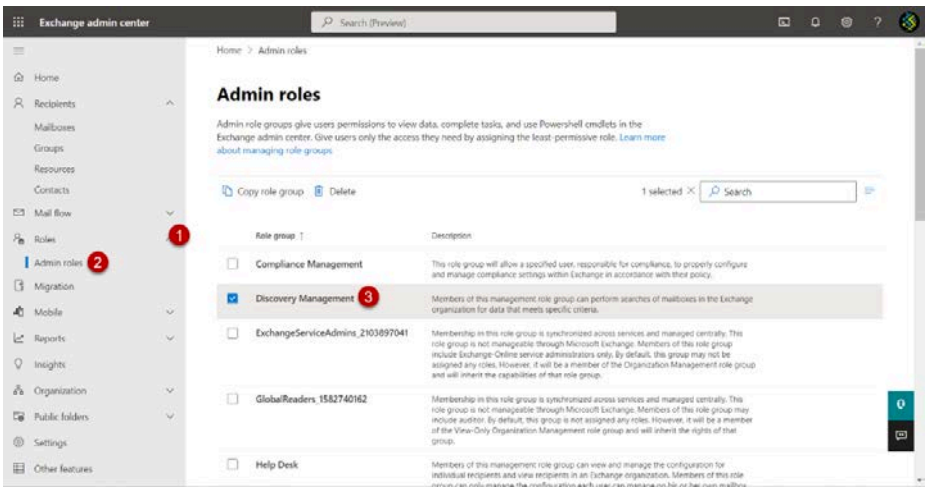
Providing Necessary Permissions to the Account

To provide necessary permissions:

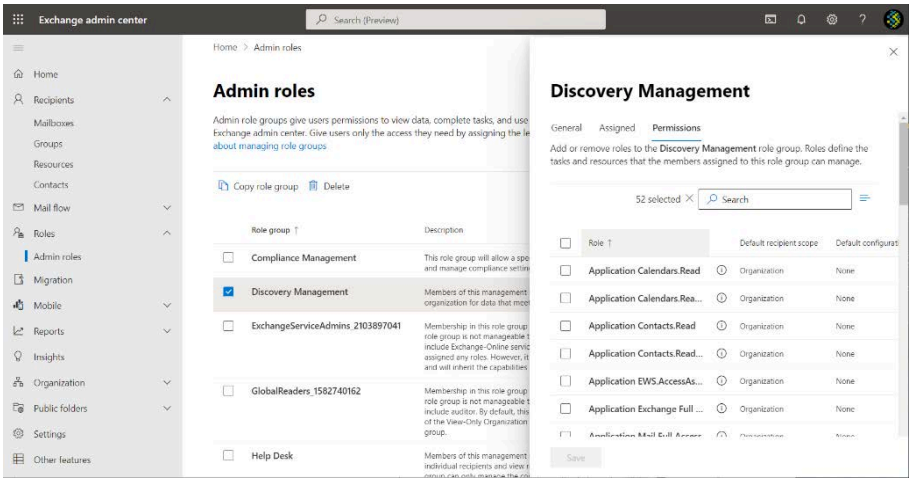
1. Go to https://portal.office.com/AdminPortal/Home.
2. Log into your account if you are not logged in yet.
3. Open **Exchange admin center**.



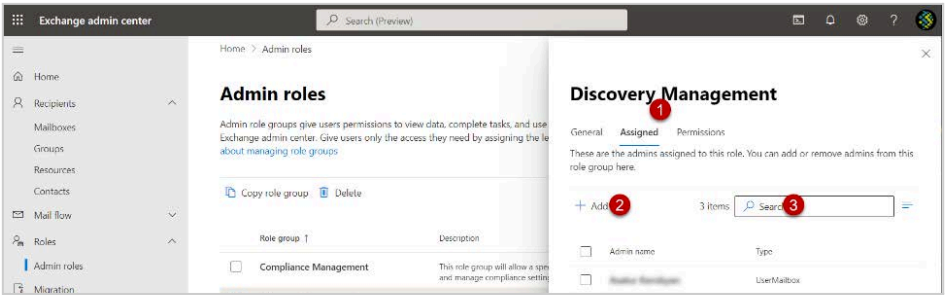
4. Go to **Roles >Admin Roles**.



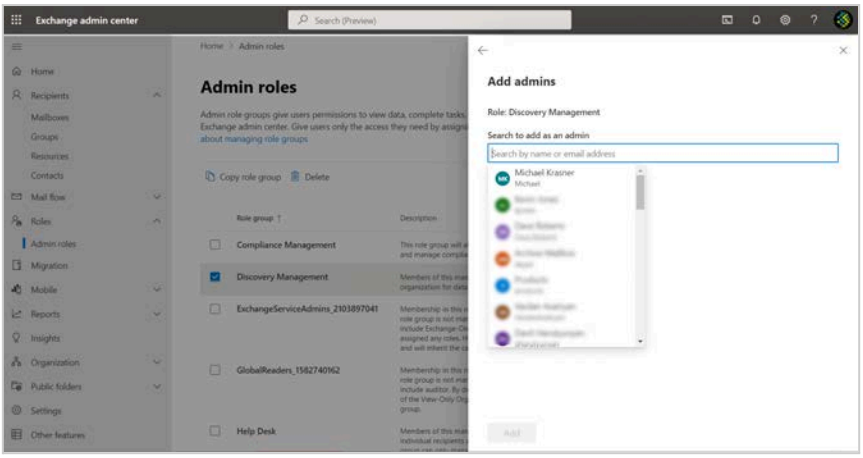
5. Click **Discovery Management** to open its settings.



6. On the **Assigned** tab, select the members to assign the **Admin** role.

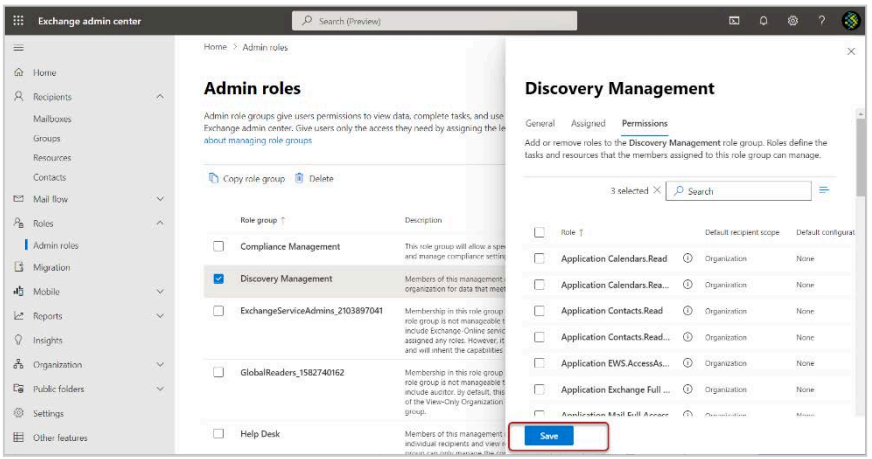


7. Select from the list and click **Add**.



8. On the **Permissions** tab, check the boxes to add roles.
9. Add **Legal Hold**, **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**
>
> **Legal Hold** and **Mailbox Import Export** do not need to be enabled if Retention Policy is going to be used. They should be enabled only in case In-Place Hold is used.



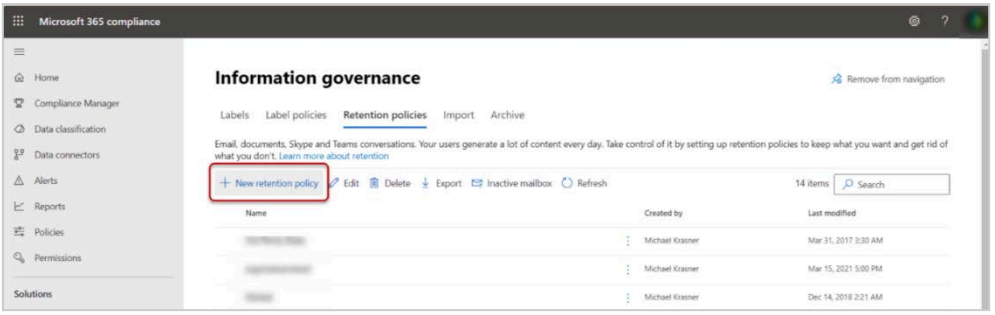
Impersonator user must have **Mailbox Search** permission if **ALL** is selected on the Monitored users tab.

10. Click **Save** in **Discovery Management** settings.

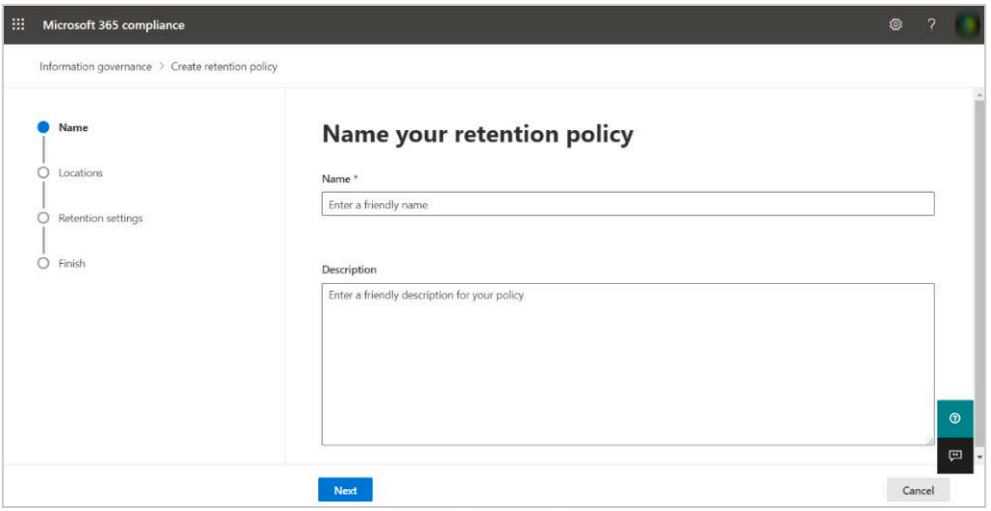
Setting Up Security and Compliance for Microsoft 365

To set up Microsoft 365 Security and Compliance:

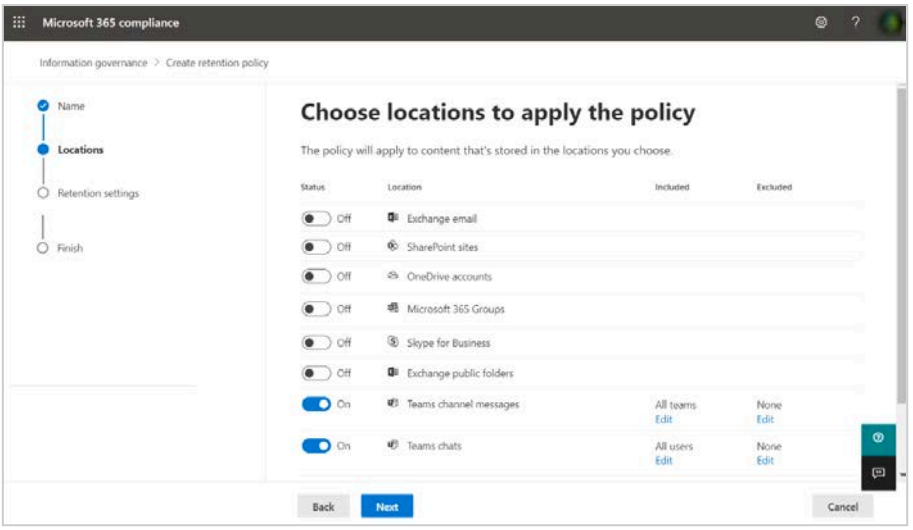
1. Navigate to Information governance, in the Microsoft Compliance center.
2. Click **New retention policy** to start the setup wizard.



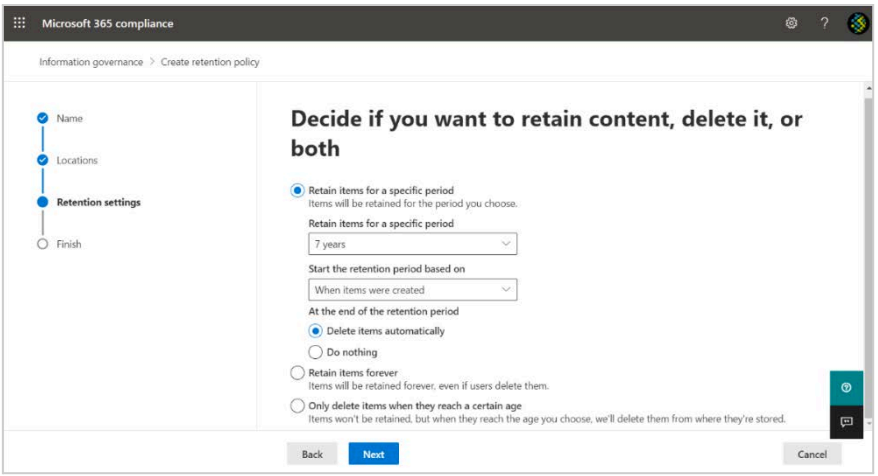
3. Add a **Name** and a **Description** for the policy and click **Next**.



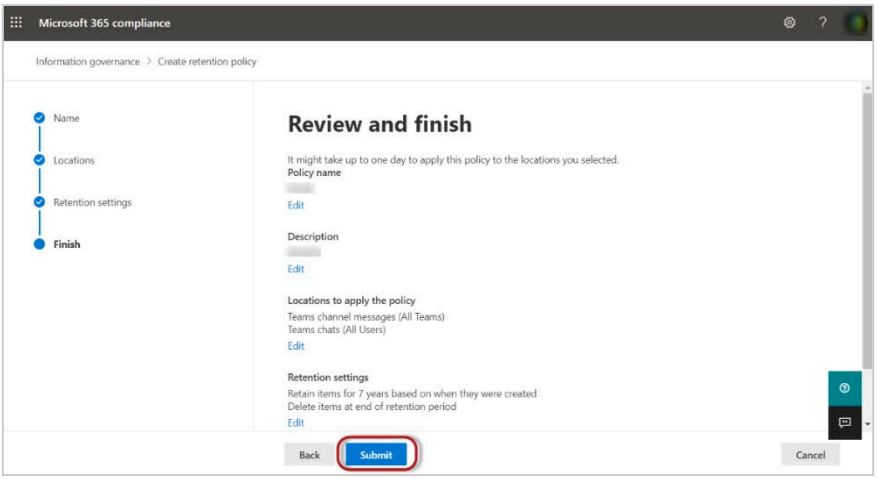
4. In the next screen you will be offered to choose the applications to apply the retention policy to. You can either select **Apply policy only to content in Exchange email**, **public folders**, **Office 365 groups**, **OneDrive,** and **SharePoint** documents.
5. Once you choose the locations where the retention policy applies, click **Next**.



6. On the next screen, you can set the retention period of the messages along with other options. Configure the settings so that they meet your compliance requirements and click **Next**.



7. Review the settings that you have chosen. If everything is correct, click **Submit**.



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

Enable In-Place Hold

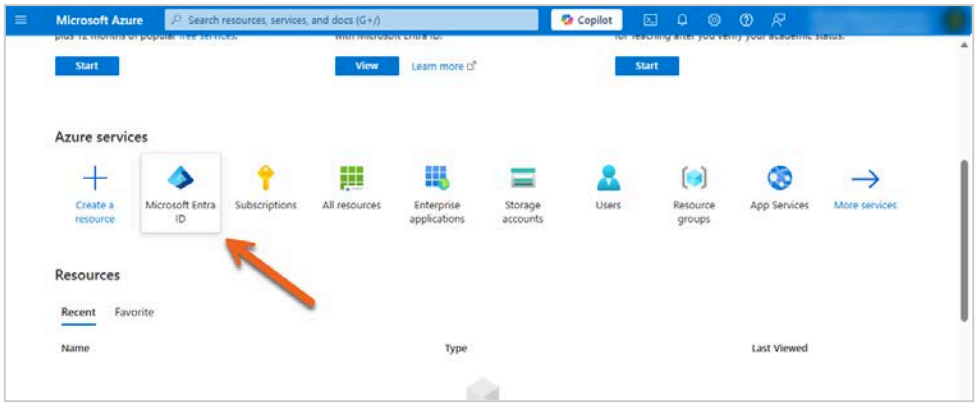
Creation of **In-Place Holds in Exchange Online** will be discontinued later this year or early next year. As an alternative to using **In-Place hold**, please, use **Retention Policy** as described in Providing Necessary Permissions to the Account.

Creating a Microsoft Entra ID Application

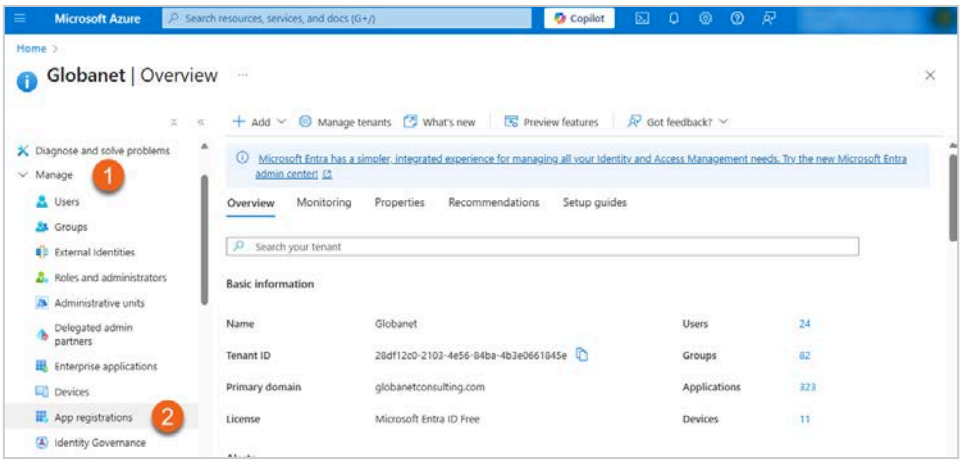
The Office 365 or Azure administrator in your organization must complete the steps detailed in the sections below.

Registering an Application

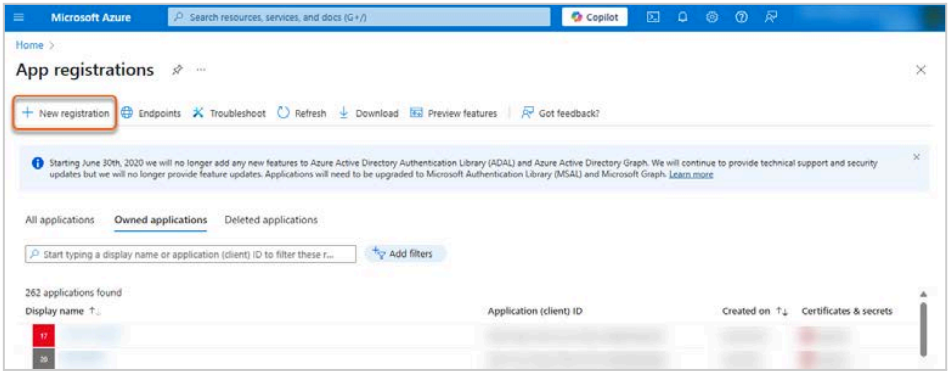
1. Sign in to **Azure Portal**.
2. Select **Microsoft Entra ID** under **Azure services**.



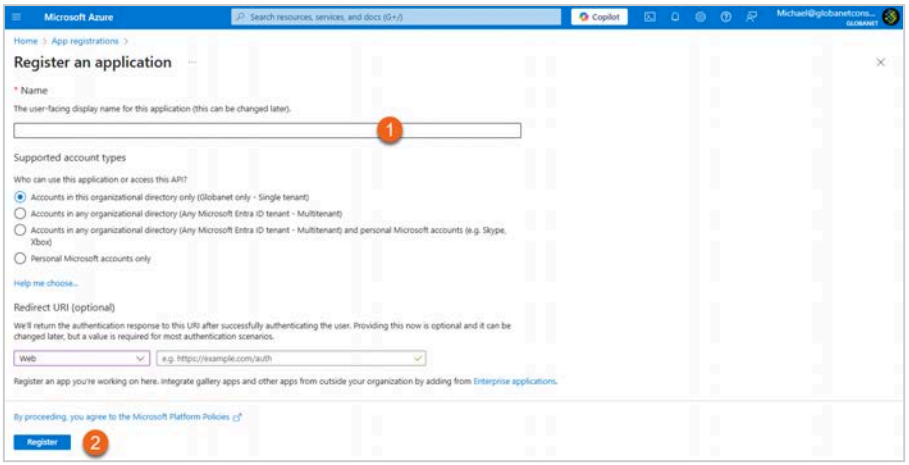
3. In the left-hand navigation pane, click **Manage > App registrations**.



4. Click **New registration**.



5. To register an application:
   5.1. Enter a **Name** for the application.
   5.2. Click **Register**.



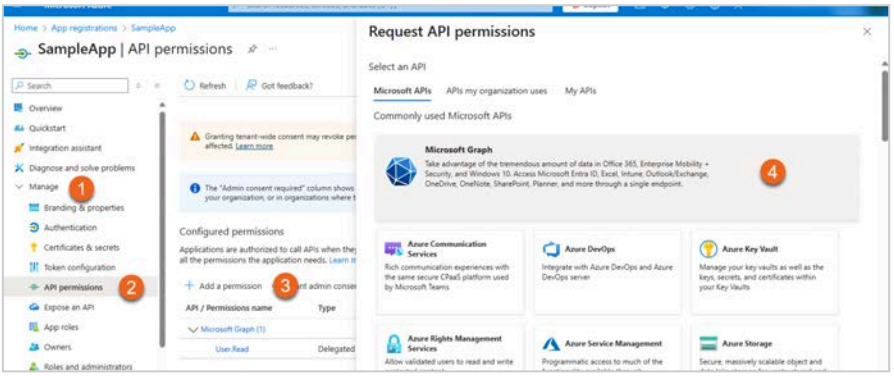
6. An **Application (client) ID** and **Directory (tenant) ID** will be generated. Keep both for configuring the collector in Merge1.

Granting Permissions

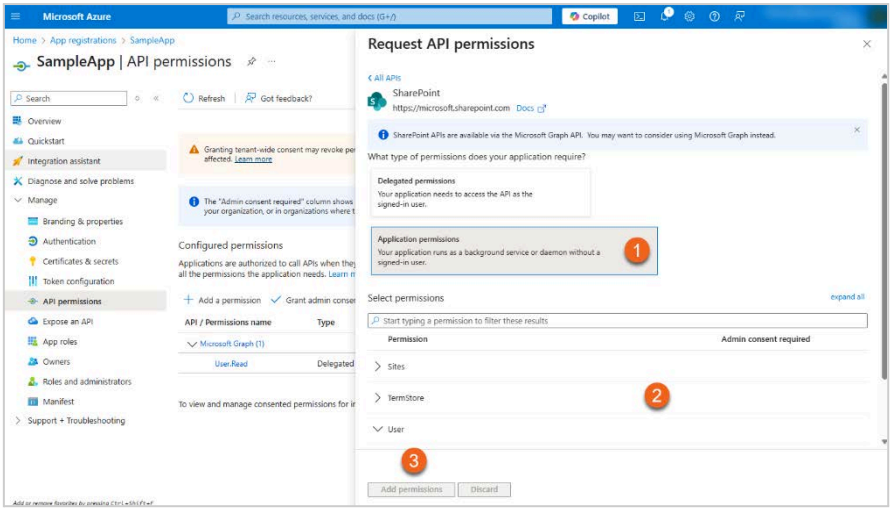
Adding Microsoft Graph API Permissions

To add **Microsoft Graph** API permissions:

1. In the left-hand navigation pane, click **Manage > API permissions**.
2. Click **Add a permission**.
3. In the opened pane select the **Microsoft Graph** API.



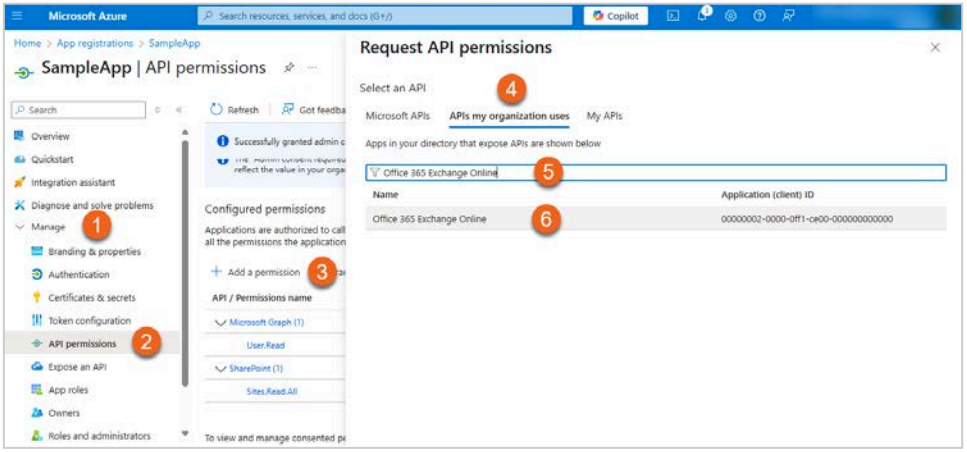
4. To add the necessary permission:
   4.1. Click **Application permissions**.
   4.2. Add the following permission:
      4.2.1. **User**: *User.Read.All*
   4.3. Click **Add permissions**.



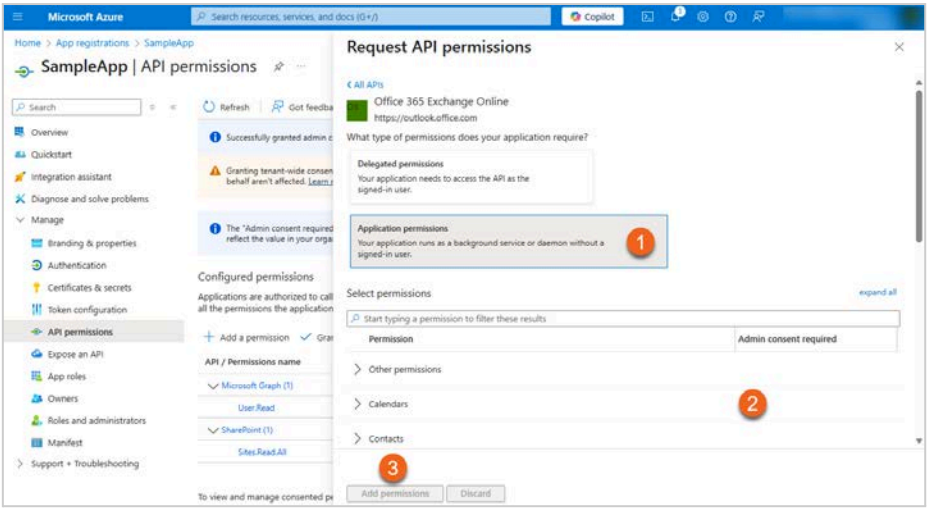
Adding Office 365 Exchange Online API Permissions

To add **Office 365 Exchange Online** API permissions:

1. In the left-hand navigation pane, click **Manage > API permissions**.
2. Click **Add a permission**.
3. Click **APIs my organization uses**.
4. Search for **`Office 365 Exchange Online`** and choose the API.

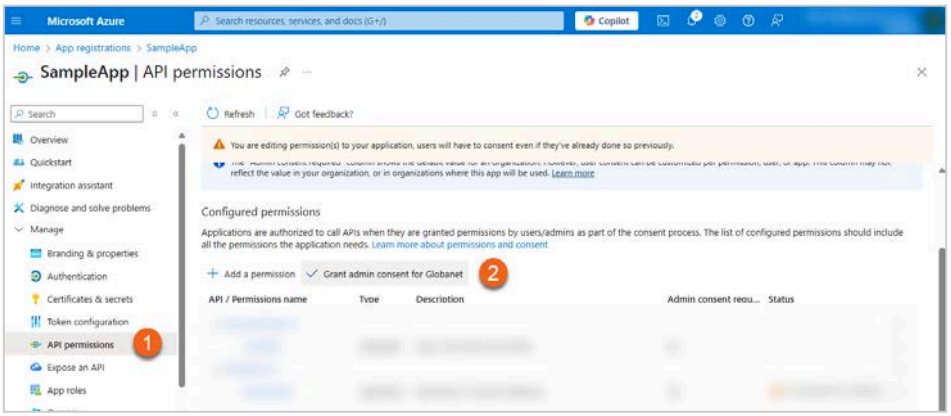


5. To add the necessary permissions:
   5.1. Click **Application permissions**.
   5.2. Add the following permissions:
      5.2.1. **Other permissions**: full_access_as_app
      5.2.2. **MailboxSettings**: MailboxSettings.Read
   5.3. Click **Add permissions**.



Granting Admin Consent

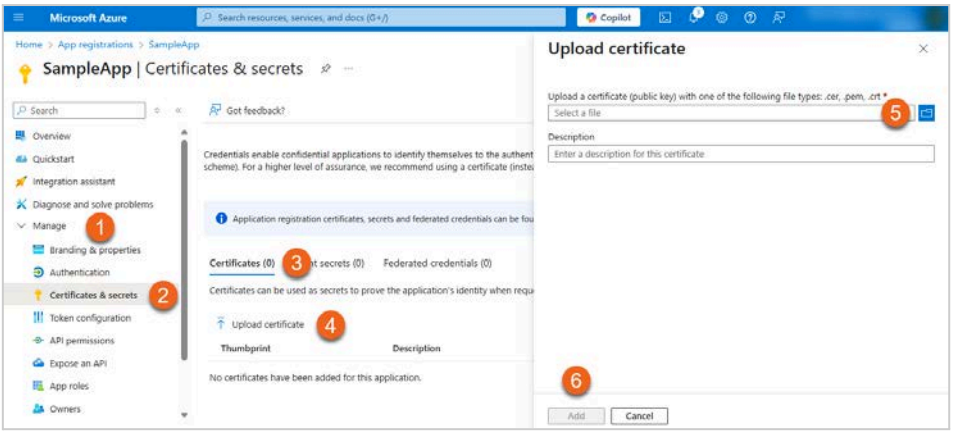
1. Go back to **API permissions**.
2. Click **Grant admin consent** for your company to grant the added permissions.



Uploading a Certificate

To upload a certificate:

1. In the left-hand navigation pane, go to **Manage > Certificates & secrets**.
2. Select **Certificates**.
3. Click **Upload certificate**.
4. Select a certificate (public key) with one of the following file types: `.cer`, `.pem`, `.crt`.
5. Click **Add**.



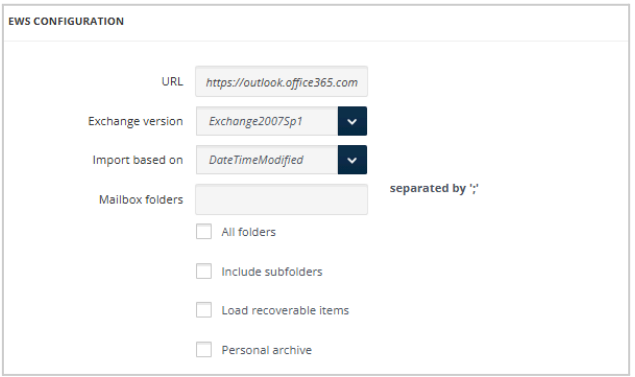
A certificate **thumbprint** will be generated. Keep the value for configuring the collector in Merge1.

For more information on how to create a certificate, see **Creating a Certificate (Private and Public Keys)**.

Collector Configuration

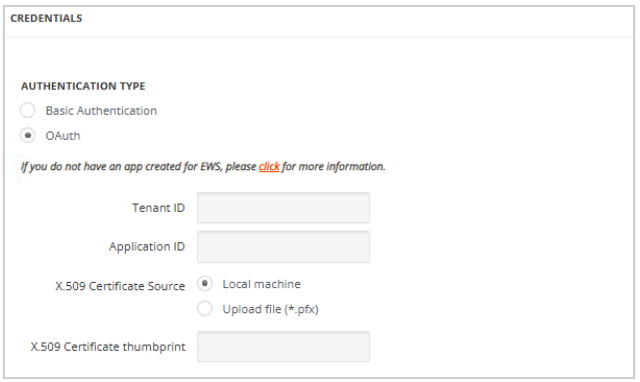
To configure the EWS collector:

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 the last modification date (DateTimeModified) or by the creation date (DateTimeCreated). 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.

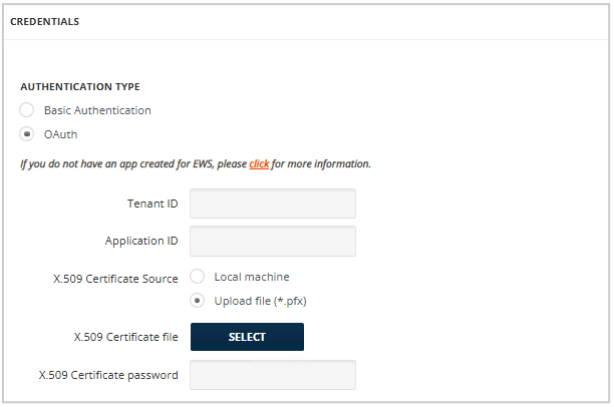


9. In case of enabling **Basic Authentication**, enter **Impersonator** and **Password**.
10. Provide **Tenant ID** and **Application ID**.

11. Provide **X.509 Certificate Thumbprint** in case you activate the **Local machine** radio button as the X.509 Certificate source.



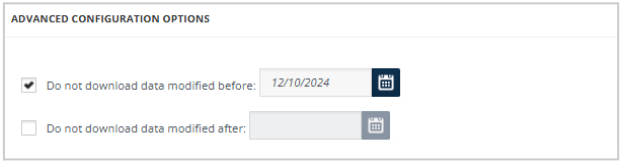
12. In case you activate **Upload file (*.pfx)**, click the **Select** button to upload the certificate and provide **X.509 Certificate password**.



The **Certificate thumbprint** field will be auto populated in case the collector was previously configured by uploading a certificate.

For step-by-step instructions on how to get **Application ID**, **Tenant ID**, and **Thumbprint**, see **Creating a Microsoft Entra ID Application** and **Creating a Certificate (Private and Public Keys)** accordingly.

13. 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 09/17/2024, only the data between these two dates will be downloaded. Data outside that timeframe will be ignored.



14. Select the **Message Class** you would like Merge1 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 Merge1 can import:

Data captured 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.

Message Classes can be edited in **Merge1.Collectors.Base.dll.config** in the Bin folder within the Merge1 7.0[13] installation directory. Default path: `C:\Program Files\Globanet Consulting Services\Merge1 7.0\Bin\Merge1.Collectors.Base.dll.config`.

History Tracking

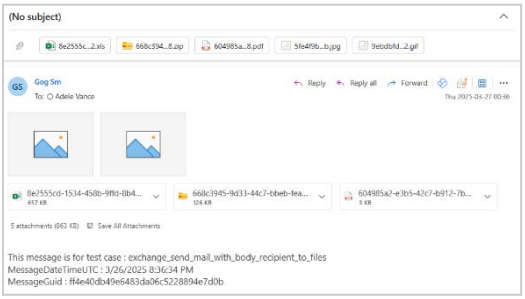
Based on the provided information, there is a chance to monitor a certain timeframe but get a message with a timestamp that is out of the specified frame. This case is applicable when import is based on DateTimeModified.

Next Steps

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

- **MONITORED USERS**
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

[13] In case of Merge1 version 6.0, the path will be `C:\Program Files\Globanet Consulting Services\Merge1 6.0\Bin\Merge1.Collectors.Base.dll.config`.

- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

Exchange Graph API

Microsoft Exchange is a business-class email platform designed to enhance productivity by providing a focused inbox, intelligent organization, and seamless integration with workplace tools. With advanced features that adapt to user workflows, Exchange enables faster and more efficient communication across organizations.

The **Merge1 Exchange Graph API collector** retrieves Exchange server data via Microsoft Graph API, ensuring secure and efficient email archiving, compliance, and data management.

Activities Captured

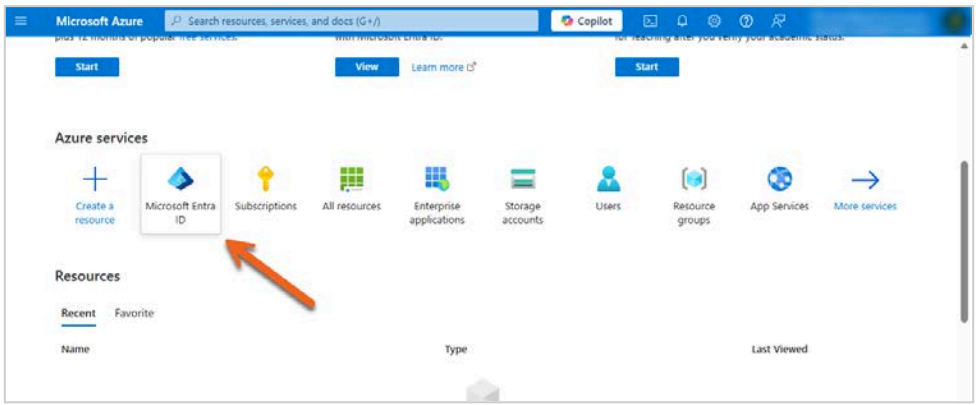
- Messages
- Meeting requests
- Meeting cancellations

Creating a Microsoft Entra ID Application

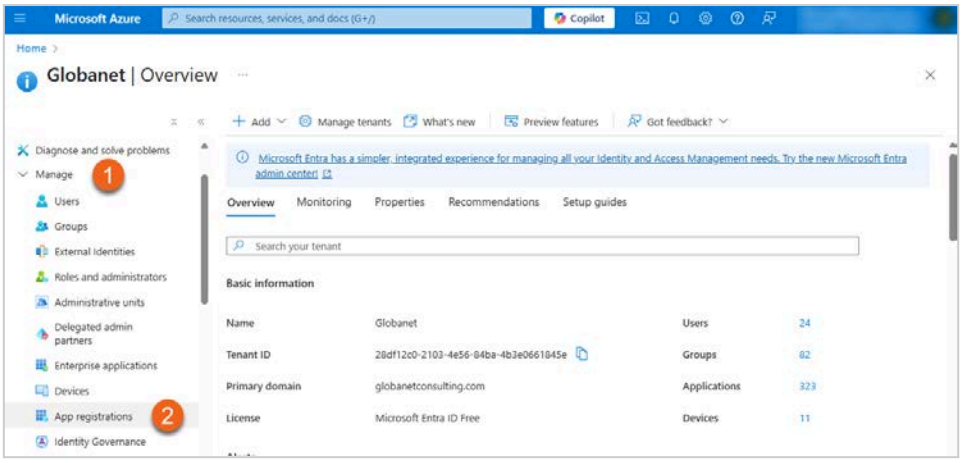
The Office 365 or Azure administrator in your organization must complete the steps detailed in the sections below.

Registering an Application

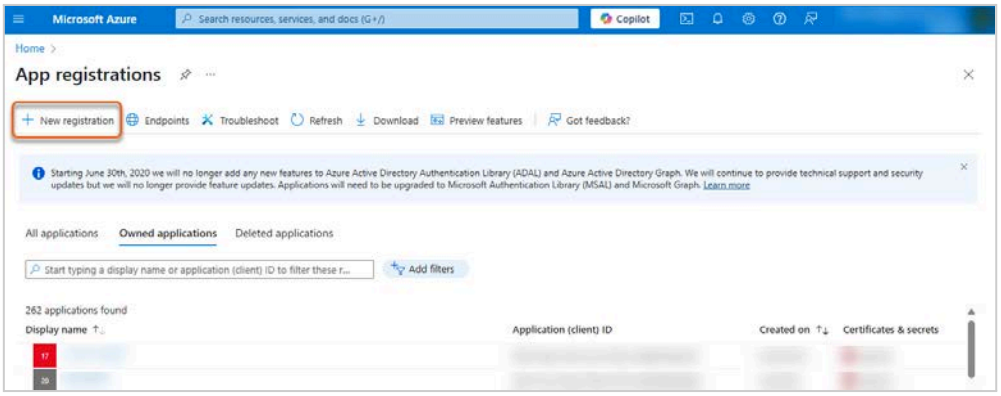
1. Sign in to Azure Portal.
2. Select **Microsoft Entra ID** under **Azure services**.



3. In the left-hand navigation pane, click **Manage > App registrations**.



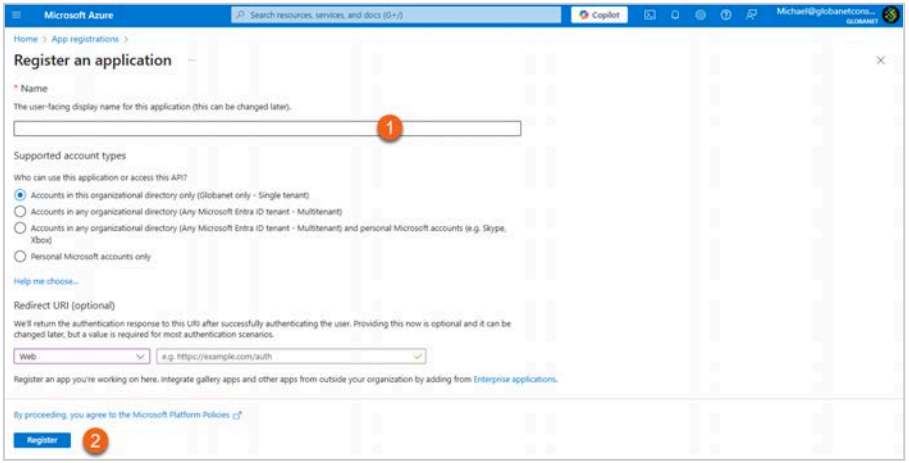
4. Click **New registration**.



5. To register an application:

   5.1. Enter a **Name** for the application.

   5.2. Click **Register**.



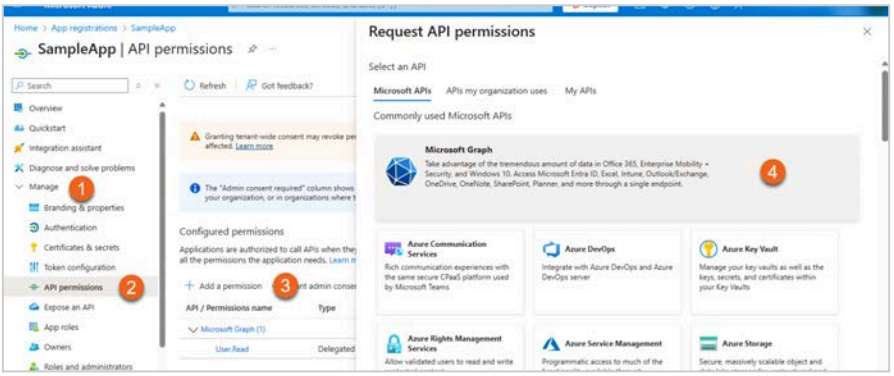
6. An **Application (client) ID** and **Directory (tenant) ID** will be generated. Keep both for configuring the collector in Mergel.

Granting Permissions

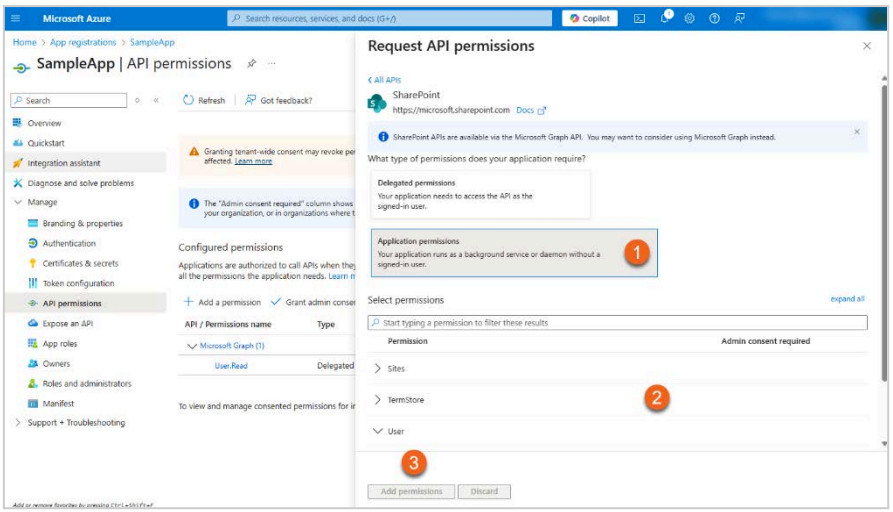
Adding Microsoft Graph API Permissions

To add **Microsoft Graph** API permissions:

1. In the left-hand navigation pane, click **Manage > API permissions**.
2. Click **Add a permission**.
3. In the opened pane select the **Microsoft Graph** API.

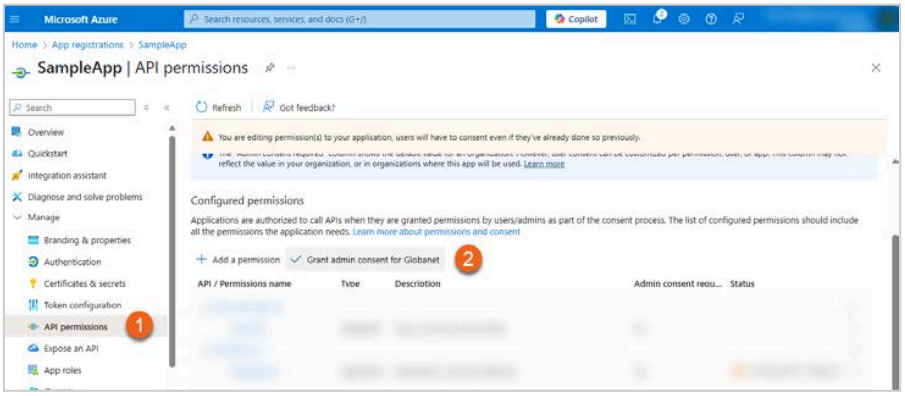


4. To add the necessary permission:
   4.1. Click **Application permissions**.
   4.2. Add the following permissions:
      4.2.1. **Mail**:
         4.2.1.1. Mail.Read
         4.2.1.2. *Mail.ReadBasic.All*
      4.2.2. **User**: *User.Read.All*
   4.3. Click **Add permissions**.



Granting Admin Consent

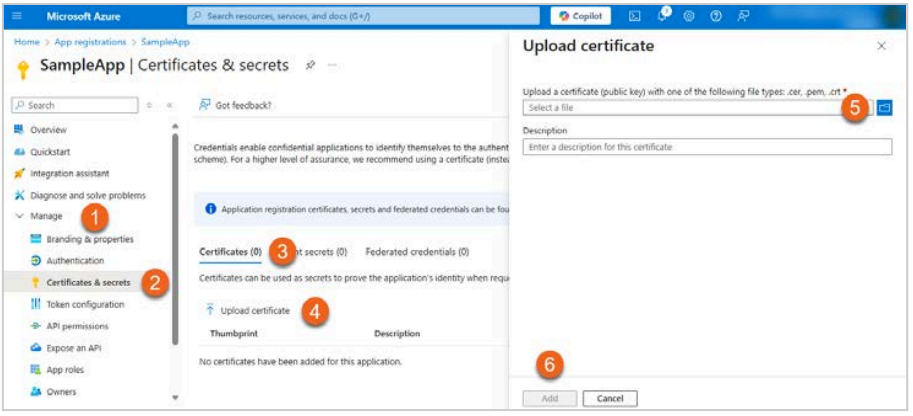
1. Go back to **API permissions**.
2. Click **Grant admin consent** for your company to grant the added permissions.



Uploading a Certificate

To upload a certificate:

1. In the left-hand navigation pane, go to **Manage > Certificates & secrets**.
2. Select **Certificates**.
3. Click **Upload certificate**.
4. Select a certificate (public key) with one of the following file types: `.cer`, `.pem`, `.crt`.
5. Click **Add**.



A certificate **thumbprint** will be generated. Keep the value for configuring the collector in Merge1.

For more information on how to create a certificate, see **Creating a Certificate (Private and Public Keys)**.

Configuring the Collector in Merge1

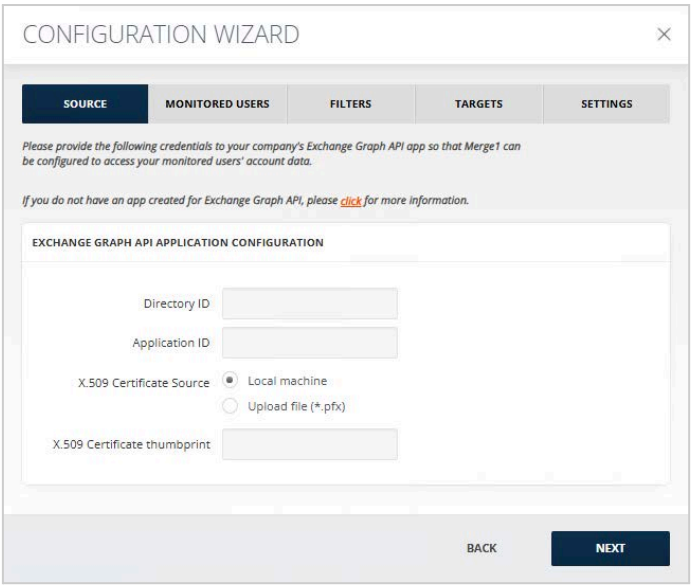
Adding the Importer

For details on adding the importer, see **Adding a New Importer**.

Source Configuration

For configuring the **Exchange Graph API** application:

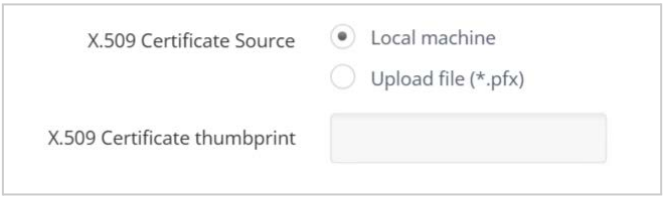
1. Add the previously saved *Directory (tenant) ID* and *Application (client) ID* in the **Directory ID** and **Application ID** fields, respectively.



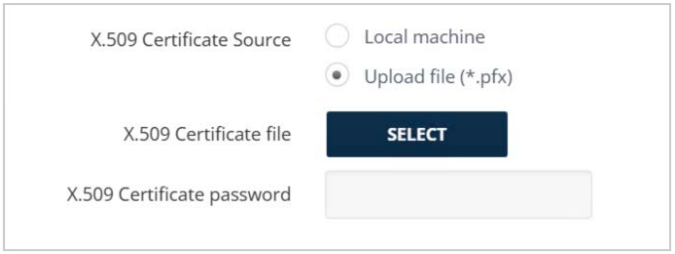
2. For **X509 Certificate** configuration:

   - Provide **X.509 Certificate thumbprint** in case you activate the **Local machine** radio button as the X.509 Certificate source.

     The **Certificate thumbprint** field will be auto populated in case the collector was previously configured by uploading a certificate.



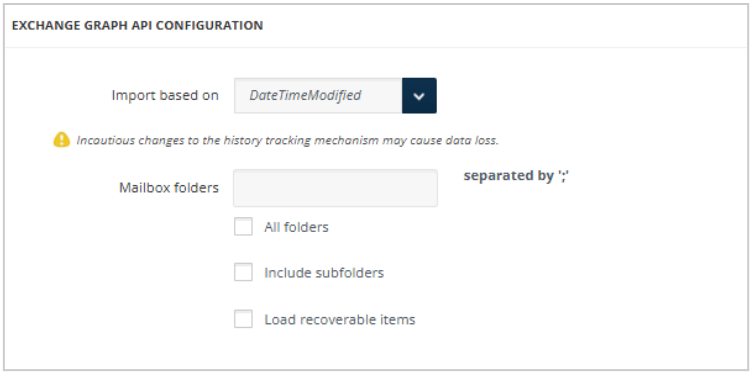
   - In case you activate **Upload file (*.pfx)**, click the **Select** button to upload the certificate provide **Password**.



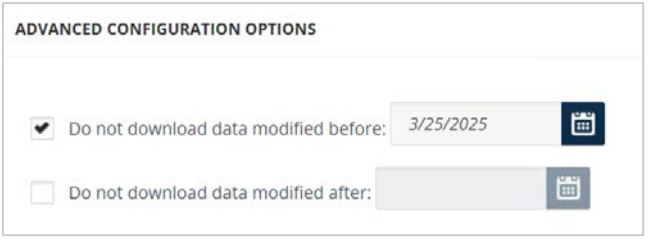
3. Click **Next**.

Exchange Graph API Configuration

1. 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.
2. 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 (";").
3. Check **All folders** to process data within all the folders.
4. To process data within the subfolders of the specified mailboxes, check **Include subfolders**.
5. To search for the mentioned mailbox folders in the recovery route folders, check **Load recoverable items**.

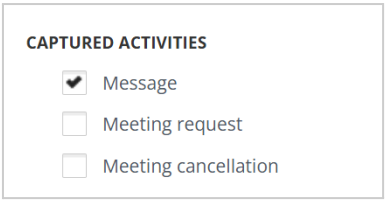


6. For **Advanced Configuration Options** - **Do Not Download Data Modified/Created Before** and **Do Not Download Data Modified/Created After** allow cutting off data outside the set date range. If the *before date* is set to 08/17/2024 and the *after date* is set to 09/17/2024, only the data between these two dates will be downloaded. Data outside that timeframe will be ignored.



7. Select the **Captured Activity** type you would like Merge1 to import and then click **Save**.

   There are the following **activities** that Merge1 can import:



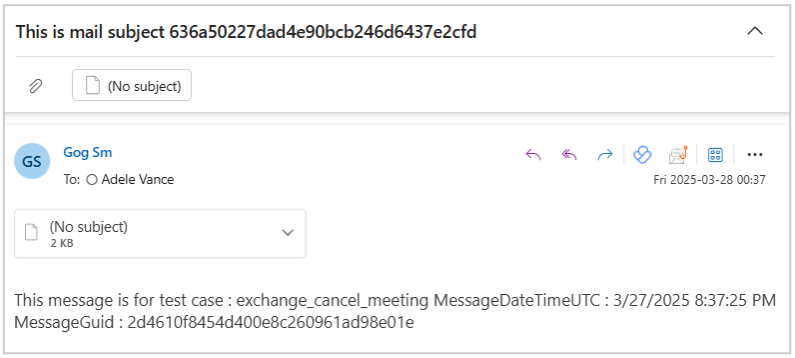
8. To include messages irrespective of their type, select all of them.

Next Steps

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

- **MONITORED USERS**
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

FX Connect

FX Connect is a market-leading FX execution venue designed to help firms efficiently manage multiple portfolios, connect with brokers, and streamline global operations. By offering electronic tools for pre- and post-trade workflows, FX Connect supports organizations in optimizing trading processes while ensuring regulatory compliance.

The **Mergel FX Connect collector** captures FX Connect-generated data, enabling businesses to archive, analyze, and integrate trade-related communications into their data management and compliance systems.

Activities Captured

- Messages

Captured activities can contain:

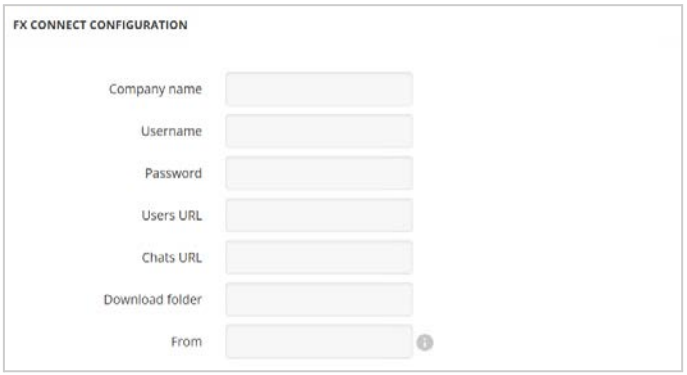
- Session ID
- Trade participants
- Message body
- Activity datetime

Collector Configuration

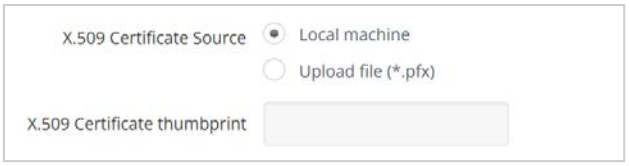
FX Connect Configuration

To configure the source:

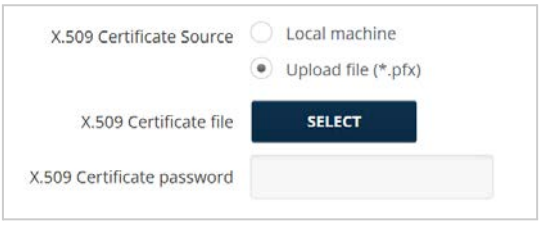
1. Fill out the following fields:
   - **Company name**: The company name provided to FX Connect.
   - **Username**: The username provided to FX Connect.
   - **Password**: The user's password.
   - **Users URL**: The user link.
   - **Chats URL**: The chat link.
   - **Download folder**: The download directory.
   - **From**: A dummy email address is being added in case the email of the event is missing.



2. Provide **X.509 Certificate Thumbprint** if you activate the **Local machine** radio button as the X.509 Certificate source.



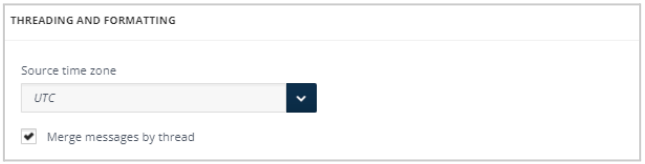
3. If you activate **Upload file (*.pfx)**, click the **Select** button to upload the certificate and provide the **X.509 Certificate password**.



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, Merge1 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.



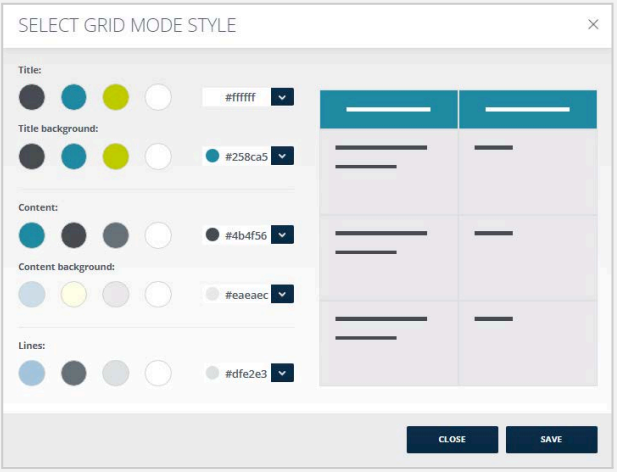
Message Body

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

- **Plain**: Displays the message in a simple text format.
- **Grid mode**: Displays output message content in a compact grid format for structured and efficient viewing. The information is structured into the following columns:
    - *Message creator*
    - *Message timestamp*
    - *Message*

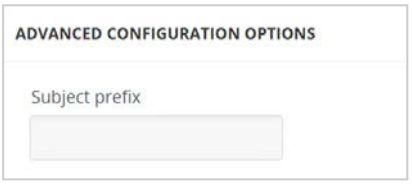
Tip

In **Grid mode**, the color scheme can be adjusted through the **Select Style** pop-up menu:



Advanced Configuration Options

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

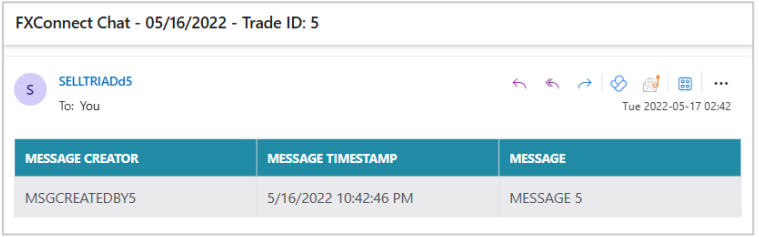


Next Steps

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

- Monitored Users (N/A)
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

FX Connect (File-Based)

FX Connect is a market-leading FX execution venue designed to help firms efficiently manage multiple portfolios, connect with brokers, and streamline global operations. By offering electronic tools for pre- and post-trade workflows, FX Connect supports organizations in optimizing trading processes while ensuring regulatory compliance.

The **Merge1 FX Connect collector** captures FX Connect-generated data, enabling businesses to archive, analyze, and integrate trade-related communications into their data management and compliance systems.

Data Import and Message Handling

- Data from FX Connect should be imported into Merge1 in CSV format. Merge1 automatically maps the columns in the CSV file to the corresponding fields in the output message.
- By default, message participants are imported using their FX Connect User ID. To map participants to their email addresses, you must add each email address along with its corresponding FX Connect User ID in the User Mappings section of the collector setup.
- The collector automatically merges messages that share the same session ID into a single output message, ensuring continuity and reducing duplication.

Activities Captured

- Messages

Captured activities can contain:

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

Collector Configuration

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

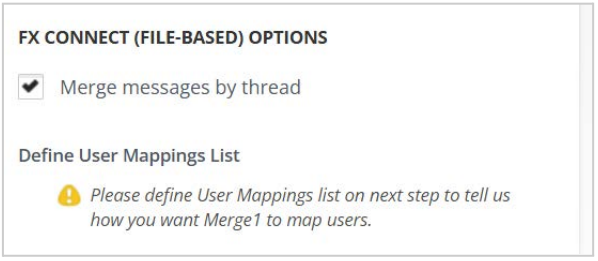
- **File Source**
- **Execute Script Against Source Files**
- **PGP Decryption**
- **Folders**
- **After Successful Importing**
- **Misc Settings**

FX Connect (File-Based) Collector Options

If you want to manually set up the **Source time zone**, select the relevant one from the drop-down list. By default, Merge1 sets the **Source time zone** as **UTC**.

FX Connect (File-Based) Options

The **Merge messages by thread** option combines all messages from a thread into a single message.



Define User Mappings List

Merge1 allows matching an **`FXUserID`** with a user's SMTP address using the **Match Email Address** feature available in the **Processing** section of the **IMPORTER SETTINGS**. While this feature is typically used to replace outdated SMTP addresses with new ones, it can also be leveraged to associate **`FXUserID`**s with corresponding email addresses.

To enable this mapping, create a CSV file containing the following five columns for each user:

- **`LastName`**
- **`FirstName`**
- **`CompanyName`**
- **`FXUserID`**
- **`SMTP address`**

Select **Change the SMTP Address** and specify the location of the CSV file. You can click **Preview Match Email Mappings** to review the data layout, then click **Save** to apply the changes.

Message Body

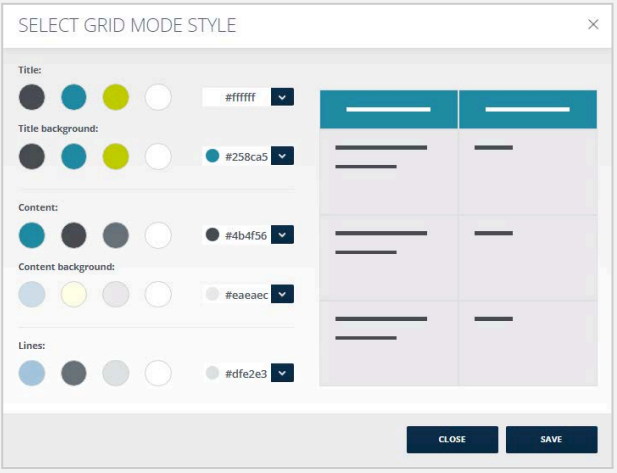
This setting determines how imported messages are displayed in the target. There are the following output message body options:

- **Plain**: Displays the message in a simple text format.
- **Grid mode**: Displays output message content in a compact grid format for structured and efficient viewing. The information is structured into the following columns:
    - *Message creator*

- *Message timestamp*
- *Message*

Tip

In **Grid mode**, the color scheme can be adjusted through the **Select Style** pop-up menu:

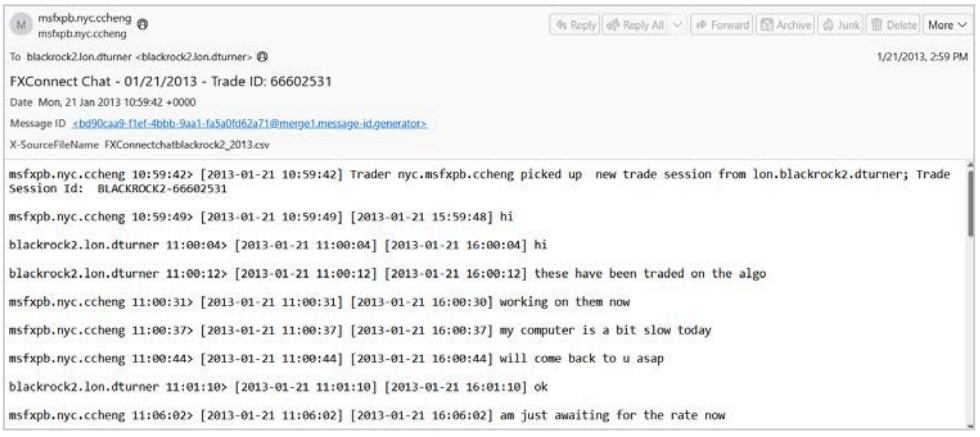


Next Steps

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

- Monitored Users (N/A)
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Quarantine file**

- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

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. Drive is also available as a standalone offering, with Drive Enterprise. Supported G Suite Plans are G Suite Business and G Suite Enterprise.

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
- Comments and replies of shared documents

Service Account Creation

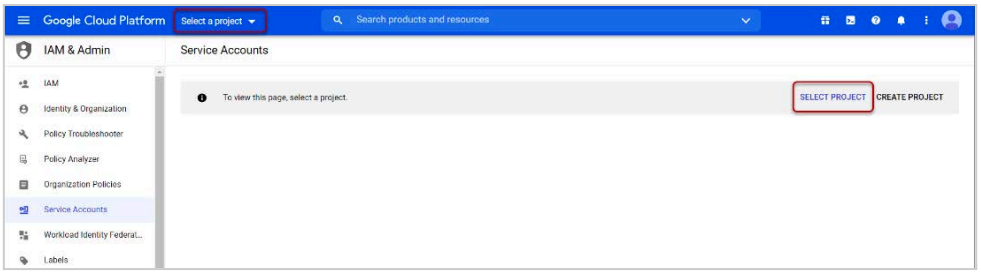
First, a service account and its credentials need to be created. During this procedure information that will be used later for the G Suite domain-wide delegation of authority and in the code to authorize with the service account needs to be gathered.

The three items that will be needed later are service account's:

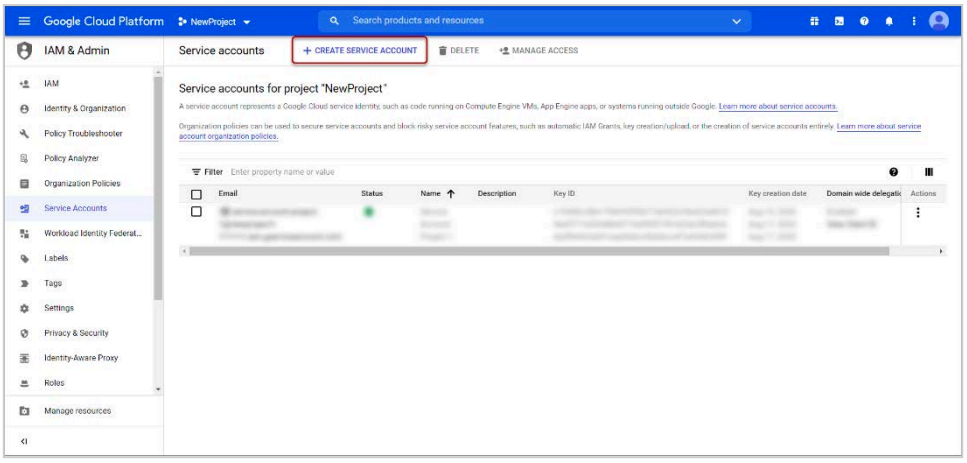
- Client ID
- Private key file
- Email address.

To create a Service Account:

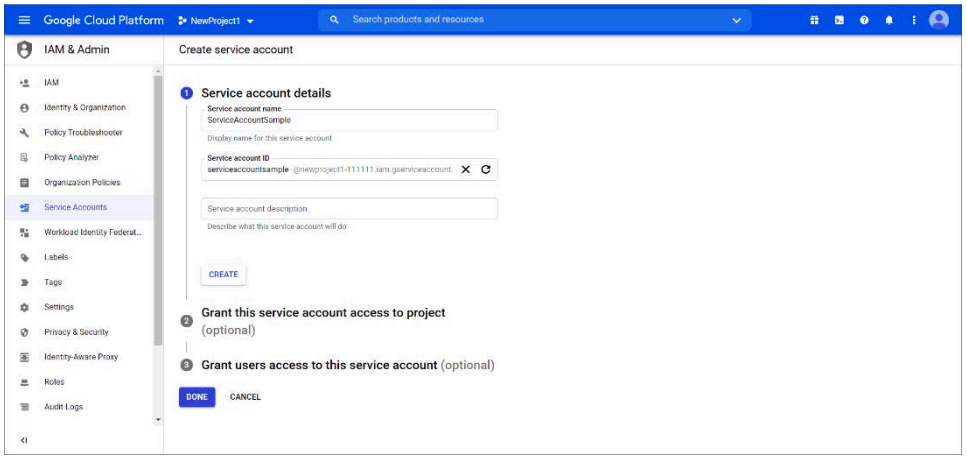
1. Login to https://console.developers.google.com/iam-admin/serviceaccounts. If prompted, select a project.



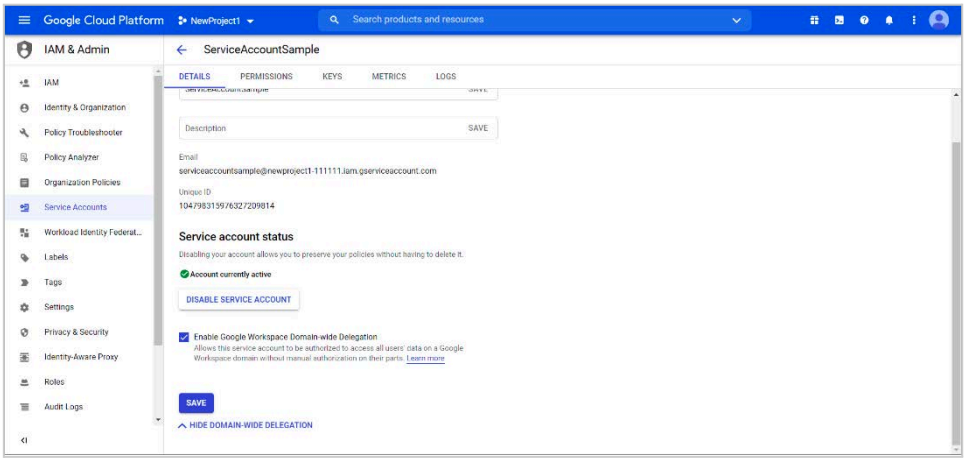
2. Click **Create service account**.



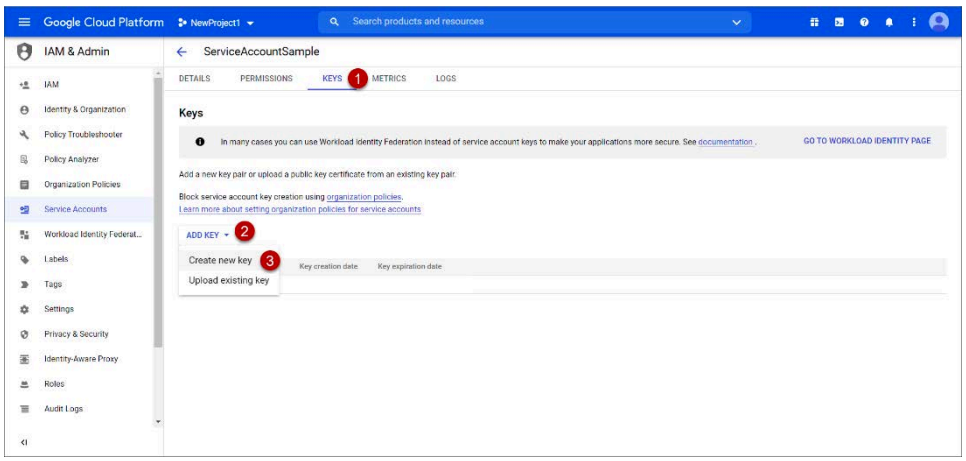
3. In the **Create service** account window, type a **name** for the service account. Note that the next two steps are optional.



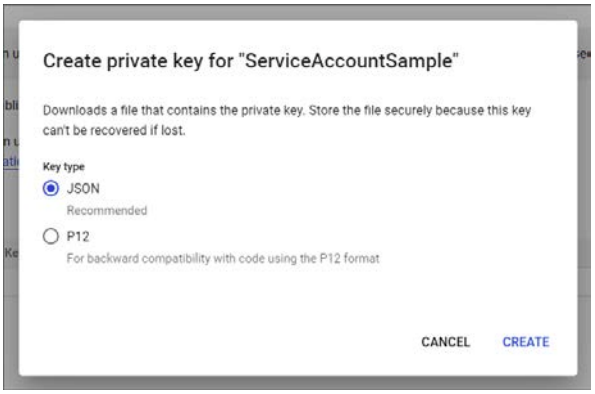
4. Once the service account is created, click it to open its settings. Open the **Show Domain-wide Delegation** menu, check **Enable Google Workspace Domain-Wide Delegation** and click **Save**.



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**.

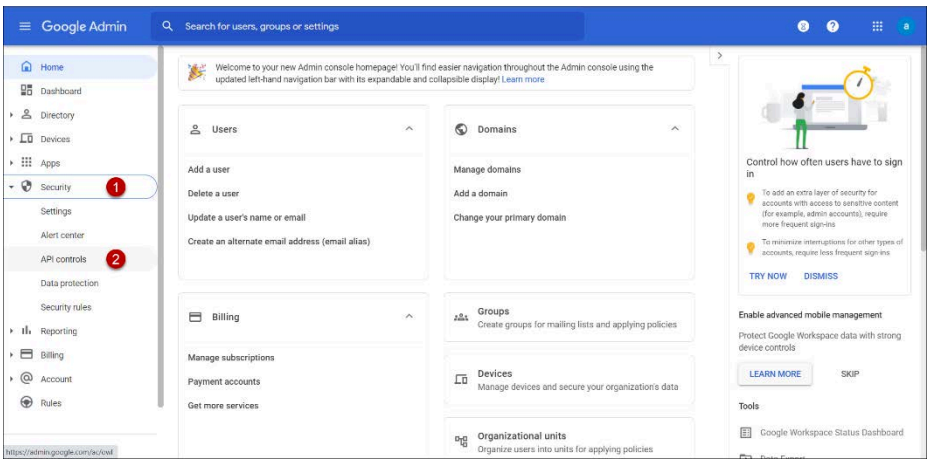


8. Your new public/private key pair is generated and downloaded to your machine; it serves as the only copy of this key. Keep it in a secure location.

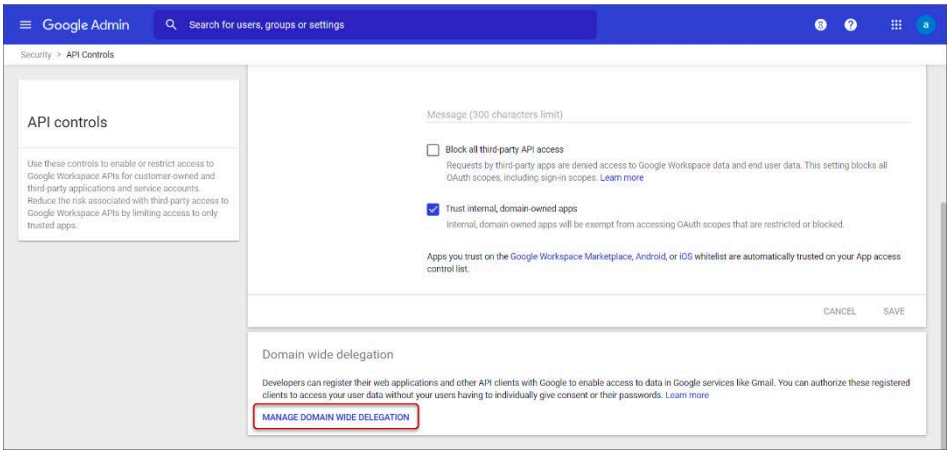
Domain-Wide Authority Delegation to the Service Account

The created service account needs to be granted access to the G Suite domain's user data that should be accessed. The following tasks should be performed by an administrator of the G Suite domain:

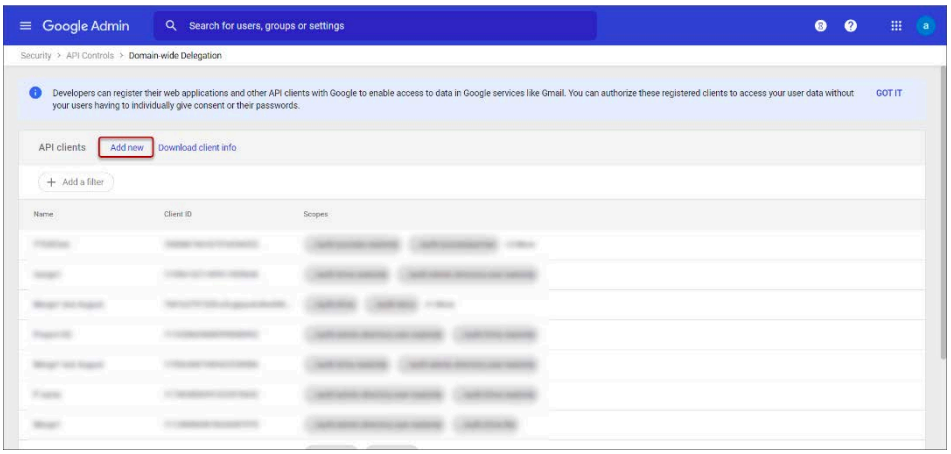
1. Go to your G Suite domain's Admin console https://admin.google.com/, click **Security > API controls**.



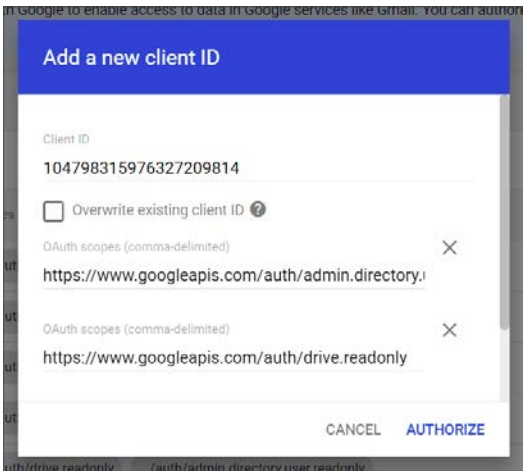
2. Scroll down to **Domain wide delegation** section and click **Manage Domain Wide Delegation**.



3. Click **Add New**.



4. Open the key file that you saved in the above section, copy the value of client_id, paste it into the **Client ID** field. Enter the list of scopes that your application should be granted access to. For example, if you need domain-wide access to Users and Groups enter `https://www.googleapis.com/auth/admin.directory.user.readonly` and `https://www.googleapis.com/auth/drive.readonly` in OAuth scopes fields and click **Authorize**.



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.

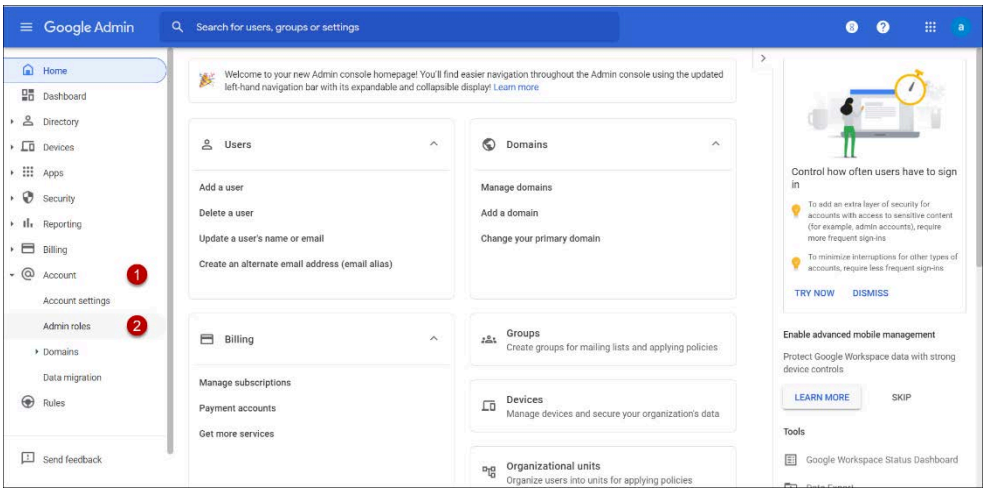
Note

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.

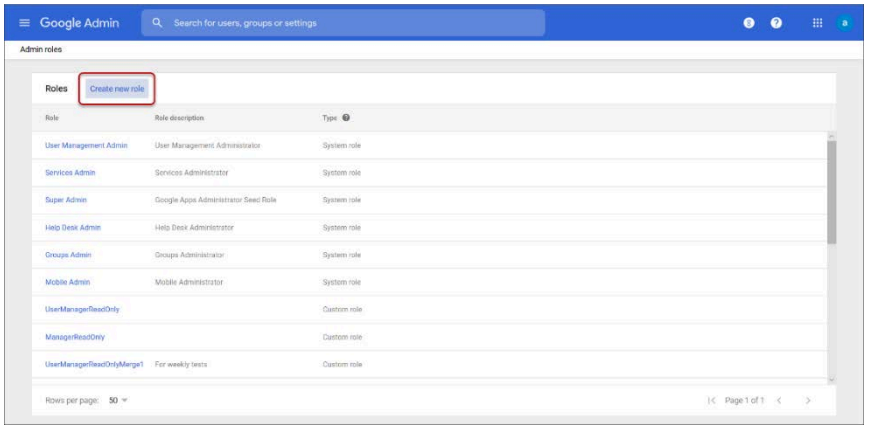
Creating Administrative Role for the User Manager Service Account

To create the account:

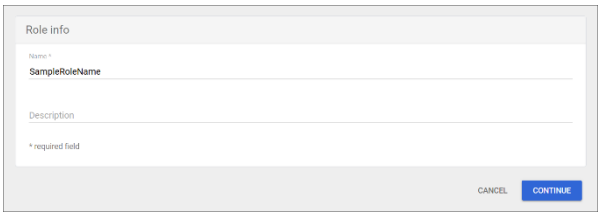
1. Go to https://admin.google.com and click **Account > Admin roles**.



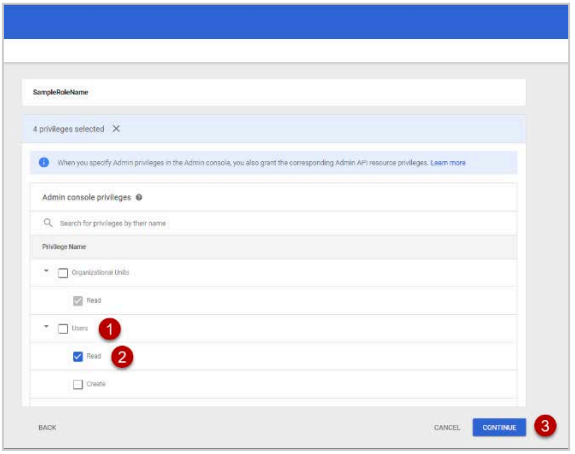
2. Click **CREATE A NEW ROLE**.



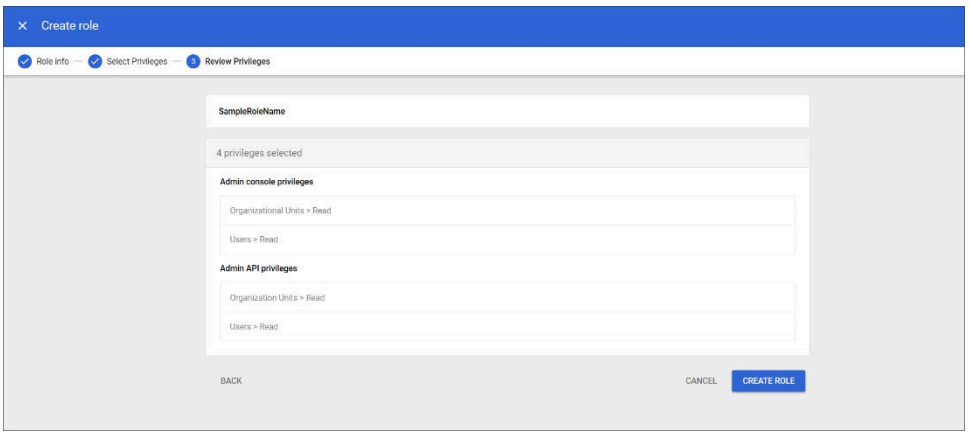
3. Name the new role and click **CONTINUE**.



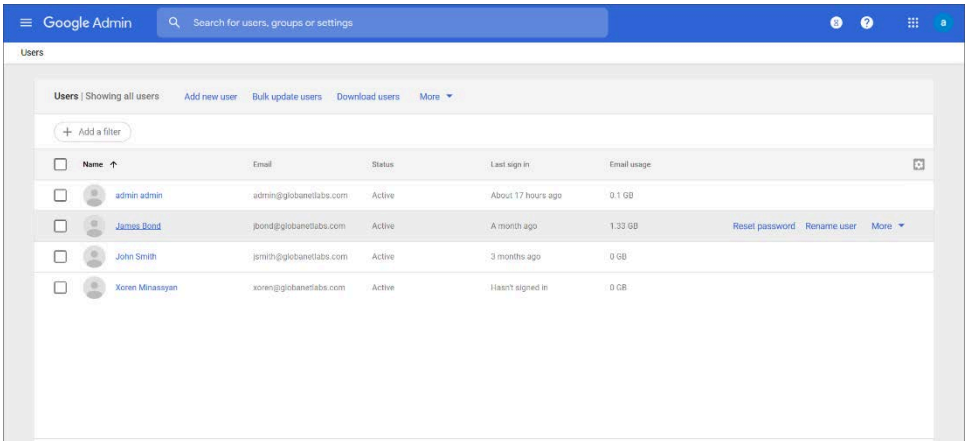
4. Expand **Users**, select **Read** and click **CONTINUE**.



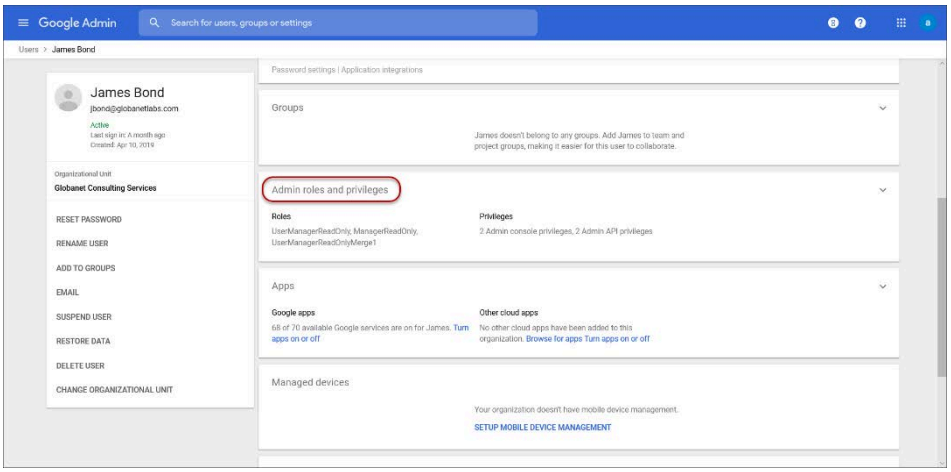
5. Review the privileges and click **CREATE ROLE**.



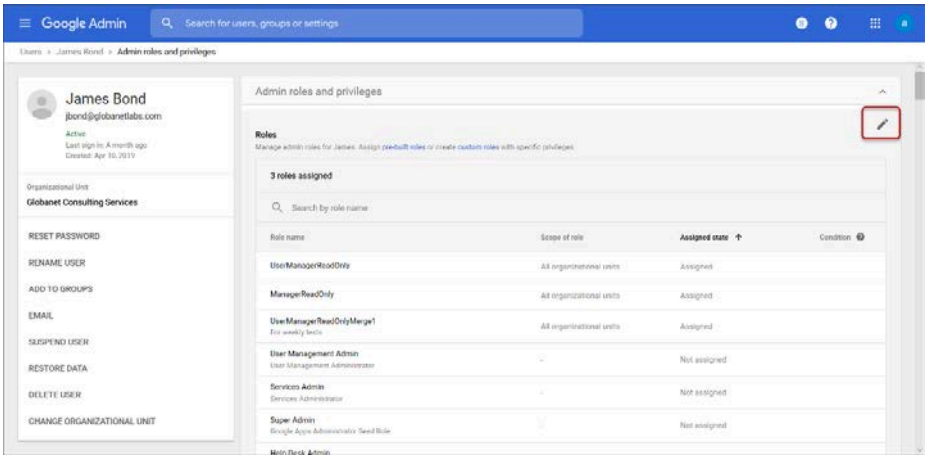
6. To assign the role to a user, go to https://admin.google.com and click **Users**, then click the user that you want to assign the role to.



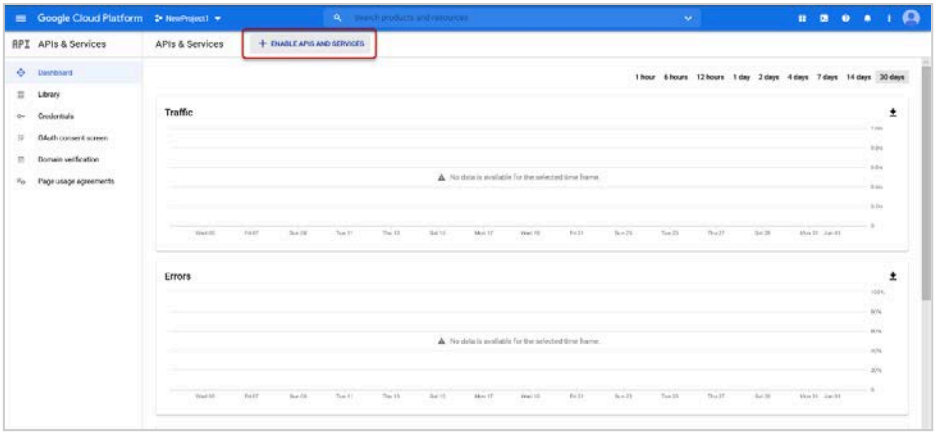
7. Select **Admin roles and privileges**.



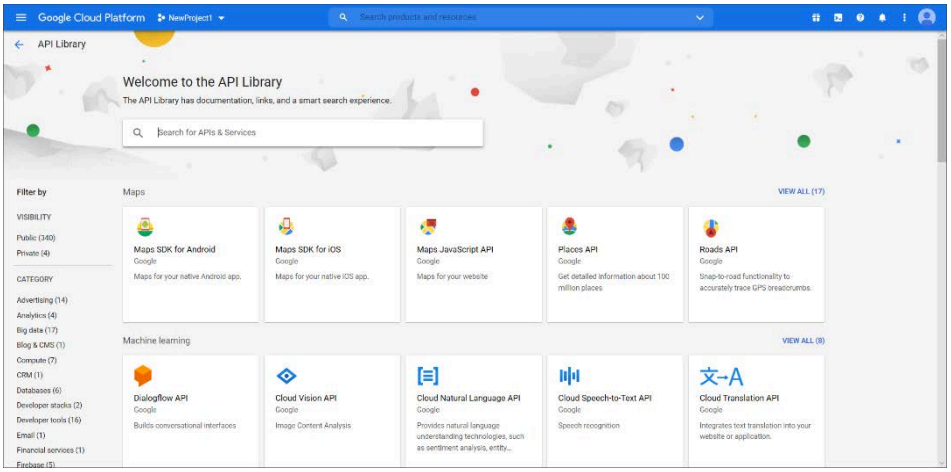
8. Click the **Edit** button, assign a role, and click **Save**.



