

Copyright © 2021 Veritas Technologies LLC. All rights reserved.

# VERITAS™

## Third-Party Connectors

### Cisco Jabber on MS SQL

### User Guide



MERGE1

## LEGAL NOTICE

The software described in this guide is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Copyright © 2021 Veritas Technologies LLC. All rights reserved.

Veritas and the Veritas Logo are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third-party software for which Veritas is required to provide attribution to the third party ("Third-party Programs"). Some of the Third-party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the Third-party Legal Notices document accompanying this Veritas product or available at:

<https://www.veritas.com/about/legal/license-agreements>.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Veritas Technologies LLC and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. VERITAS TECHNOLOGIES LLC SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Veritas Technologies LLC

2625 Augustine Dr

Santa Clara, CA 95054

<http://www.veritas.com>

# CONTENTS

CONTENTS .....	2
<b>INTRODUCTION.....</b>	<b>4</b>
OVERVIEW .....	5
PRE-REQUISITES .....	5
ACCESSING THE DATA CONNECTORS .....	6
<b>SETTING UP CISCO JABBER ON MS SQL .....</b>	<b>8</b>
OVERVIEW .....	9
TERMS OF SERVICE .....	9
CONNECTOR NAME .....	10
CONNECTION TO SOURCE.....	11
<b>CONFIGURING THE CISCO JABBER ON MS SQL CONNECTOR.....</b>	<b>14</b>
SOURCE .....	15
MONITORED USERS .....	19
TARGETS .....	20
SETTINGS .....	20
USER MAPPING.....	23
REVIEW .....	24



# 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

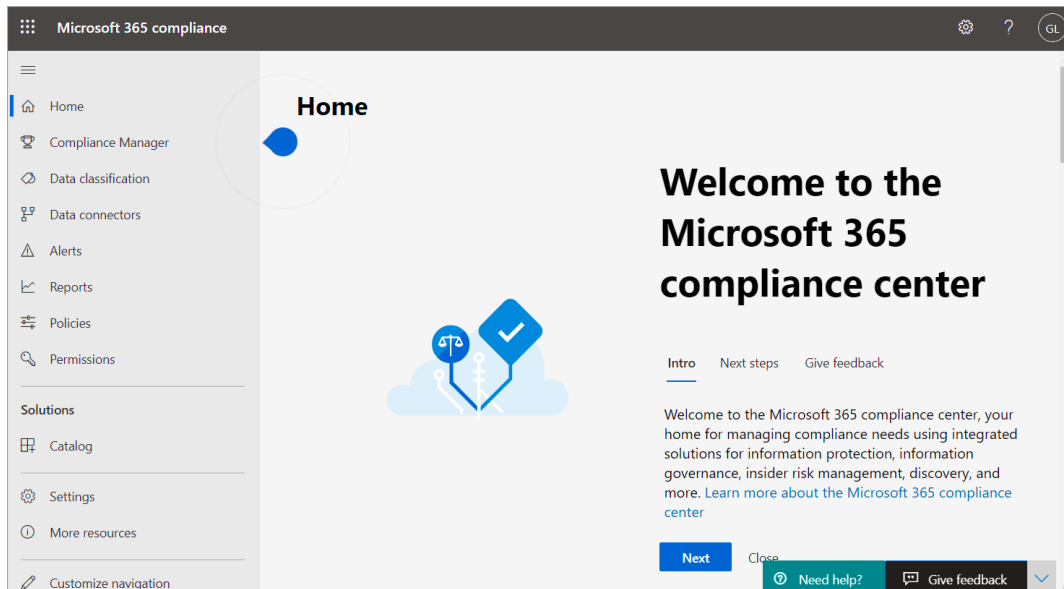
Many of the implementation steps, required to archive Cisco Jabber on MS SQL data are external to Microsoft 365 and must be completed before you can create the connector in the compliance center.

- Create a Merge1 account by accepting their terms and conditions for Cisco Jabber on MS SQL 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 Cisco Jabber on MS SQL 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”.

