VERITAS™

Third-Party Connectors

Redtail Speak

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

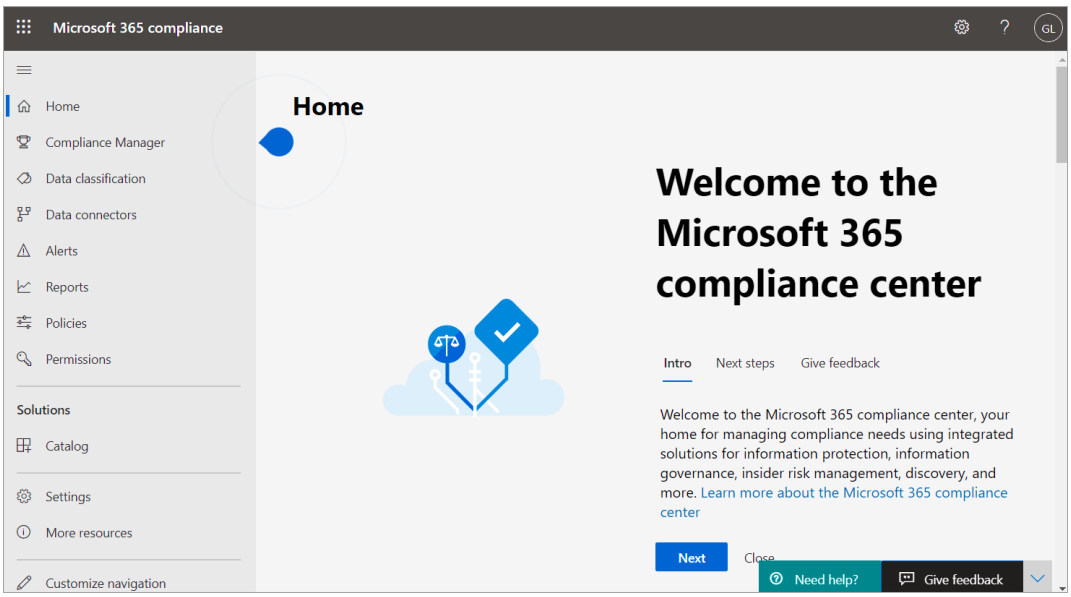
Many of the implementation steps, required to archive Redtail Speak data are external to Microsoft 365 and must be completed before you can create the connector in the compliance center.

- Create a Merge1 account by accepting their terms and conditions for Redtail Speak connector. Here you will need to contact Veritas Customer Support. You will sign into this account when you create the connector.
- The user, who creates the Redtail Speak 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".

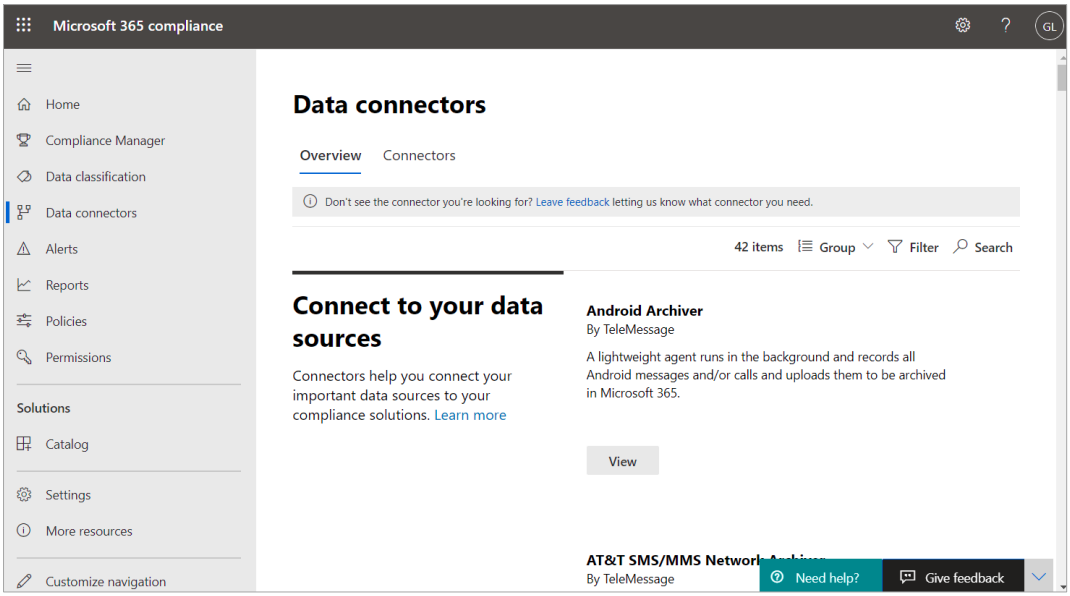
Accessing the Data Connectors

To access the Data Connectors, follow the steps below:

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

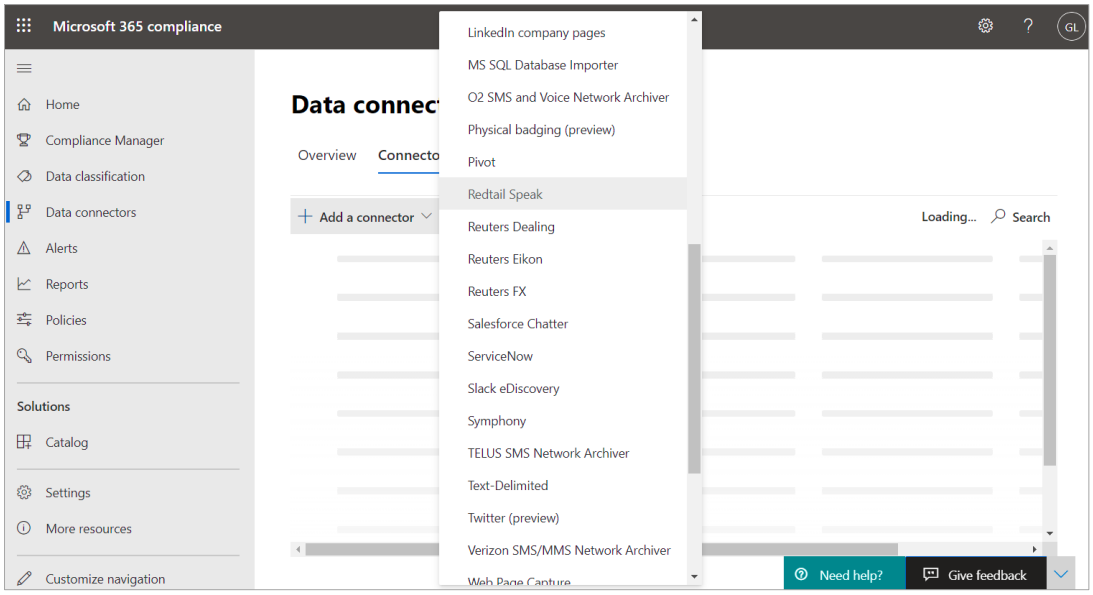


2. Navigate to **Data Connectors**. You will be presented with the **Overview** section of the Data Connectors.



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

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



5. Select the **Redtail Speak** from the list. For more details on how to set up the connector see *SETTING UP REDTAIL SPEAK*.

CHAPTER 2

Setting Up Redtail Speak

This chapter represents:

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

VERITAS

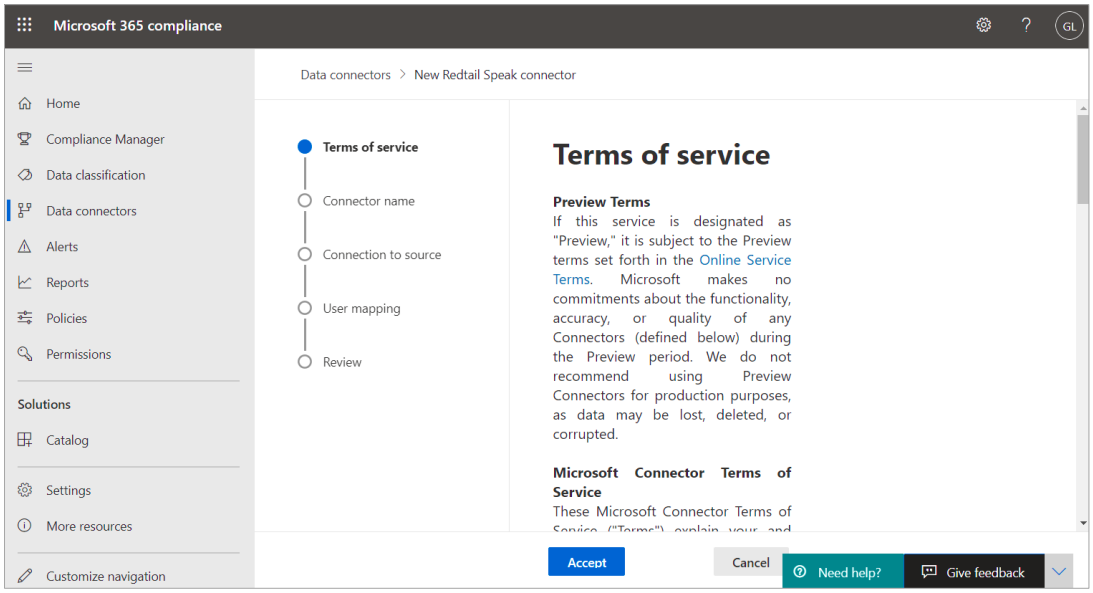
Overview

To set up a new Redtail Speak connector, you need to complete the following steps:

- Terms of service
- Connector name
- Connection to source
- User mapping
- Review.