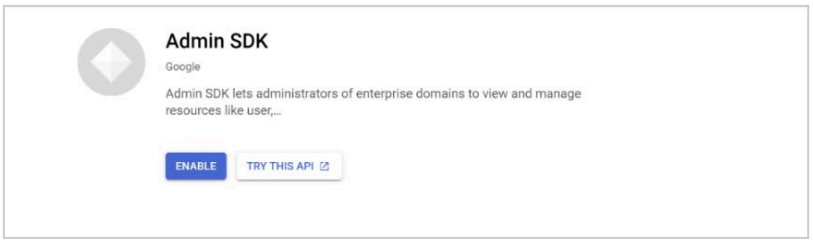
9. Go to https://console.developers.google.com/ and click **ENABLE APIS AND SERVICES**.

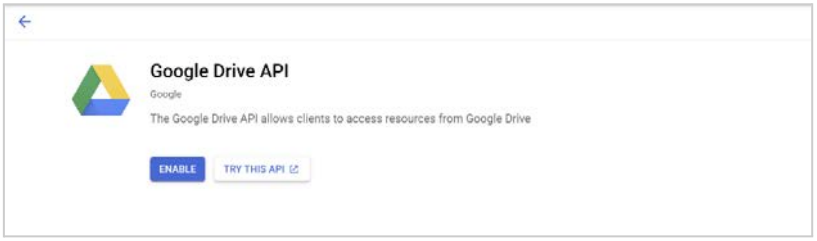


10. **API Library** will be open.



11. Search and enable **Admin SDK** and **Google Drive APIs**.



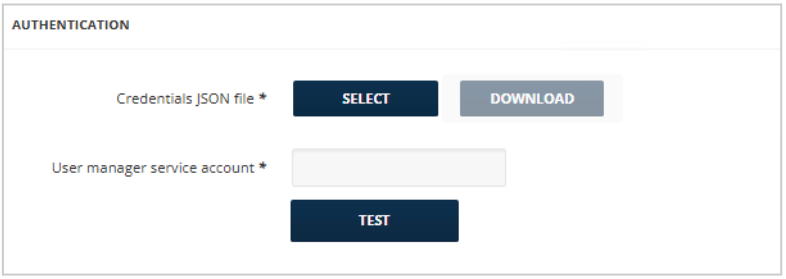


Collector Configuration

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 that the **Download** button is activated when there is a JSON file uploaded.

Time Stamp Formatting

For more details on how to configure timestamps, see **Time Stamp Formatting**.

Advanced Configuration Options

For more details on how to configure advanced configuration options, see **Advanced Configuration Options**.

Next Steps

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

- **MONITORED USERS**
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:

Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**

- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

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 **Merge1 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[14]
- 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

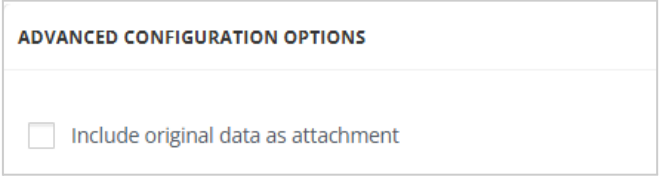
Collector Configuration

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

- **File Source**
- **Execute Script Against Source Files**
- **PGP Decryption**
- **Folders**
- **After Successful Importing**
- **Misc Settings**

Advanced Configuration Options

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



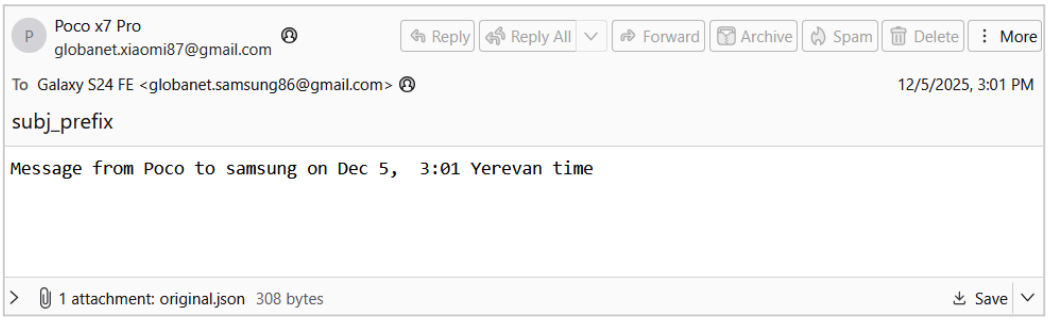
[14] Replies are captured as new messages prefixed with “Parent message”.

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**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Quarantine file**
- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

IceChat

ICE Chat robust 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

- Messages

Captured activities can contain:

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

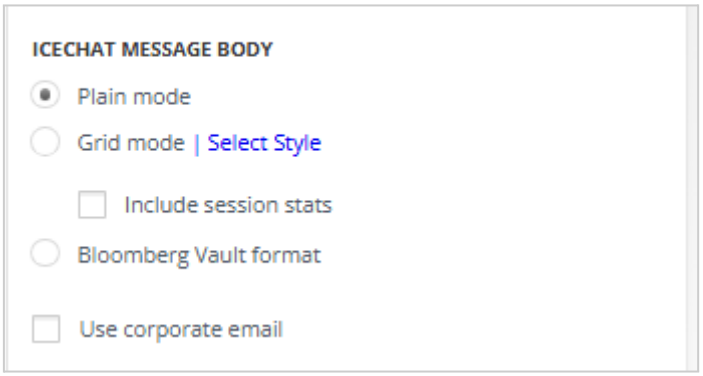
Collector Configuration

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

- **File Source**
- **Execute Script Against Source Files**
- **PGP Decryption**
- **Folders**
- **After Successful Importing**
- **Misc Settings**

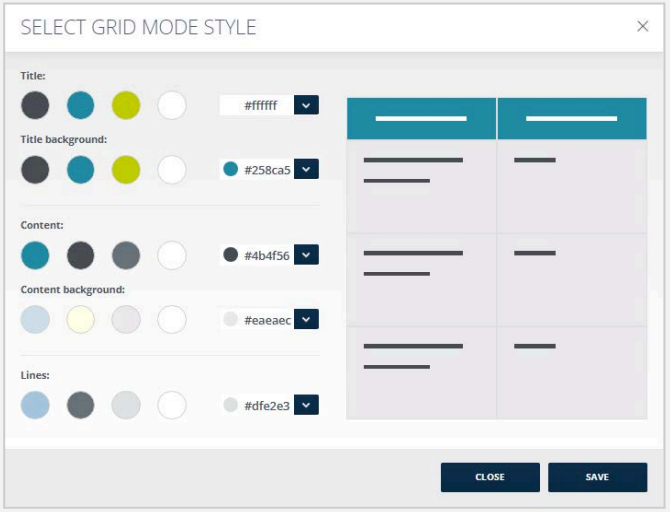
IceChat Message Body

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



- **Plain mode**: Displays the message in a simple text format.
- **Grid mode**: Displays output message content in a compact grid format for structured and efficient viewing. The information is structured into the following columns:
    - *Date*: Shows the date and time the message was sent.

    - *User info*: The user's Full Name (Company Name) <Email Address>.
    - *Content*
    - *Interaction type*: Contains information about participants and messages, such as Participant Entered, Participant Left, Participant Invited, Message, and Attachment.
  - **Include session stats:** If checked, adds *session ID*, *start time*, and *end time* to the message body.
- **Bloomberg Vault format**: Displays imported messages in Bloomberg Vault format.

> **Tip**
>
> In **Grid mode**, the color scheme can be adjusted through the **Select Style** pop-up menu:
>
> 
>

- **Use corporate email**: When checked, the corporate email address is used instead of the login email address for internal users.

Time Stamp Formatting

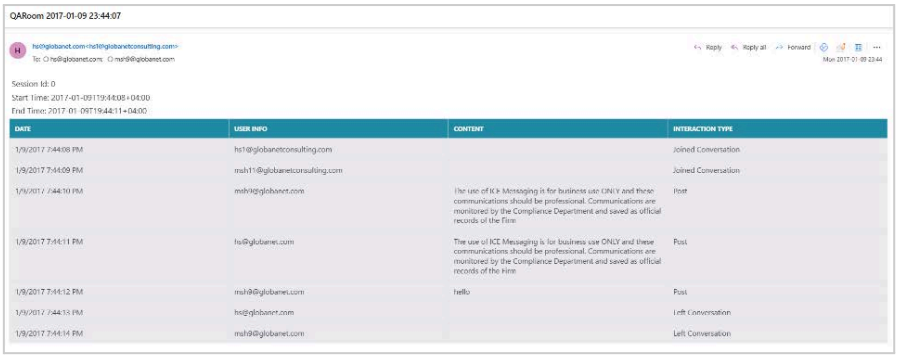
For more details on how to configure timestamps, see **Time Stamp Formatting**.

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**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Quarantine file**
- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

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 **Mergel 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, please proceed with configuring your importer.

Activities Captured

- Text messages (iMessage, SMS)
- Edited messages[15]
- Message replies
- Undo sent messages
- Deleted messages[16]
- Documents (MS Word, MS Excel, PDF, PPT)
- Images
- Videos
- Audio messages (Recordings and voice notes)[17]
- Emojis[18]
- Stickers[18]
- GIFs[18]
- Links
- Apps from Store
- Pinned locations

Collector Configuration

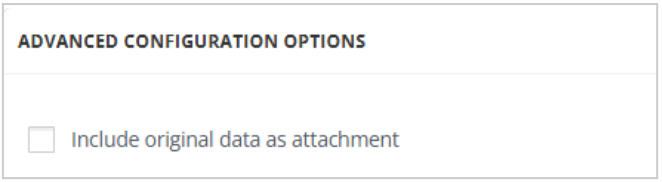
For information on how to configure the following sections of the **Source** tab, see:

- **File Source**
- **Execute Script Against Source Files**
- **PGP Decryption**
- **Folders**
- **After Successful Importing**
- **Misc Settings**

Advanced Configuration Options

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

[15] Edited messages are captured as new messages prefixed with “Edited to”.
[16] Deleted messages are not captured as separate events.
[17] Audio messages with user action “Keep” are captured.
[18] Emojis, stickers, and GIFs are captured as separate messages.

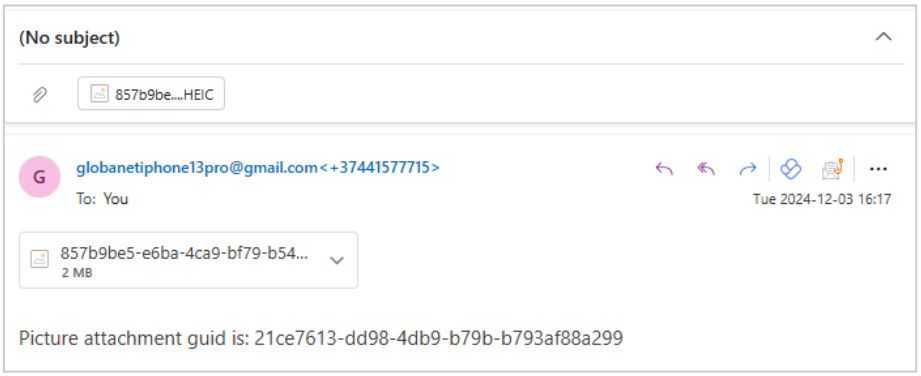


Next Steps

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

- Monitored Users (N/A)
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Quarantine file**
- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

Jabber Enterprise

Cisco Jabber is a suite of Unified Communications applications that allow seamless interaction with your contacts from anywhere. Cisco Jabber offers IM, presence, audio and video calling, voicemail, and conferencing. The applications in the Cisco Jabber family of products are:

- Cisco Jabber for Android
- Cisco Jabber for iOS
- Cisco Jabber for Mac
- Cisco Jabber for Windows.

Merge1 retrieves data from the selected database and processes it[19].

Activities Captured

- Messages between individuals
- Groups chats
- Persistent chats
- File shares[20]

Cisco Jabber database design does not support storing Unicode characters, so messages that include Unicode characters are not stored in the database, hence, cannot be captured by Merge1.

Collector Configuration

Merge1 retrieves data directly from Jabber's database. You can select from the following three types:

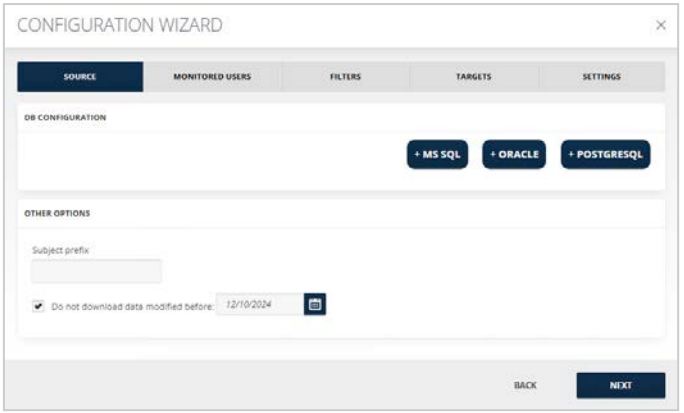
1. **Microsoft SQL Server**
2. **Oracle Database**
3. **PostgreSQL Server**

PostgreSQL Connection

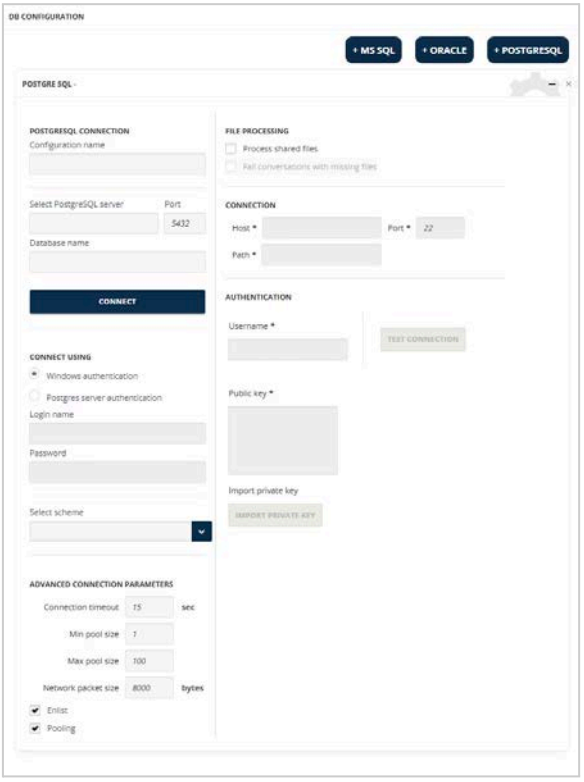
To connect to Jabber enterprise database through PostgreSQL:

1. Select the database that you want to connect by clicking the respective button.

[19] You need to add all databases, from where to retrieve the data. Use the **+** button to add the databases.
[20] This feature is only supported in the environments where the **Managed File Transfer** feature is used in the Cisco Unified Communications Manager IM and Presence Node. For more information see https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/im_presence/configAdminGuide/10_5_2/CUP0_BK_CEB3E82E_00_config-admin-guide-imp-1052/CUP0_BK_CEB3E82E_00_config-admin-guide-imp-1052_chapter_010110.html



2. For PostgreSQL:
   2.1. Enter the **Configuration name**.
   2.2. Select the **PostgreSQL Server**.
   2.3. Enter the **Port** and the **Database name**.



3. Choose the authentication method to connect to the server. If **Windows Authentication** is chosen, Merge1 will connect using the **Windows credentials** of the account. If **Postgres Server Authentication** is chosen, it can be connected to with the **Postgres server credentials**.
4. Enter the Login Name and Password.
5. **Advanced Connection Parameters** allow specifying the following:
   5.1. **Connection timeout** - the time during which the query is not processed can be specified to yield timeout.

5.2. **Min Pool Size** - the minimum number of requests the application may process concurrently.

5.3. **Max Pool Size** - the maximum number of requests the application may process concurrently.

5.4. **Network Packet Size** - the fixed-size chunk of data that transfers requests and results between clients and servers. This field specifies in what file-size chunks the file data should be transferred.

5.5. **Enlist** - when enabled, checks whether the SQL Server connection pooler automatically enlists the connection in the creation thread's current transaction context.

5.6. **Pooling** - if enabled keeps the database connection session active so that when a connection is later requested, one of the active sessions is used in preference to have to create another one.

6. **File Processing** -By activating **Process Shared Files** checkbox, which is disabled by default, you allow the files shared, using Jabber, to be processed by the collector and the fields below become mandatory.

7. **Fail conversations with missing files** - When enabled, conversations that have reference(s) to file(s) in the database but do not exist in the file store will be marked as failed (Stored in Merge1 database), the Merge1 admin then can export the messages or set the reprocessing option by navigating to the REPORTS page of Merge1.

8. **Connection.** Enter the host name of the remote SFTP server that is connected to the CUCM IM and Presence server's MFT service and the folder path in the **Host** and **Path** text boxes, respectively.

9. **Authentication** - To authenticate an SFTP connection, enter the username of the MFT server user and import the private key of the user. You can also generate a new key pair, then add the public key to the authorized_keys file of MFT server user. For more information, regarding SSH key authentication, contact your Jabber and Linux teams.

> **Important**
>
> For MFT records CUCM allows the assignment of a database different than the compliance database, as we do not support this setup. The database used for compliance and MFT must be the same.

Oracle Server

To connect through Oracle:

1. For **Oracle Connection** fields:

1.1. Specify a **Configuration Name**.

1.2. Specify **Oracle Server IP address** and **Port**.

1.3. In the **SID** field, add your Oracle SID, the **Unique name** that uniquely identifies your instance/database. Or choose to add a **Service Name** of the Oracle Database instead.

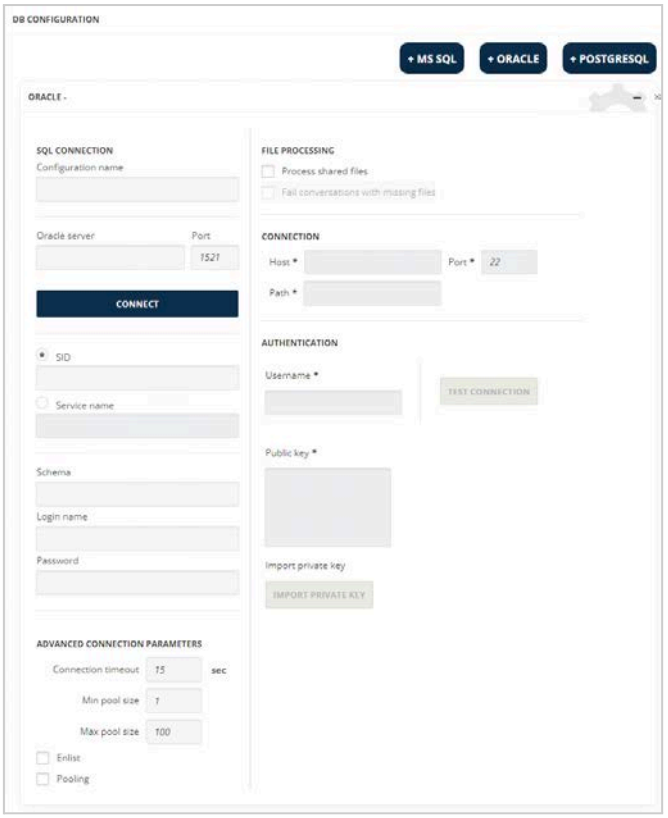
1.4. Add the name of your database schema in the **Schema** field.

1.5. Add the **Login** and **Password**.

2. For **Advanced Connection Parameters**:
    2.1. **Min Pool Size** is the minimum number of requests the application may process concurrently.
    2.2. **Max Pool Size** is the maximum number of requests the application may process concurrently.
    2.3. **Enlist**, when enabled, checks whether the SQL Server connection pooler automatically enlists the connection in the creation thread's current transaction context.
    2.4. **Pooling**, if enabled keeps the database connections active so that when a connection is later requested, one of the active ones is used in preference to have to create another one.
    2.5. In the **Connection Timeout field**, the time during which the query is not processed can be specific to yield timeout.
3. **File Processing** - By activating **Process Shared Files** checkbox, which is disabled by default, you allow the files shared, using Jabber, to be processed by the collector and the fields below become mandatory.
4. **Fail conversations with missing files** - When enabled, conversations that have reference(s) to file(s) in the database but do not exist in the file store will be marked as failed (Stored in Merge1 database), the Merge1 admin then can export the messages or set the reprocessing option by navigating to the Reports page of Merge1.
5. **Connection**. Enter the host name of the remote SFTP server that is connected to the CUCM IM and Presence server's MFT service and the folder path in the Host and Path text boxes, respectively.
6. **Authentication** - To authenticate an SFTP connection, enter the username of the MFT server user and import the private key of the user. You can also generate a new key pair and then add the public key to the authorized_keys file of the MFT server user. For more information, regarding SSH key authentication, please contact your Jabber and Linux teams.

Important

For MFT records, CUCM allows the assignment of a database different than the compliance database, we do not support this setup. The database used for compliance and MFT must be the same.



Microsoft SQL Server

To connect through Microsoft SQL:

1. Select the SQL Server from the drop-down menu.
2. Select the database, where Jabber files are stored, from the drop-down menu after connecting to the server.
3. **Advanced Connection Parameters** allow specifying the following:
    3.1. In the **Connection Timeout** field, the time during which the query is not processed can be specified to yield timeout.
    3.2. In the **Load Balance Timeout** field, the time during which the inactive connections should be kept open in a connection pool can be specified. An inactive connection is a database session that is not in use by an application.
    3.3. **Min Pool Size** - the minimum number of requests the application may process concurrently.
    3.4. **Max Pool Size** - the maximum number of requests the application may process concurrently.
    3.5. **Network Packet Size** - the fixed-size chunk of data that transfers requests and results between clients and servers. This field specifies in what file-size chunks the file data should be transferred.
    3.6. **Asynchronous Processing**, when enabled, allows various workflows to run at the same time.
    3.7. **Enlist** - when enabled, checks whether the SQL Server connection pooler automatically enlists the connection in the creation thread's current transaction context.

3.8. **Pooling** - if enabled keeps the database connection session active so that, when a connection is later requested, one of the active sessions is used in preference to have to create another one.

3.9. **Replication** is a technique through which an instance of a database is exactly copied to, transferred to, or integrated with another location. Database replication is done to provide a consistent copy of data across all the database nodes. It also removes any data redundancy, merging of two databases into one and updating secondary databases with outdated or incomplete data.

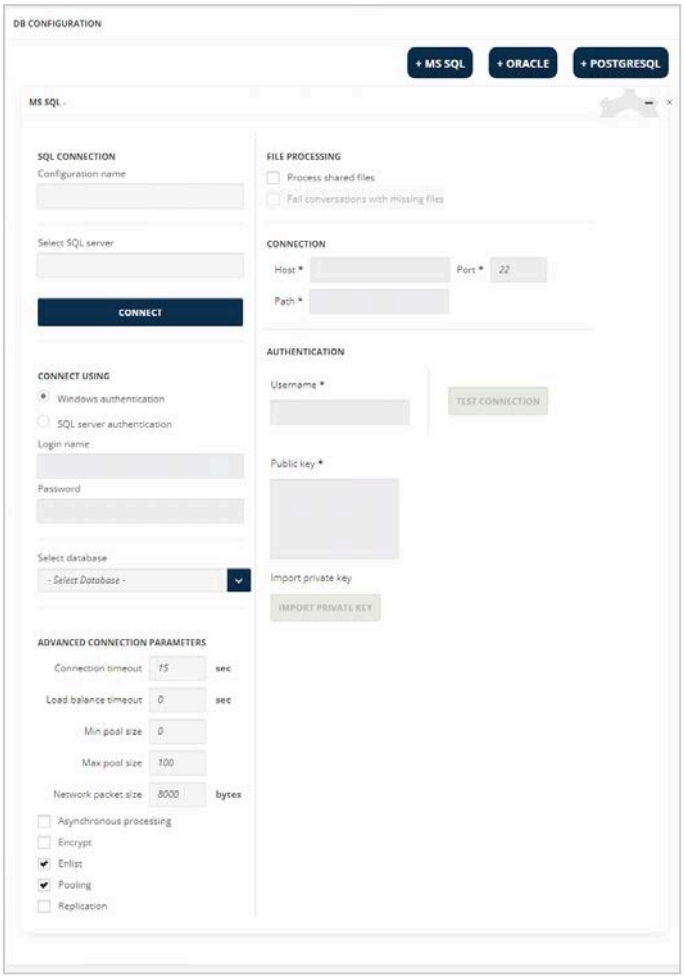
4. **File Processing** - By activating **Process Shared Files** checkbox, which is disabled by default, you allow the files shared, using Jabber, to be processed by the collector and the fields below become mandatory.

5. **Fail conversations with missing files** - When enabled, conversations that have reference(s) to file(s) in the database but do not exist in the file store will be marked as failed (Stored in Mergel database), the Mergel admin then can export the messages or set the reprocessing option by navigating to the REPORTS page of Mergel.

6. **Connection**. Enter the host name of the remote SFTP server that is connected to the CUCM IM and Presence server's MFT service and the folder path in the Host and Path text boxes, respectively.

Authentication - To authenticate an SFTP connection, enter the username of the MFT server user and import the private key of the user. You can also generate a new key pair then add the public key to the authorized_keys file of MFT server user. For more information, regarding SSH key authentication, please contact your Jabber and Linux teams.

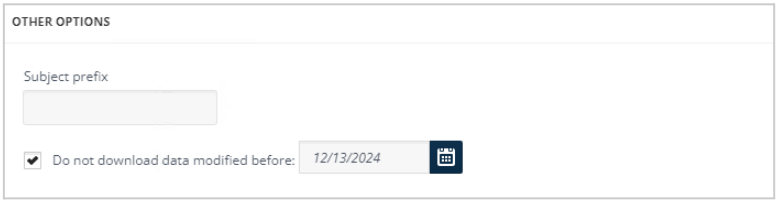
> **Important**
>
> For MFT records CUCM allows the assignment of a database different than the compliance database, we do not support this setup. The database used for compliance and MFT must be the same.



Other Options

For **Other Options**:

- The **Subject Prefix** feature will add a prefix before the message subject to facilitate the search in the target.
- The **Do not download data modified before** check will ensure that old or irrelevant data is excluded. For example, if the date selected is 8/1/2024, it will not retrieve any data modified before August 1 of 2024. Only the data after 8/1/2024 will be retrieved, archived, and imported.

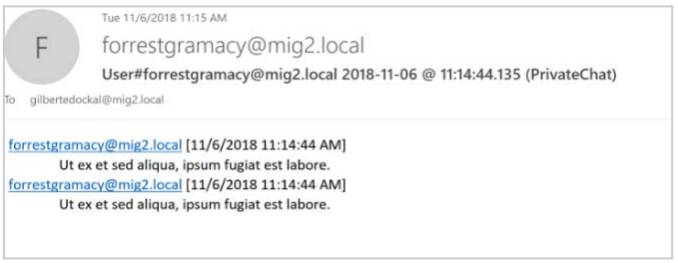


Next Steps

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

- **MONITORED USERS**
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

JSON

JSON collector allows our customers to rapidly transform JSON files using the JSON default template provided by Merge1. Once JSON is transformed, Merge1 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 activities can contain:

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

Collector Configuration

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

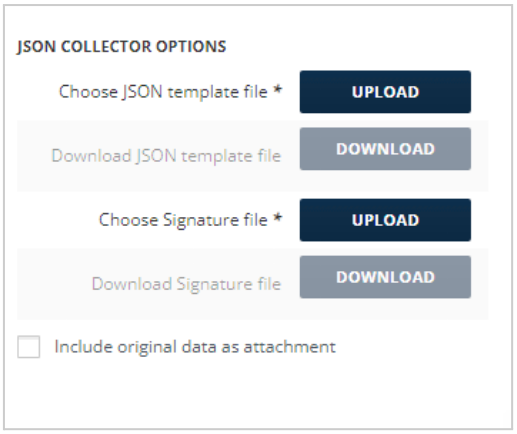
- **File Source**
- **Execute Script Against Source Files**
- **PGP Decryption**
- **Folders**
- **After Successful Importing**
- **Misc Settings**

JSON Collector Options

To configure the section:

1. Upload the JSON template.[21]
2. Upload the Signature file.
3. Enable **Include original data as attachment** in case you want to include original data as an attachment in the output message.

[21] Templates must be reviewed and cryptographically signed by Arctera.

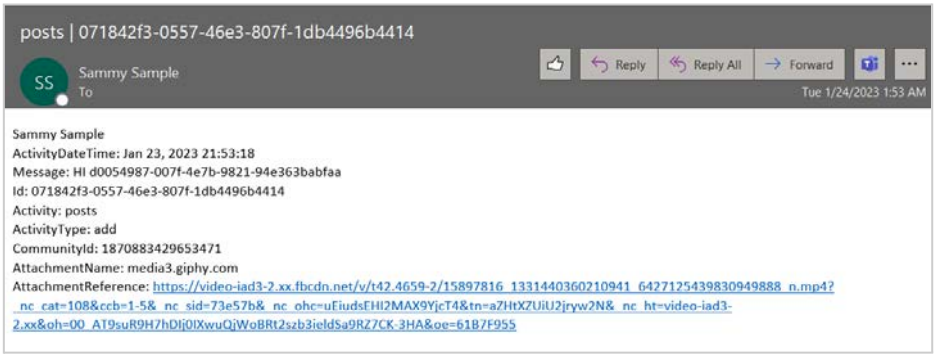


Next Steps

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

- Monitored Users (N/A)
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Quarantine file**
- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**

- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

LSEG (Refinitiv)

LSEG (Refinitiv) brings users the latest news from around the world, covering breaking news in markets, business, politics, entertainment, technology, and video. The Merge1 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 Arctera Support for more details on the mapping corresponding to the source you will use for the 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`.
- The quarantine sources column on the Dashboard shows the number of files moved to the quarantine folder while processing source files with the below-listed configured formats. All other files were initially considered unwanted and moved to the quarantine folder.

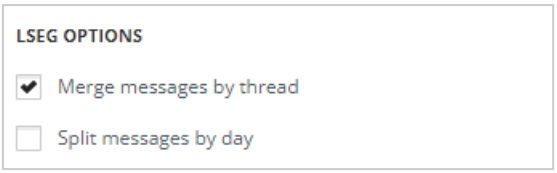
Collector Configuration

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

- **File Source**
- **Execute Script Against Source Files**
- **PGP Decryption**
- **Folders**
- **After Successful Importing**
- **Misc Settings**

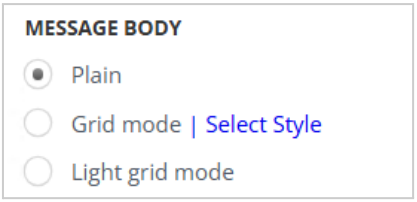
LSEG Options

The option **Split messages 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

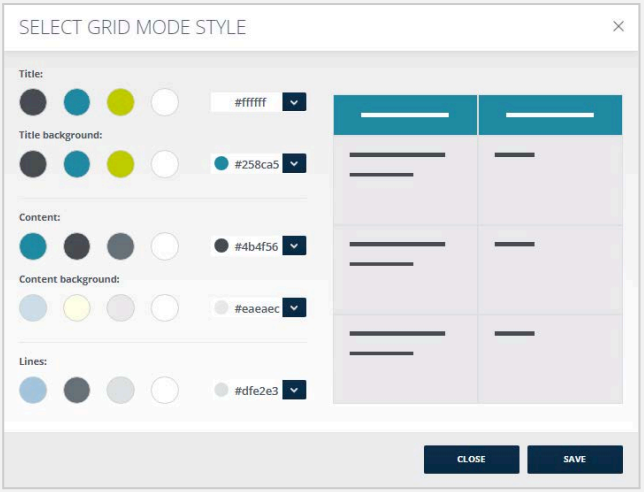
This setting determines how imported messages are displayed in the target. There are the following output message body options:



- **Plain**: Displays the message in a simple text format.
- **Grid mode**: Displays information in the following structured columns:
  - *UTC time stamp*: Includes the date of the sent message.
  - *User info*
  - *Content*
  - *Event type*: Specifies the nature of the activity (e.g., joining the chat, sending a message, etc.).
  - *Message ID*
  - *Attachment*
- **Light grid mode**: Displays data in a two-toned layout, making it visually distinct and easier to view while displaying limited metadata.

Tip

In **Grid mode**, the color scheme can be adjusted through the **Select Style** pop-up menu:



Time Stamp Formatting

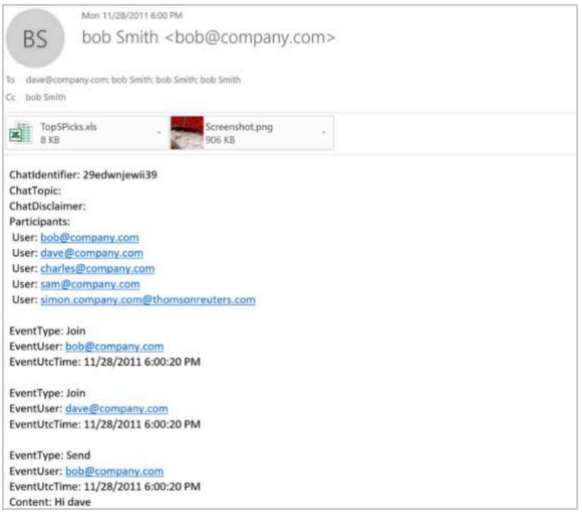
For more details on how to configure timestamps, see **Time Stamp Formatting**.

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**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Quarantine file**
- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

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 **Mergel 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

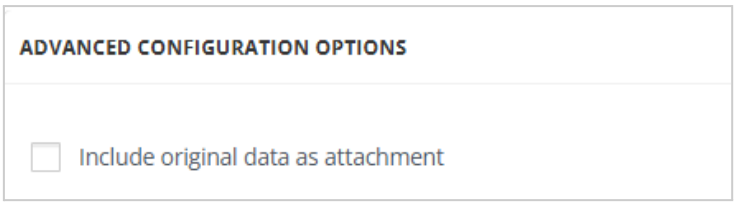
Collector Configuration

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

- **File Source**
- **Execute Script Against Source Files**
- **PGP Decryption**
- **Folders**
- **After Successful Importing**
- **Misc Settings**

Advanced Configuration Options

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

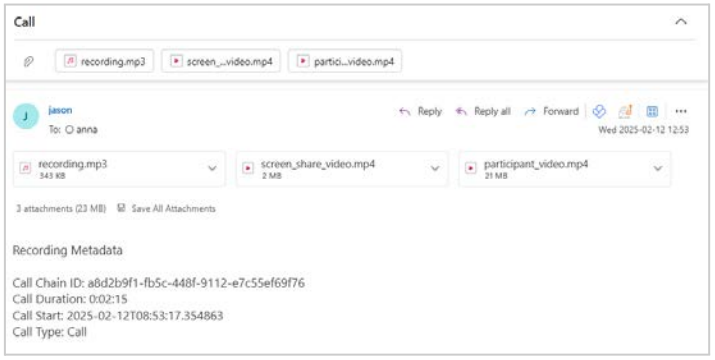


Next Steps

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

- Monitored Users (N/A)
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Quarantine file**
- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

Microsoft Teams via Export API

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 including broad support for compliance standards, and eDiscovery and legal hold for channels, chats, and files. Microsoft Teams always encrypts data, at-rest, and in-transit, and includes multi-factor authentication to enhance identity protection.

Activities Captured

- Chat messages
  - Create
  - Edit[22]
  - Delete
- Channel messages[23]
  - Create
  - Edit[22] [24]
  - Delete

Captured activities can contain:

- Chat/channel info
- Attachments[25] [26]
- Modern attachments
- Loop components[27]
- Video clips
- Voice messages
- Reactions[28]
- Praises
- Approvals
- Mentions
- System-generated events (members added/removed/joined/left)

Important

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.

---

[22] If the **Capture retained messages (edits)** checkbox is enabled, all versions of edited messages will be captured.

[23] The team owner should be included in the monitored users list to capture data from shared channels.

[24] Only the latest version of the message is captured for Private Channels due to an API limitation.

[25] It is recommended to run/capture the required data before deleting teams and/or channels.

[26] 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.

[27] Only the initial version of a Loop component is captured; subsequent edits are not captured due to API limitations.

[28] Reactions of already captured messages are not captured.

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 Graph API limitations, when this feature is enabled, the chat messages of guests, external, and deleted users are not captured. To use this feature all users in the tenant should be monitored and have the E5 licenses.

Note

Due to the API issues, we have the following limitations[29]:

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

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.

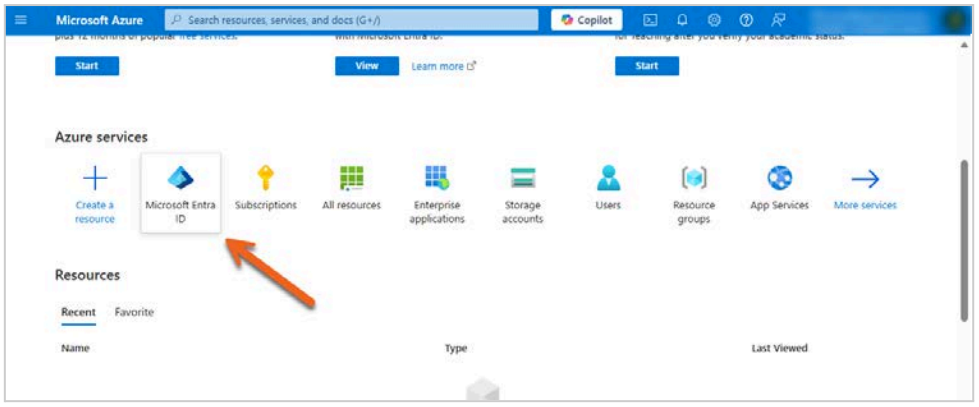
Creating a Microsoft Entra ID Application

The Office 365 or Azure administrator in your organization must complete the steps detailed in the sections below.

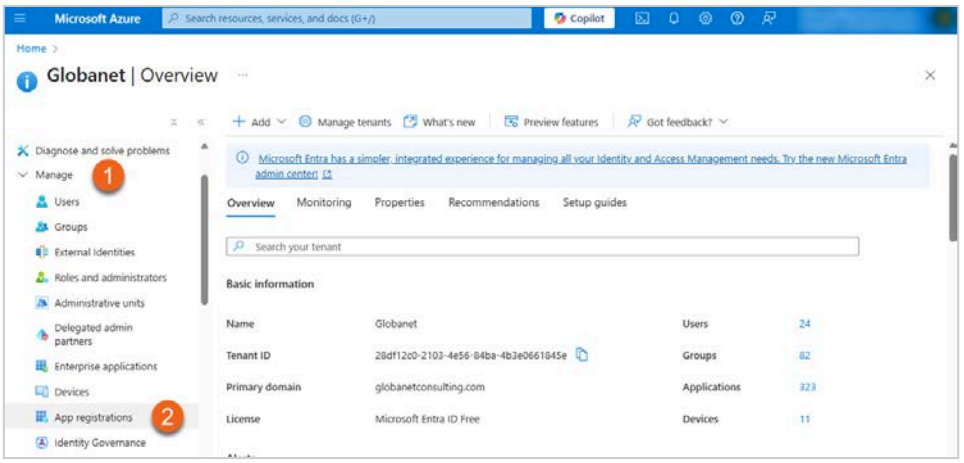
Registering an Application

1. Sign in to **Azure Portal**.
2. Select **Microsoft Entra ID** under **Azure services**.

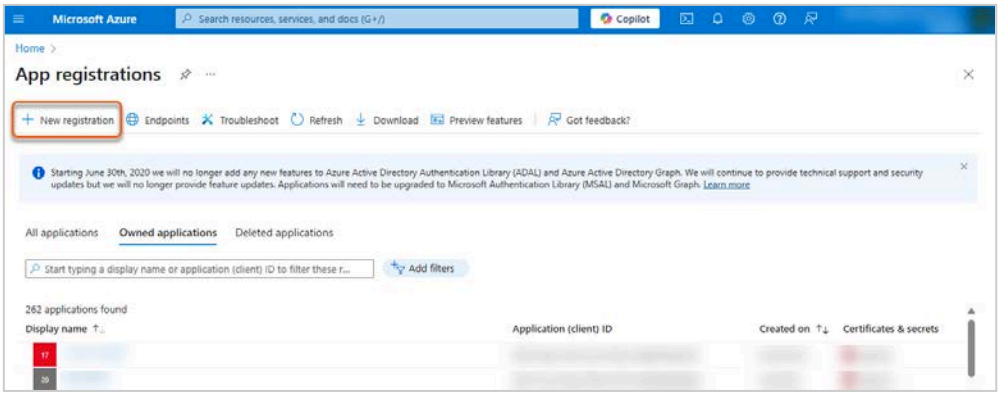
[29] The first case has been reported to Microsoft and may be resolved at a later time.



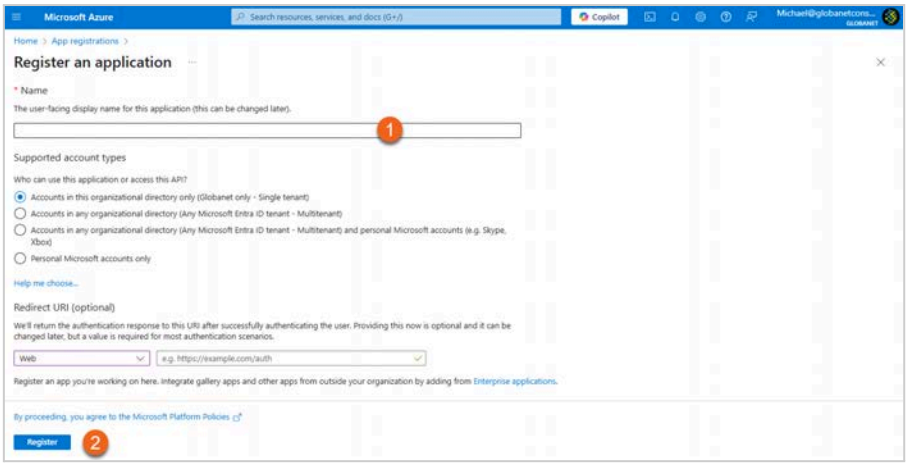
3. In the left-hand navigation pane, click **Manage > App registrations**.



4. Click **New registration**.



5. To register an application:
   5.1. Enter a **Name** for the application.
   5.2. Click **Register**.



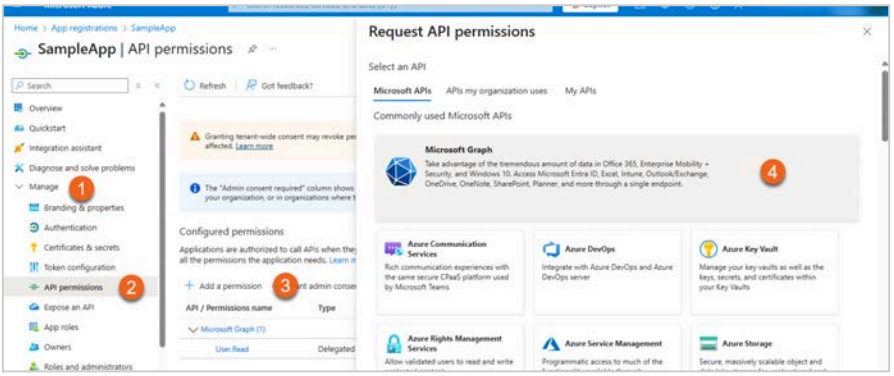
6. An **Application (client) ID** and **Directory (tenant) ID** will be generated. Keep both for configuring the collector in Merge1.

Granting Permissions

Adding Microsoft Graph API Permissions

To add **Microsoft Graph** API permissions:

1. In the left-hand navigation pane, click **Manage > API permissions**.
2. Click **Add a permission**.
3. In the opened pane select the **Microsoft Graph** API.



4. To add the necessary permissions:
    4.1. Click **Application permissions**.
    4.2. Add the following permissions:
        4.2.1. **Channel:** *ChannelBasic.All*
        4.2.2. **ChannelMember:** *ChannelMember.Read.All*
        4.2.3. **ChannelMessage:** *ChannelMessage.Read.All*
        4.2.4. **Chat:**
            4.2.4.1. Chat.Read.All

4.2.4.2. *Chat.ReadBasic.All*

4.2.5. **ChatMember:** *ChatMember.Read.All*

4.2.6. **ChatMessage:** *ChatMessage.Read.All*

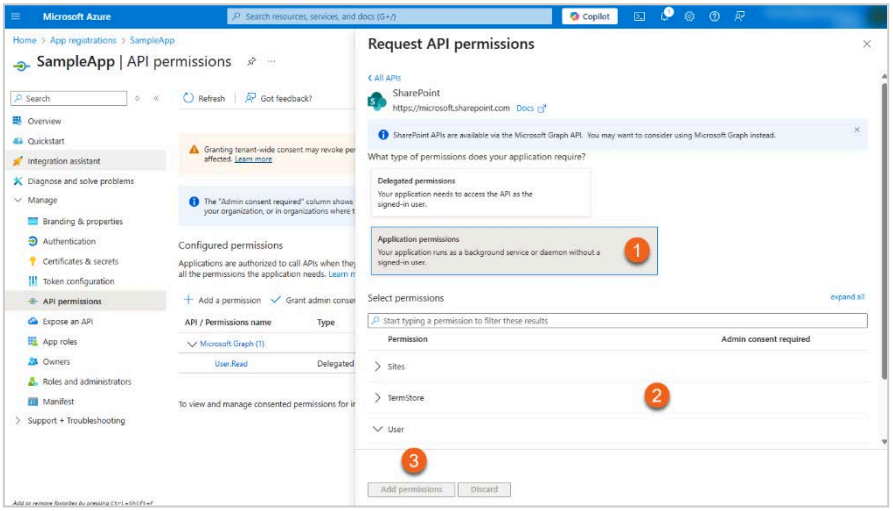
4.2.7. **Files:** *Files.Read.All*

4.2.8. **Group:** *Group.Read.All*

4.2.9. **Team**: *Team.ReadBasic.All*

4.2.10. **User:** *User.Read.All*

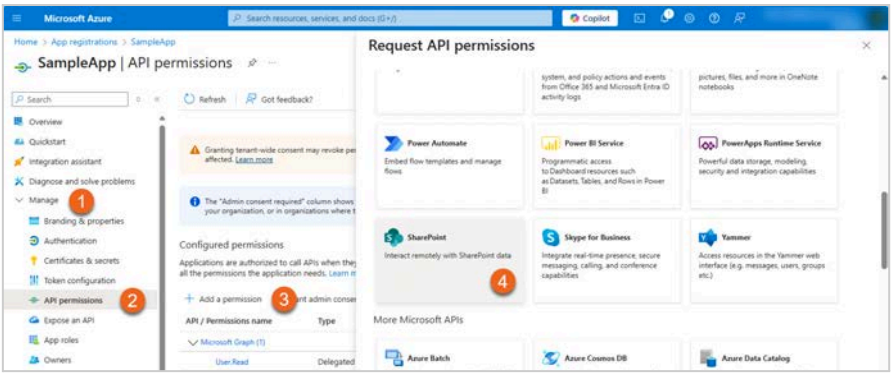
4.3. Click **Add permissions**.



Adding SharePoint API Permissions

To add **SharePoint** API permissions:

1. In the left-hand navigation pane, click **Manage > API permissions**.
2. Click **Add a permission**.
3. In the opened pane select the **SharePoint** API.



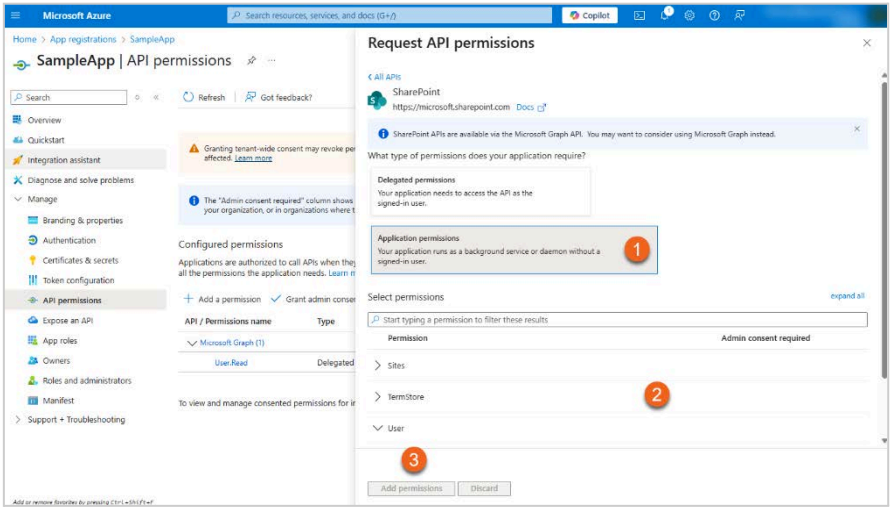
4. To add the necessary permissions:
   a. Click **Application permissions**.
   b. Add the following permissions:

i. **Sites:** *Sites.Read.All*

ii. **TermStore:** *TermStore.Read.All*

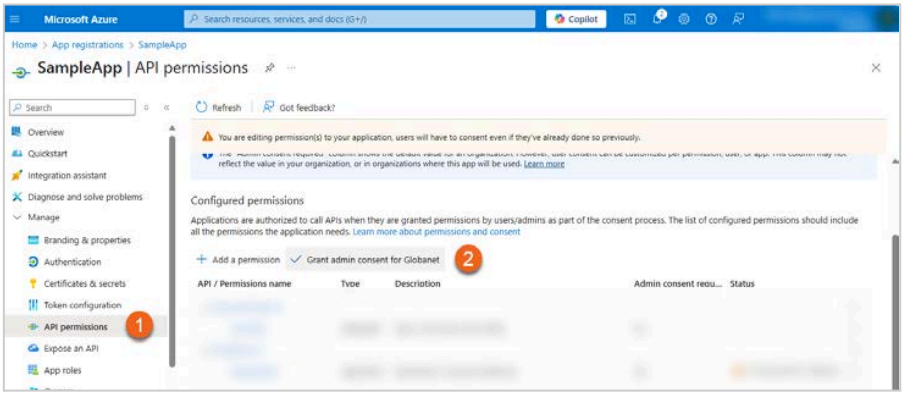
iii. **User:** *User.Read.All*

c. Click **Add permissions**.



Granting Admin Consent

1. Go back to **API permissions**.
2. Click **Grant admin consent** for your company to grant the added 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

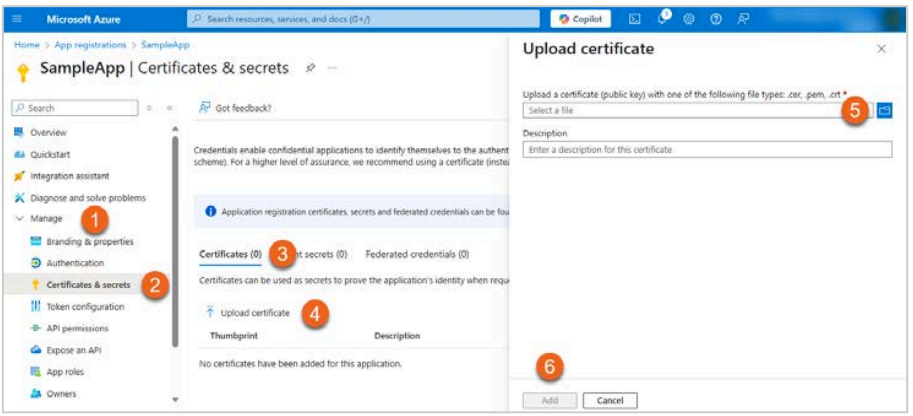
Note: The E5 IPG (Information Protection Governance) license can be added on E3 licenses.

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.

Uploading a Certificate

To upload a certificate:

1. In the left-hand navigation pane, go to **Manage > Certificates & secrets**.
2. Select **Certificates**.
3. Click **Upload certificate**.
4. Select a certificate (public key) with one of the following file types: `.cer`, `.pem`, `.crt`.
5. Click **Add**.



A certificate **thumbprint** will be generated. Keep the value for configuring the collector in Merge1.

For more information on how to create a certificate, see **Creating a Certificate (Private and Public Keys)**.

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. (GCC tenants are currently exempt from these requirements.)

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

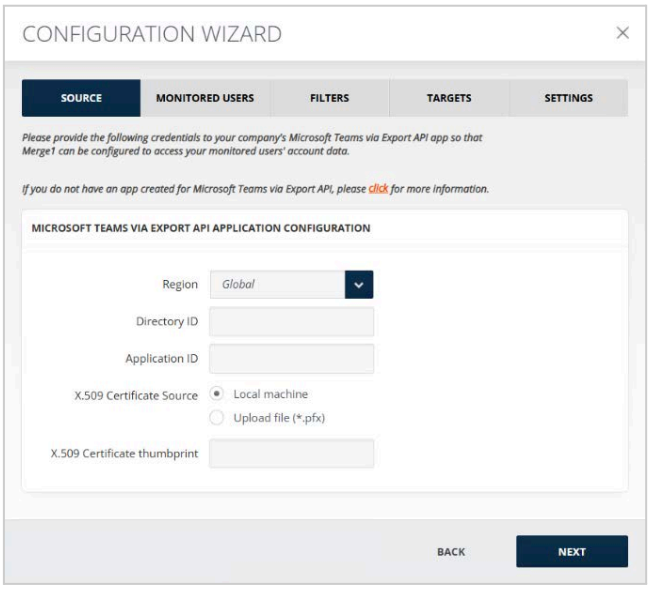
Collector Configuration

After filling in the **Name** and **Description** on the **Add Importer** window and selecting the **Source** on Configuration Wizard:

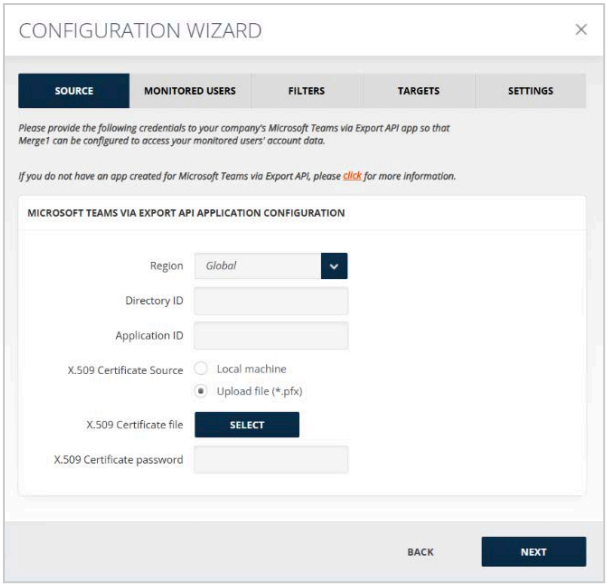
- Select **Global** from the **Region** drop-down list to process data worldwide or **China** to process data specifically from the China region.

> **Important**
>
> The collector is not supported for US Government L4 or US Government L5 (DOD) cloud deployments.

- Add Directory ID and Application ID.
- Provide **X.509 Certificate Thumbprint** in case you activate the **Local machine** radio button as the X.509 Certificate source.



- In case you activate **Upload file (*.pfx)**, click the **Select** button to upload the certificate and provide **X.509 Certificate password**.

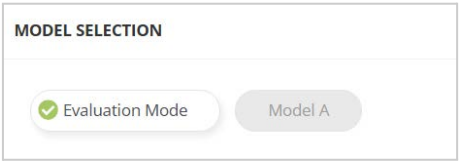


The **Certificate thumbprint** field will be auto populated in case the collector was previously configured by uploading a certificate.

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

You can specify the activities to be captured by the collector.

- Enable **All areas** to capture data from chats and channels.

- Enable **Certain areas** in case either **Chats** or **Channels**[30] data needs to be collected.

Threading and Formatting

For Threading and Formatting:

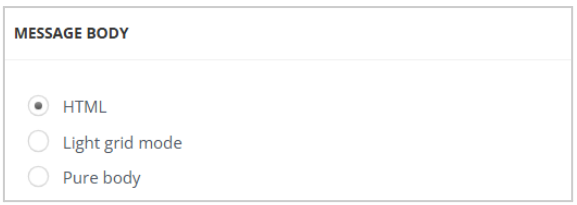
- If **No threading** is activated, a single message is generated for a message in the Chats and Channels.
- If **Per conversation** is enabled and **Contextual collection of channels** is disabled, messages that were created before the last capture date and edited/deleted after that, are captured separately, i.e., the already captured messages from the post are not included in the output message.
- If both **Per conversation** and **Contextual collection of channels** are enabled, messages that were created before the last capture date and edited/deleted after that, are captured with their post messages in the same output message.
  Note that for chats we have the same output message with both **Contextual collection of channels** enabled and disabled as this feature relates only to channels.
- If **Per room** is enabled and **Contextual collection of channels** is disabled, messages created before the last capture date and edited/deleted after that are captured separately; i.e., the already captured messages in the post are not included in the output message.
- If both **Per room** and **Contextual collection of channels** are enabled, messages created before the last capture date and edited/deleted after that are captured with their post messages in the same output message.
- Select the **Message time zone** from the drop-down list.
- When the **Process incomplete day** option is enabled, the messages of the incomplete day will be imported in a separate email.
  Note that when the **Process incomplete day** checkbox is enabled, the **Message time zone** drop-down list is disabled.

Message Body

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.
- **Light grid mode**: Displays data in a two-toned layout, making it visually distinct and easier to view while displaying limited metadata.
- **Pure body**: Displays the output message as plain text, without formatting or additional details.

[30] The shared channels' membership type is printed in the output message as "UnknownFutureValue" due to an API limitation.



When the font family **Segoe UI** is used in the output message (HTML tags) and **Bold** and *Italic* formatting styles are applied to headings (e.g., Heading 1, Heading 2, Heading 3, etc.), Outlook does not recognize the Segoe UI font. However, HTML online editors respect it.

Additionally, when the `Monospaced` formatting style is applied, neither the HTML editor nor Outlook respects the specified font family.

Time Stamp Formatting

For more details on how to configure timestamps, see **Time Stamp Formatting**.

> **Note**
>
> The message tracking (and cut-off date filtering) itself is being done by **LastModifiedTime** or **OriginalDateTime** property (determined by the "Import Based On" setting of the collector) of the message, as it is the most accurate way to ensure that no data (including edits) is missing, however, the timestamp that is being printed in the headers of the message is the message creation timestamp that we are retrieving from the ConversationXML (which becomes available only after filtering, thus, it cannot be used before the message is retrieved). That timestamp is communicated by the source vendor (Microsoft) as the only accurate timestamp.

Advanced Configuration Options

There are the following advanced options when configuring the collector with Mergel.

- **Subject prefix:** Adds a prefix before the message subject to facilitate the search in the target.
- **Do not download data modified before / after:** Filters data by excluding items modified outside the specified date range. For example, if "before" is set to 08/17/2024 and "after" is set to 09/17/2024, only data within those dates will be downloaded.

  > **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.

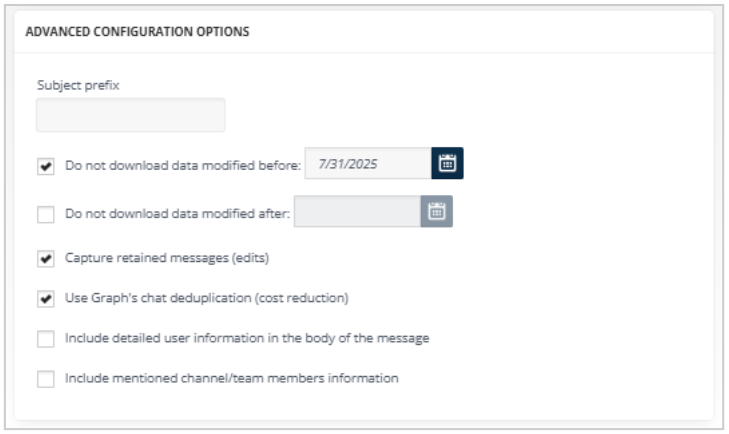
- **Capture retained messages (edits):** When enabled, collects all versions of edited messages.

Note

Before enabling this feature, review your retention policies and refer to Microsoft documentation to ensure it is supported in your environment.

Enabling this feature may result in additional Microsoft Graph API usage costs.

- **Use Graph's chat deduplication (cost reduction):** When enabled, captures only sent messages from monitored users.
- **Include detailed user information in the body of the message:** When enabled, queries Entra ID using the user principal name, and adds the display name and email address from the **Microsoft Entra ID**.
- **Include mentioned channel/team members information** When enabled, retrieves information of the mentioned members in channels/teams by enabling/disabling the corresponding checkbox.



Attachments Configuration

- **Include original data as attachment**: If checked, the message original data is attached to the output file.
- **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.[31]

- For **Captured Modern Attachments**, by selecting:

[31] In case *Ignore attachments* is checked and the user sends a message in a chat with attachments and then replies to it, the parent message will not be rendered to the reply in the output message.

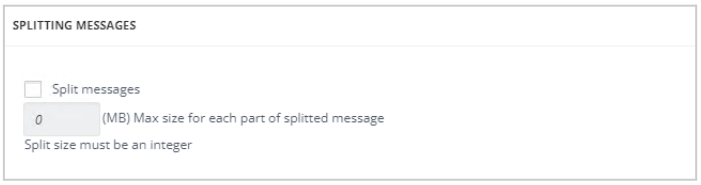
- **Latest version** - the latest saved version of the shared document available at collector runtime will be captured with the message.
- **Shared version** - the saved version of the document at the time of sharing in Microsoft Teams will be captured with the message.

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

For more details on how to configure attachments, see **Attachments Configuration**.

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 maximum size for each part of the split message is set to 25MB, and the original message is 65 MB, it will be split into 3 messages, each not exceeding 25MB.

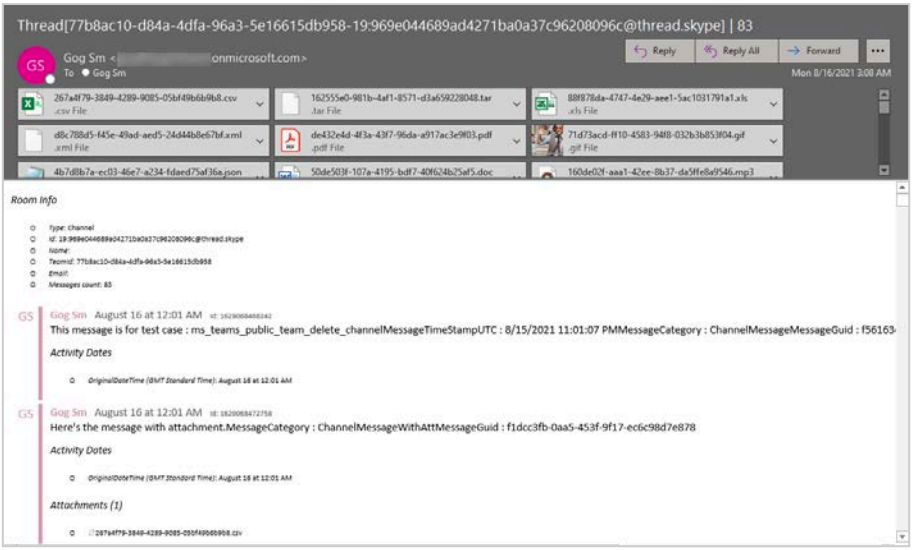


Next Steps

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

- **MONITORED USERS**
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Monitored users skipped**
- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

Microsoft Teams via Webhooks

Microsoft Teams Webhooks provides a real-time data exchange mechanism, allowing applications to receive immediate updates when events occur. Unlike traditional pull APIs, Webhooks push data to subscribed endpoints, enabling efficient, near-instant integration.

The **Merge1 Microsoft Teams via Webhooks collector** captures Teams event data via Webhooks, facilitating archiving, compliance, and secure communication management. This model requires organizations to configure subscriber endpoints to process incoming data, ensuring seamless integration into enterprise systems.

Activities Captured

- Chat messages
  - Create
  - Edit
  - Delete
- Channel messages
  - Create
  - Edit
  - Delete

Captured activities can contain:

- Chat/Channel info
- Attachments
- Modern attachments
- Archived attachments in OneDrive or SharePoint (deleted posts)
- Video clips
- Voice messages
- Reactions
- Praises
- Approvals
- Mentions
- System-generated events (call started/ended, members added/deleted/joined/left)

Warning

For users who need to use the Merge1 Microsoft Teams via Webhooks importer for reactive (targeted) discovery:

- Items are available for reactive discovery in the Webhooks portal according to the retention period set when configuring the subscription in the Working in the Globanet Portal.
- The maximum amount of time is 90 days.
- When running a targeted discovery search, please allow an end-date greater than the message date to accommodate for latency in delivery of items to the portal by Microsoft. Even though Webhooks technology is usually instantaneous, Microsoft Support has confirmed

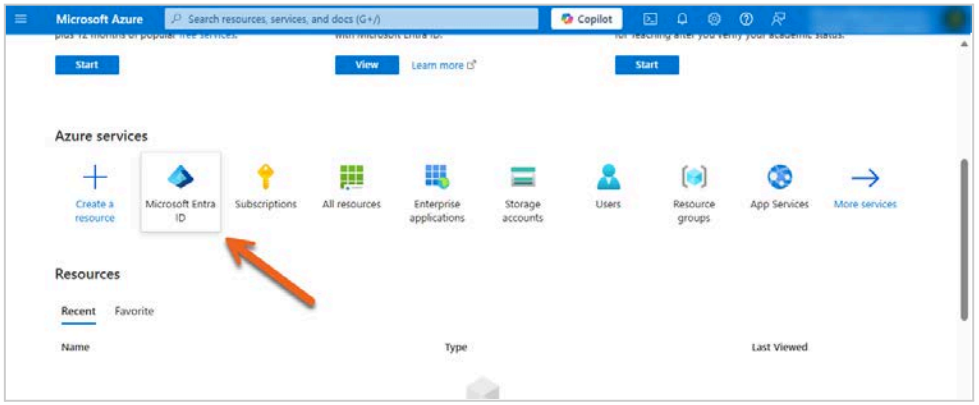
that there are sometimes delays in data processing which affects their webhooks delivery. Allowing for a larger period for cut-off, ensures that data is not missed during discovery.

Creating a Microsoft Entra ID Application

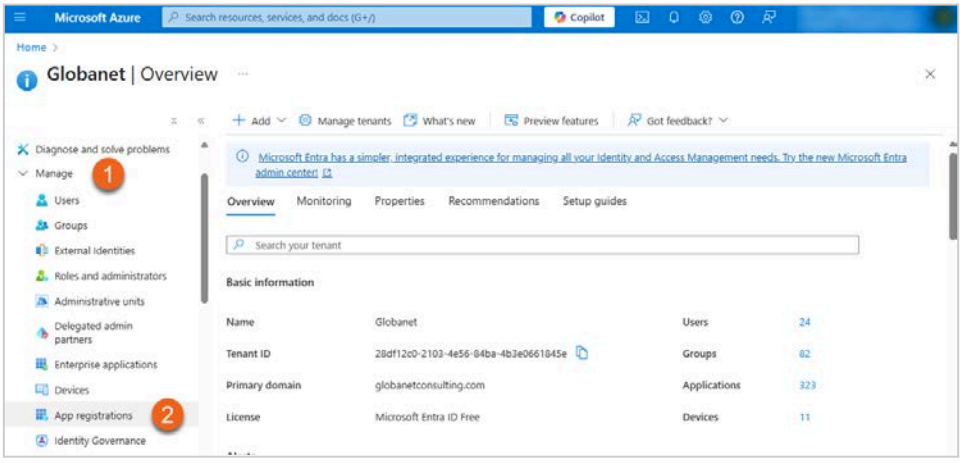
The Office 365 or Azure administrator in your organization must complete the steps detailed in the sections below.

Registering an Application

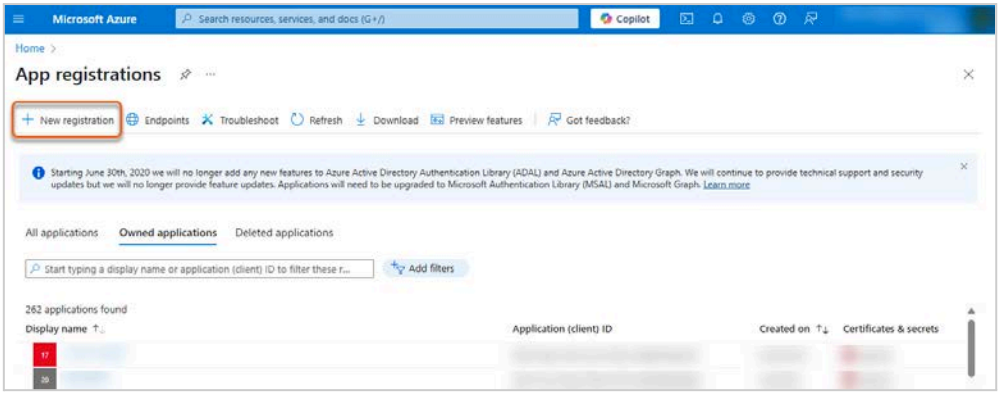
1. Sign in to Azure Portal.
2. Select **Microsoft Entra ID** under **Azure services**.



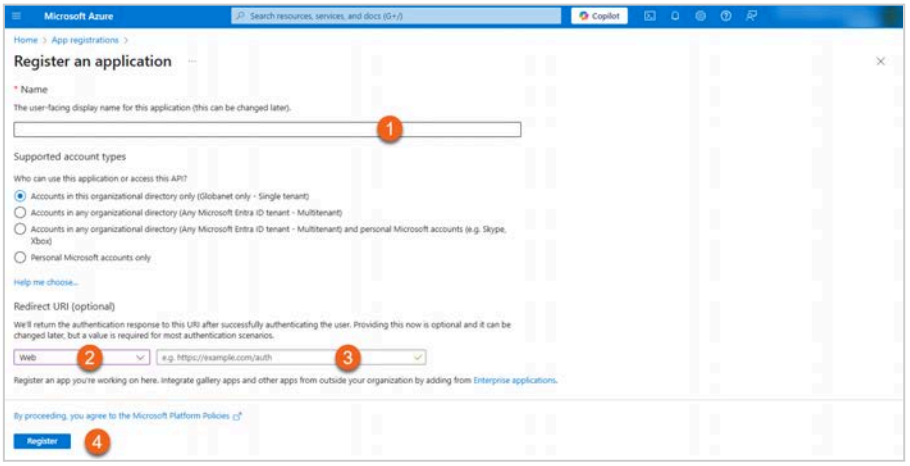
3. In the left-hand navigation pane, click **Manage > App registrations**.



4. Click **New registration**.



5. To register an application:
   5.1. Enter a **Name** for the application.
   5.2. Select **Web** under **Redirect URI (optional)**.
   5.3. Add the URL of your local Merge1 environment in the following format: `https://<merge1_instance>/Configuration/OAuthCallback`.
   5.4. Click **Register**.



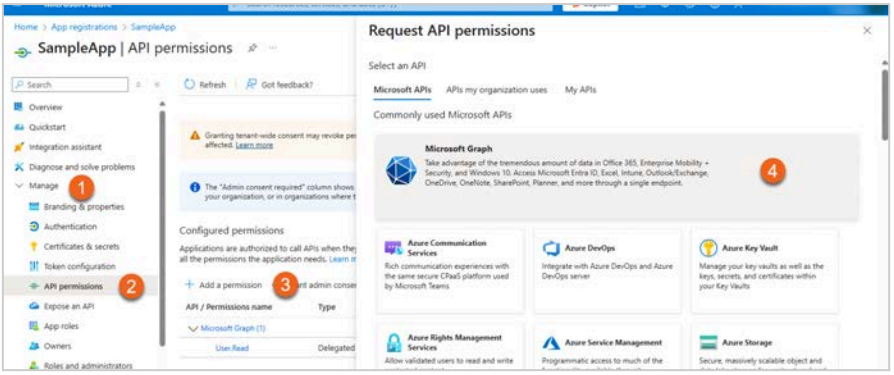
6. An **Application (client) ID** and **Directory (tenant) ID** will be generated. Keep both for configuring the collector in Merge1.

Granting Permissions

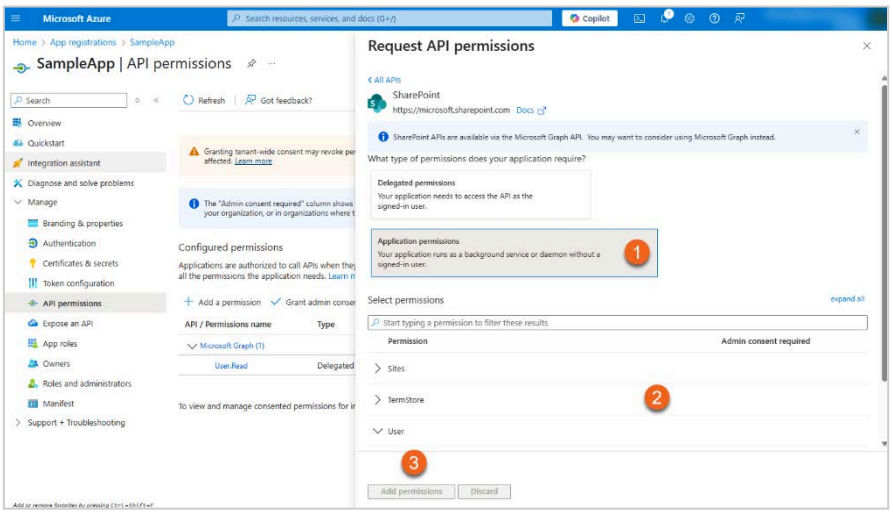
Adding Microsoft Graph API Permissions

To add **Microsoft Graph** API permissions:

1. In the left-hand navigation pane, click **Manage > API permissions**.
2. Click **Add a permission**.
3. In the opened pane select the **Microsoft Graph** API.



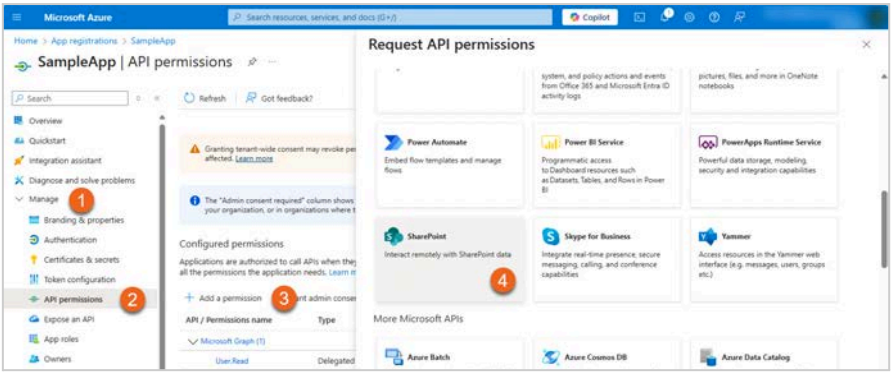
4. To add the necessary permissions:
   4.1. Click **Application permissions**.
   4.2. Add the following permissions:
      4.2.1. **ChannelMember:** *ChannelMember.Read.All*
      4.2.2. **ChannelMessage:** *ChannelMessage.Read.All*
      4.2.3. **Chat:** *Chat.Read.All*
      4.2.4. **ChatMember**: *ChatMember.Read.All*
      4.2.5. **Group:** *Group.Read.All*
      4.2.6. **User:** *User.Read.All*
   4.3. Click **Add permissions**.



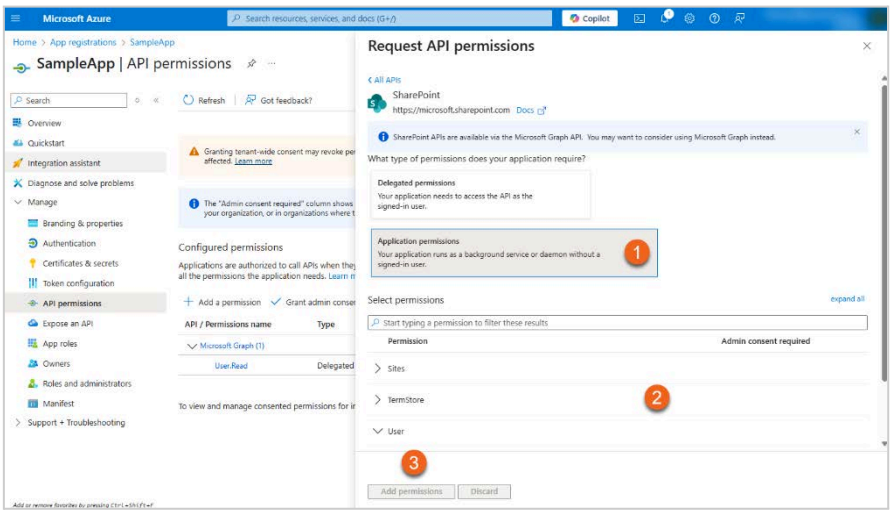
Adding SharePoint API Permissions

To add **SharePoint** API permissions:

1. In the left-hand navigation pane, click **Manage > API permissions**.
2. Click **Add a permission**.
3. In the opened pane select the **SharePoint** API.

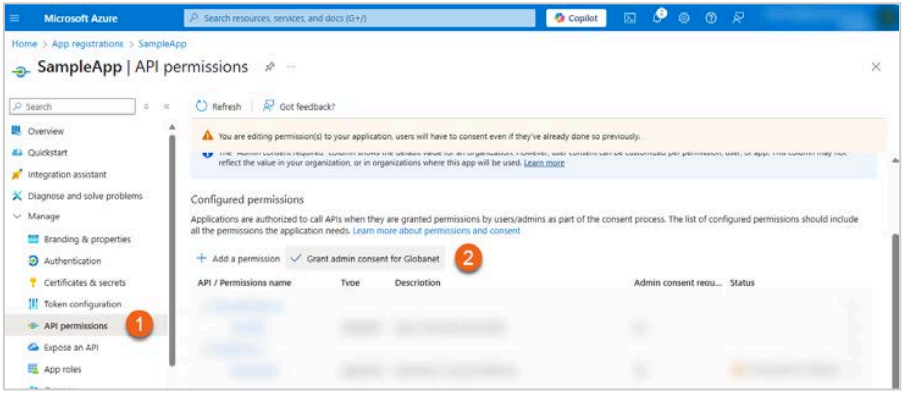


4. To add the necessary permissions:
   4.1. Click **Application permissions**.
   4.2. Add the following permission:
      4.2.1. **Sites:** *Sites.Read.All*
   4.3. Click **Add permissions**.



Granting Admin Consent

1. Go back to **API permissions**.
2. Click **Grant admin consent** for your company to grant the added permissions.



License Info

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

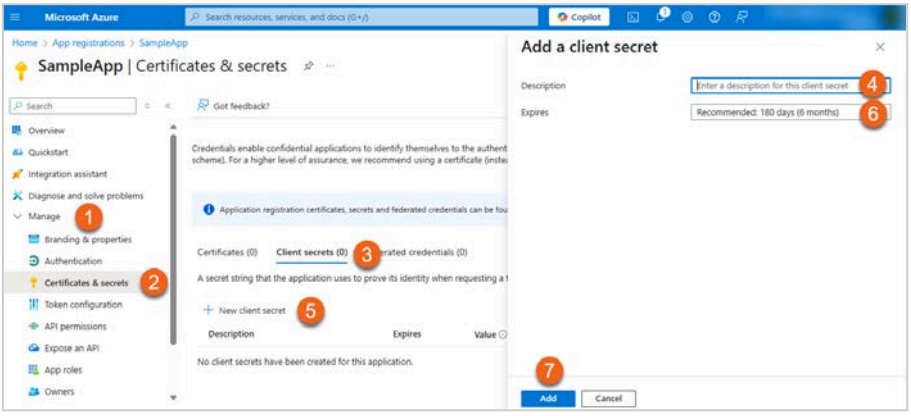
- Microsoft 365 E5/A5/G5
- Microsoft 365 E5/A5/G5 Compliance
- Microsoft 365 E5/A5/G5/F5 Security
- Microsoft 365 E5/A5/G5 Information Protection and Governance

All participants in the conversation should have the required Microsoft 365 licenses to ensure complete data collection. For additional information about Teams API Pricing and licensing models, see Licensing and payment requirements - Microsoft Graph | Microsoft Docs.

Adding a Client Secret

To add a new client secret:

1. In the left-hand navigation pane, go to **Manage > Certificates & secrets**.
2. Go to **Client secrets**.
3. Click **New client secret**.
4. Enter a **Description**.
5. Specify a **Duration**.
6. Click **Add**.



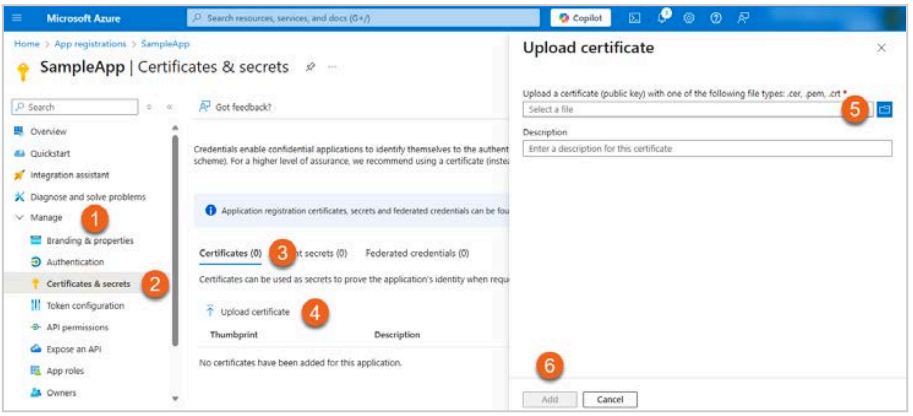
Keep the new client secret value for configuring the collector in Merge1.

Uploading a Certificate

To upload a certificate:

1. In the left-hand navigation pane, go to **Manage > Certificates & secrets**.
2. Select **Certificates**.
3. Click **Upload certificate**.

4. Select a certificate (public key) with one of the following file types: `.cer`, `.pem`, `.crt`.
5. Click **Add**.



A certificate **thumbprint** will be generated. Keep the value for configuring the collector in Merge1.

For more information on how to create a certificate, see **Creating a Certificate (Private and Public Keys)**.

Managing Encryption Keys

To create a Webhooks Platform subscription, you will need to generate an asymmetric key pair and upload the public key to the Webhooks website during subscription creation.

Note that this public key will be sent to Microsoft Graph during subscription creation and the key will be used to encrypt the data before it is sent to Arctera cloud infrastructure, i.e., only Private Key holders will be able to decrypt the notifications sent by Microsoft Graph. Arctera does not have access to the private key.

For managing Encryption keys:

1. Obtain a certificate with a pair of asymmetric keys:
    1.1. You can self-sign the certificate, since Microsoft Graph does not verify the certificate issuer, and uses the public key for only encryption
    1.2. The key must be of type `RSA`
    1.3. The key size must be between 2048 and 4096 bits.
2. Export the certificate in base64-encoded X.509 format and upload it to the Arctera Webhooks site during subscription creation.
3. Export the private key and install it on the Merge1 server that will be used to capture data gathered by the Webhooks Platform.

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. (GCC tenants are currently exempt from these requirements.)

Applications without an active Azure subscription will get an error "HTTP 402 Payment required" when accessing the metered APIs using model=A. Applications using Evaluation Mode will also get an 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.

Please note that even 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.

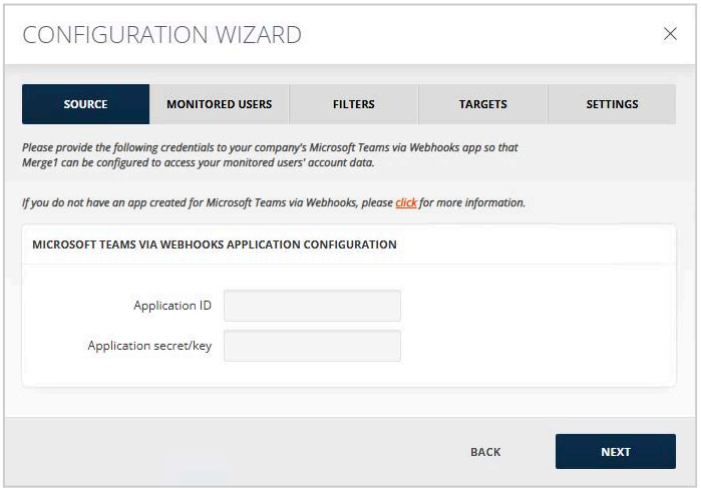
Working in the Globanet Portal

Contact Arctera Support to get access to the Globanet Portal. For more information on how to manage Globanet Portal Applications and subscriptions, see *Working in the Globanet Portal* document listed in the **References**.

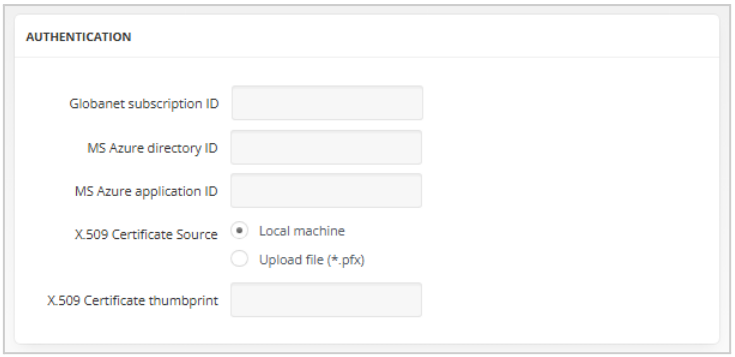
Collector Configuration

After filling in the **Name** and **Description** on the **Add Importer** window and selecting the Source on Configuration Wizard:

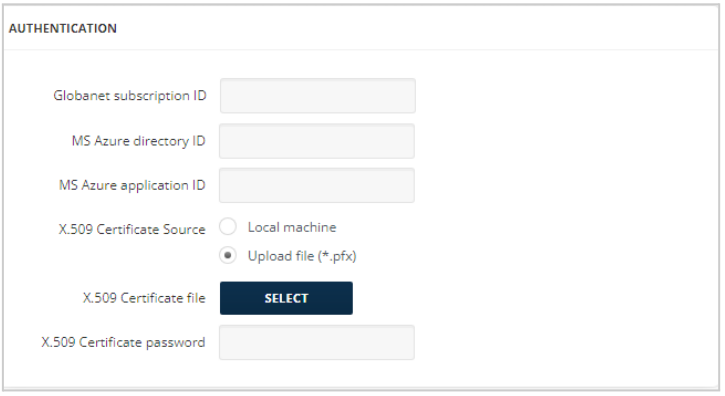
1. Enter the **Client ID** and **Client Secret** (See **Working in the Globanet Portal**), in the **Application ID** and **Application secret/key** fields correspondingly and click **NEXT**.



2. Enter the **Subscription ID** (See **Working in the Globanet Portal**), **MS Azure Directory ID**, and **MS Azure Application ID** in the **Authentication** section.
3. Provide **X.509 Certificate Thumbprint** in case you activate the **Local machine** radio button as the X.509 Certificate source.



4. In case you activate **Upload file (*.pfx)**, click the **Select** button to upload the certificate and provide **X.509 Certificate password**.



The **Certificate thumbprint** field will be auto populated in case the collector was previously configured by uploading a certificate.

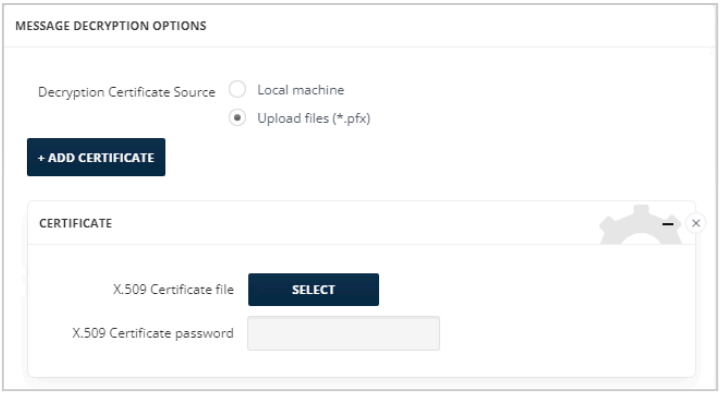
Message Decryption Options

Microsoft Graph does not verify the certificate issuer and uses the public key for only encryption. To receive the notifications decrypted, enable one of the following options:

- Local machine (default) - the collector gets decryption certificates from the local machine.
- Upload files (*.pfx)

For **Upload certificates *(.pfx)**:

1. Enable **Upload certificates *(.pfx)**.
2. Click **ADD CERTIFICATE**.
3. Select the **X.509 Certificate file**.
4. Provide the **X.509 Certificate password**.



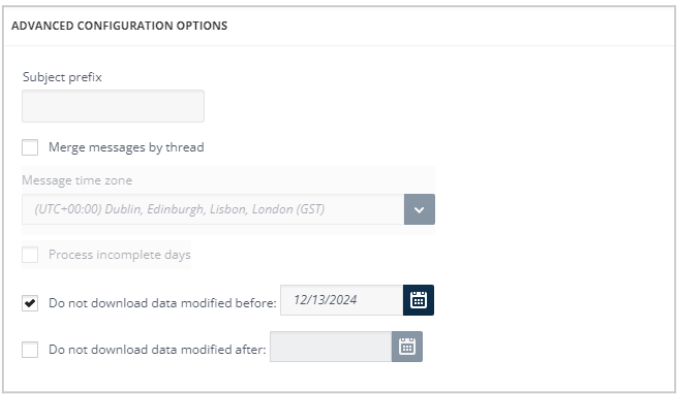
Time Stamp Formatting

For more details on how to configure timestamps, see **Time Stamp Formatting**.

Advanced Configuration Options

There are the following advanced options when configuring the collector with Mergel:

- 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** by which the messages 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 as well. 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 08/17/2024 and the *after date* is set to 09/17/2024, only the data between these two dates will be downloaded. Data outside that timeframe will be ignored.



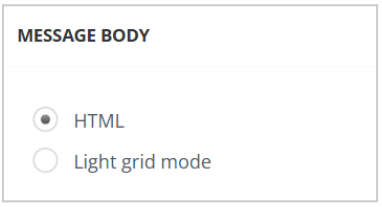
Attachments Configuration

For more details on how to configure attachments, see **Attachments Configuration**.

Message Body

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.
- **Light grid mode**: Displays data in a two-toned layout, making it visually distinct and easier to view while displaying limited metadata.

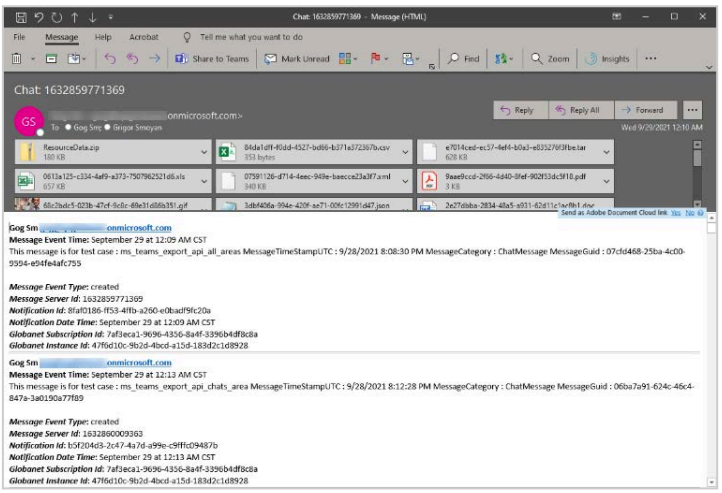


Next Steps

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

- **MONITORED USERS**
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

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

- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

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 activities can contain:

- Participants: From, To
- Call start time (as a timestamp)
- Call duration
- Audio attachment files in MP3 format

Collector Configuration

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

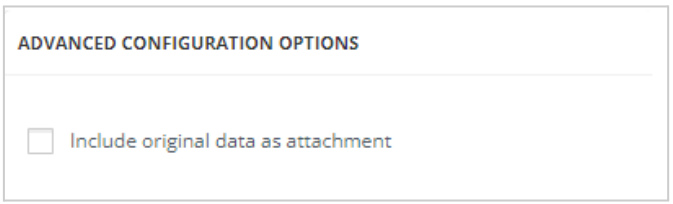
- **File Source**
- **Execute Script Against Source Files**
- **PGP Decryption**
- **Folders**
- **After Successful Importing**
- **Misc Settings**

Note

- 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 the 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, then the XML file will be attached to the output message.

