VERITAS™

Third-Party Connectors

Webex Teams

User Guide

MERGE1

LEGAL NOTICE

Veritas Technologies LLC
2625 Augustine Dr
Santa Clara, CA 95054
http://www.veritas.com

CONTENTS

CHAPTER 1

Introduction

This chapter represents:

- Overview
- Pre-Requisites
- Accessing the Data Connectors

Overview

Microsoft 365 lets administrators import and archive third-party data from social media platforms, instant messaging platforms, and document collaboration platforms, to mailboxes in your Microsoft 365 organization.

Pre-Requisites

Many of the implementation steps, required to archive Webex Teams data are external to Microsoft 365 and must be completed before you can create the connector in the compliance center.

- Create a Merge1 account by accepting their terms and conditions for Webex Teams connector. Here you will need to contact Veritas Customer Support. You will sign into this account when you create the connector.
- Create an application at https://developer.webex.com/ to fetch data from Cisco Webex Teams via APIs for Compliance and eDiscovery purposes.

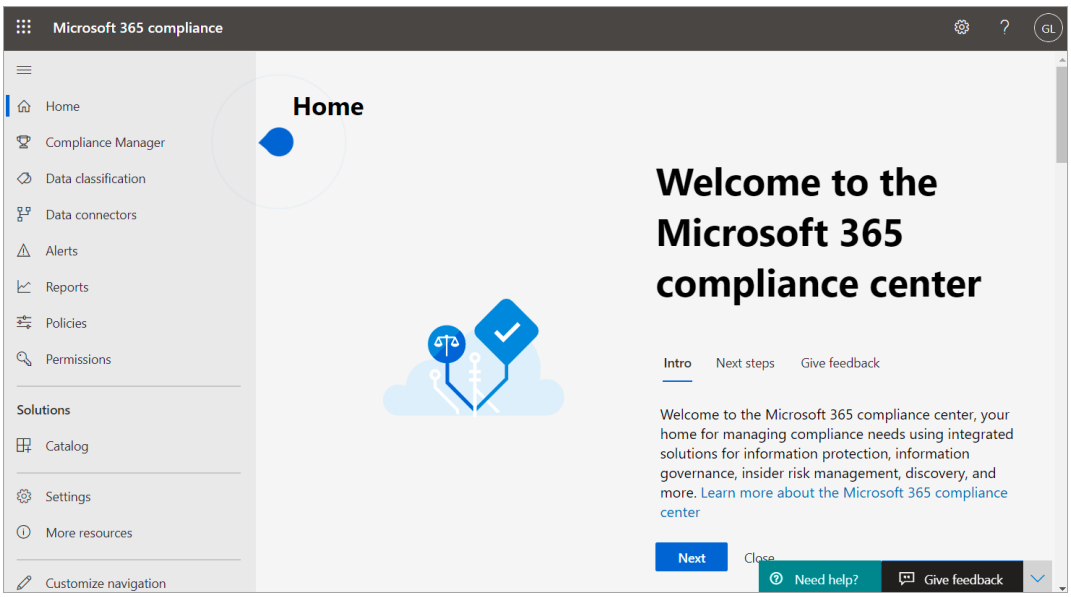
  While creating the application, the Webex Teams platform generates a set of unique credentials. They will be used in the Webex Teams connector configuration wizard in Step 2 on the Microsoft site.

  For step-by-step instructions on how to create the applications, see *Creating a Cisco Webex Teams Application*.
- The user, who creates the Webex Teams connector in Step 1 (and completes it in Step 3) on the Microsoft site, must be assigned to the Mailbox Import Export role in Exchange Online. This role is required to add connectors on the Data connectors page in the Microsoft 365 compliance center. By default, this role is not assigned to a role group in Exchange Online. You can add the Mailbox Import Export role to the Organization Management role group in Exchange Online. Or you can create a role group, assign the Mailbox Import Export role, and then add the appropriate users as members. For more information, see the Create role groups or Modify role groups sections in the article "Manage role groups in Exchange Online".

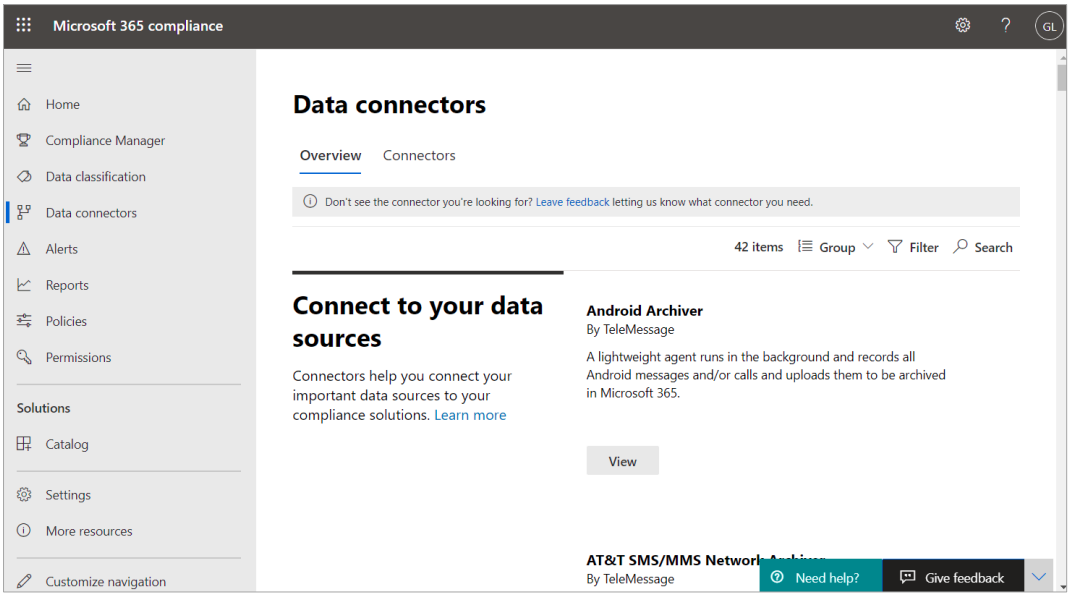
Accessing the Data Connectors

To access the Data Connectors, follow the steps below:

1. Go to https://compliance.microsoft.com web page.

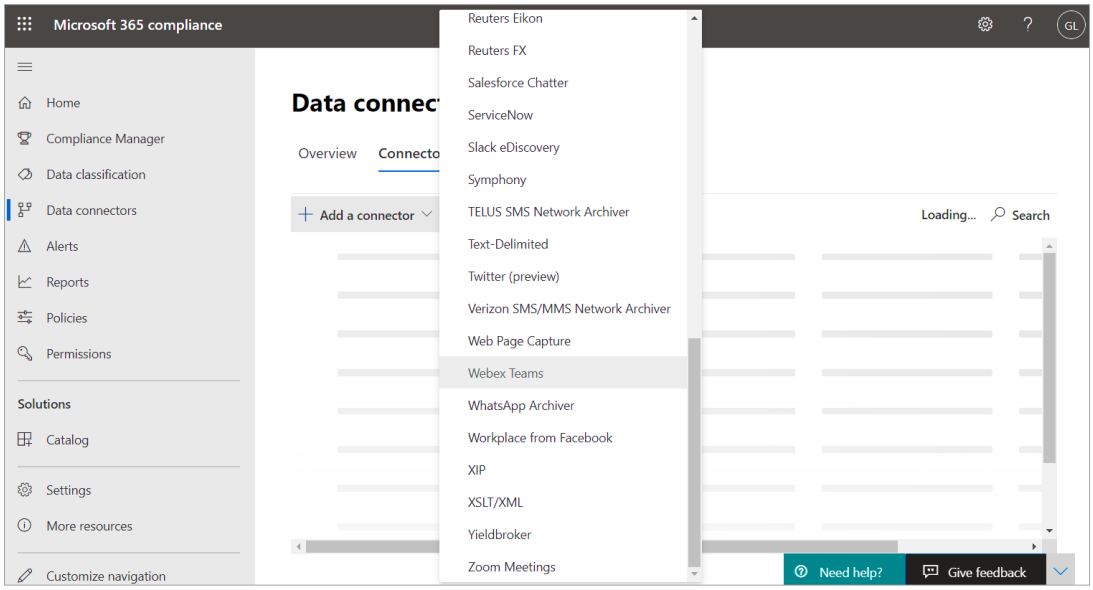


2. Navigate to **Data Connectors**. You will be presented with the **Overview** section of the Data Connectors.



3. Go to the **Connectors** tab.

4. Click the **Add new connector** button. A pop-up list of connectors will open.



5. Select the **Webex Teams** from the list. For more details on how to set up the connector see *SETTING UP WEBEX TEAMS*.

CHAPTER 2

Setting Up Webex Teams

This chapter represents:

- Overview
- Terms of Service
- Connector Name
- Connection to Source

VERITAS

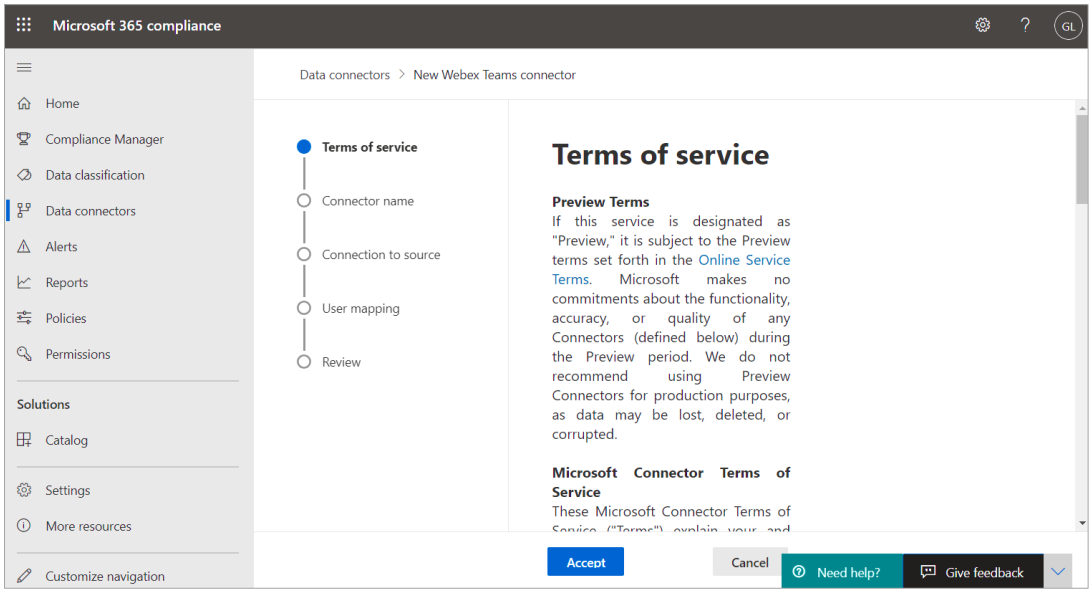
Overview

To set up a new Webex Teams connector, you need to complete the following steps:

- Terms of Service
- Connector Name
- Connection to source
- User Mapping
- Review.

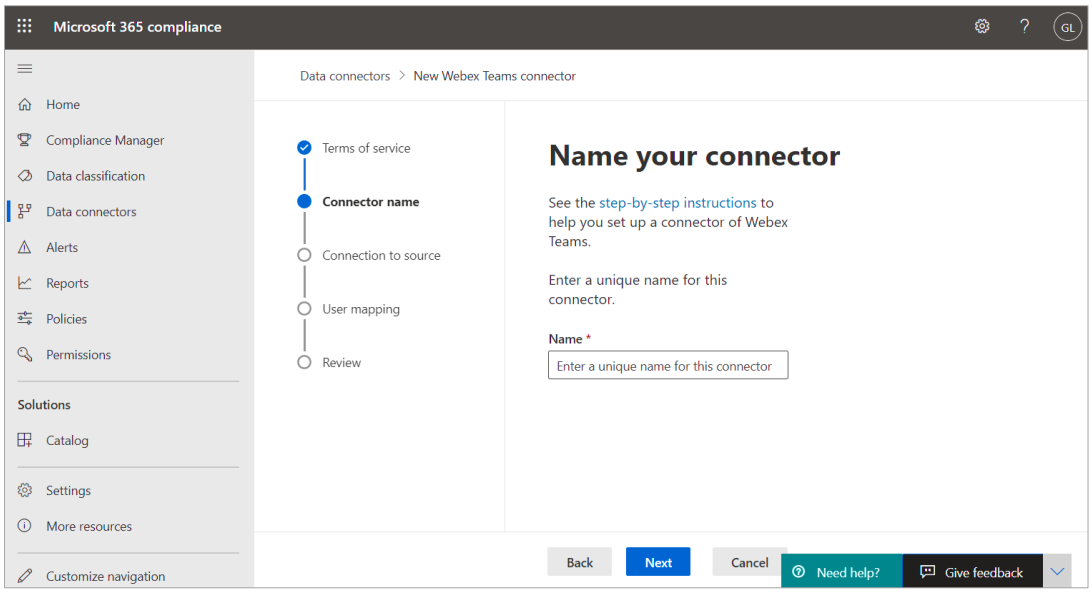
Terms of Service

For terms of service, read the terms carefully and accept them by clicking the **Accept** button.

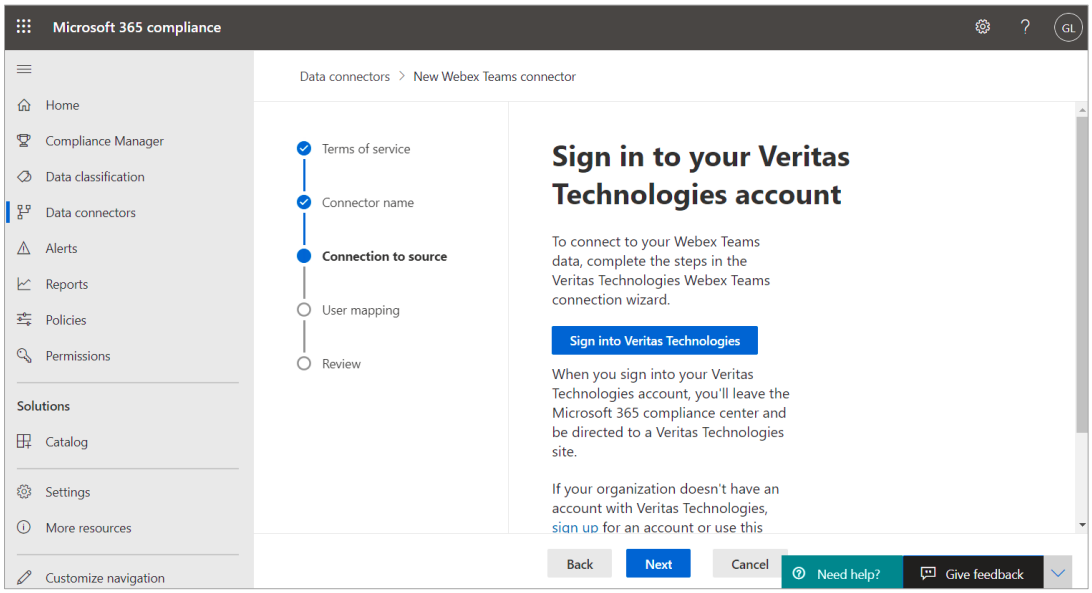


Connector Name

To create a connector, define a unique name that can represent or identify the connector:



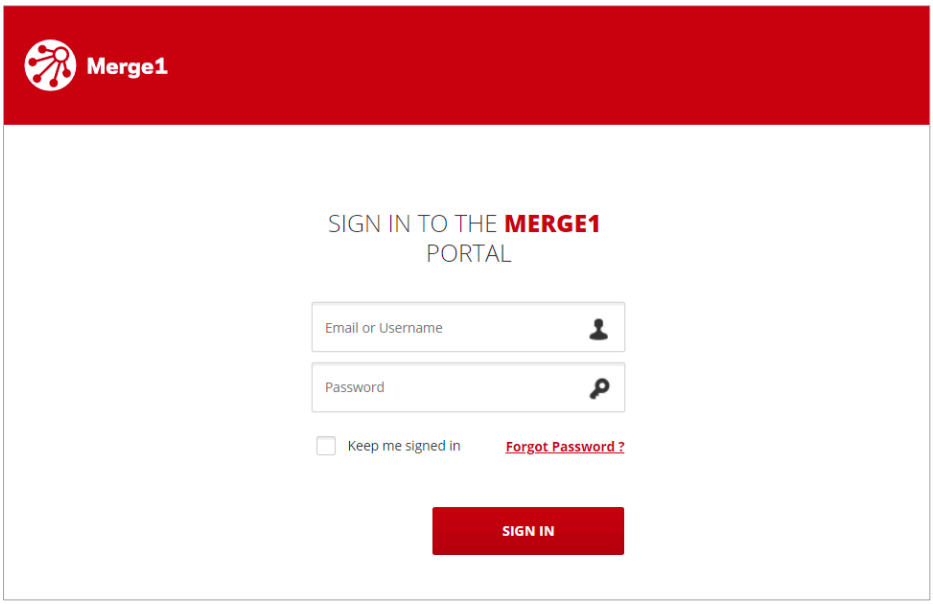
Click **Next**, to be navigated to the **Sign in to your Veritas Technologies account** page.



By clicking **Next**, you will be redirected to the Veritas Merge1 site. For more details on how to manage the source connection, see *Connection to Source*.

Connection to Source

Use the Login screen to access Merge1 or retrieve a forgotten password.



Webex Teams uses a role-based access control model to ensure the security of the data stored in the system. Only users with the appropriate access rights will be able to enter the system, access specific data, and perform certain activities.

Signing In

To sign in to Merge1 provide the following credentials:

- Email and Username
- Password.

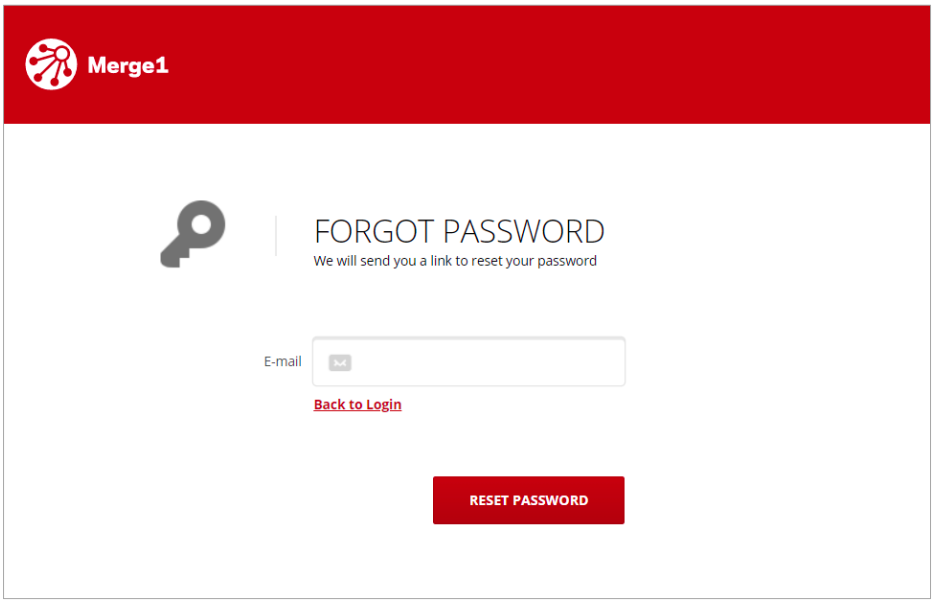
Password Recovery

The system is designed to provide the functionality of retrieving user password in case of forgetting or for some other reason. Passwords are retrieved through the identification link sent to the user's email address contained in the user profile. When a user clicks the link in the email, user's identity will be verified, and an opportunity for defining new password will be provided.

To recover the password, follow the steps below:

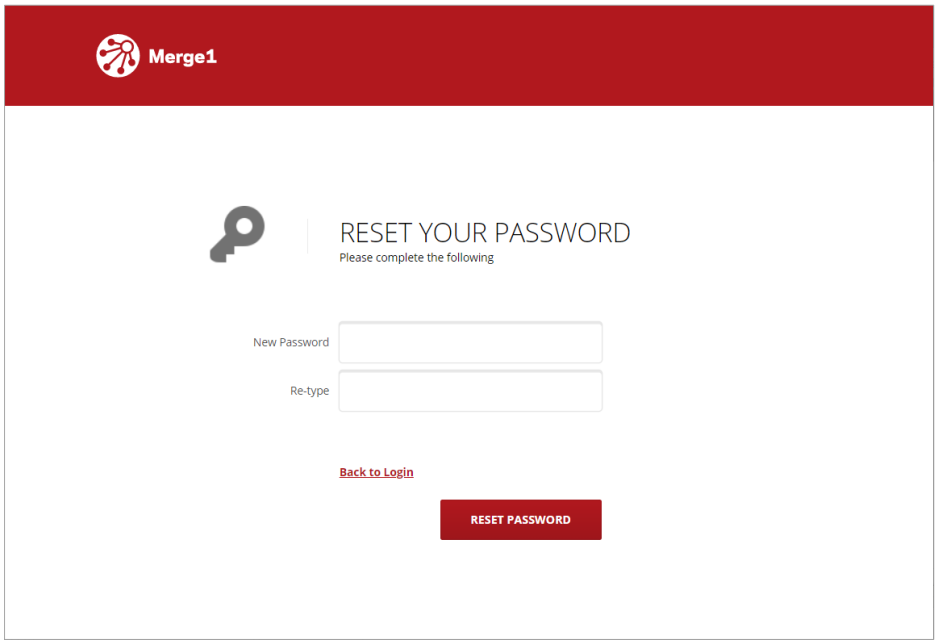
1. Click the **Forgot Password** link in the **Sign in** window.