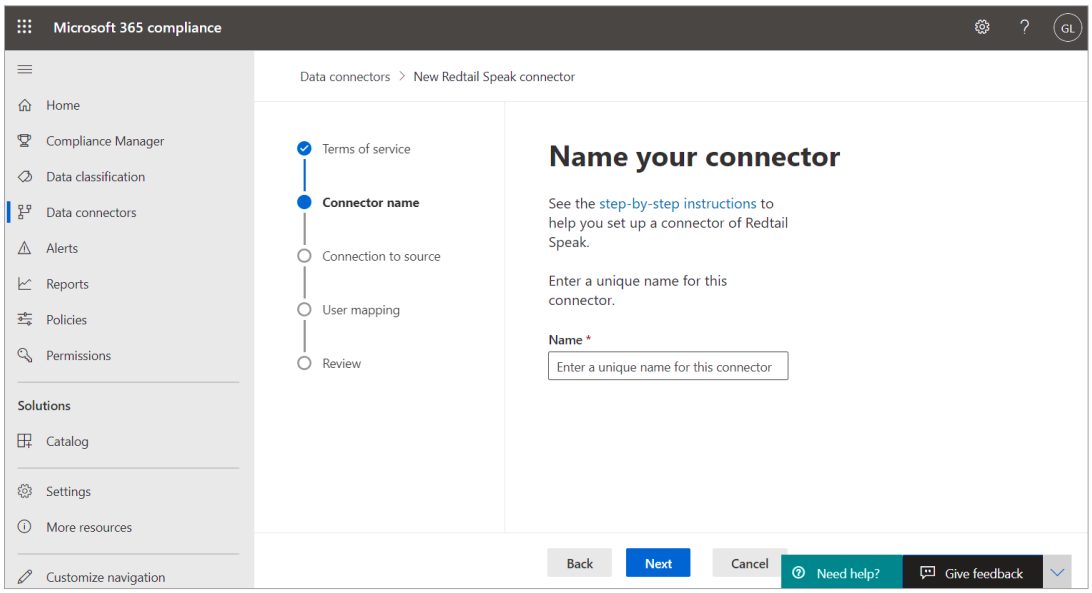
Terms of Service

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

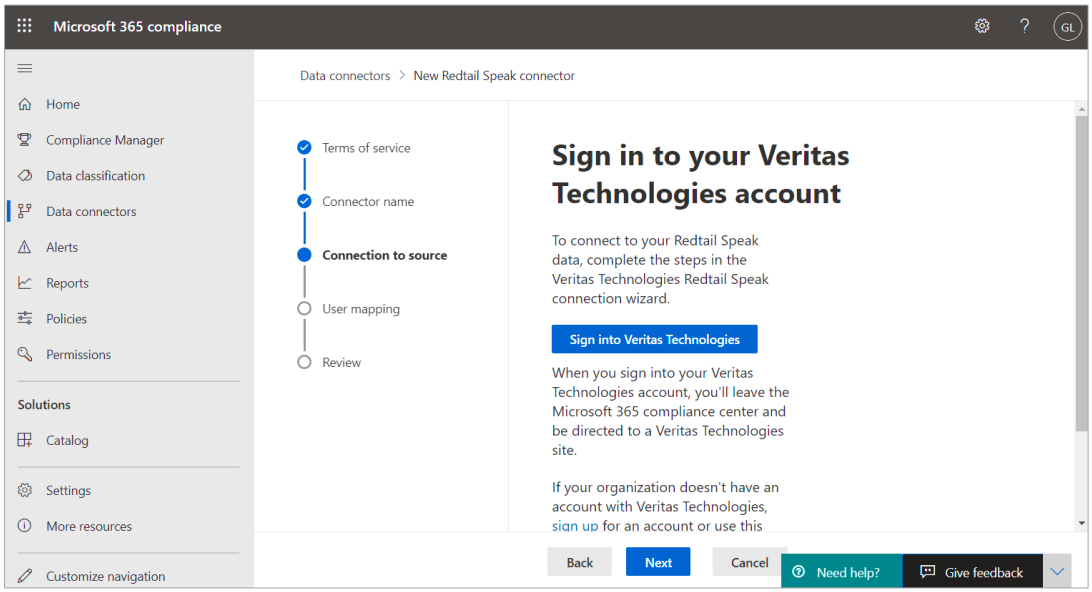


Connector Name

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



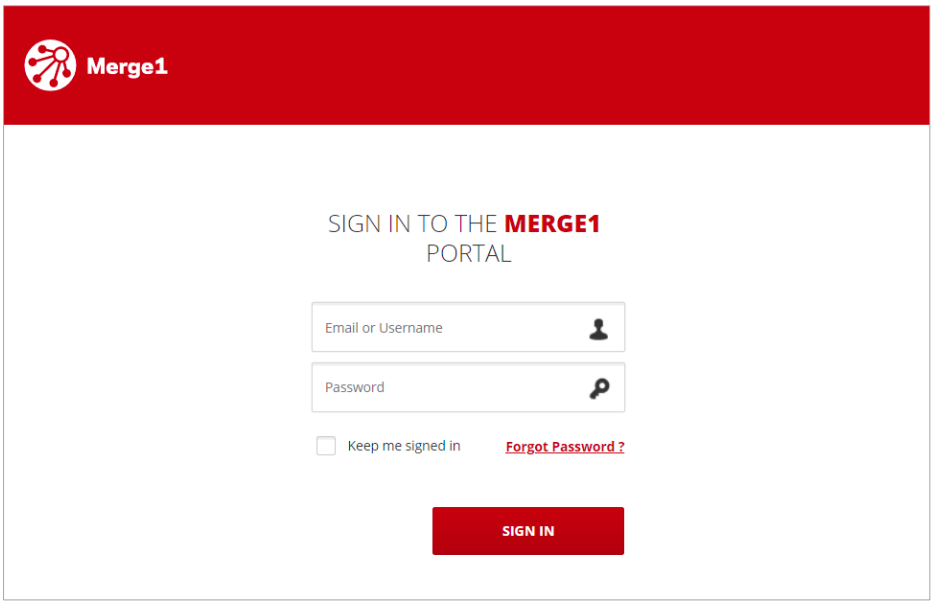
Click **Next**, to be navigated to the **Sign in to your Veritas Technologies account** page.