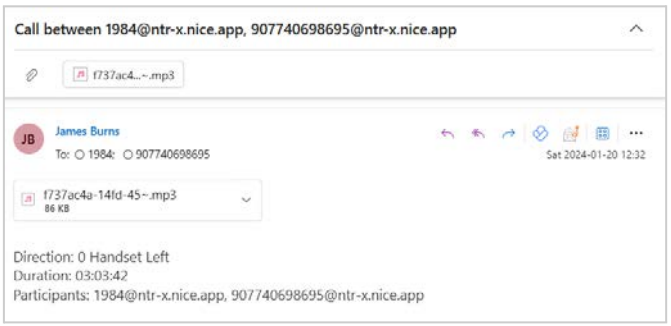


Next Steps

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

- Monitored Users (N/A)
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Quarantine file**
- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

OneDrive for Business

OneDrive is a file-hosting service operated by Microsoft as part of its suite of online services. The OneDrive collector 's 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 Mergel email file. The metadata includes document creator (author in the Mergel 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[32] [33] [34]
- New created documents via browser with the file

Note

- Microsoft OneNote files (where users' notes, drawings, screen clippings, and audio commentaries are gathered) are captured.
- If there are multiple activities performed in the same file, only the most recent one will be recorded.

Creating a Microsoft Entra ID Application

The Office 365 or Azure administrator in your organization must complete the steps detailed in the sections below.

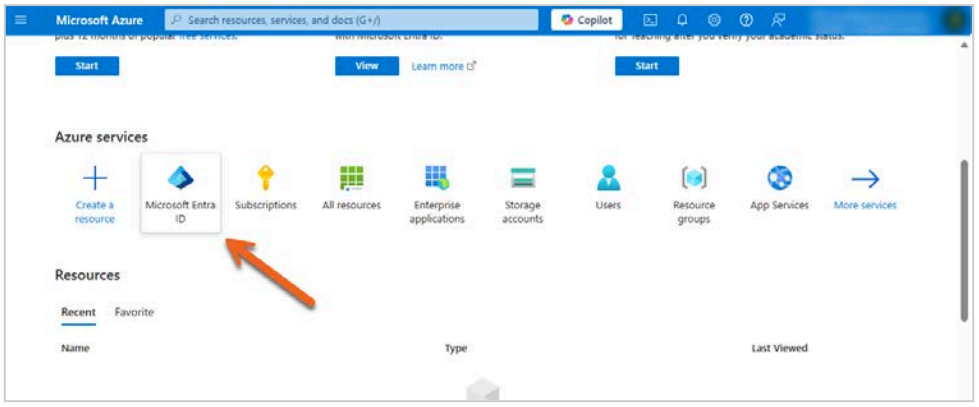
Registering an Application

1. Sign in to **Azure Portal**.
2. Select **Microsoft Entra ID** under **Azure services**.

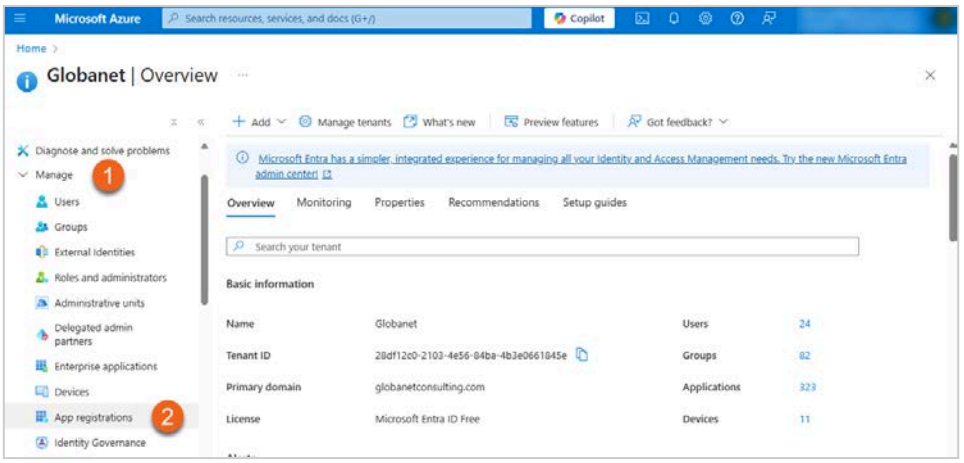
[32] Delete events are not captured during the first run as the Microsoft API does not provide history data.

[33] Hard deleted items, i.e., items deleted from Recycle bin, are not captured.

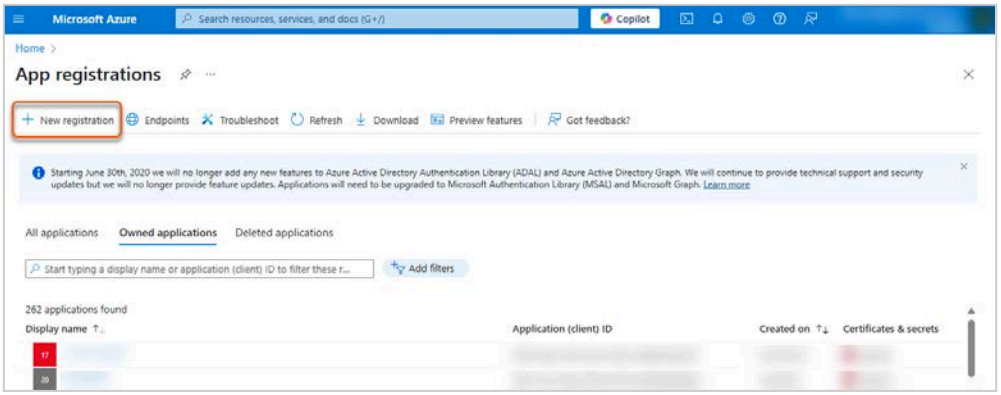
[34] Delete events are not recorded, and thus are not captured immediately after the deletion.



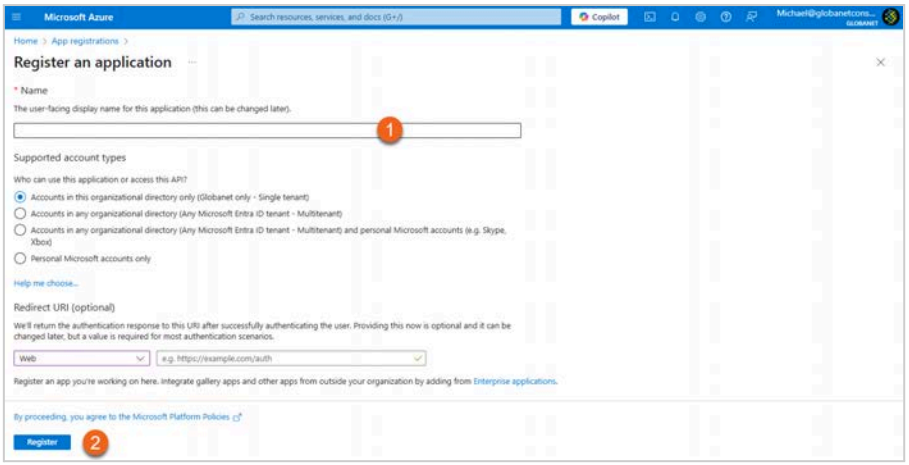
3. In the left-hand navigation pane, click **Manage > App registrations**.



4. Click **New registration**.



5. To register an application:
   5.1. Enter a **Name** for the application.
   5.2. Click **Register**.



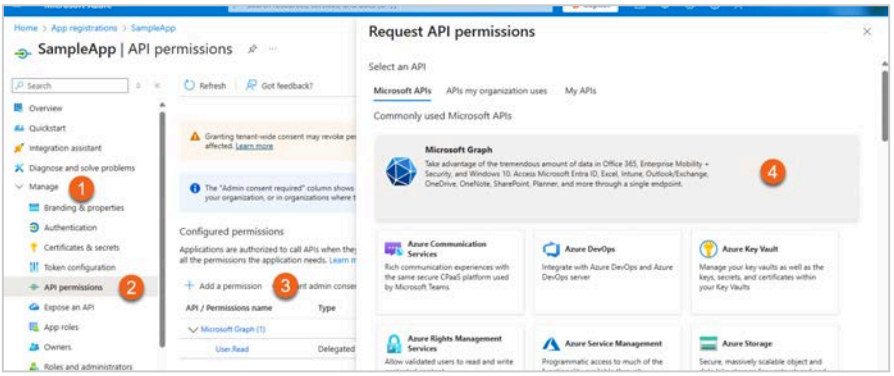
6. An **Application (client) ID** and **Directory (tenant) ID** will be generated. Keep both for configuring the collector in Merge1.

Granting Permissions

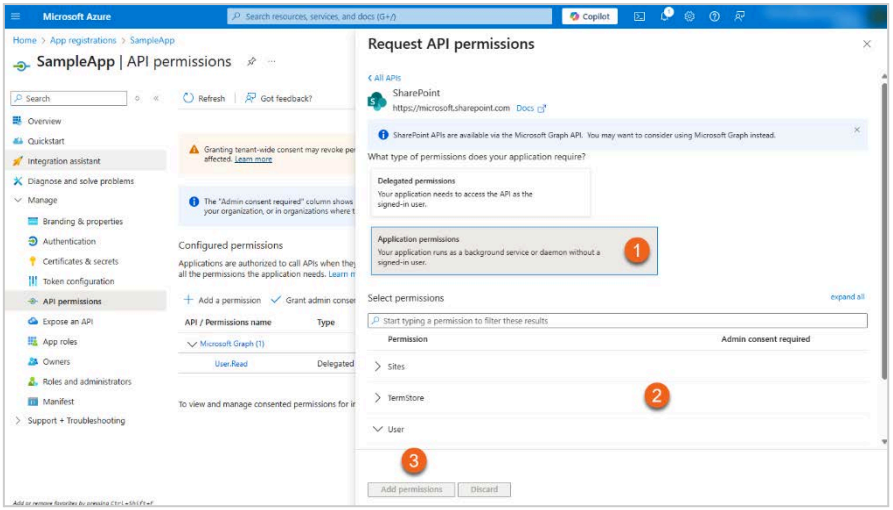
Adding Microsoft Graph API Permissions

To add **Microsoft Graph** API permissions:

1. In the left-hand navigation pane, click **Manage > API permissions**.
2. Click **Add a permission**.
3. In the opened pane select the **Microsoft Graph** API.



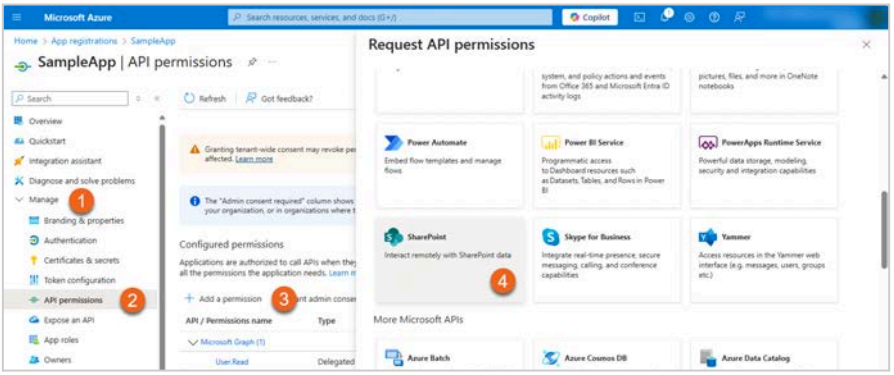
4. To add the necessary permission:
   4.1. Click **Application permissions**.
   4.2. Add the following permissions:
      4.2.1. Directory: *Directory.Read.All*
      4.2.2. Files: *Files.Read.All*
      4.2.3. **User:** *User.Read.All*
   4.3. Click **Add permissions**.



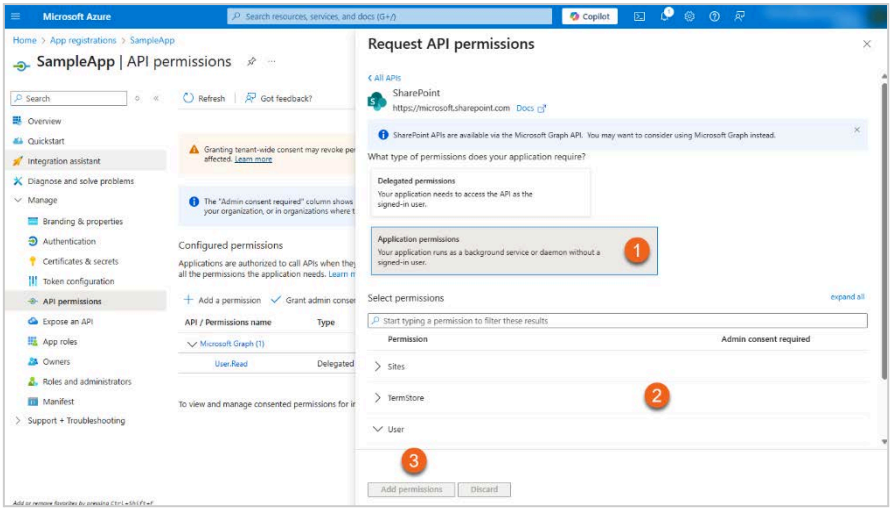
Adding SharePoint API Permissions

To add **SharePoint** API permissions:

1. In the left-hand navigation pane, click **Manage > API permissions**.
2. Click **Add a permission**.
3. In the opened pane select the **SharePoint** API.

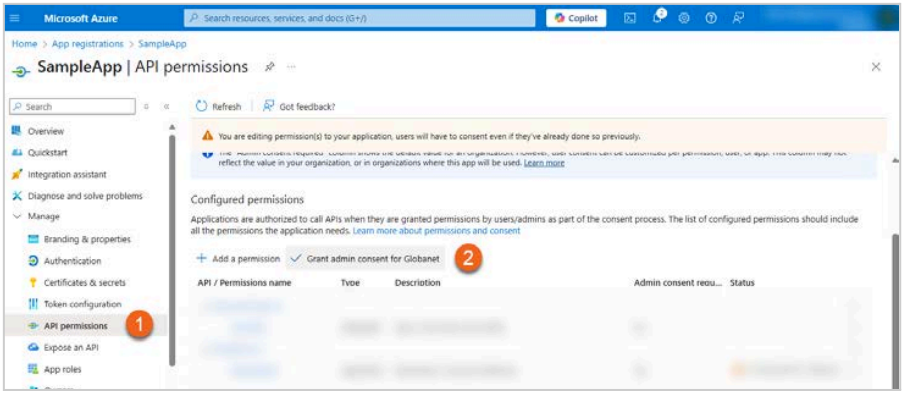


4. To add the necessary permission:
    4.1. Click **Application permissions**.
    4.2. Add the following permissions:
        4.2.1. Sites:
            4.2.1.1. Sites.FullControl.All
            4.2.1.2. Sites.Read.All
        4.2.2. **TermStore:** *TermStore.Read.All*
        4.2.3. **User:** *User.Read.All*
    4.3. Click **Add permissions**.



Granting Admin Consent

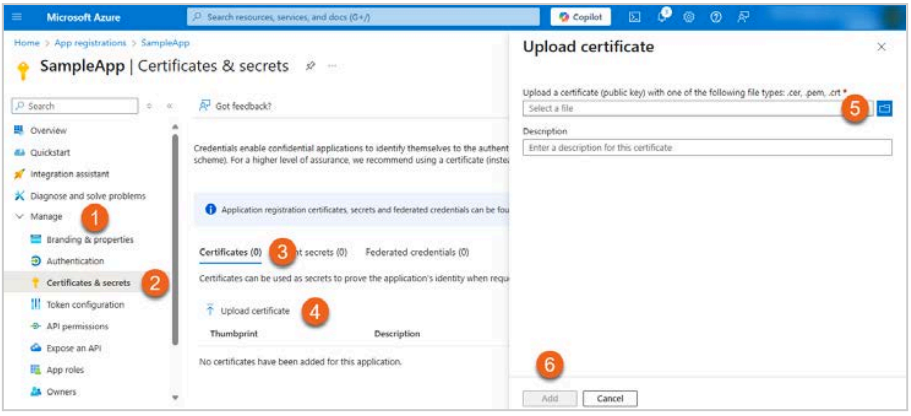
1. Go back to **API permissions**.
2. Click **Grant admin consent** for your company to grant the added permissions.



Uploading a Certificate

To upload a certificate:

1. In the left-hand navigation pane, go to **Manage > Certificates & secrets**.
2. Select Certificates.
3. Click **Upload certificate**.
4. Select a certificate (public key) with one of the following file types: `.cer`, `.pem`, `.crt`.
5. Click **Add**.



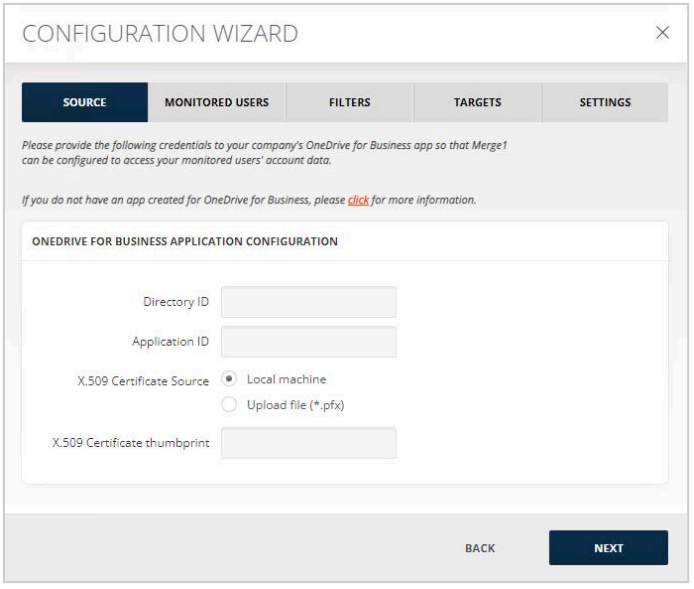
A certificate **thumbprint** will be generated. Keep the value for configuring the collector in Merge1.

For more information on how to create a certificate, see **Creating a Certificate (Private and Public Keys)**.

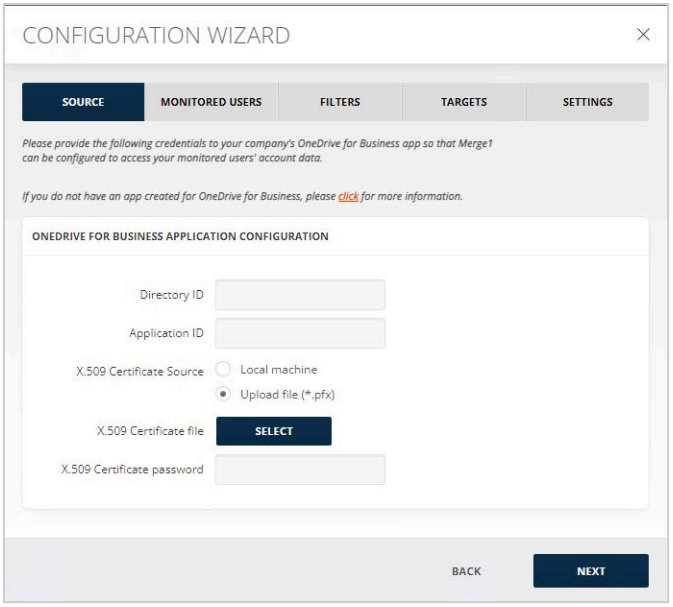
Collector Configuration

After filling in the **Name** and **Description** on the **Add Importer** window and selecting the source on **Configuration Wizard**:

1. In the new window, add the **Directory ID** and **Application ID**.
2. Provide **X.509 Certificate Thumbprint** in case you activate the **Local machine** radio button as the X.509 Certificate source.



3. In case you activate **Upload file (*.pfx)**, click the **Select** button to upload the certificate and provide **X.509 Certificate password**.



The **Certificate thumbprint** field will be auto populated in case the collector was previously configured by uploading a certificate.

4. Click **Next**.

Attachments Configuration

- **Include original data as attachment**: If checked, the message original data is attached to the output file.
- **Ignore attachments**: If checked, all the attachments are excluded from the message enhancing the collector's performance. Each message will contain info and the link to the excluded attachment.

Otherwise, additional configurations will open for setup. See Attachments Configuration.

Time Stamp Formatting

For more details on how to configure timestamps, see **Time Stamp Formatting**.

Advanced Configuration Options

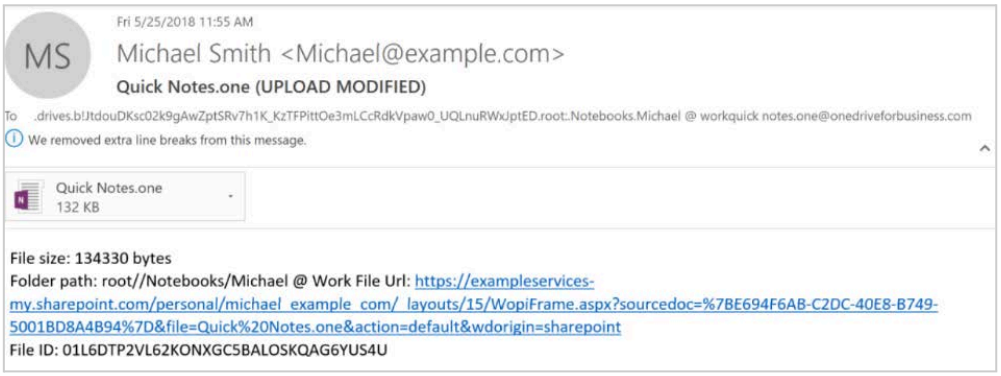
For more details on how to configure advanced configuration options, see **Advanced Configuration Options**.

Next Steps

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

- **MONITORED USERS**
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

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
  - Content
- Participant left:
  - Date time
  - Corporate email ID

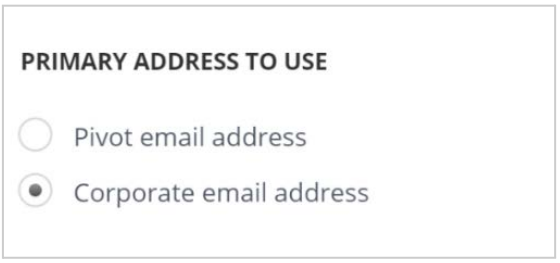
Collector Configuration

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

- **File Source**
- **Execute Script Against Source Files**
- **PGP Decryption**
- **Folders**
- **After Successful Importing**
- **Misc Settings**

Primary Address to Use

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

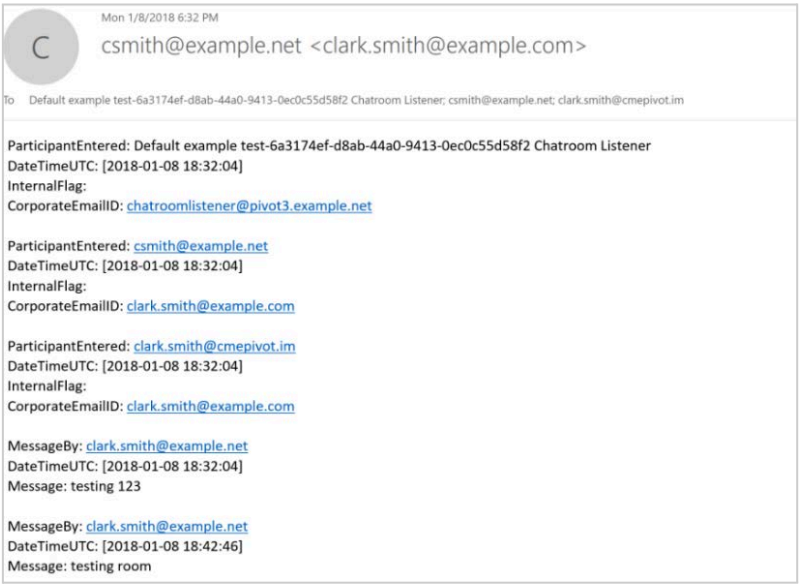


Next Steps

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

- Monitored Users (N/A)
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Quarantine file**
- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

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 company overall. Through its Speak platform, Redtail can send text messages to communicate with the clients and recognizes the need for compliance.

Mergel 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

Collector Configuration

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

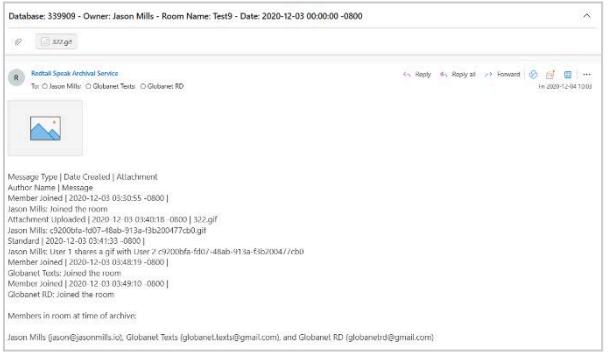
- **File Source**
- **Execute Script Against Source Files**
- **PGP Decryption**
- **Folders**
- **After Successful Importing**
- **Misc Settings**

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**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Quarantine file**
- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

RingCentral

RingCentral Team Messaging is a collaboration platform designed to streamline team communications by providing centralized messaging and organization tools.

The **Merge1 RingCentral collector** utilizes the RingCentral compliance API to retrieve messages and meeting-based content, ensuring secure archiving and compliance management for enterprise communication.

Activities Captured

- Chats
- Tasks
- Notes
- Events
- SMS chats[35]
- Attachments[36]

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.

https://developers.ringcentral.com/guide/team-messaging/manual/compliance-export-structure

When you download a compliance export, you will receive a .zip file that contains a number of files and folders that contain all the data associated with your data export.

Note

Only the content and items within the archive's specified period are included in the downloaded/compliance export file. Therefore, data outside that time range is not captured.

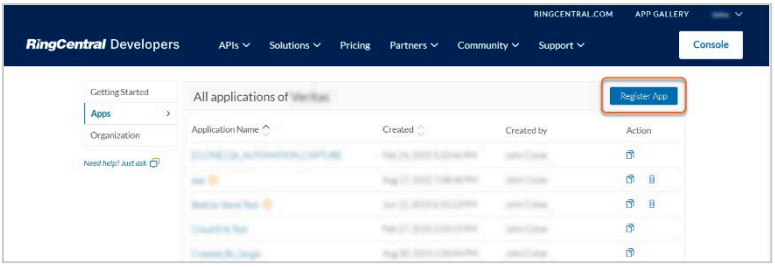
Creating a RingCentral Application

To create the application:

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

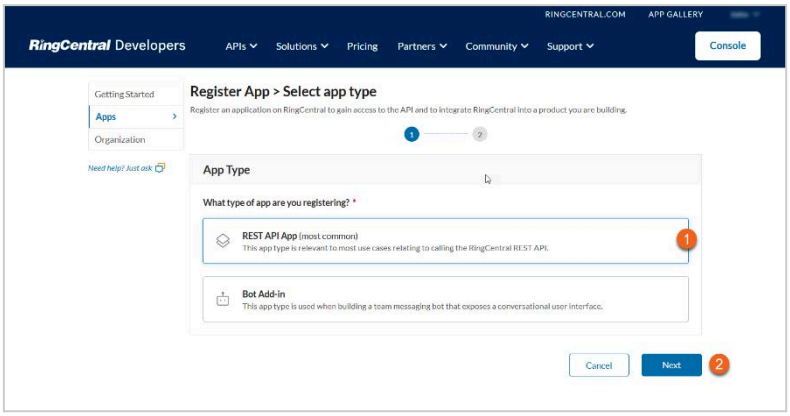
[35] The outgoing SMS chats of internal users and incoming SMS chats of external users are captured.

[36] 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.

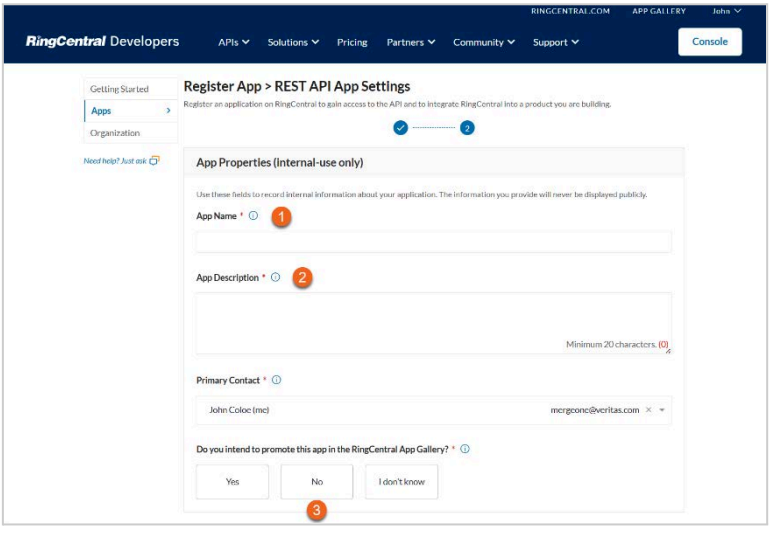


Note that if you see the **Register App** button, but it is disabled, then your account lacks the permission required to create an app. Contact your account administrator to request this permission.

3. Select **REST API App** and click **Next**.



4. In the **App Properties** window:
   4.1. Enter **App Name**.
   4.2. Enter **App Description**.
   4.3. Select **No** for **Do you intend to promote this app in the RingCentral App Gallery?**.

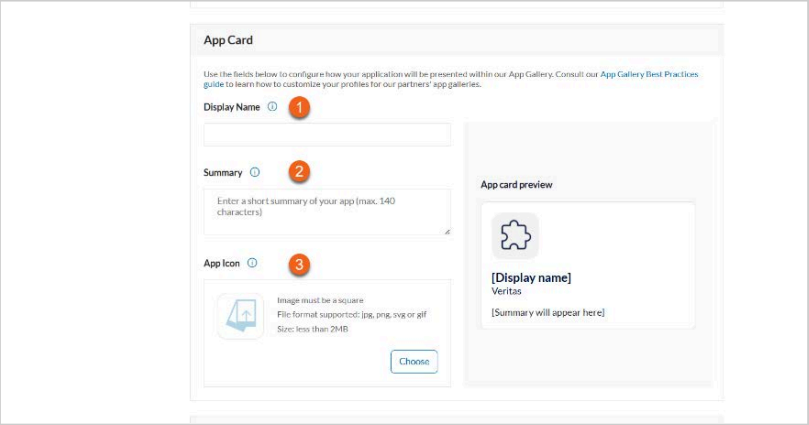


5. In the **App Card** section:
   5.1. Enter **Display Name**.

5.2. Enter **Summary**.

5.3. Upload **App Icon** in PNG format.

> **Tip**
>
> - Image must be a square.
> - File format supported: jpg, png, svg or gif.
> - Size: less than 2MB.
> - Find attached one here: 

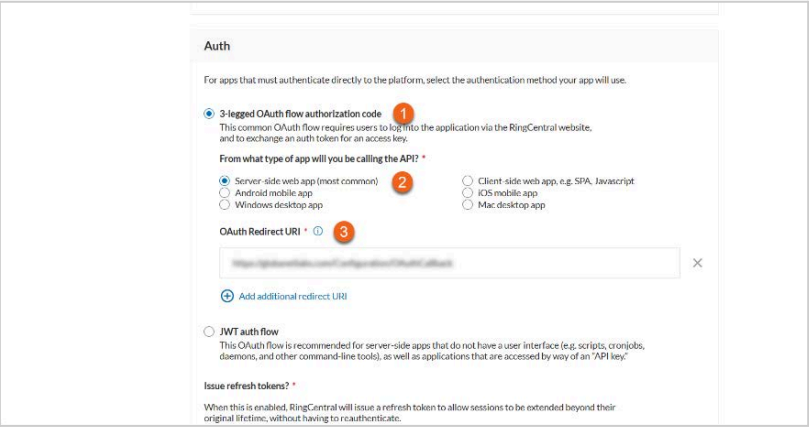


6. In the **Auth** section:

6.1. Ensure **3-legged OAuth flow authorization code** is enabled.

6.2. Select **Server-side web app (most common)**.

6.3. Enter the URL of your local Merge1 environment in the following format: `https://<merge1_instance>/Configuration/OAuthCallback` in **the OAuth Redirect URI** field.

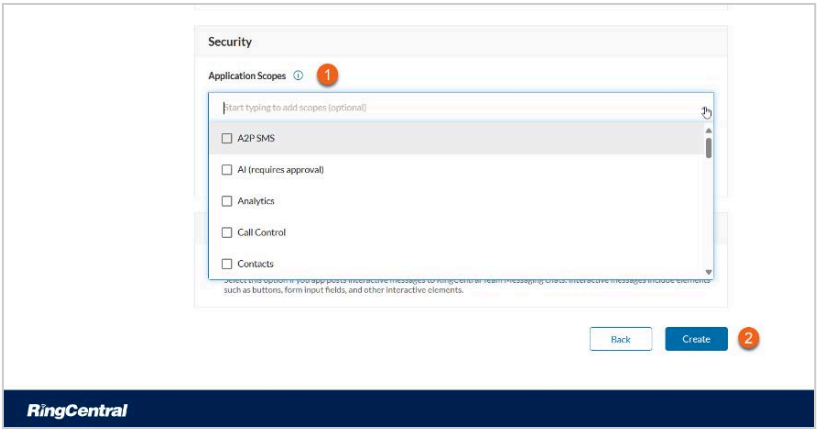


7. In the **Security** section, select the following scopes from the **Application Scopes** drop-down list, then click **Create**:

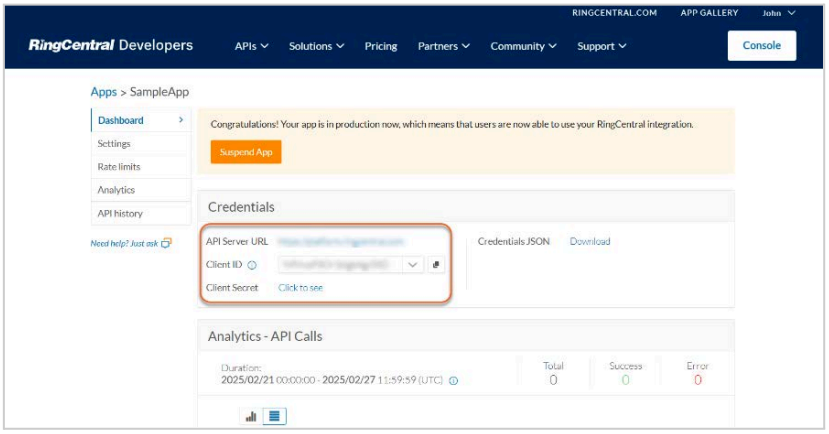
7.1. **Read Accounts**

7.2. **Read Messages**

7.3. **Team Messaging**



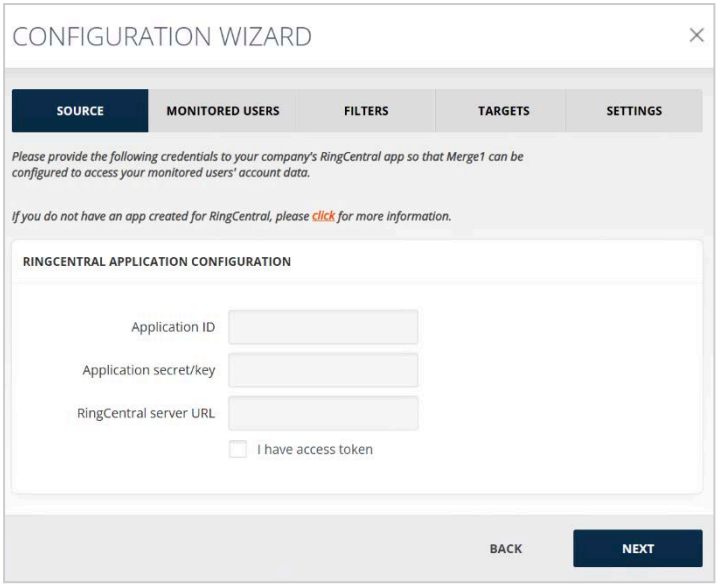
8. The **API Server URL**, **Client ID**, and **Client Secret** will be generated. Use these credentials to configure the collector.



Collector Configuration

To set up the collector:

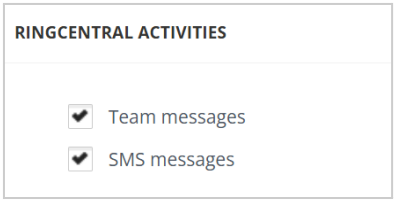
1. Click **Add Importer**, specify **Name** and a **Description**(optional), and select the collector from the list. The **RingCentral Application Configuration** window will open.
2. In the **Application ID** field enter **Client ID** copied previously, in **Application secret/key**, enter the copied **Client Secret**, enter the **API server URL** in the **RingCentral server URL** field, and then click **Next**.



RingCentral Activities

There are the following types of activities which can be captured with the collector:

- Team messages
- SMS messages



By enabling the **Team messages** or/and **SMS messages** checkboxes, the activities from teams or/and SMS chats will be processed.

Time Stamp Formatting

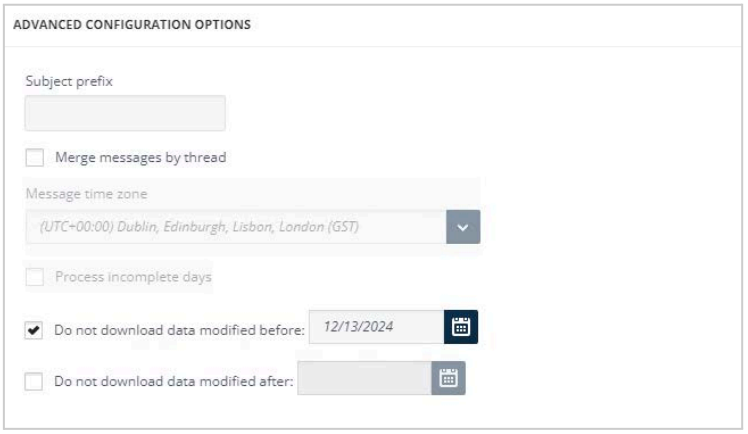
For more details on how to configure timestamps, see **Time Stamp Formatting**.

Advanced Configuration Options

There are following advanced options when configuring the collector with Merge1.

- 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 **Process incomplete days** option is enabled, the messages of the days that have not yet ended will be imported in a separate email as well. 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 08/17/2024 and the *after date* is set to 09/17/2024, only the data between these two dates will be downloaded. Data outside that timeframe will be ignored.



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.

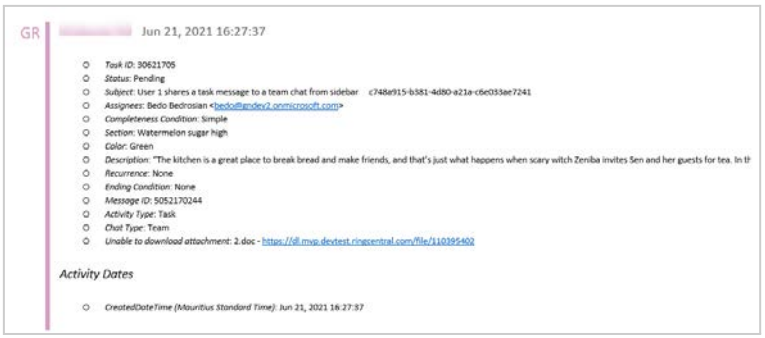
For more details on how to configure attachments, see **Attachments Configuration**.

Next Steps

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

- **MONITORED USERS**
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

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 that when the group is deleted, the messages are not captured.

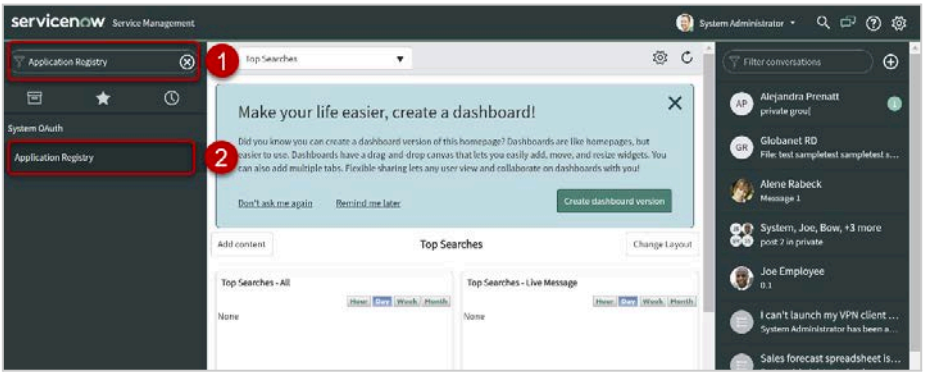
Activities not Captured

- Record feed
- Tasks with comments
- Incidents with comments
- Requests with comments
- Requested items with comments
- Problem with comments
- Change request
- Change task

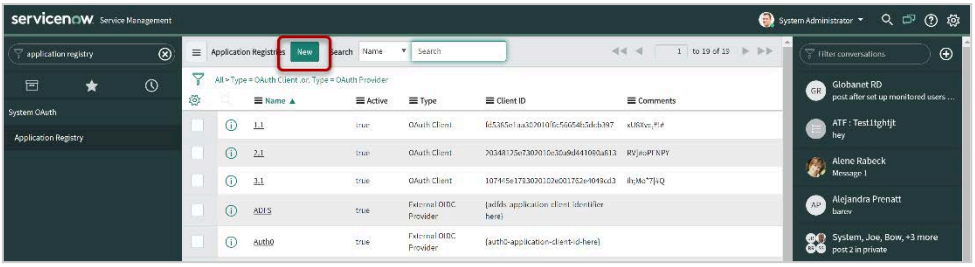
Creating a ServiceNow Application

The administrator of your organization must perform the following steps:

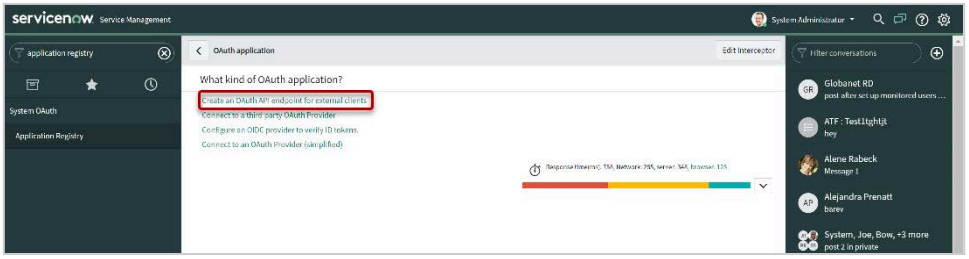
1. Log in to ServiceNow instance and navigate to **System OAuth > Application Registry.**



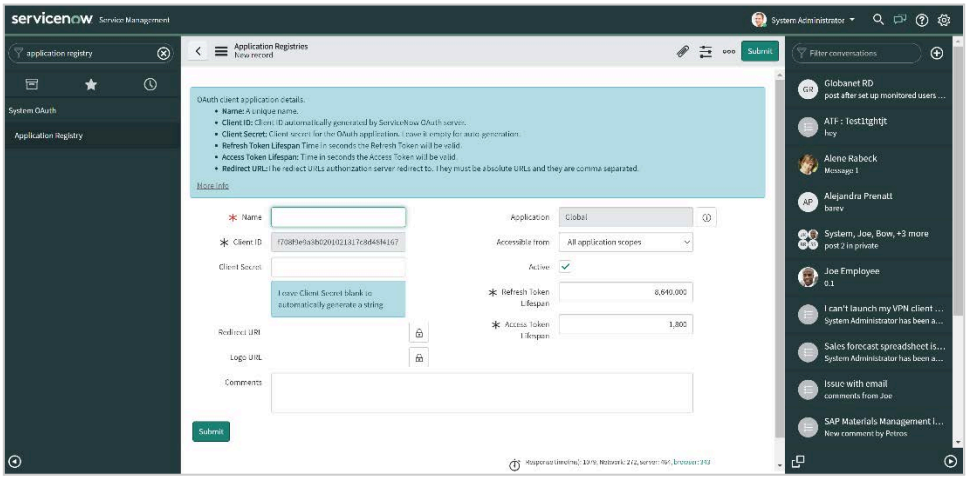
2. Click the **Application Registry** and the applications list will open. Click **New**.



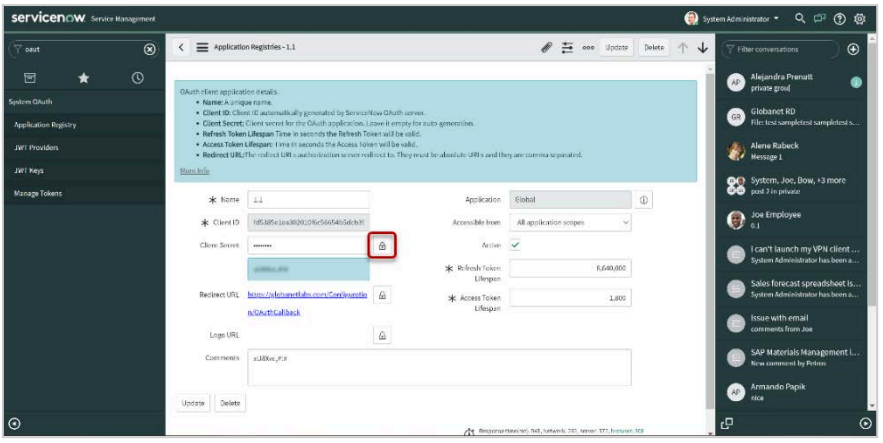
3. Select the Create an OAuth API endpoint for external clients option.



4. Enter a name for the application.
5. Unlock the **Redirect_URI** field and enter the URL of your local Merge1 environment with the following format: `https://merge1_instance/Configuration/OAuthCallback` and click the **Submit** button.



6. After executing the provided steps, you will find the application you have just created on the Application Registry page. Click your application, and in the window that opens, you will find your application details, including **Client ID** and **Client Secret**.

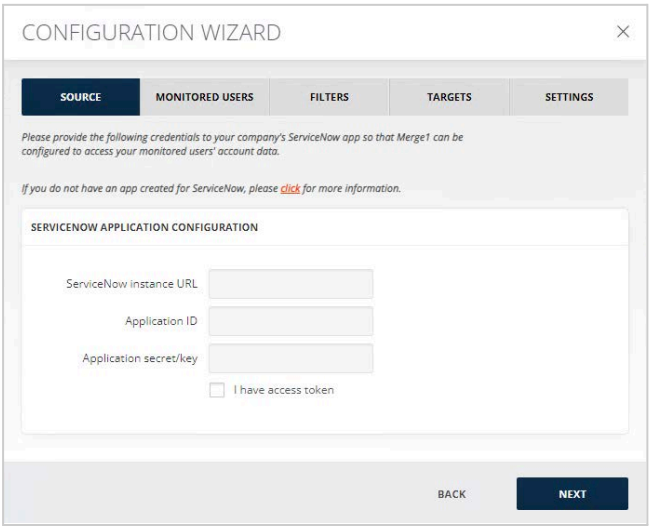


7. Copy and save the **Client ID** and Secret to later provide them to Merge1 as part of ServiceNow configuration.

Collector Configuration

To set up the collector:

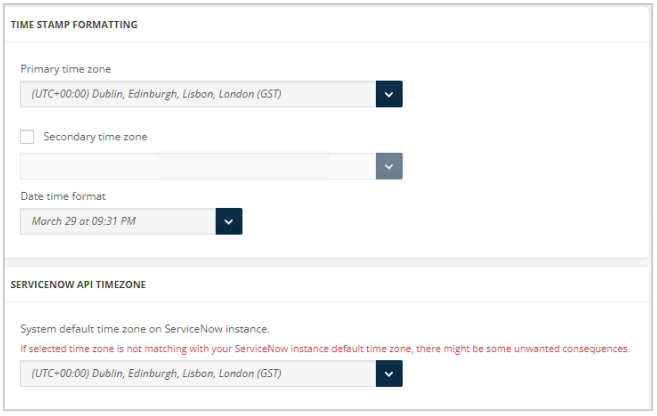
1. Click **Add Importer**, specify **Name** and a **Description** (optional), and select the collector from the list. The **ServiceNow Application Configuration** window will open.
2. Add your **ServiceNow Instance URL**, the **App Key** copied previously in the **Application ID** field, and in **Application 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 list, 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. You should also select ServiceNow API Time zone which shows system default time zone on the ServiceNow instance[37].

[37] This is a mandatory field.



Note that if selected time zone is not matching with your ServiceNow instance default time zone there might be some unwanted consequences.

Advanced Configuration Options

For more details on how to configure advanced configuration options, see **Advanced Configuration Options**.

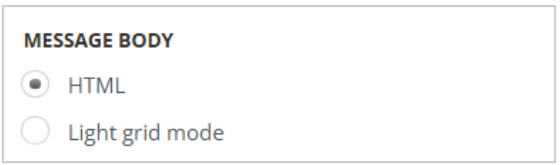
Attachment Configuration

For more details on how to configure attachments, see **Attachments Configuration**.

Message Body

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.
- **Light grid mode**: Displays data in a two-toned layout, making it visually distinct and easier to view while displaying limited metadata.

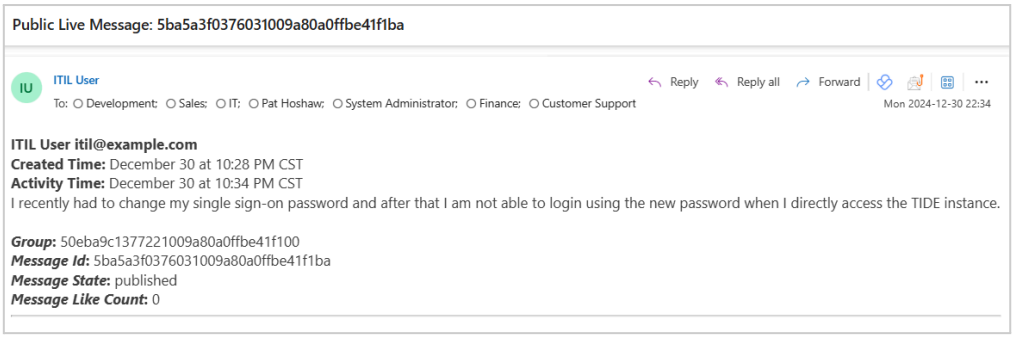


Next Steps

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

- **MONITORED USERS**
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

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 Merge1 SharePoint collector captures data from SharePoint Online.

Activities Captured

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

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

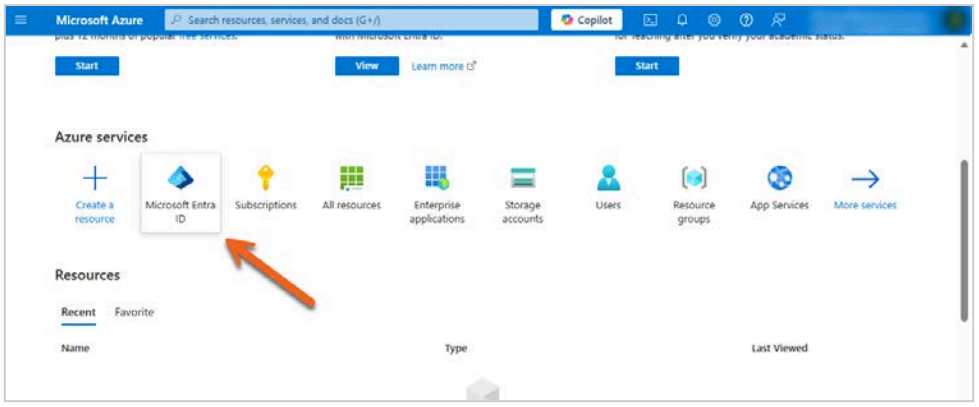
Creating a Microsoft Entra ID Application

The Office 365 or Azure administrator in your organization must complete the steps detailed in the sections below.

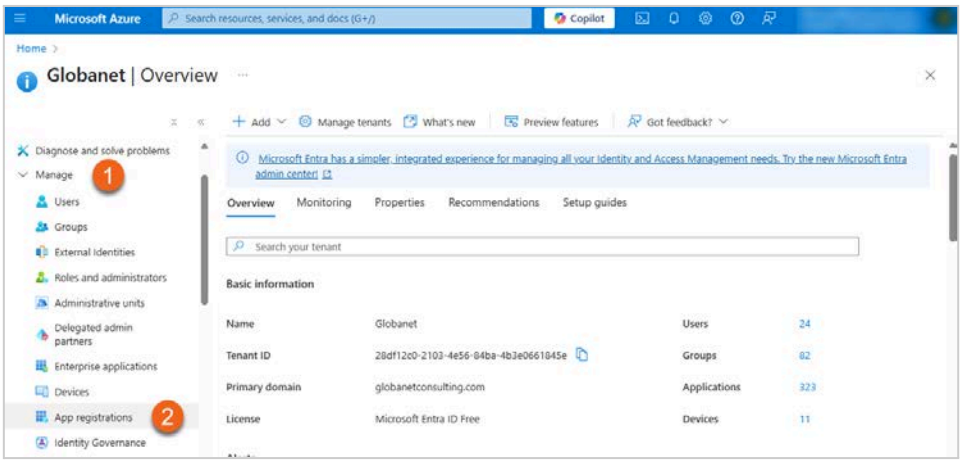
Registering an Application

Sign in to **Azure Portal**.

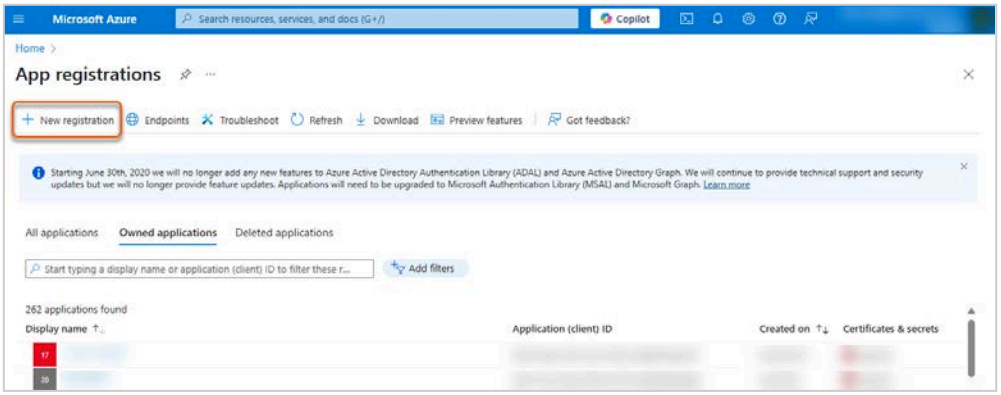
1. Select **Microsoft Entra ID** under **Azure services**.



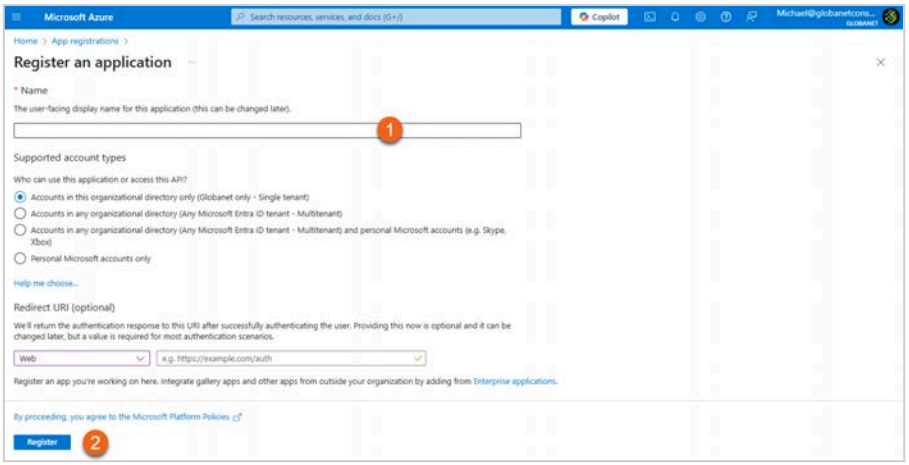
2. In the left-hand navigation pane, click **Manage > App registrations**.



3. Click **New registration**.



4. To register an application:
   4.1. Enter a **Name** for the application.
   4.2. Click **Register**.



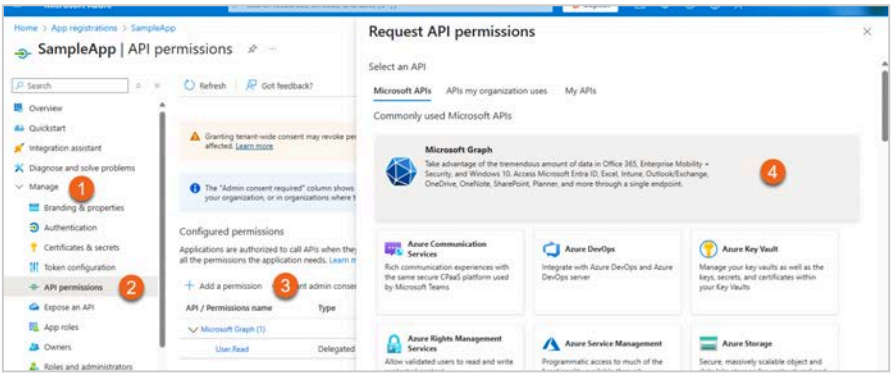
5. An **Application (client) ID** and **Directory (tenant) ID** will be generated. Keep both for configuring the collector in Mergel.

Granting Permissions

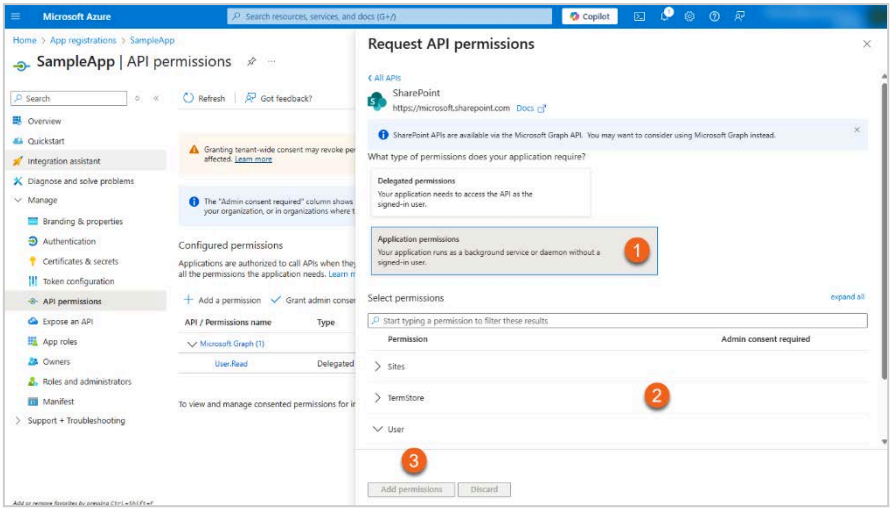
Adding Microsoft Graph API Permissions

To add **Microsoft Graph** API permissions:

1. In the left-hand navigation pane, click **Manage > API permissions**.
2. Click **Add a permission**.
3. In the opened pane select the **Microsoft Graph** API.



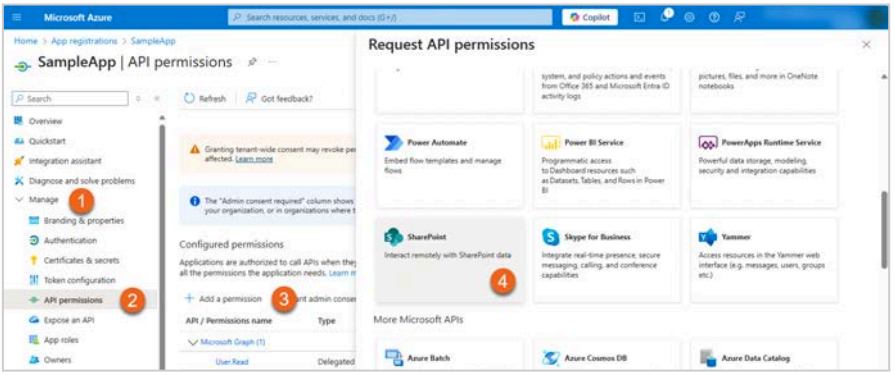
4. To add the necessary permission:
   4.1. Click **Application permissions**.
   4.2. Add the following permissions:
      4.2.1. Directory: *Directory.Read.All*
      4.2.2. Files: *Files.Read.All*
      4.2.3. **User:** *User.Read.All*
   4.3. Click **Add permissions**.



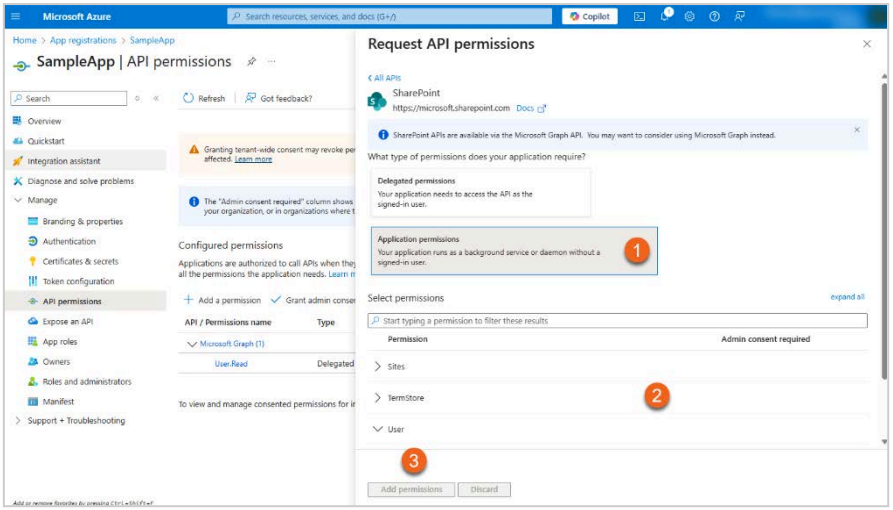
Adding SharePoint API Permissions

To add **SharePoint** API permissions:

1. In the left-hand navigation pane, click **Manage > API permissions**.
2. Click **Add a permission**.
3. In the opened pane select the **SharePoint** API.

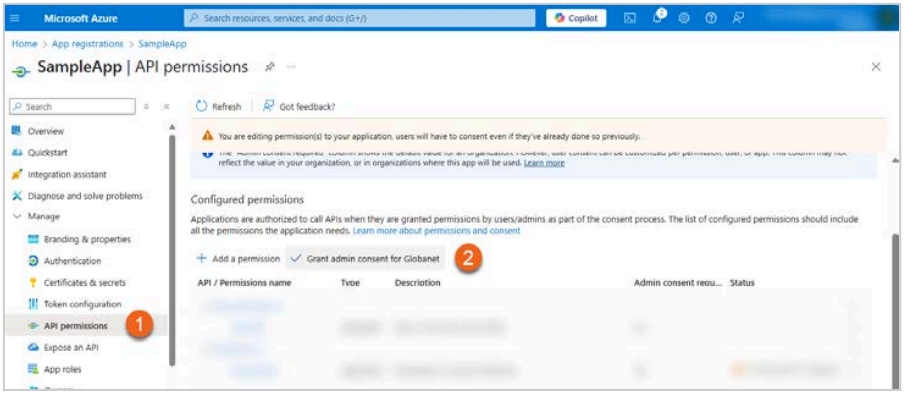


4. To add the necessary permission:
    4.1. Click **Application permissions**.
    4.2. Add the following permissions:
        4.2.1. **Sites:**
            4.2.1.1. Sites.FullControl.All
            4.2.1.2. Sites.Read.All
        4.2.2. **TermStore:** *TermStore.Read.All*
        4.2.3. **User:** *User.Read.All*
    4.3. Click **Add permissions**.



Granting Admin Consent

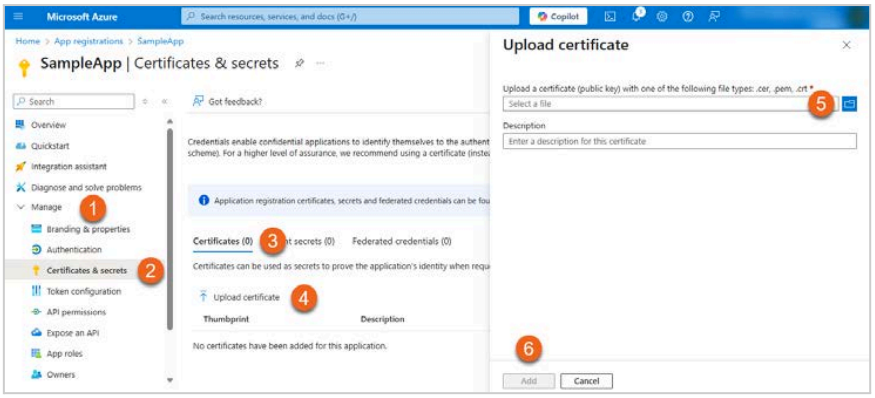
1. Go back to **API permissions**.
2. Click **Grant admin consent** for your company to grant the added permissions.



Uploading a Certificate

To upload a certificate:

1. In the left-hand navigation pane, go to **Manage > Certificates & secrets**.
2. Select **Certificates**.
3. Click **Upload certificate**.
4. Select a certificate (public key) with one of the following file types: `.cer`, `.pem`, `.crt`.
5. Click **Add**.



A certificate **thumbprint** will be generated. Keep the value for configuring the collector in Merge1.

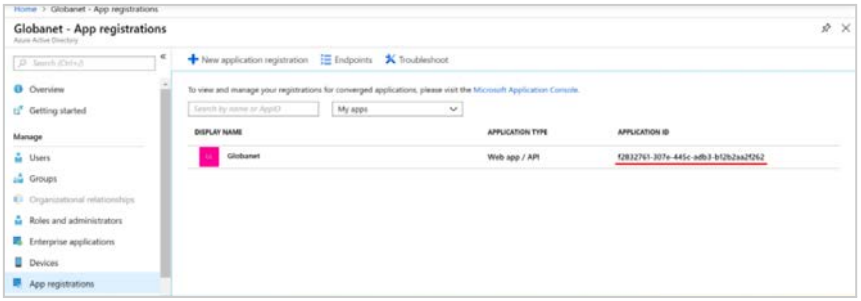
For more information on how to create a certificate, see **Creating a Certificate (Private and Public Keys)**.

Collector Configuration

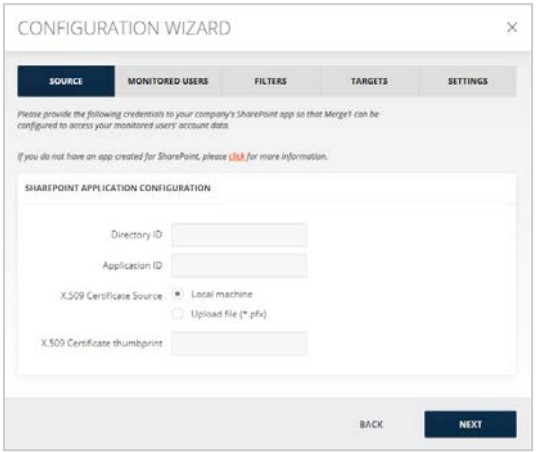
To set up the collector:

1. After you click **Add Importer**, and specify **Name** and a **Description** (optional).
2. In the new window opened, add **Directory ID**, and **Application ID**.

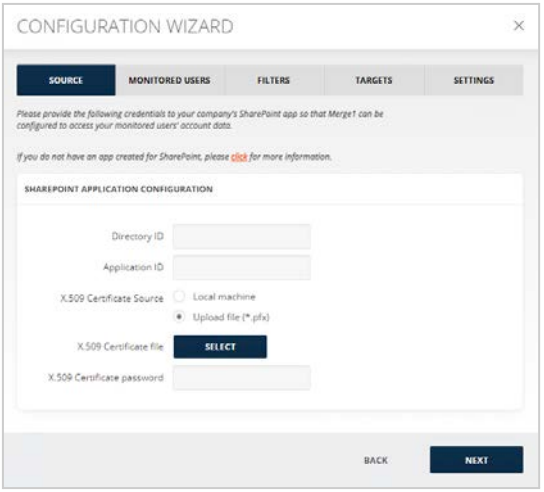
You can copy the **Application ID** from the **Microsoft Entra ID > App Registrations > <your app name>** section.



3. Provide **X.509 Certificate Thumbprint** in case you activate the **Local machine** radio button as the X.509 Certificate Source.



4. In case you activate **Upload file (*.pfx)**, click the **Select** button to upload the certificate and provide **X.509 Certificate password**.



The **Certificate thumbprint** field will be auto populated in case the collector was previously configured by uploading a certificate.

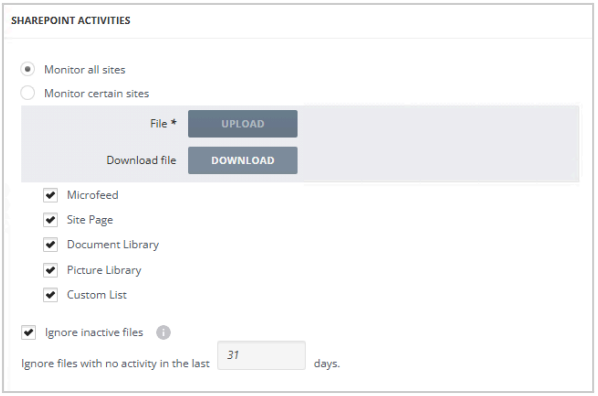
SharePoint Activities

For SharePoint activities:

1. Activate **Monitor all sites** in case all SharePoint sites should be monitored. In this case, the 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.
5. The following activities will be captured if selected[38]:
    - Microfeed
    - Site Page
    - Document Library
    - Picture Library
    - Custom List
6. The **Ignore inactive files** checkbox is enabled by default, and the **Ignore files with no activity in the last X days** parameter is set to 31 days. As a result, only the files with their comments modified

[38] If the file names contain the "#" and "%" symbols, they will not be downloaded.

within the specified days will be captured.
If the checkbox is disabled, all files will be captured regardless of their activity.



Time Stamp Formatting

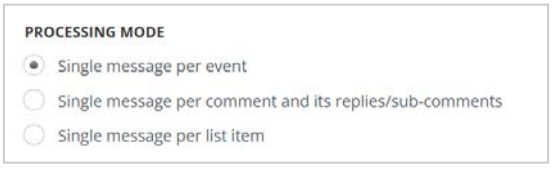
For more details on how to configure timestamps, see **Time Stamp Formatting**.

Advanced Configuration Options

For more details on how to configure advanced configuration options, see **Advanced Configuration Options**.

For **Processing Mode,** here 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 Merge1 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.

Attachments Configuration

- **Include original data as attachment**: If checked, the message original data is attached to the output file.
- **Ignore attachments**: If checked, all the attachments are excluded from the message enhancing the collector's performance. Each message will contain info and the link to the excluded attachment.

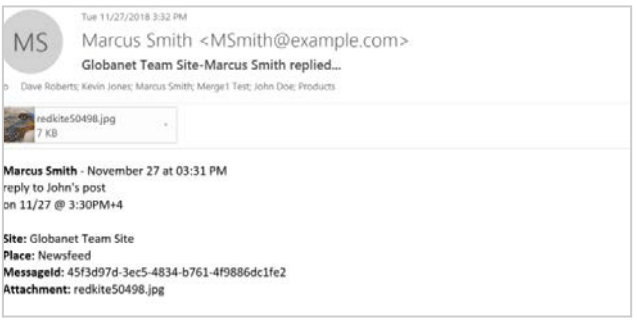
Otherwise, additional configurations will open for setup. See **Attachments Configuration.**

Next Steps

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

- **MONITORED USERS**
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

Skype for Business

Skype for Business is an instant messaging client used with Skype for Business Server or with Skype for Business Online. Skype for Business is an enterprise software.

Merge1 captures OCS/Lync/Skype for Business chats from SQL databases. Attachments are not captured, so they should be disabled for the compliance.

The configuration page consists of three database configurations:

- Archive database, usually named LCSLogs, contains all the communications between the users.
- Persistent Chat database is MGC containing persistent chats.
- Compliance database is only used to capture participant entered, participant left, room deleted events, it must be configured along with the Persistent Chat database, otherwise, the information will not be captured.

To capture messages from persistent chat rooms, **Enable Chat History** option should be selected from **Persistent Chat** category section.

Activities Captured

- Messages between users
- Persistent chats
- Message deletes not allowed by the system
- Message edits not allowed by the system

Collector Configuration

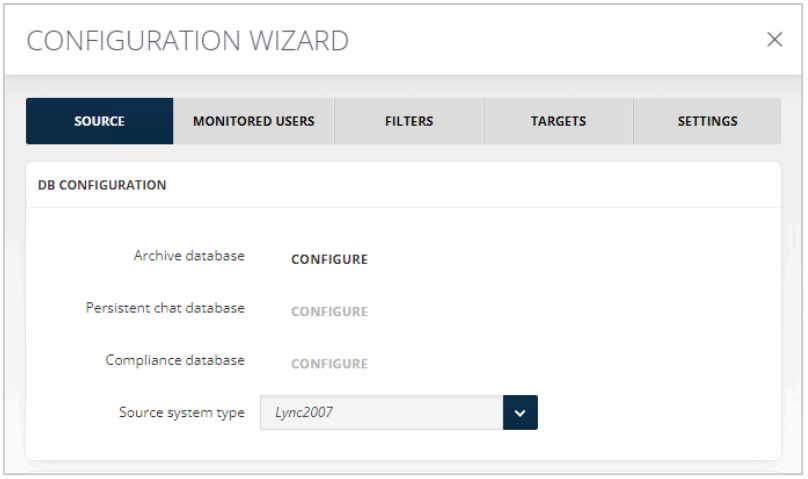
DB Configuration

Merge1 retrieves data from Lync/Skype for Business directly from its database(s).

Select the **Source System Type** from the drop-down list. (Merge1 supports Lync/Skype for Business versions 2007 through 2013) Persistent Chat and Compliance databases are configurable for version 2013 only.

Note

Your Merge1 service account must have read access to your Skype for Business Compliance Databases (the default database names for Skype for Business are: LCSlogs, mgc, mgccomp).



In the Merge1 Configuration for Skype for Business, we have three types of databases: **Archive**, **Persistent Chat**, and **Compliance**, which are configured individually by providing database server addresses and authentication credentials.

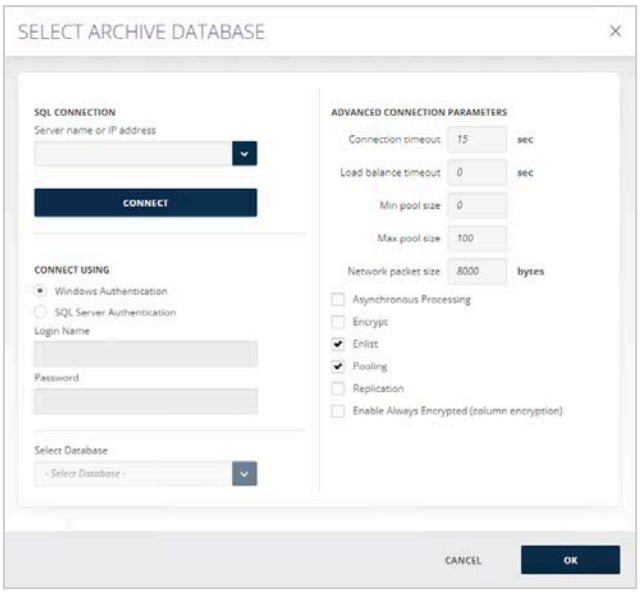
To change the configurations of individual database types, click **Configure** next to the **Archive Database**.

All three types of databases are configured as follows:

1. Select the SQL Server from the drop-down menu.
2. Choose the authentication method to connect to the server. If **Windows Authentication** is chosen Merge1 will connect to it using the **Windows credentials** of the account, it is set upon. If **SQL Server Authentication** is chosen it can be connected to with the **SQL Server** credentials.
3. Select the database, where Skype files are stored, from the drop-down list after connecting to the server.
4. **Advanced Connection Parameters** allow specifying the following:
    - In the **Connection timeout** field, the time during which the query is not processed can be specified to yield timeout.
    - In the **Load balance timeout** field, the time during which the inactive connections should be kept open in a connection pool can be specified. An inactive connection is a database session that is not in use by an application.
    - **Min pool size** is the minimum number of requests the application may process concurrently.
    - **Max pool size** is the maximum number of requests the application may process concurrently.
    - **Network packet size** is the fixed-size chunk of data that transfers requests and results between clients and servers. This field specifies in what file-size chunks the file data should be transferred.
    - **Asynchronous Processing**, when enabled, allows various workflows to run at the same time.
    - **Encrypt** should be checked, when SQL Server uses SSL encryption for all data sent between the client and server if the server has a certificate installed.
    - **Enlist** when enabled, checks whether the SQL Server connection pooler automatically enlists the connection in the creation thread's current transaction context.
    - **Pooling**, if enabled keeps the database connections active so that, when a connection is later requested, one of the active ones is used in preference to have to create another one.
    - **Replication** is a technique through which an instance of a database is exactly copied to, transferred to, or integrated with another location. Database replication is done to provide a

consistent copy of data across all the database nodes. It also removes any data redundancy, merging of two databases into one and updating the secondary databases with outdated or incomplete data.

- Enable **Always Encrypted (column encryption)** enables **SQL Always Encrypted** on existing Merge1 databases.

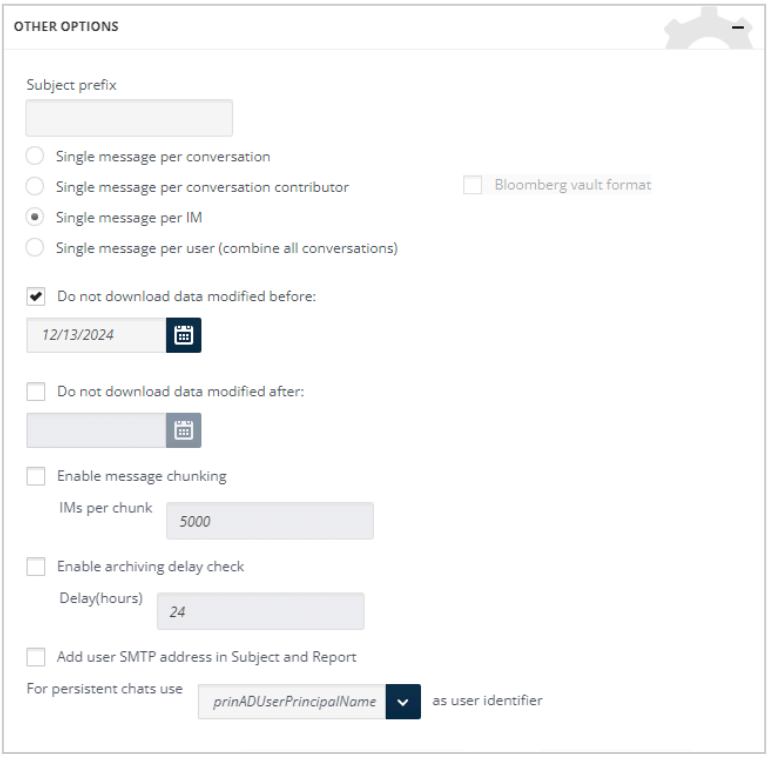


Other Options

For other options:

- 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.
- When **Single Message per Conversation** is selected, a single message is archived for each conversation.
- When **Single Message per Conversation Contributor** is selected, a single message is archived for each conversation with one version of the conversation per participant. This allows for the data to be searched for based on the participant's name. You can enable **Bloomberg Vault Format** to enable Bloomberg archive formatting.
- If **Single Message per IM** is enabled, each **IM** in the conversation is imported as a separate message.
- If **Single Message per User (Combine all conversations)** is enabled, a separate archive is created for each **User** and includes all conversation of that participant. The **From** field will contain the user's email address, the **To** field will contain all the email addresses of those with whom that user has chatted, and the **Body** will contain all the user's conversations.
- 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 08/17/2024 and the *after date* is set to 09/17/2024, only the data between these two dates will be downloaded. Data outside that timeframe will be ignored.
- Enable **Message Chunking** if you want to break down the data segments into chunks containing the specified number of messages.
- If you want to exclude messages that were sent within the past X number of hours, you can enable **Archiving Delay Check**.

- **For persistent chats use _ as user identifier** option allows specifying the values from which columns of the source DB should be assigned to the monitored users. The options are: prinUri, prinEmail, prinADUserPrincipalName.
- Enabling **Bloomberg Vault Format** checkbox output message will be as shown.



Archiving Delay Check Warning

The **Delayed Archive** feature is meant to mitigate a problem caused by a perceived deficiency in Skype for Business whereby messages may enter the Compliance database later than anticipated. Mergel can be configured to not only address current (daily) messages but also re-examine messages up to 72 hours in the past (look back period) to determine if there were late arriving messages and process those as well. The bigger the look back period, the more processing Mergel will have to do. We recommend choosing a minimal look back period only when necessary and to never exceed 72 hours.

Recommended Use Case

The Skype for Business database, where the messages are stored, is not updated synchronously with the application. It takes some time for the messages to be synchronized into the Skype for Business database. Therefore, we recommend running the Skype for Business collector only one time a day on a non-working hour.

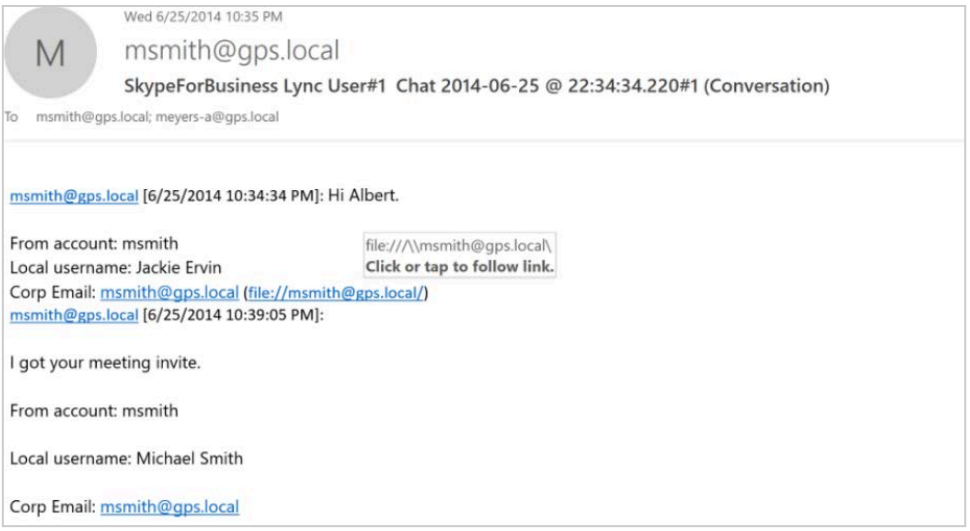
Next Steps

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

- **MONITORED USERS**
- **FILTERS**
- **TARGETS**

- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

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.

It is required to have Compliance SKU enabled for the Slack Enterprise Grid.

To set up the Slack eDiscovery collector, open the `C:\Program Files\Arctera Inc\Merge1 7.0\UserSettings.config` folder[39] and replace the last four lines with the following:

```
    <add key="SiteUrl" value="https://localhost/" />
    <add key="ResourcesUrl" value="https://localhost/" />
    <add key="OAuthCallbackUrl" value="https://localhost/" />
</UserSettings>
```

In addition, you should contact Slack at exports@slack.com and ask to enable **Discovery API** for your organization before finishing the collector setup.

You should use `https://localhost` to access the Merge1 portal for passing the OAuth for eDiscovery.

Note that after setting it up, you can change it back to your IP address.

Activities Captured

- Activities from all workspaces
- Direct messages
- Canvases[40] [41]
    - Canvas activities[42]
    - Canvas comments
    - Canvas content[43]
- Multi-participant direct messages
- Channel conversations/messages
- Attachments (the attachment itself is included in the message generated by Merge1 as an attachment)
- Attachments shared using third-party integrations such as OneDrive (only the link is included in the body of the message generated by Merge1)
- Emojis (as texts)
- GIFs
- Deletes (including the deleted message and the event itself)[44]
- Edits (including the message before and after it is edited)

[39] For Merge1 version 6.0, the path will be `C:\Program Files\Globanet Consulting Services\Merge1 6.0\UserSettings.config`.

[40] Canvas download activities of the admin account are not captured.

[41] Reauthentication is required for capturing canvases.

[42] Deleted canvases and canvas items are not captured.

[43] The latest edit in the canvas content is captured in case of multiple edits.

[44] Deleted messages of external users are not captured.

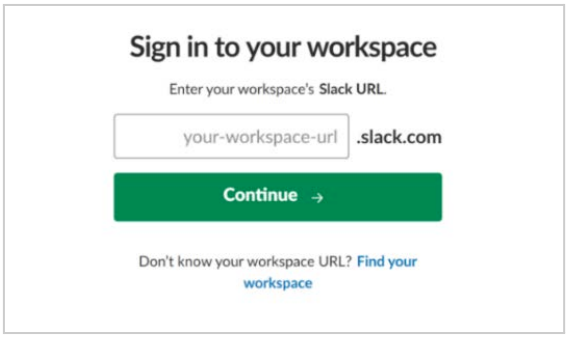
- Guest conversations
- Message reactions[45]
- Shared channel events (channels shared with external organizations[46])
- Channel join event
- Set channel purpose event
- Files delete event
- Emails sent from supported email services

Note that 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.

Collector 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 Mergel collector.

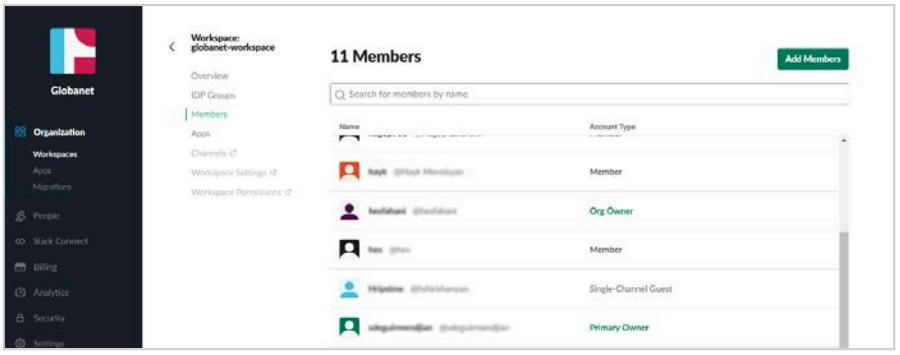


2. Click **Manage Organization** on the upper right corner.

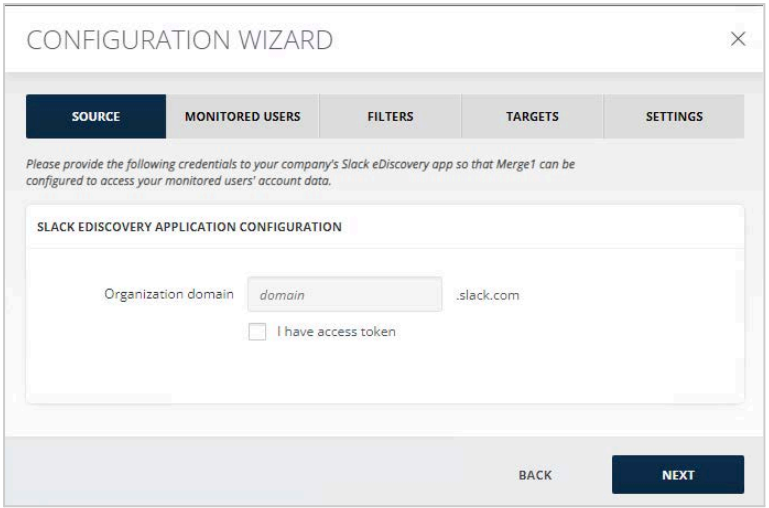
3. Enter the necessary workspace.
4. Confirm that the account used for configuring Mergel has the necessary permissions, i.e., is either an **Org. Owner** or a **Primary Org. Owner**.

[45] Reactions for deleted messages are not captured.

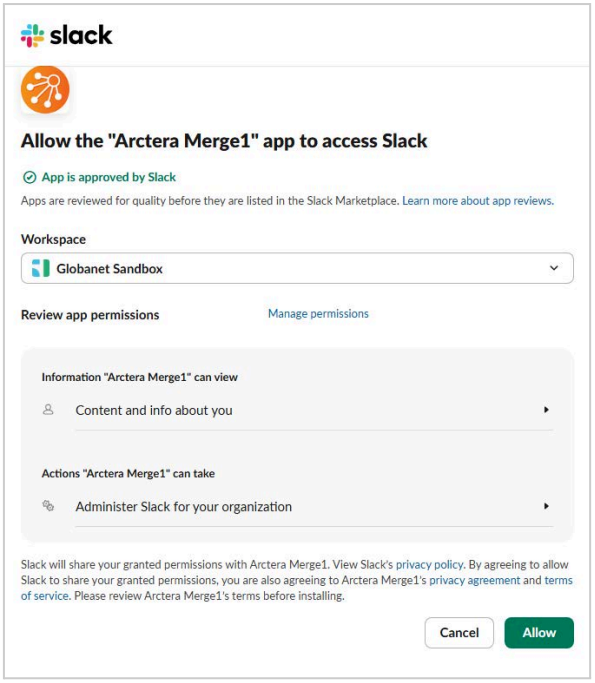
[46] Including the external users' names.



5. Leave the window open.
6. Go to Merge1 collector and 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 Merge1) to export, archive, or meet other security and compliance obligations for any organization content.



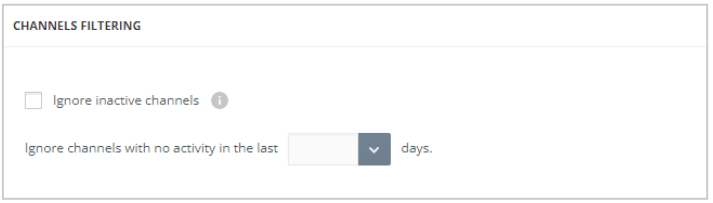
11. Authorize the connection between Slack eDiscovery and Merge1.



12. Click **Next**.

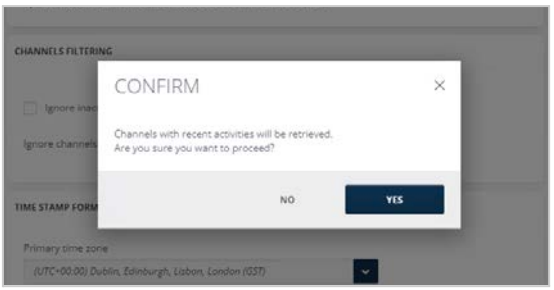
Channels Filtering

This section allows filtering inactive channels for the specified period. When the Ignore Inactive Channels checkbox is enabled, any channels that have not had any activity within the user-specified time frame of 2-7 days before the collector run will be disregarded.



To configure the filtering:

1. Click **Ignore inactive channels**. A confirmation pop-up opens.



2. Click **Yes,** to enable the checkbox for retrieving channels with recent activities. Or click **No** to cancel the channel filtering.
3. Select the number of days from the drop-down list. The maximum value is 7.

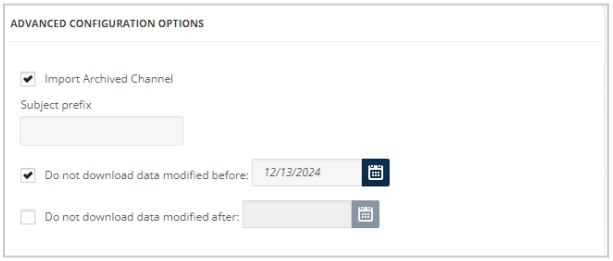
Time Stamp Formatting

For more details on how to configure timestamps, see **Time Stamp Formatting**.

Advanced Configuration Options

There are the following advanced options when configuring the collector with Mergel:

- **Import Archived Channel** – when this option is selected, Mergel 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 08/17/2024 and the *after date* is set to 09/17/2024, only the data between these two dates will be downloaded. Data outside that timeframe will be ignored.



Attachments Configuration

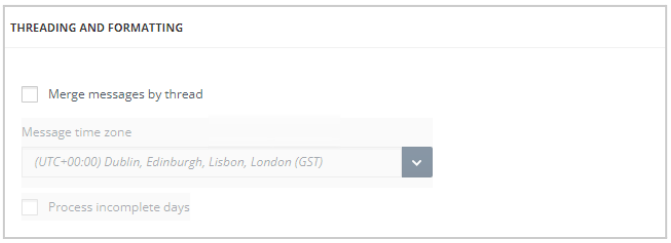
- **Include original data as attachment**: If checked, the message original data is attached to the output file.
- **Ignore attachments**: If checked, all the attachments are excluded from the message enhancing the collector's performance. Each message will contain info and the link to the excluded attachment.

Otherwise, additional configurations will open for setup. See **Attachments Configuration**

Threading and Formatting

- The **Merge Message by Thread** if checked combines messages by threads rather than sending them one by one.
    - Select the time zone by which the messages from the drop-down menu.
    - The message time zone by which the messages are split, can be selected 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 as well. This option can be selected only if **Merge Messages by Thread** is selected.