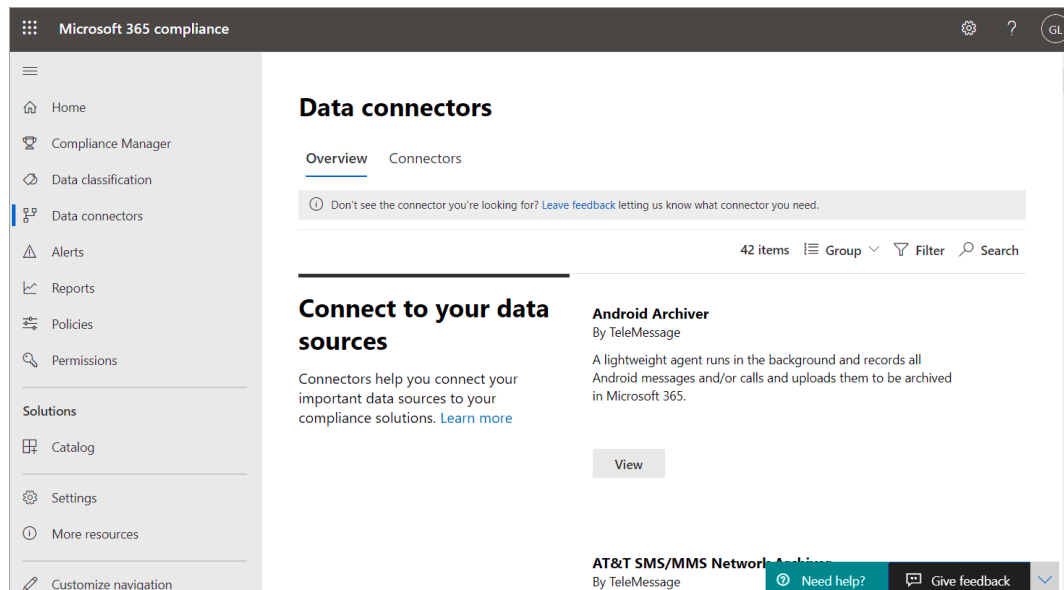
# Accessing the Data Connectors

To access the Data Connectors, follow the steps below:

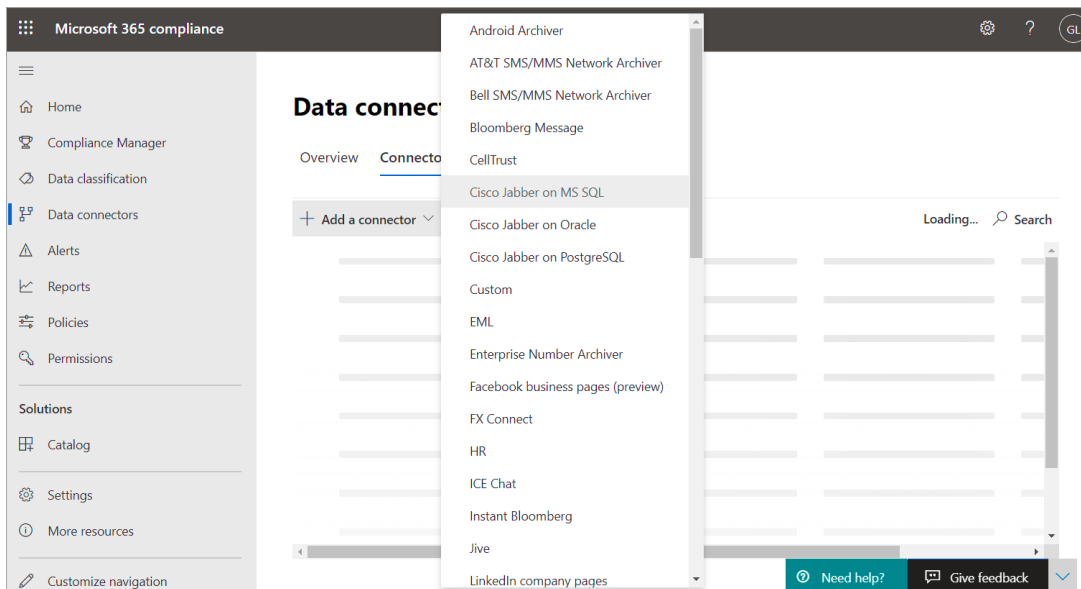
1. Go to <https://compliance.microsoft.com> web page.