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.



Redtail Speak 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.

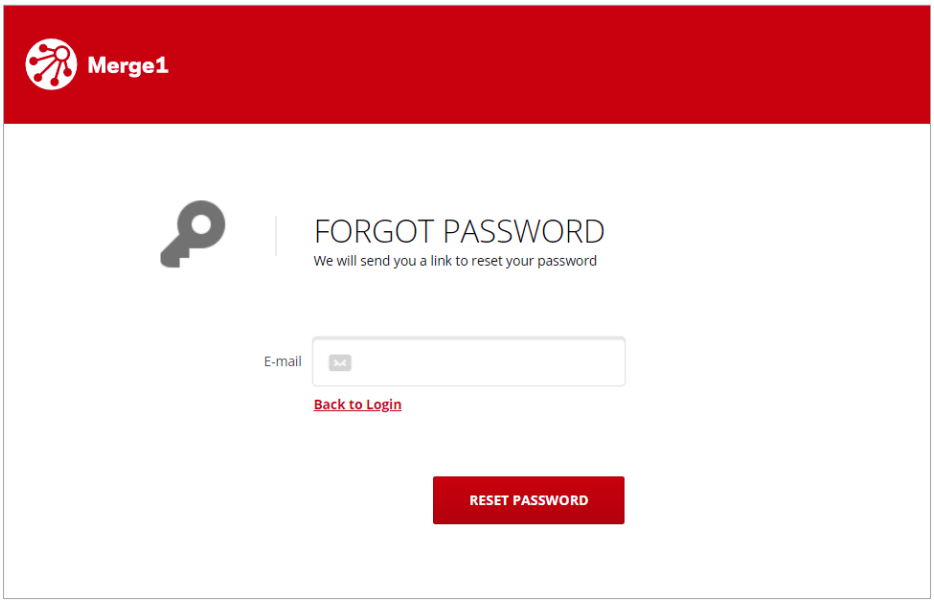
Password Recovery

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:

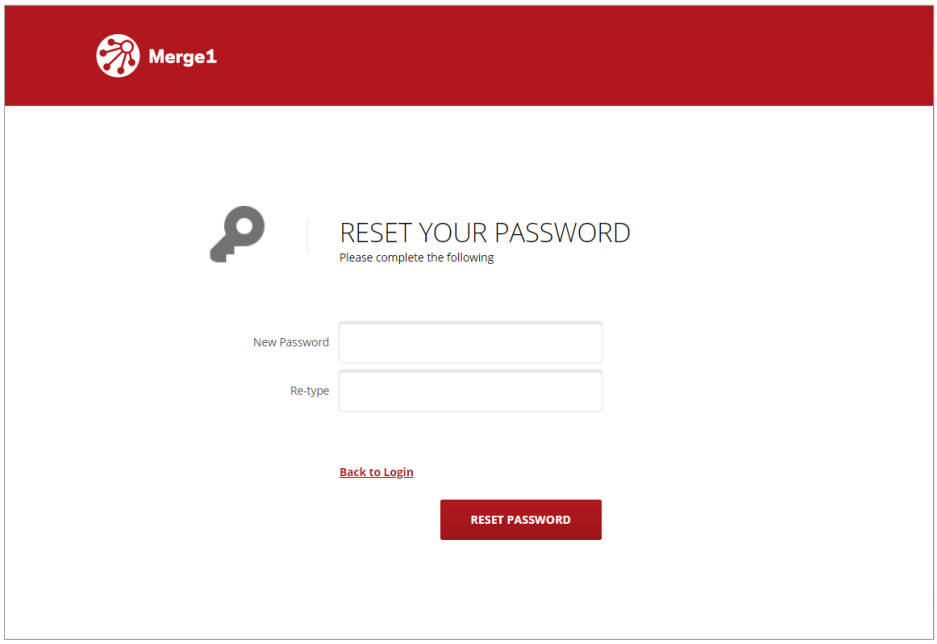
1. Click the **Forgot Password** link in the **Sign in** window.

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.

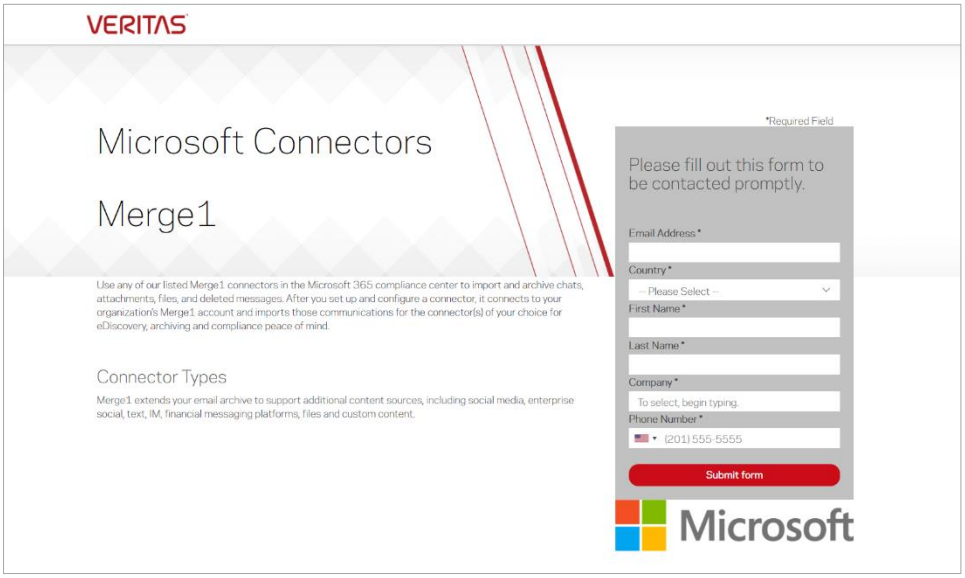
4. Provide a new password and re-enter it for verification.