Message Body

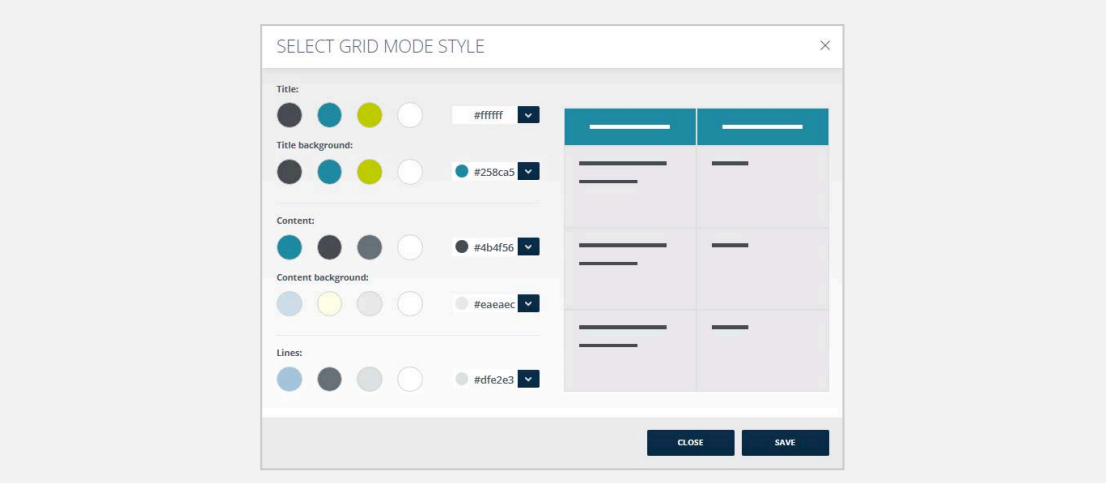
This setting determines how imported messages are displayed in the target. There are the following output message body options:

- **HTML**: Displays the message in HTML format.
- **Light grid mode**: Displays data in a two-toned layout, making it visually distinct and easier to view while displaying limited metadata.
- **Grid mode**: Displays output message content in a compact grid format for structured and efficient viewing. The information is structured into the following columns:
    - *Date*
    - *User info*
    - *Text*
    - *Action*
    - *Attachment*
    - *Reaction*
    - *Message ID*
    - *Reply to ID*
- **Pure body**: Displays the output message as plain text, without formatting or additional details.

Note that **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.

Tip

In **Grid mode**, the color scheme can be adjusted through the **Select Style** pop-up menu:

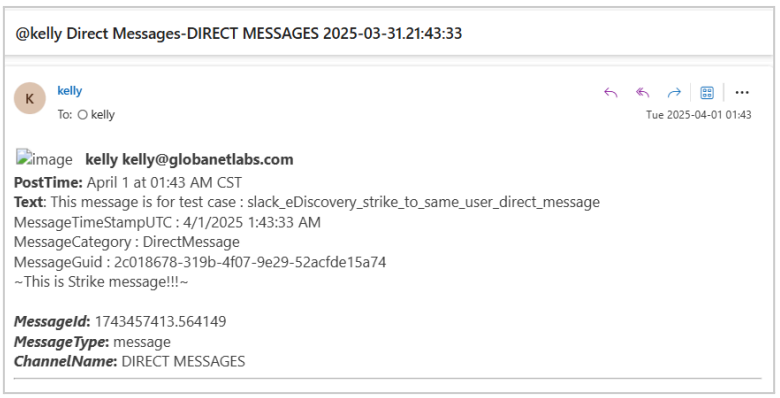


Next Steps

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

- **MONITORED USERS**
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**

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

For more information refer to **Notification Preferences**.

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 workflows.

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 that the Symphony collector can process only zipped XML files.

Activities Captured

- Records

Captured activities can contain:

- Post date
- From
- Message content
- Reaction
- Record type
- Message ID
- Attachment
- Downloaded by
- Event action
- Read by

Collector Configuration

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

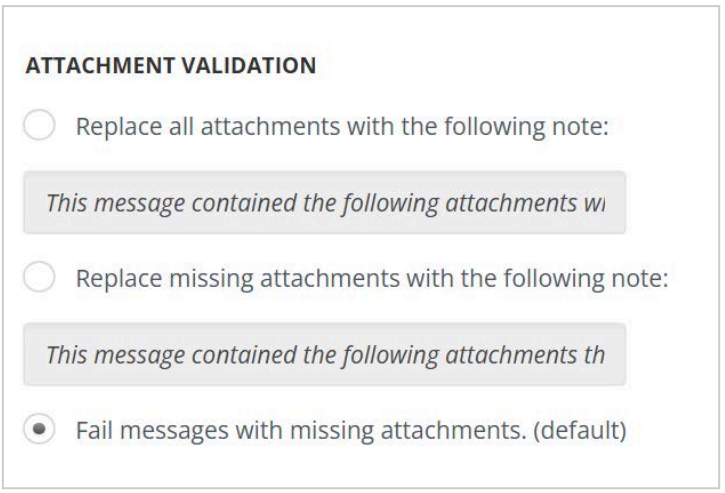
- **File Source**
- **Execute Script Against Source Files**
- **PGP Decryption**
- **Folders**
- **After Successful Importing**
- **Misc Settings**

Attachment Validation

Mergel enables you to develop customized notes for attachment validation.

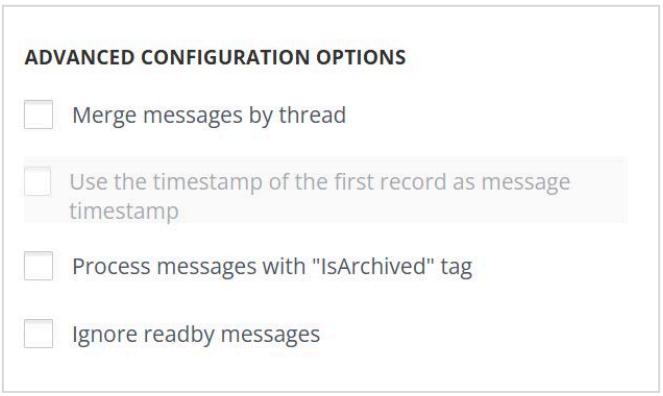
- If you select **Replace all the attachments with the following note** and input your custom note, all the attachments to the messages will not be processed and in their place under the **Reports**, you will see only the custom message that you have entered.

- If you select **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.
- The default setting is **Fail Messages with missing attachments**, so the messages that do not have attachments are failed and can be viewed under the **Reports**.



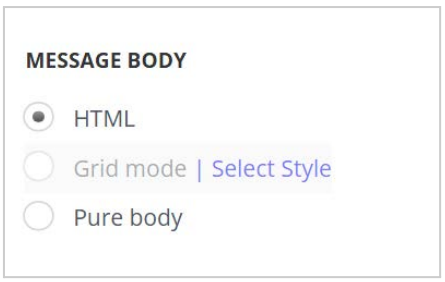
Advanced Configuration Options

- **Merge messages by thread**: If checked, 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 (*DownloadedBy* and *ReadBy*) to be added to the merged message.
- **Use the timestamp of the first record as message timestamp**: If checked, it uses the timestamp of the first Symphony message as a message timestamp, instead of one of the last messages. This option becomes active, only when **Merge messages by thread** is selected.
- **Process messages with "IsArchived" tag**: If checked, messages that have the *IsArchived* tag are processed as well.
- **Ignore readby messages**: If checked, messages with the *ReadBy* field in them will be ignored.



Message Body

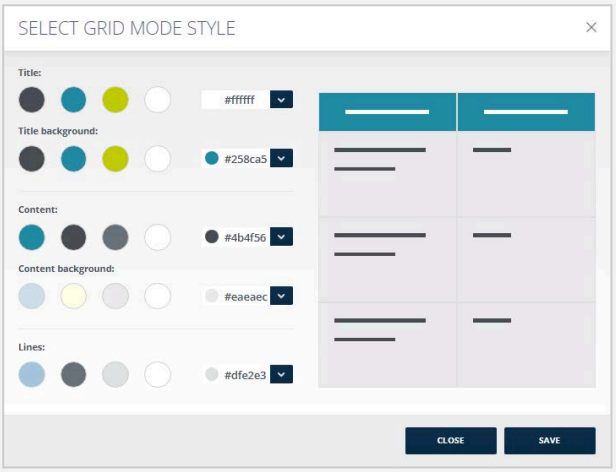
This setting determines how imported messages are displayed in the target. There are the following output message body options:



- **HTML**: If selected, the output message will be displayed in HTML format. The following additional checkboxes will appear for configuration, allowing the output message to include the following information:
    - *Downloaded by*
    - *Read by*
- **Grid mode**: Allows viewing output message content in a compact grid format. This option becomes active, only when **Merge messages by thread** is selected. The following additional checkboxes will appear for configuration, allowing the output message to include the following information:
    - *Downloaded by*
    - *Read by*
    - *Attachment*
    - *Event action*
- **Pure body**: Displays the output message as plain text, without formatting or additional details.

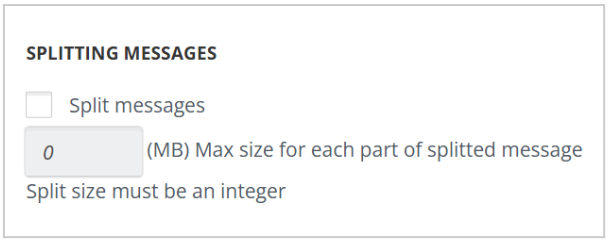
Tip

In **Grid mode**, the color scheme can be adjusted through the **Select Style** pop-up menu:



Splitting Messages

The **Splitting Messages** 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.

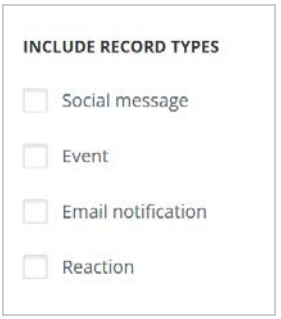


In case you have a limitation of 25 MB on your server, you must split your message max to 17MB as the server also must have space for some encryption and decryption tasks that are being carried out by Mergel.

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. The following types of records from Symphony can be chosen:

- **Social message**
- **Event**
- **Email notification**
- **Reaction**

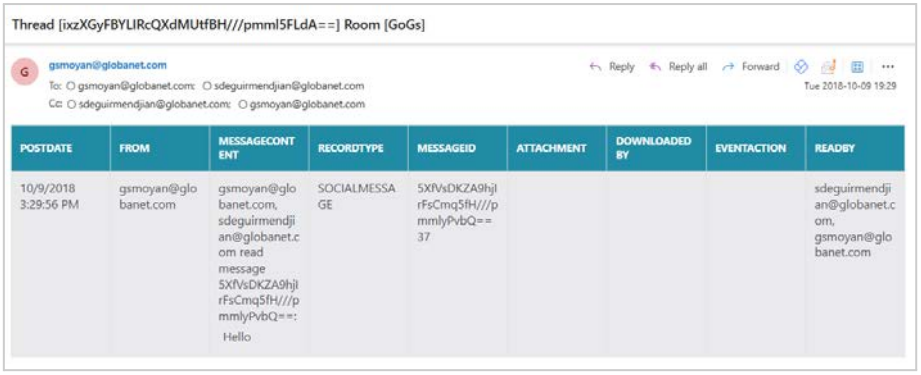


Next Steps

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

- Monitored Users (N/A)
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:


Thread [ixzXGyFBYLIRcQXdMUtfBH///pmml5FLdA==] Room [GoGs]

gsmoyan@globanet.com

To: gsmoyan@globanet.com; sdeguirmendjian@globanet.com
Cc: sdeguirmendjian@globanet.com; gsmoyan@globanet.com

Reply Reply all Forward

Tue 2018-10-09 19:29

POSTDATE	FROM	MESSAGECONTENT	RECORDTYPE	MESSAGEID	ATTACHMENT	DOWNLOADEDBY	EVENTACTION	READBY
10/9/2018 3:29:56 PM	gsmoyan@globanet.com	gsmoyan@globanet.com, sdeguirmendjian@globanet.com read message 5XfVsDKZA9hjlrFsCmq5fH///pmmlyPvbQ==: Hello	SOCIALMESSAGE	5XfVsDKZA9hjlrFsCmq5fH///pmmlyPvbQ==37				sdeguirmendjian@globanet.com, gsmoyan@globanet.com

Supported Notifications

The importer supports the following notification preferences:

- **Quarantine file**
- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

Text-Delimited

Merge1 Text- Delimited is designed to allow rapidly developing text-delimited file processing. The collector aims to map the text-delimited fields to the required format. The mapping is done based on the uploaded XML template. It varies from source to source and 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 activities can contain:

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

Note

- To process the attachments, add the full path to each attachment in the CSV document. We recommend creating attachments with a folder structure to prevent files with similar names from clashing to avoid files with similar names shared on different days and in different conversations.
- The CSV/TXT and the ZIP files should have the same name to process the files properly.

Collector Configuration

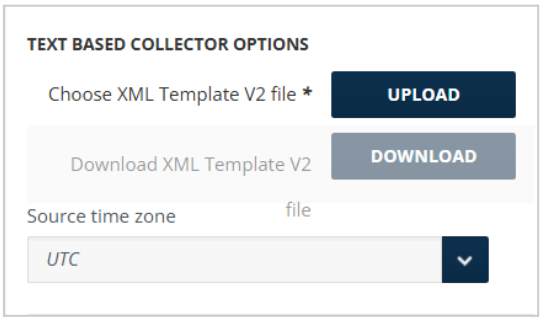
For information on how to configure the following sections of the **Source** tab, see:

- **File Source**
- **Execute Script Against Source Files**
- **PGP Decryption**
- **Folders**
- **After Successful Importing**
- **Misc Settings**

Text-Based Collector Options

- Upload an XML template. The XML file should include details about the file, such as *headers*, *number of columns*, *delimiter type*, and *text qualifier*. The next section of the XML file should define *column names*, *data type*, and whether columns are optional. Finally, it should map the columns to expected data fields like *From/Sender*, *To*, *Subject/Title*, *Date/ActivityDateTime*, and *Body/Content*.

- If you want to manually set up the **Source time zone**, select the relevant one from the drop-down list. By default, Mergel sets the **Source time zone** as **UTC**.
  The **Source time zone** setting will attempt to retrieve the time zone from the data itself automatically.



Message Body

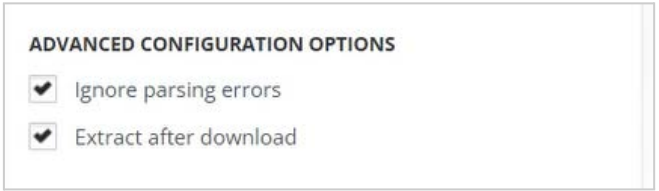
This setting determines how imported messages are displayed in the target. There are the following output message body options:

- **Plain**: Displays the message in a simple text format.
- **Light grid mode**: Displays data in a two-toned layout, making it visually distinct and easier to view while displaying limited metadata.

Advanced Configuration Options

Ignore parsing error: When checked, the importer continues running when corrupted/unexpected lines occur or when attachments are missing, logging a warning in the logs. Otherwise, it stops running and an exception is thrown.

Extract after download: When enabled, the collector automatically unpacks ZIP archives that are not part of a paired file group (TXT+ZIP or CSV+ZIP). If the option is disabled, Mergel will automatically quarantine the files.



XML Template Configuration Guideline

To configure the XML template sample:

1. Configure the information about the file itself: if the file contains *headers*, *number of columns*, *delimiter type*, *text qualifier*, and *attachment method* [47].

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <version>TD_3.0</version>
    <options>
        <containsHeader>Yes</containsHeader>
        <maxCols>6</maxCols>
        <delimiter>","</delimiter>
        <text_qualifier>"</text_qualifier>
        <attachmentMethod>Archive</attachmentMethod>
        <content_type>Html</content_type>
    </options>
```

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

```
    <columns>
        <column>
            <order>1</order>
            <name>Date</name>
            <datatype>DateTime</datatype>
            <datatype_options>
                <format>XX/DD/YYYY HH:MM</format>
            </datatype_options>
        </column>
        <column>
            <order>2</order>
            <name>From Email</name>
            <datatype>String</datatype>
        </column>
        <column>
            <order>3</order>
            <name>To Email</name>
            <datatype>String</datatype>
        </column>
        <column>
            <order>4</order>
            <name>Subject</name>
            <datatype>String</datatype>
        </column>
        <column>
            <order>5</order>
            <name>Body</name>
            <datatype>String</datatype>
        </column>
        <column>
            <order>6</order>
            <name>FILE_NAME</name>
```

[47] Note that if you want attachments to be processed properly, they should be in the same zipped folder and have the **attachments.zip** format.

```
            <datatype>StringList</datatype>
            <datatype_options>
                <delimiter>";"</delimiter>
                <append>""<append>
            </datatype_options>
        </column>
    </columns>
```

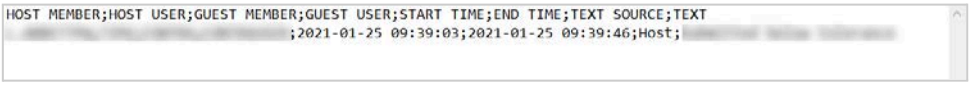
3. The last part of the XML file maps the columns to the expected data fields: *Sender*, *Participants*, *Title*, *ActivityDateTime*, *Body* and *Threading* [48]:

```
<mappings>
    <mapping can_be_empty = "Yes">
        <property>Sender</property>
        <items>
            <item>From Email</item>
        </items>
    </mapping>
    <mapping can_be_empty = "Yes">
        <property>Participants</property>
        <items>
            <item Role="To">To Email</item>
        </items>
    </mapping>
    <mapping can_be_empty = "Yes">
        <property>Title</property>
        <items>
            <item>Subject</item>
        </items>
    </mapping>
    <mapping can_be_empty = "Yes">
        <property>Content</property>
        <items>
            <item>Body</item>
        </items>
    </mapping>
    <mapping can_be_empty = "Yes">
        <property>ActivityDateTime</property>
        <items>
            <item>Date</item>
        </items>
    </mapping>
    <mapping can_be_empty = "Yes">
        <property>Attachments</property>
        <items>
            <item>FILE_NAME</item>
        </items>
    </mapping>
    <mapping can_be_empty = "Yes">
```

[48] Only if threading is required.