2. Provide an email associate with the Merge1 account so that the recovery link is sent to this address.



3. Check your email and click the recovery link.

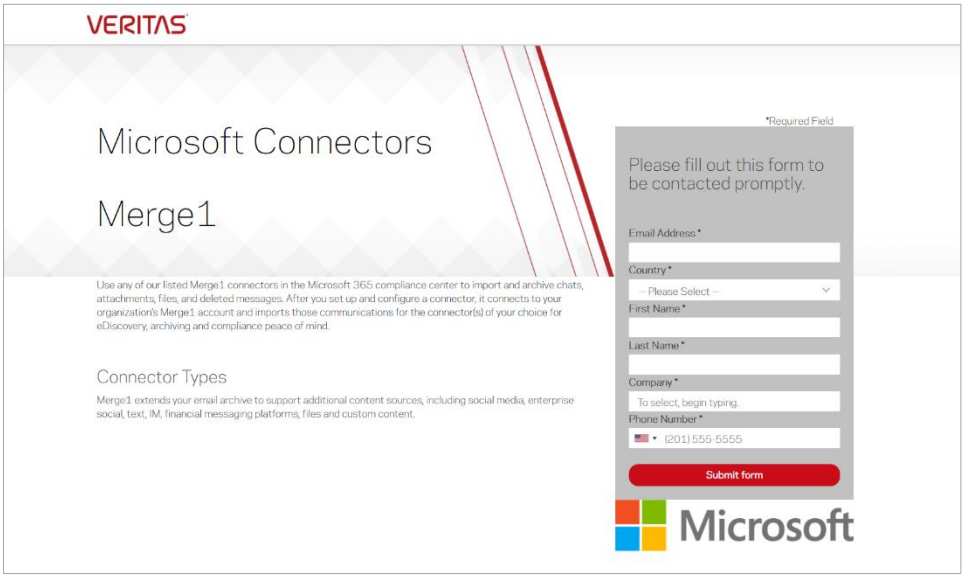
4. Provide a new password and re-enter it for verification.



Creating an Account

If you are new to Merge1 and do not have an account:

1. Request a call from Veritas Technologies by filling out the following information:
   - Email Address
   - Country
   - First Name
   - Last Name
   - Company
   - Phone Number



2. Click **Submit form** and a Veritas Sales Representative will follow up with you by phone or e-mail.

3. After getting approval you can make use of Webex Teams from the Merge1 product.

Now, when you are redirected to the Veritas Merge1 page, you can start configuring the Webex Teams connector. For more details on how to configure the connector, see *CONFIGURING THE WEBEX TEAMS CONNECTOR*.

CHAPTER 3

Configuring the Webex Teams Connector

This chapter represents:

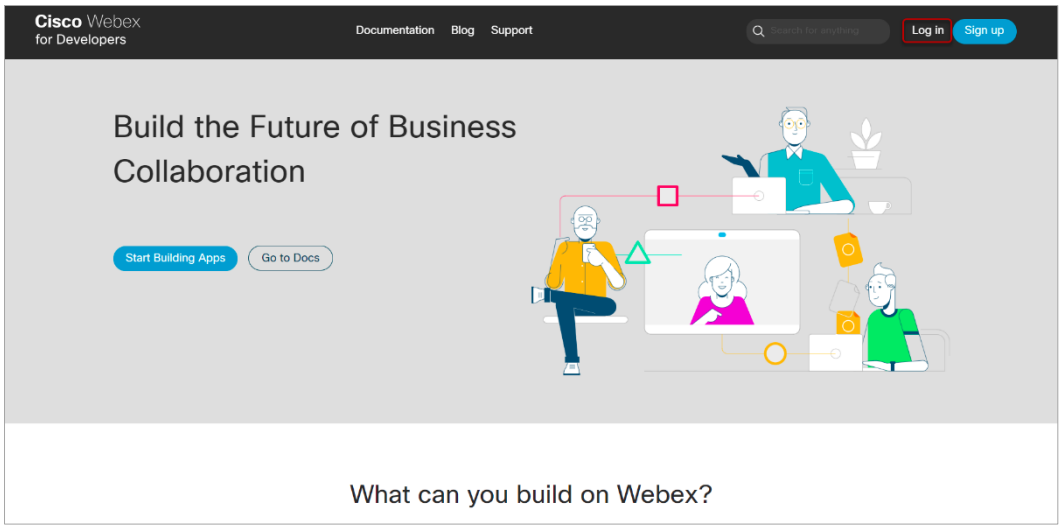
- Creating a Cisco Webex Teams Application
- Configuring the Webex Teams Connector
- Monitored Users
- Targets
- Settings
- User Mapping
- Review

Creating a Cisco Webex Teams Application

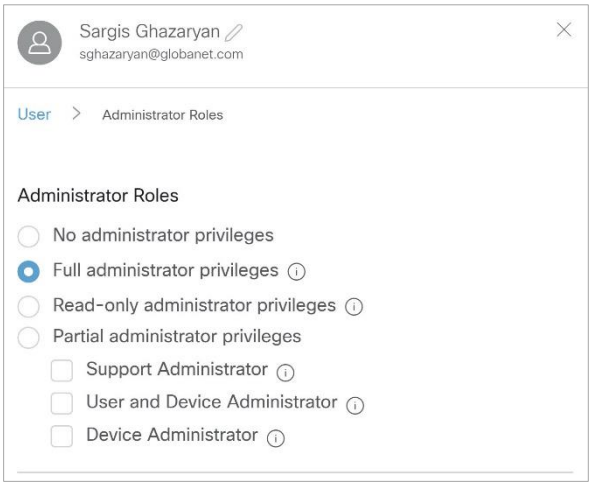
Webex Teams allows third parties to fetch data from its APIs for Compliance and eDiscovery purposes, this is achieved by using Custom Integrations.

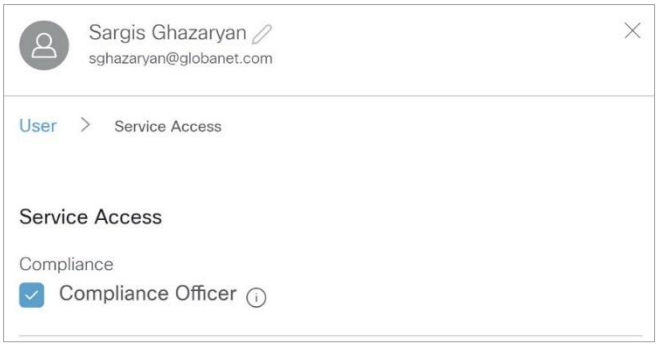
To create an app, follow the steps below:

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

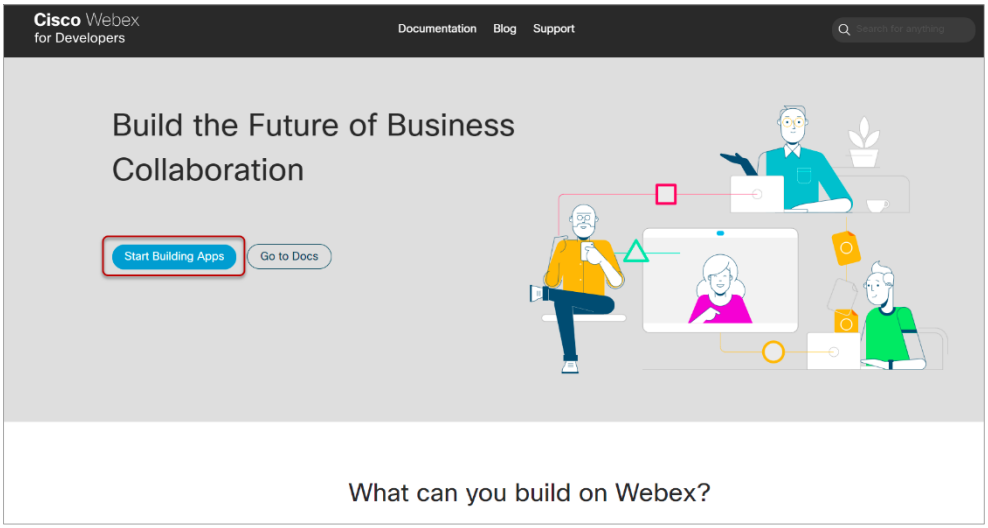


Note that the account should have Full Administrative Privileges and be a Compliance Officer. Permission for full administrator privileges can be checked at https://admin.webe.g.com/users > **Select User > Administrative Roles** and for compliance https://admin.webe.g.com/users > **Select User > Service Access**:

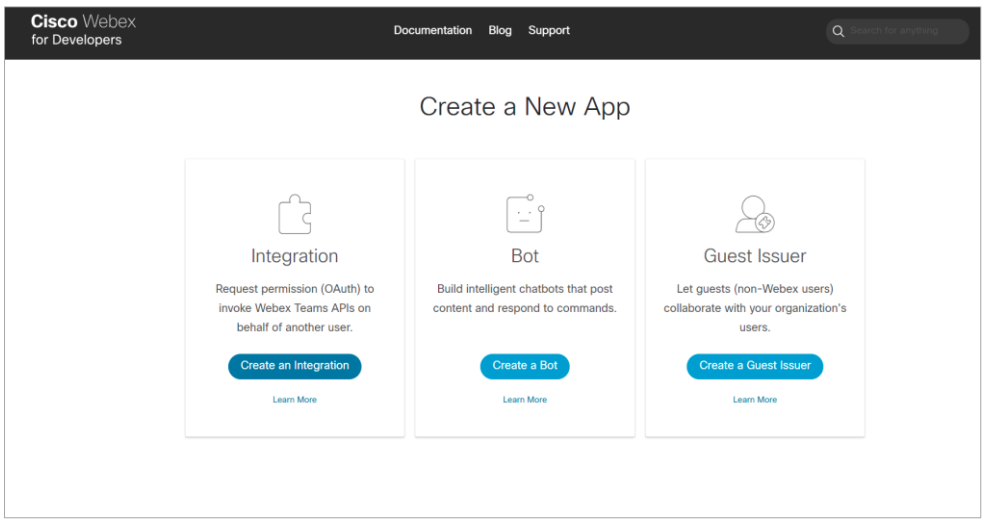




2. When logged in and permissions are set, click **Start Building Apps**.

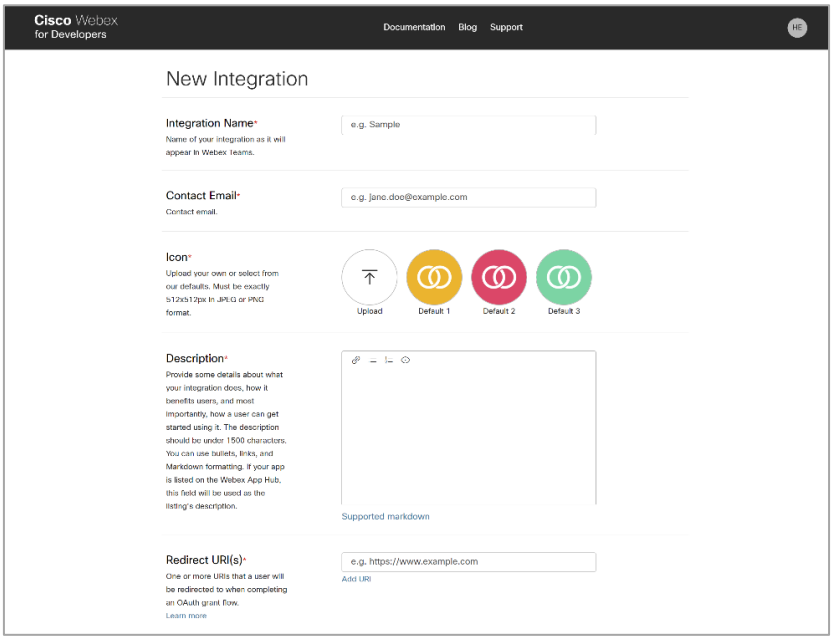


3. Choose **Create an Integration**.

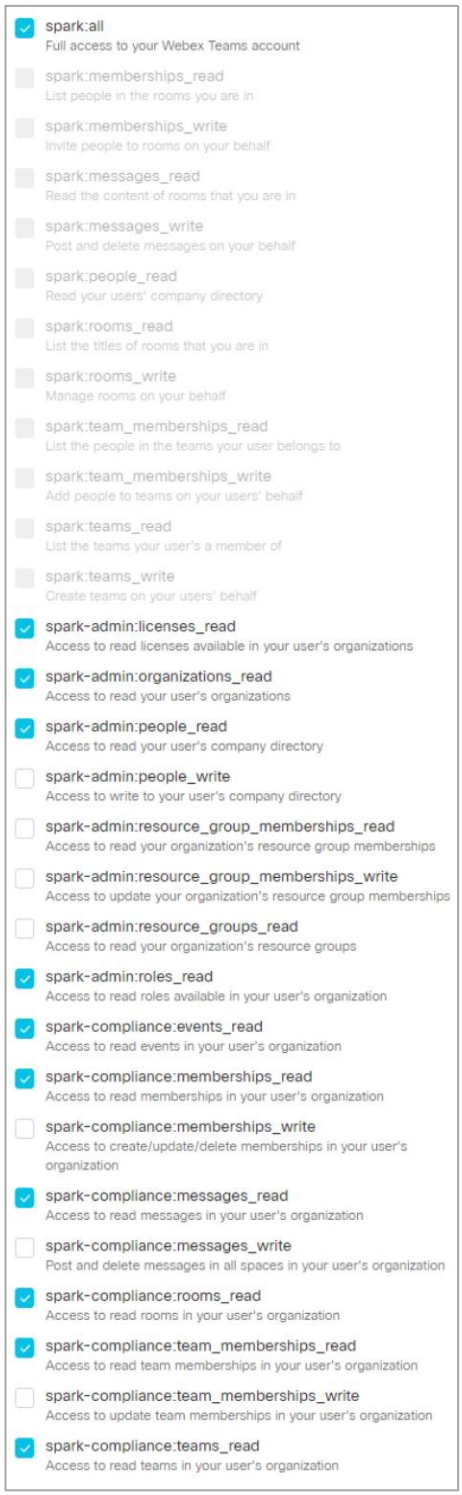


4. Fill in the **Integration Name**, **Contact Email**, **Icon**, **Description fields**.

5. In the Redirect URI(s) field add `https://<your_merge1_domain>/Configuration/OAuthCallback` URL address.



6. Select the following scopes:



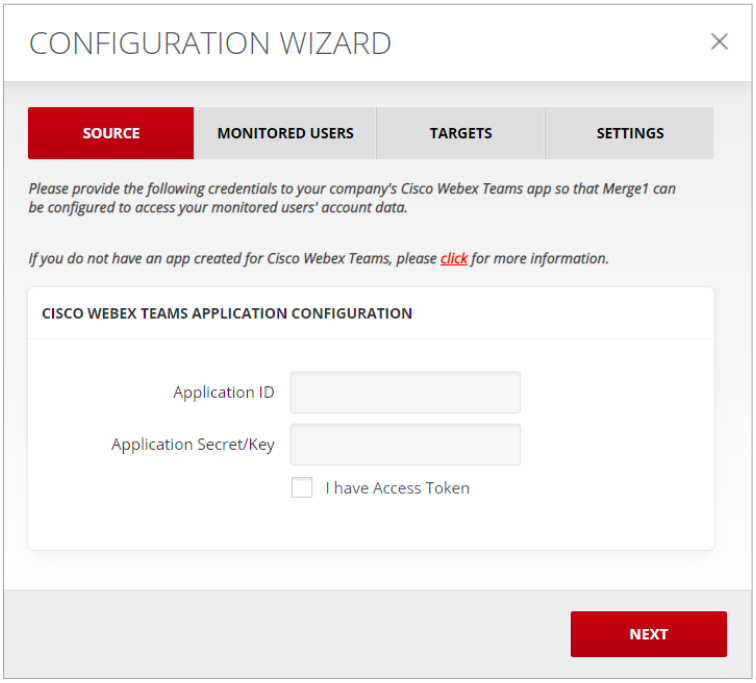
- spark:all
- spark-admin:license_read
- spark-admin:organizations_read
- spark-admin:people_read
- spark-admin:roles_read
- spark-compliance:events_read
- spark-compliance:memberships_read
- spark-compliance:messages_read
- spark-compliance:rooms_readspark-compliance:team_memberships_read
- spark-compliance:teams_read

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

8. Copy the **Client ID** and **Client Secret** and save it in a secure location.

Configuring the Webex Teams Connector

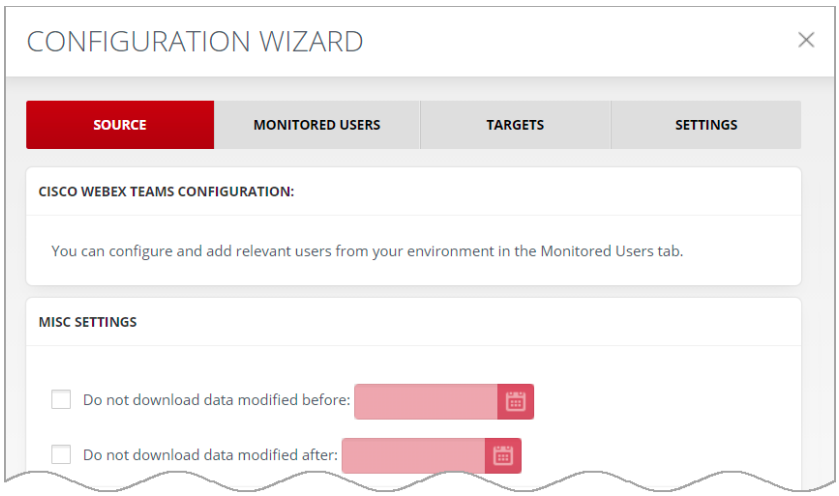
1. Add the **Client ID** into **Application ID** field.
2. Fill in **Application Secret/Key** with the **Client Secret**.
3. Click **Next**.



Miscellaneous Settings

For Misc Settings:

- 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 04/17/2019 and the **after** is set to 03/25/2021 only the data between these two dates will be downloaded. Data outside that timeframe will be ignored. Note that both options can be used independently as well.

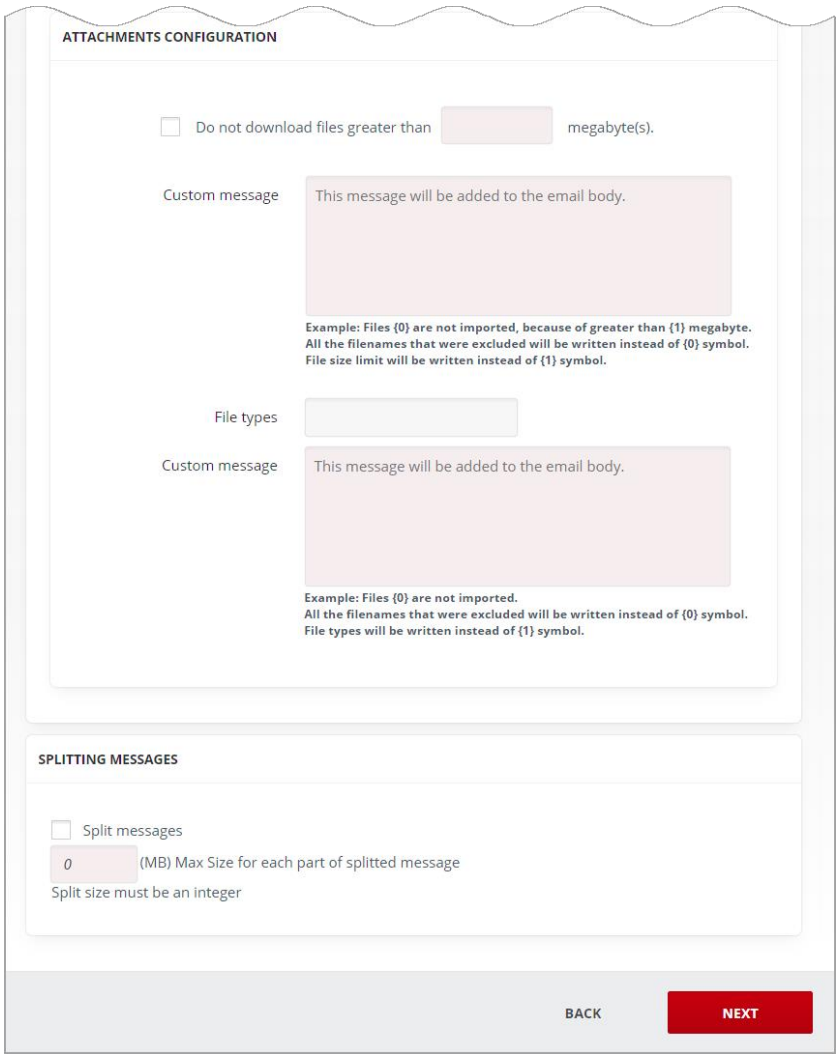


Part 1

Attachments Configuration

For Attachments Configuration:

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



Part 2

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. 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.

Important: 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 Merge1.

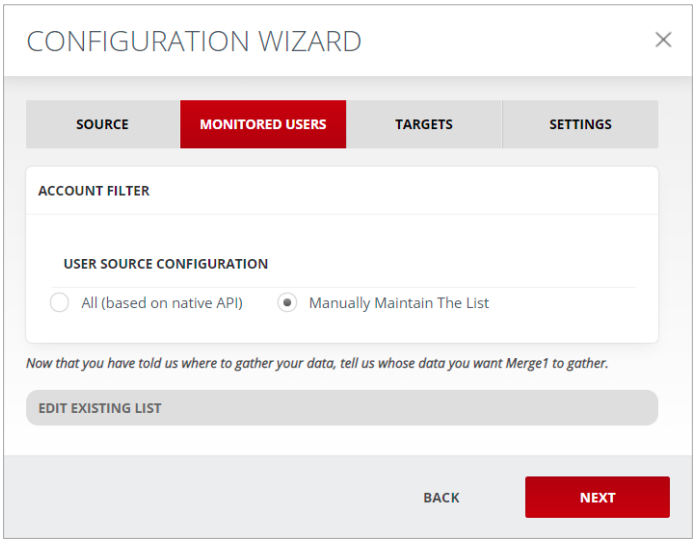
By clicking **Next**, you will be navigated to the *Monitored Users* tab.