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 **Cisco Jabber on MS SQL** from the list. For more details on how to set up the connector see [SETTING UP CISCO JABBER ON MSSQL](#).



## CHAPTER 2

# Setting Up Cisco Jabber on MS SQL

This chapter represents:

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



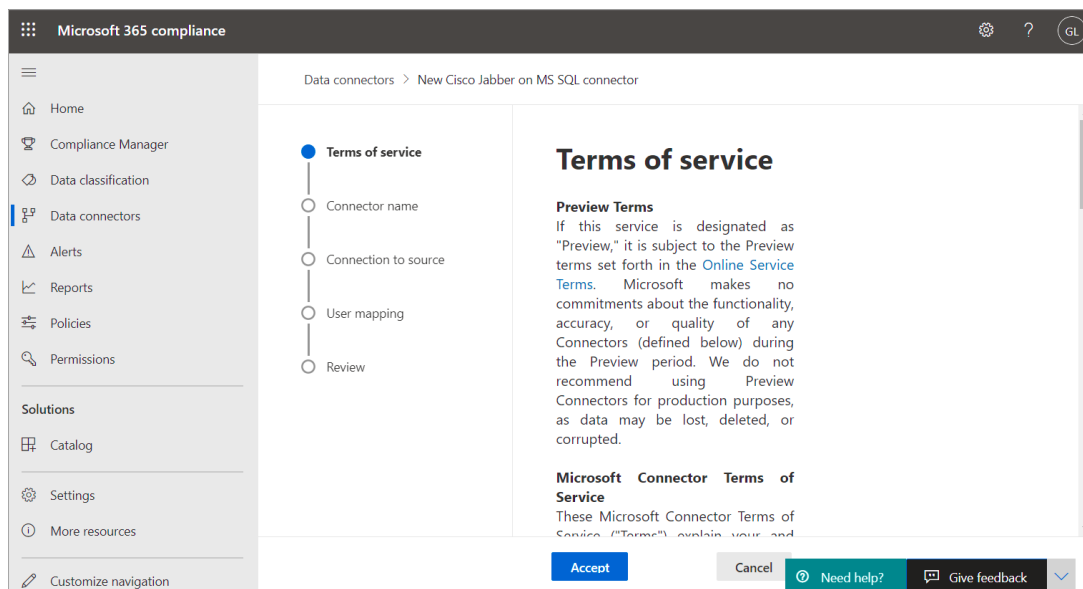
# Overview

To set up a new Cisco Jabber on MS SQL connector, you need to complete the following steps:

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

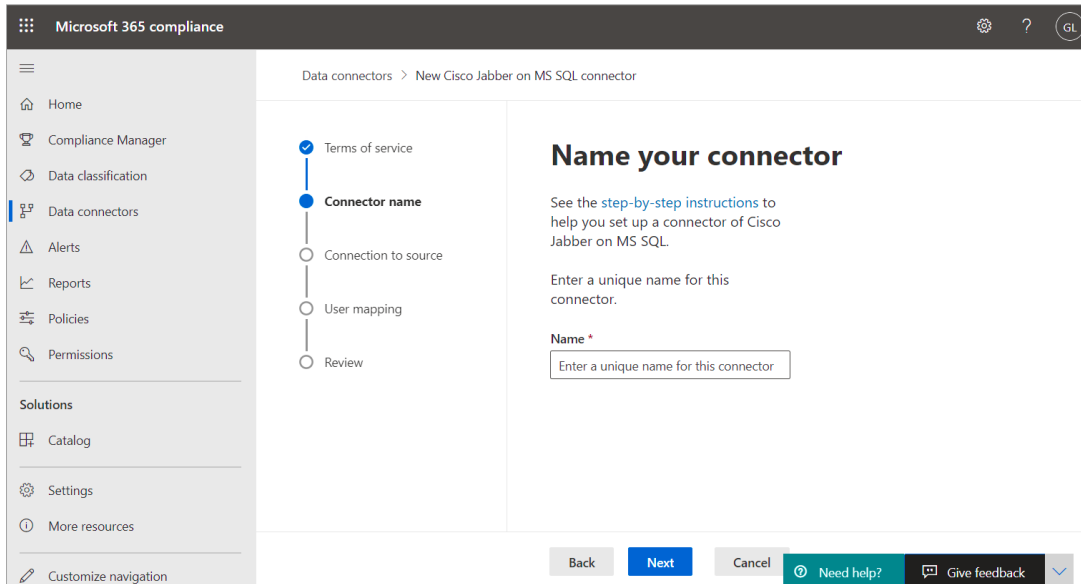
# Terms of Service

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

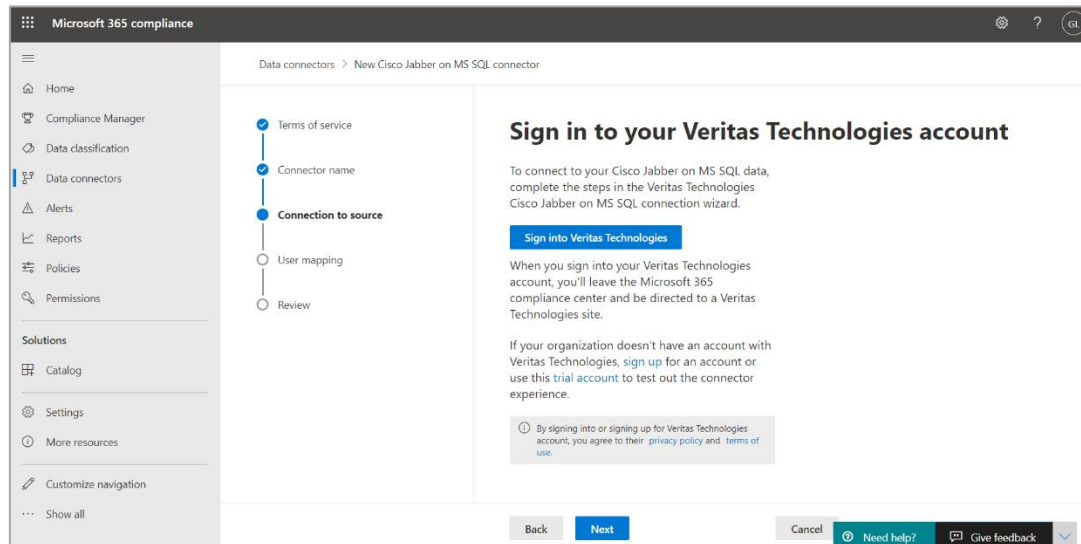


# Connector Name

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



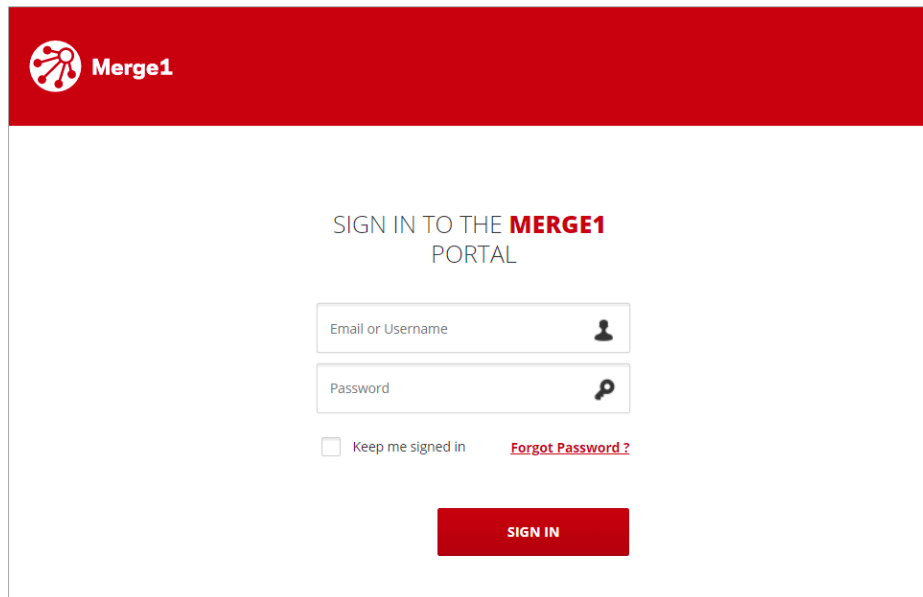
Click **Next**, to be navigated to the **Sign in to your Veritas Technologies account** page.



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.