```
            <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>
```

Example of a source TXT file:

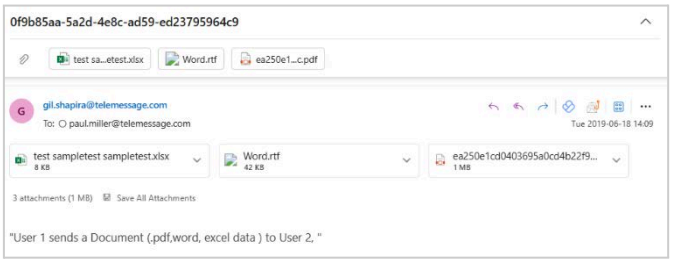


Next Steps

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

- Monitored Users (N/A)
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Quarantine file**
- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

UBS

UBS provides financial advice and solutions to private, institutional, and corporate clients worldwide.

Activities Captured

- Messages

Captured activities can contain:

- Datetime
- First name
- Last name
- Company name
- Says
- Content
- Participant's full name
- Email
- User ID

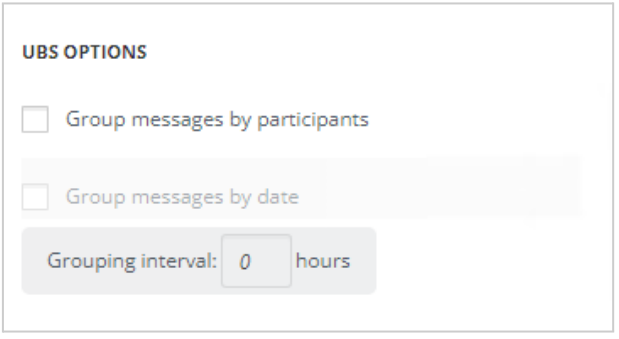
Collector Configuration

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

- **File Source**
- **Execute Script Against Source Files**
- **PGP Decryption**
- **Folders**
- **After Successful Importing**
- **Misc Settings**

UBS Options

Mergel 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 intervals. The time is calculated in hours.

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**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:

Supported Notifications

The importer supports the following notification preferences:

- **Quarantine file**
- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

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 **Merge1 Verba 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

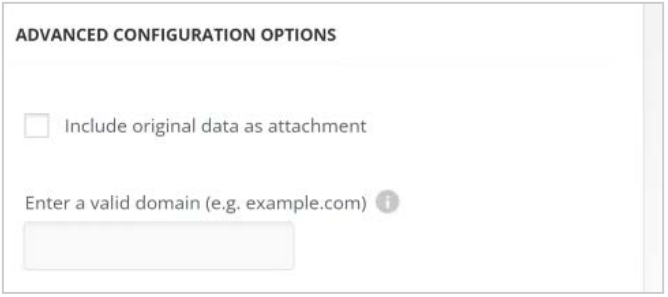
Collector Configuration

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

- **File Source**
- **Execute Script Against Source Files**
- **PGP Decryption**
- **Folders**
- **After Successful Importing**
- **Misc Settings**

Advanced Configuration Options

- **Include original data as attachment**: If enabled, the CSV file will be attached to the output message.
- **Enter a valid domain (e.g. example.com)**: If specified, and a user lacks an email address, Merge1 will generate one by using the domain and the user's phone number, ensuring a valid email format for processing.

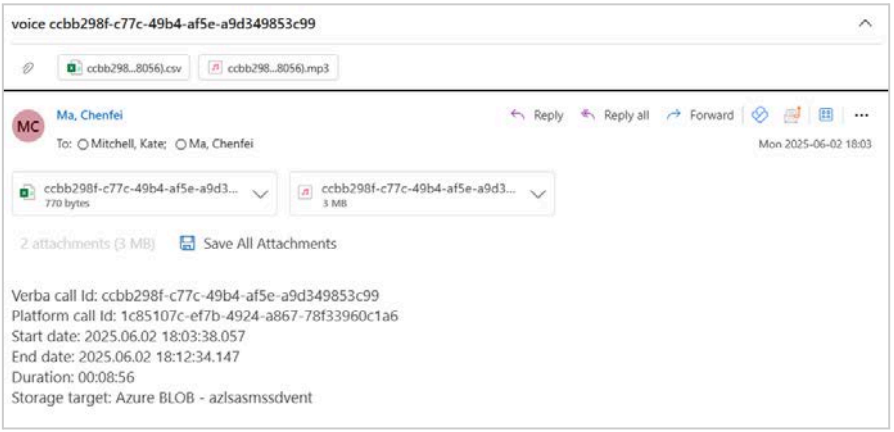


Next Steps

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

- Monitored Users (N/A)
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Quarantine file**
- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

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 **Merge1 Verint collector** is a file-based collector to parse Avaya and Cisco call XML formatted interaction file sources.

Activities Captured

- Recorded calls

Captured activities can contain:

- Call start time (as a timestamp)
- Call duration
- Audio attachment files in WAV format
- Subject
- Participants
- Message body

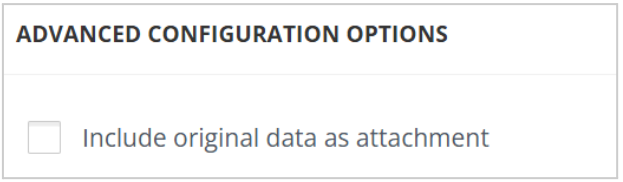
Collector Configuration

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

- **File Source**
- **Execute Script Against Source Files**
- **PGP Decryption**
- **Folders**
- **After Successful Importing**
- **Misc Settings**

Advanced Configuration Options

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

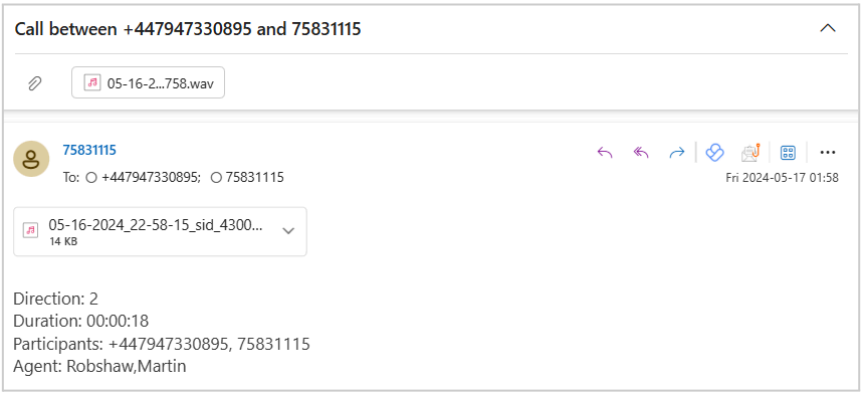


Next Steps

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

- Monitored Users (N/A)
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Quarantine file**
- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

Viva Engage (Yammer)

Viva Engage (formerly Yammer) is an enterprise collaboration platform within Microsoft 365, designed to spark meaningful conversations, enhance teamwork, and streamline project management. It fosters an engaging work environment, ensuring effective communication and knowledge-sharing across organizations.

The **Mergel Viva Engage (Yammer) 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 to posts in public and private groups
- Private messages[49]
- Attachments (including SharePoint files)
- Edit activities of posts/comments/replies/private messages
- Polls[50] [51]
- Praises (the text of the praise and the replies)
- Announcements (the text of the announcement and replies)
- Deleted private messages, posts, and comments (including attachments)[52]

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 a message is GDPR hard deleted, any attachments it contained cannot be retrieved due to the source limitations.
- A dummy SMTP address is generated for a deleted message missing the **`deleted_by_id`** field.
- Both 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. For more details on enabling Legal Hold, see **Enable In-Place Hold**.
- When sharing an already existing file from SharePoint, the attachment is not captured—only the URL of that attachment is retrieved.
- The created message does not say it was deleted from Viva Engage. To capture the deletes, the data retention setting needs to be set to *Delete*. Instructions can be found here.

[49] Unless the conversation has been started by an external user.

[50] Votes are not captured.

[51] The poll options for deleted polls are displayed on the same line.

[52] The delete event of the message/post will be captured in case there is a create/edit activity before the Mergel run.

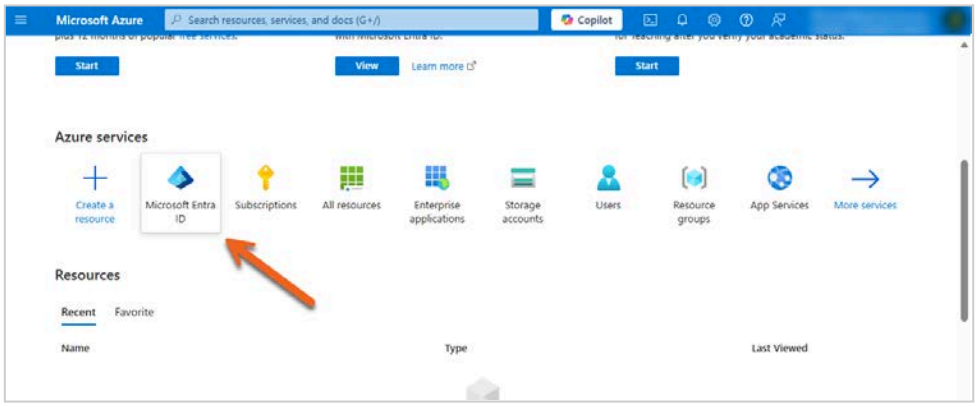
- Events from former members are not captured due to limited permissions associated with admin-generated tokens.
- For files larger than 2 GB, a link to the attachment will be created and included in the body of the output message, along with a log warning noting the file exceeds 2 GB.
- When running two or more collectors simultaneously, a separate Import folder path should be provisioned on the Source Configuration tab for each collector.
- 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 Mergel run process.

Creating a Microsoft Entra ID Application

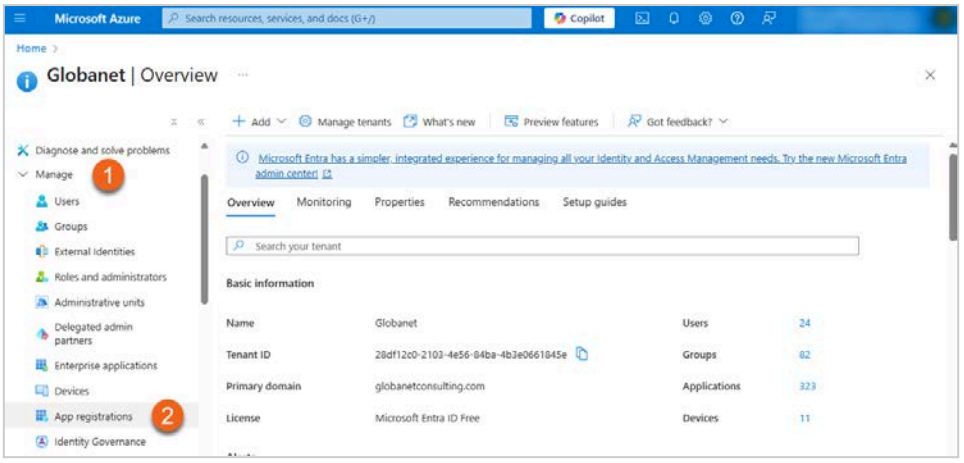
The Office 365 or Azure administrator in your organization must complete the steps detailed in the sections below.

Registering an Application

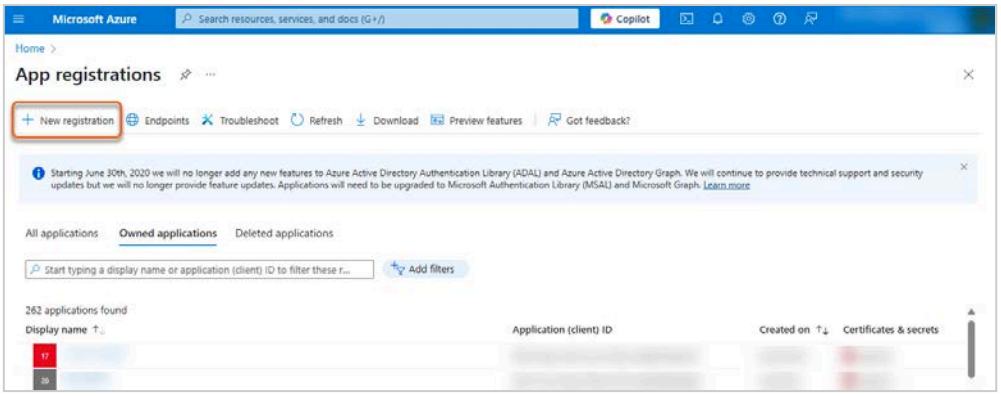
1. Sign in to Azure Portal.
2. Select **Microsoft Entra ID** under **Azure services**.



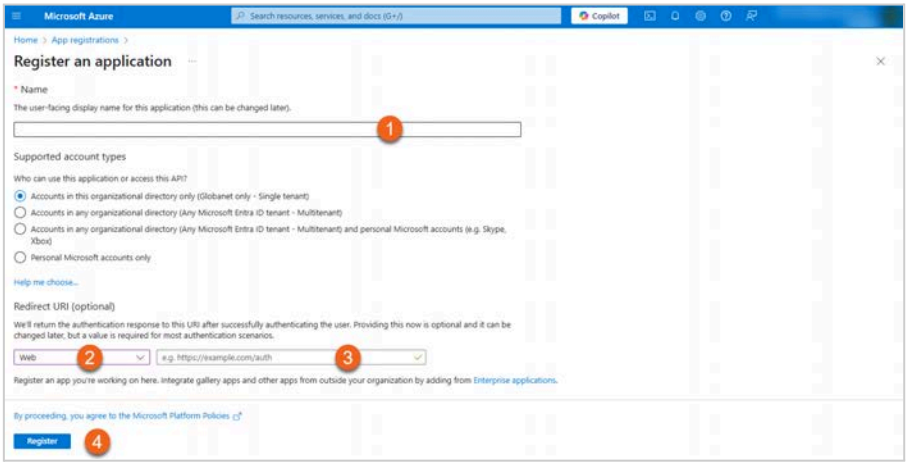
3. In the left-hand navigation pane, click **Manage > App registrations**.



6. Click **New registration**.



7. To register an application:
   7.1. Enter a **Name** for the application.
   7.2. Select **Web** under **Redirect URI (optional)**.
   7.3. Add the URL of your local Merge1 environment in the following format: `https://<merge1_instance>/Configuration/OAuthCallback`.
   7.4. Click **Register**.



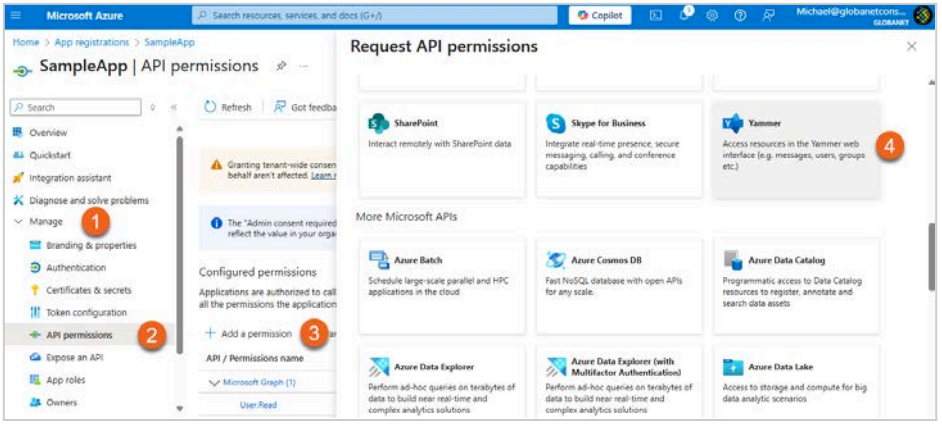
8. An **Application (client) ID** and **Directory (tenant) ID** will be generated. Keep both for configuring the collector in Mergel.

Granting Permissions

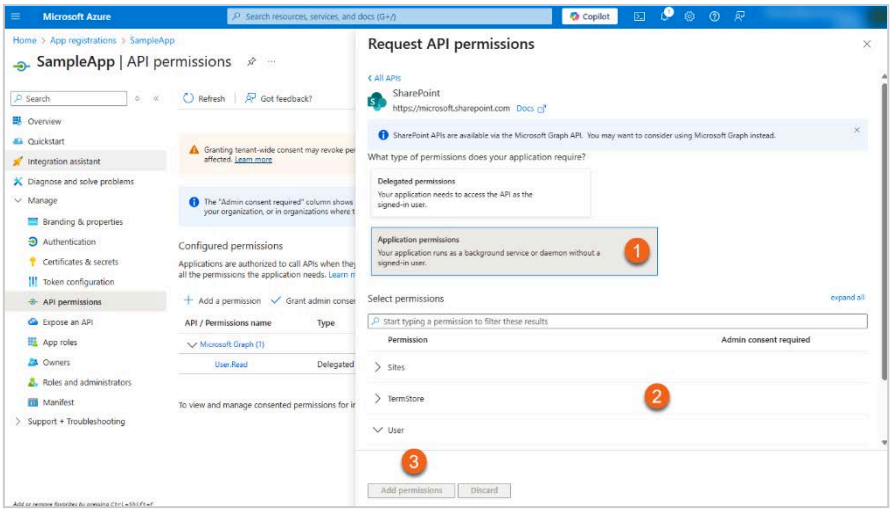
Adding Yammer API Permissions

To add **Yammer** API permissions:

1. In the left-hand navigation pane, click **Manage > API permissions**.
2. Click **Add a permission**.
3. In the opened pane, select the **Yammer** API.



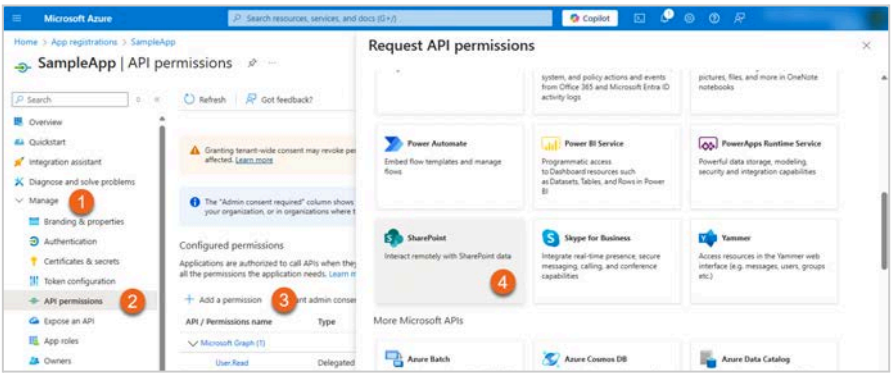
4. To add the necessary permission:
   4.1. Click **Delegated permissions**.
   4.2. Add the following permission: **Other permissions**: *user_impersonation*.
   4.3. Click **Add permissions**.



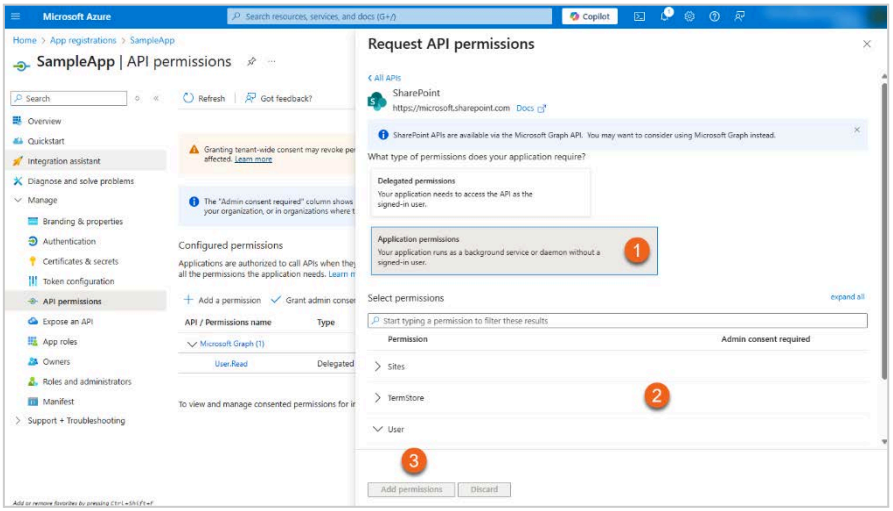
Adding SharePoint API Permissions

To add **SharePoint** API permissions:

1. In the left-hand navigation pane, click **Manage > API permissions**.
2. Click **Add a permission**.
3. In the opened pane select the **SharePoint** API.

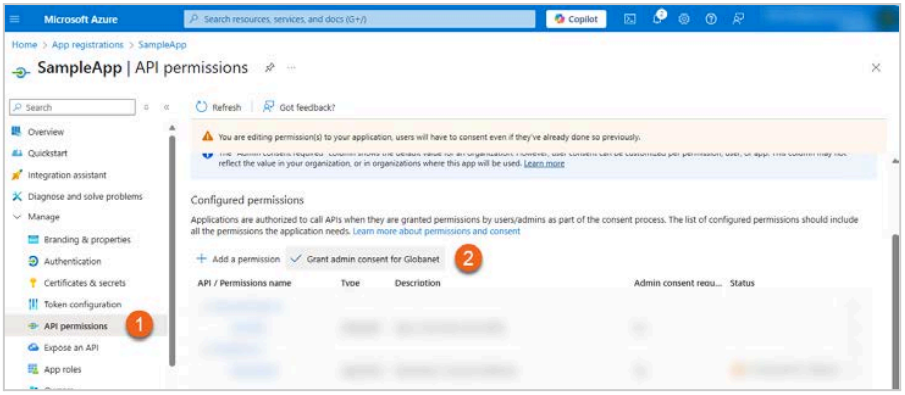


4. To add the necessary permission:
   4.1. Click **Application permissions**.
   4.2. Add the following permission: **Sites**: *Sites.Read.All*.
   4.3. Click **Add permissions**.



Granting Admin Consent

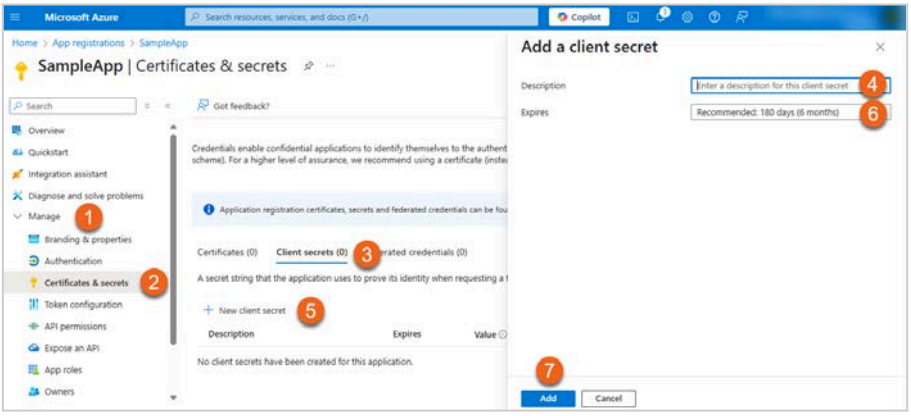
1. Go back to **API permissions**.
2. Click **Grant admin consent** for your company to grant the added permissions.



Adding a Client Secret

To add a new client secret:

1. In the left-hand navigation pane, go to **Manage > Certificates & secrets**.
7. Go to **Client secrets**.
8. Click **New client secret**.
9. Enter a **Description**.
10. Specify a **Duration**.
11. Click **Add**.

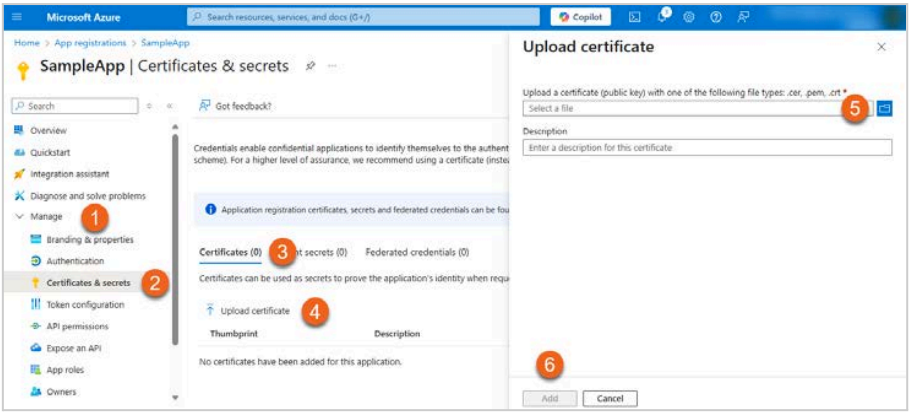


Keep the new client secret value for configuring the collector in Mergel.

Uploading a Certificate

To upload a certificate:

1. In the left-hand navigation pane, go to **Manage > Certificates & secrets**.
2. Select **Certificates**.
3. Click **Upload certificate**.
4. Select a certificate (public key) with one of the following file types: `.cer`, `.pem`, `.crt`.
5. Click **Add**.



A certificate **thumbprint** will be generated. Keep the value for configuring the collector in Merge1.

For more information on how to create a certificate, see **Creating a Certificate (Private and Public Keys)**.

Configuring the Collector in Merge1

Adding the Importer

For details on adding the importer, see **Adding a New Importer**.

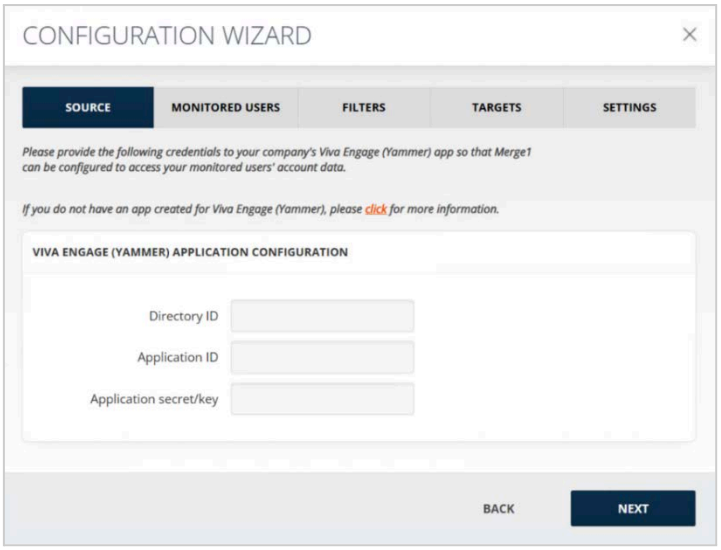
Source Configuration

For configuring the **Viva Engage (Yammer)** application:

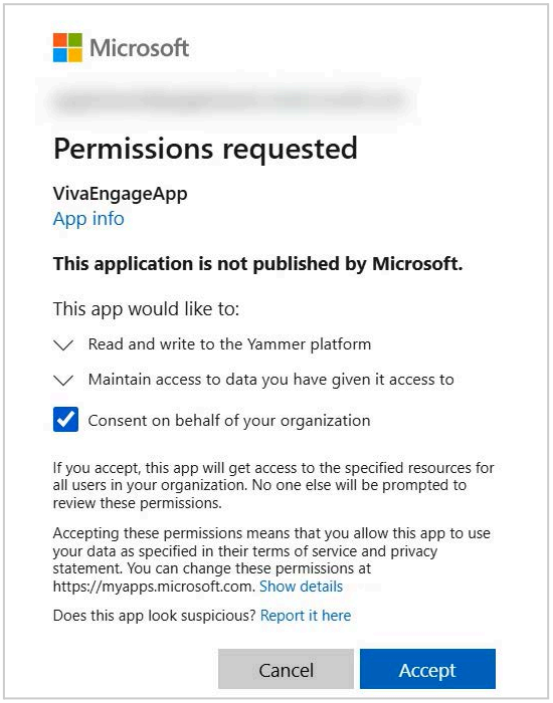
1. Add the previously saved *Directory (tenant) ID* and *Application (client) ID* in the **Directory ID** and **Application ID** fields, respectively.
2. Add the previously saved *client secret* value in the **Application secret/key** field.

> **Important**
>
> 1. To successfully authenticate with Merge1, the user must have a **Global Administrator Role** in the Azure Portal.
> 4. To use Merge1, the user must meet the following requirements:
>
> 4.1. **Yammer Administrator Role** assigned in the Azure Portal.
>
> 4.2. **Verified Administrator** in the Yammer Admin Portal.
>
> **Note:** These permissions must remain active and must not be removed while Merge1 is in use. Revoking or restricting access may result in importer run failure.

3. Click **Next**.



4. A pop-up window will appear (make sure that pop-ups are enabled in your browser). To allow the app to access the specified resources for all users in the organization:
   4.1. Select the **Consent on behalf of your organization** checkbox.
   4.2. Click **Accept**.



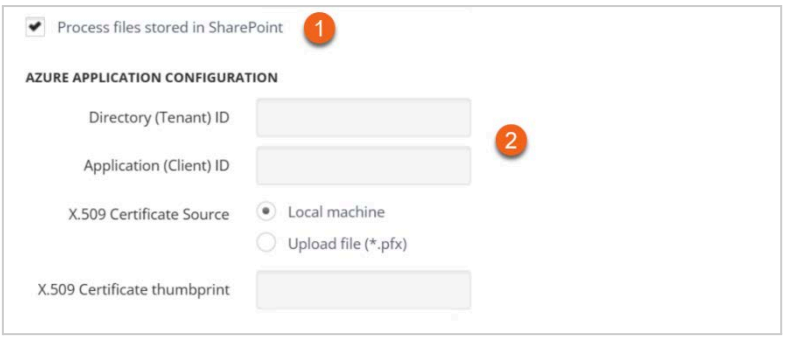
Viva Engage (Yammer) Configuration

Specify an **Import folder** in the host machine for storing temporary files. Merge1 needs an import folder to download, store and process data from Yammer. This is because Yammer's APIs are limited in their abilities to send and receive data. The import folder used for Yammer configuration must be empty for the importer to function correctly.

Azure Application Configuration

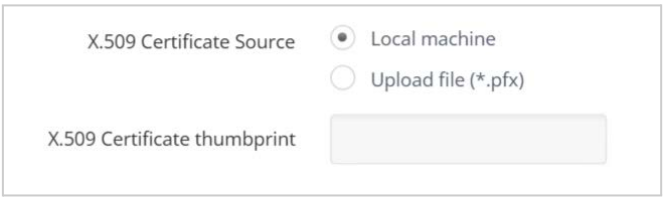
To capture SharePoint files:

1. Enable the **Process files stored in SharePoint** checkbox.
2. Add the previously saved *Application (client) ID* and *Directory (tenant) ID* values in the **Application (Client) ID** and **Directory (Tenant) ID** fields, respectively.

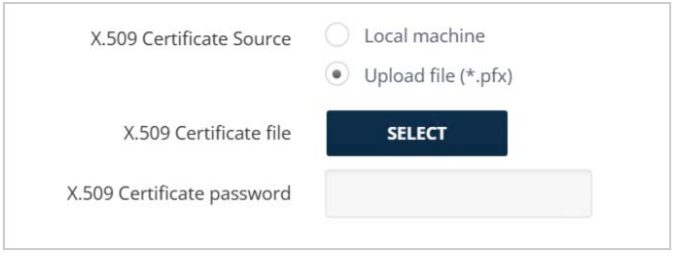


3. For **X509 Certificate** configuration:
   - Provide **X.509 Certificate thumbprint** in case you activate the **Local machine** radio button as the X.509 Certificate source.

   The **Certificate thumbprint** field will be auto populated in case the collector was previously configured by uploading a certificate.



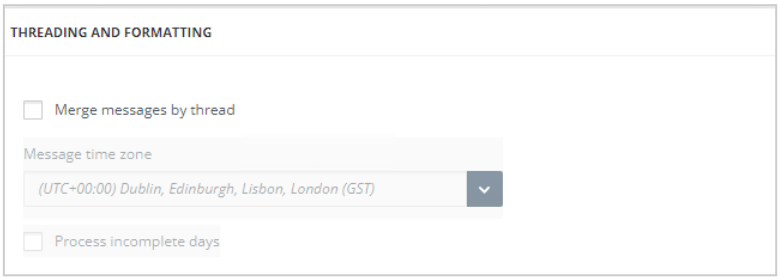
   - In case you activate **Upload file (*.pfx)**, click the **Select** button to upload the certificate provide **Password**.



Threading and Formatting

- **Merge messages by thread**: If checked combines messages by thread rather than sending them one by one.
    - **Message time zone**: The messages will be split by day with the specified time zone from the drop-down list.
    - **Process incomplete days**: If checked, the messages of the days that have not ended yet will be imported in a separate email.

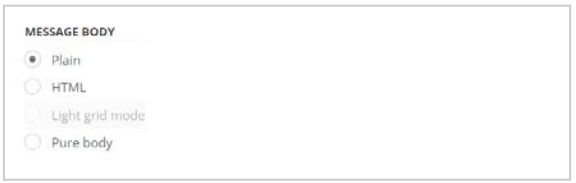
> **Note**
>
> **Message time zone** can be specified and/or the **Process incomplete days** checkbox can be enabled ONLY IF **Merge messages by thread** is checked.



Message Body

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

- **Plain**: Displays the message in a simple text format.
- **HTML**: Displays the message in HTML format.
- **Light grid mode**: Displays data in a two-toned layout, making it visually distinct and easier to view while displaying limited metadata.
- **Pure body**: Displays the output message as plain text, without formatting or additional details.



> **Notes**
>
> - The **Light grid mode** becomes active ONLY if **Merge messages by thread** is checked.
> - The **Pure body** option is active when **Merge messages by thread** is unchecked.
> - Formatted messages are captured as plain text.

Time Stamp Formatting

For more details on how to configure timestamps, see **Time Stamp Formatting**.

Advanced Configuration Options

For more details on how to configure advanced configuration options, see **Advanced Configuration Options**.

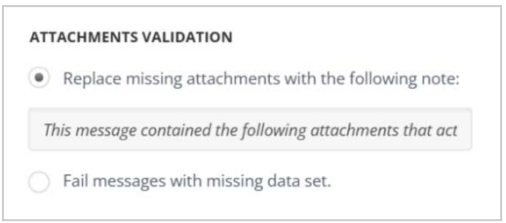
Content Capturing

In the **Content capturing** section, you can enable the corresponding option to capture *all content* or only *private content*.

Attachments Validation

Mergel enables you to develop customized notes for attachment validation.

- **Replace missing attachments with the following note**: Displays only the custom message entered, without processing missing attachments.
- **Fail messages with missing data set**: Marks messages without attachments as failed, making them viewable in the **REPORTS** section.



Attachments Configuration

- **Include original data as attachment**: If checked, the message original data is attached to the output file.
- **Ignore attachments**: If checked, all the attachments are excluded from the message enhancing the collector's performance. Each message will contain info and the link to the excluded attachment.

Otherwise, additional configurations will open for setup. See **Attachments Configuration**.

Splitting Messages

The **Splitting Messages** 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 the split message is set to 25 MB, and the original message is 65 MB, it will be split into 3 messages, each not exceeding 25 MB.

Next Steps

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

- **MONITORED USERS**
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:

Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**
- **No data captured**

- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

Web Page Capture

The Merge1 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

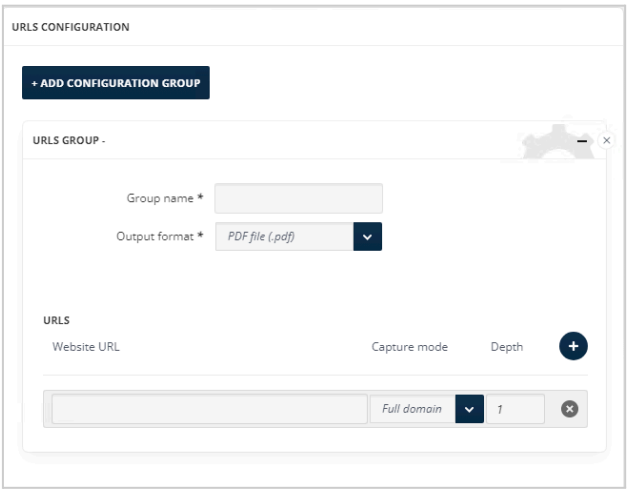
- Web page in PDF
- Web page in PNG
- Web page in custom formats

Heavy pages with a depth of capture greater than 1 may not be captured fully, as all the pages may not be loaded completely by the time of the capture.

Collector 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, please 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.



Time Stamp Formatting

For more details on how to configure timestamps, see **Time Stamp Formatting**.

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.

Advanced Configuration Options

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

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**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:

Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

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 Mergel 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
- Edited messages[53]
- Emojis
- Message replies
- Deleted messages for everyone[54]
- Mentions
- Documents (MS Word, MS Excel, PDF, PPT)
- Images
- Videos
- GIFs
- Links
- Music
- Apps from Store (App links)
- Drawing
- AI Imagine
- Stickers[55]
- Audio messages
- Reactions to messages
- Messages with images
- Messages with videos

Collector Configuration

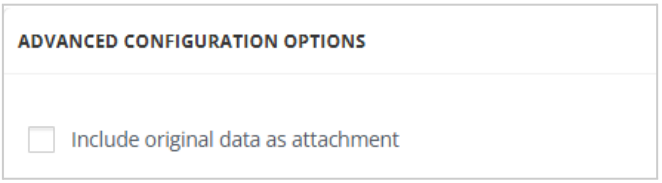
For information on how to configure the following sections of the **Source** tab, see:

- **File Source**
- **Execute Script Against Source Files**
- **PGP Decryption**
- **Folders**
- **After Successful Importing**
- **Misc Settings**

[53] Only the last version of edited messages is captured.
[54] Only the events are captured; the content of the message is not captured.
[55] Unknown sticker types are not captured.

Advanced Configuration Options

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

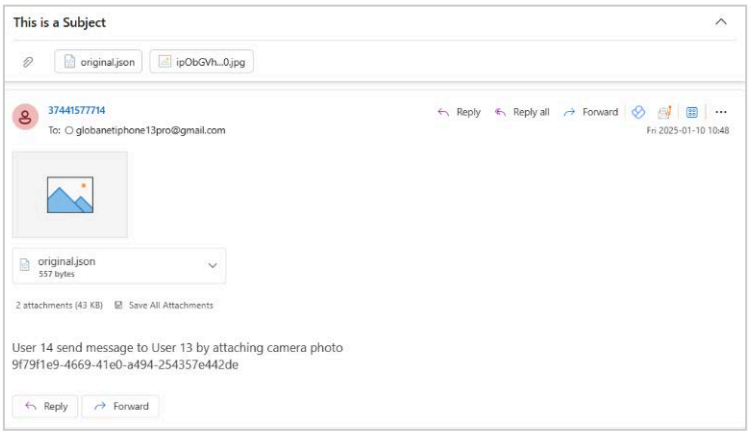


Next Steps

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

- Monitored Users (N/A)
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Quarantine file**
- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**

- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

Workplace from Facebook

Workplace is an enterprise connectivity platform developed by Facebook, Inc., featuring tools like groups, instant messaging, and News Feed. Workplace allows third parties to fetch data from its APIs for Compliance and eDiscovery purposes, which 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)[56]
  - "Add" events in group chats
- Posts:
  - Group posts (except multi-company groups, and main posts of buy & sell groups)
  - Attachments[57]
  - Polls (without attachments)
  - GIFs
  - Emojis
  - GIF posts (MP4 format only)
  - Likes & reactions to posts
  - Comments and replies[58]
  - 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

[56] If there is only one participant in the group chat, the deleted message/attachment is not captured.

[57] Workplace side internal server error occurs in case of having 80+ attachments.

[58] Specify the number of previous days (maximum 31) prior to the current run for Merge1 to scan for edits and new comments on a post.

- Check-ins
- Feeling/Activity
- Comments deleted
- Created events
- Hidden chats
- Posts created on someone's timeline
- Previous versions of posts

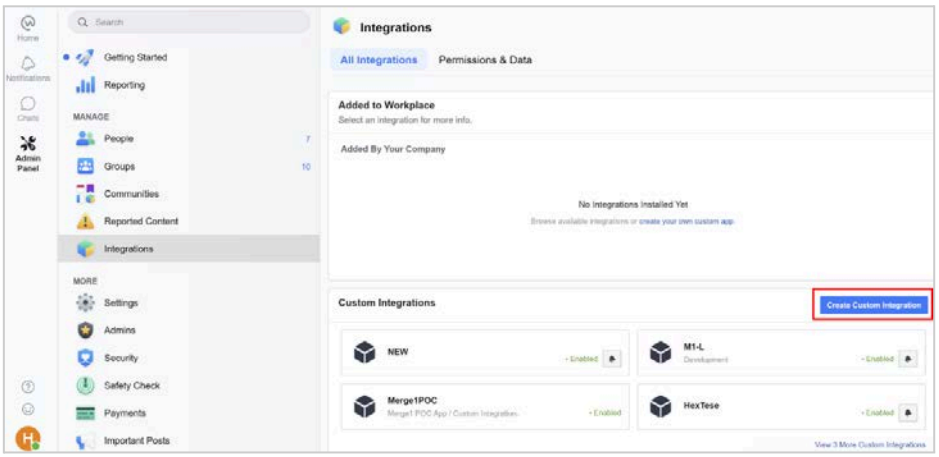
Custom Integration Creation in Workplace from Facebook

Workplace from Facebook allows third parties to fetch data from its APIs for Compliance and eDiscovery purposes - this is achieved by using Custom Integrations.

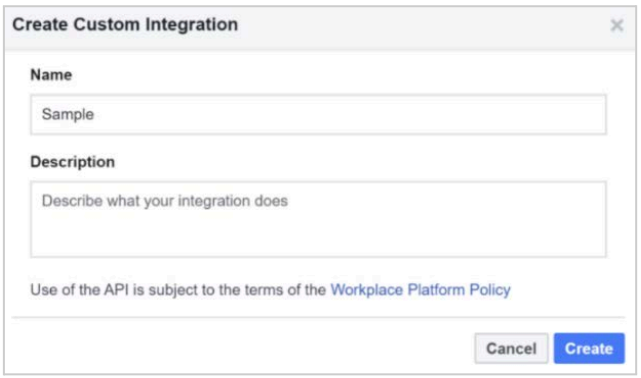
Custom Integrations are not available in free Workplace plans, so customers who need to meet Compliance and eDiscovery must have a Premium plan.

To create a custom integration:

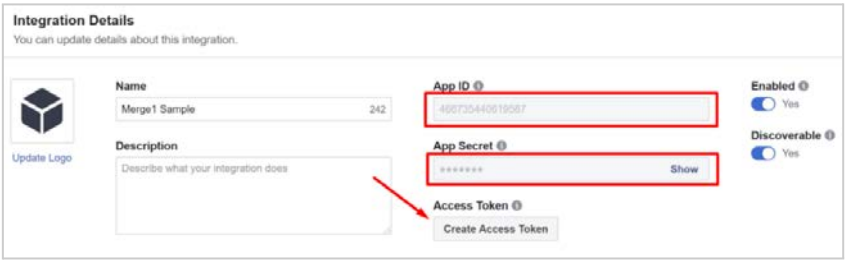
1. Login to the workplace using a **System Administrator** account.
2. Navigate to https://my.workplace.com/work/admin/apps/.
3. Sign in if prompted to.
4. Click **Create Custom Integration**.



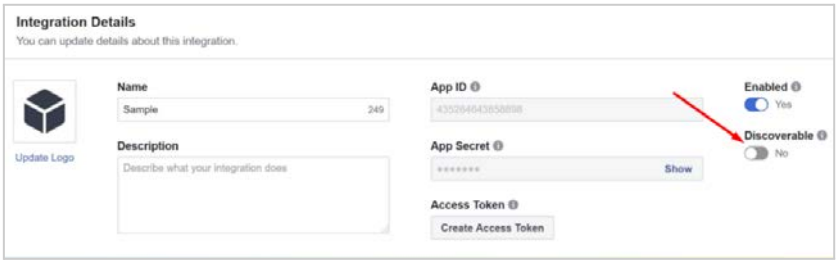
5. Enter a **name** for the Integration and click **Create**.



6. Copy **App ID** and **App Secret**. Click **Create Access Token** and copy the generated token.

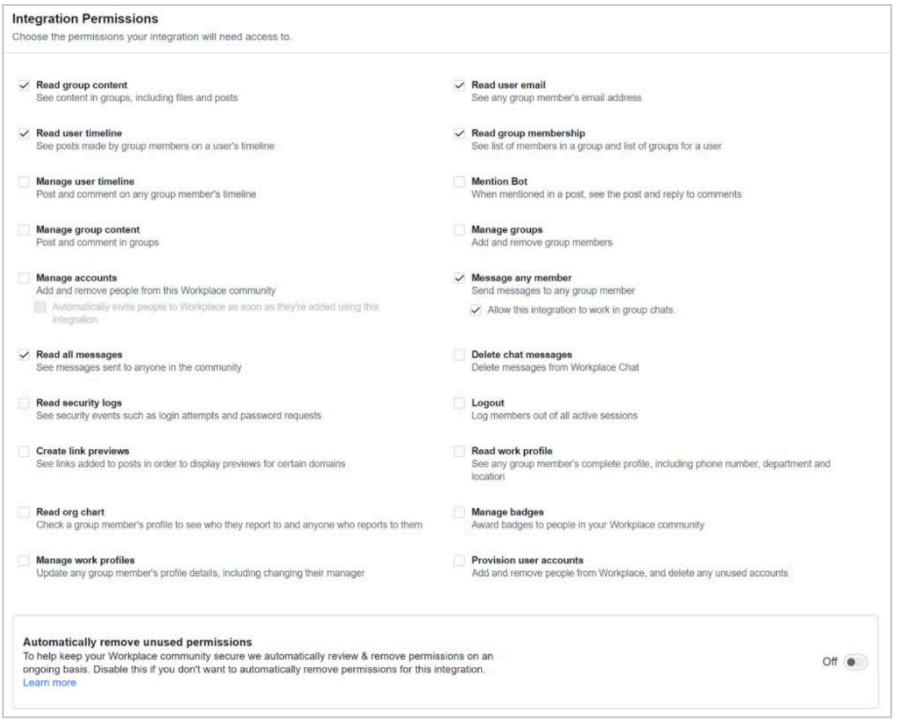


7. If **Discoverable** is set to **Yes**, change it to **No**. This is not required but it is best practice to make sure the users are not aware of existence of the application.



8. 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.

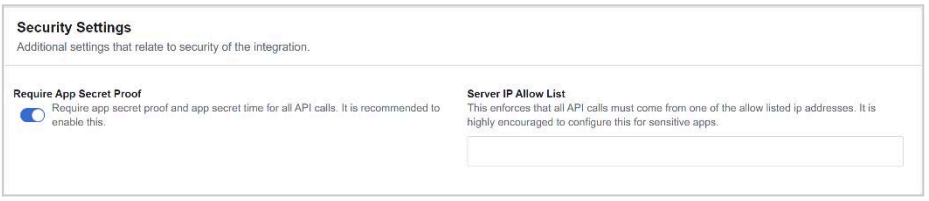


9. To make sure the permissions remain available for Merge1, disable **Automatically remove unused permissions**. This is not required; you can leave it on for better security, but you might need to come back to this page and re-add the permissions.

   Note that Facebook allows you to scope the App's permissions to specific groups.

   This is recommended if you only need to monitor users of certain groups.

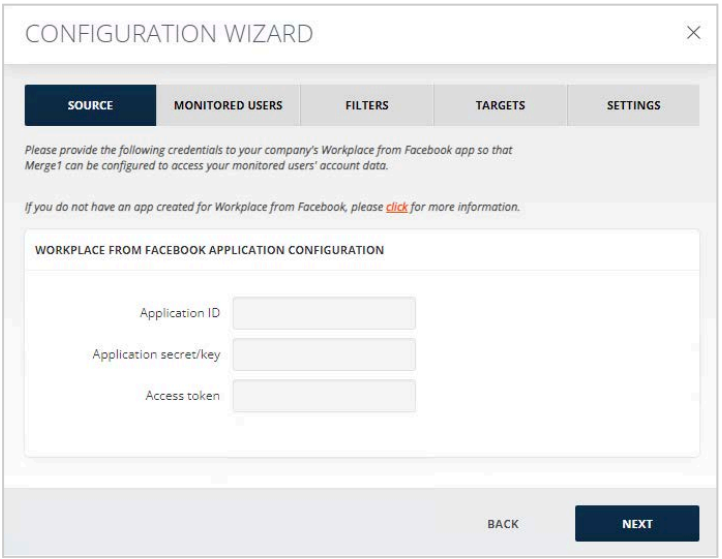
10. Enable **Require App Secret Proof** and allow list the public **IP** addresses of your Merge1 server(s), gateways and/or proxy server(s).



Collector Configuration

To configure the collector:

1. Enter the **App ID** copied in the Step 6 of the previous section in the **Application ID** field, the **App Secret** in the **Application Secret/Key** field, and the **Access Token** in the **Access Token** field.



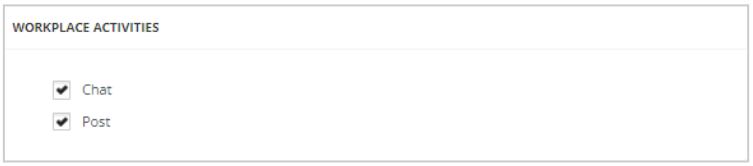
2. Click **Next**.

Workplace Activities

There are the following types of activities which can be captured with the collector:

- Chat

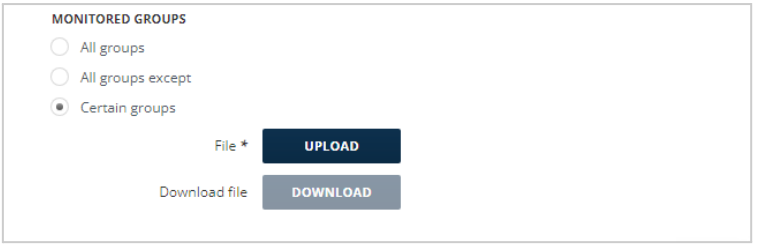
- Post



Enabling the **Chat** or/and **Post** checkboxes will process the activities from Chats or/and Posts.

To set up **Monitored Groups**:

1. Enable **All groups**, to capture content from all groups.
2. Enable **All groups except** and upload the list of monitored users in a CSV format to capture content from all users except the uploaded ones in the file.
3. Enable **Certain groups** and upload the list of monitored users in a CSV format to capture content from the users in the uploaded file.



Time Stamp Formatting

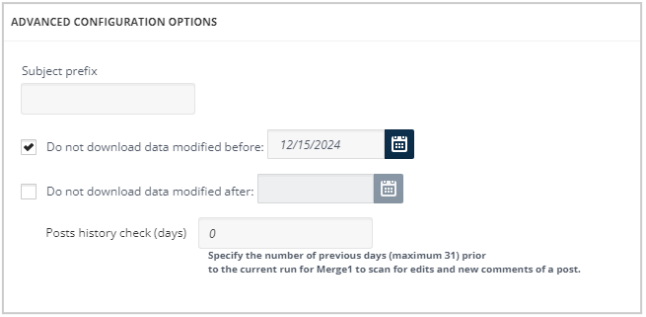
For more details on how to configure timestamps, see **Time Stamp Formatting**.

Attachments Configuration

For more details on how to configure attachments, see **Attachments Configuration**.

Advanced Configuration Options

- For more details on how to configure advanced configuration options, see **Advanced Configuration Options**.
- Specify the number of the previous days (0-31) prior to the current run so that Merge1 can scan for edits and new comments on a post.

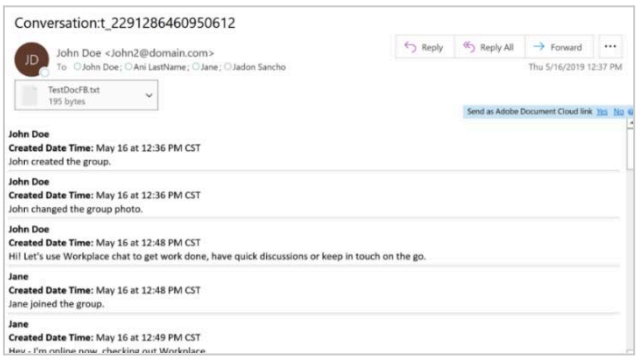


Next Steps

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

- **MONITORED USERS**
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

X (Twitter)

X, formerly referred to as Twitter, is a social media website based in the United States. It is an online news and social networking site where people communicate in short messages called tweets.

> **Note**
>
> X (Twitter) business/professional accounts are not supported.

Activities Captured

- GIFs captured as links
- Attachments captured as links
- Replies
- Reposts
- Quoted posts
- Emojis
- Timeline posts
- Poll post note (poll options are not captured)

Note that follows, direct messages, and deleted posts are not captured.

Creating an X (Twitter) Application

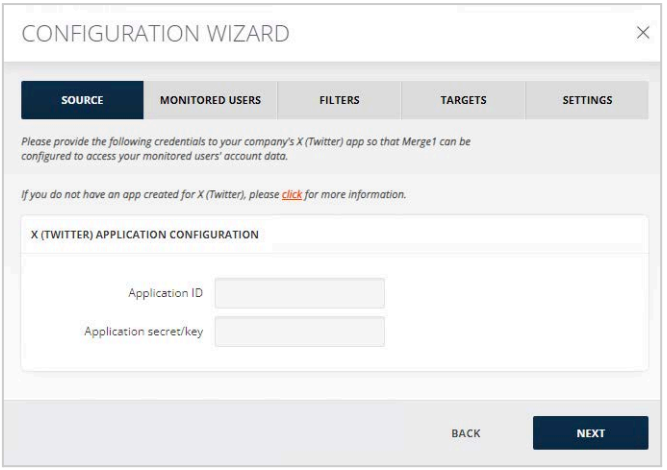
To create an X (Twitter) app:

1. Log in to https://developer.x.com/en.
2. Click **Create New App**.
3. Complete the form by:
   3.1. Providing a name for the application, i.e.," Mergel X (Twitter) App".
   3.2. Entering the URL of your organization's website.
   3.3. Entering the URL of your local Mergel environment with the following format: `https://mergel_instance/Configuration/OAuthCallback`.
   3.4. 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.

Collector Configuration

To create the X (Twitter) importer, fill in the following information in the **Configuration Wizard** of the **Source** tab:

1. Provide your X (Twitter) **Application ID.**
2. Enter the Application Secret/Key.
3. Click **Next**.



Time Stamp Formatting

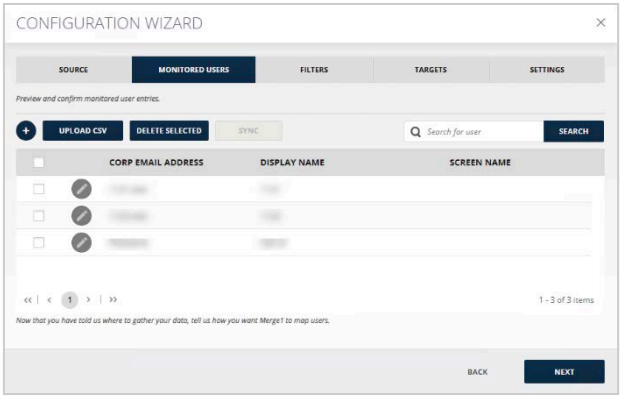
For more details on how to configure timestamps, see **Time Stamp Formatting**.

Advanced Configuration Options

For more details on how to configure advanced configuration options, see **Advanced Configuration Options**.

Monitored Users

Here the user can add, edit, and delete the listed monitored users or browse among them by searching the users.

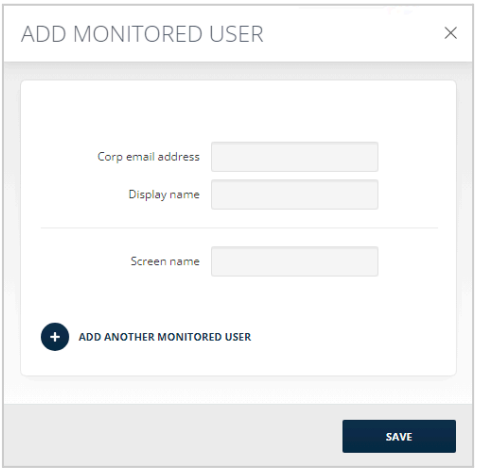


The following activities can be performed:

1. When **+** (Add Monitored User Manually) is chosen, the **Add Monitored User** pop-up opens to fill the following fields:
    1.1. **Corp email address.** The email address of the user to be monitored. It is used for the output message construction. This field is a required field.
    1.2. **Display name.** The display name of the user to be monitored. It is used to print the monitored user's display name in the output message. This field is not a required field. If the field is not filled when adding a monitored user, the X name is captured as the display name.

1.3. **Screen name.** The username of the user to be monitored. It is used to find the monitored user in X. This field is a required field.

> **Note**
>
> The user's posts are captured by the screen name, not by the email address.



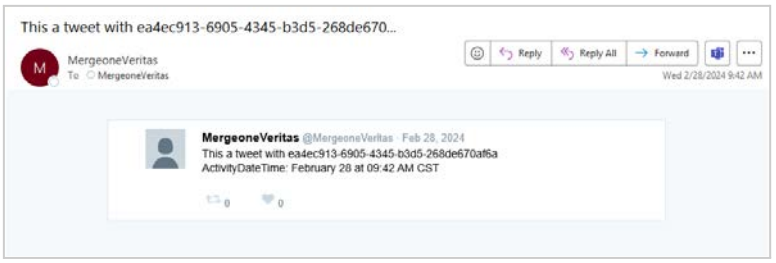
2. Click **Upload CSV** for uploading the Monitored users' list as a CSV.
3. Click **Delete selected** for deleting the below selected list of monitored users.

Next Steps

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

- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**

- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

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.

Collector Configuration

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

- **File Source**
- **Execute Script Against Source Files**
- **PGP Decryption**
- **Folders**
- **After Successful Importing**
- **Misc Settings**

XIP Collector Options

If you want to manually set up the **Source time zone**, select the relevant one from the drop-down list.

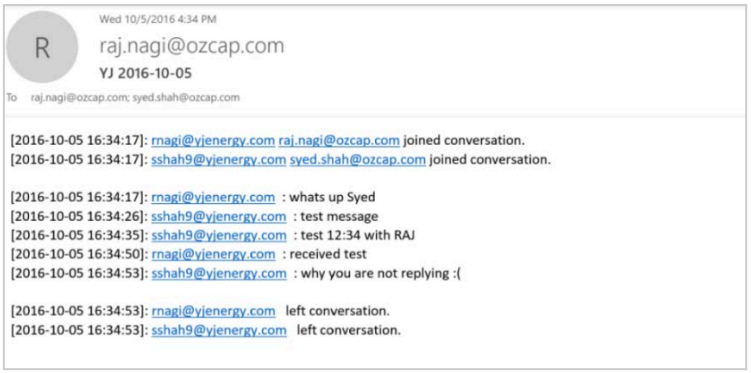
Provide the **Source time zone** information. Mergel assumes that the messages in the source file are of the set time zone, and based on that data, the dates in the messages are processed to the UTC time zone. By default, Mergel sets the **Source time zone** as **UTC**.

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**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Quarantine file**
- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

XSLT/XML

Mergel XSLT/XML collector allows our customers to rapidly transform an XML file using XSLT to a predefined format. Once the XML is transformed, Mergel can process it by generating the required mapping "From" "To," "Subject," "Date," and "body" fields to appropriate elements of the XML file. The mapping varies from source to source and must be written separately. Contact Artcera Support to get the template and the signature file corresponding to the source you are going to use it for.

Activities Captured

- Messages

Captured activities can contain:

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

Collector Configuration

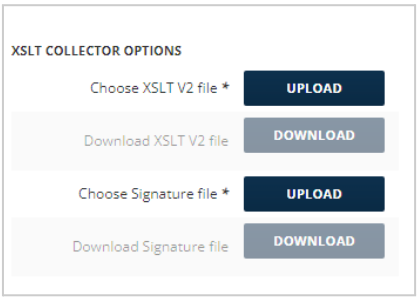
For information on how to configure the following sections of the **Source** tab, see:

- **File Source**
- **Execute Script Against Source Files**
- **PGP Decryption**
- **Folders**
- **After Successful Importing**
- **Misc Settings**

XSLT/XML Collector Options

To configure the section:

1. Upload the signed XSLT template.[59]
2. Upload the Signature file.



[59] Templates must be reviewed and cryptographically signed by Arctera LLC.

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**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:

TommySou - Tony Zhu@摩根大通 JP Morgan-UAT

TommySou@wechat.jpmorganclient.com

To: TommySou@wechat.jpmorganclient.com; Tony Zhu@摩根大通 JP Morgan-UAT

Fri 2022-09-23 05:23

Conversation Type: Chat
Conversation Start Date: 2022-09-23-05.23.17.231
Conversation End Date: 2022-09-23-05.31.11.728

Sent time	From	Message	Attachment
2022-09-23-05.23.17.231	TommySou@wechat.jpmorganclient.com	Testing	
2022-09-23-05.30.14.856	tony.x.zhu@jpmorgan.com	Ok	
2022-09-23-05.30.31.011	tony.x.zhu@jpmorgan.com	Let me know if u need others t also generate content	
2022-09-23-05.31.11.728	TommySou@wechat.jpmorganclient.com	Sure! Thank you Tony!	

Supported Notifications

The importer supports the following notification preferences:

- **Quarantine file**
- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

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 unrivaled liquidity and coverage of the AUD and NZD debt capital markets. Merge1 Yieldbroker collector processes data from Yieldbroker messages.

Activities Captured

- Messages

Captured activities can contain:

- 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

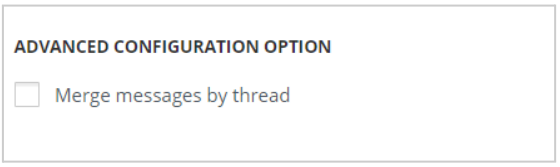
Collector Configuration

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

- **File Source**
- **Execute Script Against Source Files**
- **PGP Decryption**
- **Folders**
- **After Successful Importing**
- **Misc Settings**

Advanced Configuration Options

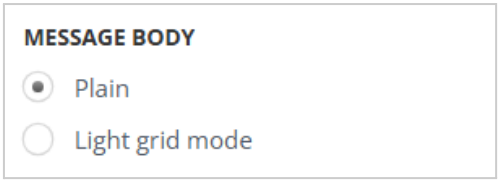
The **Merge messages by thread** option combines all messages from a thread into a single message.



Message Body

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

- **Plain**: Displays the message in a simple text format.
- **Light grid mode**: Displays data in a two-toned layout, making it visually distinct and easier to view while displaying limited metadata.

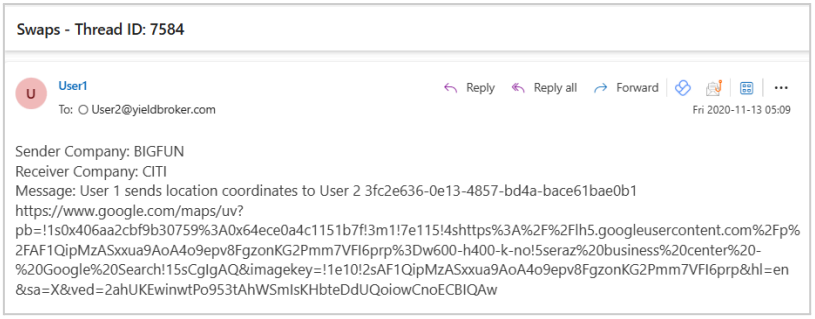


Next Steps

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

- Monitored Users (N/A)
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Quarantine file**
- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

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 that the deleted comments and replies are not captured due to the YouTube API limitations.

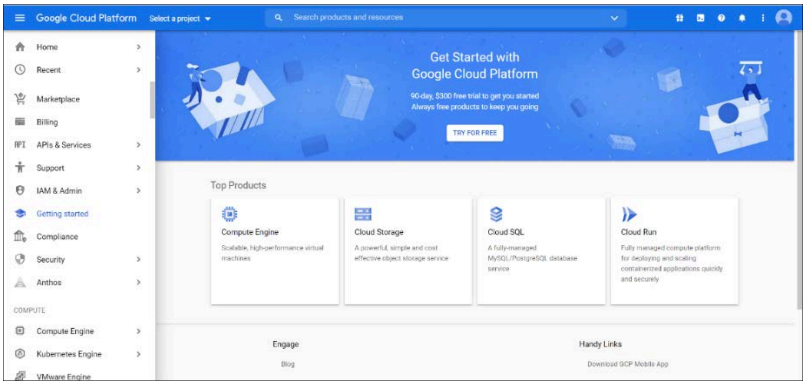
Creating a YouTube Application

To create a YouTube application, the user should create a new project, create credentials, and manage domain-wide authority delegations.

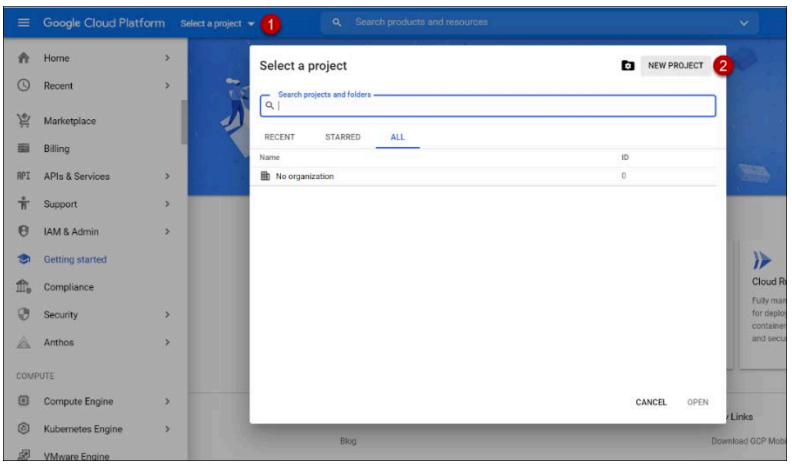
Creating a New Project

To create a new project:

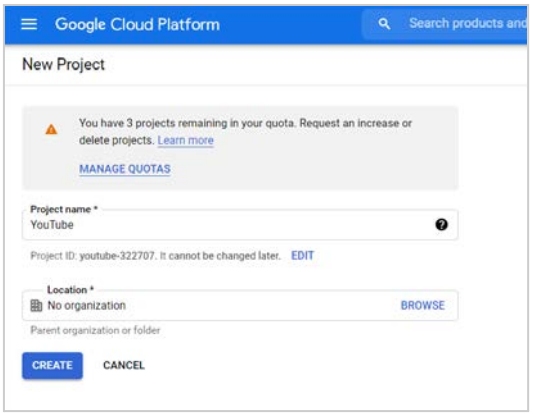
1. Sign in to Google Cloud Platform.



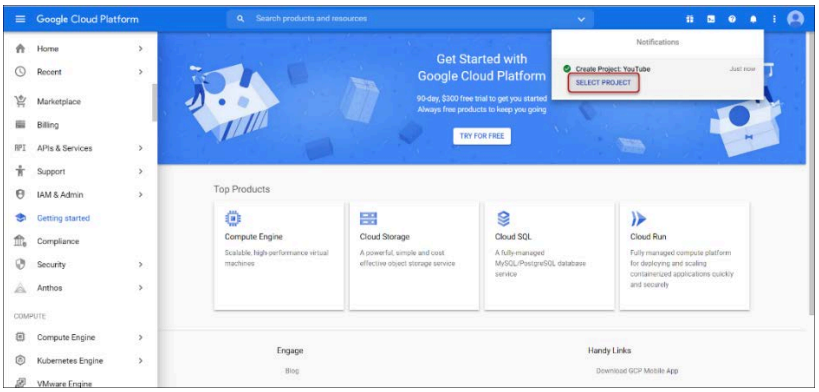
2. Click **Select a project**, then **NEW PROJECT**.

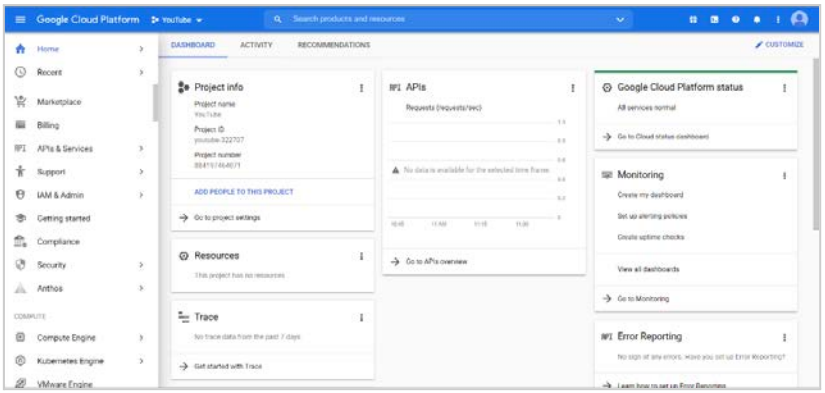


3. Enter a name for the project and click **CREATE**.

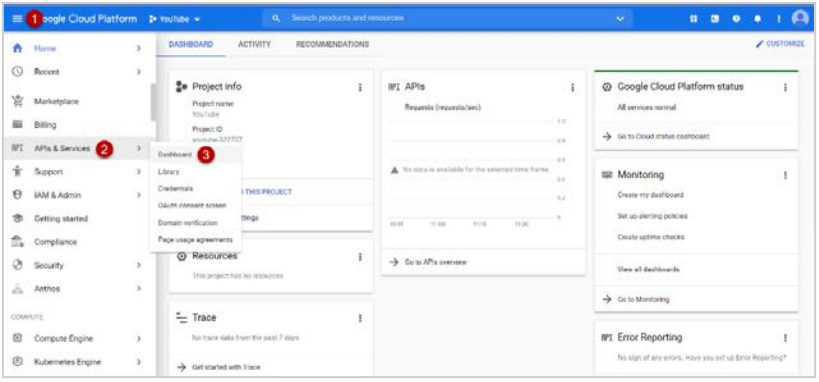


4. Once the project is created, click **SELECT PROJECT** from the **Notifications** and you are navigated to the **Project** page.

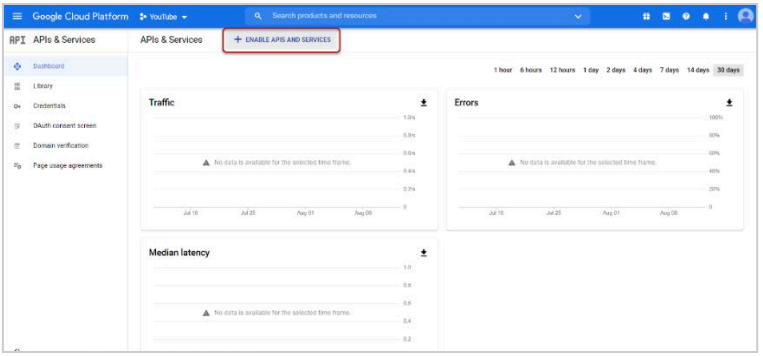




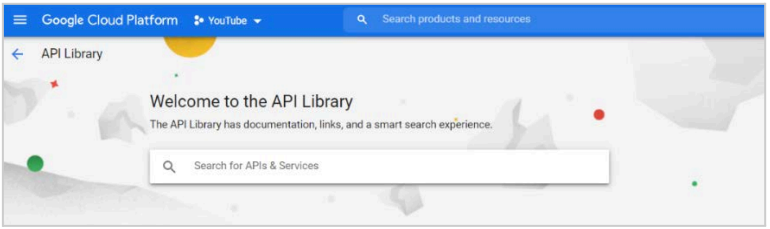
5. From the left side navigation menu, select **APIs & Services > Dashboard**.



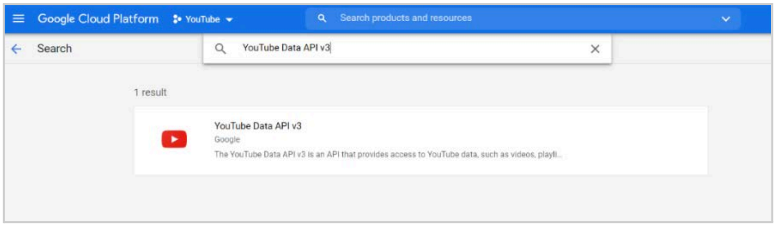
6. Click **ENABLE APIS AND SERVICES**.



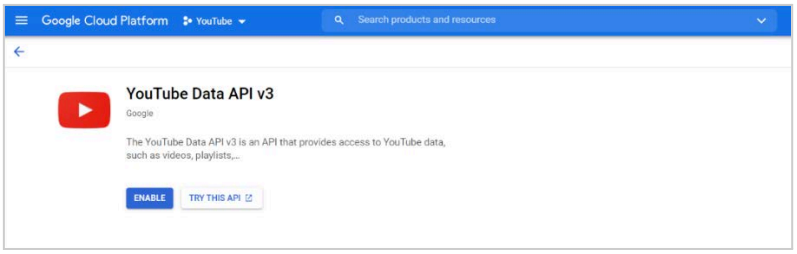
7. In the **Search for APIs & Services** search box, type `YouTube Data API v3`.



8. Click **YouTube Data API v3**.



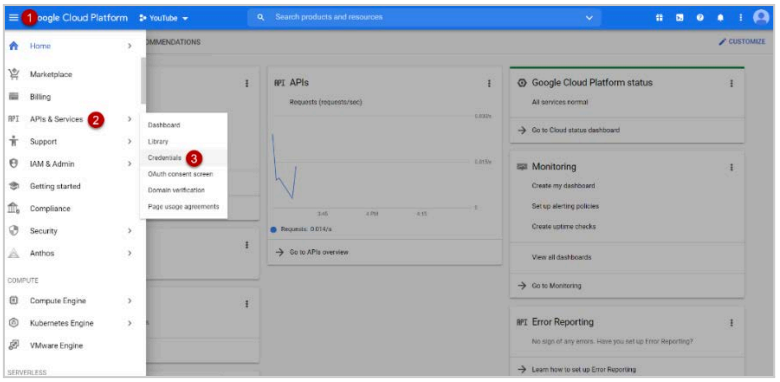
9. Once you are on the Gmail API page, click **ENABLE**.



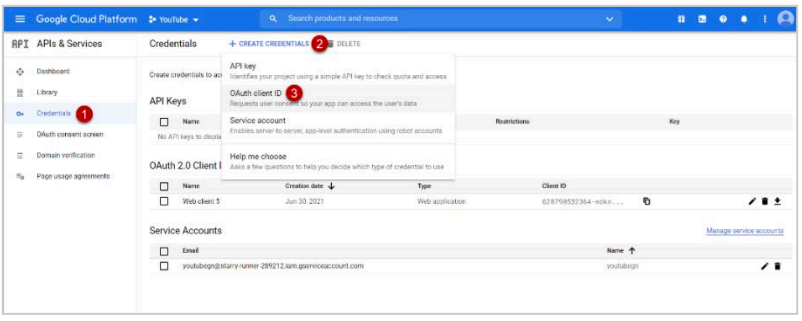
Creating Credentials

To create the credentials:

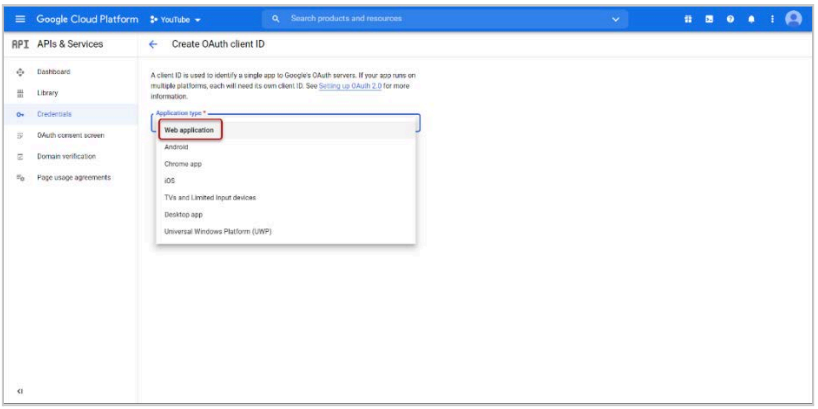
1. Select **APIs & Services > Credentials** from the left navigation menu.



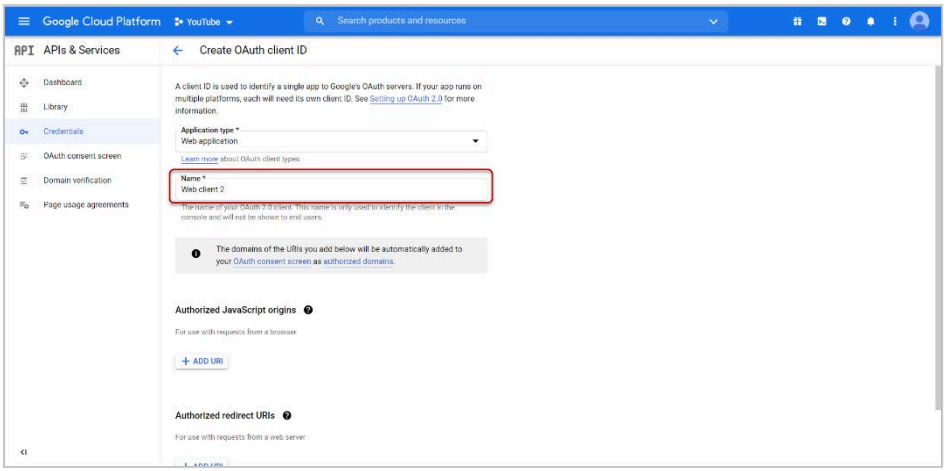
2. Click **CREATE CREDENTIALS** and select **OAuth client ID**.



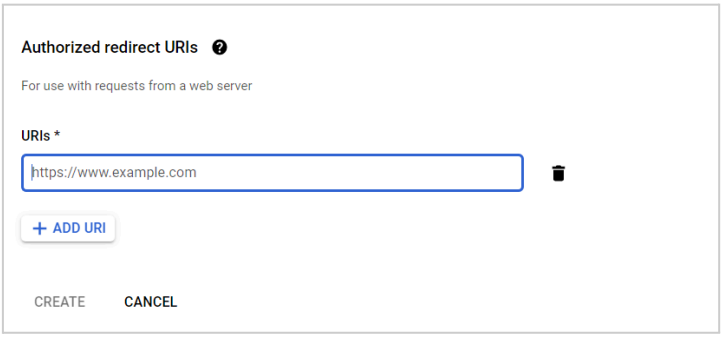
3. From the **Application type** drop-down menu, select **Web application**.



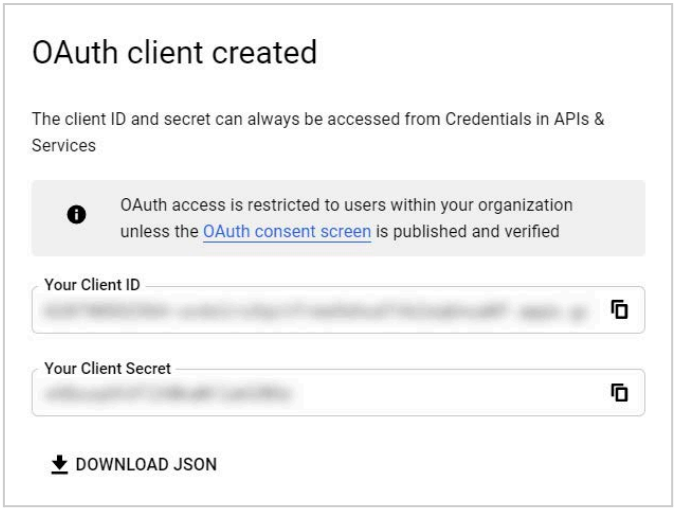
4. Enter the name for the application.



5. In the **Authorized redirect URIs** section, click **ADD URI** and add the URL of your local Merge1 environment in the following format: `https://<merge1_instance>/Configuration/OAuthCallback` and click **CREATE**, which you can find in the 10th point of the **Click** information.

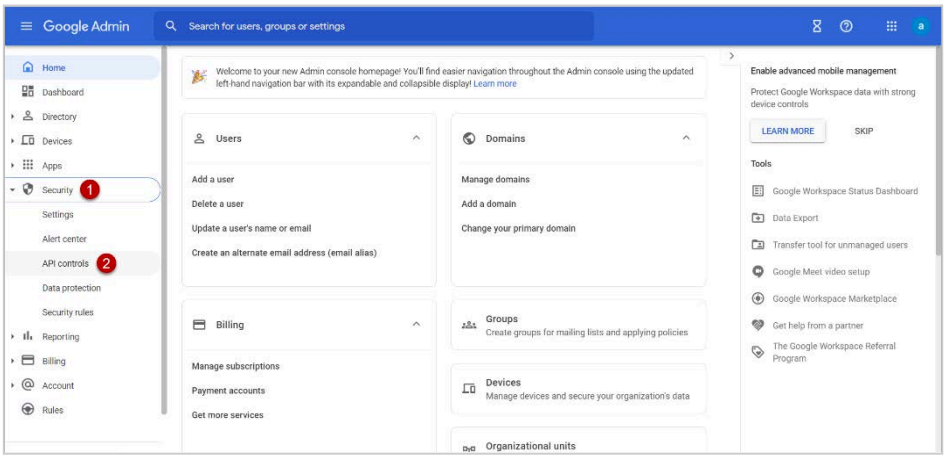


6. Copy and save the **Client ID** and **Client ID** from the created **OAuth client** pop-up window.

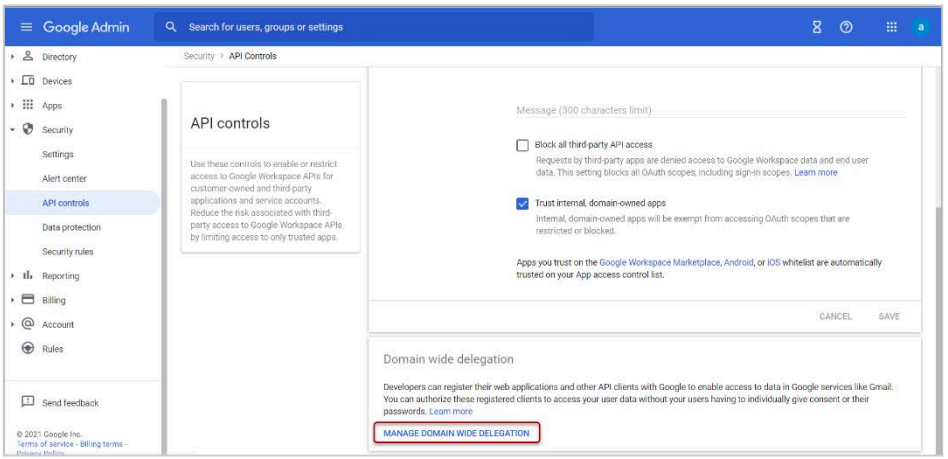


Managing Domain-Wide Authority Delegation

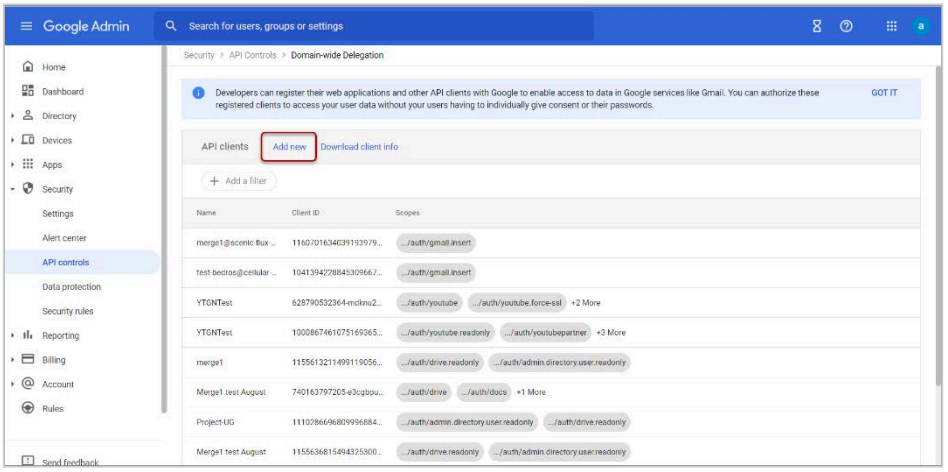
1. Sign in to Google Admin Console.
2. On the left side menu, click **Security > API controls**.



3. Scroll down to **Domain wide delegation** section and click **MANAGE DOMAIN WIDE DELEGATION**.

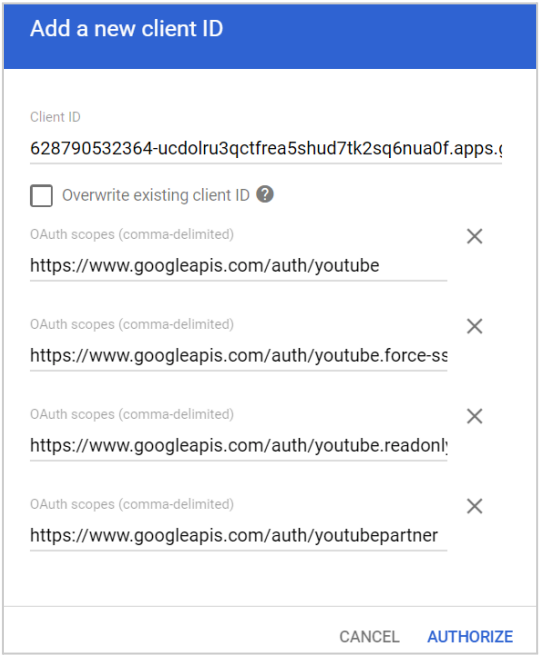


4. Click **Add new**.



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**.

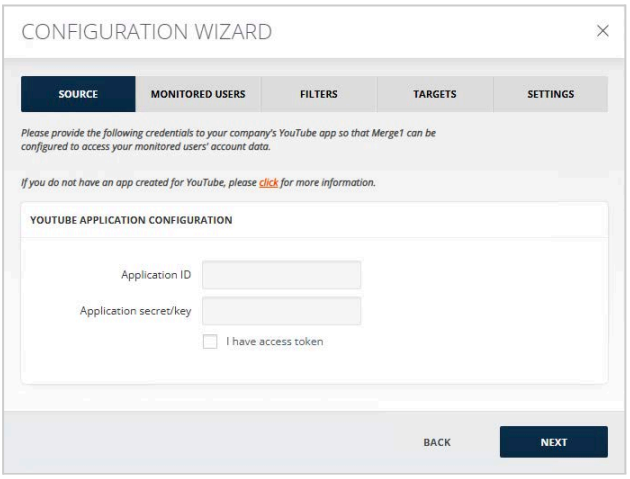
Note

By using this importer, you are agreeing to the YouTube terms: https://www.youtube.com/t/terms, https://policies.google.com/privacy.

Collector Configuration

To set up the collector:

1. Click **Add Importer**, specify **Name** and a **Description**(optional), and select the collector from the list. The **YouTube Application Configuration** window will open.
2. In the **Application ID** field, enter **Client ID** copied previously, in **Application secret/key**, enter the copied **Client Secret** and click **Next**.



3. Select the account the content of which you want to capture and click **Allow**.

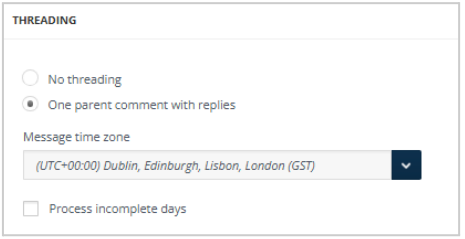
Time Stamp Formatting

For more details on how to configure timestamps, see **Time Stamp Formatting**.

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 as well. This option can be selected only if **One parent comment with replies** is activated.



Message Body

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.
- **Light grid mode**: Displays data in a two-toned layout, making it visually distinct and easier to view while displaying limited metadata.

Advanced Configuration Options

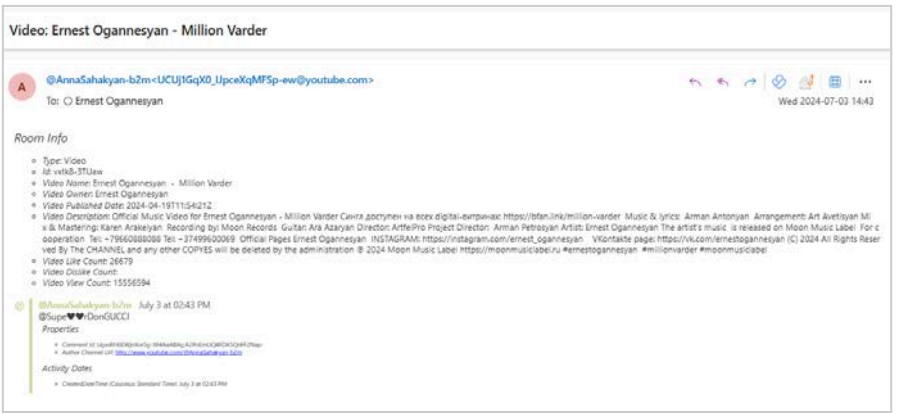
For more details on how to configure advanced configuration options, see **Advanced Configuration Options**.

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**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**
- **No data captured**

- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

Zoom Chat

Zoom Team Chat is a tool within Zoom's cloud-based collaboration suite, designed to support messaging, file sharing, and multimedia exchange. It helps teams stay connected through text, audio, and video messages, along with shared content like files, screenshots, and emojis, contributing to smoother everyday interactions and workflow coordination.

The **Merge1 Zoom Chat collector** enables secure data capture and delivery for archiving, compliance, and communication management. It helps organizations maintain visibility across internal conversations while preserving important information.

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

- One-on-one chat messages
  - Create
  - Edit
  - Delete
- Group chat messages
  - Create
  - Edit
  - Delete
- Channel messages
  - Create
  - Edit
  - Delete
- Membership activities (joined/left)

Captured activities can contain:

- Links[60]
- Emojis
- GIFs[61]
- Attachments
- Forwarded messages
- Voice messages
- Video messages
- Code snippets
- Hosted GIFs
- Message reactions

[60] Both inserted and regular links are captured.
[61] The link of the GIFs.

Notes

- Text formatting (rich text) is captured as plain text.

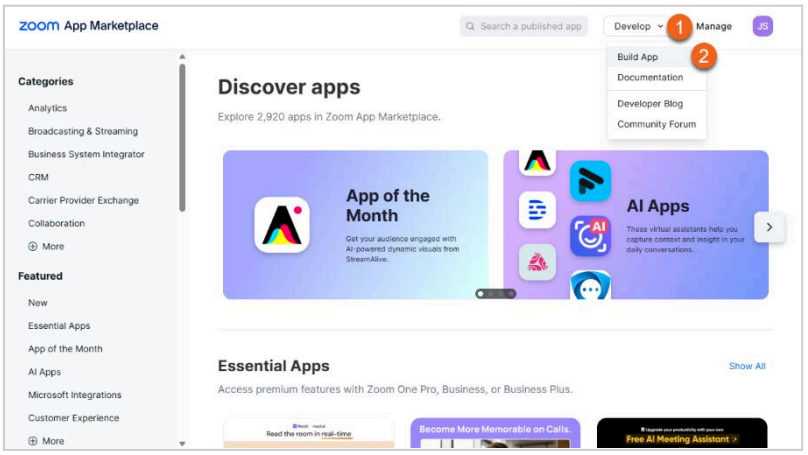
Due to current API limitations, the following constraints apply:

- Chats only from the last 6 months can be captured.
- Deleted forwarded messages are not captured.
- If a message has multiple versions (such as edits or deletions), all reactions are captured alongside the message's most recent version.
- Reactions on previously captured messages are not retrieved unless the message's modified date has been updated.

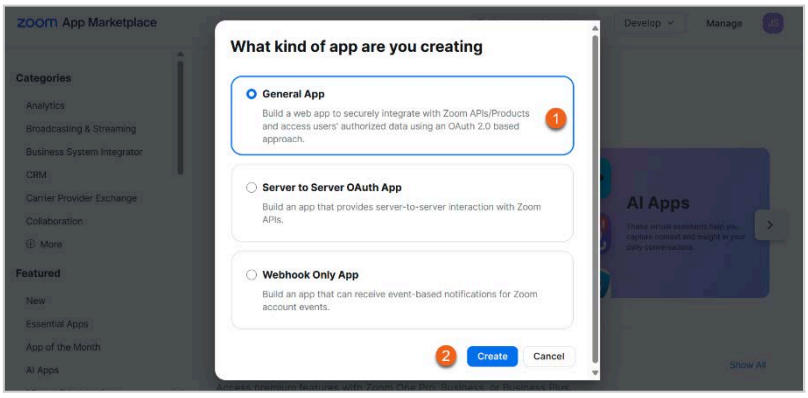
Creating a Zoom App

To create a Zoom app:

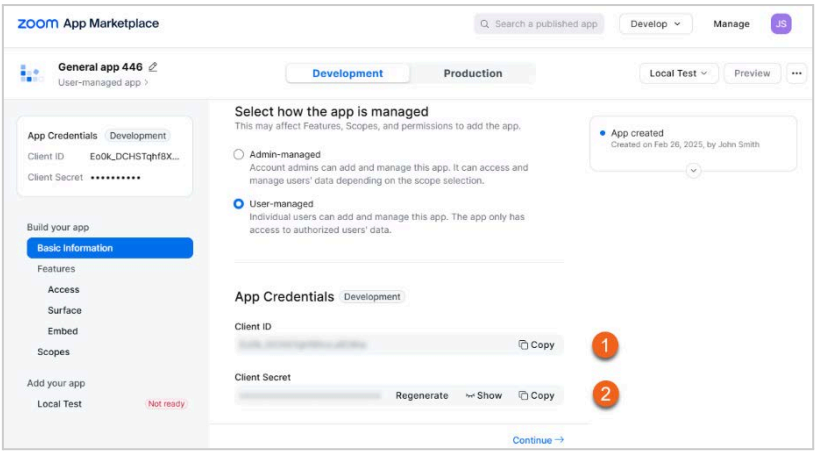
1. Sign in to the Zoom App Marketplace.
2. Select **Develop > Build App**.



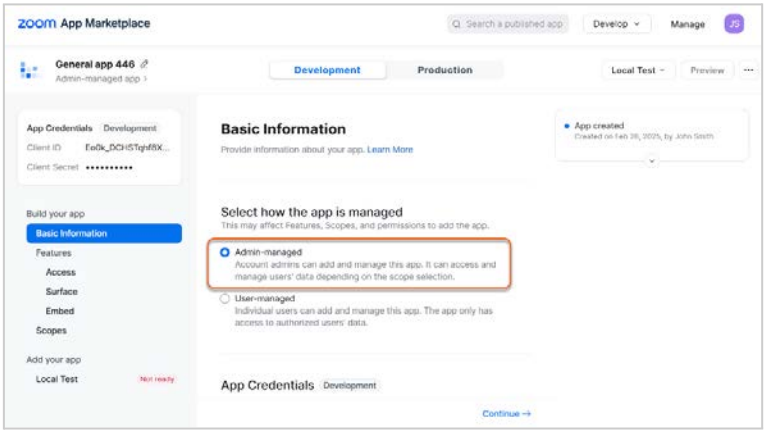
3. Select **General App** and click **Create**.



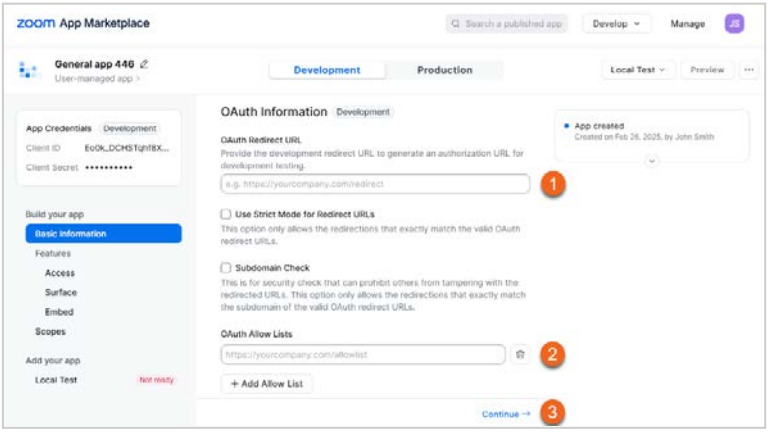
4. A **Client ID** and **Client secret** will be generated. Use these credentials to configure the collector.



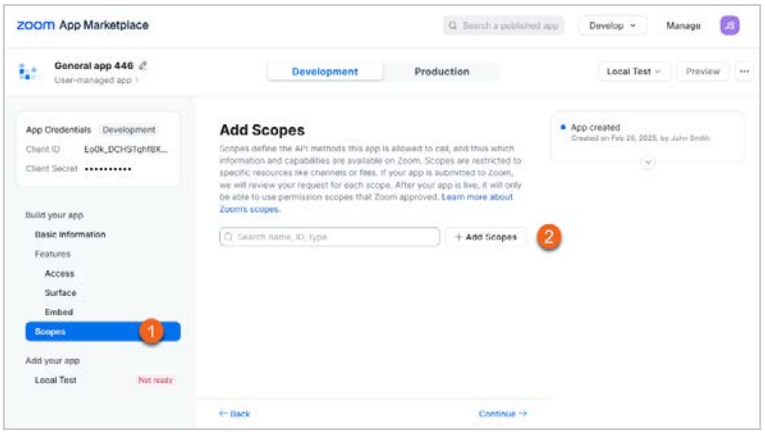
5. On the **Basic Information** page, under **Select** how the app is managed, choose **Admin-managed** and click **Save**.



6. Scroll down to the **OAuth Information** and add the URL of your local Merge1 environment in the following format: `https://<merge1_instance>/Configuration/OAuthCallback` to the **OAuth Redirect URL**. Ensure that **OAuth Allow lists** field is filled with the same URL as well.

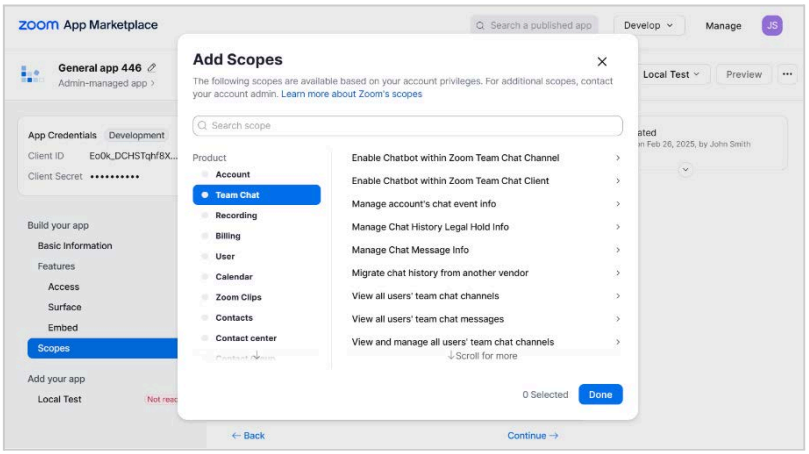


7. Go to **Scopes** and click **Add Scopes**.



8. Add the following scopes to the application and click **Done**:

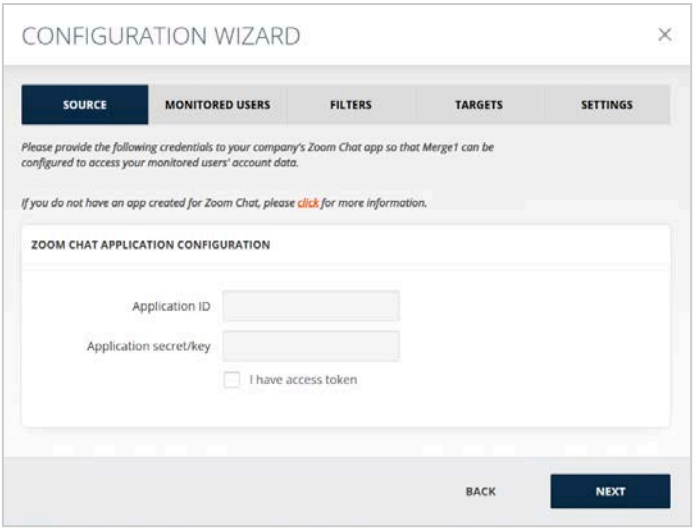
   - **team_chat:read:list_channel_activity_logs:admin**
   - **team_chat:read:list_user_channels:admin**
   - **team_chat:read:list_members:admin**
   - **team_chat:read:message_emoji:admin**
   - **team_chat:read:user_message:admin**
   - **user:read:user:admin**
   - **user:read:list_users:admin**
   - **report:read:chat_session:admin**
   - **report:read:list_chat_sessions:admin**



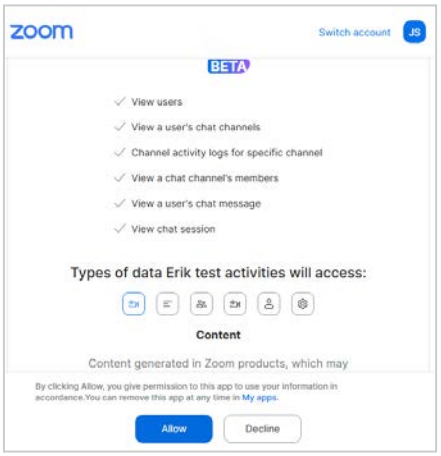
Collector Configuration

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.



Time Stamp Formatting

For more details on how to configure timestamps, see **Time Stamp Formatting**.

Advanced Configuration Options

For more details on how to configure advanced configuration options, see **Advanced Configuration Options**.

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

For more details on how to configure attachments, see **Attachments Configuration**.

Next Steps

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

- **MONITORED USERS**
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:

Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

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

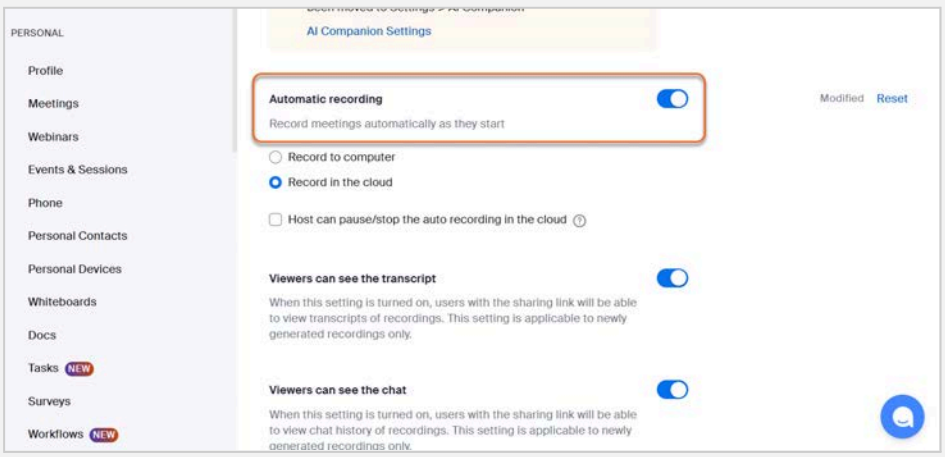
To use the collector, the Zoom account must be on a Business, Business Plus, or Enterprise plan; Pro plan access is not supported.

Activities Captured

- Meeting metadata
- Meeting recording files:
  - Audio and video
  - Audio
  - Audio transcripts
- Meeting chats
  - Messages
  - Replies
  - Emojis

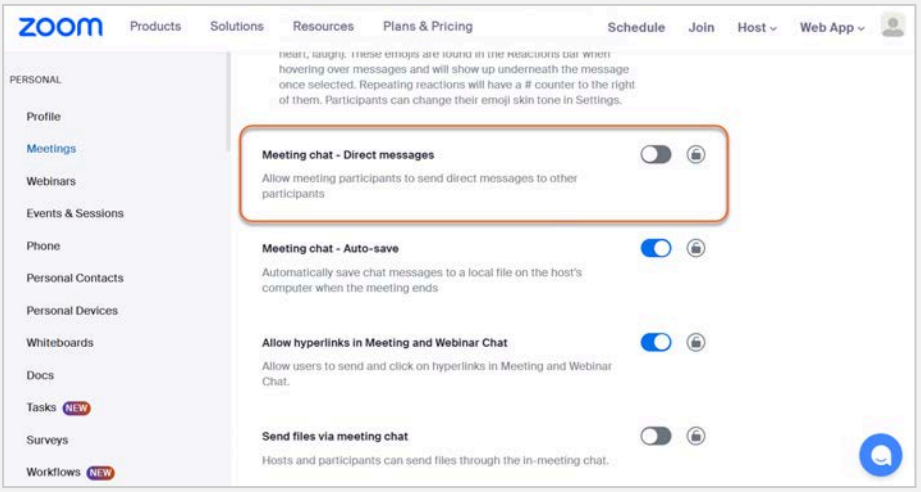
Note

- Only meetings from the last 6 months can be captured. Selecting a longer cut-off date in the Merge1 GUI has 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**.

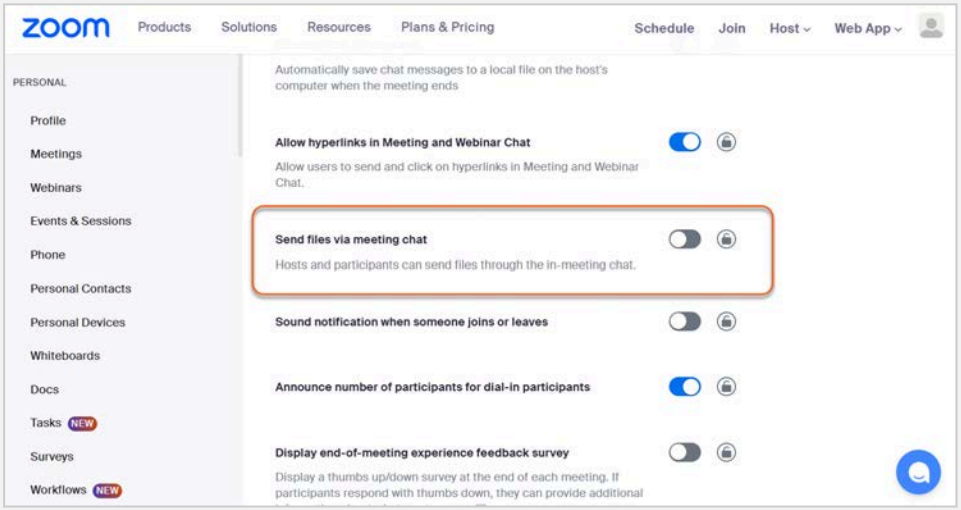


- If a message was sent privately to one of the meeting participants, it is not added to the recording file, as the Zoom API does not provide that option. We recommend disabling the

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**.

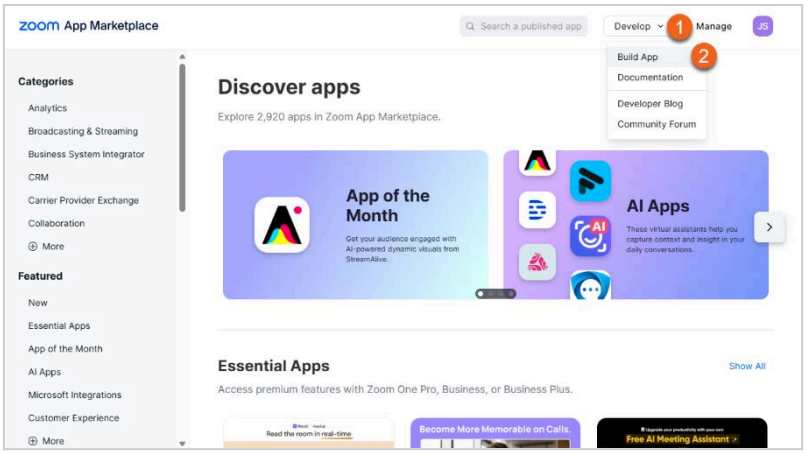


- In addition, the following features should be disabled for the hosts:
  - **General > Host can pause/stop the auto recording in the cloud**
  - **General > The host can delete cloud recordings**
  - **Notification > Delete cloud recordings and transcripts after a specified number of days**

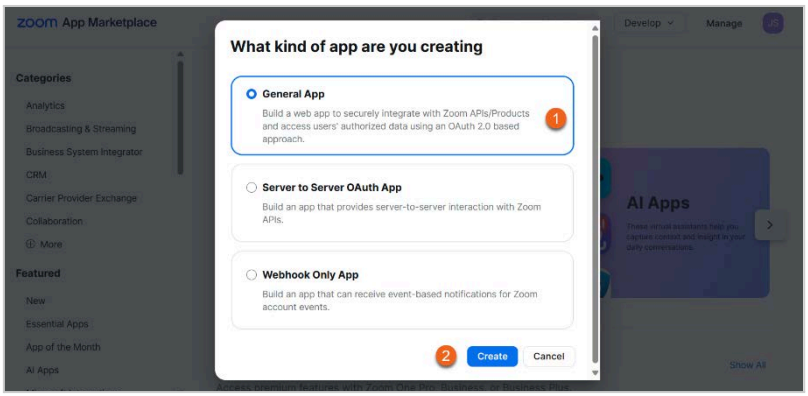
Creating a Zoom App

To create a Zoom app:

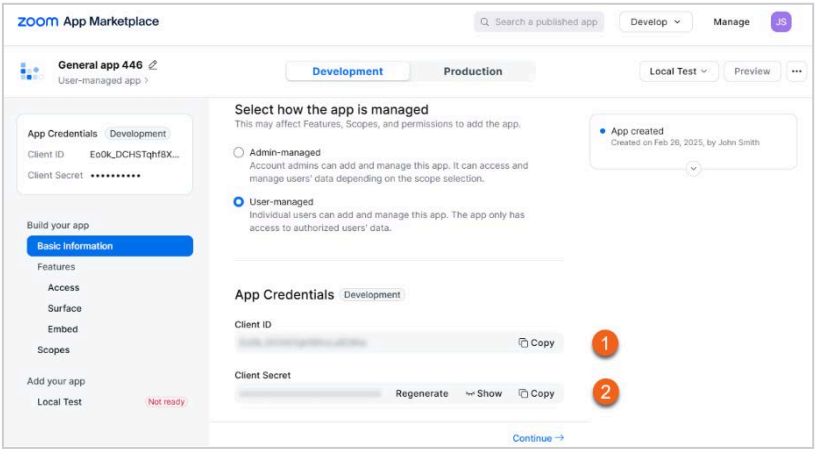
1. Sign in to the:
   - Zoom App Marketplace if using Zoom Commercial.
   - Zoom Gov App Marketplace if using Zoom for Government.
2. Select **Develop > Build App**.



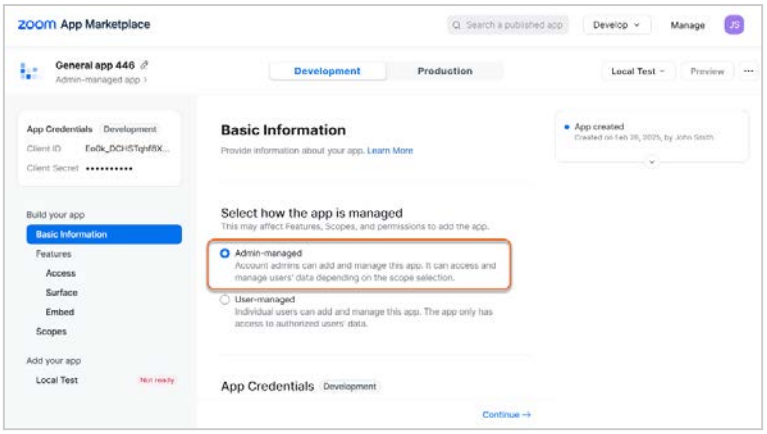
3. Select **General App** and click **Create**.



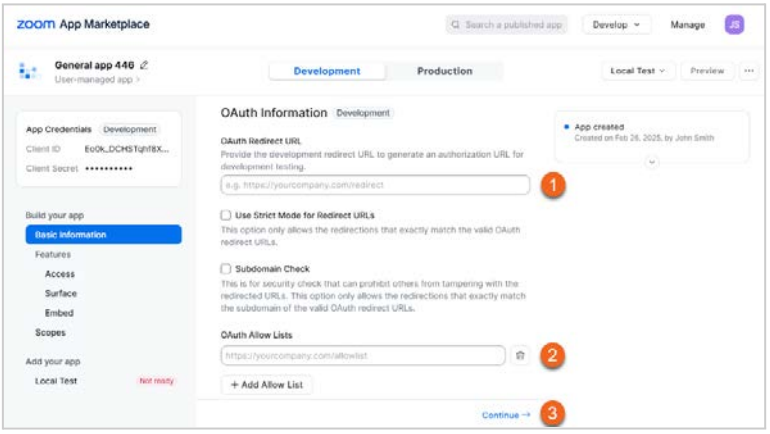
4. A **Client ID** and **Client secret** will be generated. Use these credentials to configure the collector.



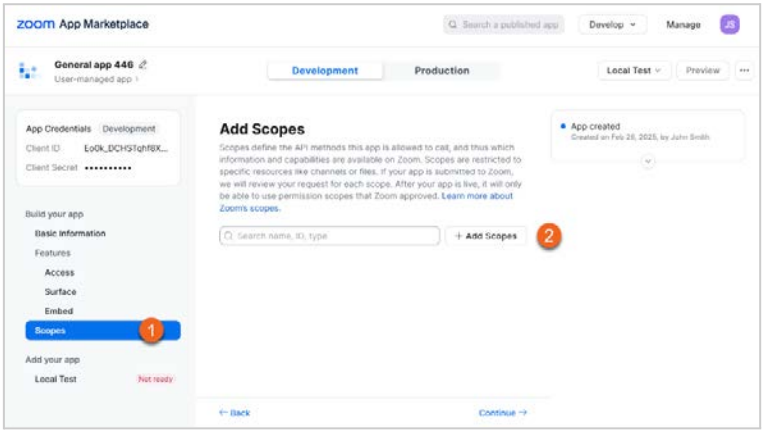
5. On the **Basic Information** page, under Select how the app is managed, choose **Admin-managed** and click **Save**.



6. Scroll down to the **OAuth Information** and add the URL of your local Merge1 environment in the following format: `https://<merge1_instance>/Configuration/OAuthCallback` to the **OAuth Redirect URL**. Ensure that **OAuth Allow lists** field is filled with the same URL as well.

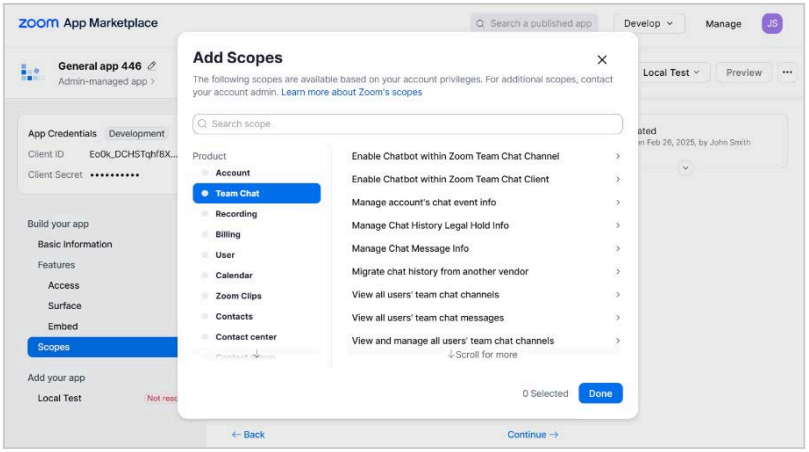


7. Go to **Scopes** and click **Add Scopes**.



8. Add the following scopes to the application and click **Done**:
    - **user:read:user:admin**
    - **user:read:list_users:admin**
    - **dashboard:read:list_meetings:admin**
    - **dashboard:read:list_meeting_participants:admin**

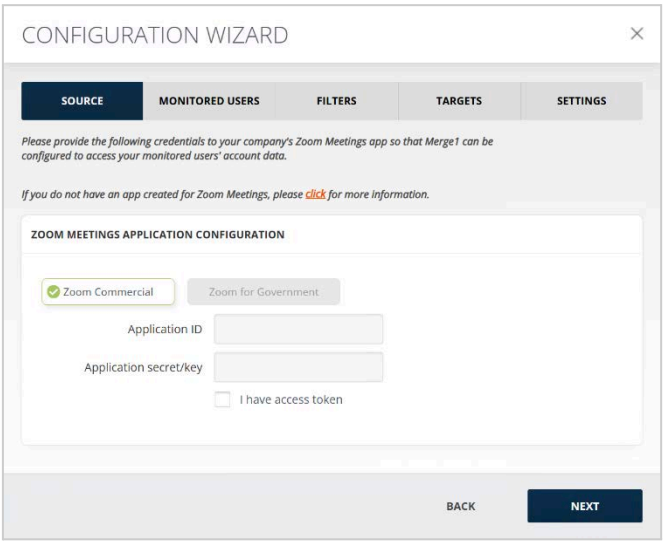
- **cloud_recording:read:list_recording_files:admin**
- **cloud_recording:read:list_recording_files:master**



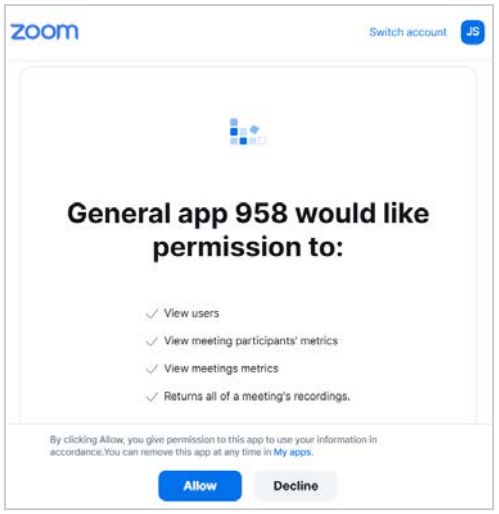
Collector Configuration

To configure the collector:

1. Select **Zoom Commercial** or **Zoom for Government** and use the respective credentials of the application.
2. 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.



3. 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.



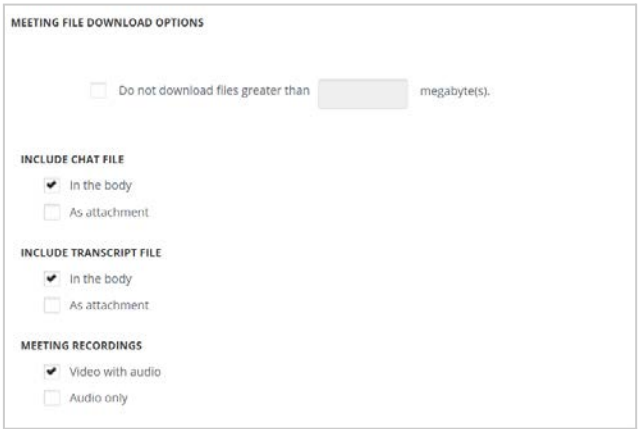
Time Stamp Formatting

For more details on how to configure timestamps, see **Time Stamp Formatting**.

Meeting File Download Options

This section includes:

- 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 whether the chat file is added to the body of the imported message or attached as a separate file.
- **Include Transcript File** specifies whether the transcript file is *added to the body of the imported message* or *attached as a separate file*.
- **Meeting Recordings** specifies whether the imported message includes *video with audio* or *only audio*.



Advanced Configuration Options

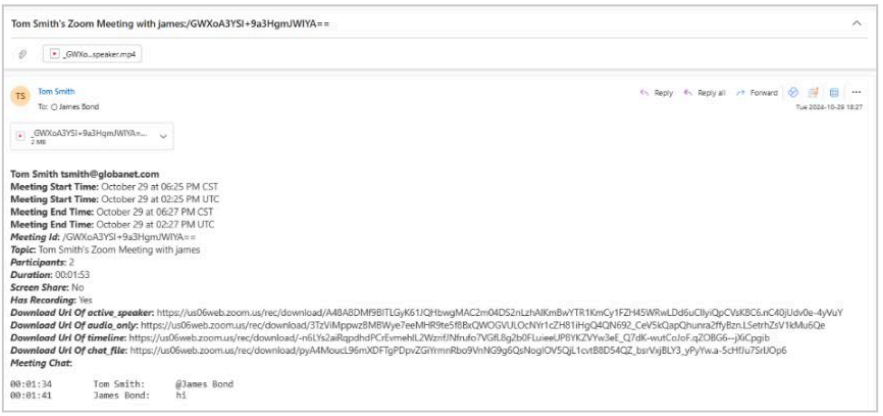
For more details on how to configure advanced configuration options, see **Advanced Configuration Options**.

Next Steps

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

- **MONITORED USERS**
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

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 third-party platform of their choice, satisfying FINRA and/or other compliance requirements. Only account administrators can manage what data is archived and what is displayed in the disclaimer and enable archiving for specific groups as well. Mergel uses this API to retrieve archived meetings or webinar chats.

Note that the Meeting Archiving feature is enabled for your account by Zoom Support.

Note

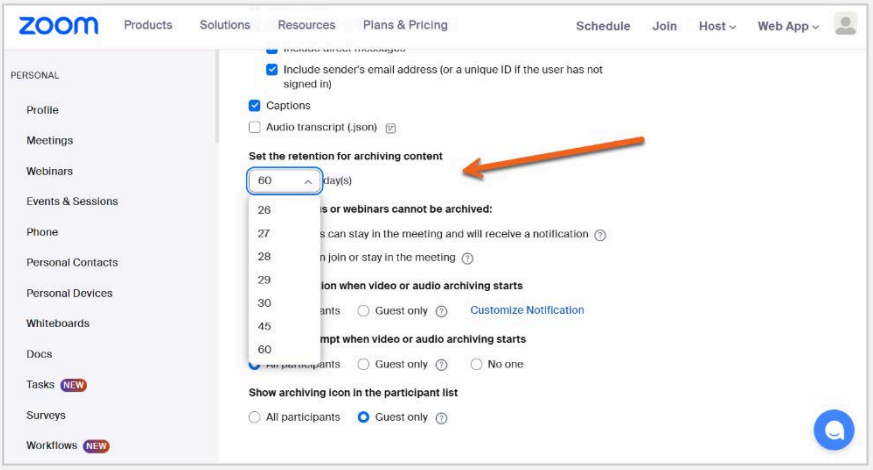
To use the collector, the Zoom account must be on a Business, Business Plus, or Enterprise plan; Pro plan access is not supported.

Activities Captured

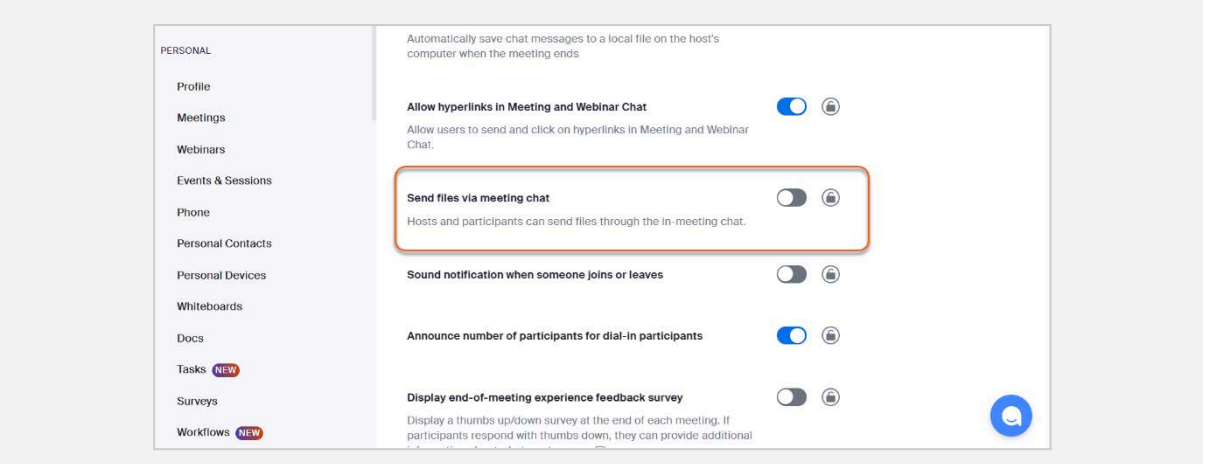
- Webinar/Meeting metadata
- Webinar/Meeting chats
- Polls in chats

Note

- 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**.



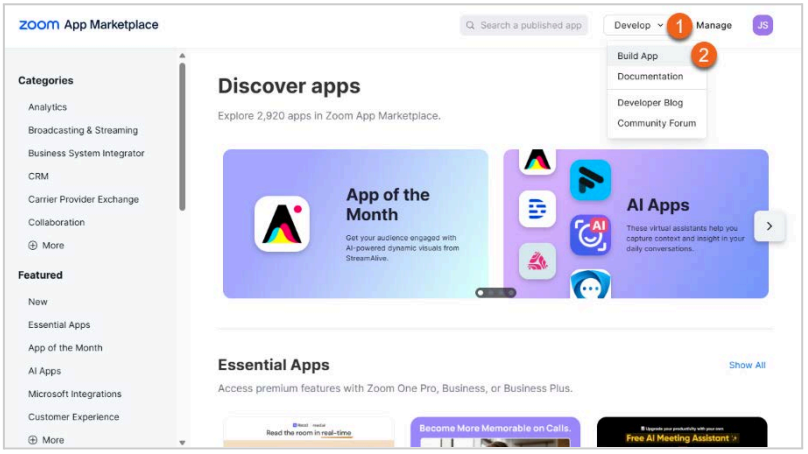
- Attachments sent during a meeting are not captured. To prevent data loss, the option to send files via meeting chat should be disabled from Account Settings - Zoom **> In Meeting (Basic) > Send files via meeting chat**.



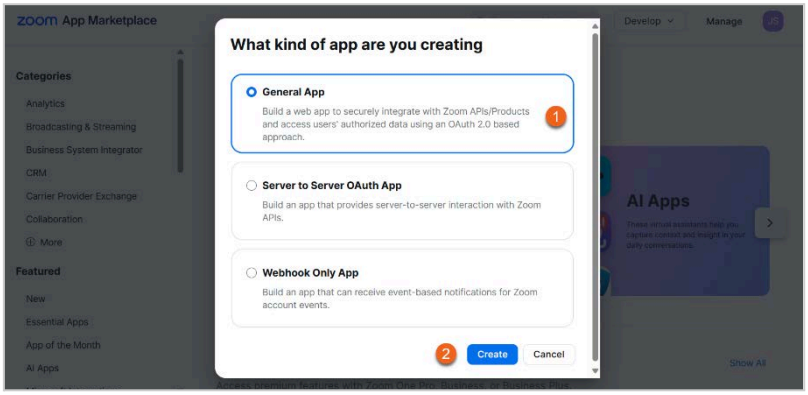
Creating a Zoom App

To create a Zoom app:

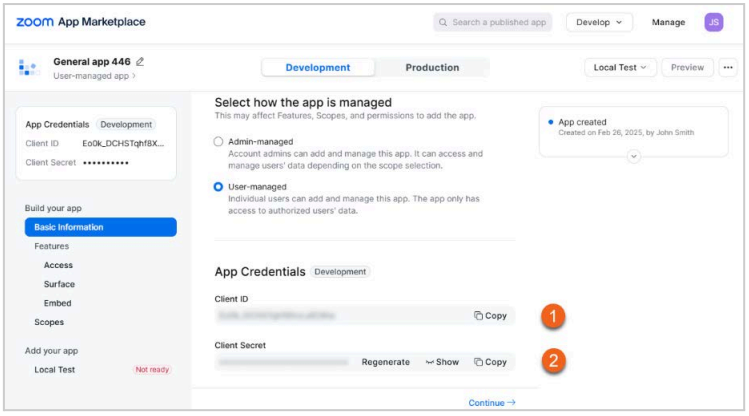
1. Sign in to the Zoom App Marketplace.
2. Select **Develop > Build App**.



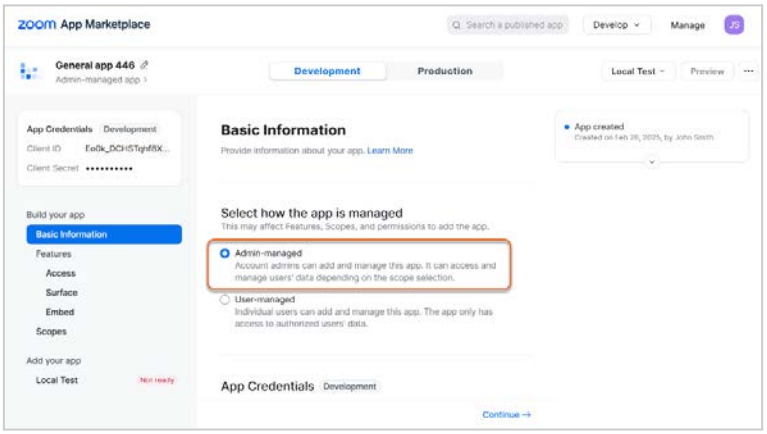
3. Select **General App** and click **Create**.



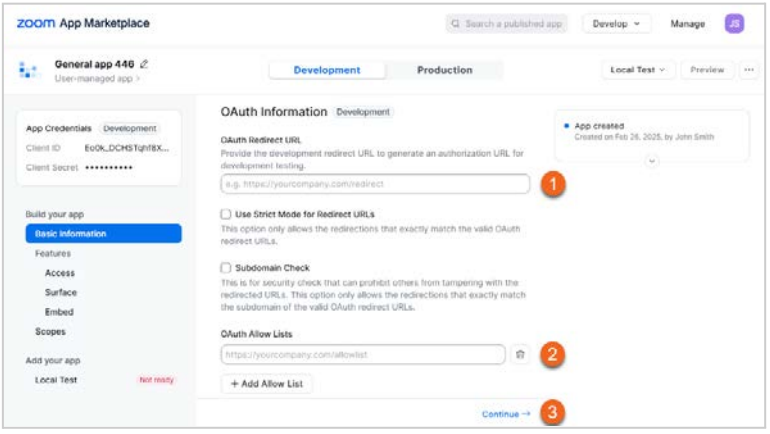
4. A **Client ID** and **Client secret** will be generated. Use these credentials to configure the collector.



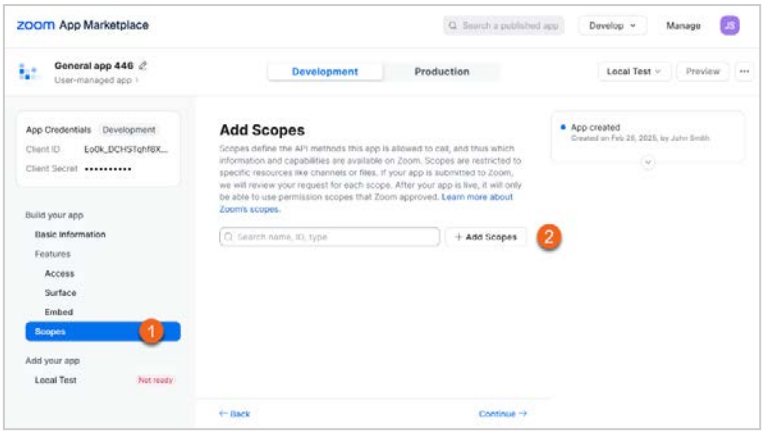
5. On the **Basic Information** page, under **Select how the app is managed**, choose **Admin-managed** and click **Save**.



6. Scroll down to the **OAuth Information** and add the URL of your local Merge1 environment in the following format: `https://<merge1_instance>/Configuration/OAuthCallback` to the **OAuth Redirect URL**. Ensure that **OAuth Allow lists** field is filled with the same URL as well.

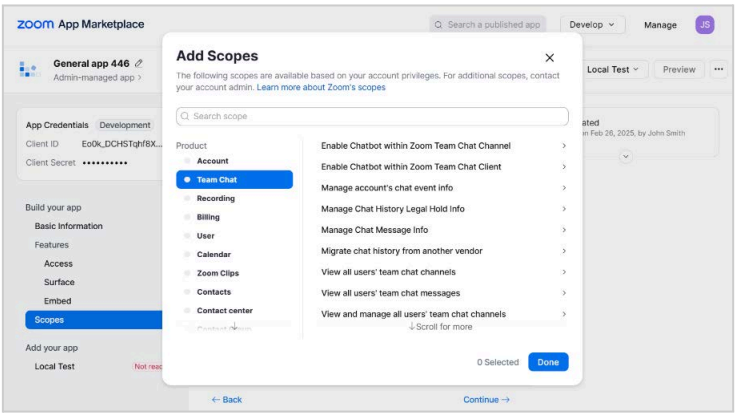


7. Go to **Scopes** and click **Add Scopes**.



8. Add the following scopes to the application and click **Done**:

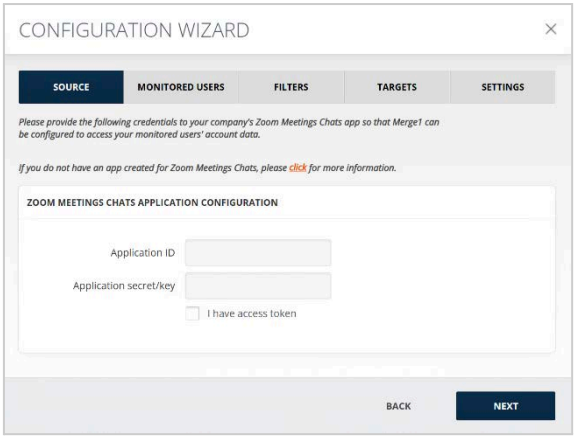
   - **user:read:user:admin**
   - **user:read:list_users:admin**
   - **archiving:read:list_archived_files:admin**
   - **archiving:read:list_archived_files:master**
   - **meeting:read:list_past_participants:admin**
   - **meeting:read:list_poll_results:admin**



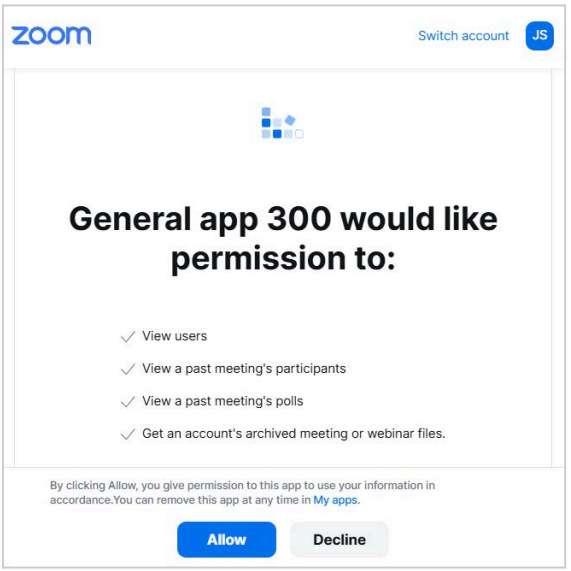
Collector Configuration

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

For more details on how to configure timestamps, see **Time Stamp Formatting**.

Advanced Configuration Options

For more details on how to configure advanced configuration options, see **Advanced Configuration Options**.

Next Steps

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

- **MONITORED USERS**
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:

Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

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 third-party platform of their choice, satisfying FINRA and/or other compliance requirements. Only account administrators can manage what data is archived and what is displayed in the disclaimer and enable archiving for specific groups as well.

Merge1 uses this API to retrieve archived meeting or webinar files of an account.

Note that the Meeting Archiving feature is enabled for your account by Zoom Support.

Note

To use the collector, the Zoom account must be on a Business, Business Plus, or Enterprise plan; Pro plan access is not supported.

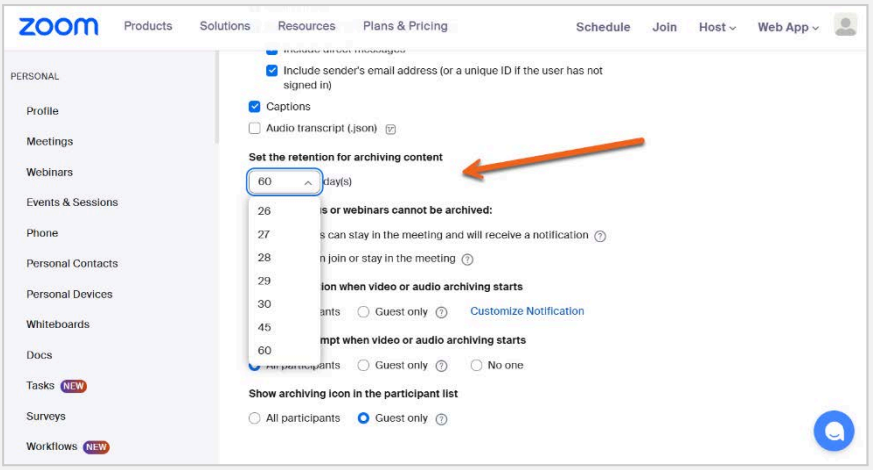
Activities Captured

- Webinar/Meeting metadata
- Webinar/Meeting recording files:
  - Audio and video
  - Audio
  - Closed captions (only if the option is enabled by the user from the Zoom Settings)
- Webinar/Meeting chats
- Polls in chats
- Recording files as attachments[62]

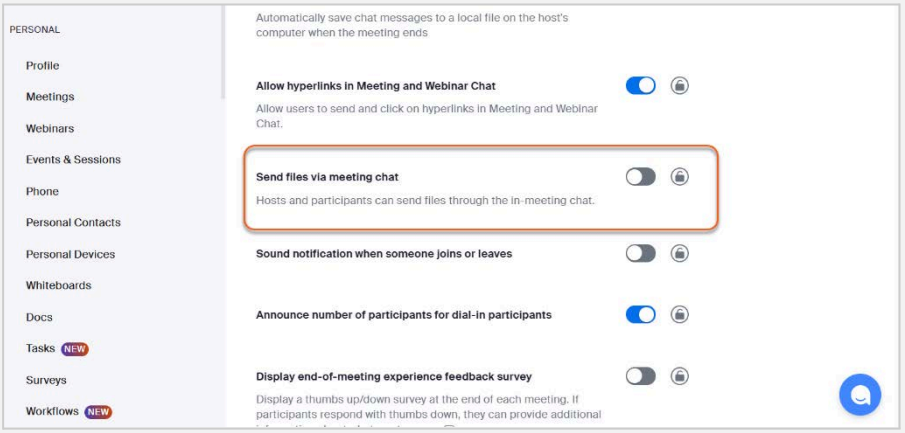
Note

- 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**.

[62] A token should be added to download files with the download URLs.



- 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**.

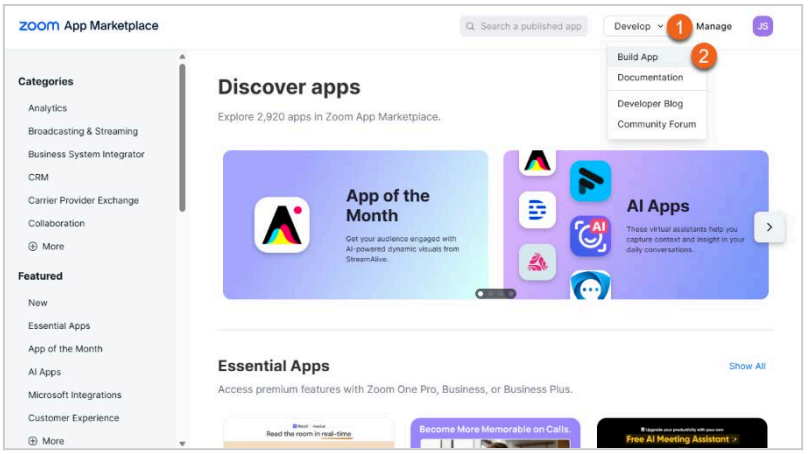


- In addition, the following features should be disabled for the hosts:
  - **General > Host can pause/stop the auto recording in the cloud**
  - **General > The host can delete cloud recordings**
  - **Notification > Delete cloud recordings and transcripts after a specified number of days**

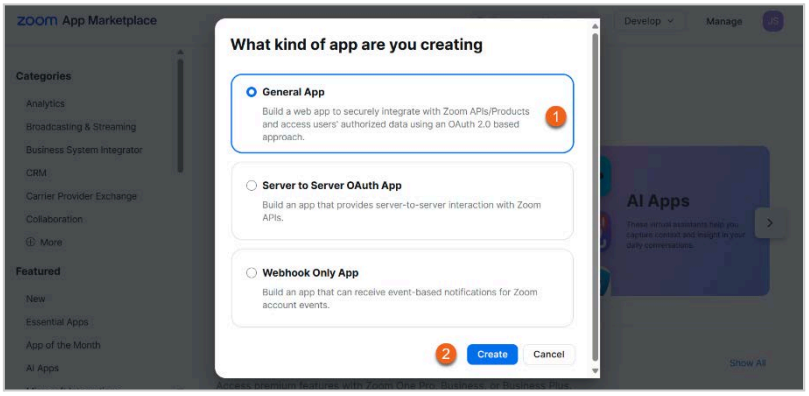
Creating a Zoom App

To create a Zoom app:

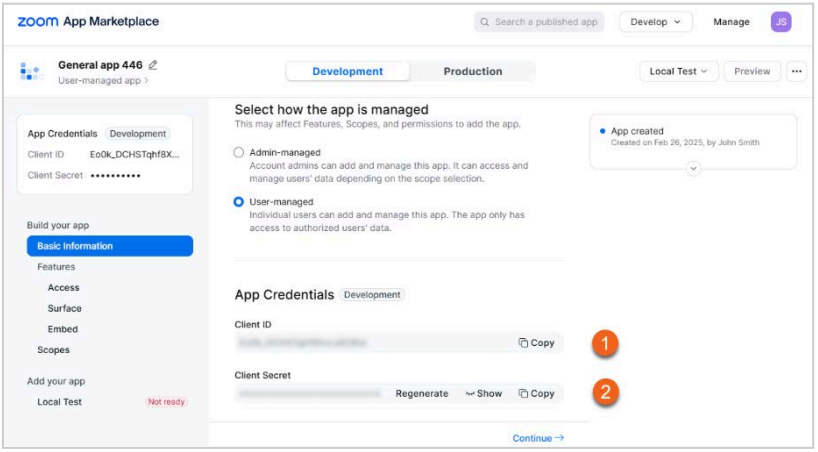
1. Sign in to the Zoom App Marketplace.
2. Select **Develop > Build App**.



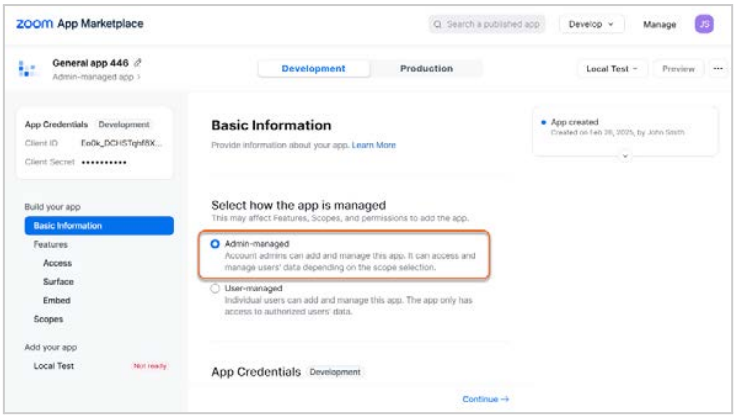
3. Select **General App** and click **Create**.



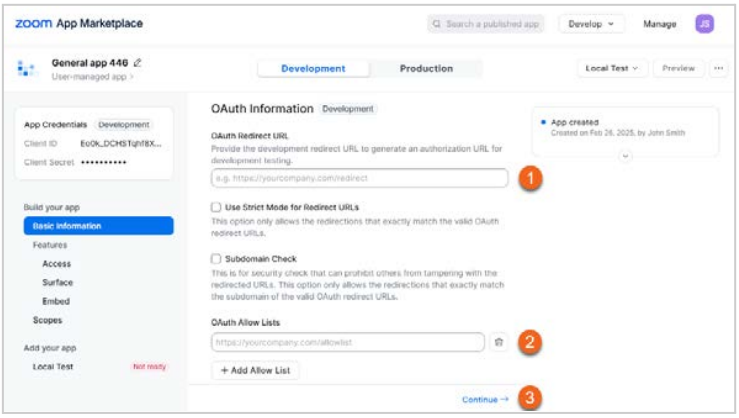
4. A **Client ID** and **Client secret** will be generated. Use these credentials to configure the collector.



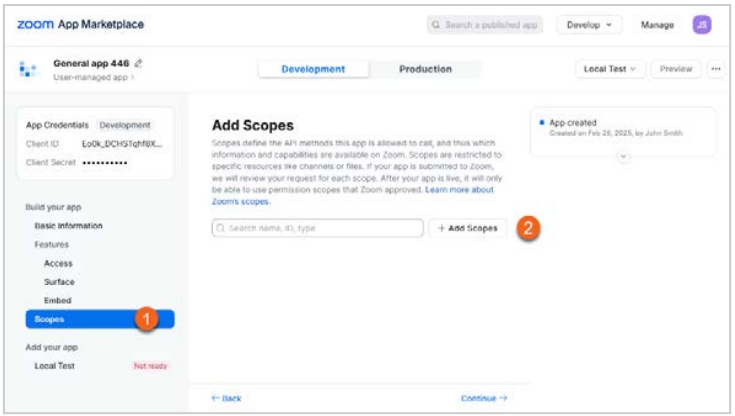
5. On the **Basic Information** page, under **Select how the app is managed**, choose **Admin-managed** and click **Save**.



6. Scroll down to the **OAuth Information** and add the URL of your local Merge1 environment in the following format: `https://<merge1_instance>/Configuration/OAuthCallback` to the **OAuth Redirect URL**. Ensure that **OAuth Allow lists** field is filled with the same URL as well.



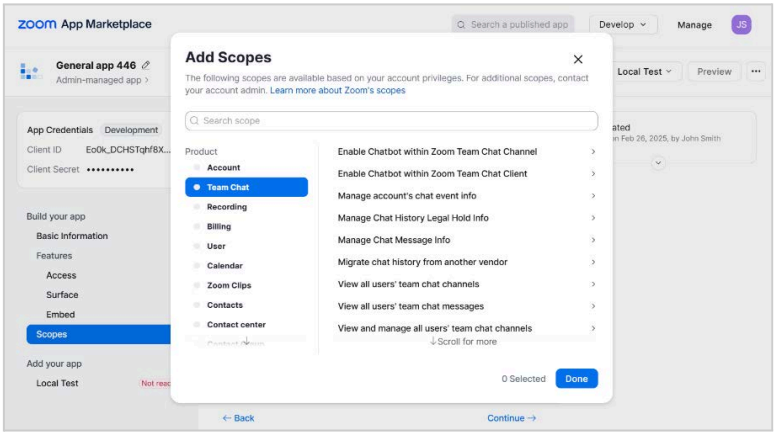
7. Go to **Scopes** and click **Add Scopes**.



8. Add the following scopes to the application and click **Done**:

- **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**

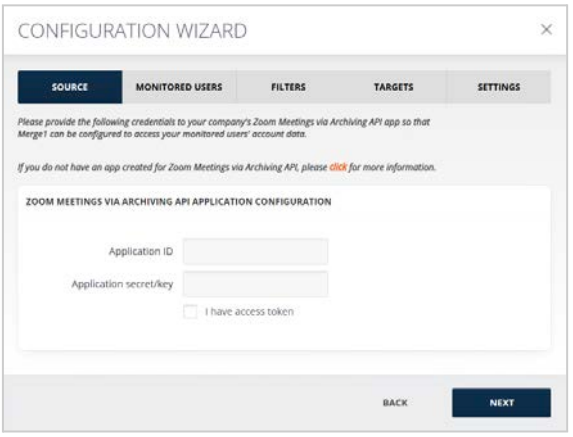
- **webinar:read:list_past_participants:admin**



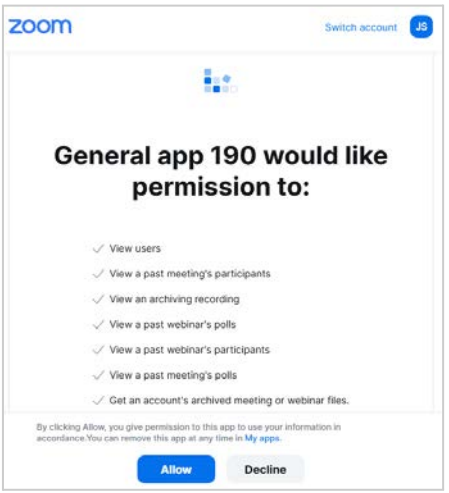
Collector Configuration

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.



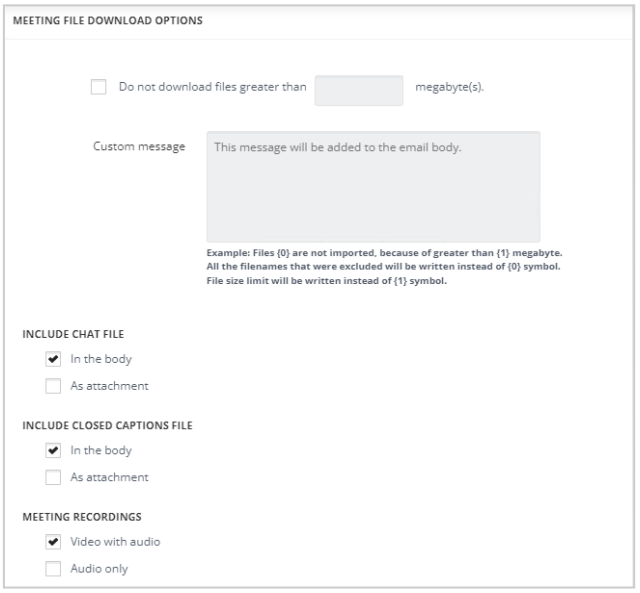
Time Stamp Formatting

For more details on how to configure timestamps, see **Time Stamp Formatting**.

Meeting File Download Options

This section includes:

- 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 whether the chat file is added to the body of the imported message or attached to the message as a separate file.
- The **Include Closed Captions File** option specifies whether the closed captions file is *added to the body of the imported message* or *attached to the message as a separate file*.
- The **Meeting Recordings** option specifies whether the imported message includes *video with audio* or *only audio*.



Advanced Configuration Options

For more details on how to configure advanced configuration options, see **Advanced Configuration Options**.

Next Steps

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

- **MONITORED USERS**
- **FILTERS**
- **TARGETS**

- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:

Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

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 **Merge1 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[63]

- One-on-one SMS/MMS messages
- Group SMS/MMS messages

Captured activities can contain:

- Emojis
- GIFs
- Attachments

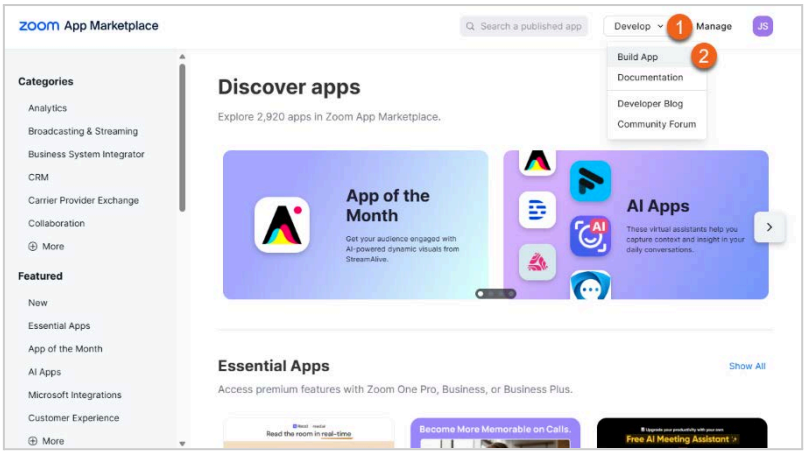
> **Note**
>
> It is possible to capture data from the past six months, which is the maximum timeframe available through the API.

Creating a Zoom App

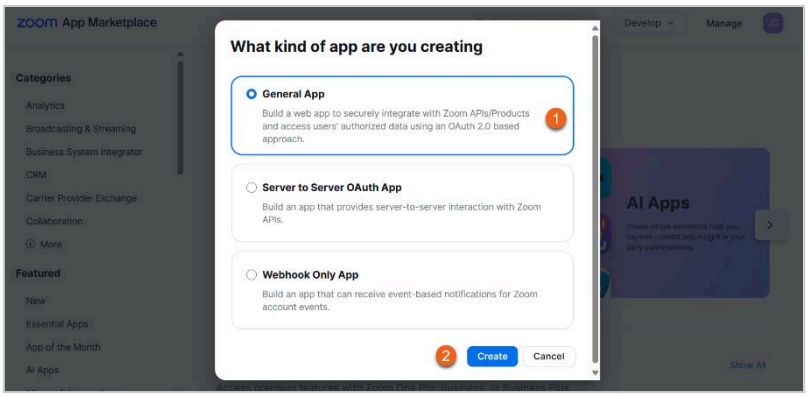
To create a Zoom app:

1. Sign in to the Zoom App Marketplace.
2. Select **Develop > Build App**.

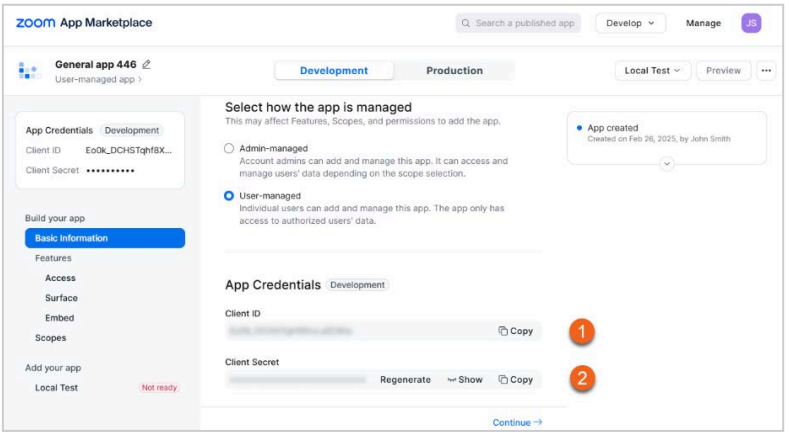
[63] As long as Zoom Phone's SMS/MMS features remain enabled on the user's side, activities will be captured.



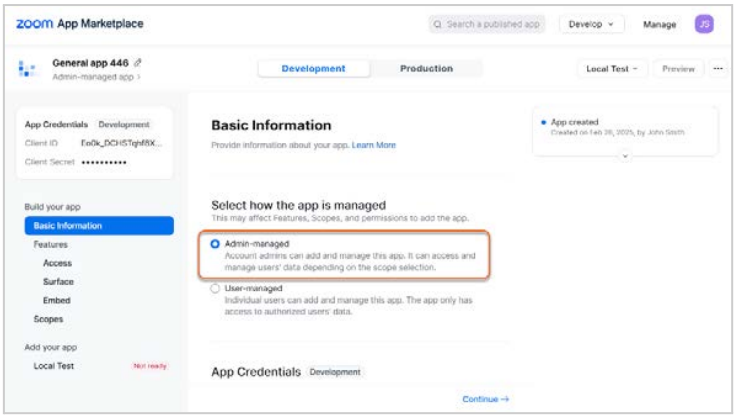
3. Select **General App** and click **Create**.



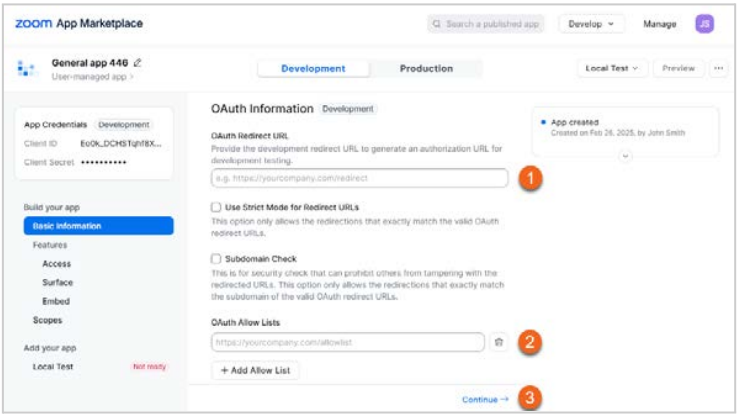
4. A **Client ID** and **Client secret** will be generated. Use these credentials to configure the collector.



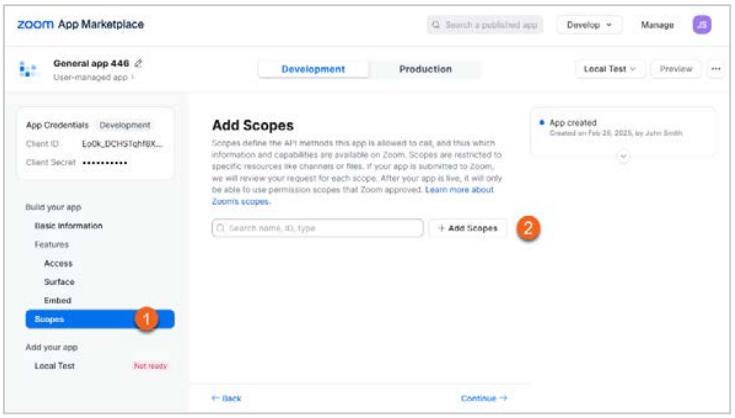
5. On the **Basic Information** page, under **Select** how the app is managed, choose **Admin-managed** and click **Save**.



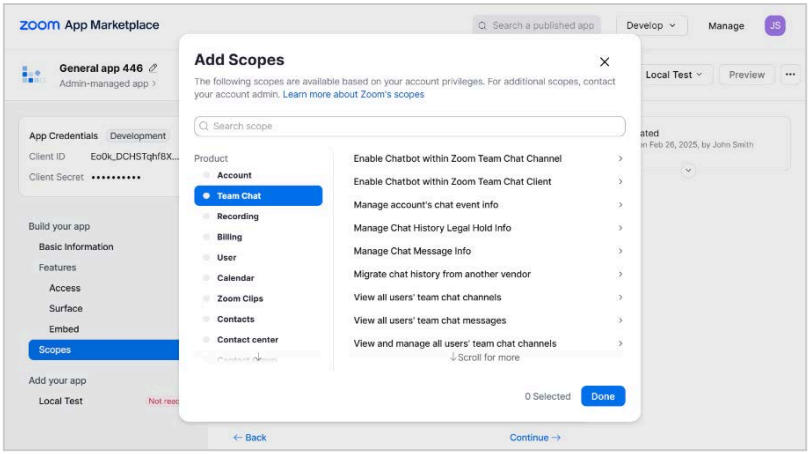
6. Scroll down to the **OAuth Information** and add the URL of your local Merge1 environment in the following format: `https://<merge1_instance>/Configuration/OAuthCallback` to the **OAuth Redirect URL**. Ensure that **OAuth Allow lists** field is filled with the same URL as well.



7. Go to **Scopes** and click **Add Scopes**.



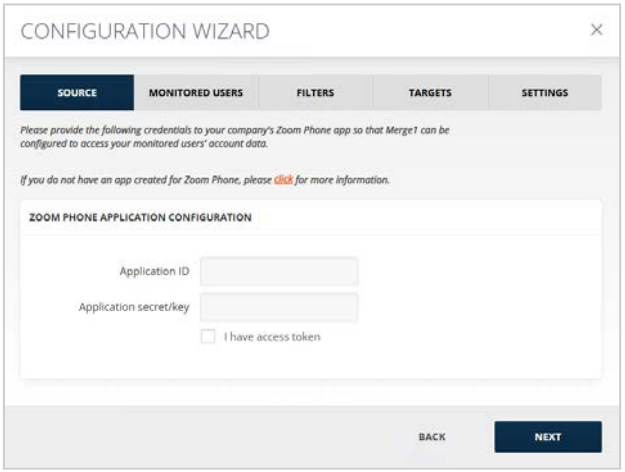
8. Add the following scopes to the application and click **Done**:
    - **phone:read:user:admin**
    - **phone:read:list_users:admin**
    - **phone:read:sms_message:admin**
    - **phone:read:sms_session:admin**
    - **phone:read:list_sms_sessions:admin**



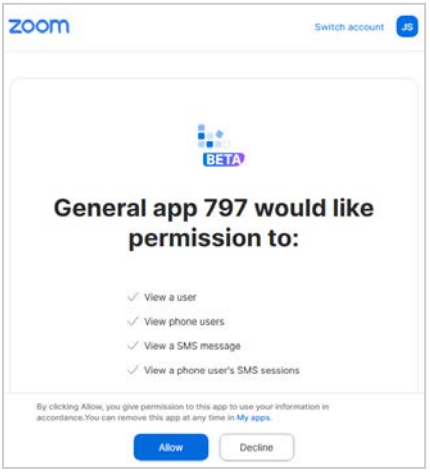
Collector Configuration

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.



Time Stamp Formatting

For more details on how to configure timestamps, see **Time Stamp Formatting**.

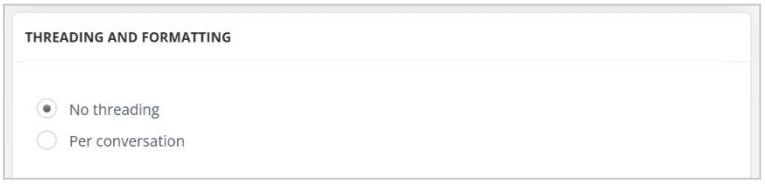
Advanced Configuration Options

For more details on how to configure advanced configuration options, see **Advanced Configuration Options**.

Threading and Formatting

You can control how messages are grouped in the output message using 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.



Message Body

Choose how imported messages should be displayed in the target. The available output message body formats are:

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

Note

The **Pure body** mode is active ONLY if the **No threading** mode is checked.

Attachments Configuration

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

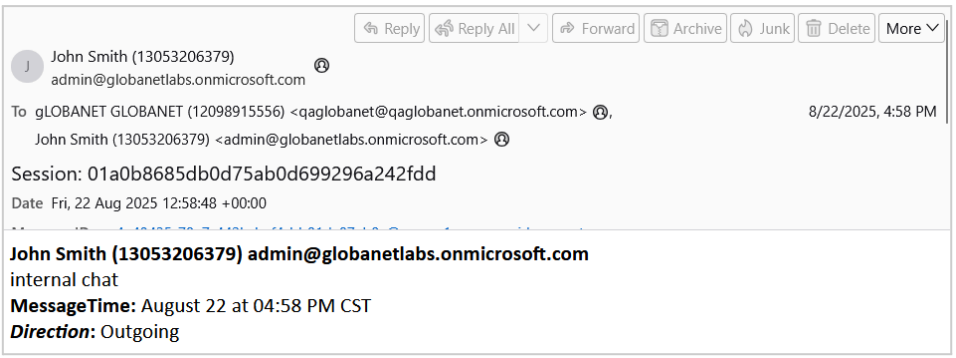
Otherwise, additional configurations will open for setup. See **Attachments Configuration**.

Next Steps

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

- **MONITORED USERS**
- **FILTERS**
- **TARGETS**
- **IMPORTER SETTINGS**

Once the configurations are completed and the importer is executed, data will be successfully processed and delivered to the target. Below is an example of an output message:



Supported Notifications

The importer supports the following notification preferences:

- **Import job finished**
- **Import job stopped**
- **No data captured**
- **Component deleted**
- **Importer deleted**
- **Failed to send webhook notification to target**
- **Import job finished with fatal error**
- **Import job finished with transient error**
- **Import job successfully completed**
- **Importer metric anomaly detected**
- **Importer metric deviation detected**
- **Importer performance metric anomaly detected**
- **Importer performance metric deviation detected**

For more information refer to **Notification Preferences**.

Monitored Users

Monitored users are individuals whose data is collected by Mergel.

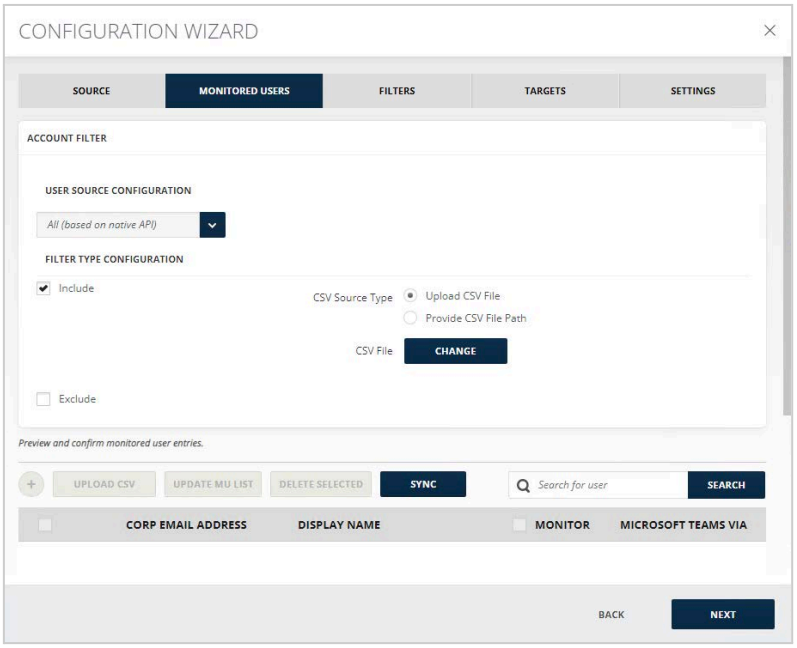
There are the following user sources from where monitored users can be added to the collector.

- **All (based on native API)**
- **Active Directory**
- **CSV File**
- **Manually maintain the list**
- **Microsoft Entra ID**

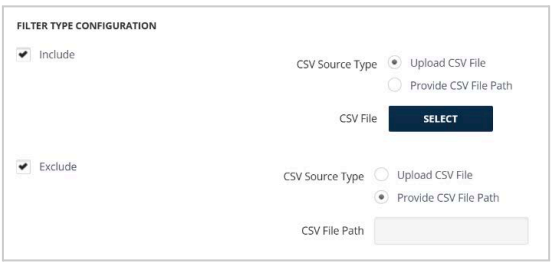
After configuring a user source, the monitored users will be added to the list either when clicking **SYNC** or once the importer setup is completed and run.

All (Based on Native API)

The **All (based on native API)** option dynamically imports the collector's users via its API during each subsequent session. It works for sources connected to Mergel by the API, such as Slack eDiscovery, Zoom Meetings, Microsoft Teams, etc.



- Enable **Include** and either provide a path to a CSV file or upload the CSV file directly to add users to the Monitored Users list who have not been retrieved via API.