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 Redtail Speak from the Merge1 product.

Now, when you are redirected to the Veritas Merge1 page, you can start configuring the Redtail Speak connector. For more details on how to configure the connector, see *CONFIGURING THE REDTAIL SPEAK CONNECTOR*.

CHAPTER 3

Configuring the Redtail Speak Connector

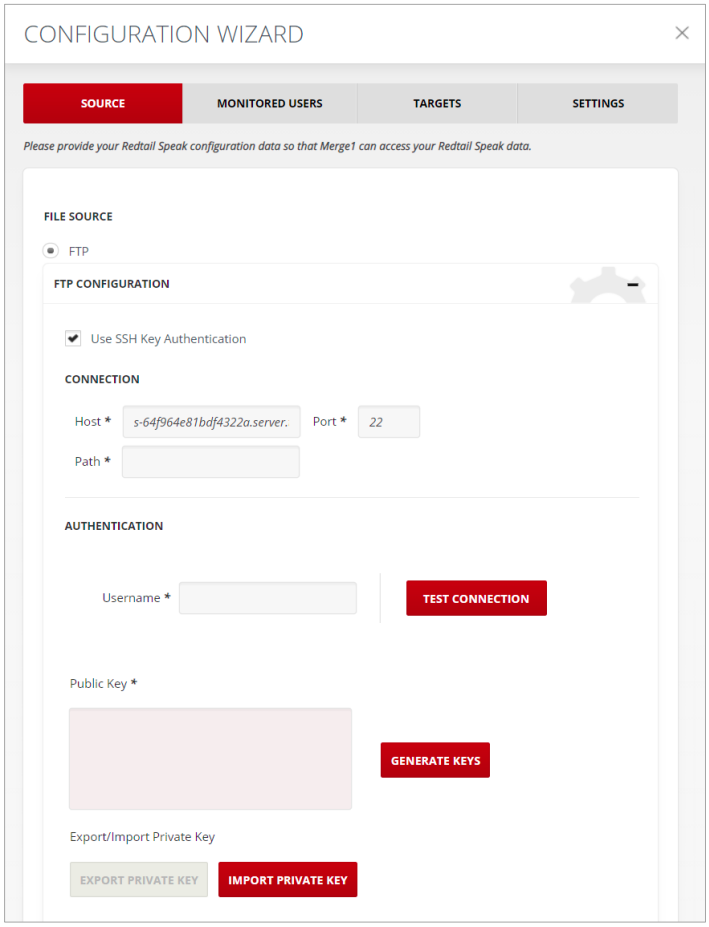
This chapter represents:

- Source
- Targets
- Settings
- User Mapping
- Review

Source Configuration

Redtail Speak SFTP Configuration

To use SSH key authentication method, follow the step below:



1. Enable **Use SSH Key Authentication** to view the SSH key generator in the **SFTP Configuration Options** window. SSH Key Authentication is used for connecting to Redtail Speak SFTP Server.

2. Make sure the connection settings match those of the SFTP server. Enter the **Path** to the required folder. The defaults port used for SSH Authentication by Redtail Speak is 22.

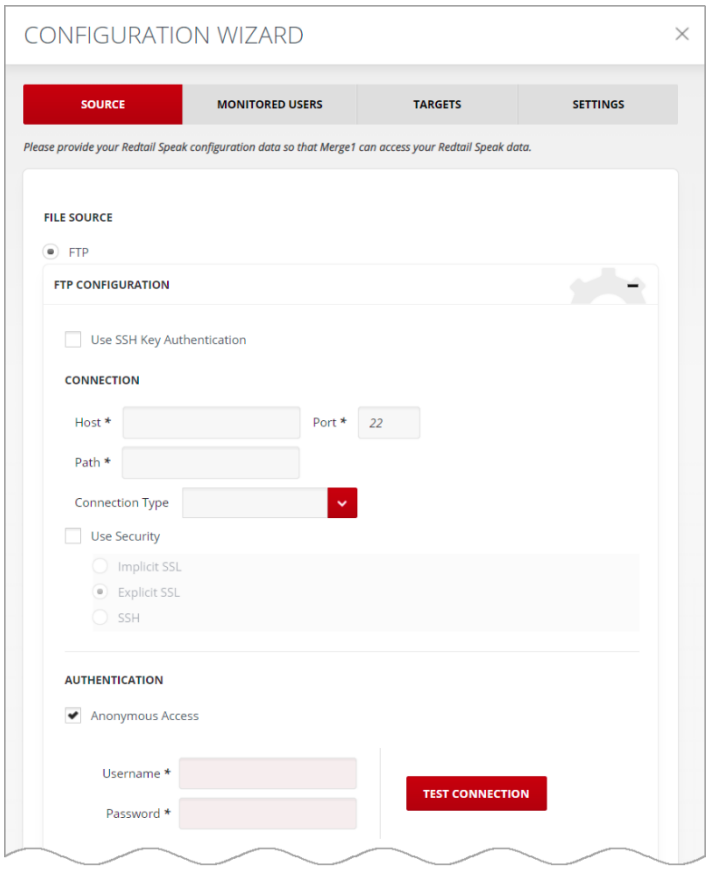
3. For **Authentication** enter the username set in your SFTP server.