The screenshot shows the Merge1 login interface. At the top left is the Merge1 logo. The main heading is "SIGN IN TO THE MERGE1 PORTAL". Below the heading are two input fields: "Email or Username" with a user icon and "Password" with a key icon. Below the password field is a checkbox labeled "Keep me signed in" and a red link "Forgot Password?". At the bottom center is a red button labeled "SIGN IN".

Cisco Jabber on MS SQL 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.

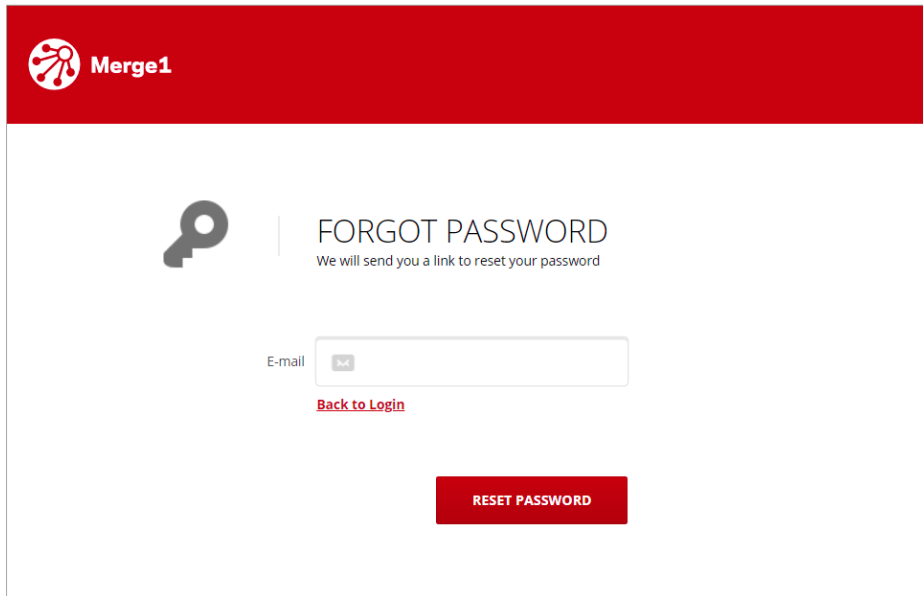
## Password Recovery

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.



Merge1

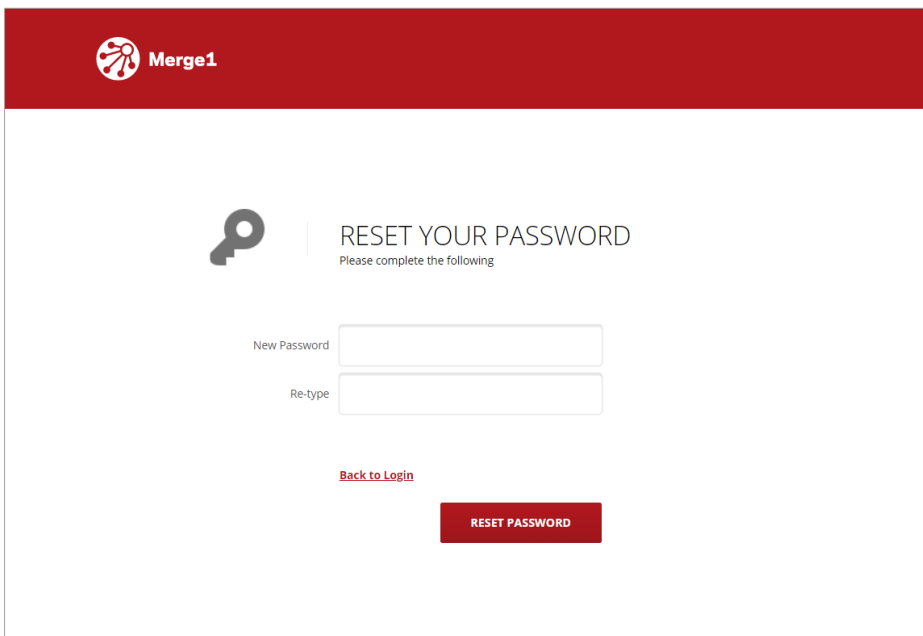
 **FORGOT PASSWORD**  
We will send you a link to reset your password