- Enable **Exclude** and either specify the path of a CSV file or upload a CSV file containing their information to avoid monitoring specific users.

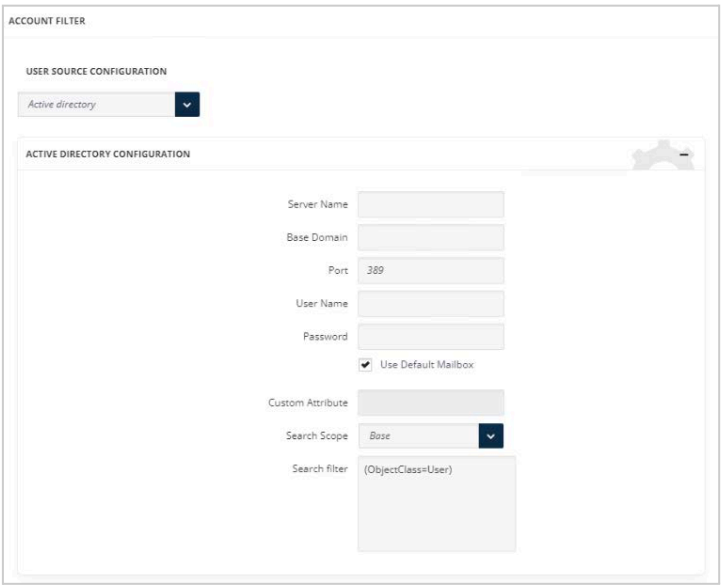


Active Directory

Active Directory (AD) is a directory service that Microsoft developed for the Windows domain networks. **Active Directory** allows retrieving a user list during each subsequent session dynamically via LDAP.

Once you select the **Active Directory** option, click **Active Directory Configuration** to set it up.

- **Server Name**: Enter the name of the LDAP server in the **Server Name** field.
- **Base Domain**: Specify the section of the directory where the search should begin in the **Base Domain** field (e.g., *ou=finance*, *dc=example*, *dc=com*).
- **Port**: Define the port of the LDAP server in the **Port** field.
- **Username**: Provide the username of the LDAP account in the **Username** field.
- **Password**: Enter the password corresponding to the LDAP account in the **Password** field to enable signing in.
- **Use Default Mailbox**: Mark the checkbox to activate or deactivate the **Custom Attribute** field.
- **Custom Attribute**: Use this field to extend the search of an asset.
- **Search Scope**: Define the scope of the search starting from the *Base Domain*. Select one of the following options from the drop-down menu:
    - **Base**: Considers only the specified *Base Domain* for the search.
    - **OneLevel**: Considers only the immediate children of the specified *Base Domain*.
    - **Subtree**: Considers the specified *Base Domain* and all its subordinate entries.
- **Search Filter**: Add filters in the **Search Filter** field to restrict the users or groups permitted to access the application.



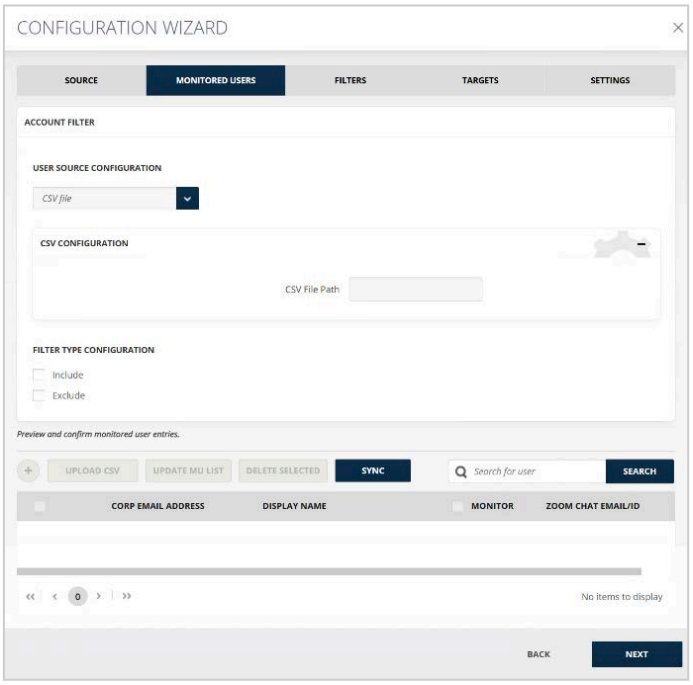
Users who do not have the selected attribute or a Display Name will not be returned by the LDAP query.

- **Include** is used for providing a path to a CSV file or uploading a CSV file with a list of users that have not been retrieved via API should be included in the Monitored Users.
- **Exclude** is used for providing a path CSV file or uploading a CSV file with the users that should not be monitored as opposed to **Include**.

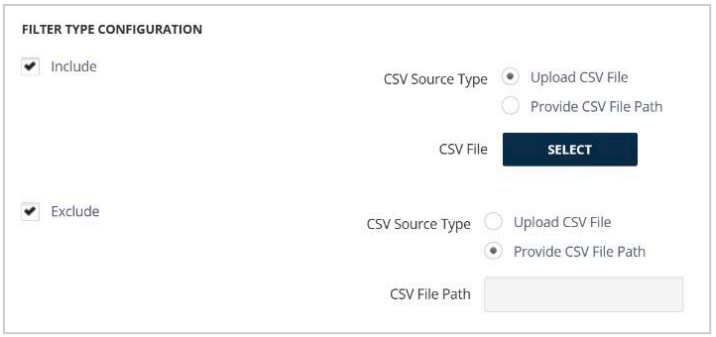
CSV File

The **CSV file** option allows adding our own CSV file based on which the monitored users will be added.

The CSV file should include two columns: email address of the user and display name of the user, both required. The rest of the columns will be ignored. If the display name is not available, it can be filled instead with the email address.

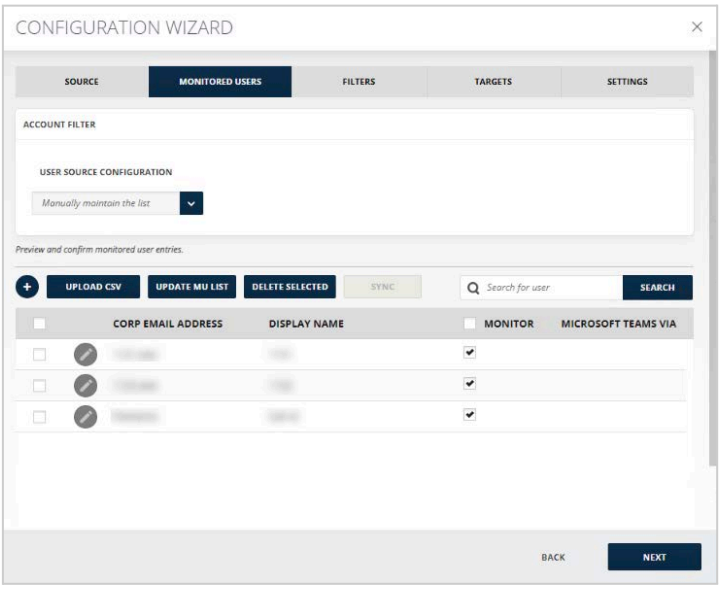


- **Include** is used for providing a path to a CSV file or uploading a CSV file with a list of users that have not been retrieved via API should be included in the Monitored Users.
- **Exclude** is used for providing a path CSV file or uploading a CSV file with the users that should not be monitored as opposed to **Include**.



Manually Maintain the List

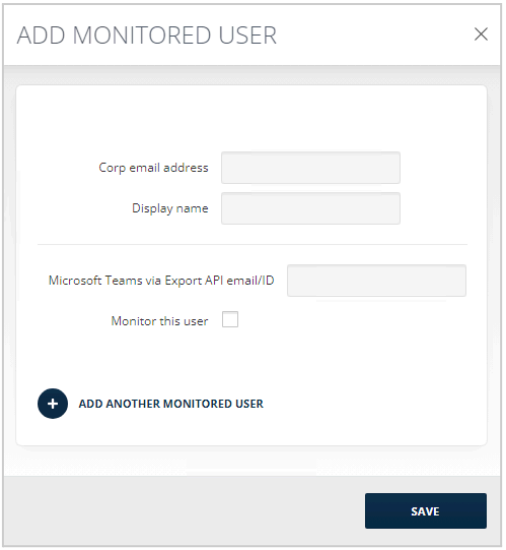
This option allows manually adding and managing users.



After selecting **Manually maintain the list** from **User Source Configuration**, the below list of monitored users will become active, where you can make the following changes.

1. **Add Monitored User** opens a window where you can add details of a user to be monitored.
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. **Monitor.** If checked, monitors the user, if not, the user is not monitored.

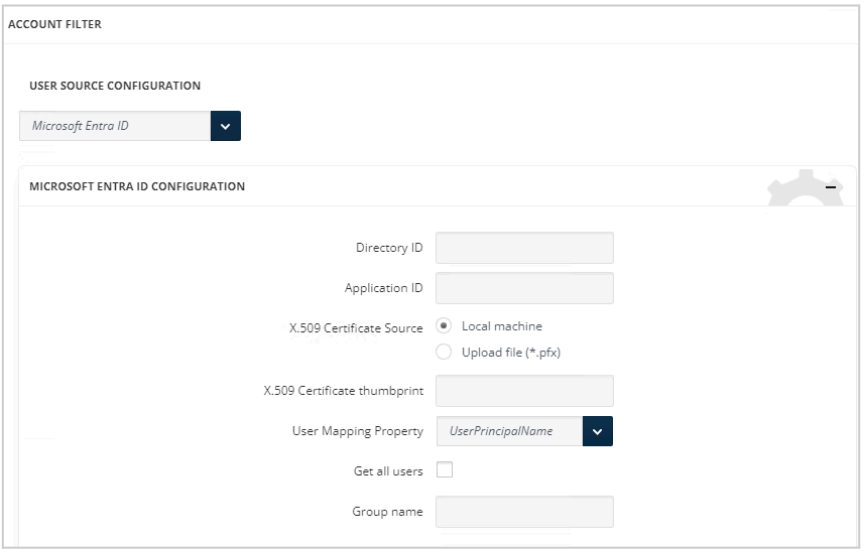
To add a monitored user, click **Add Monitored User** and fill in the necessary information. The same information can later be edited by clicking **Edit Monitored User** as described in point 8.



- **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.
- **Monitor this user** option if checked monitors the user and vice versa.

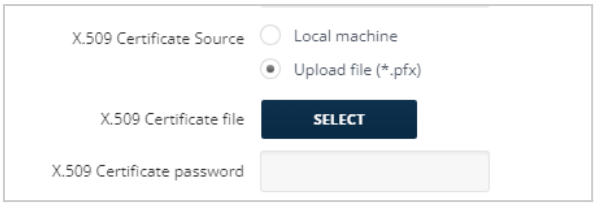
Microsoft Entra ID

The **Microsoft Entra ID** option dynamically imports users from the Microsoft Azure Directory during each subsequent session. By expanding **Configure Microsoft Entra ID**, the **Microsoft Entra ID Configuration** screen opens.



To configure the section:

1. Specify **Directory ID** and **Application ID**. For more details on how to create an app in Microsoft Azure and grant permissions, see **Creating a Microsoft Entra ID Application**.
2. Provide **X.509 Certificate Thumbprint** in case you activate the **Local machine** radio button as the X.509 Certificate source.
3. In case you activate **Upload file (*.pfx)**, click the **Select** button to upload the certificate and provide **X.509 Certificate password**.



The **Certificate thumbprint** field will be auto populated in case the collector was previously configured by uploading a certificate.

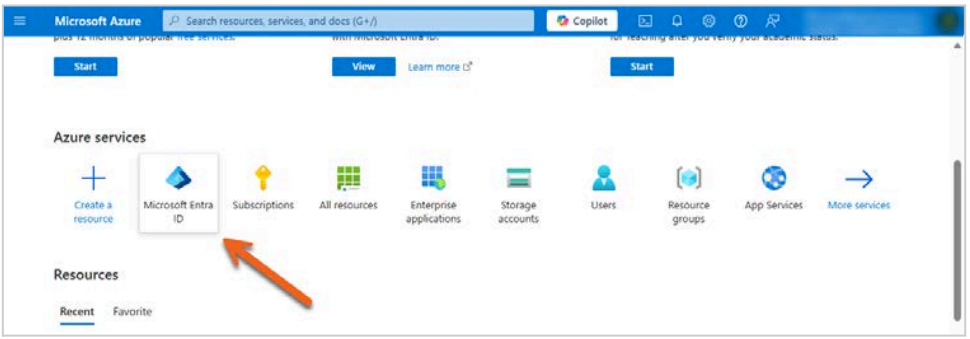
4. Select **User Mapping Property** from the drop-down list. Note that **User Principal Name** always exists.
5. Enable **Get all users** checkbox to get all users from the source.
6. Enter **Group name** in case the **Get all users** checkbox is disabled.

Creating a Microsoft Entra ID Application

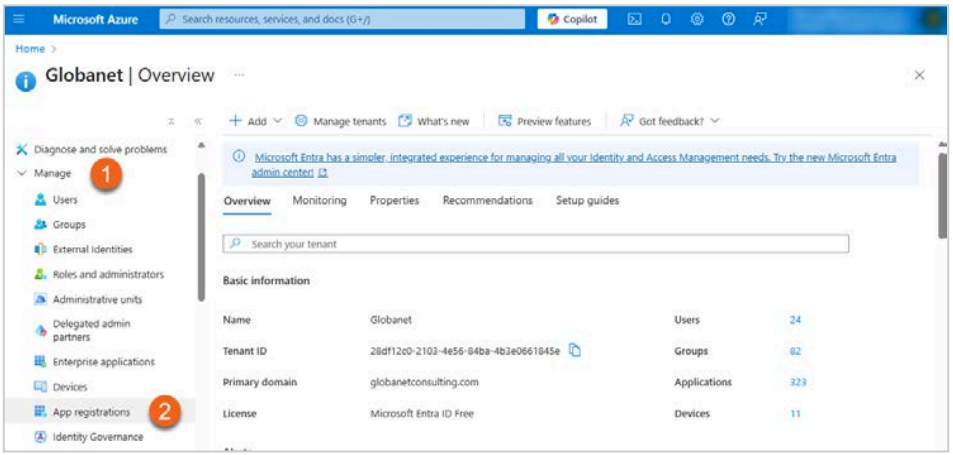
The Office 365 or Azure administrator in your organization must complete the steps detailed in the sections below.

Registering an Application

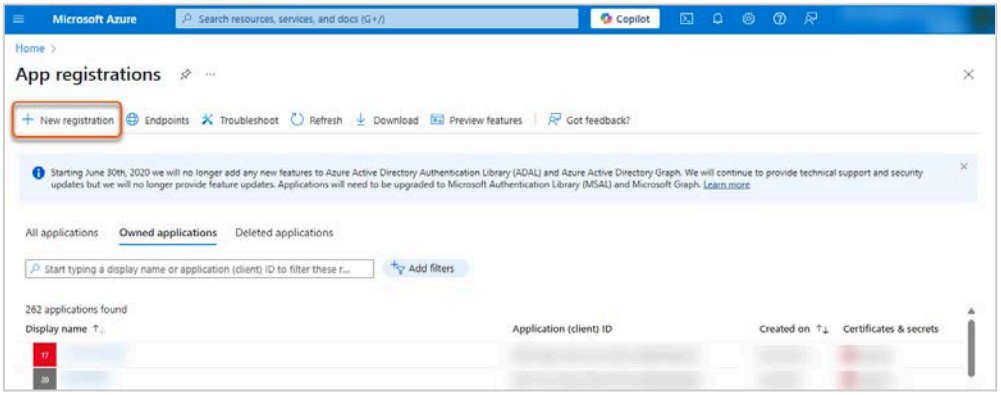
1. Sign in to Azure Portal.
2. Select **Microsoft Entra ID** under **Azure services**.



3. In the left-hand navigation pane, click **Manage > App registrations**.



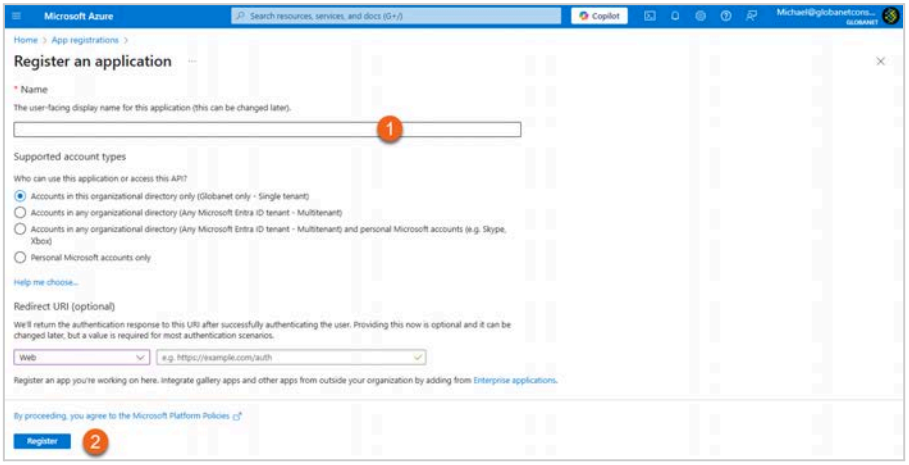
4. Click **New registration**.



5. To register an application:

   5.1. Enter a **Name** for the application.

   5.2. Click **Register**.



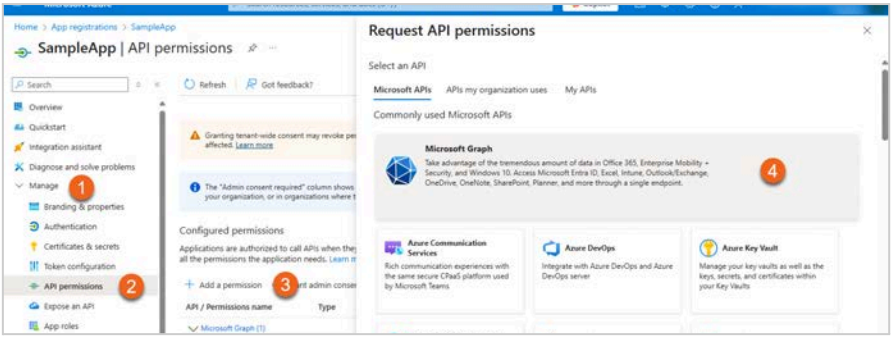
6. An **Application (client) ID** and **Directory (tenant) ID** will be generated. Keep both for configuring the option in Mergel.

Granting Permissions

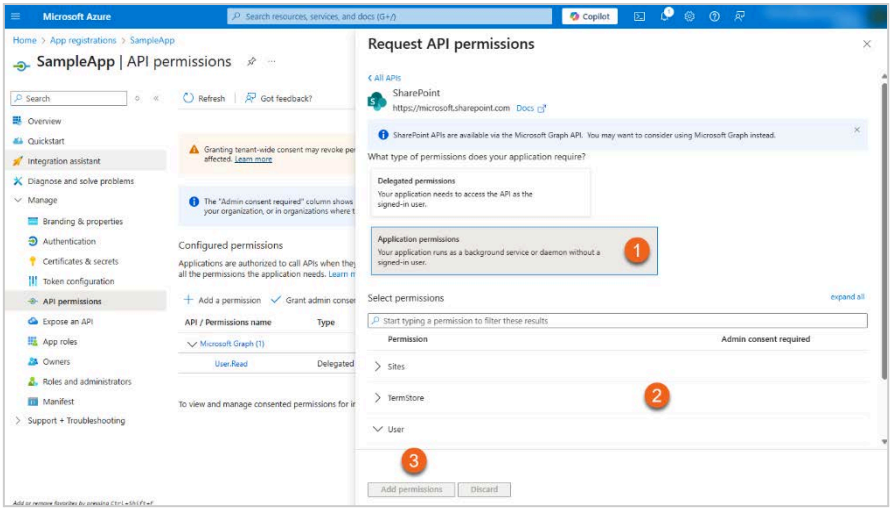
Adding Microsoft Graph API Permissions

To add **Microsoft Graph** API permissions:

1. In the left-hand navigation pane, click **Manage > API permissions**.
2. Click **Add a permission**.
3. In the opened pane select the **Microsoft Graph** API.

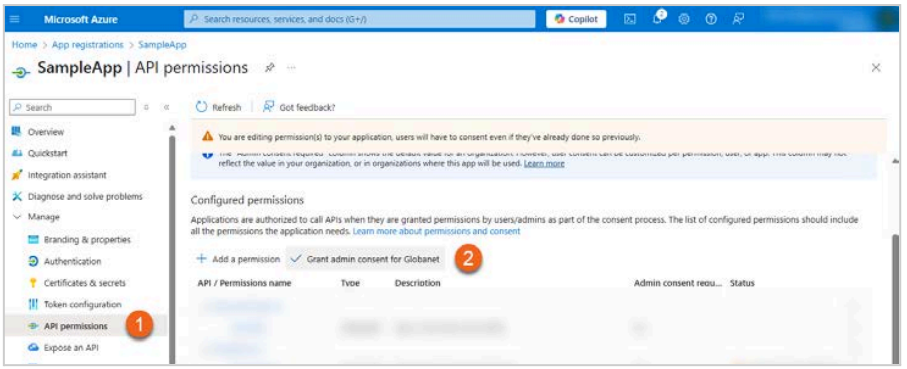


4. To add the necessary permission:
   4.1. Click **Application permissions**.
   4.2. Add the following permissions:
      4.2.1. GroupMember.Read.All
      4.2.2. User.Read.All
   4.3. Click **Add permissions**.



Granting Admin Consent

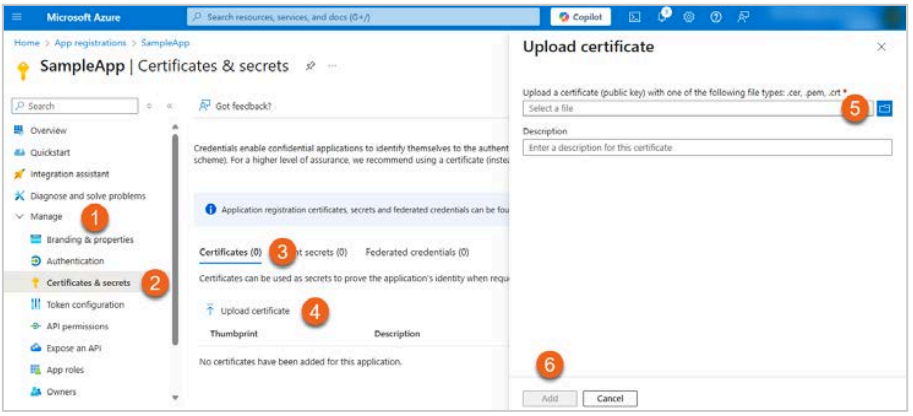
1. Go back to **API permissions**.
2. Click **Grant admin consent** for your company to grant the added permissions.



Uploading a Certificate

To upload a certificate:

1. In the left-hand navigation pane, go to **Manage > Certificates & secrets**.
2. Select Certificates.
3. Click **Upload certificate**.
4. Select a certificate (public key) with one of the following file types: `.cer`, `.pem`, `.crt`.
5. Click **Add**.

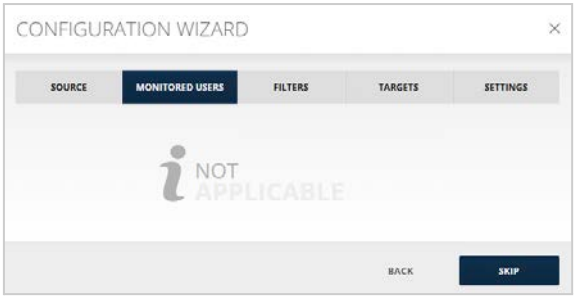


A certificate **thumbprint** will be generated. Keep the value for configuring the collector in Merge1.

For more information on how to create a certificate, see **Creating a Certificate (Private and Public Keys)**.

Skip Monitored Users

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:

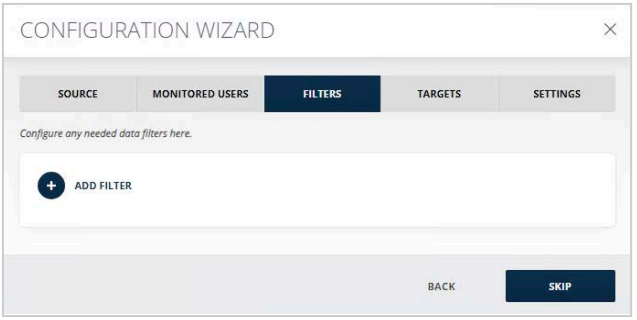
- Amazon S3
- Audio Video
- Bloomberg
- BlackBerry
- CellTrust
- DB
- Dubber SMS
- Dubber Recordings
- EML
- FX Connect
- FX Connect (File-Based)
- Google Messages
- IceChat
- iMessage
- JSON
- LSEG (Refinitiv)
- Microsoft Teams for Audio and Video
- NTR-X
- Pivot
- Redtail Speak
- Symphony
- Text-Delimited
- UBS
- Verba
- Verint
- Web Page Capture
- WhatsApp
- XIP
- XSLT/XML
- Yieldbroker
- YouTube

Filters

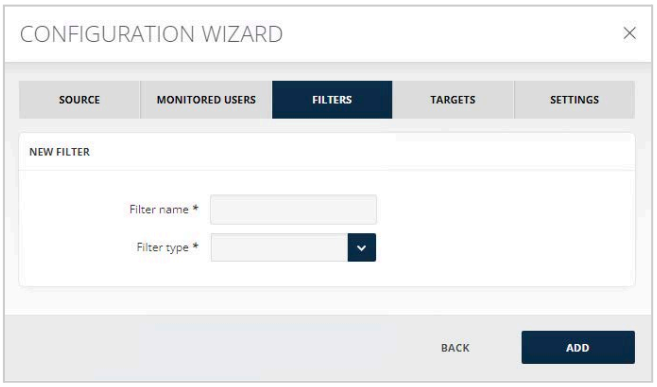
Filters are used to filter or separate data according to content. They can be configured to match specific email addresses, XML tags with specific values, or other information using LDAP queries.

To configure the filters:

1. Click **Add Filter**.



2. Enter a **Filter Name** and select **Filter Type**. Mergel has the following filter types:
   - **Active Directory Filter**
   - **Keyword Filter**
   - **Mail Filter**
   - **XML Filter**
   - **Message Size Filter**
   - **Time Stamp Filter**
   - **Participants Count Filter**.

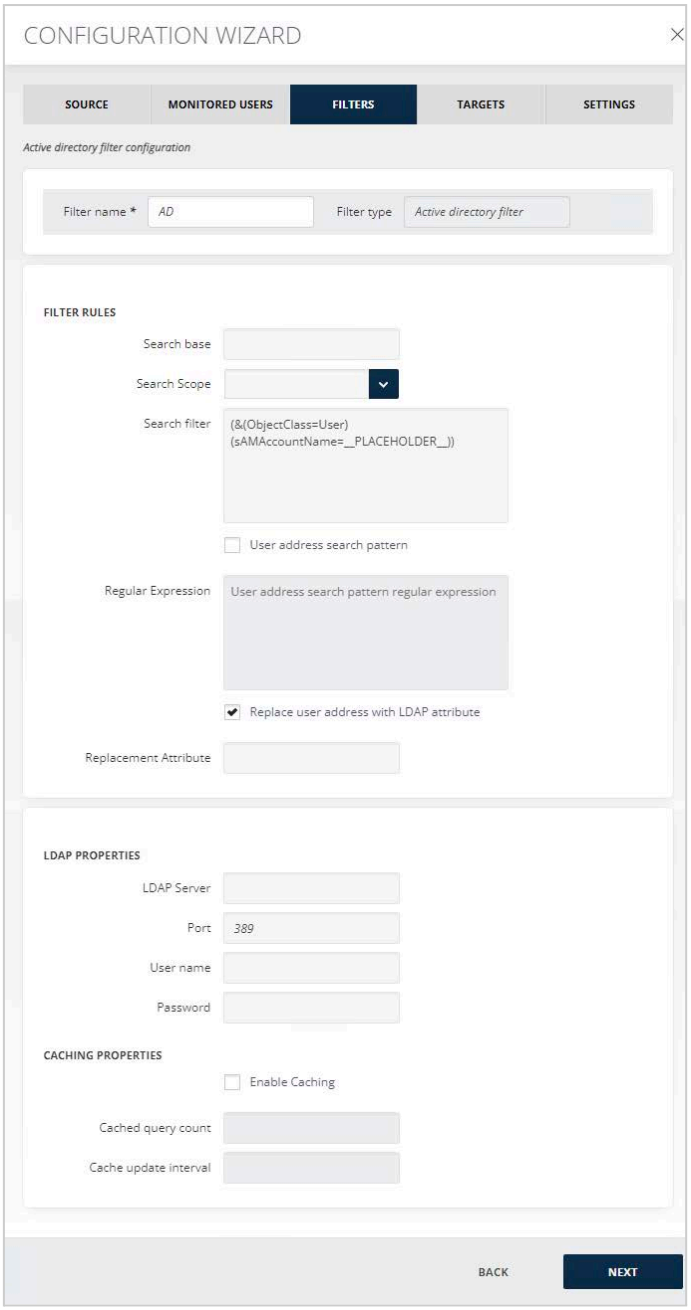


Active Directory Filter

Note

The installation of the following filter requires proficiency in LDAP.

The **Active Directory** filter matches segments that contain values specified with an LDAP expression. Values are retrieved each time the importer is run.



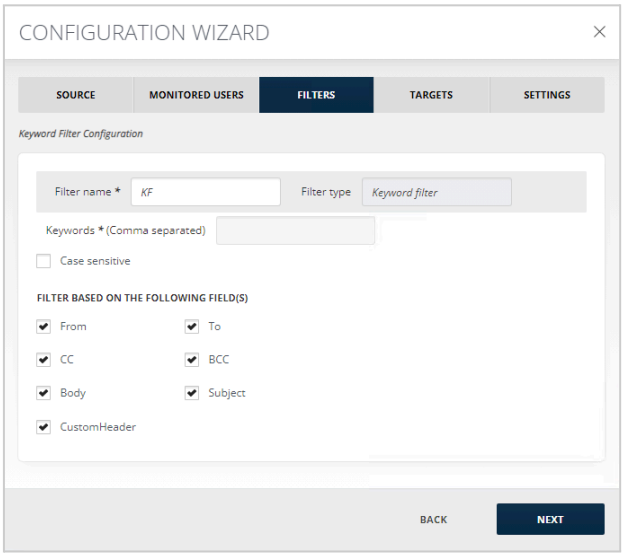
1. **Search Base** sets the starting point for the search in the directory tree. For example, you might need to query the entire directory, in which case the search base must specify the root of the directory service. Or you might need to query a specific organizational unit (OU) in the directory. For example: ou=finance, dc=example, dc=com.
2. **Search Scope** sets the scope of the search starting from the search base:
    - **All** - all levels inside Active Directory are searched.
    - **Sub Level** - only levels under selected Search Base are searched.
    - **This Level** - only searches the specified by the Search Base level.
3. **Search Filter** defines search criteria and provides more efficient and effective searches. A filter specifies the conditions that must be met for a record to be included in the record set (or collection) that results from a query.

4. When **User Address Search Pattern** is enabled, the placeholder in the **Search Filter** field is replaced with each address that is returned by the Regular Expression (5). The default expression retrieves values from all objects returned by the Regular Expression and classified as a **User**. For example, the following line if input in Regular Expression field, will return all users with the relevant domain: Z^_a-z{|}~])*@[b | B]loomberg.net$^[-!#$%&'*+/0-9=?A-Z^_a-z{|}~](\.?[-!#$%&'*+/0-9=?A-
5. In the **Regular Expression** field, the default expression is input for retrieving values when **User Address Search Pattern** is enabled (see pt. 4).
6. If **Replace User Address with LDAP Attribute** is checked and **Replacement Attribute** is added below, it replaces each user's address with their respective AD attributes as specified.
7. Write the Mail address in this field, that is activated when **Replace User Address with LDAP Attribute** is checked (see pt. 6).
8. In the **LDAP Server** field, fill in the name of the **LDAP Server**.
9. In the **Port** field, define the **Port** of the LDAP Server.
10. In the **User Name** field, add the username of the LDAP account.
11. In the **Password** field, fill in the corresponding password to the LDAP account for signing in.
12. Check **Enable Caching** option if you want to enable saving the query result for future imports. This will allow skipping searching in the AD during the next Import and will automatically fetch the cached results.
13. In the **Cached Query Count** field, specify the number of queries that should be cached.
14. In the **Cache Update Interval** field, specify the time after which the cached queries should be updated.

Users who do not have the selected attribute or a Display Name will not be returned by the LDAP query.

Keyword Filter

Keyword filter allows you to retrieve and refine the data by mentioned keywords and collect it in the specified target.

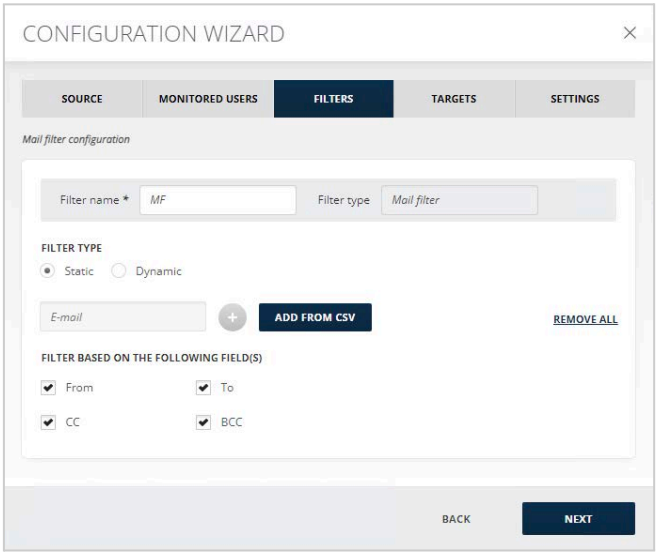


1. In the **Keywords (Comma separated)** field, the keywords, by which the data will be filtered, should be added. The keywords need to be separated by commas for the filtering to work. Keywords are searched for in the body of the message, as well as in its subject.
2. If **Case Sensitive** option is 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 Mergel 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.

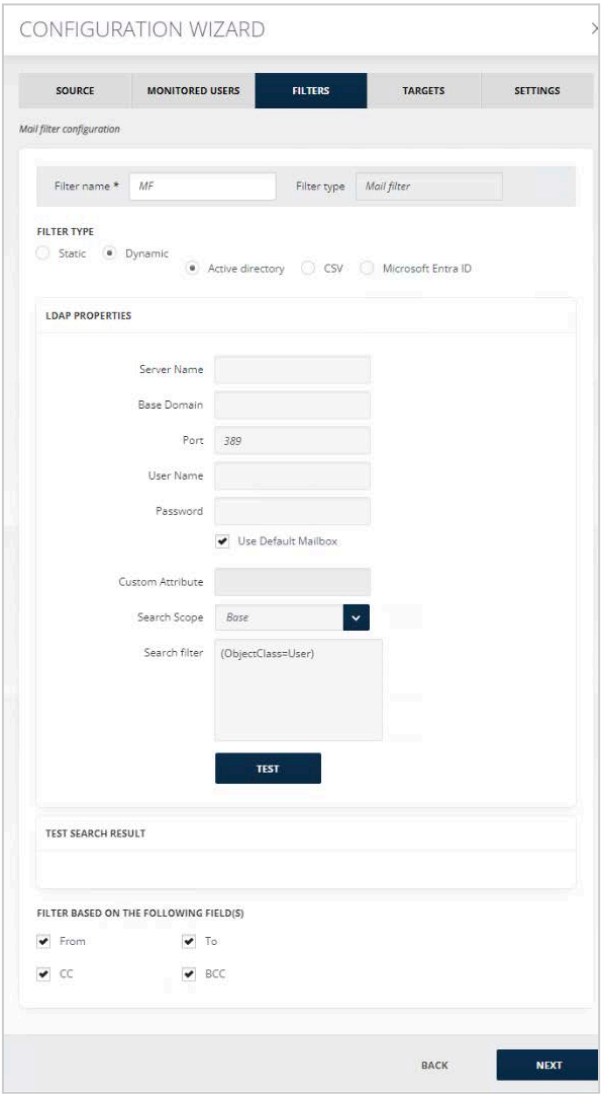


Dynamic Filter is used to specify email addresses dynamically from an LDAP server, from a CSV file, or Microsoft Entra ID. This means, that if any changes are applied to the user list in the server or in the CSV file, the filter settings are refreshed, and values are retrieved newly each time the Importer is run.

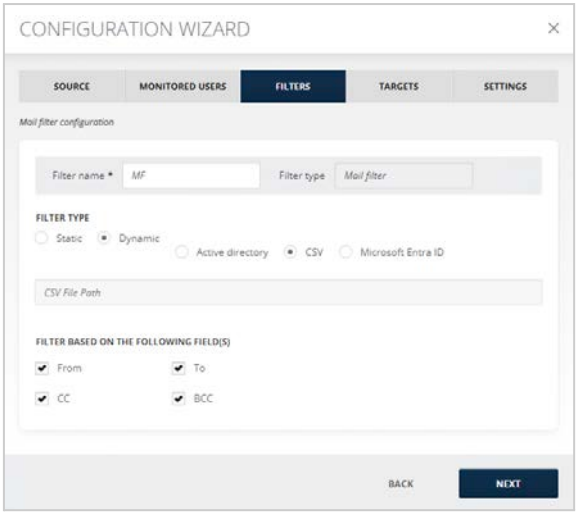
Here are the steps for setting up LDAP Server to set up Dynamic Filter:

1. In the **Server Name** field, fill in the name of the LDAP Server.
2. Enter the **Base Domain**.

3. In the **Port** field, define the Port of the LDAP Server.
4. In the **User Name** field, add the username of the LDAP account.
5. In the **Password** field, fill in the corresponding password to the LDAP account for signing in.
6. Mark the **Use Default Mailbox** checkbox to activate/deactivate the **Custom Attribute** field.
7. Use the **Custom Attribute** field to extend the search of an asset.
8. **Search Scope** defines the scope of the search starting from the Base Domain.
   - **Base** - only the specified Base Domain should be considered for search.
   - **OneLevel** - only the immediate children of the specified Base Domain should be considered.
   - **Subtree** - the specified entry as Base Domain, as well as all its subordinates should be considered.
9. In **Search Filter** field, add filters that can be used to restrict the number of users or groups that are permitted to access an application.
10. Click **Export to CSV** to export results of total count after CSV file LDAP query successful execution.

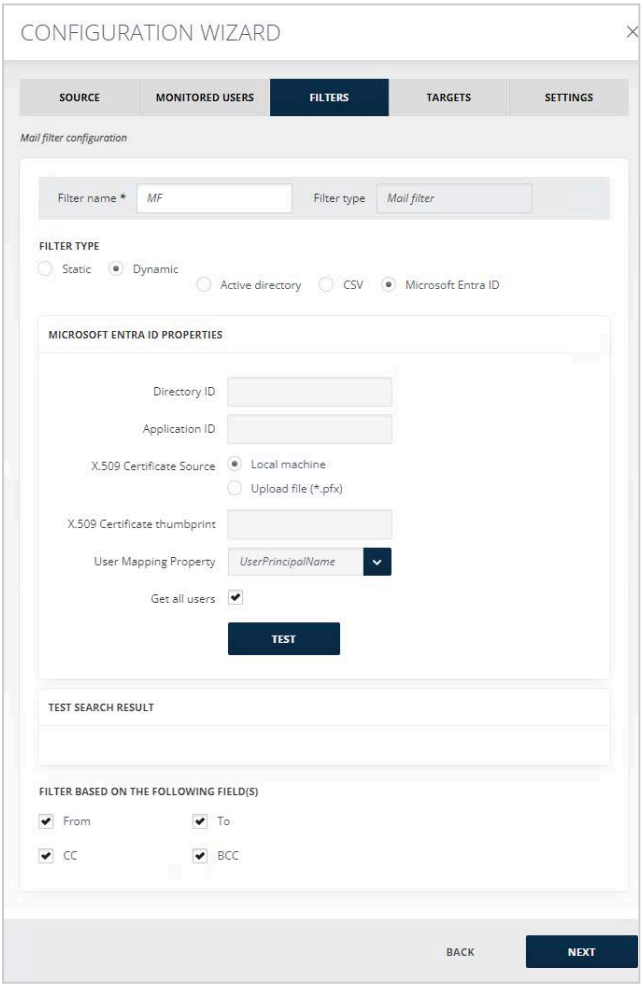


For using a **CSV file** as a dynamic filter, add the path to the CSV file in the field. If something is updated in the CSV file, it will be applied the next time the Importer is run.



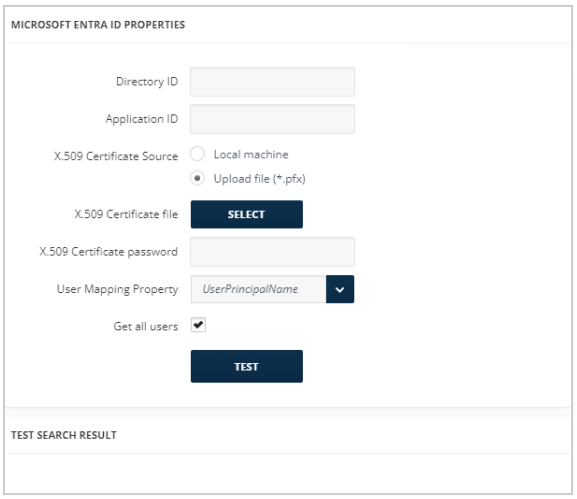
To configure the **Microsoft Entra ID** section:

1. Specify **Directory ID** and **Application ID**. For more details on how to create an app in Microsoft Azure and grant permissions, see **Creating a Microsoft Entra ID Application**.



2. Provide **X.509 Certificate Thumbprint** in case you activate the **Local machine** radio button as the X.509 Certificate source.

3. In case you activate **Upload file (*.pfx)**, click the **Select** button to upload the certificate and provide **X.509 Certificate Password**.



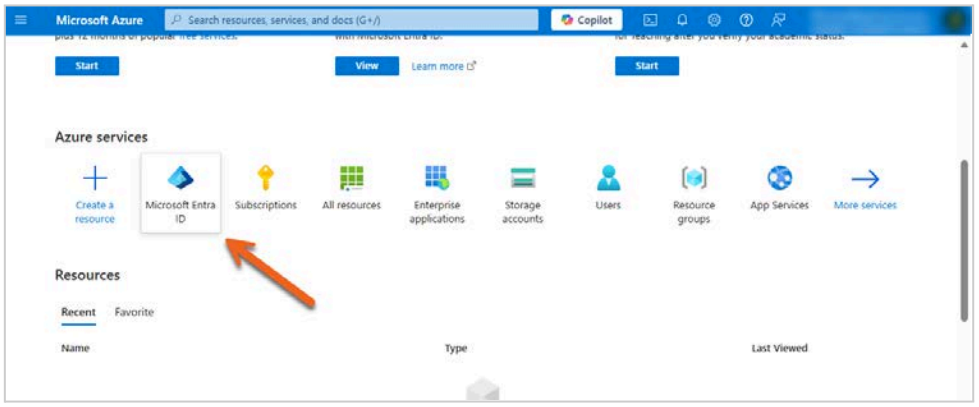
4. Select **User Mapping Property** form the drop-down list. Note that **User Principal Name** always exists.
5. Enable **Get all users** checkbox to get all users from the source.
6. Enter **Group name** in case the **Get all users** checkbox is disabled.
7. Click **Test.**
8. Click **Export to CSV** to see the **Test Search Results**.

Creating a Microsoft Entra ID Application

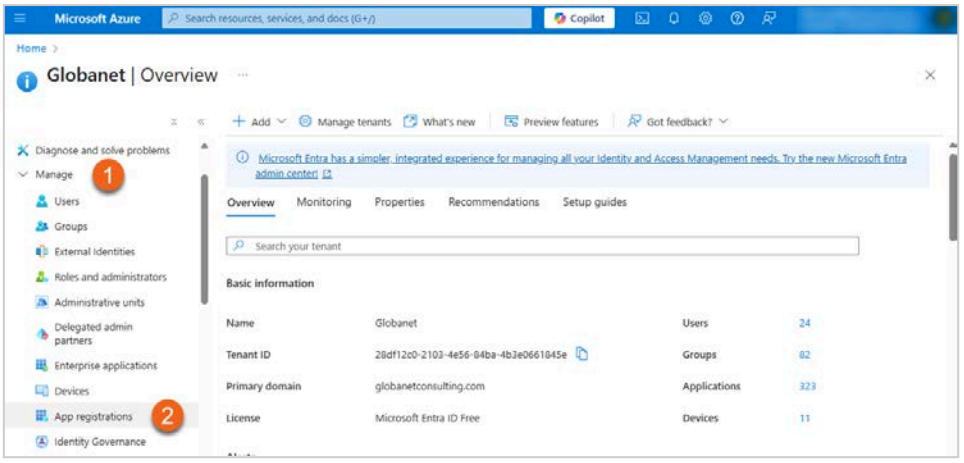
The Office 365 or Azure administrator in your organization must complete the steps detailed in the sections below.

Registering an Application

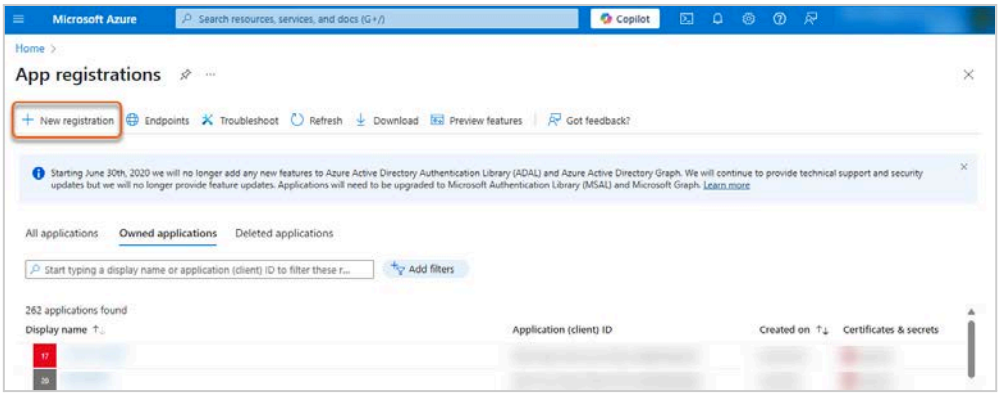
1. Sign in to Azure Portal.
2. Select **Microsoft Entra ID** under **Azure services**.



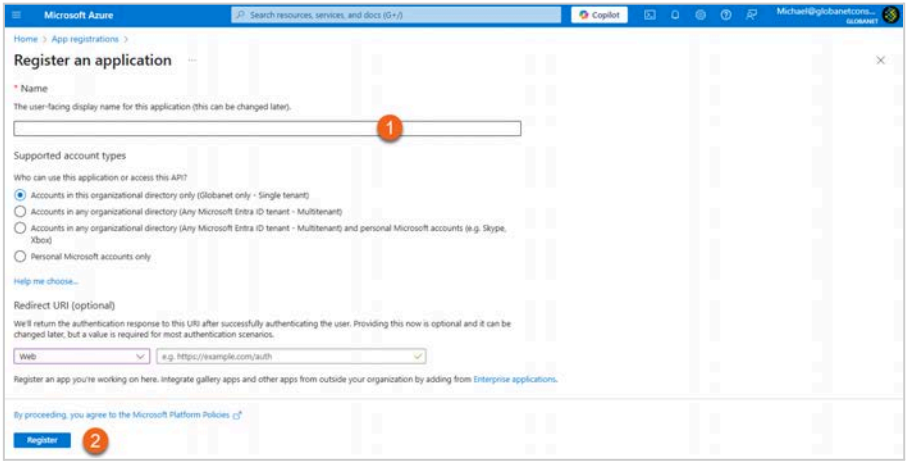
3. In the left-hand navigation pane, click **Manage > App registrations**.



4. Click **New registration**.



5. To register an application:
   5.1. Enter a **Name** for the application.
   5.2. Click **Register**.



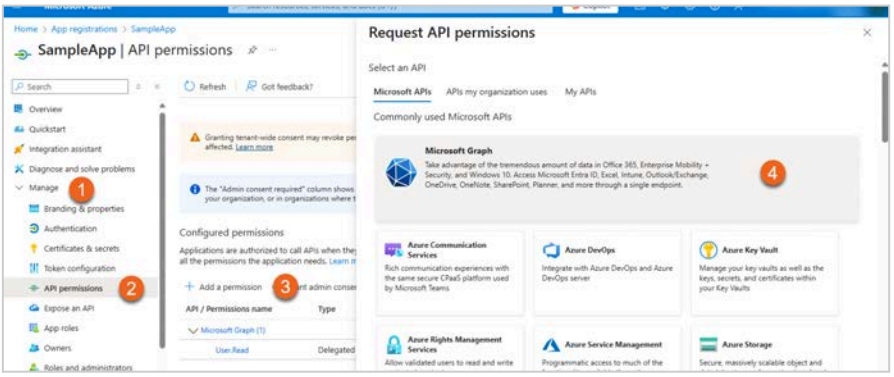
6. An **Application (client) ID** and **Directory (tenant) ID** will be generated. Keep both for configuring the filter in Mergel.

Granting Permissions

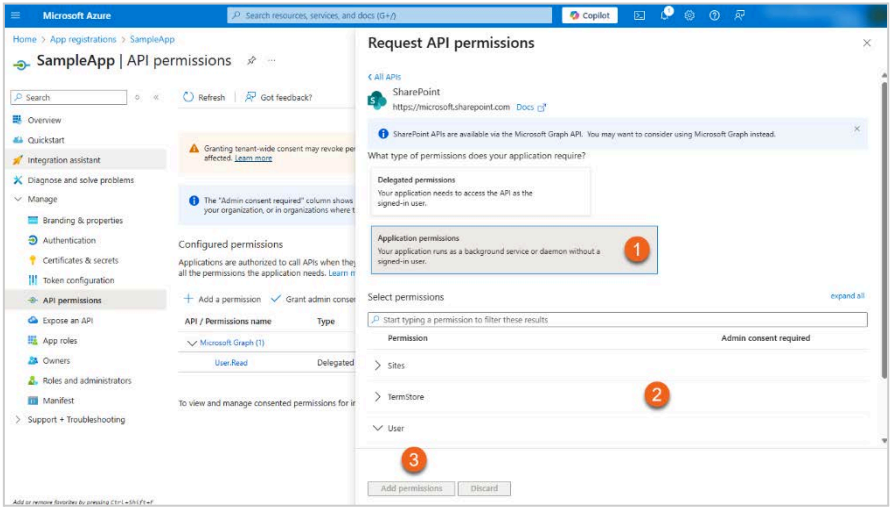
Adding Microsoft Graph API Permissions

To add **Microsoft Graph** API permissions:

1. In the left-hand navigation pane, click **Manage > API permissions**.
2. Click **Add a permission**.
3. In the opened pane select the **Microsoft Graph** API.

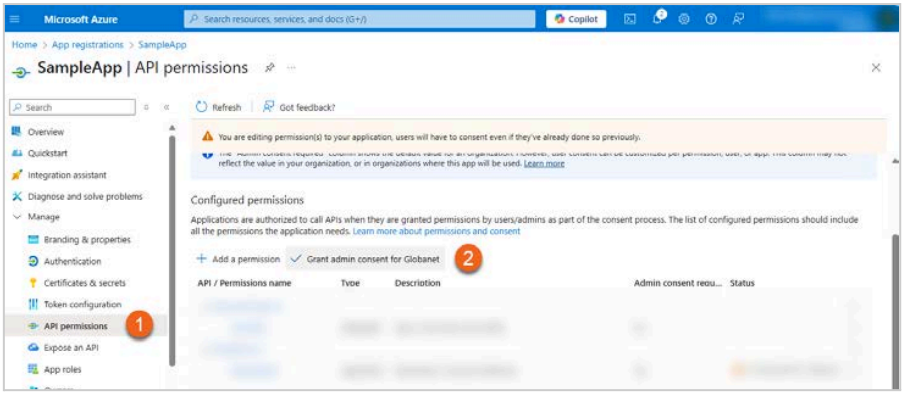


4. To add the necessary permission:
   4.1. Click **Application permissions**.
   4.2. Add the following permissions:
      4.2.1. GroupMember.Read.All
      4.2.2. User.Read.All
   4.3. Click **Add permissions**.



Granting Admin Consent

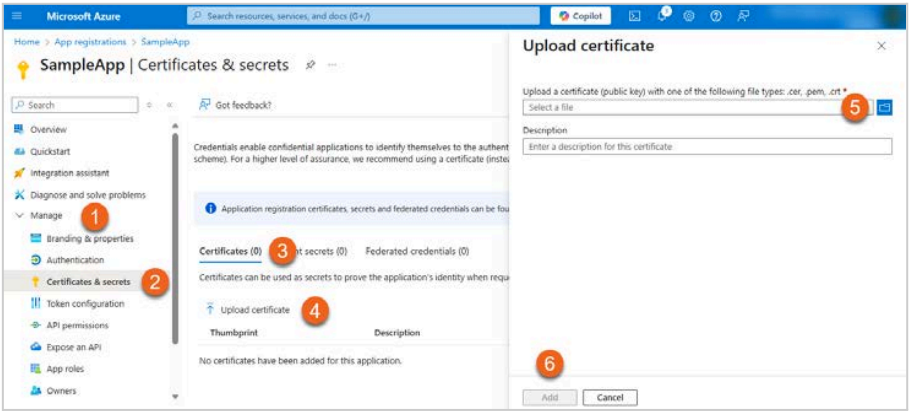
1. Go back to **API permissions**.
2. Click **Grant admin consent** for your company to grant the added permissions.



Uploading a Certificate

To upload a certificate:

1. In the left-hand navigation pane, go to **Manage > Certificates & secrets**.
2. Select **Certificates**.
3. Click **Upload certificate**.
4. Select a certificate (public key) with one of the following file types: `.cer`, `.pem`, `.crt`.
5. Click **Add**.

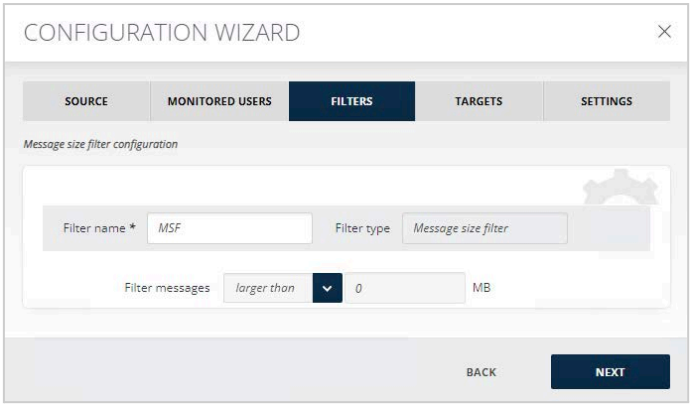


A certificate **thumbprint** will be generated. Keep the value for configuring the collector in Mergel.

For more information on how to create a certificate, see **Creating a Certificate (Private and Public Keys)**.

Message Size Filter

This allows filtering messages to a different target based on their size.

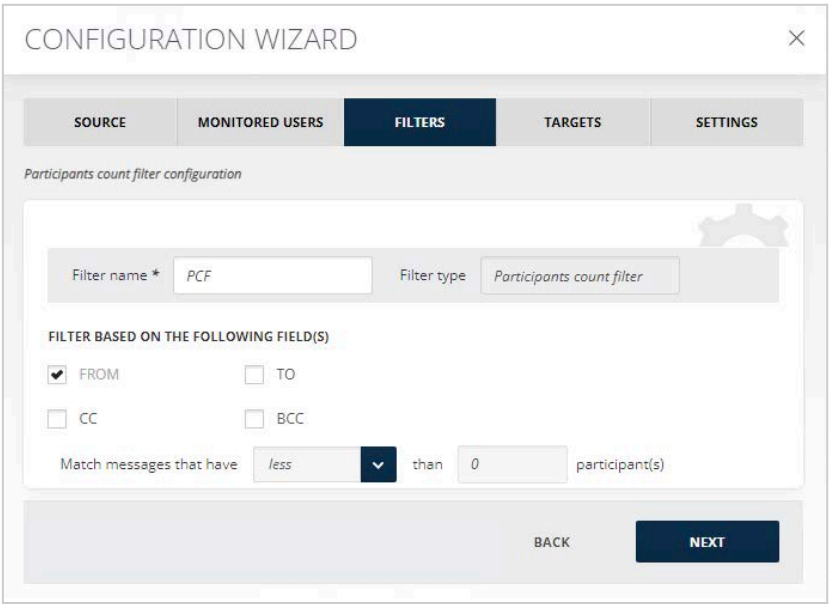


In the **Filter messages larger than/smaller than _ MB**, **larger than** or **smaller than** should be selected and the size of messages should be entered:

- 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.

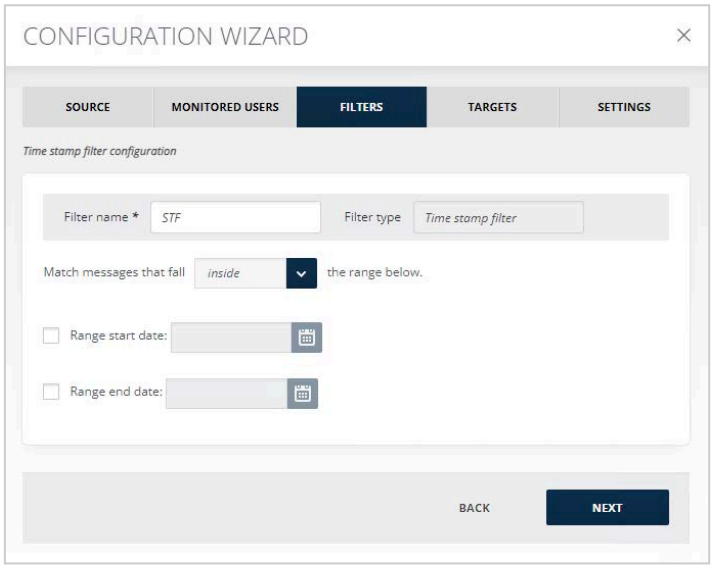


The filter is configured based on the **FROM**, **TO**, **CC**, and **BCC** checkboxes. Note that the **FROM** field is always marked as checked and is not editable.

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.

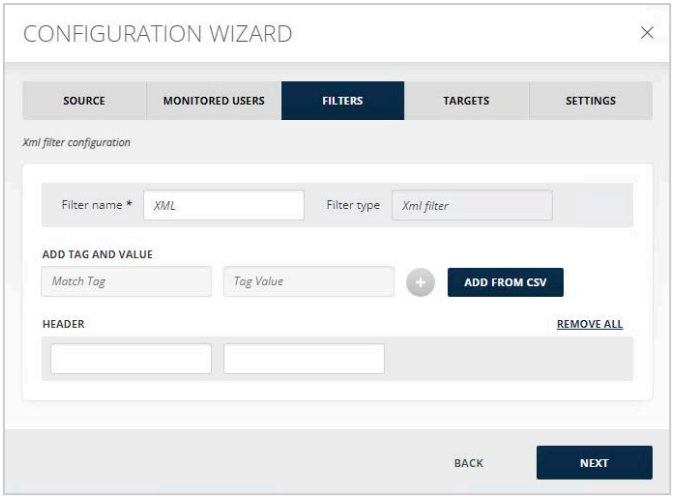


Here are the steps for configuring the filter:

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, the content between that cut-off dates 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, the content after that specified start date is filtered.
    - In case only the **Range start date** is specified, and the **outside** option is selected from the drop-down list, 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, the content before that specified end date 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.



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 that only one header can be added to a single filter, so for each country, in this case, a separate filter needs to be created.

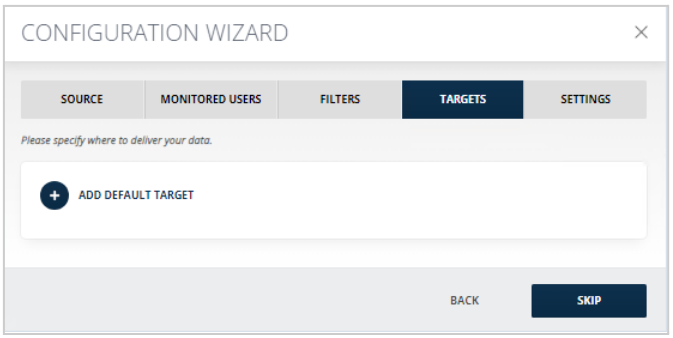
This filter works only with XML sources:

- Bloomberg
- CellTrust
- IceChat
- Pivot
- Symphony
- UBS
- XSLT/XML

Targets

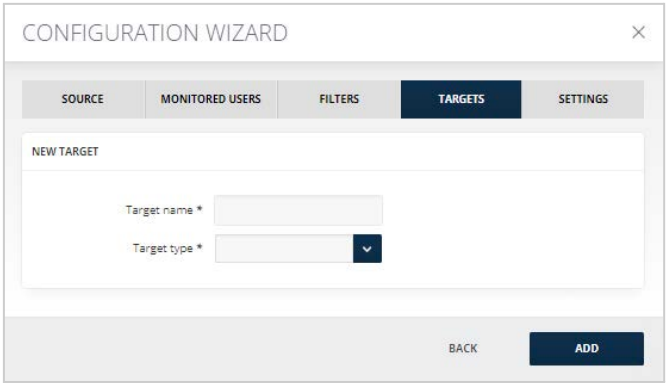
After filling in all the information related to the Filters, click **Next** and you will be redirected to the **Targets** tab. You can either fill in the **Targets** or skip it and fill out later, from the **Importer** panel under the **Configurations**.

Please 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 that these are mandatory fields.

When you have selected the exact target, click **Next**.

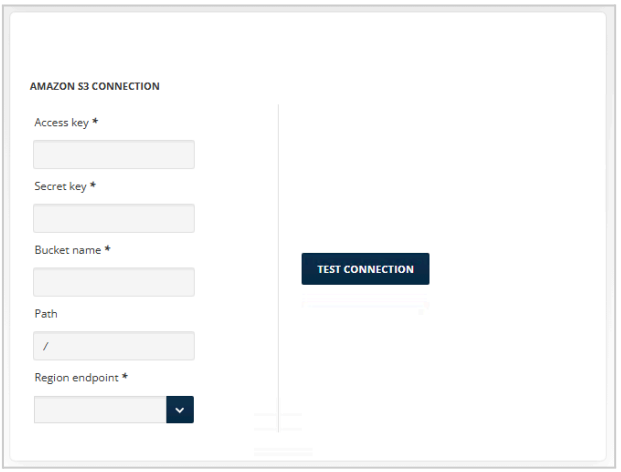
Mergel offers the following types of targets:

1. **Amazon S3**: Delivers data directly to the Amazon S3 storage.
2. **Azure Blob**: Delivers data directly to the Azure Blob target.
3. **Direct SMTP**: Delivers data to an SMTP server address directly from the server.
4. **EV Server**: Archives data in an Enterprise Vault archive in EML or MSG formats.
5. **EWS Server**: Delivers data to an Exchange Web Services server.
6. **Failed**: Lists all imports as failed delivery attempts.
7. **Folder**: Delivers data in EML, MSG or JSON formats to specified folder.
8. **Google Vault**: Delivers data to Google Vault.
9. **Ignored**: Ignored target is used to mark all items sent to it as Ignored.

10. **Report**: Prints the output of the data inside the log file, usually used for diagnostics.
11. **SFTP**: Delivers data to an FTP/SFTP server address.
12. **SMTP**: Delivers data to an SMTP server address using a relay.

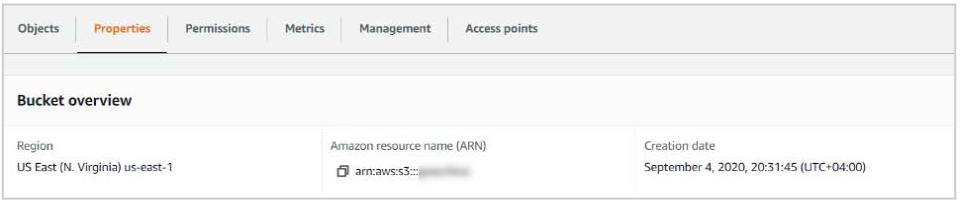
Amazon S3 Target

To deliver data collected from different sources to the Amazon S3 storage, the storage should be configured accordingly.



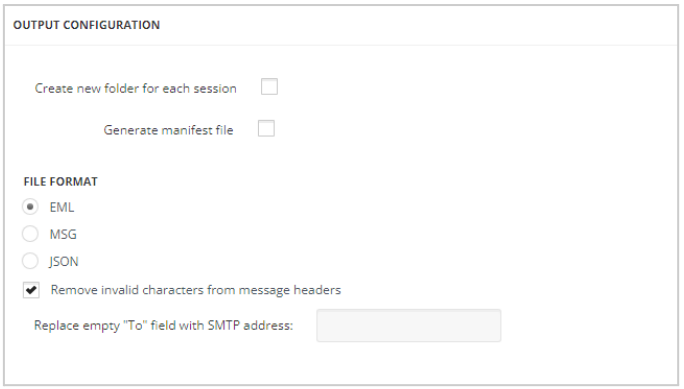
The following information is required:

- **Access key:** Enter the access key found under *Users* > *Security Credentials* in your Amazon S3 account. This field is required for authentication.
- **Secret key:** Enter the secret key obtained during the setup of *Security Credentials*. Save it securely, as this key is provided only once. If the secret key is incorrect, the connection will fail.
- **Bucket name:** Enter the name of the archive bucket where your data is stored. If the bucket name is invalid, data will not be retrieved.
- **Path:** If specified, data will be delivered to the designated folder within the bucket.
- **Region endpoint:** Enter the *Region Endpoint* located under *Bucket Overview* > *Properties* in your Amazon S3 bucket. Note that if the *Region Endpoint* is not set correctly, the archive content will not be captured or processed.



Output Configuration

1. **Create new folder for each session**. If checked will create a separate folder for each time the importer is run, named after the date and time of the run.
2. **Generate manifest file**. If checked, a CSV file containing the list of generated message files will be generated.



3. **EML, MSG, JSON**. If one of the options is enabled, the exported message will be in the respective format. See the difference between the file types in the table below.

EML	MSG	JSON
An extension supported by multiple email clients like Outlook Express, Thunderbird, and Windows Live Mail.	An extension supported by Microsoft Outlook.	A lightweight data-interchange format.
Files can be read by its email client along with others like Outlook can read EML files.	Files can only be saved for emails and messages.	Easy to read and write.
Files can be opened in a text editor similar to text files.	Files can only be opened by MAPI-based applications.	Easy for machines to parse and generate.

   You can easily convert your MSG file to 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.

4. **Remove invalid characters from message headers**. The 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.

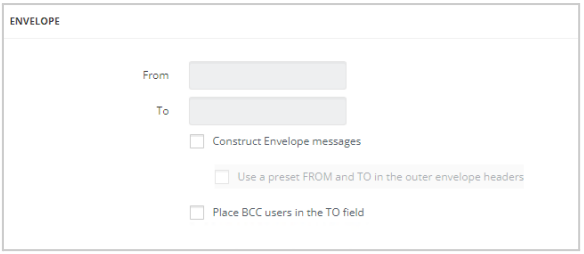
Note that JSON file format is available in all the collectors' folder targets but currently is supported only for the below-listed collectors. For other collectors, an error will be thrown.

- Amazon S3
- Audio Video
- Box
- ChatGPT
- Chatter / Chatter Cipher Cloud
- Cloud9
- Copilot
- DB (newly created ones, not upgraded)
- Dropbox Business
- Dubber Speik Recordings

- Dubber Speik SMS
- FX Connect
- FX Connect (File-Based)
- Google Messages
- iMessage
- Jabber Enterprise
- JSON
- Microsoft Teams for Audio and Video
- Microsoft Teams via Export API
- NTR-X
- OneDrive for Business
- Pivot
- Redtail Speak
- LSEG (Refinitiv)
- RingCentral
- ServiceNow
- SharePoint
- Slack eDiscovery
- Skype for Business
- Symphony
- Text-Delimited (newly created ones, not upgraded)
- X (Twitter)
- Verba
- Verint
- 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

Envelope

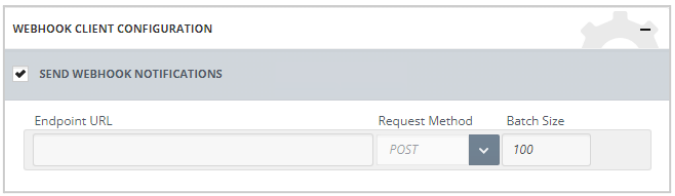
1. The **Construct Envelope messages** option when enabled envelopes the original output message in a new message with the **From** and **To** email addresses set in the corresponding fields.
2. The **Use a preset FROM and TO in the outer envelope headers** option adds the **From** and **To** email addresses 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.



The service account that runs the service should have read/write permission for the specified folder.

Webhook Client Configuration

1. Enable **Send Webhook Notifications**.



2. Specify **Endpoint URL**.
3. Specify **Batch Size**. The default size is 100.

The default value for Request Method is POST.

Status Update Configuration

1. Enable **Send Status Update**.

2. Specify **Endpoint URL**.

The default value for Request Method is POST.

Azure Blob Target

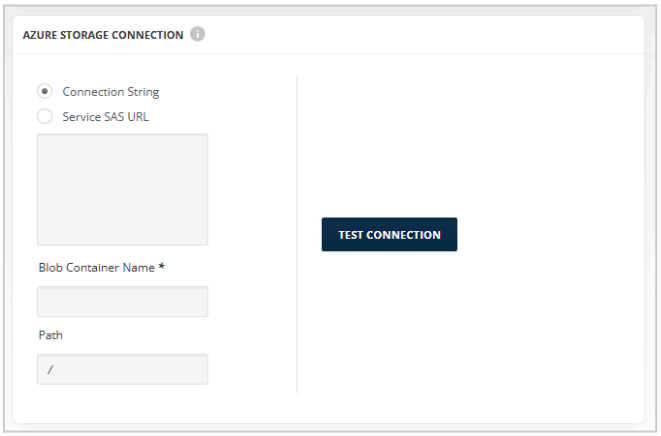
To deliver data collected from different sources to the Azure Blob storage, Azure storage should be configured accordingly. For more information on how to configure Azure Storage, see the Configuring Azure Storage.

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

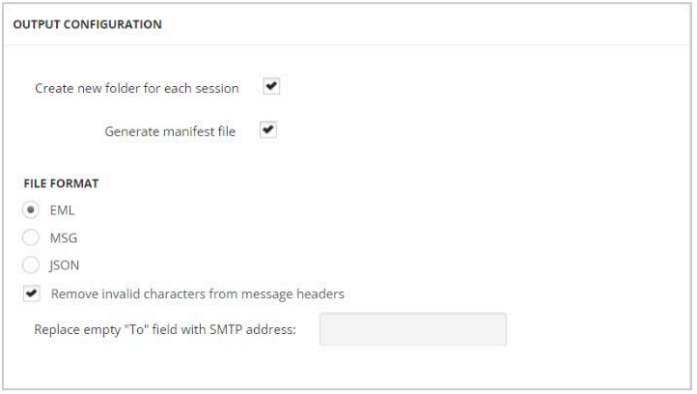
To configure **Azure Storage**:

1. Enable **Connection String** and enter the **Connection String** copied in step 9.[64]
   Or,
2. Enable **Service SAS URL** and enter the Service SAS URL copied in step 9.[64]
3. Enter **Blob Container Name** from step **10**.
4. If needed, specify the **Path** field to deliver data to the designated folder within the bucket.



Output Configuration

1. **Create new folder for each session**. If checked will create a separate folder for each time the importer is run, named after the date and time of the run.
2. **Generate manifest file**. If checked, a CSV file containing the list of generated message files will be generated.



3. **EML, MSG, JSON**. If one of the options is enabled, the exported message will be in the respective format. See the difference between the file types in the table below.

EML	MSG	JSON
An extension supported by multiple email clients like Outlook Express, Thunderbird, and Windows Live Mail.	An extension supported by Microsoft Outlook.	A lightweight data-interchange format.

[64] Only the Storage Account-level connection string and service SAS URL are supported.

Files can be read by its email client along with others like Outlook can read EML files.	Files can only be saved for emails and messages.	Easy to read and write.
Files can be opened in a text editor similar to text files.	Files can only be opened by MAPI-based applications.	Easy for machines to parse and generate.

You can easily convert your MSG file to 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.

4. **Remove invalid characters from message headers**. The 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.

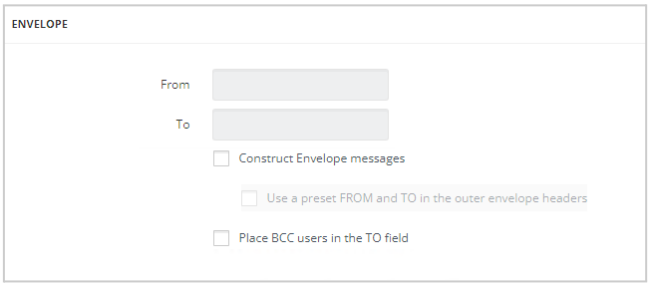
Note that JSON file format is available in all the collectors' folder targets but currently is supported only for the below-listed collectors. For other collectors, an error will be thrown.

- Amazon S3
- Audio Video
- Box
- ChatGPT
- Chatter / Chatter Cipher Cloud
- Cloud9
- Copilot
- DB (newly created ones, not upgraded)
- Dropbox Business
- Dubber Speik Recordings
- Dubber Speik SMS
- FX Connect
- FX Connect (File-Based)
- Google Messages
- iMessage
- Jabber Enterprise
- JSON
- Microsoft Teams for Audio and Video
- Microsoft Teams via Export API
- NTR-X
- OneDrive for Business
- Pivot
- Redtail Speak
- LSEG (Refinitiv)
- RingCentral
- ServiceNow
- SharePoint
- Slack eDiscovery
- Skype for Business

- Symphony
- Text-Delimited (newly created ones, not upgraded)
- X (Twitter)
- Verba
- Verint
- 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

Envelope

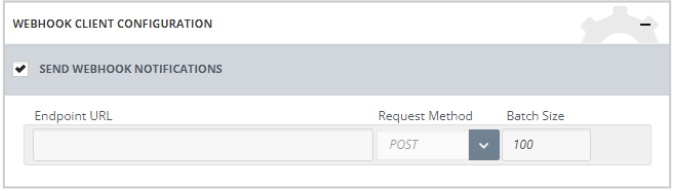
1. The **Construct Envelope messages** option when enabled envelopes the original output message in a new message with the **From** and **To** email addresses set in the corresponding fields.
2. The **Use a preset FROM and TO in the outer envelope headers** option adds the **From** and **To** email addresses 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.



The service account that runs the service should have read/write permission for the specified folder.

Webhooks Client Configuration

1. Enable **Send Webhook Notifications**.



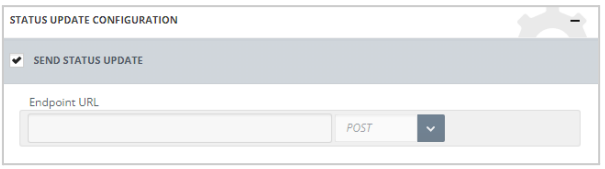
2. Specify **Endpoint URL**.

3. Specify **Batch Size**. The default size is 100.

The default value for Request Method is POST.

Status Update Configuration

1. Enable **Send Status Update**.



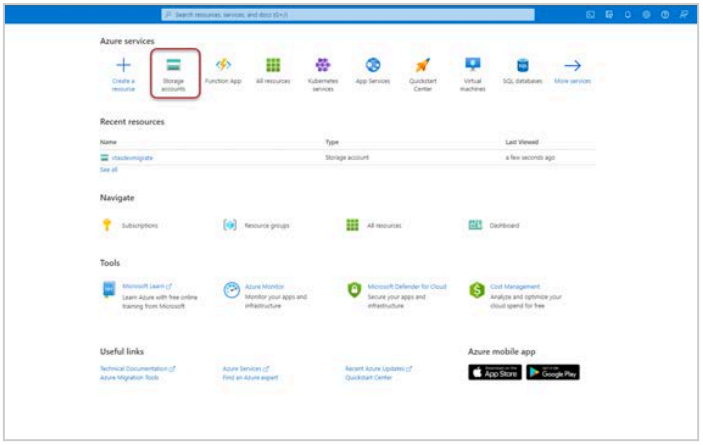
2. Specify **Endpoint URL**.

The default value for **Request Method** is **POST**.

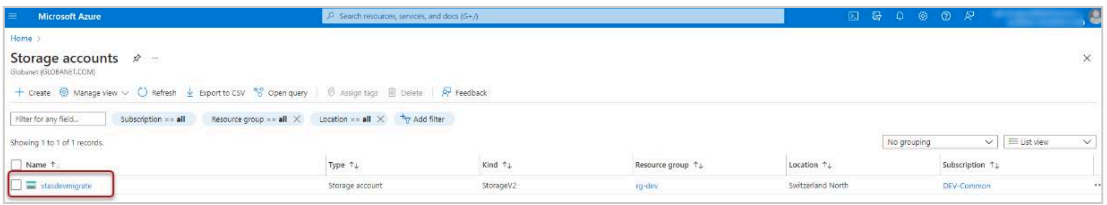
Configuring Azure Storage

For Azure Blob storage:

1. Login to your Azure portal account.
2. Navigate to **Storage Accounts**.[65]



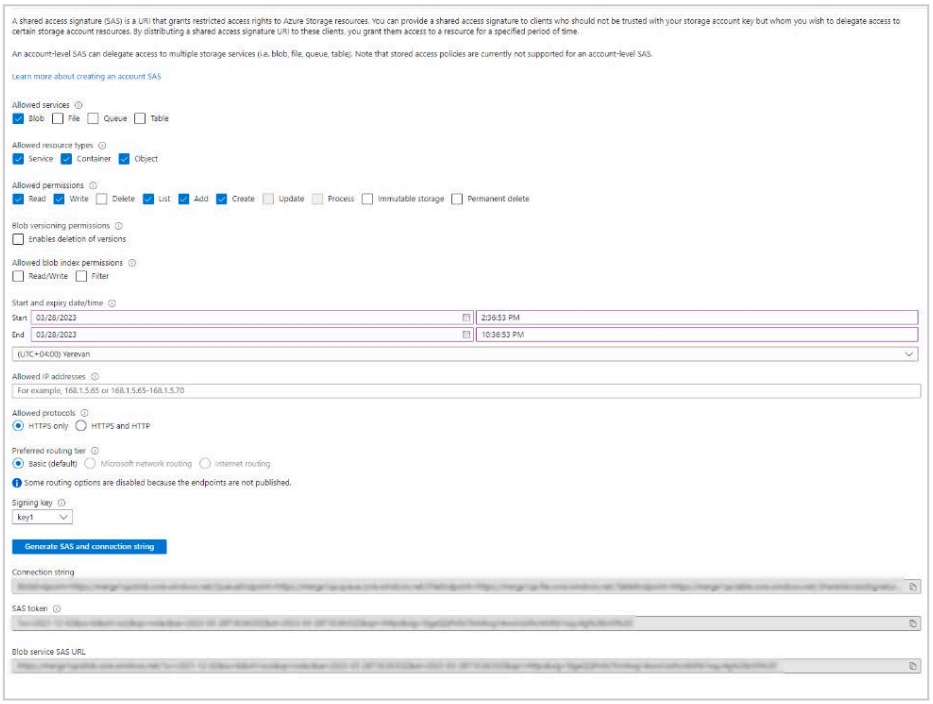
3. Click the account **Name**.



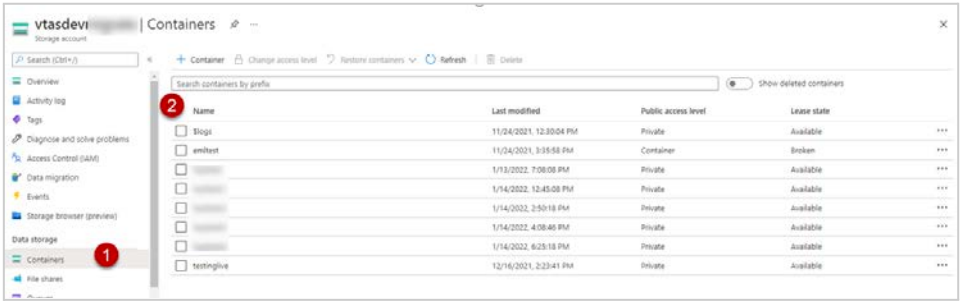
4. On the left side navigation pane, navigate to **Shared Access Signature**.
5. For Allowed services, enable Blob.
6. For Allowed resource types, enable Service, Container, and Object.

[65] Only the Storage Account-level connection string and service SAS URL are supported.

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** (1) and click the name of the container you want (2).

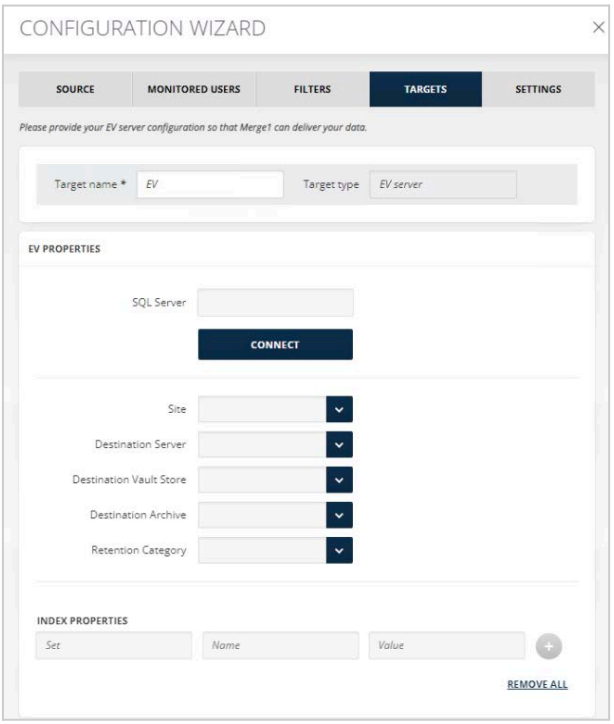


EV Server Target

The **EV Server** target requires the Enterprise Vault API Runtime (12 or above) installed on the machine hosting Merge1 Agent.

1. To set up an EV target, enter the instance name or IP address of the server that hosts your EV Directory **SQL Server** and click **Connect** to populate the other form fields.

2. After successfully connecting to the database, provide the relevant information from the drop-down fields and click **Next**:
    - Site
    - Destination Server
    - Vault Store
    - Archive
    - Retention Category
3. Fill in the fields of the **Index Properties** section:
    - Set
    - Name
    - Value



Index Properties are used to assign search parameters to data stored in the archive. These parameters will appear in the **Other Attribute Name** and corresponding Value fields in Enterprise Vault Shopping Service.

For **Advanced Configuration Options**:

1. Select the message format by activating the **MSG** or **EML** radio buttons from **Message format option**.
2. Fill in the replace empty "To" field with SMTP address and validate the SMTP address by enabling the corresponding checkbox.

Note

Merge1 officially supports Domino Journal, Journal Archive and SMTP archives, however, most other archive types are usually compatible as well.

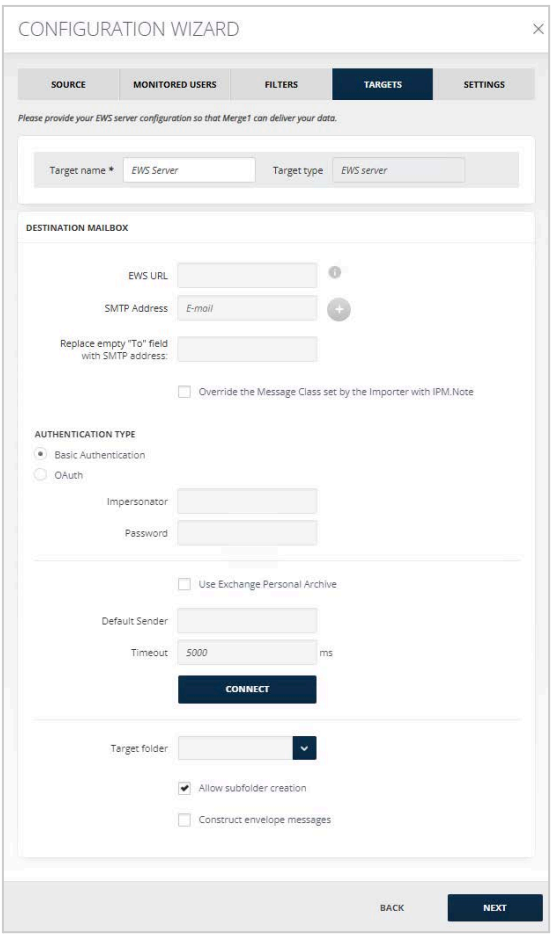
Note that by default, the value for Vault.MsgType is set to EXCH by Merge1. To change this, add a new index property with **Vault** in the **Set** field, **MsgType** in the **Name** field, and the value of your choice in the **Value** field.

To include the x-KVSMessageType header, find and enable the option on the SETTING page.

EWS Server Target

Merge1 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 that in case of connecting to the Microsoft Exchange Server Online, only Microsoft OAuth is supported.

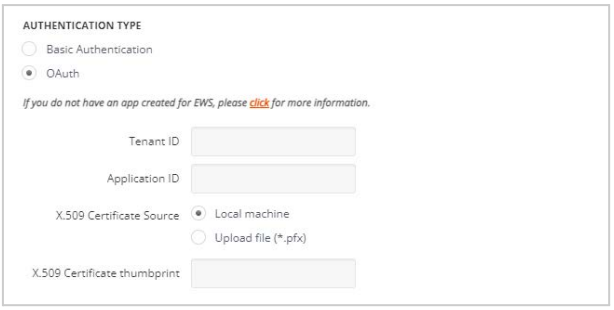


To set up the target:

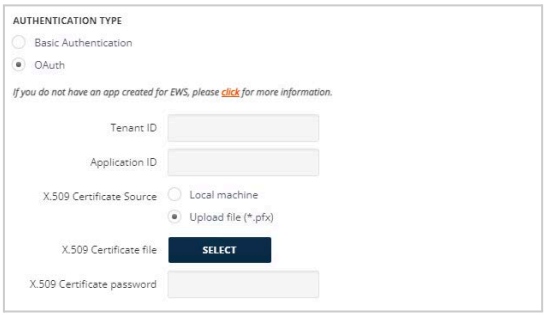
1. Enter **EWS URL**.
2. Enter the **SMTP address** in the relevant field.

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. If you activate **Basic Authentication**, provide the **Impersonator** information and **Password** of the target Exchange Web Services account.
   Or,
7. If you 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 **Creating a Microsoft Entra ID Application** and **Uploading a Certificate** accordingly.



8. In case you activate **Upload file (*.pfx)**, click the **Select** button to upload the certificate and then provide **X.509 Certificate Password**.



The **Certificate thumbprint** field will be auto populated in case the collector was previously configured by uploading a certificate.

9. Enable **Use Exchange Personal Archive** checkbox to import data to the Personal Archive folder of the Target folder.
10. Specify a **Default Sender** for emails with empty FROM fields (EWS rejects such emails).
11. Specify **Timeout** in milliseconds.
12. Click **Connect** to get the folder list.

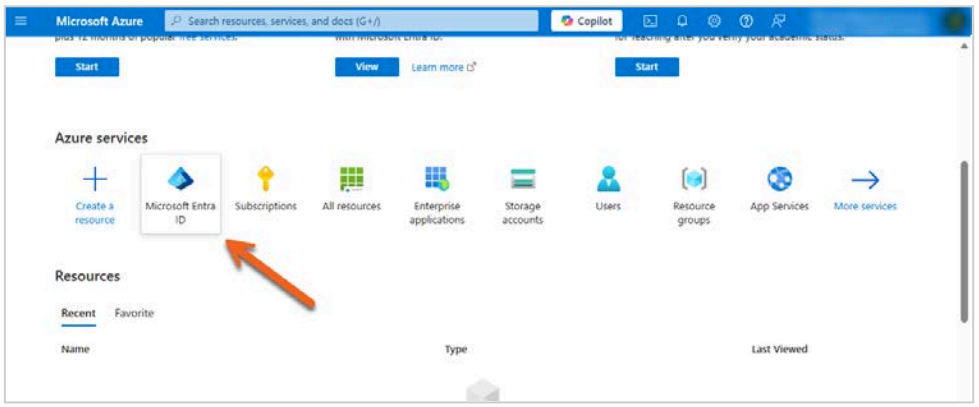
13. Specify a **Target folder** for imported data.
14. Enable **Allow subfolder creation** to create subfolders within the specified root folder.
15. Enable **Construct Envelope Message** to import data in MS Exchange journal report format (the **`X-MS-journal-report`** header is also added).
16. Click **Next**.

Creating a Microsoft Entra ID Application

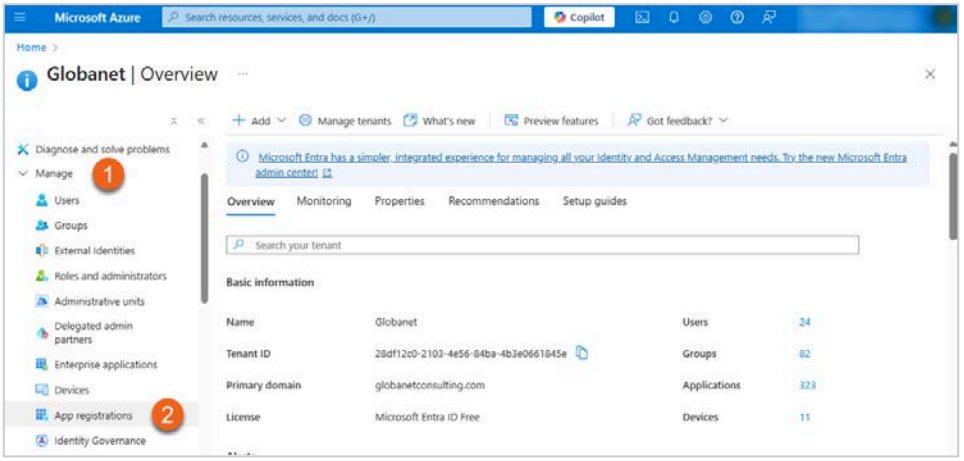
The Office 365 or Azure administrator in your organization must complete the steps detailed in the sections below.

Registering an Application

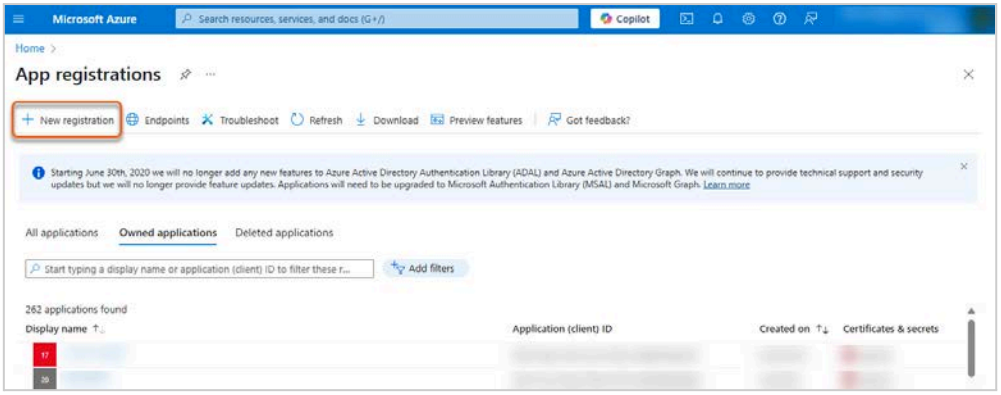
1. Sign in to Azure Portal.
2. Select **Microsoft Entra ID** under **Azure services**.



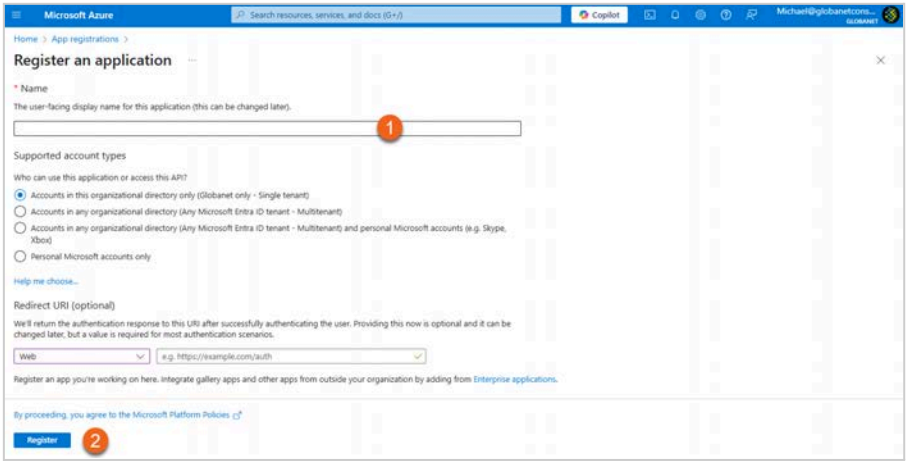
3. In the left-hand navigation pane, click **Manage > App registrations**.



4. Click **New registration**.



5. To register an application:
   5.1. Enter a **Name** for the application.
   5.2. Click **Register**.

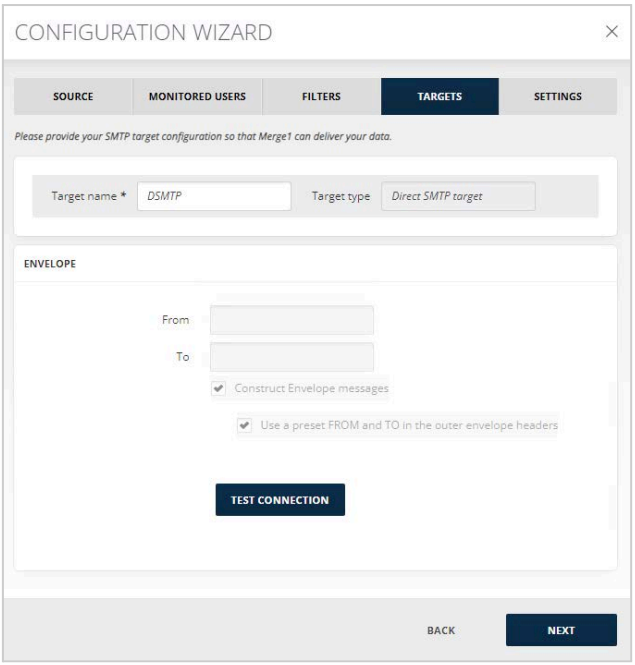


6. An **Application (client) ID** and **Directory (tenant) ID** will be generated. Keep both for configuring the target in Mergel.

Direct SMTP Target

The **Direct SMTP** target allows Mergel to deliver the processed messages directly to the recipients' SMTP server without requiring relaying through a secondary SMTP server like in the SMTP target.

Below you can find information on how to setup the **Direct SMTP** target for your collector.

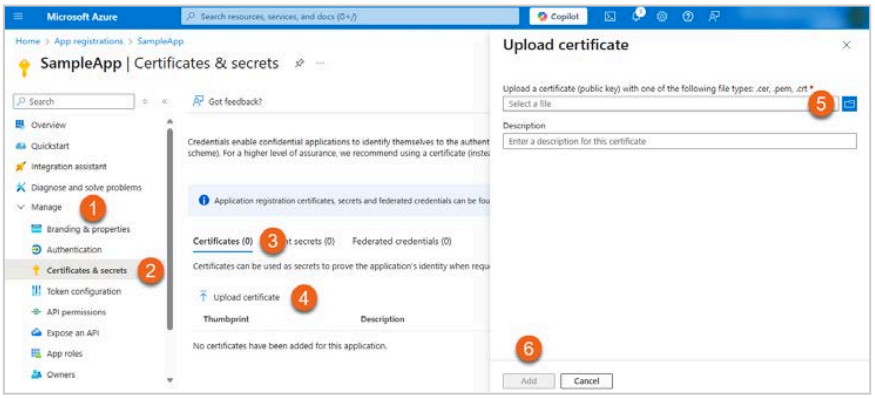


1. Specify the sender SMTP address that you want to use in the **From** field. We recommend using an existing email address so the emails will not be spammed.
2. Specify a destination email address in the **To** field.
3. When you have filled in all the fields, click **Next**.
4. When the **Place BCC users in the TO** field is selected, the BCC emails of the message will be added to the TO field.

Uploading a Certificate

To upload a certificate:

1. In the left-hand navigation pane, go to **Manage > Certificates & secrets**.
2. Select **Certificates**.
3. Click **Upload certificate**.
4. Select a certificate (public key) with one of the following file types: `.cer`, `.pem`, `.crt`.
5. Click **Add**.



A certificate **thumbprint** will be generated. Keep the value for configuring the collector in Merge1.

For more information on how to create a certificate, see **Creating a Certificate (Private and Public Keys)**.

Folder Target

If you choose the **Folder** target, Merge1 delivers the data to the specified folder in EML, MSG or JSON formats. Below you can find information on how to setup the **Folder** target for your collector.

Output Folder

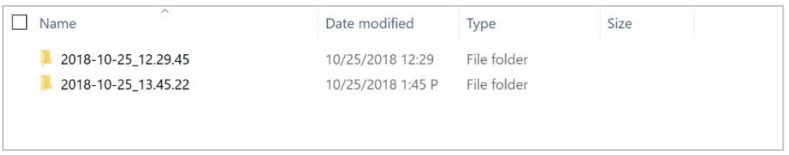
1. Select the output folder, to where the exported messages will be sent.
2. Specify the format of the exported message, **EML**, **MSG** or **JSON**. See the difference between the file types in the table below.

EML	MSG	JSON
An extension supported by multiple email clients like Outlook Express, Thunderbird, and Windows Live Mail.	An extension supported by Microsoft Outlook.	A lightweight data-interchange format.
Files can be read by its email client along with others like Outlook can read EML files.	Files can only be saved for emails and messages.	Easy to read and write.
Files can be opened in a text editor similar to text files.	Files can only be opened by MAPI-based applications.	Easy for machines to parse and generate.

   You can easily convert your MSG file to 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.

3. If the **Generate manifest file** box is enabled, a CSV file is generated that will contain the list of generated message files.

4. **Create New Folder Per Session** if enabled will create a separate folder for each time the Importer is run, named after the date and time of the run.



5. The Remove invalid characters from message headers checkbox is activated by default.
6. Enter the **SMTP address** in case you want to **Replace the empty "To" with an SMTP address** in the corresponding field.

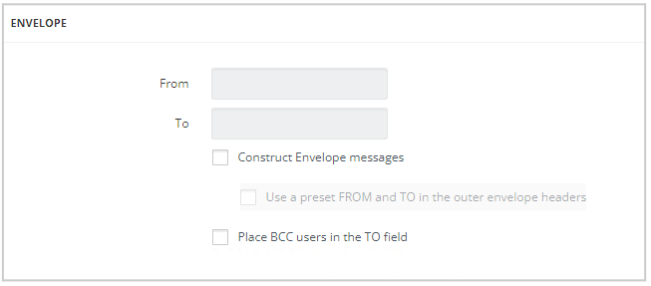
Note that JSON file format is available in all the collectors' folder targets but currently is supported only for the below-listed collectors. For other collectors, an error will be thrown.

- Amazon S3
- Audio Video
- Box
- ChatGPT
- Chatter / Chatter Cipher Cloud
- Cloud9
- Copilot
- DB (newly created ones, not upgraded)
- Dropbox Business
- Dubber Speik Recordings
- Dubber Speik SMS
- FX Connect
- FX Connect (File-Based)
- Google Messages
- iMessage
- Jabber Enterprise
- JSON
- Microsoft Teams for Audio and Video
- Microsoft Teams via Export API
- NTR-X
- OneDrive for Business
- Pivot
- Redtail Speak
- LSEG (Refinitiv)
- RingCentral
- ServiceNow
- SharePoint
- Slack eDiscovery
- Skype for Business
- Symphony
- Text-Delimited (newly created ones, not upgraded)
- X (Twitter)
- Verba
- Verint

- 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

Envelope

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.



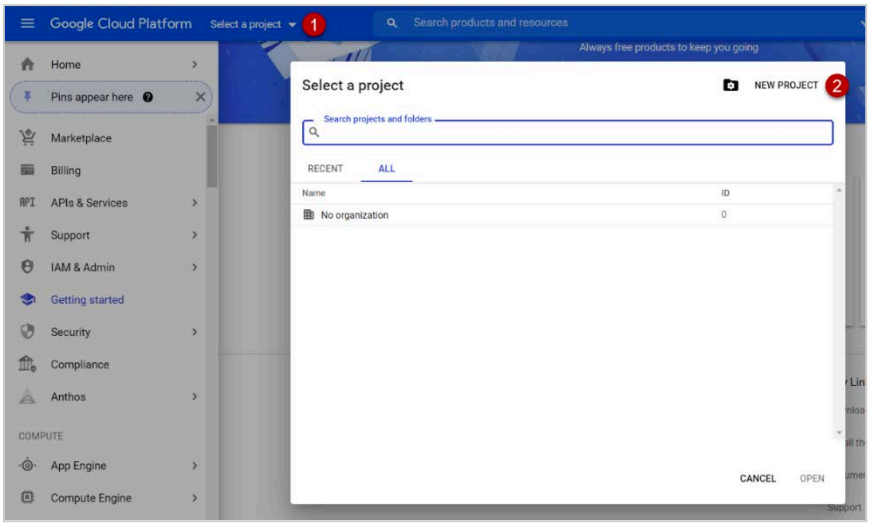
The service account that runs the service should have read/write permission for the specified folder.

Google Vault Target

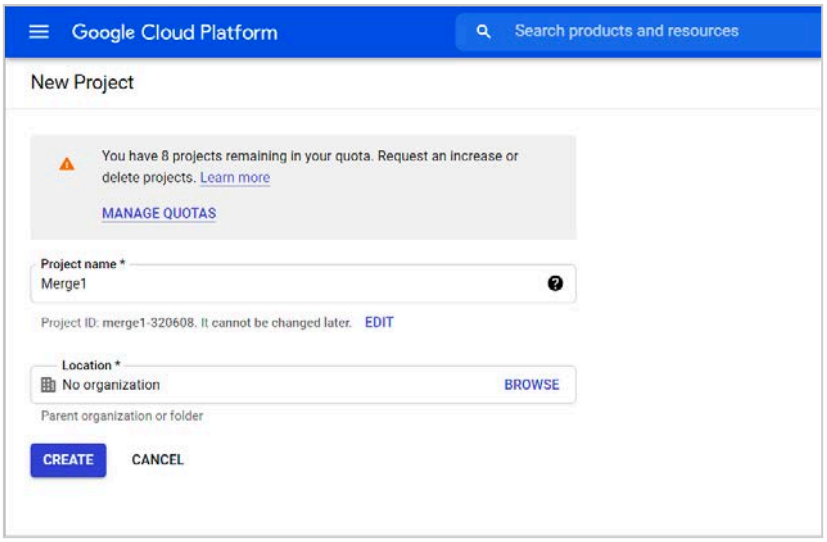
Before configuring the **Google Vault** target in the Merge1 GUI, the following configurations should be done in Google Admin Console.

Google Vault Configuration

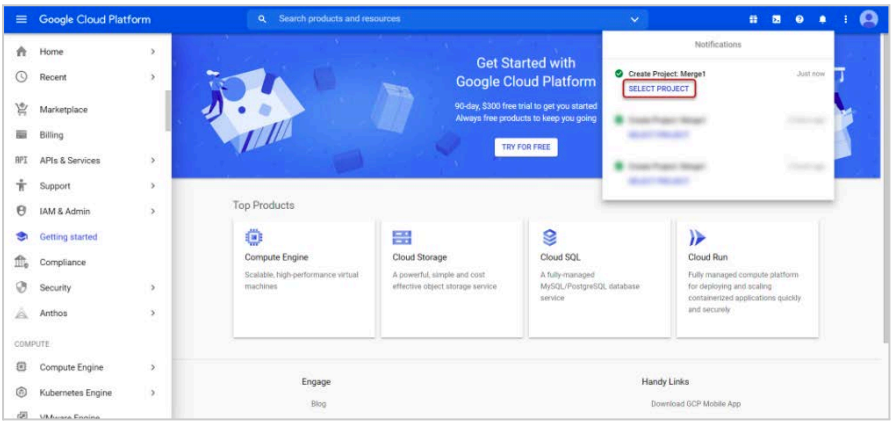
1. Login to https://console.cloud.google.com/ using an Administrator account, click **Select a project**, then **NEW PROJECT**.



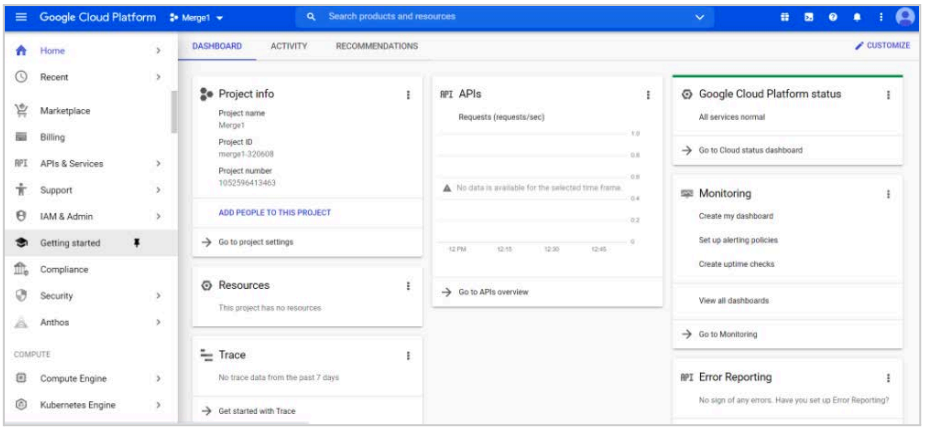
2. Enter a name for the project (example: Merge1) and click **CREATE**.



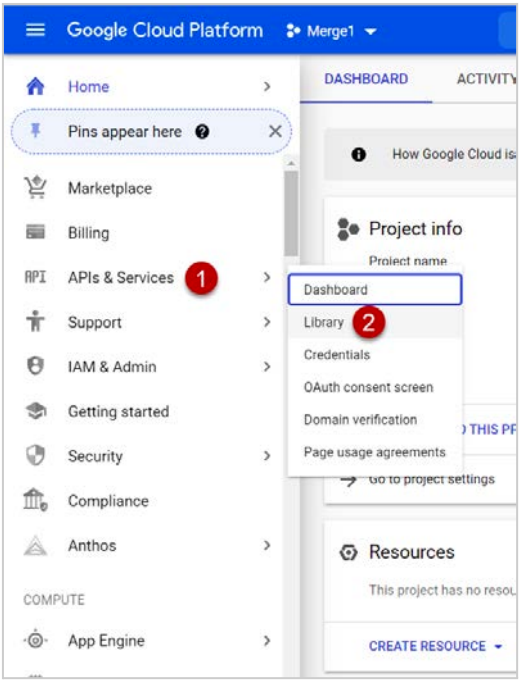
3. Once the project is created, and there are multiple projects, click **SELECT PROJECT** from the **Notifications**. You will be navigated to the created project dashboard.



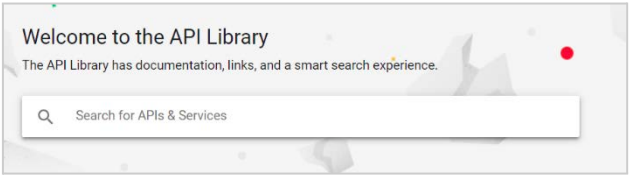
Note that if this is the first project created, you will automatically be navigated to the project dashboard.



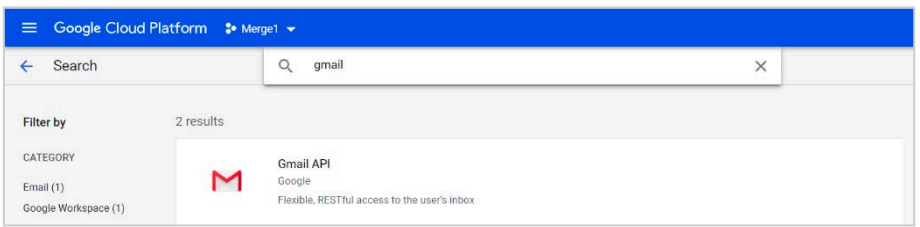
4. Hover **APIs & Services**, then select **Library**.



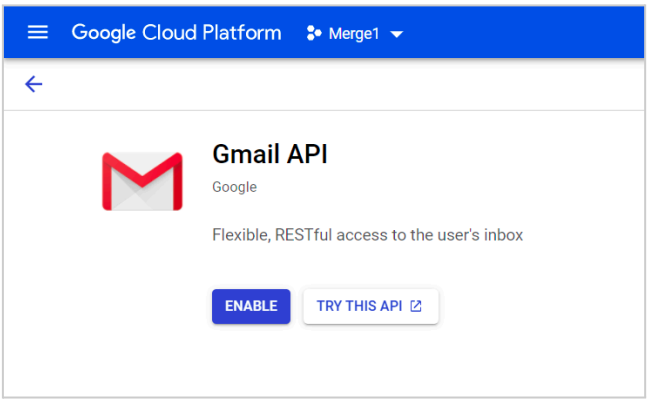
5. In the **Search for APIs & Services** search box, type `Gmail`.



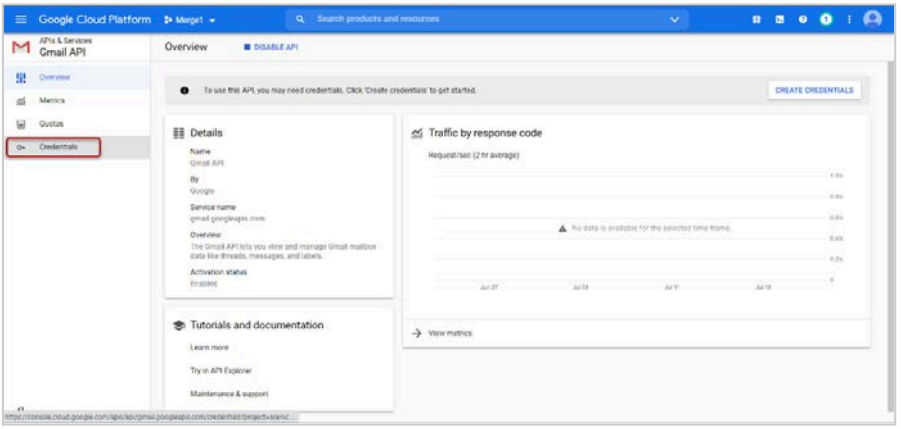
6. Click **Gmail API**.



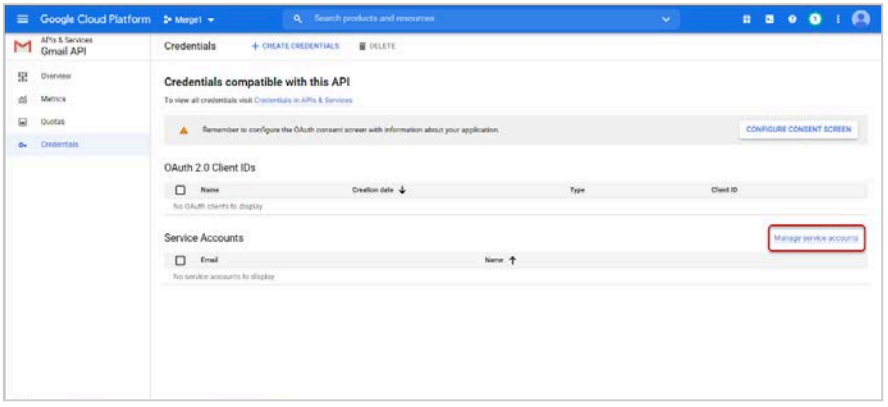
7. Once you are in the **Gmail API** page, click **ENABLE**.



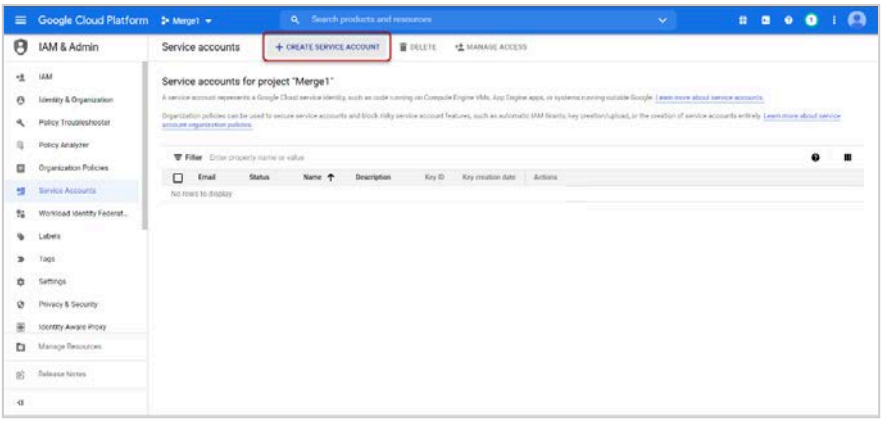
8. Click **Credentials**.



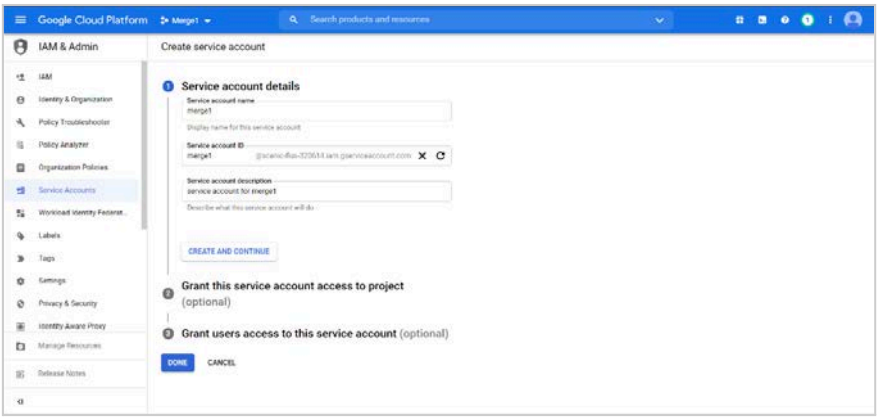
9. Click **Manage service accounts**.



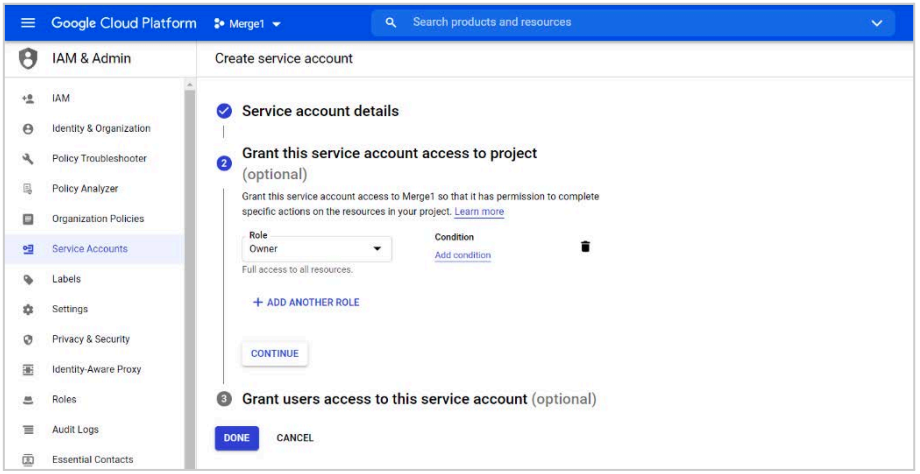
10. Click **CREATE SERVICE ACCOUNT**.



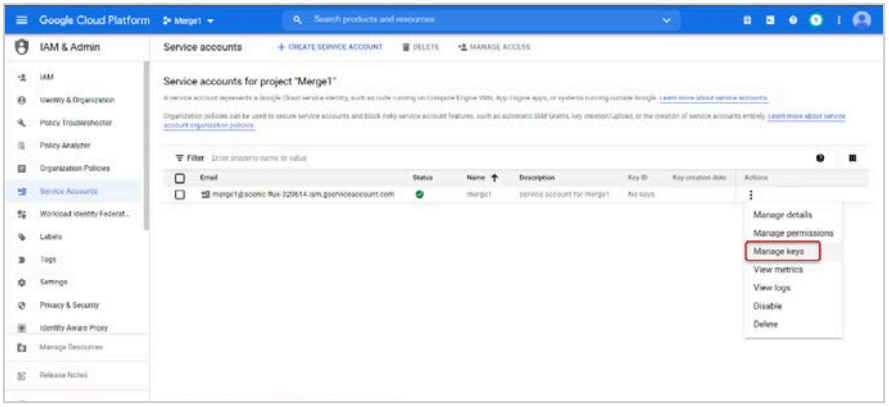
11. Enter a name and a description for the service account and click **CREATE AND CONTINUE**.



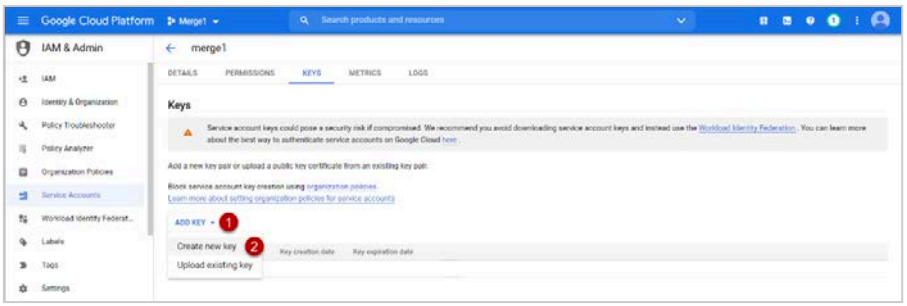
12. Select **Owner** as a role and click **CONTINUE**, then click **DONE**.



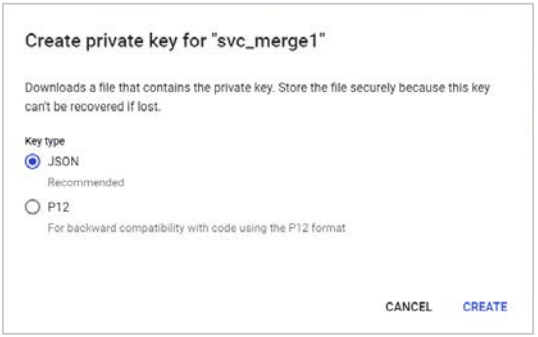
13. You will be redirected to the service accounts for the project page. Click the **Actions** button and select **Manage keys**.



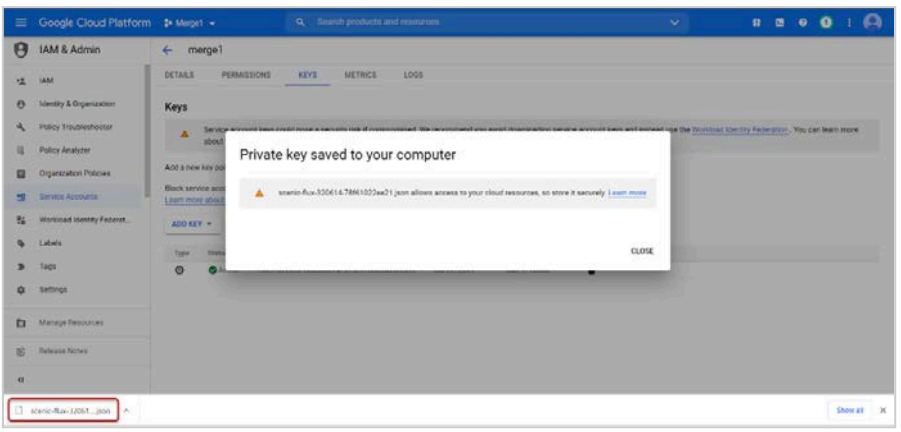
14. Select **ADD KEY > Create new key**.



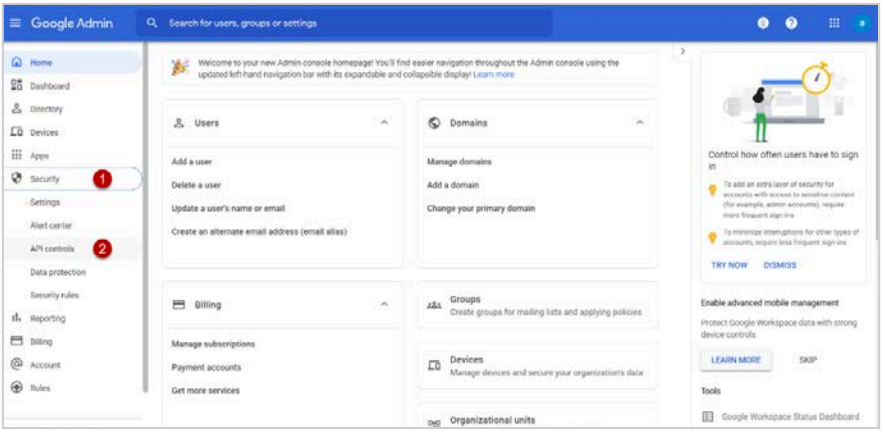
15. Select **JSON** as a key type and click **CREATE**.



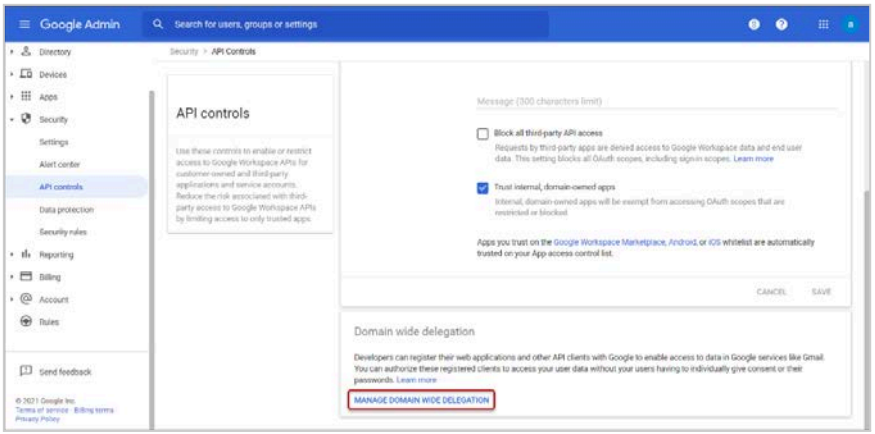
16. Once the key is created, you should get prompted to save the file on your computer, save it somewhere secure, you will need it when configuring Merge1.



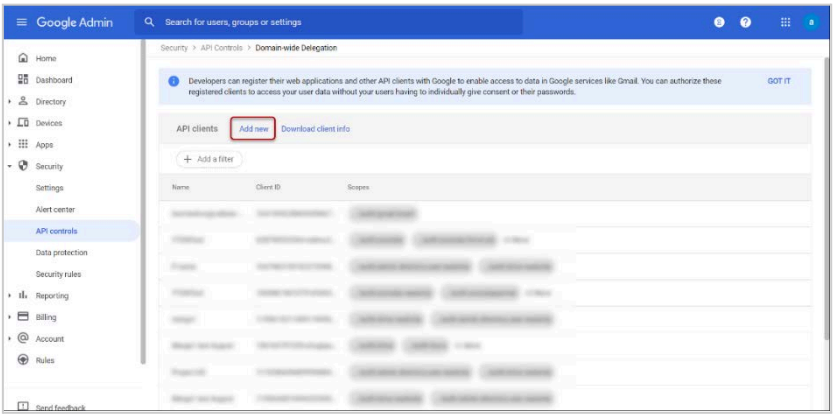
17. To grant permissions to the application, go to https://admin.google.com then **Security > API controls**.



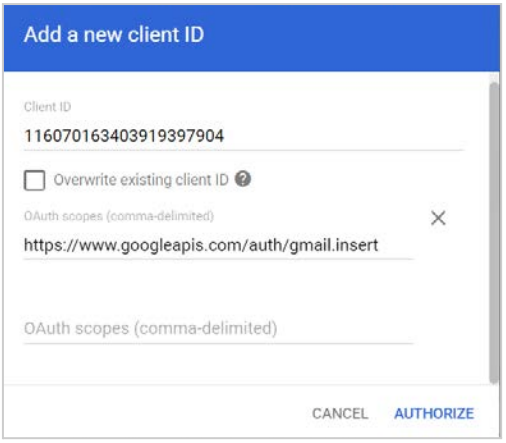
18. Scroll down to Domain wide delegation section and click MANAGE DOMAIN WIDE DELEGATION.



19. Click **Add new**.



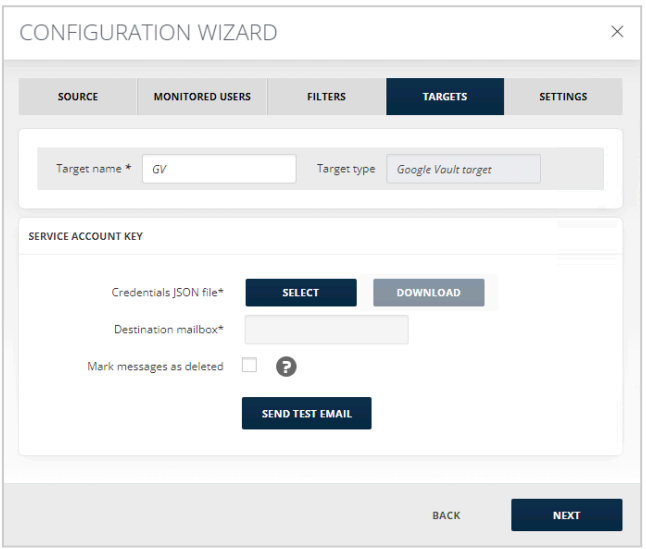
20. Open the key file that you saved as JSON above, copy the value of client_id, then paste it in the **Client ID field**. Enter `https://www.googleapis.com/auth/gmail.insert` in **OAuth scopes** field and click **AUTHORIZE**.



Now you can start configuring Merge1's Google Vault target.

Google Vault Target

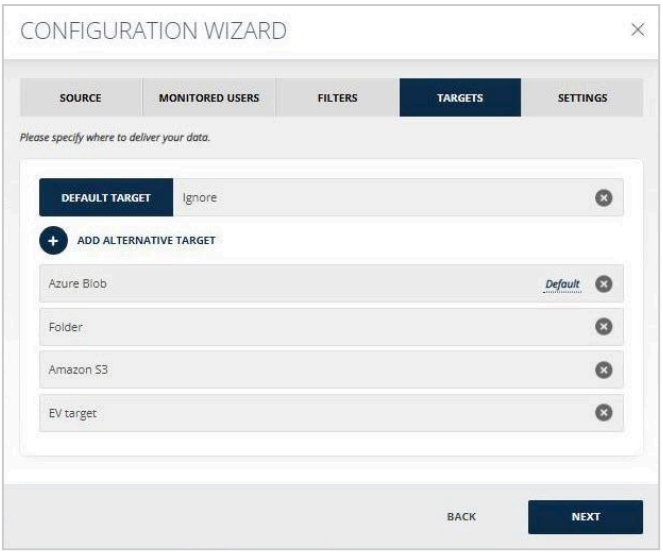
1. Upload JSON file saved in the step 15 of the previous section by clicking **SELECT**.
2. Specify the mailbox, to which the imported messages should be delivered, in the **Destination mailbox** field.
3. When **Mark messages as deleted** option is checked, the imported messages are not visible in the "All Mail" section but are still available for compliance search.
4. Click **SEND TEST EMAIL** to test the connection to the target.



Note that you can download the uploaded JSON file by clicking **Download**. It is active only when there is a JSON file to download.

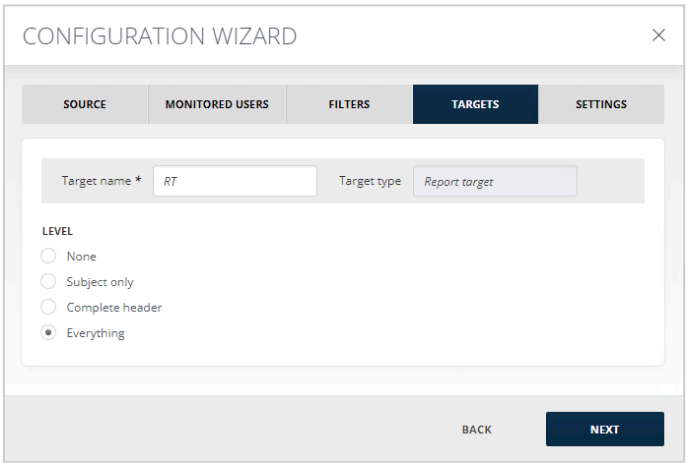
In Merge1, you can have one default target and a number of **Alternative Targets**.

In case you want to make an Alternative target as the **Default** one next to the X 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.



Report Target

The **Report** target is used to check whether data can be analyzed successfully. The Importer will list certain details for viewing in its activity logs. The **Complete header** option includes subject lines with complete headers as well as the messages themselves.



1. Select the relevant level.
2. Click **Next**.

SFTP Target

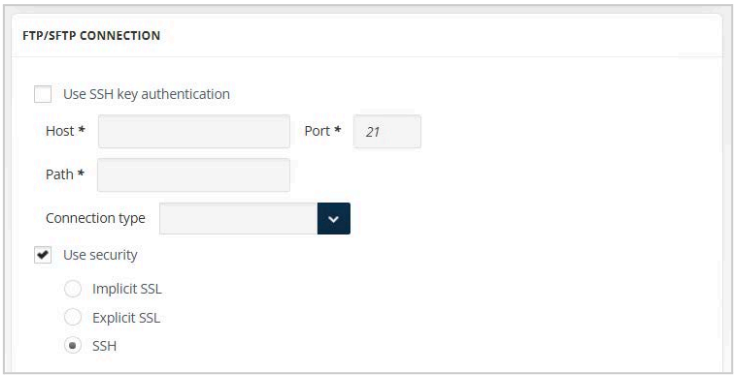
The **SFTP** target allows Mergel to deliver data to an FTP/SFTP server address.

Below you can find information on how to setup the **SFTP** target for your collector.

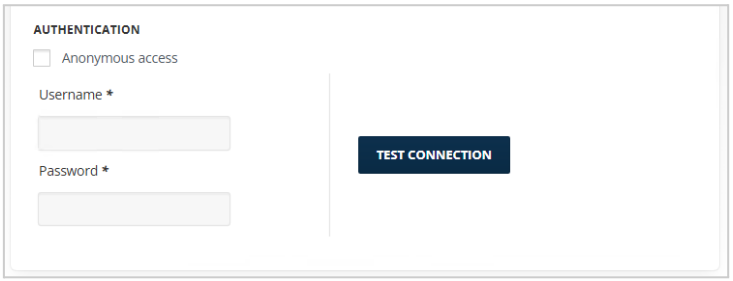
FTP/SFTP Connection

1. Enter the hostname of the remote FTP server and the folder path in the **Host** and **Path** fields, respectively. The default port is 21.

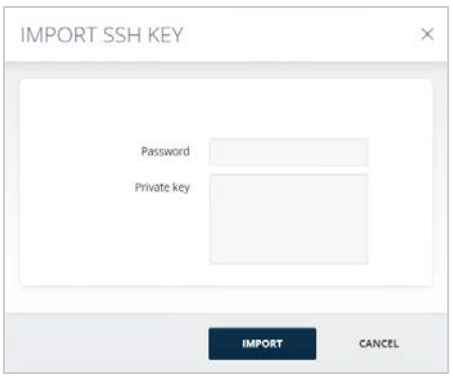
2. Choose an FTP connection type from the **Connection Type** drop-down list. FTP can run in either passive or active mode. The information about the connection type should be provided by the FTP host.
3. If you wish to use FTP over SSL, mark the **Use Security** checkbox and choose the connection method **Implicit SSL**, **Explicit SSL**, or **SSH**.



4. For authentication of an FTP connection, enter the appropriate information in the **Username** and **Password** fields, respectively.
5. To enable anonymous FTP connections, mark the **Anonymous Access** checkbox.
6. Click **Test Connection**. If the connection is successful, a green check sign is displayed.

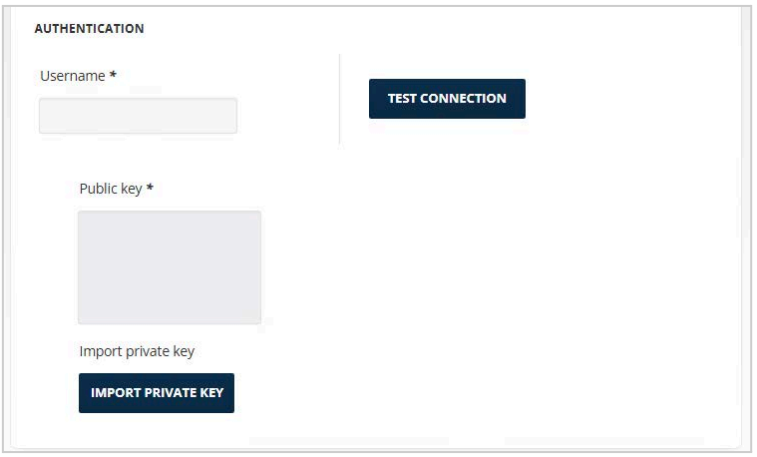


7. To use SSH key authentication method, mark **Use SSH key authentication**. SSH key authentication is used to connect to the source SFTP Server.
8. Enter the FTP server **Username**.
9. Click the **Import Private Key** button and the **Import SSH Key** pop-up window will open.



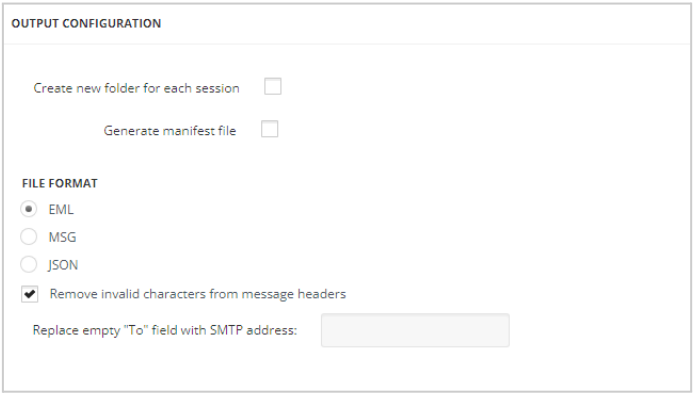
10. Enter the **Password** of the Private key, if it has a password.

11. Copy and paste the **Private Key**.
12. Click **Import** and the **Public Key** field will be populated automatically.



Output Configuration

1. **Create new folder for each session**. If checked will create a separate folder for each time the importer is run, named after the date and time of the run.
2. **Generate manifest file**. If checked, a CSV file containing the list of generated message files will be generated.



3. **EML, MSG, JSON**. If one of the options is enabled, the exported message will be in the respective format. See the difference between the file types in the table below.

EML	MSG	JSON
An extension supported by multiple email clients like Outlook Express, Thunderbird, and Windows Live Mail.	An extension supported by Microsoft Outlook.	A lightweight data-interchange format.
Files can be read by its email client along with others like Outlook can read EML files.	Files can only be saved for emails and messages.	Easy to read and write.
Files can be opened in a text editor similar to text files.	Files can only be opened by MAPI-based applications.	Easy for machines to parse and generate.

You can easily convert your MSG file to 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.

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.

Note that JSON file format is available in all the collectors' folder targets 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
- DB (newly created ones, not upgraded)
- Dropbox Business
- Dubber Speik Recordings
- Dubber Speik SMS
- FX Connect
- FX Connect (File-Based)
- Google Messages
- iMessage
- Jabber Enterprise
- JSON
- Microsoft Teams for Audio and Video
- Microsoft Teams via Export API
- NTR-X
- OneDrive for Business
- Pivot
- Redtail Speak
- LSEG (Refinitiv)
- RingCentral
- ServiceNow
- SharePoint
- Slack eDiscovery
- Skype for Business
- Symphony
- Text-Delimited (newly created ones, not upgraded)
- X (Twitter)
- Verba
- Verint
- 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

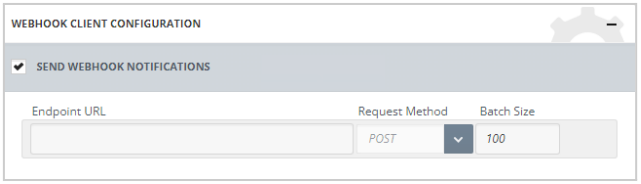
Envelope

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.

The service account that runs the service should have read/write permission for the specified folder.

Webhook Client Configuration

1. Enable **Send Webhook Notifications**.

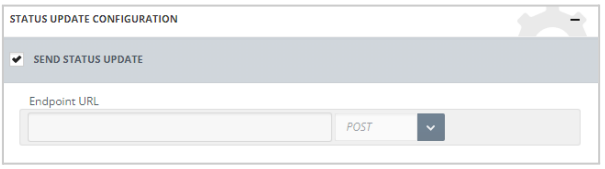


2. Specify **Endpoint URL**.
3. Specify **Batch Size**. The default size is 100.

The default value for **Request Method** is POST.

Status Update Configuration

1. Enable **Send Status Update**.



2. Specify **Endpoint URL**.

The default value for **Request Method** is POST.

SMTP Target

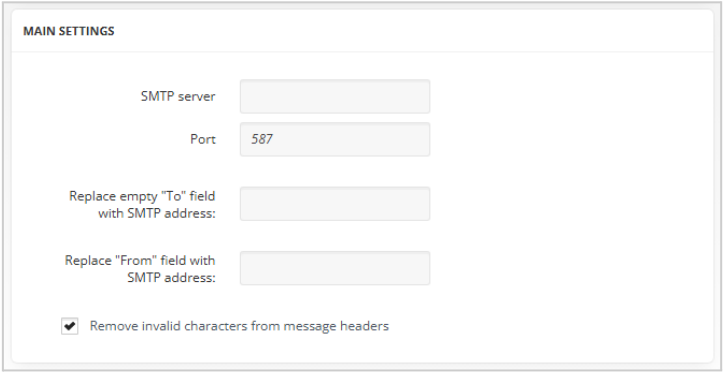
If you choose an **SMTP** target, Mergel will deliver collected data to an SMTP server address you specify. Below you can find information on how to setup the **SMTP** target for your collector.

To configure **Main Settings**:

1. **SMTP Server**: Enter the hostname or IP address of your outgoing mail server.
2. **Port**: Specify the port number used by the SMTP server. The default port is 587.
3. **Replace empty "To" field with SMTP address**: 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.
4. **Replace "From" field with SMTP address**: If needed, enter a valid email address that will be used to replace the "From" address in outgoing emails.

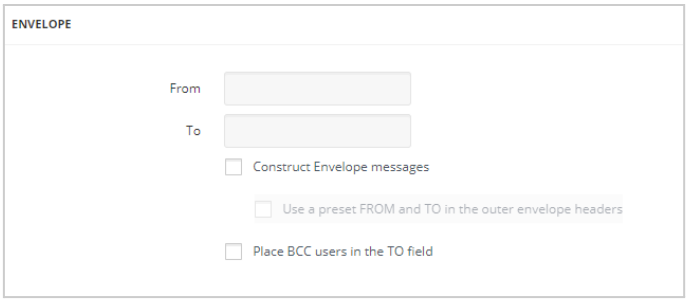
> **Note**
>
> If the "Sender" and "From" headers contain different email addresses, Mergel does not support replacing the "Sender" address with the value specified in the **Replace "From" field with SMTP address** field.

5. **Remove invalid characters from message headers**: When selected, this option automatically detects and strips out unsupported or malformed characters from the email header fields.



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.
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.



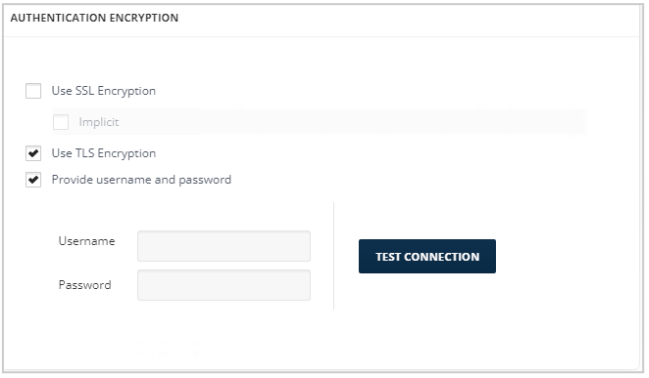
The **SMTP** target is not recommended for delivering messages to **Exchange Online Mailboxes** due to various throttling policies set by **Microsoft**. Also, **Exchange Online** does not accept **Journal Envelope messages** which can result in loss of original message time stamps and other metadata.

Notes

- When enabling the **Construct Envelope Messages** checkbox, Mergel will import data in MS Exchange journal report format (the X-MS-journal header also be added).
- When enabling the **Place BCC users in the TO field** checkbox, Mergel will move all BCC recipients to the TO field.

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 **Provide username and password** to enter username and password.

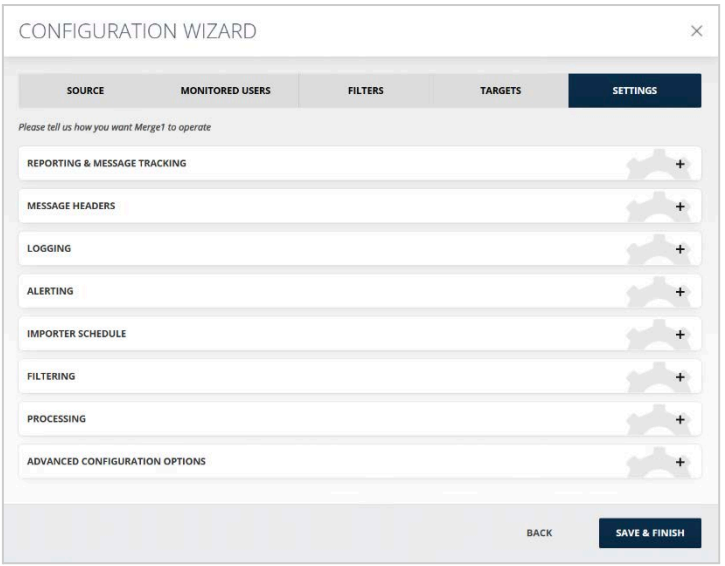


Encryption: SSL and TLS encryption settings should match those of the target SMTP server. Click **Test Connection** to check the connection and to ensure that your settings are accurate.

Importer Settings

The final step for the Importer **Configuration Wizard** is the **Importer Settings**. Under this tab, you will have the opportunity to configure the following:

- Reporting & Message Tracking
- Message Headers
- Logging
- Alerting
- Importer Schedule
- Filtering
- Processing
- Advanced Configuration Options



Reporting & Message Tracking

This section of the **Importer Settings** refers to email reports, which are used to deliver statistical information (also available on the Dashboard) via email.

Enable Message Reconciliation

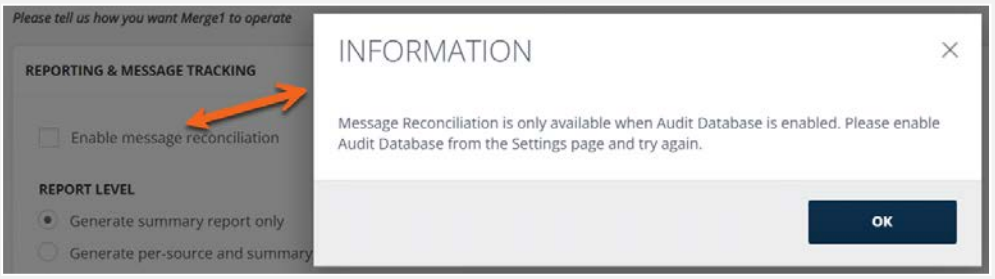
When message reconciliation is enabled, Merge1 adds specific headers to the generated messages. These headers can be found in the message properties:

- **`X-Merge1-Reconciliation-Id`:** This header is provided by collectors and corresponds to the ID of the message in the source. For the EWS collector, it represents the ID retrieved from Exchange Server mailboxes. Currently, only the EWS collector sets this header. If the collector does not provide a **`Reconciliation ID`**, this header will replicate the value of the **`Message-ID`** header, which is uniquely generated by Merge1 for each message.
- **`X-MessageSource`.** Each collector sets its own value for this header. For example, the EWS collector uses the user mailbox and mailbox folder name to populate this header in the following format: **`Mailbox:Foldername`**.

These headers are present in both embedded and enveloped messages. Note that the `Message-ID` differs between the embedded and enveloped versions, while the `Reconciliation ID` remains consistent across both.

Important

The **Enable message reconciliation** option can only be activated when the Audit DB is configured. If the Audit DB is not set up, the following pop-up message will appear:



Report Level

In Merge1, you will find two types of report levels, which set the level of details. You can:

- **Generate summary report only**: The summary report includes **Source Statistics** and **Message Statistics**.
    - *Source Statistics* show the number of unprocessed, quarantined, failed, and imported sources.
    - *Message Statistics* display the number of unprocessed, failed, successful, excluded, and ignored messages.
- **Generate per-source and summary report**: This report type, in addition to the **Summary Report**, includes statistics for each source. For each source, the report provides data on unprocessed, processed, imported, failed, and monitored users (if applicable).

Note

- Detailed reports are longer and may take more time to review. Reports that exceed 5 MB in size are automatically shortened.
- Report formats vary depending on the collector. Each collector generates reports based on the specific activities it is capable of capturing.
- Starting with Merge1 7.0.2510 version, the **Generate per-message, per-source and summary report** configuration option is no longer available.
  If your setup previously relied on this option, it will now default to **Generate per-source and summary report** automatically after the update.

Misc

When the **Delete reported and archived sources and sessions from database** checkbox is selected, all reported and archived sources and sessions will be deleted from the database once the reports are sent.

As a result, the deleted data will no longer appear in Importer Jobs widget within the **Dashboard** section.

Email Report Settings

In this section, you can specify the email address to which reports should be sent. The following fields must be completed:

1. **Message Subject**: Enter the subject line for the report email.
2. **Recipient Email**: Enter the email address where the report will be delivered.

Custom Headers

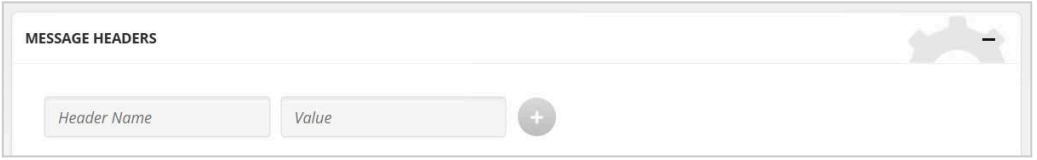
Custom headers are used to label and sort messages.

To add a custom header, fill in the **Header Name** and **Value** fields, then click the **+** button to add it to the list.

Message Headers

Message headers are custom headers that are used to label and sort messages.

To add a message header, fill in the **Header Name** and **Value** fields, then click the **+** button to add it to the list.



Existing custom headers can be overridden if the user specifies another header name. However, the user cannot specify one of the following headers, and any added header must comply with the **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

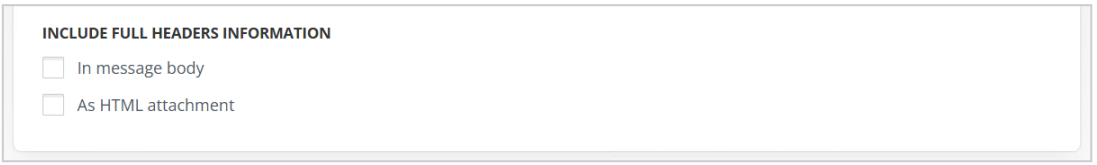
Note

Filters are not applied to headers generated by these settings and do not apply to the EML and Exchange Graph API sources.

Include Full Headers Information

You can choose to include full header information in one of the following ways:

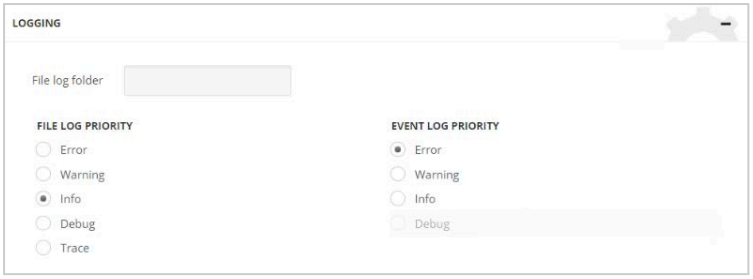
- **In the message body**, with metadata separators between each header.
- **As an HTML attachment**, named Metadata.HTML.



Logging

Enter a file path in the file log folder field. File logs are typically used for troubleshooting purposes. This field is required.

With **File Log Priority**, logs are saved in a separate log file, and with Event Log Priority, event Logs are stored in the Windows Event Viewer. The latter is used to avoid third-party tools in Windows. It also helps customize the logging process and facilitate monitoring based on requirements.



File Log Priority:

- **Error**. Only errors are recorded in the log file.
  Example:

```
ERROR Merge1.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 Merge1.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 Merge1.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:

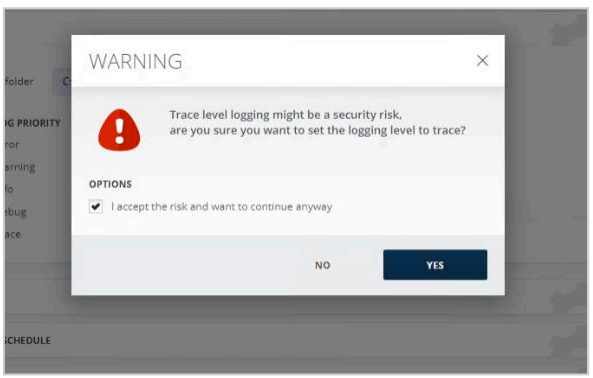
```
DEBUG Merge1.Core.Importer - Creating new session for Importer: 1
```

- **Trace**. The trace level is the lowest logging level, e.g., is the most detailed one.

Example:

```
TRACE Merge1.Core.SenderThread - <31> Preparing message #820 for
sending
```

When choosing logging level **Trace**, a warning message will appear notifying about possible security risks with this level of logging. Some sensitive data can be stored in the log as plain text.



Log File Size Configuration

The log files do not have a size limit, which means they can grow up to couple of GBs. Files that large cannot be opened. Therefore, a log file size limit needs to be set. The log file size cannot be configured through Merge1 GUI. However, it is possible to do by adding appropriate appendix to the log config file in the Merge1 installation folder. It is done the following way:

1. Go to `C:\Program Files\Arctera Inc\Merge1 7.0\Bin` path[66] in the Merge1 installation folder.
2. Open **`Merge1.Logging.config`**. Add the following appendix to the file before the root element at the end:

```
    <appendix name="RollingFile"
type="log4net.Appender.RollingFileAppender">
    <file value="" />
    <datePattern value="'.'yyyy-MM-dd'.log'" />
    <appendToFile value="true" />
    <rollingStyle value="Composite" />
    <maxSizeRollBackups value="-1" />
    <maximumFileSize value="1KB" />
    <staticLogFileName value="false" />
    <countDirection value="0"></countDirection>
    <layout type="log4net.Layout.PatternLayout">
        <conversionPattern value="%date [%thread] %-5level %logger -
%message%newline" />
        </layout>
    </appender>
```

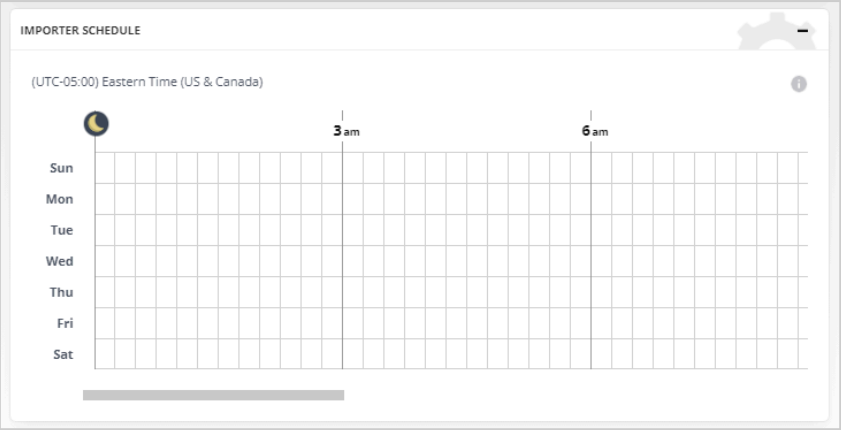
3. Specify the size of the log file in the `<maximumFileSize value="1KB" />` field. For example, 10MB limit should be specified as `<maximumFileSize value="10MB" />`.
4. Save the file.

As Merge1 is multi-threaded, always allow a +30% threshold between the size you set in the config file and the actual file size you will see.

Importer Schedule

Here, the portal server time zone is displayed. This enables you to set a weekly automated option.

[66] In case of Merge1 version 6.0, the path will be `C:\Program Files\Globanet Consulting Services\Merge1 6.0\Bin`.



It is recommended that you schedule an importer once every 24 hours, preferably at night.

Even if the **scheduler** is enabled, but a time is not selected through **Importer Schedule**, the job will not be queued.

Note

The Importer schedules must be re-configured after upgrading Merge1 from 6.0 to 7.0.

Alerting

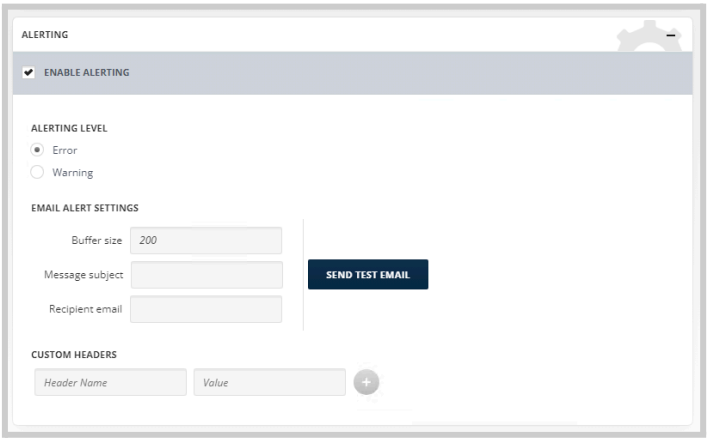
In this section the option to alert on errors the collector encounters during importing.

There are two levels of alerting:

- **Error.** Alert is sent when an Error is registered in the logs.
- **Warning.** Alert is sent when an Error or a Warning is registered in the logs.

To configure the alerting, enter the following information:

- Specify **Buffer size**.
- Enter **Message subject**.
- Provide **Recipient email**.



You can test the connection by clicking **Send Test Email**.

Message Headers

Message headers are custom headers that are used for labeling and sorting messages.

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 an HTML attachment (as Metadata.HTML attachment).

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

Filtering

Filters will not be applied unless filtering is enabled. 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 filter condition.
   - **Process any 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.

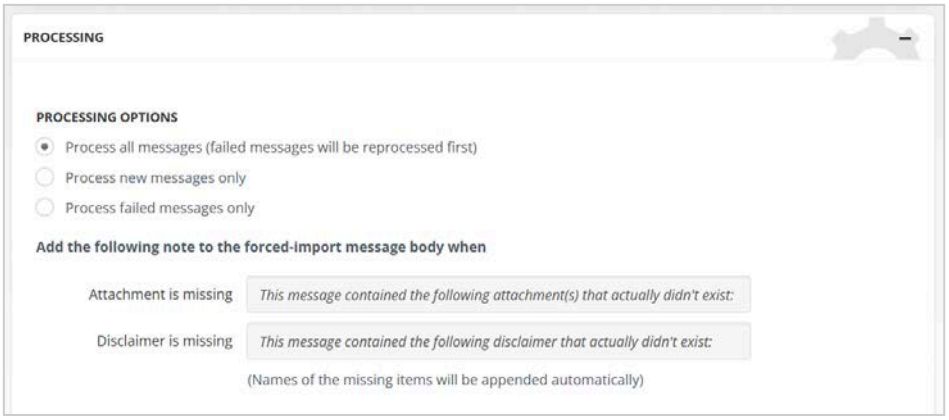
Processing

Processing Options

- **Processing Options -** This option is mostly used for troubleshooting purposes.

It is advised to use **Process Failed Messages Only** when there is a large number of failed messages. If the connection problems 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, referencing the missing disclaimers.



Content Options

- **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, Mergel 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 fields.

Match Email Address

The **Match Email Address** option can match the existing ID or SMTP Address and replace:

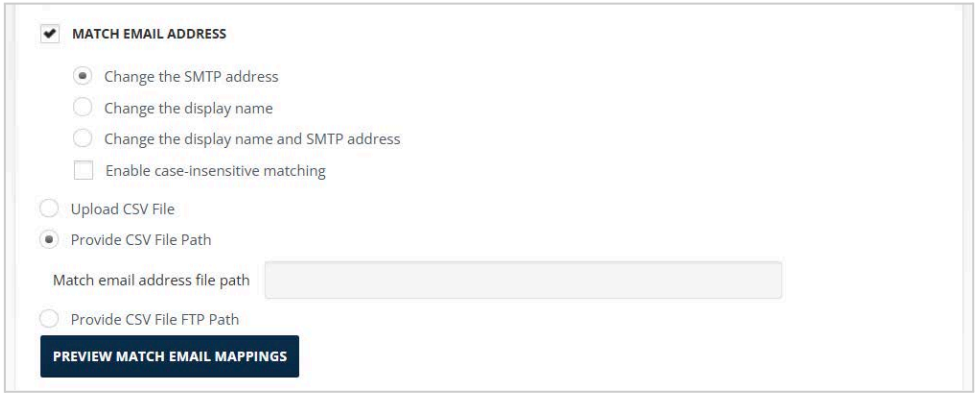
- SMTP Address
- Display Name
- Display Name and SMTP Address

The CSV file should contain the following columns:

- Last Name (A)
- First Name (B)
- Company Name (C)
- Old Email (D)
- New Email (E).

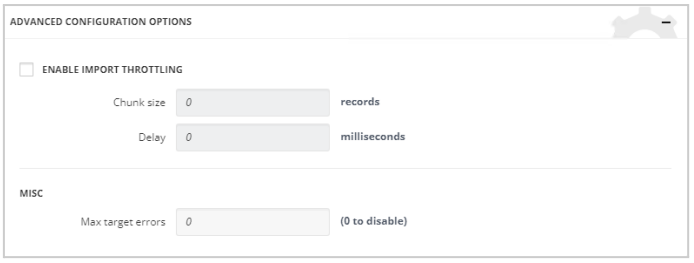
The CSV file can be provided by:

- Uploading the CSV file
- Specifying the file path
- Providing the file FTP path. For FTP configuration refer to **SFTP/FTP Configuration**.



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, click **Save & Finish**.

In case you want to make changes in the Wizard, click **Back** and you will be redirected to the Importer Settings.

CHAPTER 6

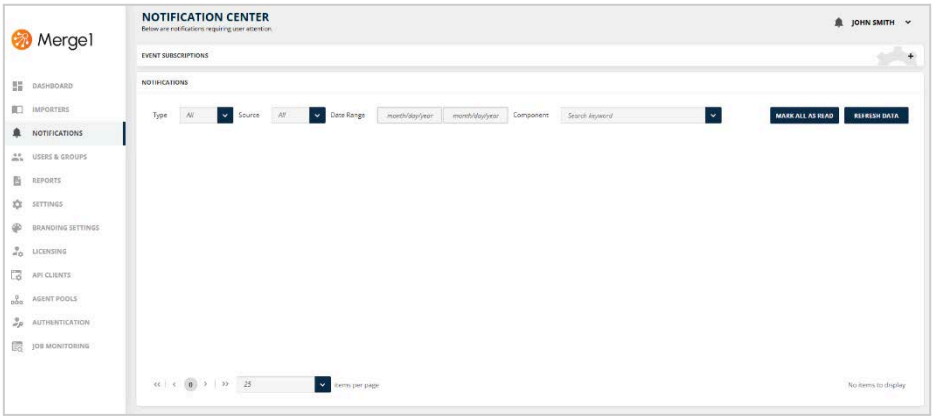
Notifications

This chapter represents:

- Overview
- Event Subscriptions
- Notifications

Overview

The **Notifications** section provides visibility into the Merge1 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**.



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 Merge1 Notification Center.
- **Webhook Push Notification:** Sends the events to a configured webhook endpoint.

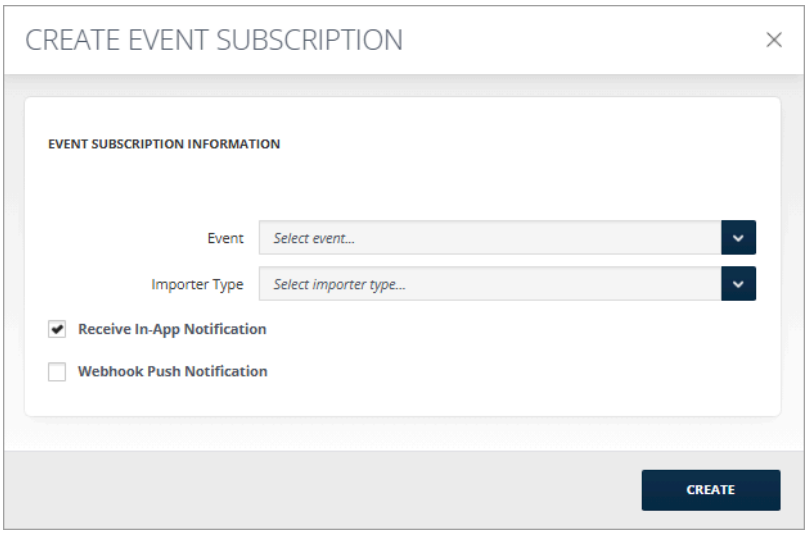
By creating specific subscriptions, users can monitor important event triggers in real time, ranging from successful data processing to critical pipeline interruptions.

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**.



The new subscription becomes active immediately and appears in the subscription list.

> **Info**
>
> Select **All importers** if you want to receive this notification type for every configured pipeline in the system.

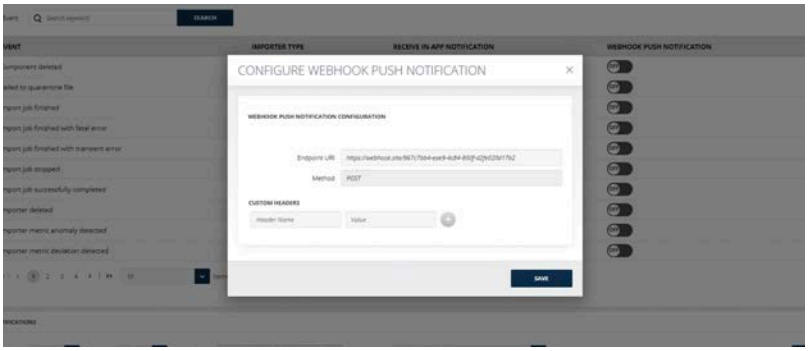
Configuring Webhook Push Notifications

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

Listener Endpoint Requirements

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 Merge1 receives a non-2xx response, it may attempt to redeliver the notification.

Example in Node.js:

```javascript
{
  "CreatedDate": "2025-12-26T07:15:52.000Z",
  "SentDate": "2025-12-26T07:15:51.000Z",
  "Title": "No data captured",
  "Body": "No data has been captured by Importer.",
  "BodyType": 0, //PlainText
  "Severity": 1, //Info
  "Source": "Importer",
  "ImporterId": "52587403-0dfe-4fc6-8344-82fffa267bf1",
  "ImporterName": "Bloomberg",
  "EventCode": 40005 //NoDataCaptured
}
```

Notification Object

The notification object sent to your listener endpoint may have the following structure:

- **CreatedDate**: The date and time when the event was created.
- **SentDate**: The date and time when the notification was sent.
- **Title**: A brief summary of the event.
- **Body**: A detailed description of the event. In this case, it explains why monitored users were skipped.
- **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 component or system that generated the event, which is "Importer" in this example.
- **ImporterId**: A unique identifier (GUID) for the specific importer that generated the event.
- **ImporterName**: The name of the importer, which is "ExportAPI" here.
- **EventCode**: A numerical code that represents the specific type of event. Indicates that 10002 corresponds to the "MonitoredUsersSkipped" event. See all codes in Event Codes.

Event Codes

Value	Name	Description
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

Event Definitions

Once a subscription is active, Merge1 generates notifications based on the specific events defined below. Each event provides detailed metadata to help you monitor pipeline health and administrative changes.

- **Quarantine file:** Triggered when a corrupt or incomplete file set is being quarantined.
- **Failed to quarantine file**: Triggered when a file fails to be quarantined.

- **Monitored users skipped**[67]**:** Triggered when user/users is/are skipped due to thrown *PaymentRequired* or *NotFound* errors.
- **Failed to send webhook notification to target:** Triggered when the Webhook Notifier fails to send the request to the specified endpoint.
- **Import job finished:** Triggered when the importer finishes the run process. The import job duration, starting and ending time are included in the event details.
- **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 anomaly detected:** Triggered when a critical statistical outlier is identified, indicating a severe deviation from normal operational parameters.
- **Importer metric deviation detected:** Triggered as a warning when metrics cross the established boundary for expected behavior.

Managing the Subscriptions

Filtering Events

To quickly find a specific subscription without scrolling:

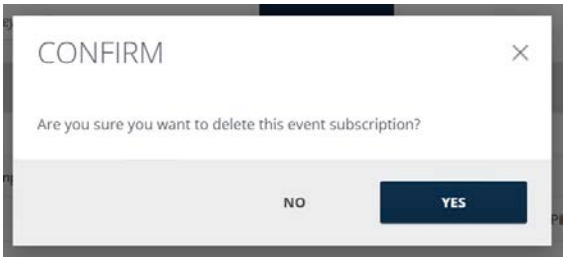
1. Type a keyword related to the Event Type into the search bar.
2. Click **Search**. The list will filter to show only the Event subscriptions that match your keyword.

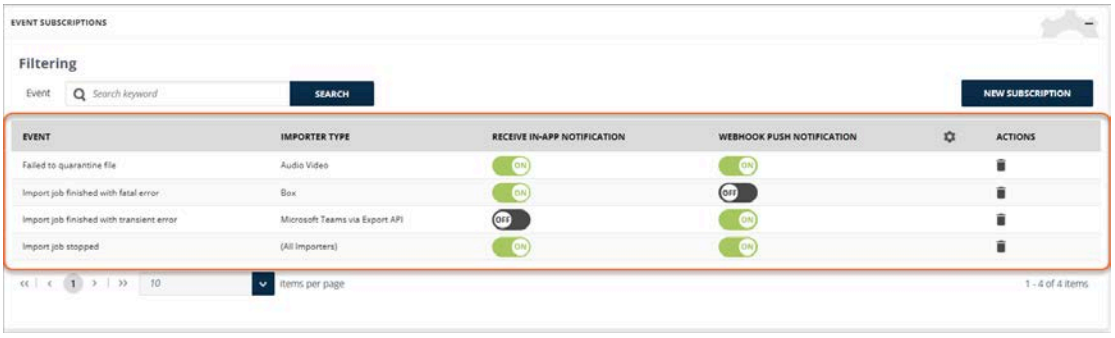
[67] Applicable only to the **Microsoft Teams via Export API** collector.

The Subscription List

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.

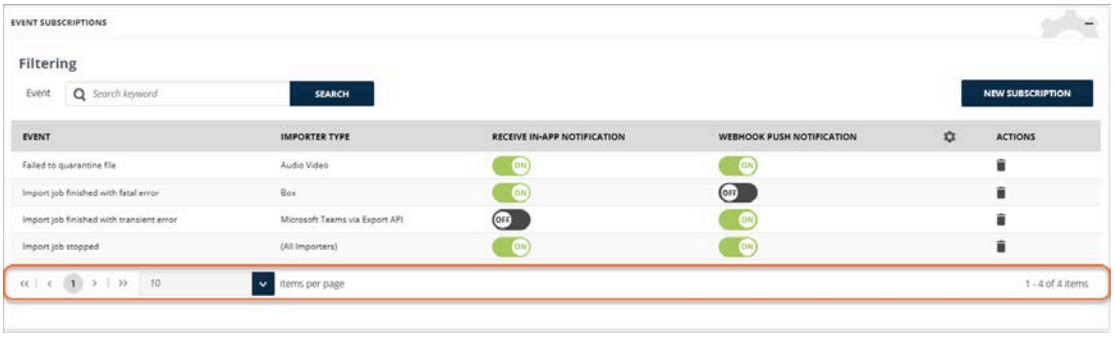




Navigation and Pagination

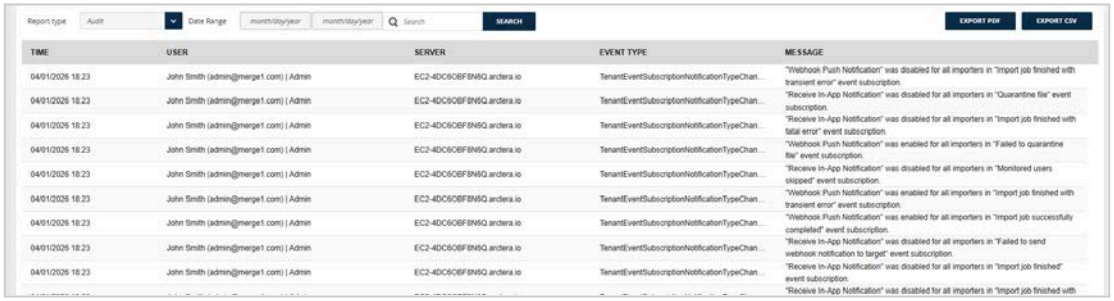
If you have a large number of subscriptions, use the pagination tools located at the bottom of the section:

- **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).



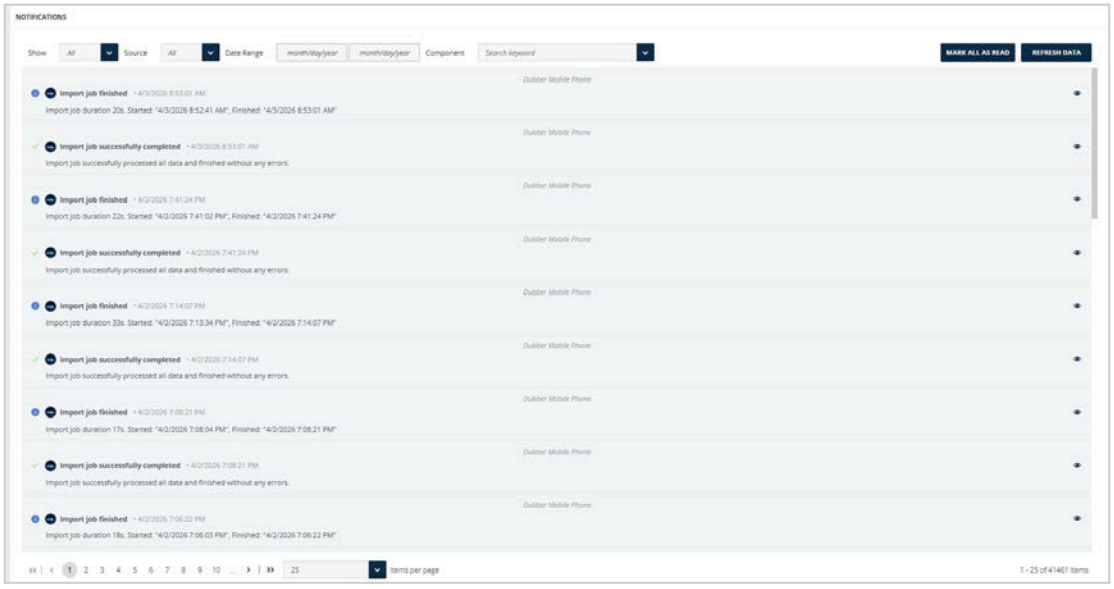
Audit Tracking

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.



Notifications

The **Notifications** sub-section displays a chronological log of all triggered events, ordered from newest to oldest. Use this screen to track recent importer activity and manage your notification history.



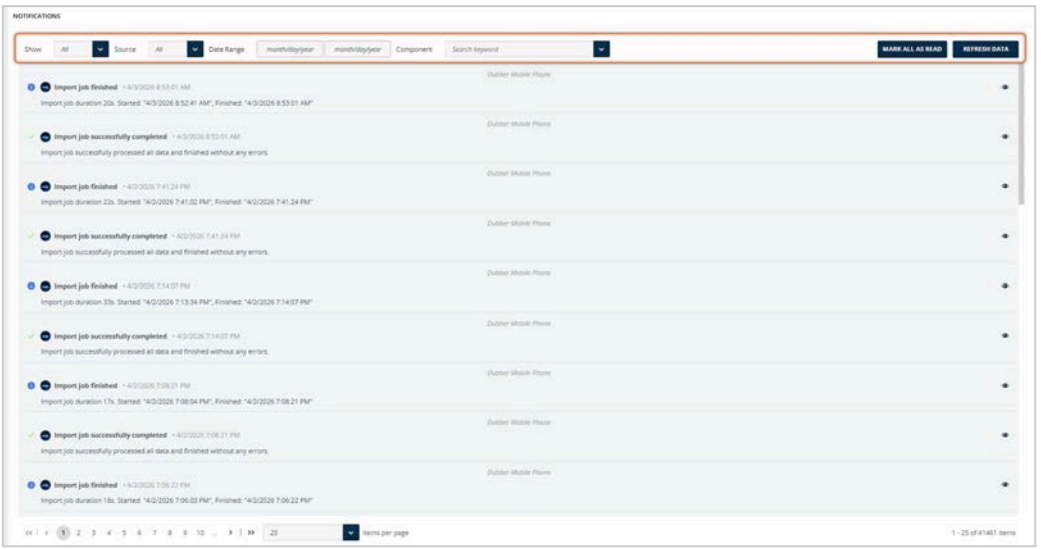
Managing Notifications

Filtering Notifications

To help you navigate large volumes of data, the Notifications section includes advanced filtering and management tools to narrow your view and keep your logs organized.

Use the following filters to refine the list of displayed notifications:

- **Show:** Display notifications based on the status or the nature of the alert. Notifications are classified into the following types:
    - **Read/Unread:** Filter notifications based on whether they have been marked as read or remain unread.
    - **Failure:** Marks critical issues or failures that require immediate intervention, such as system errors, file parsing issues, or connectivity problems.
    - **Warning:** Highlights non-critical issues that may require attention, such as skipped tasks or minor configuration problems.
    - **Info:** Indicates general status updates and routine system information.
    - **Success:** Indicates operations that have completed successfully without issues.
- **Source:** Categorize notifications by their origin, choosing between System-level events or Importer-specific events.
- **Date Range:** Specify a timeframe by selecting *Before* and *After* dates to view events from a particular period.
- **Component:** Narrow results down to specific components, including Importers, Collectors, Filters, and Targets.



Notification Actions

Users can perform the following actions to manage their notification history:

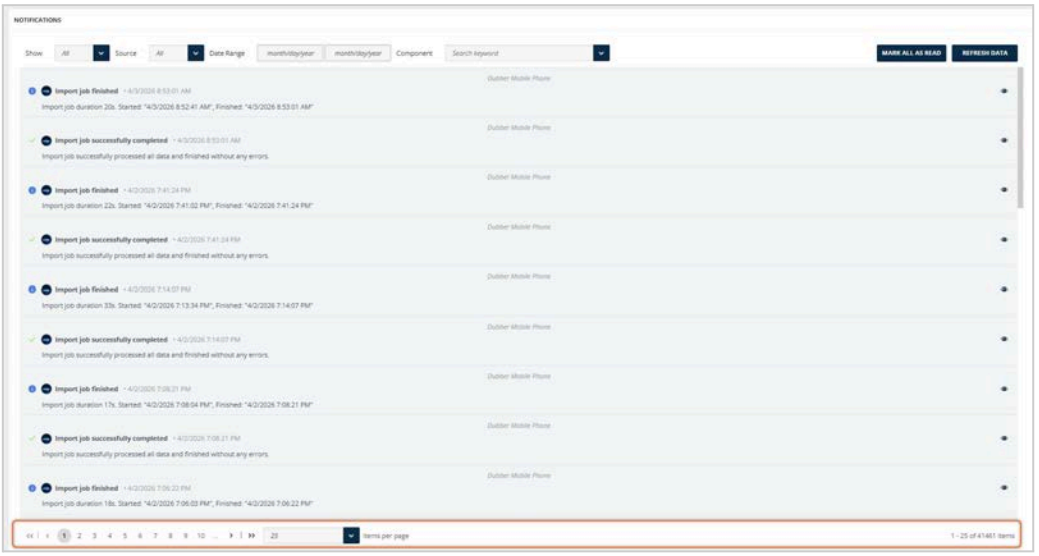
- **Mark as Read:** Acknowledge individual alerts by clicking the *eye* icon next to the notification.
- **Mark All as Read:** Instantly update the status of all current notifications by clicking **Mark All as Read**.

- **Refresh Data:** Update the notification list with the most recent events without needing to refresh the entire browser page.

Navigation and Pagination

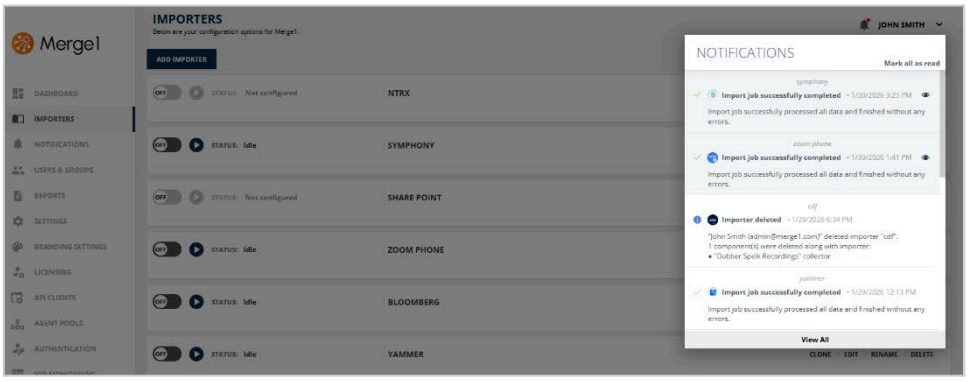
If you have a large number of notifications, use the pagination tools located at the bottom of the section:

- **Page navigation:** Click the page numbers or arrows to move through multiple pages of notifications.
- **Items per page:** Use the drop-down menu to adjust how many notifications are displayed at once (25, 50, or 100 items per page).



Quick Access Notifications

Recent notifications are displayed in the right upper corner of the main screen without leaving your current page.



Here, the latest 10 notifications are instantly displayed.

The following actions can be performed:

- Click **Mark all as read** to quickly mark all notifications as read, including those beyond the visible 10.
- Click **View all** to open the Notification Center page for comprehensive management.

CHAPTER 7

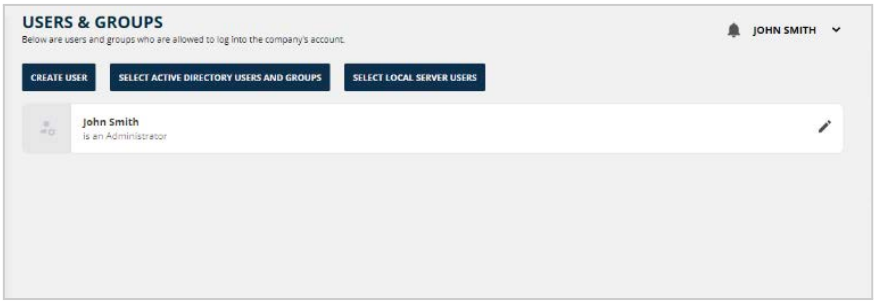
Users & Groups

This chapter represents:

- Users and Groups
- Creating a Merge1 User
- Selecting an AD User Account
- Selecting Local Server Users

Users and Groups

To manage Merge1 user accounts, click **User Profile** on the **Navigation Pane** located on the left side.



Users can be added to Merge1 in three ways:

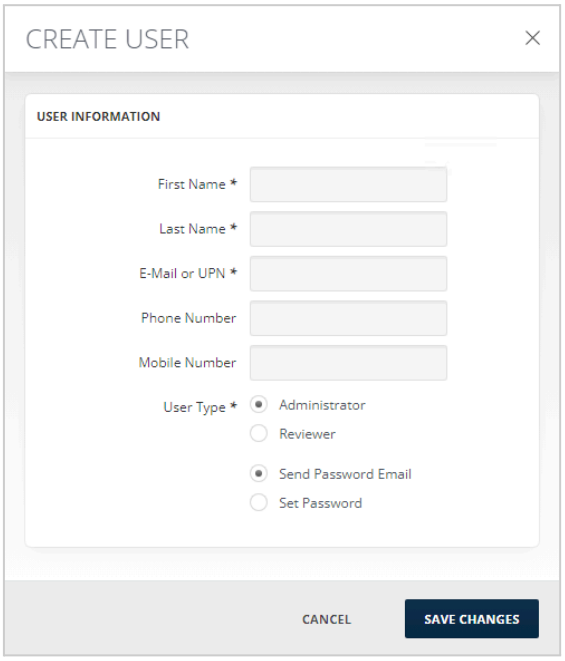
1. **Creating a User**
2. **Selecting Active Directory Users and Groups**
3. **Selecting Local Server Users**

Creating a Merge1 User

With this option, a user can be created directly in the Merge1 environment.

- Click **Create Merge1 User** to add a new account.
- You can edit user information and passwords by clicking the edit icon next to the username.
- You can easily delete the user account by clicking the trash can.

To create a user:



1. Provide Merge1 the following information:

- First name (required)
- Last name (required)
- Email address (required)

- Phone number
- Mobile number

2. Assign the user type: **Administrator** (has full access) or **Reviewer** (can view only Reports and Dashboard). Once you select the user type, click **SAVE CHANGES**.
3. Enable **Send Password Email**. Note that the password should be changed after entering the temporary password.
4. Enable **Set Password** and enter **Password** and confirm it.

Password requirements are:

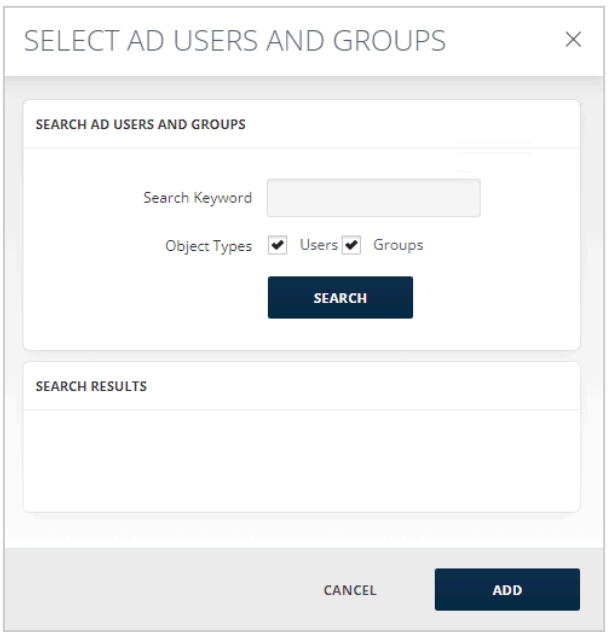
- Minimum length of 12 characters.
- Combination of upper and lowercase letters, numbers, and symbols.

Note

To search for a particular user, enter the value of one of the following Active Directory user attributes: "cn", "samaccountname", "givenname", "sn", or "mail".

Selecting an AD User Account (Recommended per industry best practice)

This option allows picking a user directly from the Active Directory of the Windows server the device is part of.

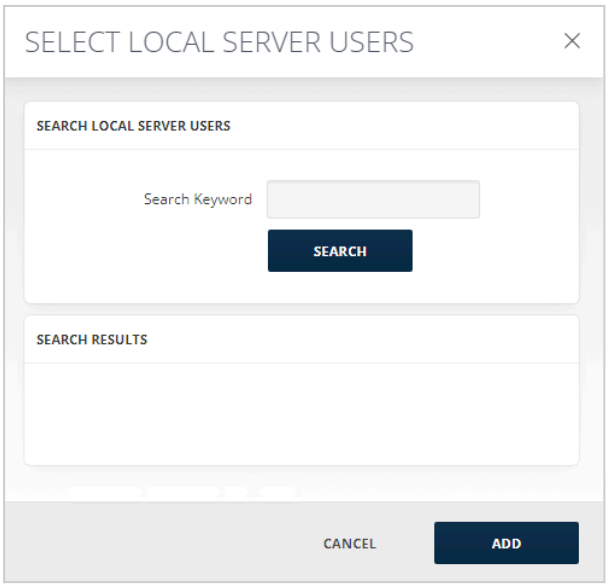


1. Click **Select AD Users and Groups** to add a new account.
2. Search for **Active Directory** users by a keyword. If no keyword is added, all Active Directory users will be shown.
3. Select the user(s) you want to add and click **Add Users**.

4. Select the type of the user (Administrator or Reviewer).

Selecting Local Server Users

This option allows picking a user directly from the users on the device Merge1 is installed on.



1. Click **Select Local Server User Account** to add a new account.
2. Search for **Active Directory** users by a keyword. If no keyword is added, all local users will be shown.
3. Select the user(s) you want to add and click **ADD USERS**.
4. Select the type of the user (Administrator or Reviewer).