4. Click **Generate Keys** for **Public Key**.

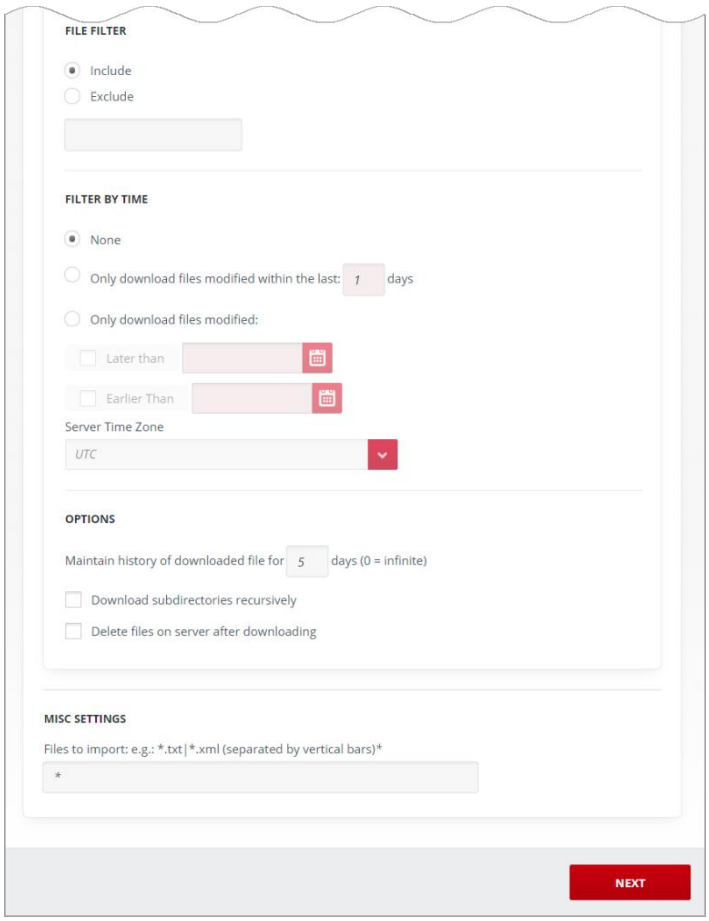
5. Click **Import Private Key**.

FTP Configurations

Merge1 retrieves data from Redtail Speak FTP and stores it in the **Import Folder** for processing. Corrupt files are moved to the **Quarantine Folder**. The **Download files from FTP** checkbox is enabled to get data from Redtail Speak through FTP.



Part 1



Part 2

It includes the following:

1. **Connection** - Enter the hostname of the remote FTP server and the folder path in the **Host** and **Path** text boxes, respectively. The default port is 22. Choose the **AutoActive** connection type from the **Connection Type** drop-down list. The information about the connection type should be provided by the FTP host. If you wish to use FTP over SSL, select **Use Security** check box and choose connection method: **Implicit SSL**, **Explicit SSL** or **SSH**.

2. **Authentication** - To authenticate an FTP connection, enter the appropriate information in the **Username** and **Password** text boxes, respectively. To enable anonymous FTP connections, select the **Anonymous Access** check box, which is the default setting.

3. **File Filter** - Exclude file types. 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.

4. **Filter by Time** - Separate the data by time.

    - **None** - If this option is selected, the data is not filtered by time.

- **Only download files modified within the last X days** - When this option is selected, only the data modifies within the mentioned days will be downloaded.
- **Only download files modified earlier than/later than** - When this option 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.
- **Server Time Zone** - Specifies the time zone in which the FTP server is to correctly determine the timestamp of downloadable files.

5. **Options**
   - **Maintain history of downloaded file for X days (0 = infinitive)** - This 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.
   - **Download subdirectories recursively** - If checked, files from the subdirectories of mentioned path will be downloaded too.
   - **Delete files on server after downloading** - If checked, the files downloaded will be deleted from the server.

Miscellaneous Settings

If you want to import specific files or filetypes, note them in the **Files to import** field. You can separate each file or filetype with a vertical bar **I**. Simply write the name of the file (e.g. delimited.txt) or use wildcards to import the whole filetype (ex. *.txt | *.xml).