Monitored Users

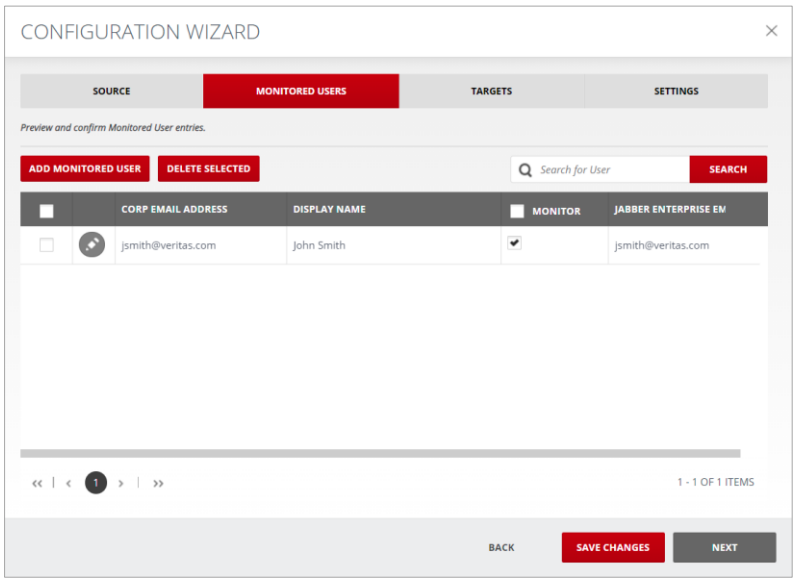
Monitored Users are individuals whose data is collected by Merge1. There are two User Sources from where Monitored Users can be added to the connector.

- **All (Based on Native API)**
- **Manually Maintain the List**

Once **Manually Maintain the List** is selected, the **Edit Existing List** option will appear.



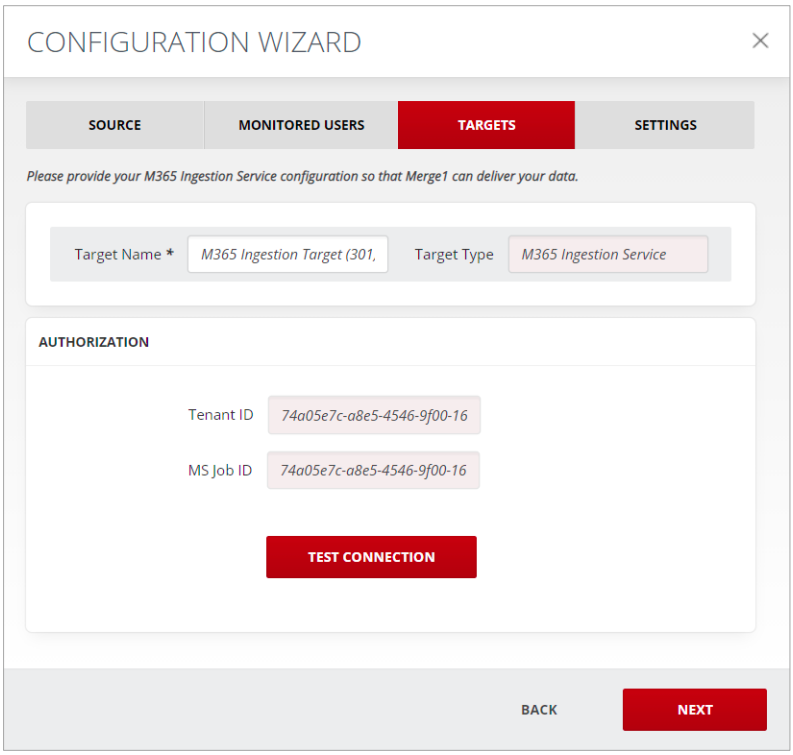
This will allow manually adding and managing users.



By clicking **Next**, you will be navigated to the *Targets* tab of the Configuration Wizard.

Targets

The information required for configuration of the targets is pre-populated on this screen. This information cannot be edited.



By clicking **Next**, you will be navigated to the *Settings* tab.

Settings

The final step for the Importer Configuration Wizard is the Settings. Under this tab you will have the opportunity to configure the following:

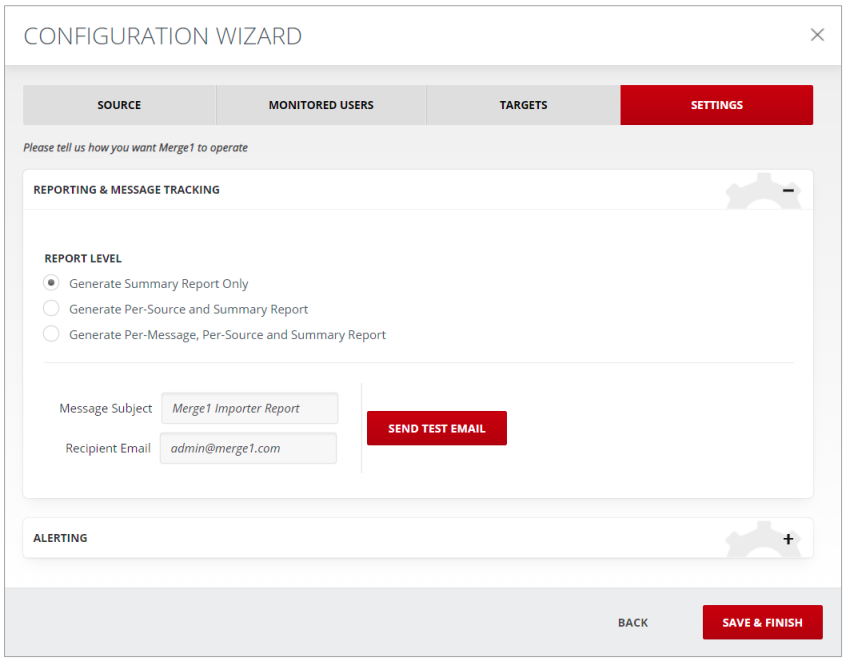
- Reporting & Message Tracking
- Alerting.

Reporting & Message Tracking

The following section of the Settings tab refers to email reports, which may be used to deliver statistical information via email.

1. **Report Level:** In Merge1 you will find three types of Report Level, which set the level of details. You can:
   - **Generate Summary Report Only**. Summary reports include Source Statistics and Message Statistics. Source Statistics includes the number of unprocessed, quarantined, failed, and imported sources. Message Statistics includes the number of unprocessed, failed, successful, excluded, and ignored messages.
   - **Generate Per-Source and Summary Report**. This report type in addition to the Summary Report includes statistics for each source. For each source there is statistics for unprocessed, processed, imported, failed, monitored users (if applicable).
   - **Generate Per-Message, Per-Source and Summary Report**. This report is useful only for file connectors. The per message report in addition to the reports described above is generated only in case a message has failed.