CHAPTER 8

Reports

This chapter represents:

- Overview
- Managing Reports

Overview

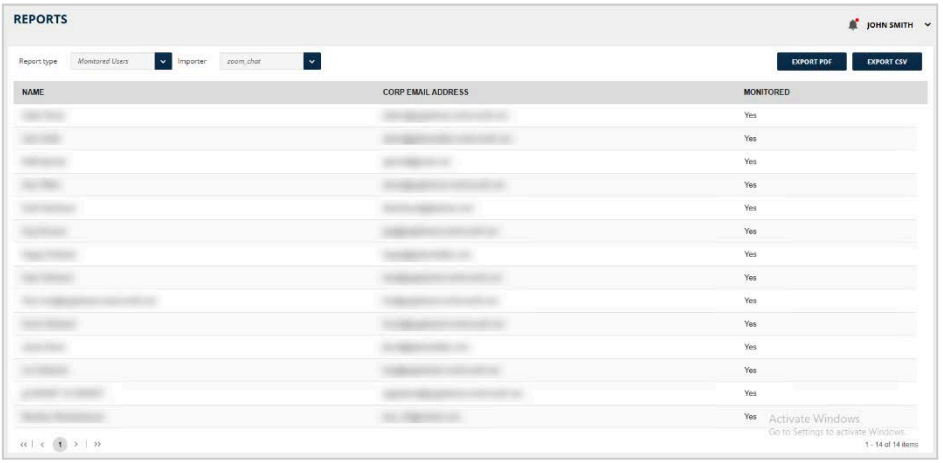
To view and extract detailed information on Mergel user activity and delivery failures, click **Reports** in the **Navigation Pane**.

- **Audit:** View Mergel user activity.
- **Monitored Users:** View monitored users by Mergel.
- **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.

Finally, you can export the report information either in a PDF or CSV format.

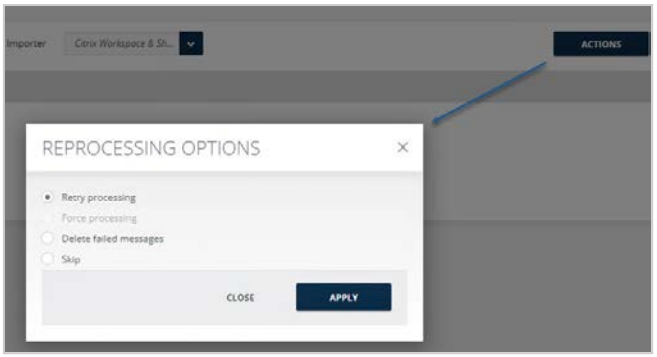


For **Audit** and **Monitored Users** reports data can be exported as a PDF or CSV file when clicking the corresponding button on the right side.

The **Target Delivery Failure, Missing Attachment Failure, Missing Disclaimer Failure**, and **Data Acquisition Failure** reports have some of the following functionalities as not all actions are active for the given report types:

- **Actions**

  The **Reprocessing Options** are the following:
  - 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.

Important

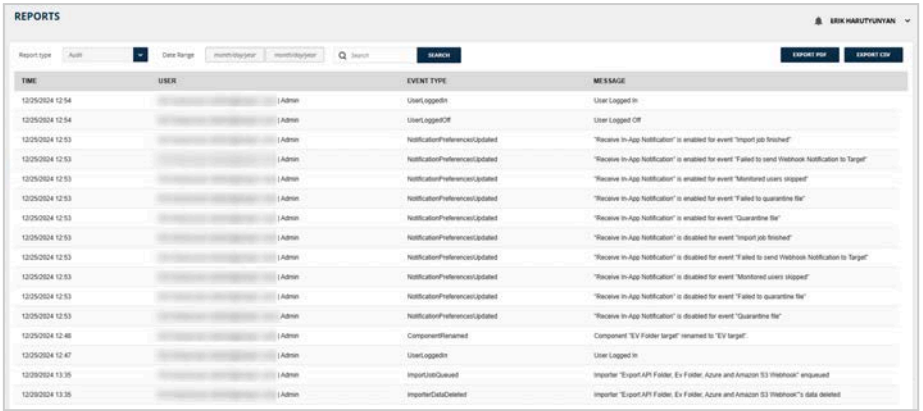
The Reprocessing Options are applied in pairs with the **Importer Settings > Processing > Processing Options**, i.e., Processing Options should also be configured, so the **Reprocessing Options** configuration is applied properly.

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.

By clicking **Export Messages**, the report messages will be downloaded as a ZIP file containing EML, JSON, or TXT files. The files contain all the generated data. Above the message body, the failure reason is specified with an ERROR status. This functionality is useful in cases when target delivery failure occurs: the messages can be downloaded here and manually sent to the archive.

Audit Report

Many important actions that users make such as logging in or configuring importers, are listed in Audit.



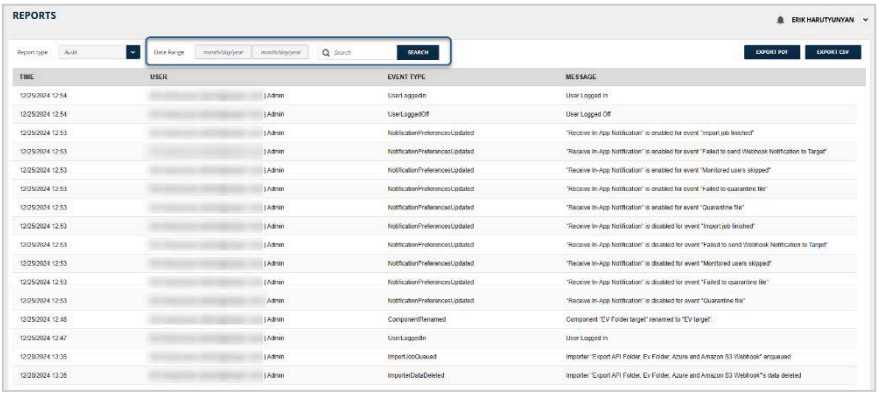
The following event types are captured:

- LicenseChanged
- SqlConfigurationUpdate
- TargetAdded
- ConnectorAdded

- FilterAdded
- ImporterAdded
- ComponentSettingsModified
- ImporterServiceStart
- ImporterServiceStop
- TargetRemoved
- ConnectorRemoved
- FilterRemoved
- ImporterRemoved
- NetworkSettingsChanged
- AuditSettingsUpdated
- MessageHeadersSettingsUpdated
- ComponentRenamed
- ComponentDataDeleted
- ImporterDataDeleted
- ManualImportStart
- ScheduledImportStart
- ImporterCloned
- FilterCloned
- ConnectorCloned
- TargetCloned
- UserLoggedIn
- UserLoggedOff
- UserIsCreated
- UserIsDeleted
- UserUpdatedProfileInfo
- UserTypeUpdated
- ImporterSchedulerEnable
- ImporterSchedulerDisable
- AgentEnabled
- AgentDisabled
- AgentCreated
- AgentDeleted
- AgentUpdated
- MonitoredUserSourceUpdated
- APIClientApplicationAdded
- APIClientApplicationRemoved
- APIClientApplicationChanged
- SmtpServerSettingsChanged
- ImportJobQueued
- ImportJobCanceled
- ImporterScheduledRunSkipped
- ImporterSchedulerEnabled
- ImporterSchedulerDisabled
- NotificationPreferencesUpdated
- JITUserIsProvisioned
- JITUserRoleIsUpdated

Filtering Audit Reports

The filtering option allows filtering out the list of records from the section using the date range filter and the search functionality.



Unprocessed Messages Report

The Unprocessed Messages report generates information on messages which have been constructed and stored in the database, but there has not 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 that to process the unprocessed messages, the **Processing Options** of Importer Settings should be configured.

Target Delivery Failure Report

This report type generates information on messages that are constructed and stored in the database—an attempt is made to send them to the target, but the attempt fails.

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 Report

For collectors, such as Bloomberg or Symphony, the Attachment Validation sub-section of the Source configuration provides an option to fail messages with missing attachments.

Information on failed messages with missing attachments is reflected in the **Missing Attachment Failure** report.

Missing Disclaimer Failure Report

For collectors, such as Bloomberg, the Disclaimer Validation sub-section of the Source configuration provides an option to fail messages with missing disclaimers.

Information on failed messages with missing disclaimers is reflected in the **Missing Disclaimer Failure** report.

Data Acquisition Failure Report

When Merge1 captures incomplete or damaged data, the information will be reflected in the Data Acquisition Failure report in case a report is generated.

Initially, this report was 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) is 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.

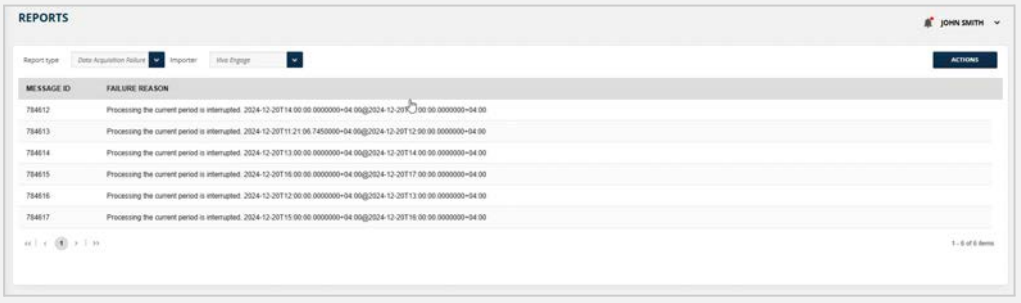
When the data processing failure occurs, an output message is constructed. The body of the message contains the start and end dates (separated with ":") of the processing data (chunk), and the failure type is mentioned as **Data Acquisition Failure**.

When Merge1 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.

Note

- 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** and **Microsoft Teams via Webhooks** collectors, the Data Acquisition Failure report information is generated differently. Specifically, Merge1 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 Merge1 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.



CHAPTER 9

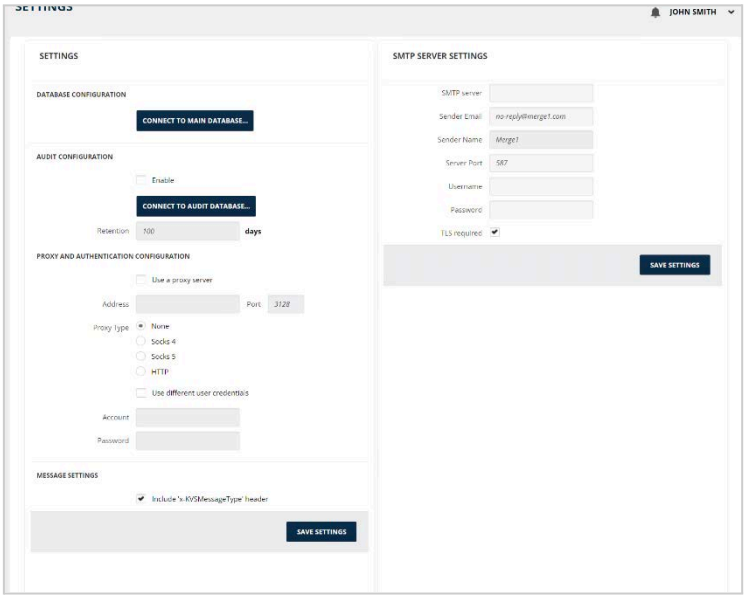
Settings

This chapter represents:

- Overview
- Merge1 Settings
- SMTP Server Settings

Overview

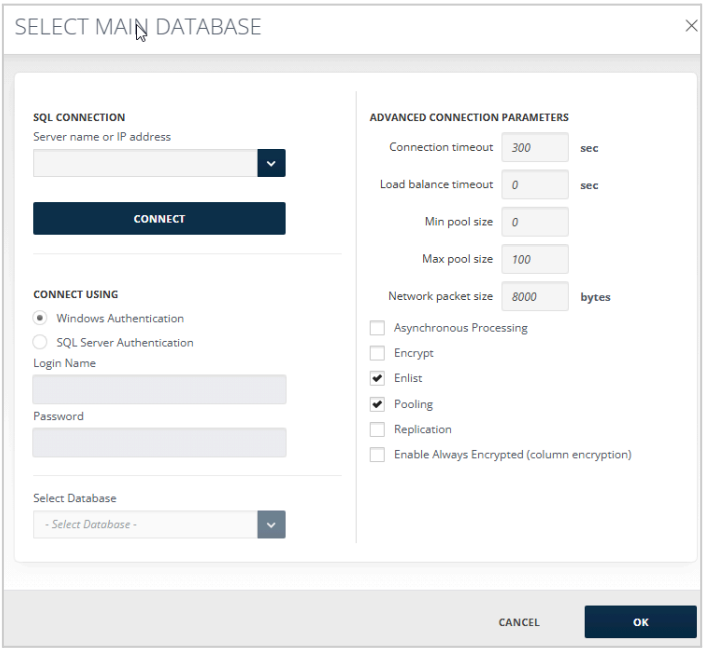
To view or configure Settings, navigate to the **Settings** section of the **Navigation Pane**. **Settings** and **SMTP Server Settings** sections show up.



Settings

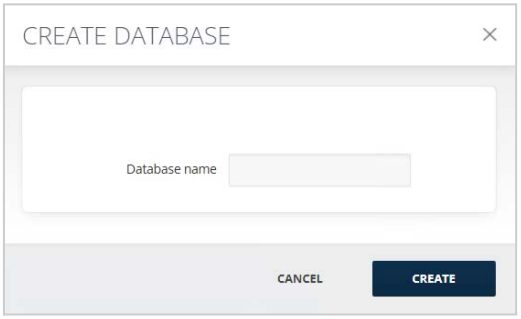
Database Configuration

1. Click **Connect to Database** to view the database configuration menu.



2. Select an **SQL server** from the drop-down list or enter one in the same field.
3. Click **Connect**. The **Select Database** drop-down becomes active.

4. When picking **Create New** from the drop-down list, a prompt appears.



5. Specify a name for the database and click **Create**. Select the database from the drop-down menu.
6. Choose between Windows or SQL Server Authentication and enter the Login Name and Password.

> **Note**
>
> When **Windows Authentication** is selected, **Login Name** and **Password** fields will be disabled because the credentials during installation will be used.

> **Note**
>
> Users who wish to specify a custom disk and path on the SQL Server, must perform the following steps:
>
> 1. Create a new empty database in SQL Server.
> 2. Specify the desired LogFile and DataFile paths.
> 3. Add a new File group named **LargeDataFileGroup**.
>   a. Add a new file named **LargeDataFile1** to this group, specifying the desired path.
> 4. Select the newly created database from Mergel Settings GUI and select **YES** when prompted to initialize the database.

1. Configure **Advanced Connection Parameters** by specifying:

- Connection timeout
- Load balance timeout
- Min pool size
- Max pool size
- Network packet size
- Asynchronous processing
- Encrypt
- Enlist
- Pooling
- Replication
- Enable always encrypted (column encryption)

2. Once you have carried out all the required steps, click **OK**. A **Success** pop-up window with **Database successfully selected** info will show up.
3. Click **Save Settings**, then **Yes** to re-login Merge1.

Audit Configuration

Audit Database is used to log the activity performed in Merge1 GUI, such as logging in, setting up a collector, running an importer, etc.

To set up the Audit Database:

1. Click **Connect to Audit Database** and fill in the database information as shown in the **Database Configuration** steps.

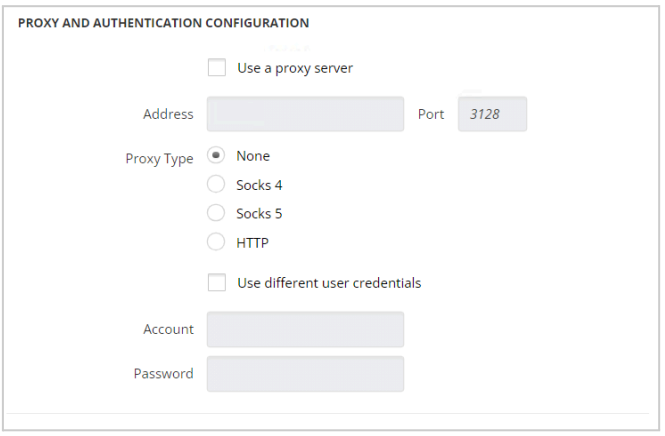
   Note that the **Enable** option should be checked to record the audit logs in the database.
2. To check the **Audit logs** in the Reports section, select Audits in the Report Type drop-down list.

Proxy and Authentication Configuration

A proxy server allows the traffic to flow through the proxy server to the address you requested.

To configure the proxy:

1. Enable **Use a proxy server**.
2. Specify **Address** and **Port**.
3. Select **Proxy type**:
   - None
   - Socks 4
   - Socks 5
   - HTTP
4. If you want to use credentials of a different user, enable the corresponding checkbox, and enter the **Account** and **Password**.



Note

If your organization uses a proxy server, make sure the address and port information match those of your browser's proxy settings.

Message Settings

The **x-KVSMessageType header** is used for e-discovery tasks associated with Arctera Compliance Accelerator and Discovery Accelerator.

Click **SAVE SETTINGS** to save the settings for the Merge1 Settings.

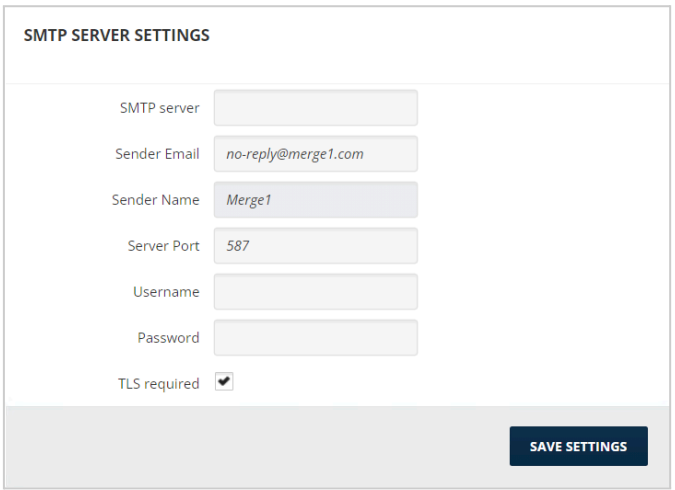
SMTP Server Settings

SMTP is an internet standard communication protocol for electronic mail transmission. When an email is sent, the SMTP server processes the email, decides which server to send the message to, and relays the message to that server.

To set up the SMTP Server settings, enter the required information in the following fields:

- SMTP Server
- Server Email
- Server Port
- Username
- Password

If you want to ensure privacy between communicating applications, check **TLS required** [68].



Click **SAVE SETTINGS** to save the settings for the SMTP Server.

[68] Transport Layer Security (TLS) is a cryptographic protocol designed to provide communications security over a computer network. Merge1 is compliant with TLS version 1.3.

CHAPTER 10

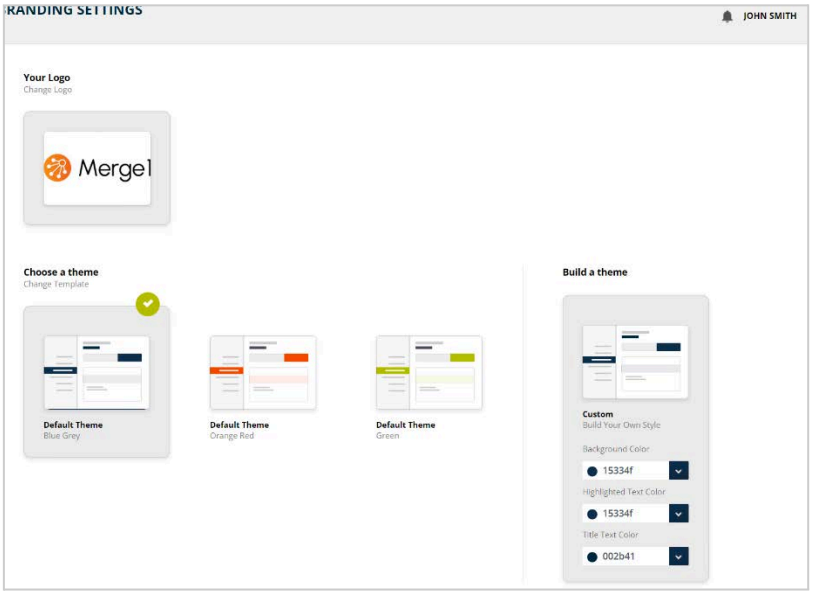
Branding Settings

This chapter represents:

- Managing Brand Settings

Managing Branding Settings

The Merge1 interface look can be changed to make it closer to the corporate colors. The color palette, as well as the logo, can be changed by clicking **Branding Settings** in the **Navigation Pane**.



CHAPTER 11

Licensing

This chapter represents:

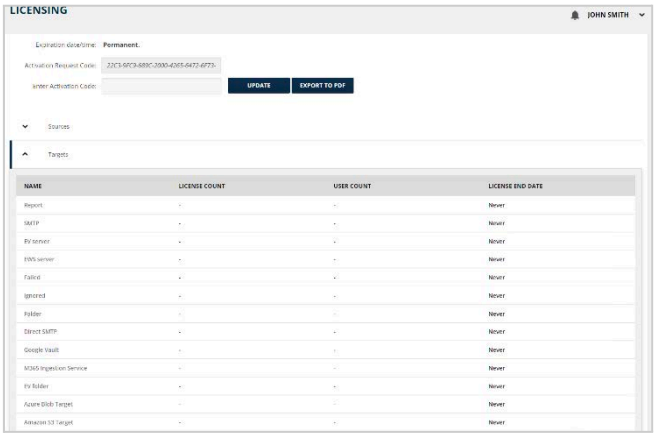
- Overview
- License Details
- Activating License
- Exporting to PDF

Overview

Licenses are distributed for **Collector** and **Target** types individually. To activate a component or components, send the **Activation Request Code** to Arctera Support.

When installing Mergel V7 for the first time, a trial version of Mergel will be installed offering the fully functional version of the product for 30 days.

When upgrading Mergel V6 to Mergel V7, License Activation Key will be required. To see the licensing info, navigate to the **Licensing** section of the **Navigation Pane**.



License Details

All license information can be found under **License Details**:

- The **License Status** can be marked as **Valid**, or the following status will show up:

License Status: **License has been marked as inactive on this computer. Please request Veritas for a new valid License Key.**

- **Mergel Version.** The currently used Mergel version.
- **Client ID.** The ID generated for you as a client.
- **Expiration date/time.** The expiration date/time will be specified: it can be permanent or for a specific date.
- **Activation Request Code.** The code that is sent to the support team for getting the activation code.
- **Enter Activation Code.** The field to enter the requested activation code. Click **UPDATE** to activate the license.

The following information is included in the license report:

- Name
- License Count
- User Count
- License End Date.

Activating License

Licenses are distributed for **Sources** and **Target** types individually. To activate a component or components, send the **Activation Request Code** to Arctera Support.

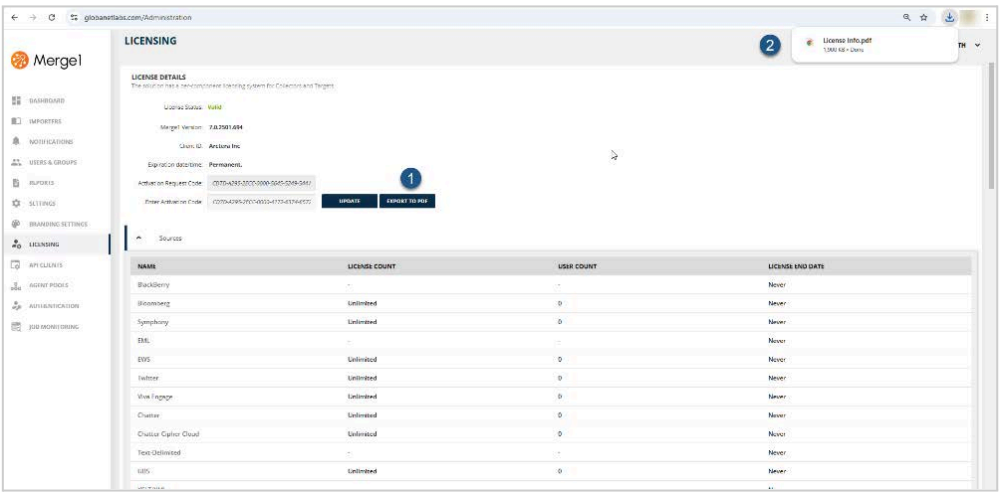
If you fail to see **License Status** marked as **Valid** contact the Arctera Support team to activate the license.

Note

If you go over the limit of the license of the API-based collectors, Bloomberg, LSEG (Refinitiv), a warning message will be generated in the logs. Contact the support team for a new license.

Exporting to PDF

To have the details of the license page in a PDF file click **EXPORT TO PDF** and Merge1 license info will be downloaded to your local PC.



CHAPTER 12

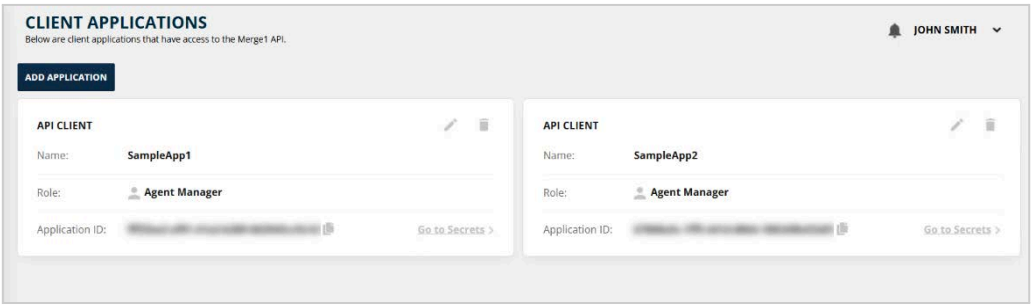
API Clients

This chapter represents:

- Overview
- Managing API Clients
- Managing Secrets
- Managing JSON Web Keys

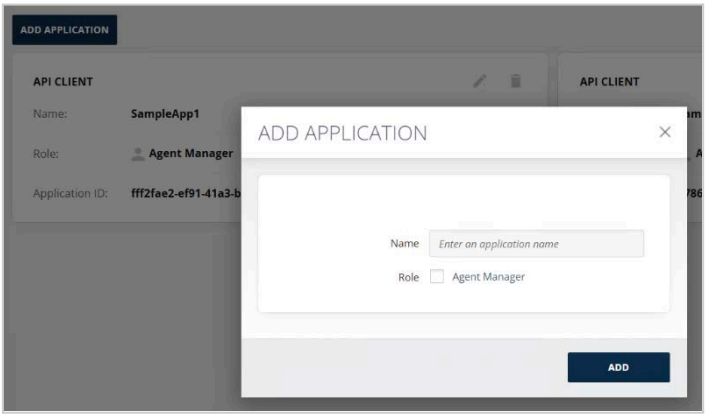
Managing API Clients

The sub-section represents how the apps can be added, edited, and deleted.

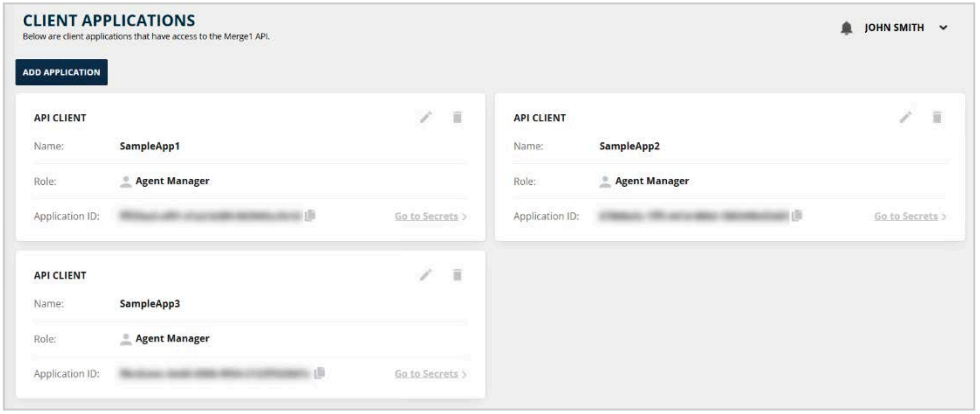


Adding a New Application

1. Go to the **API Clients** section of the **Navigation Pane**.
2. Click **Add Application** and a pop-up window will open.



3. Specify a name (maximum 64 characters in length).
4. Select the **Agent Manager** role.
5. Click **Add** and a new card will be added to the page.



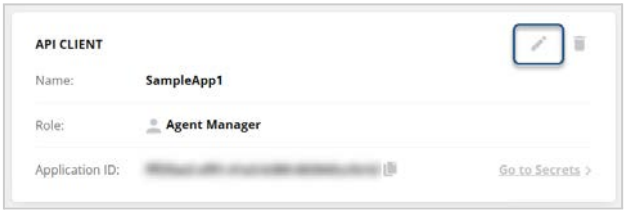
The application consists of the following fields:

- **Name.** The application name is specified.

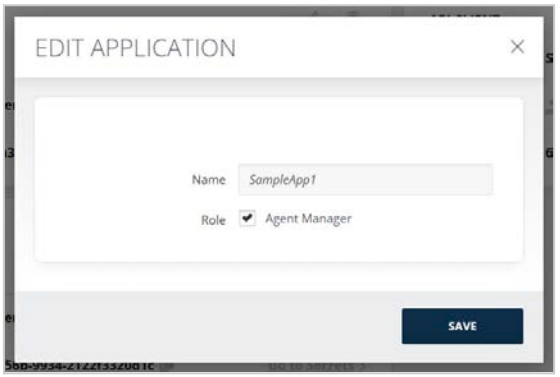
- **Role.** The level of accessibility is specified.
- **Application ID.** Application ID is presented. The user can copy the ID by clicking the *copy* button.

Editing an Application

1. Click **Edit** on the card and a popup will open to edit the application info.

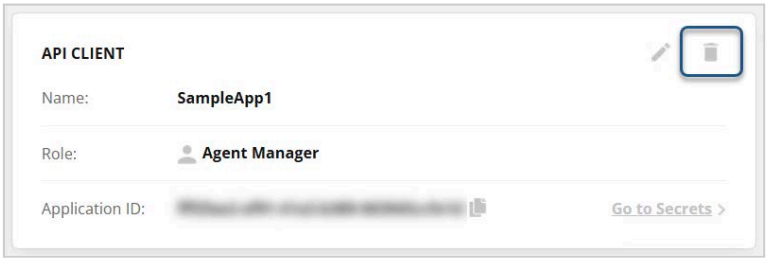


2. Modify the **Name** and click **Save**.



Deleting an Application

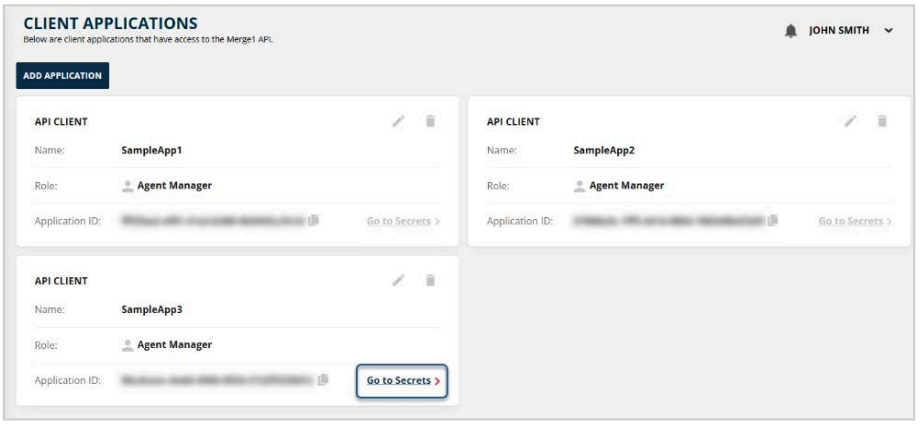
1. Click **Delete** at the top right corner of the application.



2. Click **Yes** if you want to proceed or **No** to cancel the deletion.

Managing Secrets

1. Click **Go to Secrets** on the application card's bottom corner.

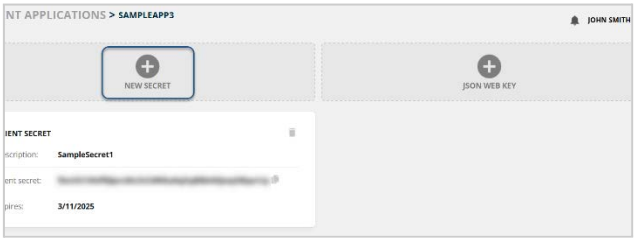


2. Add a **Secret** or a **JSON web key** to pass an OAuth authentication (see **Configuring an Agent via `agentConfiguratorGUI.exe`** for using the Secret).

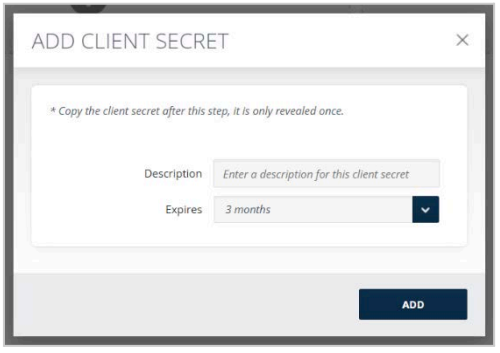
Adding a Secret

To add a secret:

1. Click **New Secret**.



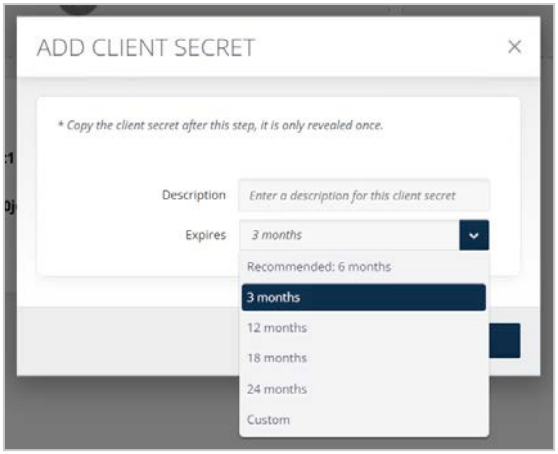
2. In the opened pop-up window, enter a **Description** (maximum 500 characters in length) for the secret.



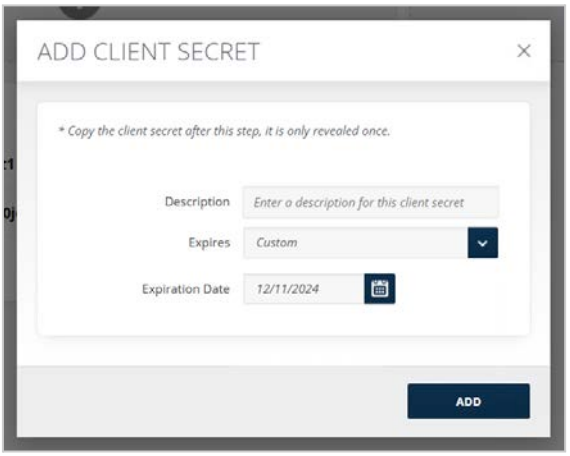
3. Select an expiration period from the drop-down list. Available periods:

   - Recommended: 6 months
   - 3 months
   - 12 months
   - 18 months
   - 24 months
   - Custom

> **Note**
>
> The specified expiration period is used to invalidate the secret.



If **Custom** is selected, the **Expiration Date** picker will be shown below with the current system date. Select a date.



4. After filling in the required fields, click **Add** and a new card will be added to the page.
   The secret card consists of the following fields:

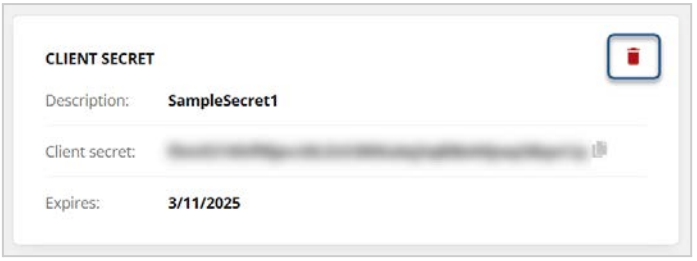
   - Description. The description of the secret is specified.
   - Client secret. The client secret is specified.
     The Client secret will be shown only when creating the secret. It should be copied using the **Copy** button and saved in a secure location for later usage.

- **Expires.** The expiration date will be specified. And if Custom is selected, the user can manually set the date using Calendar.

> **Note**
>
> - All secrets are immutable (not editable). Once generated, it will be active until the expiration date.
> - Shared Secrets are stored in the database in a hashed format; hence the system can/will show it in a plain text mode only at the generation time.

Deleting a Secret

1. Click **Delete** at the top right corner of the secret card.



2. Click **Yes** if you want to proceed or **No** to cancel the deletion.

Managing JSON Web Keys

Adding a JSON Web Key

To add a JWK public key:

1. Click **JSON Web Key**.

2. In the opened pop-up window, enter a **Display Name** (maximum 500 characters in length) for the public key and provide a **JWK Public Key** (maximum 4000 characters in length).

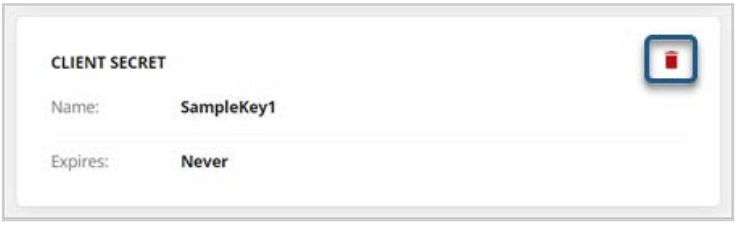
3. After filling in the required fields click **Add** and a new card will be added to the page.
   The JWK public key card consists of the following fields:

   - **Name.** The JWK public key name is specified.
   - **Expires.** The expiration date will be specified.

> **Note**
>
> JWK public keys do not have an expiration period. They are valid until they are deleted from the system.

Deleting a JSON Web Key

1. Click **Delete** at the top right corner of the JSON web key card.



2. Click **Yes** if you want to proceed or **No** to cancel the deletion.

> **Note**
>
> JWK Public Keys do not have an expiration period. They are valid until the User deletes them from the system.

CHAPTER 13

Agent Pools

This chapter represents:

- Overview
- Managing Agents
- Managing Agent Pools

Overview

The Agent Pool is a virtual/logical container for one or multiple agents.

The agent is the component that executes jobs. When a job execution request is queued, the Agent manager selects an agent from the pool and sends the job request to the agent. For an agent to get selected by the manager, it must meet certain conditions:

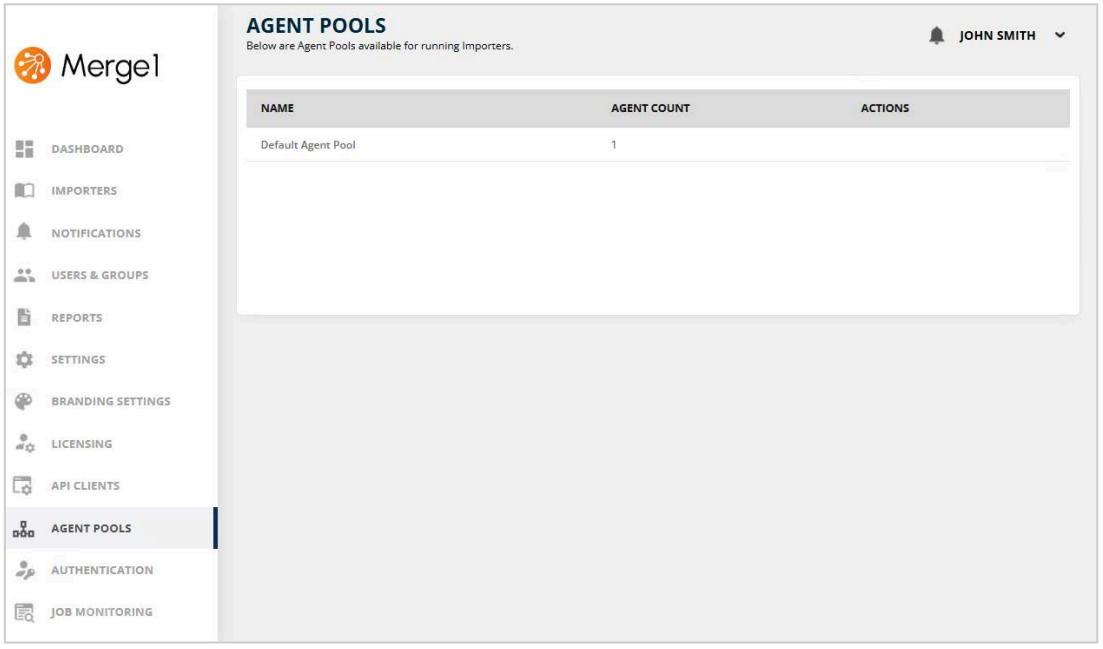
- It must be on the same version of Merge1 Web Service.
- It must be online and enabled.
- It must be idle or have the capacity[69] to execute a job.

Note

Each agent must be registered by the user in Merge1 Web and Agent Pool. All jobs are assigned to the default agent pool.

Managing Agent Pools

This section represents how agent pools can be managed.



In the **Agent Pools** section of the **Navigation Pane**, the following information is available:

- **Name**: The name of the Agent Pool.
- **Agent Count**: The count of the agents in the pool.

Note that an Agent Pool cannot be added. Only the Default Agent Pool is available for managing agents.

[69] The capacity is set by the user during the agent registration.

Managing Agents

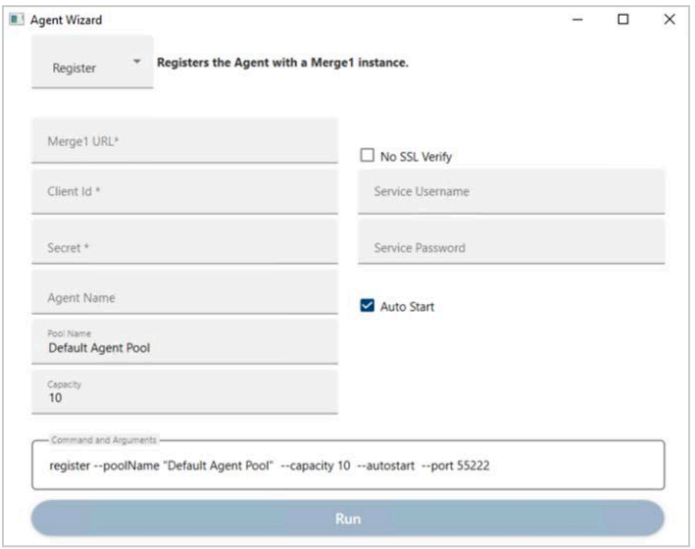
This section represents how agents are configured - registered, started, edited, and deleted/unregistered.

Configuring an Agent via `agentConfiguratorGUI.exe`

An Agent can be configured - registered, run, reset to its initial state, or unregistered via the Agent Configurator GUI. Here you can also start or stop Windows Service, get information on the registration status of the Agent, get help on a specific command, and more.

To register an Agent:

1. Open the `C:\Program Files\Arctera Inc\Merge1 Agent` folder.
2. Double-click the `agentConfiguratorGUI.exe` file. The **Agent Wizard** will open.
3. On the top left corner drop-down menu, select register and fill out the following information:
   - **Merge1 URL**: Specify the Merge1 instance URL.
   - **Client Id**: Specify the application ID of the created application in API Clients.
   - **Secret**: Specify the secret of the above-used application copied and saved priorly.
   - **Agent Name**: Specify the Agent name.
   - **Pool Name**: Specify the Agent Pool name. By default, the name is Default Agent Pool.
   - **Capacity**: Specify the maximum capacity of parallel jobs that an Agent should execute. The default value is set to 10.
   - **No SSL Verify**: Enable the checkbox to skip SSL validation both for the configurator and the Agent. Otherwise, keep it disabled.
   - **Service Username**: Specify Windows Service log on account username.
   - **Service Password**: Specify Windows Service log on account password.
   - **Auto Start**: Disable the checkbox to turn off Windows Service automatic start behavior. Otherwise, keep it enabled.



4. Click **Run**.

The Agent Configurator also includes the following configuration options:

- **Unregister:** Unregisters the Agent from the Merge1 instance and cleans up the Agent's local state.
- **Cleanup:** Cleans up the Agent's local state: The Agent will reset to its initial state.
- **Status:** Prints the registration status of the Agent.
- **Stop Service:** Stops the Windows service if it exists.
- **Start Service:** Starts the Windows service if it exists.
- **Help:** Displays more information on a specific command.

Note that each command can be configured by typing the relevant script in the **Command and Arguments** field and clicking **Run**.

Registering an Agent via PowerShell

1. Open the Merge1 Agent folder from `C:\Program Files\Arctera Inc` folder in Windows PowerShell as an administrator.
2. In PowerShell, type the following command to unblock the possible blocked files:

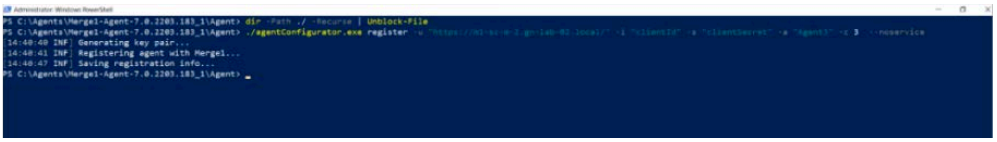
```
dir -Path ./ -Recurse | Unblock-File
```

3. Use the following command to register an Agent:

```
./agentConfigurator.exe register -u "<Portal>" -i "<ApplicationID>"
-s"<ClientSecret>" -a "<AgentName>"
```

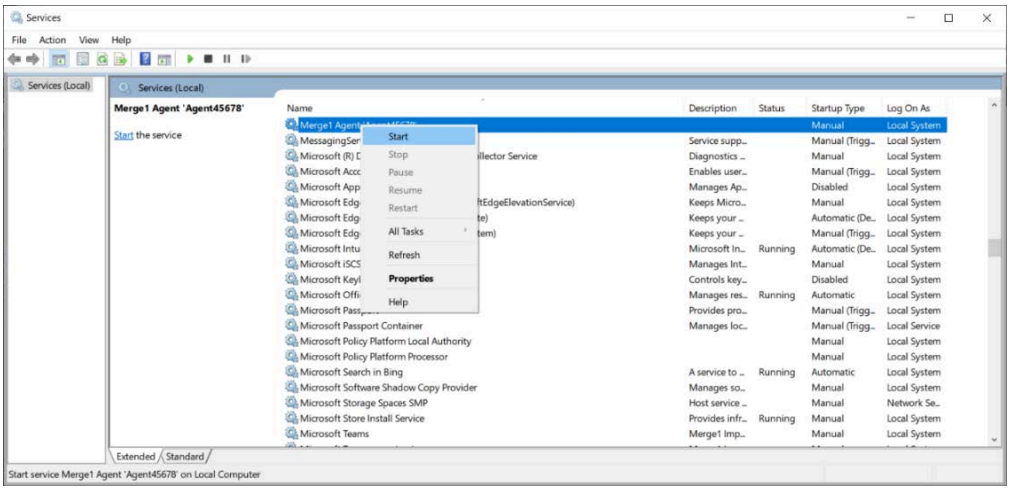
4. Make sure to set the following variables in the command:
   - 4.1. `-u "<Portal>"`: The Merge1 instance URL. You can find it in `</Merge1_installation_directory/Arctera Inc\Merge1 7.0 >`.[70]
   - 4.2. `-i "<ApplicationID>"`: The application ID of the created application in API Clients (see **Adding a New Application**).
   - 4.3. `-s "<ClientSecret>"`: The secret of the above-used application was copied and saved priorly (see **Adding a Secret**).
   - 4.4. `-a "<AgentName>"`: An agent name.
   - 4.5. `-c <capacity>`: Defines the maximum capacity of parallel jobs that an Agent should execute.
   - 4.6. `-p <PoolName>`: Specifies the name of the pool under which the agent should be registered.
   - 4.7. `--serviceUsername`: Windows Service logs on account username.
   - 4.8. `--servicePassword`: Windows Service log-on account password.
   - 4.9. `--autostart`: Windows Service start behavior.
   - 4.10. `--sslNoVerify`: Uses this command to skip SSL validation both for the configurator and the agent.

[70] In case of Merge1 version 6.0, the path will be `C:\Program Files\Globanet Consulting Services\Merge1 6.0\`.

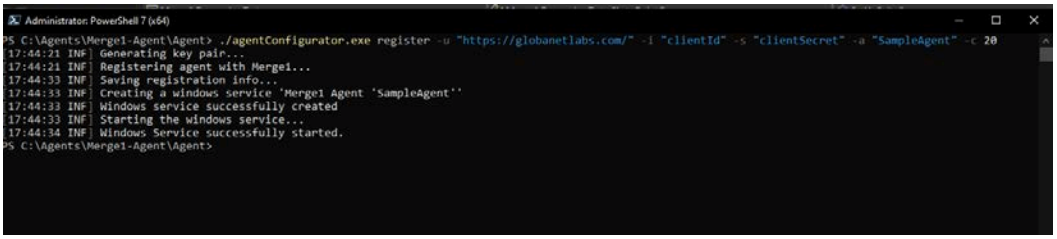


Starting an Agent

A windows service will be created after registration. An Agent will be started/stopped using the Services app.

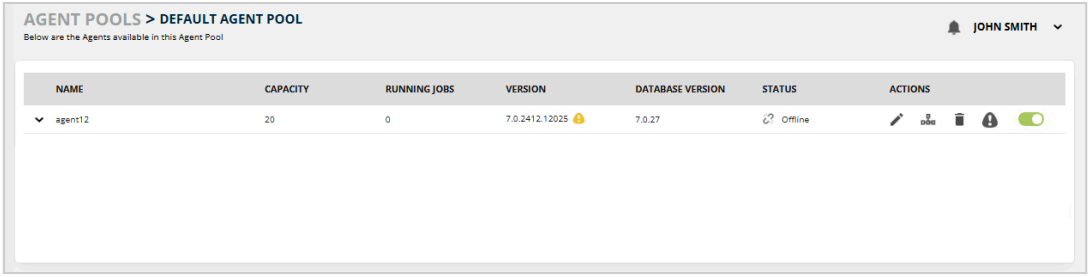


To open the **Services** app, click **Windows Start**, and type `Services`.



Managing Agents on the Merge1 GUI

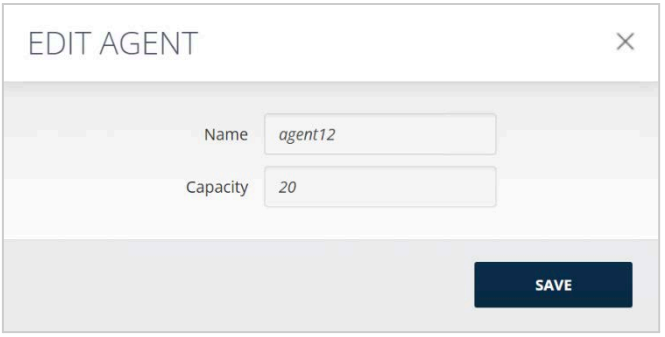
1. Go to **Merge1 > Agent Pools**.
2. Click **Default Agent Pool** and the Agent Pool details page will open.



It consists of the following columns:

- **Name**: The name of the Agent.

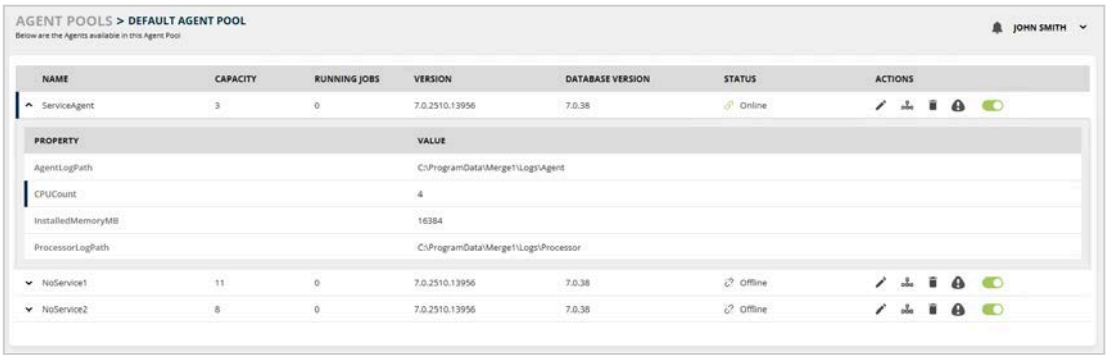
- **Capacity**: The maximum number of parallel jobs that the Agent should execute.
- **Running Job**: The number of ongoing jobs that the Agent is executing.
- **Version**: The Agent version.
- **Database Version**: Merge1 database version.
- **Status**: The status of the Agent:
    - **Online**: The Agent is up and can receive commands.
    - **Offline**: The Agent is down and cannot receive commands.
- **Actions**:
    - **Edit**: The Agent name and capacity can be edited.



    - **Move**: The Agent can be moved to another pool. [71]
    - **Delete:** See **Deleting/Unregistering an Agent**.
    - **Agent Diagnostics**: See **Viewing Diagnostic Data**.
    - **Enable/Disable**: The agent can be enabled or disabled.
      Note that when an Agent is online, but it is disabled, it will not run a job.

3. Click the *expand* button left to the Agent name to see the following additional information:

- **AgentLogPath**: Shows the logs folder path of an Agent. This is a full path that can be found in the Agent server.
- **CPUCount**: Shows the available resources on an Agent server. This is the number of logical processors of the CPU installed on the Agent server.
- **InstalledMemoryDB**: Shows the actual memory available for an Agent job.
- **ProcessorLogPath**: Shows the logs folder path of a Processor. This is a full path that can be found in the Agent server.



[71] Not applicable for on-prem users.

Deleting/Unregistering an Agent

An Agent can be deleted/unregistered by:

- Deleting an Agent from the Agents grid.
  1. Go to **Agent Pools > Default Agent Pool**.
  2. Click the *delete* button under **Actions** and the Agent will be deleted.
- Unregister an Agent using a command line.

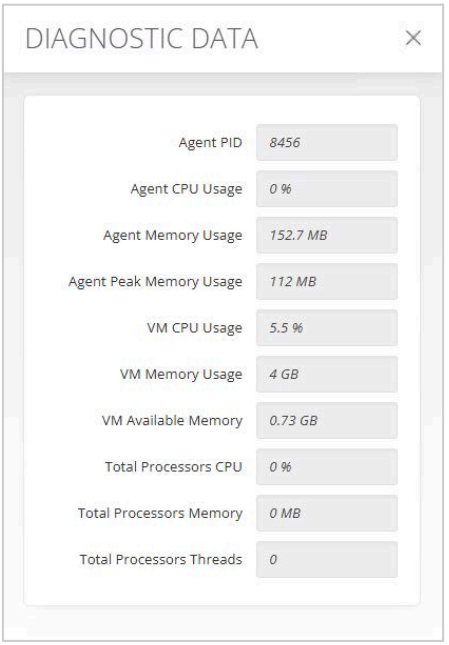
  Use the following command to unregister the Agent:

  ```
  ./agentConfigurator.exe unregister
  ```
- Unregister an Agent through the Agent Configurator. See **Configuring an Agent via `agentConfiguratorGUI.exe`**.

Viewing Diagnostic Data

To see the diagnostic data, click the *info* icon and a pop-up will open with the following information:

- Agent PID
- Agent CPU Usage
- Agent Memory Usage
- Agent Peak Memory Usage
- VM CPU Usage
- VM Memory Usage
- VM Available Memory
- Total Processors CPU
- Total Processors Memory
- Total Processors Threads



CHAPTER 14

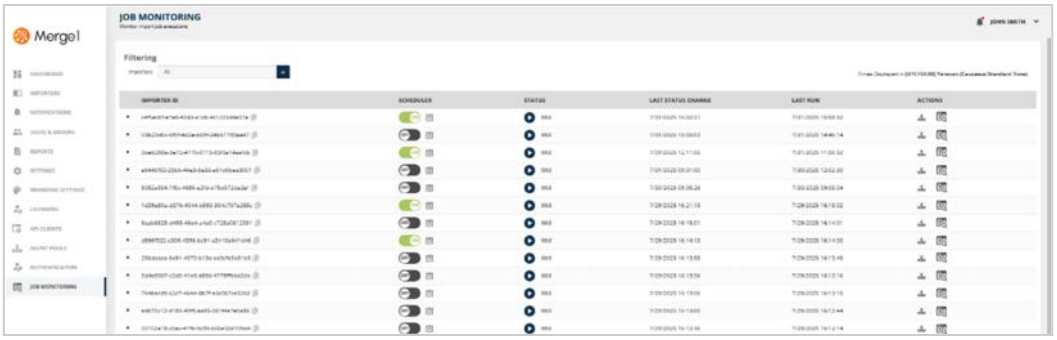
Job Monitoring

This chapter represents:

- Overview
- Managing Job Executions

Overview

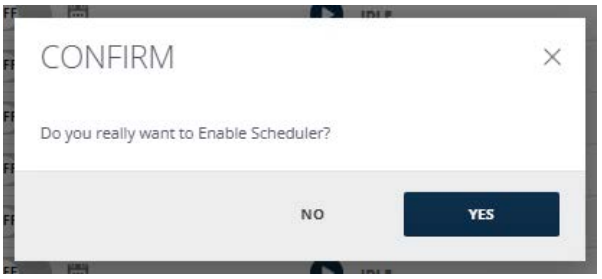
This **Job Monitoring** section allows Merge1 admins to monitor import jobs with their job executions.



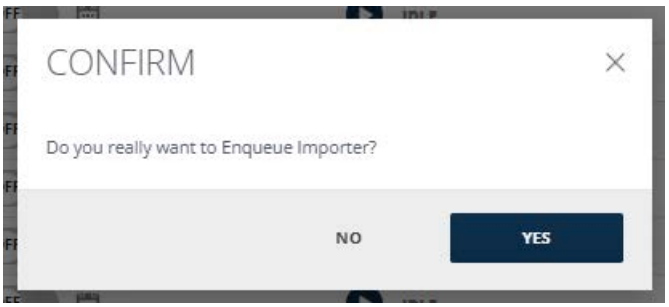
Monitoring Job Executions

Each job execution contains the following information:

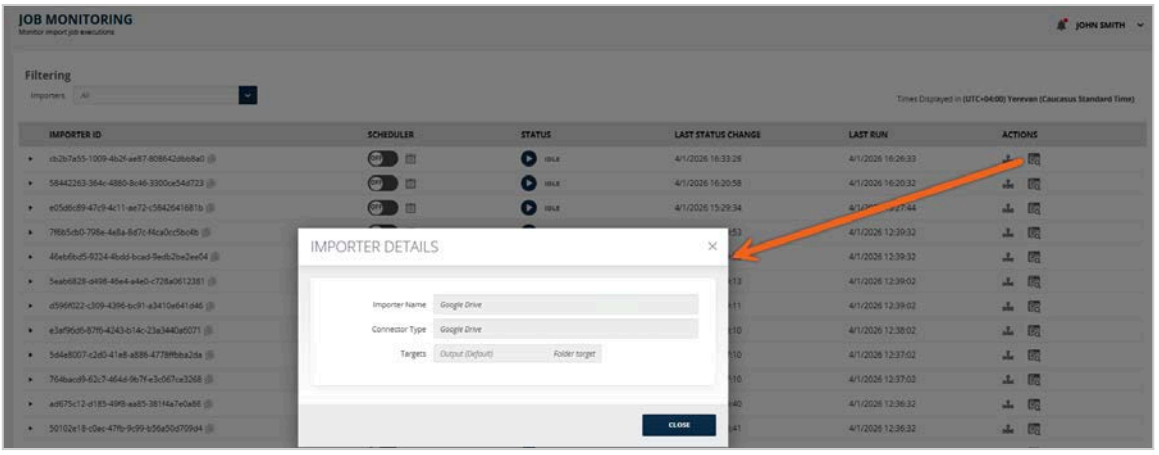
- **Importer ID:** Displays the unique identifier for the importer. Use the copy button to easily copy the ID when needed.
- **Scheduler:**
    - **Status On/Off:** Displays whether the scheduler is turned *On* or *Off*. In addition to monitoring job execution statuses, this setting allows jobs to be scheduled or unscheduled. When toggled, a confirmation pop-up will appear to confirm scheduling or unscheduling of the importer.
      For more information on the Scheduler action button, see **Running an Importer**.



    - **See Schedule Info:** Displays a preview of the Import Job Schedule when the calendar icon is clicked.
- **Status:** Indicates the current state of a job - *Idle*, *Queued*, *Running*, or *Stopping*. This field is used to monitor job execution. Additionally, jobs can be enqueued or cancelled as needed. Changing the job status triggers a pop-up window for confirmation of the enqueueing or cancellation.
  For more information on the start import button, see **Running an Importer**.



- **Last Status Change:** Displays the date and time when the job's status was last updated.
- **Last Run:** Shows the date and time of the job's most recent execution.
- **Actions:**
    - **Change Agent Pool:** Allows the user to modify the assigned Agent Pool for a specific Import Job. For more details, see **Changing an Agent Pool**.
    - **Importer Details:** Displays the following importer information when clicking the button:
        - **Importer name**
        - **Collector type**
        - **Targets**
        - **Filters**



Click the *arrow* button left to the Importer ID to see the following additional information:

Executions

The **Executions** tab represents the historical and operational metadata of each job execution.

- **Status:** Displays the current job status. Possible values include *Pending*, *SentToAgent*, *AgentAccepted*, or *Finished*.
- **Start Date:** Shows the date and time when the job was initially triggered.
- **Last Heartbeat Date:** Indicates the date and time of the agent's latest heartbeat signal.
- **Duration:** Displays the total runtime duration of the job execution.
- **Result:** Displays the job completion outcome and an associated error message for each execution, if applicable:
    - A *green success icon* indicates the job completed successfully.
    - An *amber warning icon* highlights the presence of warnings that may require attention.

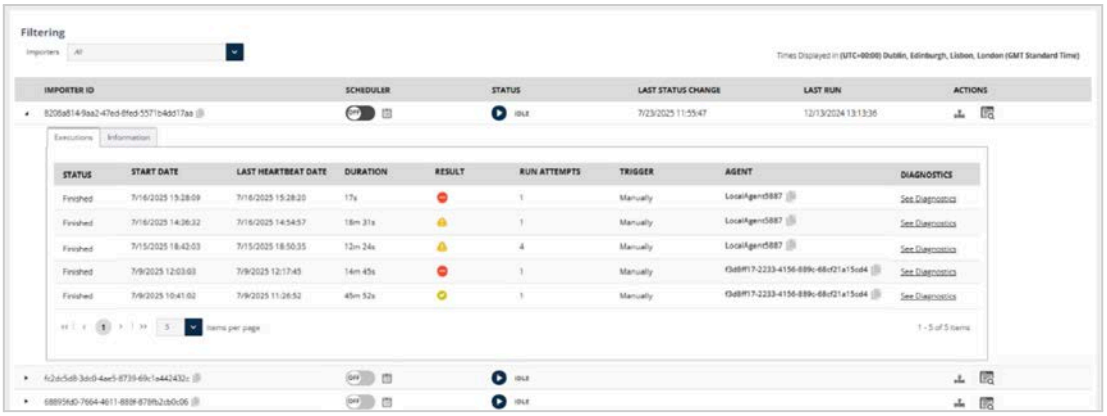
- A *red error icon* signifies that the job finished with errors or failures.
- A *red stop icon indicates* the job was manually stopped by the user.

> **Tip**
>
> Hovering over the icons reveals additional information.

- **Run Attempts:** Indicates how many times the job has been attempted.
- **Trigger:** Specifies how the job was initiated - either Manually by a user or via the Scheduler.
- **Agent:** Displays the Agent name if available; otherwise, shows the Agent ID.

> **Tip**
>
> When copying this value, the Agent ID will be copied - even if an Agent name is displayed.

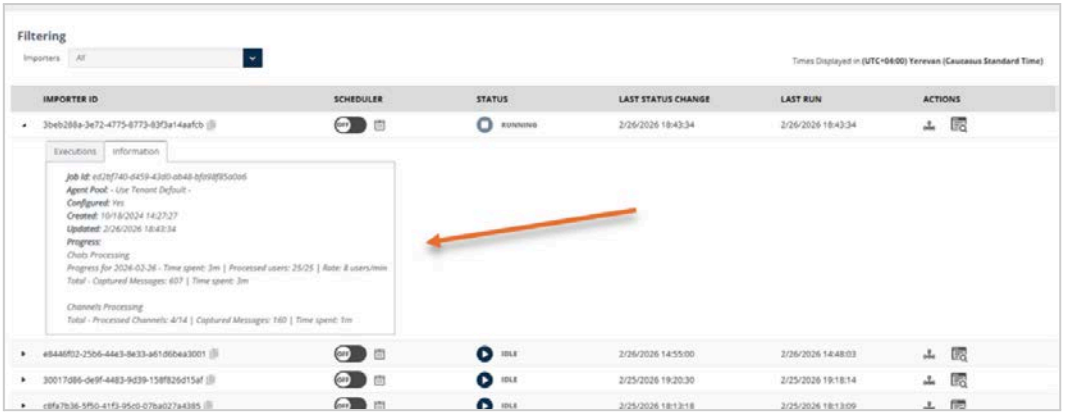
- **Diagnostics:** Provides system-level diagnostic data related to the job. For additional insights, see **Viewing Diagnostic Data**.



Information

The **Information** tab represents the real-time progress of the ongoing job execution.

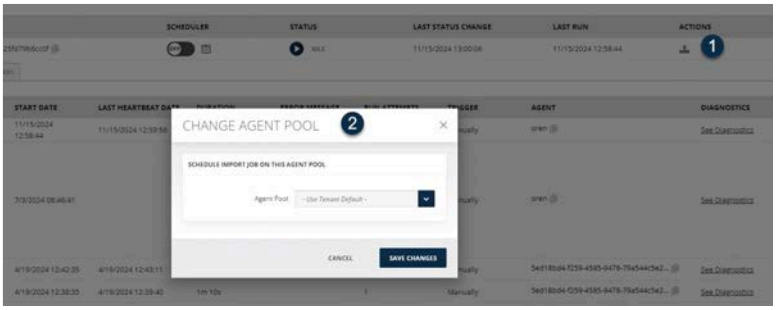
- **Job ID:** Displays the unique identifier assigned to the job.
- **Agent Pool:** Displays the Agent Pool from which the assigned agent originates.
- **Configured:** Displays whether the importer has been successfully configured.
- **Created:** Displays the date and time when the job was created.
- **Updated:** Displays the date and time when the job was last updated.
- **Progress:** Displays the job's progress (if progress tracking is supported).



Changing an Agent Pool

To change the assigned Agent pool for each Import job:

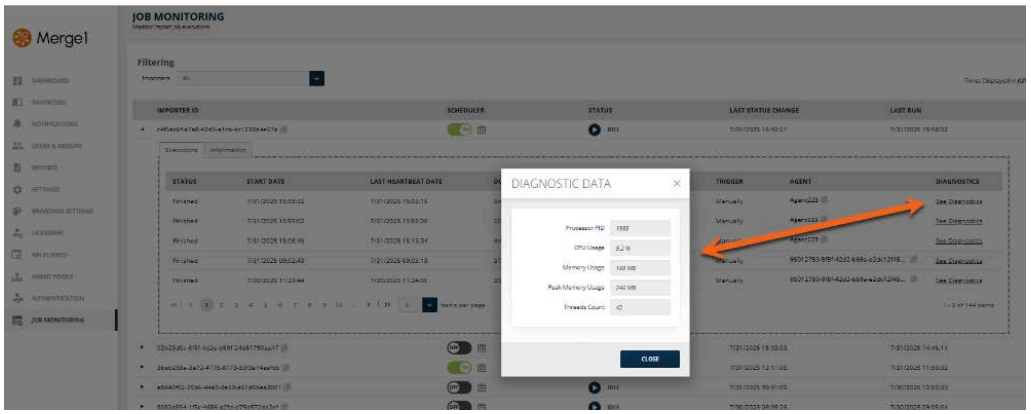
1. Click the **change agent pool** button for an importer and select a new Agent pool from the **Agent Pool** drop-down list on the opened pop-up window.
2. Click **Save Changes**.



Viewing Diagnostic Data

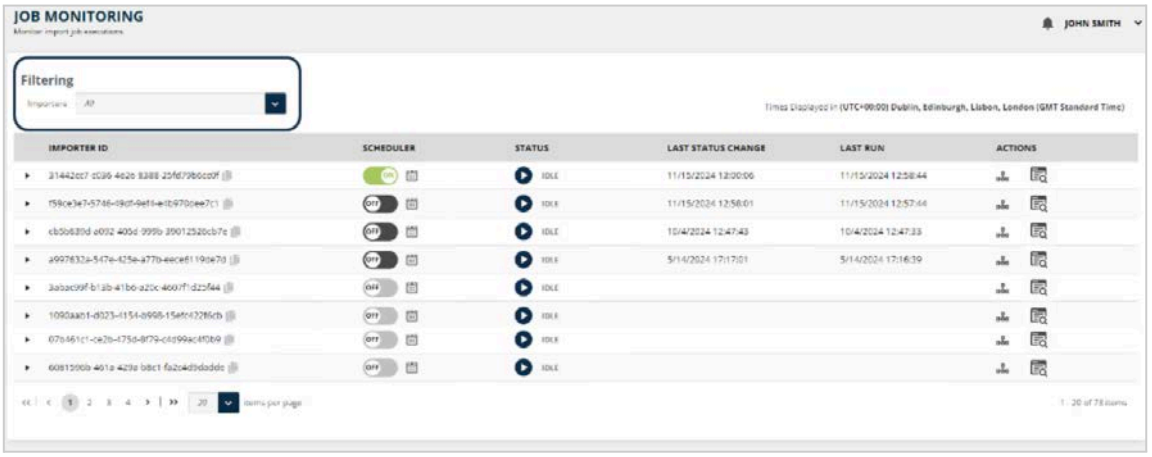
To see the diagnostic report, click **See Diagnostics**, and a pop-up will open with the following information:

- Processor PID
- CPU Usage
- Memory Usage
- Peak Memory Usage
- Threads Count

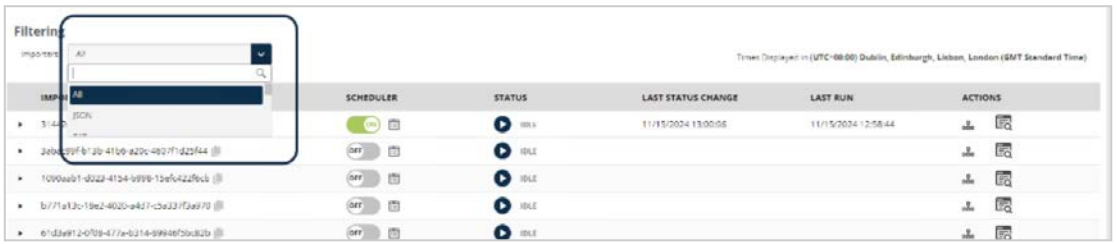


Filtering Importer Jobs

The **Filtering** option allows filtering out the list of records from the sub-section.



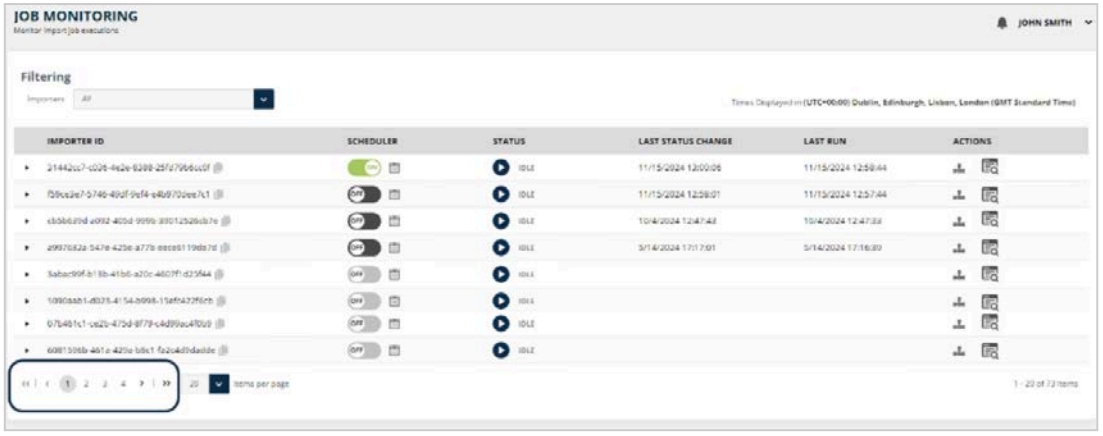
You can also search for a specific job by typing the ID or the name of the importer.



By selecting the importer from the drop-down list, only the importer with its job executions will be displayed.

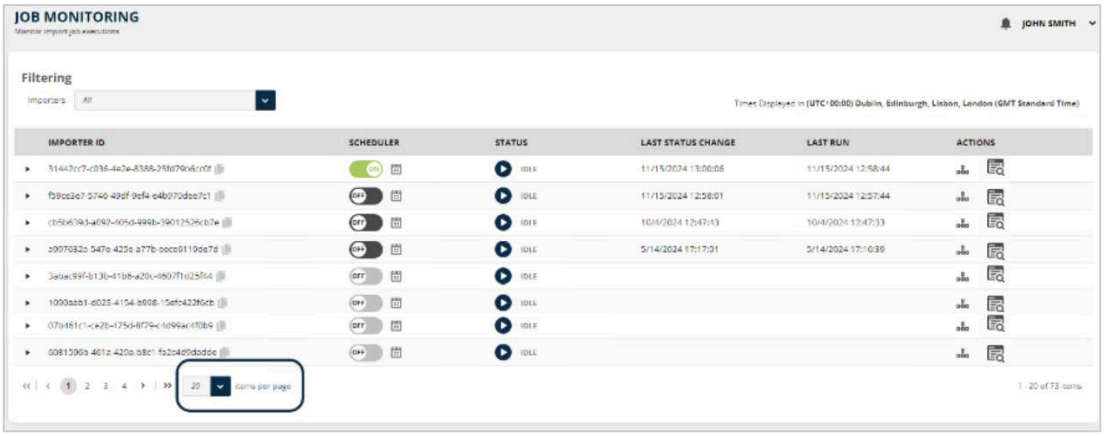
Browsing Importer Jobs

This sub-section has 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.



Setting the Number of Entries per Page

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.



CHAPTER 15

Appendix

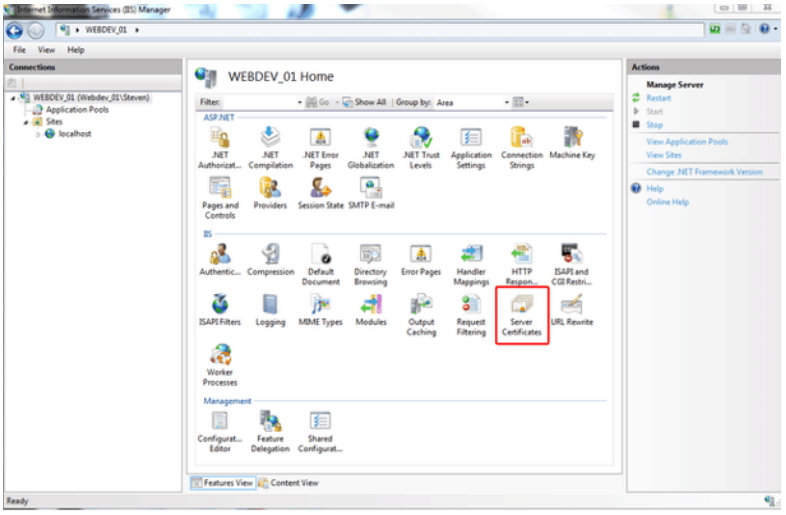
This chapter represents:

- Creating a Certificate (Private and Public Keys)
- References

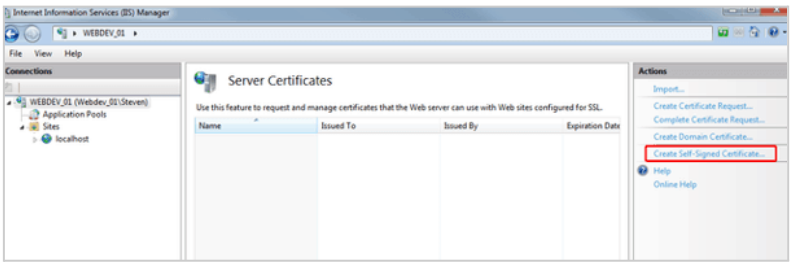
Creating a Certificate (Private and Public Keys)

For private key:

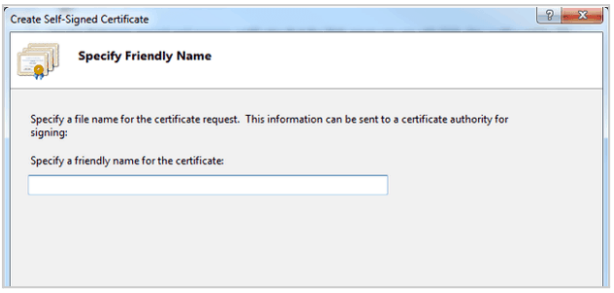
1. Go to the **Start menu & click Administrative Tools > Internet Information Services (IIS) Manager**.
2. Click the server's name in the **Connections** column on the left and double-click **Server Certificates.**



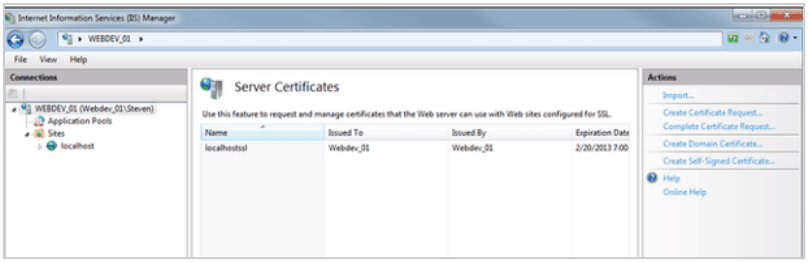
3. Click **Create Self-Signed Certificate** in the **Actions** column on the right.



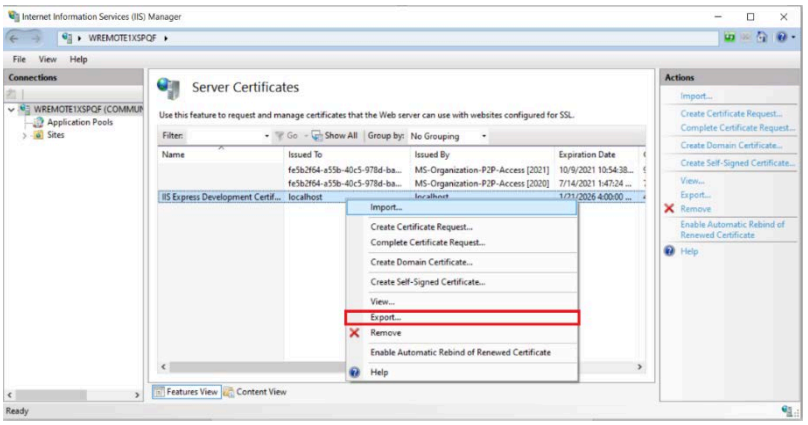
4. Type any meaningful name and then click **OK** to proceed.



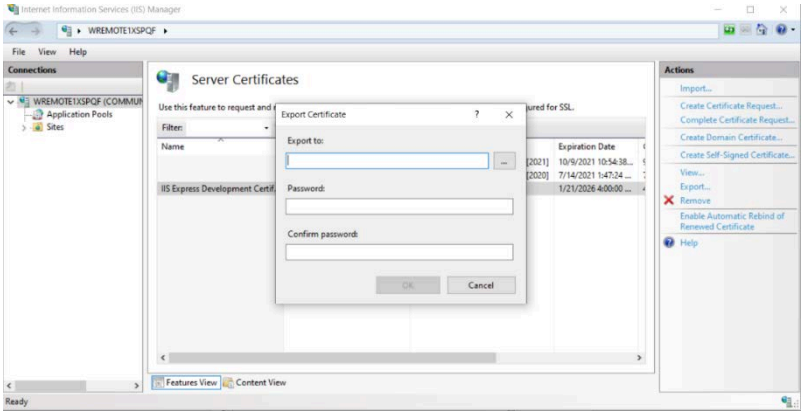
5. Click **OK**. Once that is complete, you should now see the SSL in the list of Self-Signed certificates. Now, you have IIS Self-Signed Certificate with 1 year validation.



6. Right-click on that certificate and click **Export**.



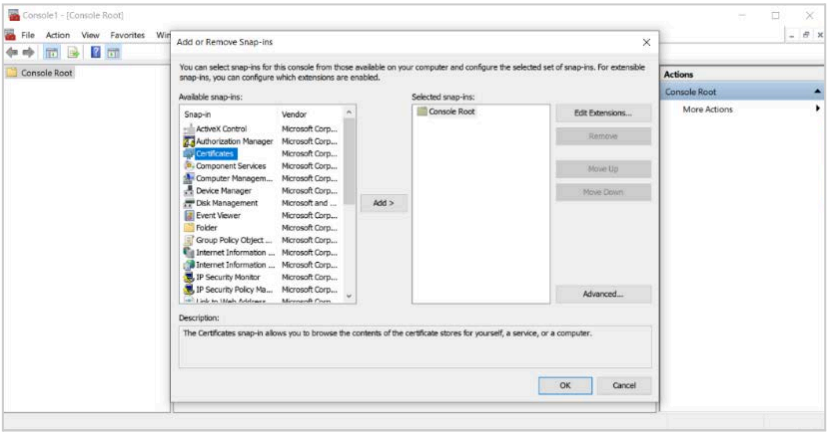
7. Specify the path, type the password, confirm the password, and click **OK**. Now, you have exported the Private key.



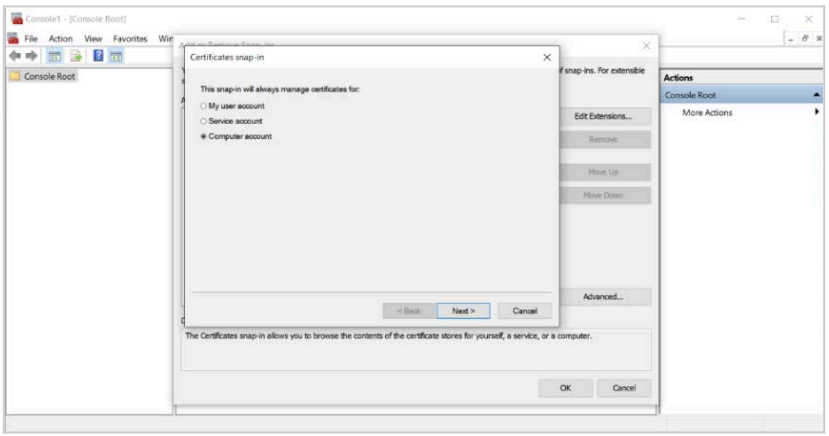
For private key:

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.

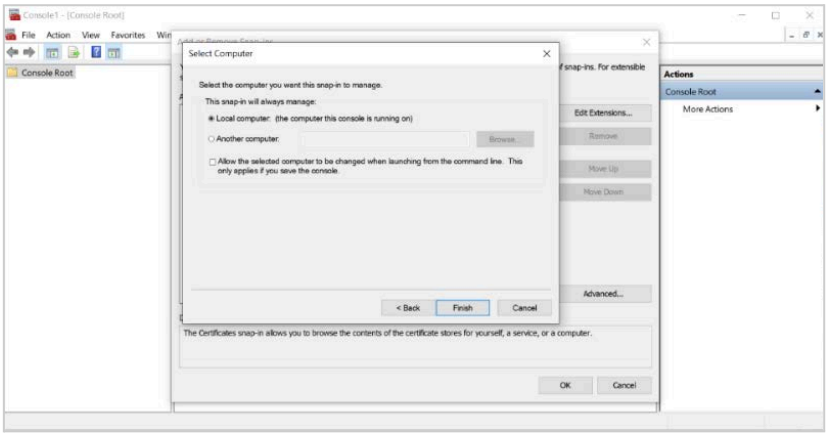
3. Click **Certificates** in the list of **Available snap-ins** and then click **Add**.



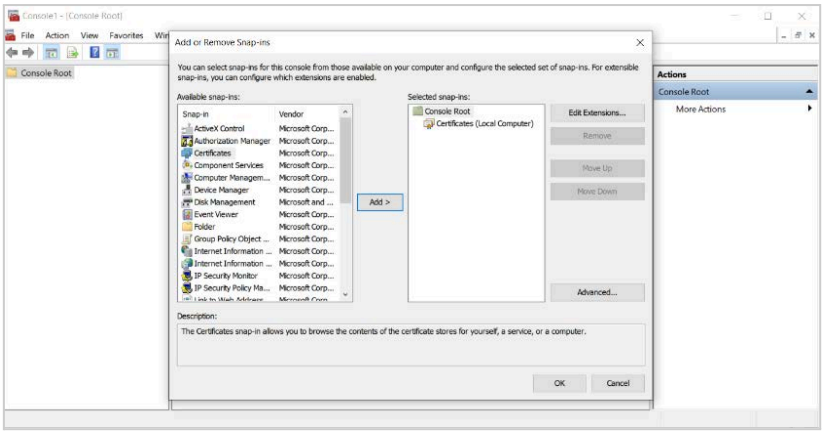
4. Select **Computer** account and click **Next**.



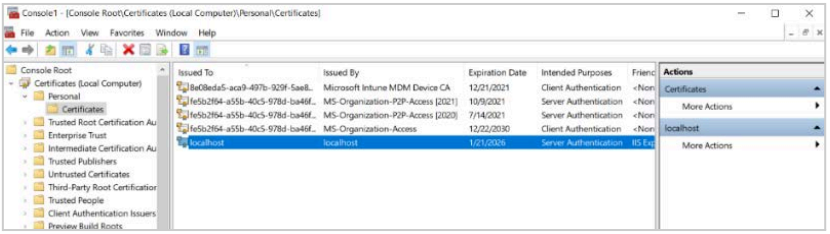
5. Choose **Local Computer** and click **Finish**.



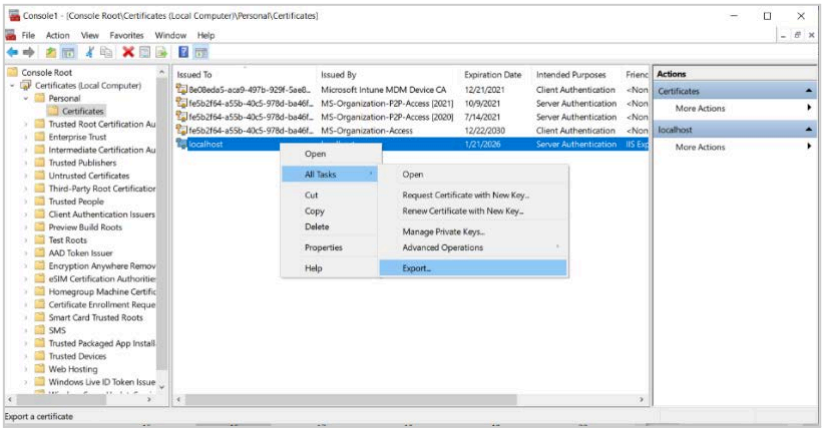
6. Click **OK** to add the certificate snap-in and get back to console.



7. Expand the **Personal** folder in the left-side menu and choose **Certificates**.

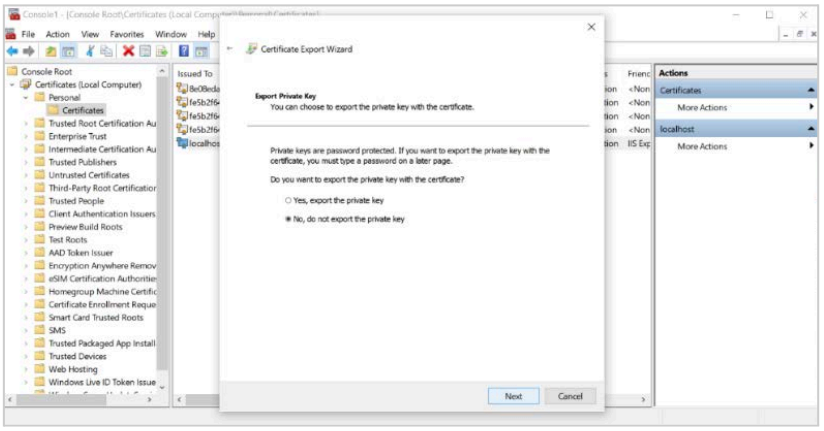


8. Right-click the certificate you want to export - **All Tasks** > **Export**.

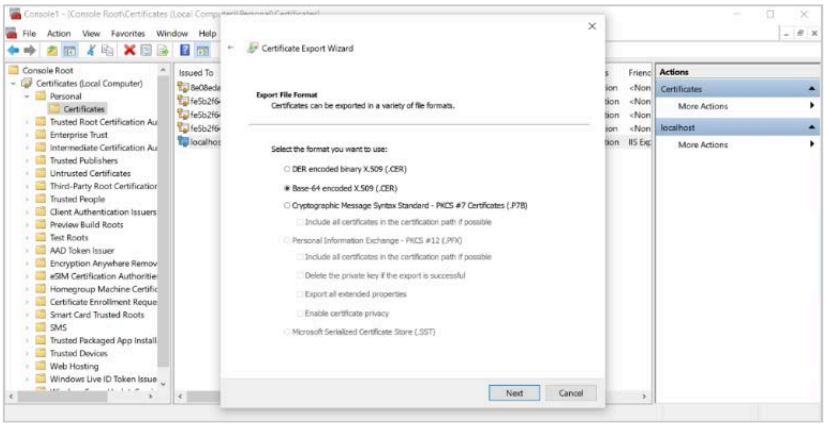


9. On the prompt menu, click **Next**.

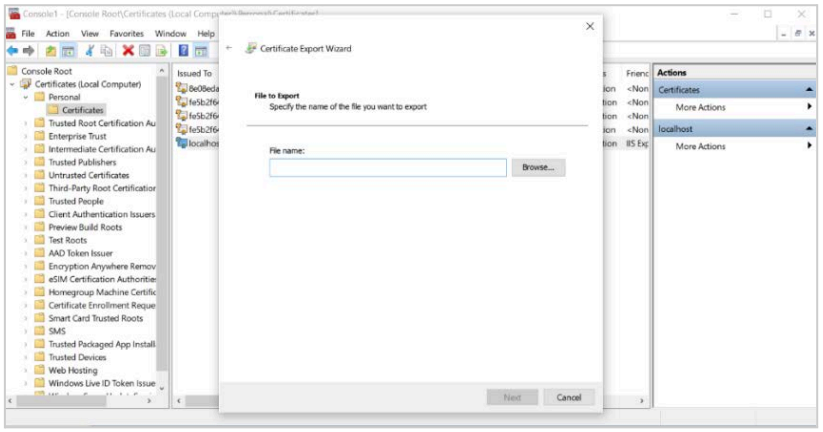
10. Click **No**. Do not export the private key!



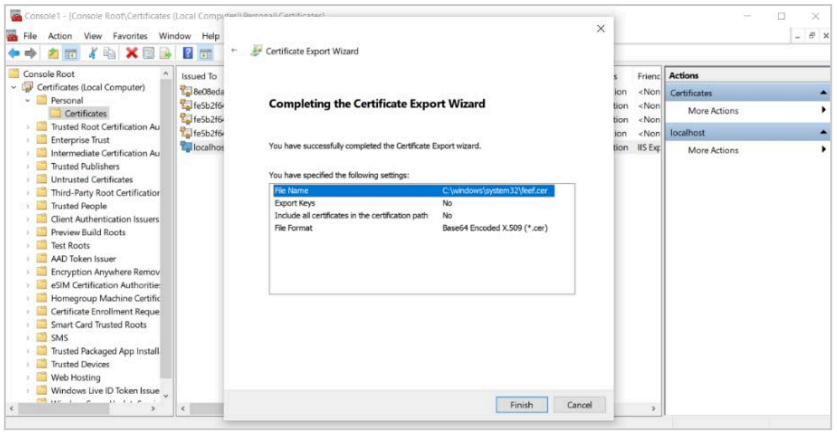
11. Choose **Base-64 encoded X.509 (.CER)** and click **Next**.



12. Fill in the file path and click **Next**.



13. Click **Finish** and now you have the **Public key**.



Note

CNG certificates are not supported.

References

Please, refer to the following related documents to obtain more information about the system and how it functions, which can be found in the Documents folder of the downloaded Merge1 7.0 file:

- Microsoft SQL Always Encrypted Configuration Guide
- Installation Instructions
- Working in the Globanet Portal