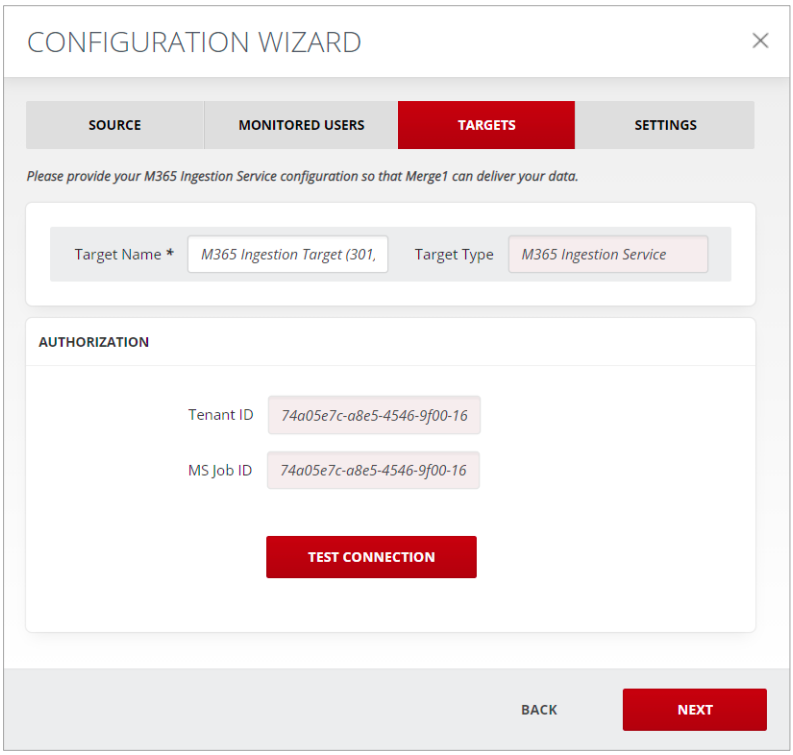
By clicking **Next**, you will be navigated to the **Monitored Users** tab.

Note that **Monitored Users** tab is not applicable for this connector.

By clicking **Skip**, 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:

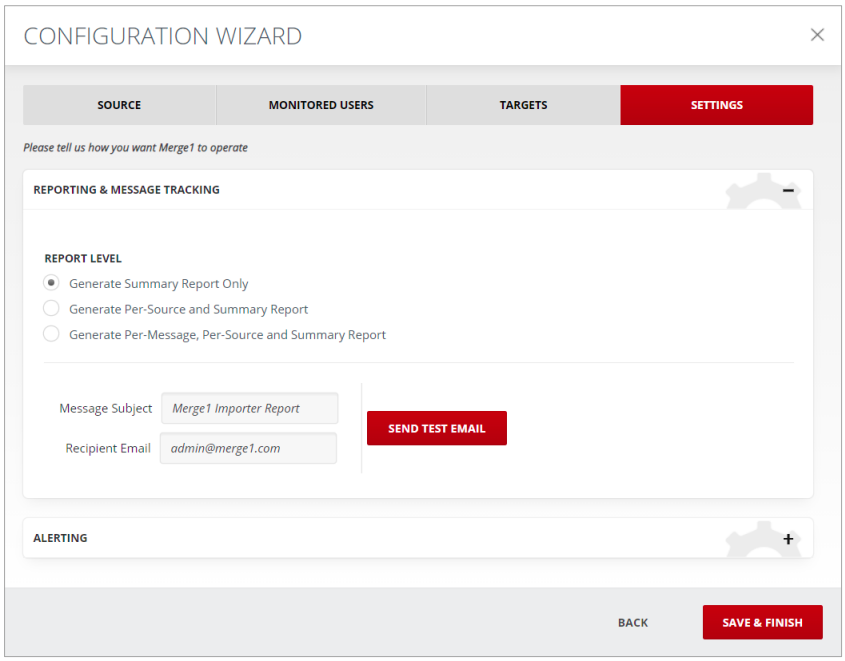
- Reporting & Message Tracking
- Alerting.

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.

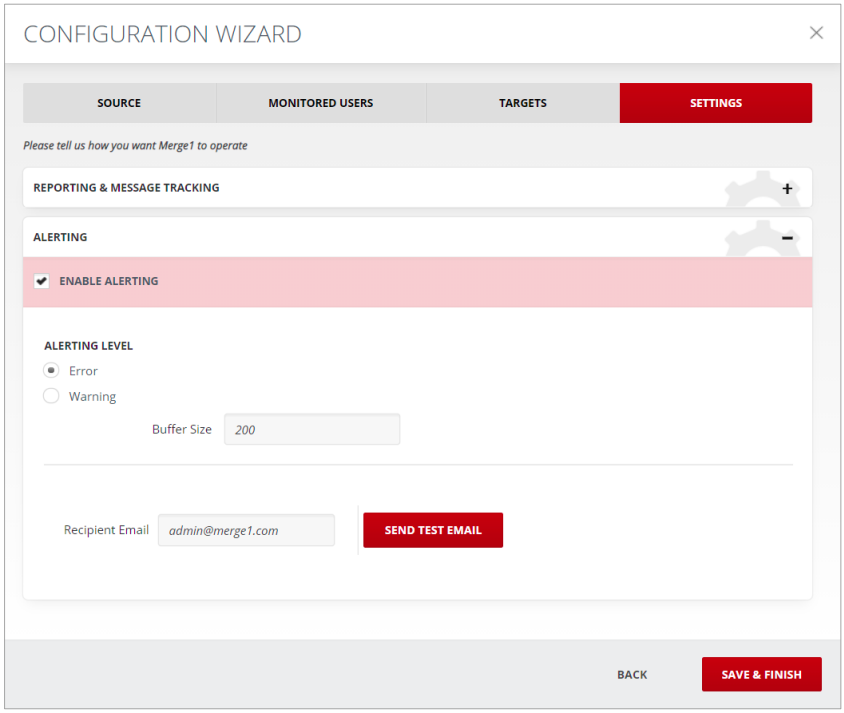
Reports are based on the activities that can be captured from the connectors.