E-mail


[Back to Login](#)

**RESET PASSWORD**

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



Merge1

 **RESET YOUR PASSWORD**  
Please complete the following

New Password

Re-type

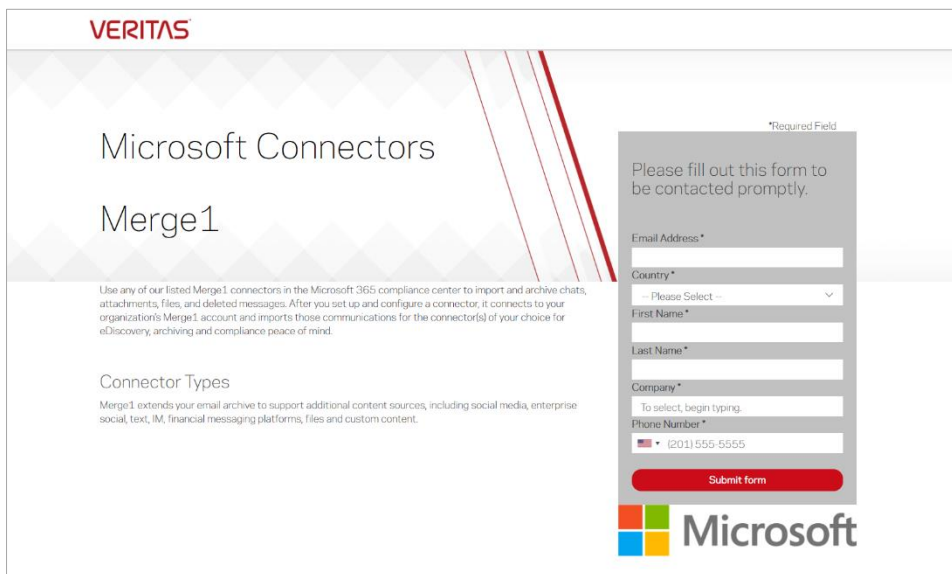
[Back to Login](#)

**RESET PASSWORD**

## 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



The screenshot shows a registration form titled "Microsoft Connectors Merge1" with the Veritas logo at the top left. The form includes a "Required Field" label and a prompt: "Please fill out this form to be contacted promptly." The form fields are: Email Address\*, Country\*, a dropdown menu for "Please Select -", First Name\*, Last Name\*, Company\*, a text field for "To select, begin typing", and Phone Number\* with a country code dropdown set to "(201) 555-5555". A red "Submit form" button is at the bottom of the form. The Microsoft logo is visible at the bottom right of the form area. Below the form, there is a section titled "Connector Types" with a brief description: "Merge1 extends your email archive to support additional content sources, including social media, enterprise social, text, IM, financial messaging platforms, files and custom content."

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 Cisco Jabber on MS SQL from the Merge1 product.

Now, when you are redirected to the Veritas Merge1 page, you can start configuring the Cisco Jabber on MS SQL connector. For more details on how to configure the connector, see [CONFIGURING THE CISCO JABBER ON MS SQL CONNECTOR](#).



## CHAPTER 3

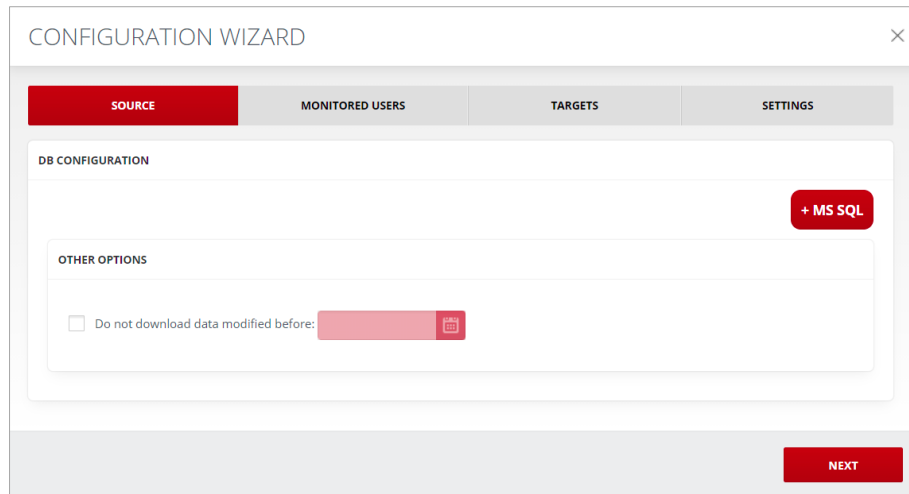
# Configuring the Cisco Jabber on MS SQL Connector