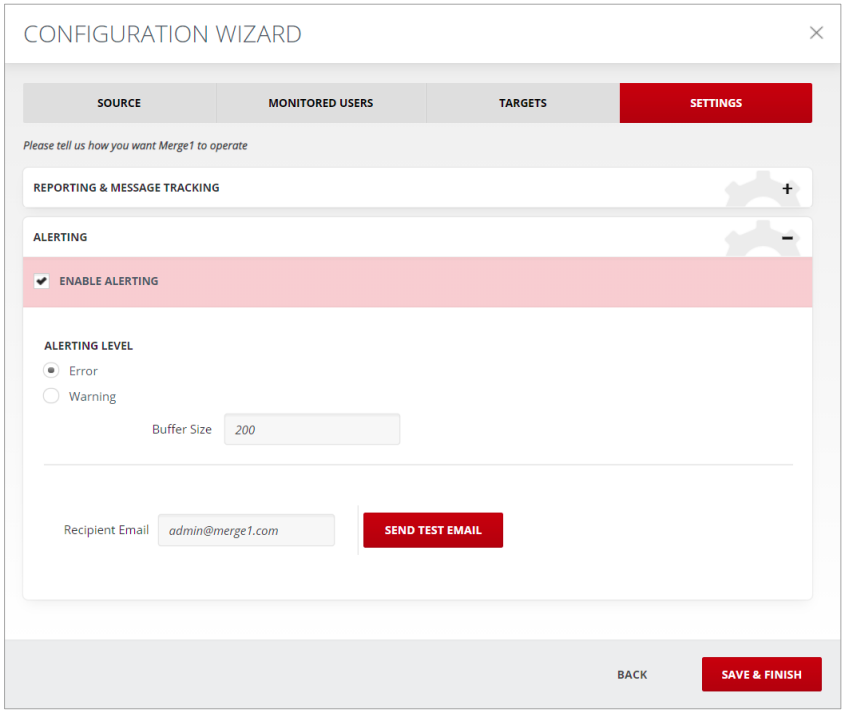
Reports are based on the activities that can be captured from the connectors.



2. **Message Subject:** Enter the subject for the report message.
3. **Recipient Email:** Enter an email address for delivering reports.

Alerting

Merge1 can automatically create an alert in case there are issues during an import process.



When enabled, there are two levels of alerting:

- **Error** - Alert is sent when an Error is registered in the logs.
- **Warning** - Alert is sent when a Warning is registered in the logs.

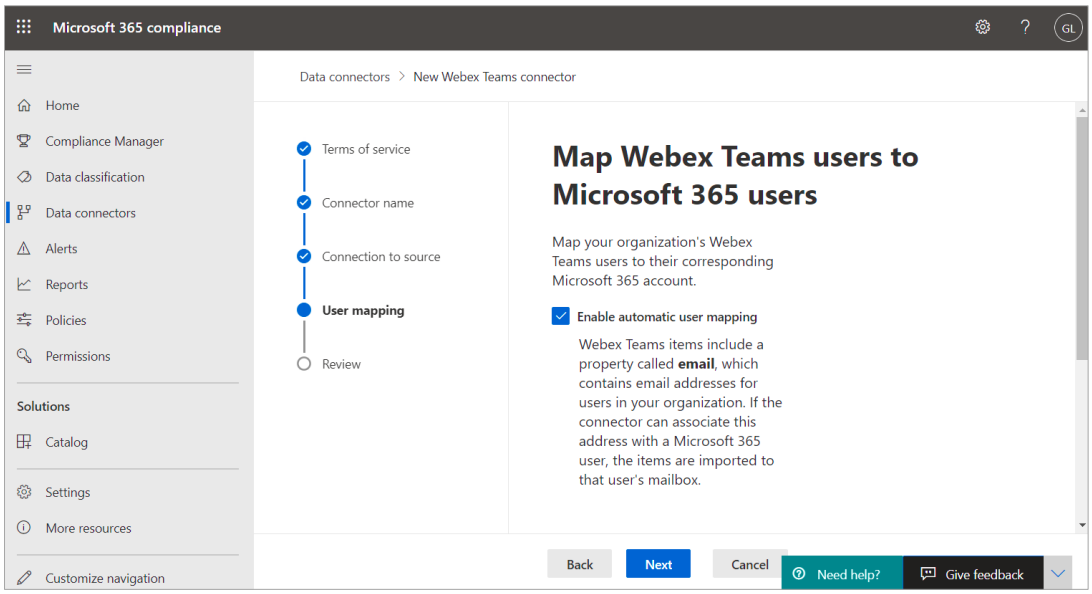
To configure the alerting, specify the **Buffer Size**.

You can also test the connection by entering the **Recipient Email**. Click **Send Test Email**.

By clicking **Save & Finish** you will be navigated to the *User Mapping* section of the M365 Compliance Center.

User Mapping

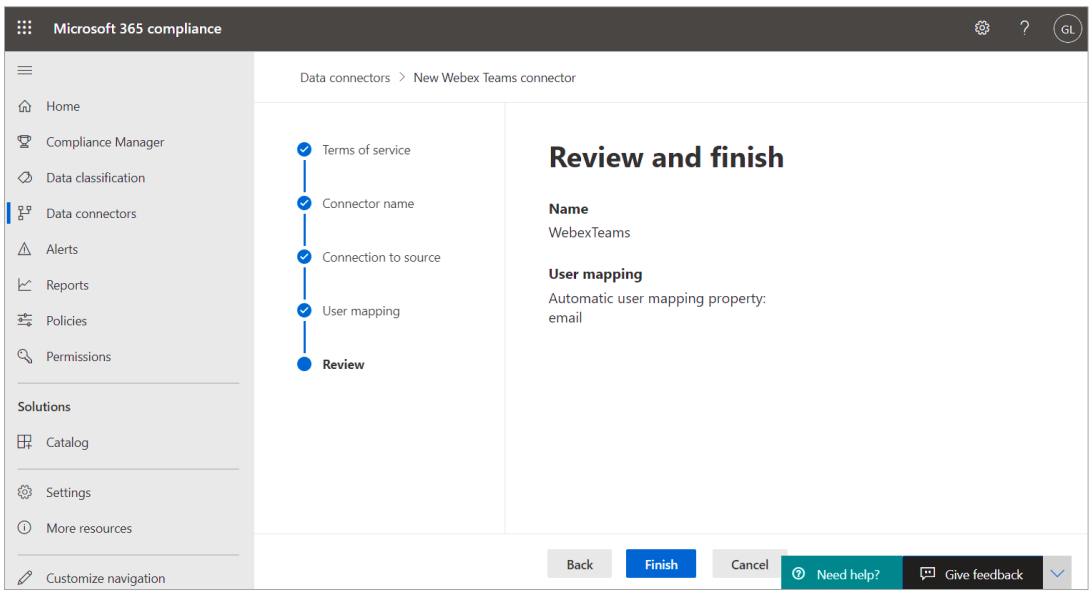
Provide the required user mapping.



By clicking **Next**, you will be navigated to the *Review* section.

Review

Here you can review connector name that you configured and the type of the User Mapping you have selected. Once you have reviewed the accuracy of this information, click the **Finish** button to complete the configuration. Otherwise, click **Back** and make any modifications.



Congratulations! You are all set up!