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.

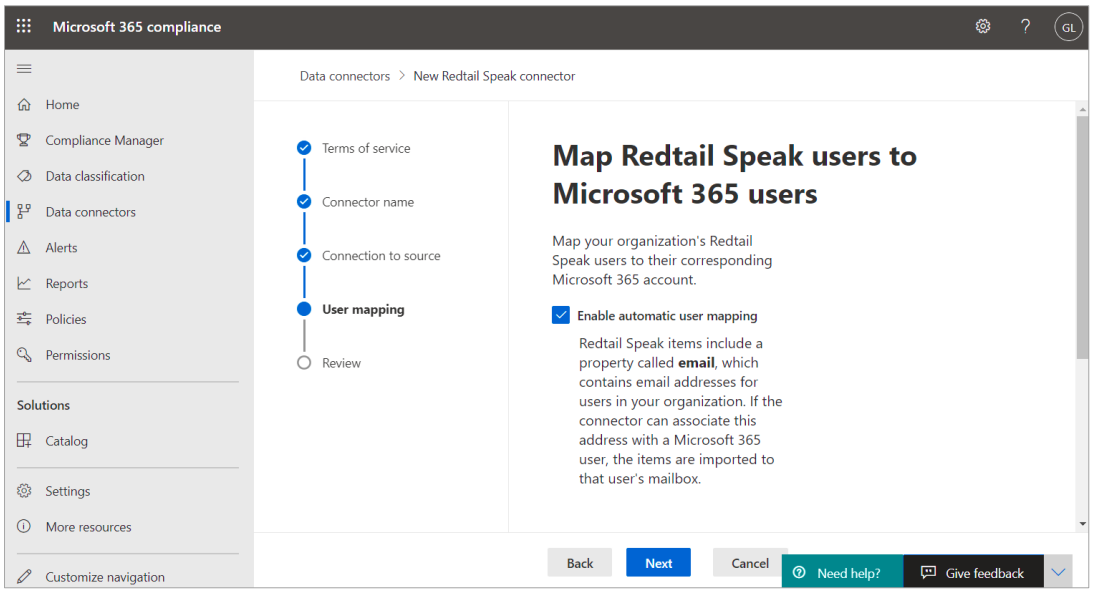
To configure the alerting, specify the **Buffer Size**.

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

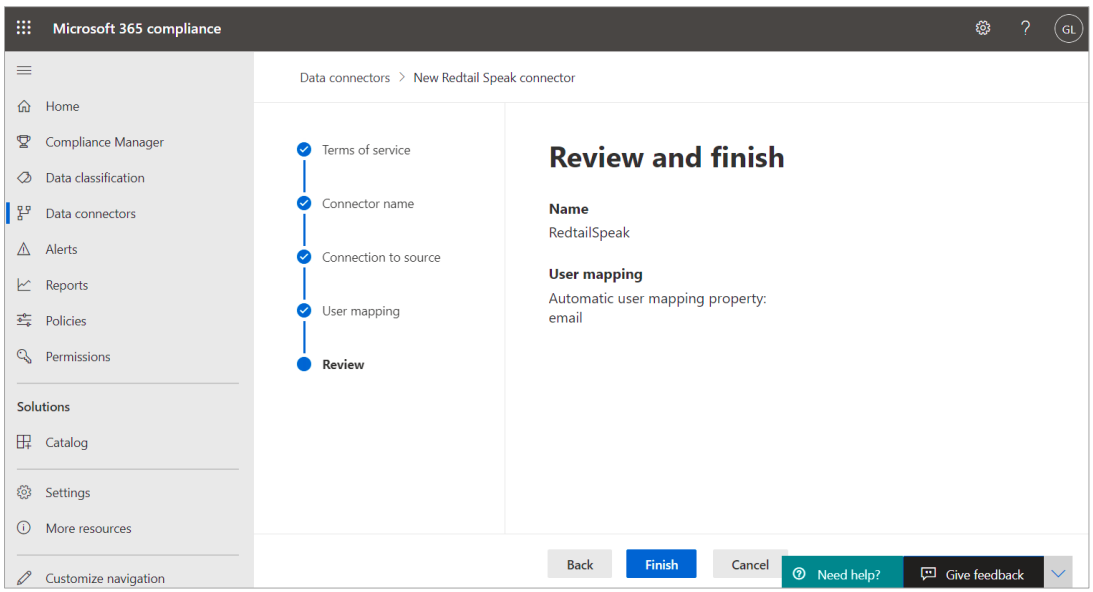
Provide the required user mapping.



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!