This chapter represents:

- Source
- Monitored Users
- Targets
- Settings
- User Mapping
- Review

## Source Configuration

Merge1 retrieves data directly from Jabber's MS SQL Server database.



By clicking the **+ MS SQL** button at the left upper part of the window, the database configuration page will open. For more details, see [Microsoft SQL Server](#).

## Microsoft SQL Server

For MS SQL Server follow the steps below:

1. Insert the **Configuration Name** and **SQL Server** in the fields of **SQL Connection**.
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 up on. If **SQL Server Authentication** is chosen it can be connected to with the SQL Server credentials.
3. Select the database where Jabber files are stored, from the drop-down menu after connecting to the server.

The screenshot shows the 'CONFIGURATION WIZARD' window with the 'SOURCE' tab selected. Under 'DB CONFIGURATION', there is a '+ MS SQL' button. Below it, the 'MS SQL' configuration panel is visible. It is divided into several sections: 'SQL CONNECTION' with fields for 'Configuration Name' and 'Select SQL Server', and a 'CONNECT' button; 'FILE PROCESSING' with checkboxes for 'Process shared files' and 'Fail conversations with missing files'; 'CONNECTION' with fields for 'Host \*', 'Port \*' (set to 22), and 'Path \*'; 'AUTHENTICATION' with fields for 'Username \*', 'Public Key \*', and buttons for 'TEST CONNECTION' and 'GENERATE KEYS'; and 'CONNECT USING' with radio buttons for 'Windows Authentication' (selected) and 'SQL Server Authentication', along with fields for 'Login Name' and 'Password'. At the bottom, there is a 'Select Database' dropdown menu and buttons for 'EXPORT PRIVATE KEY' and 'IMPORT PRIVATE KEY'.

### Part 1


The screenshot shows the 'ADVANCED CONNECTION PARAMETERS' section of the configuration wizard. It includes several input fields: 'Connection timeout' (15 sec), 'Load balance timeout' (0 sec), 'Min pool size' (0), 'Max pool size' (100), and 'Network packet size' (8000 bytes). Below these are several checkboxes: 'Asynchronous Processing', 'Encrypt', 'Enlist' (checked), 'Pooling' (checked), and 'Replication'. At the bottom, there is an 'OTHER OPTIONS' section with a checkbox 'Do not download data modified before:' followed by a red input field and a calendar icon. A 'NEXT' button is located at the bottom right of the wizard.

### Part 2

#### 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 slave databases with outdated or incomplete data.
5. **File Processing** - By activating the **Process shared files** checkbox, which is disabled by default, you allow the files shared, using Jabber, to be processed by the connector and the fields below become mandatory. When the **Fail conversations with missing files** checkbox is enabled, conversations that have reference(s) to file(s) in the database but actually do not exist in the file store will be marked as failed (Stored in Merge1 database), the Merge1 admin then can make a decision to export the messages or set the reprocessing option by navigating to the Reports page of Merge1.
  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** textboxes, respectively.
  7. **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.

**8. Other Options:**

**Do not download data modified before** - this will ensure that old or irrelevant data is excluded. For example, if the date selected is 9/1/2020, it will not retrieve any data modified before September 1 of 2020. Only the data after 9/1/2020 will be retrieved, archived, and imported.

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 is a User Source Configuration from where Monitored Users can be added to the connector:  
**Manually Maintain the List.**

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

CONFIGURATION WIZARD

SOURCE **MONITORED USERS** TARGETS SETTINGS

ACCOUNT FILTER

USER SOURCE CONFIGURATION

Manually Maintain The List

Now that you have told us where to gather your data, tell us whose data you want Merge1 to gather.

EDIT EXISTING LIST

BACK NEXT

This will allow manually adding and managing users.

CONFIGURATION WIZARD

SOURCE **MONITORED USERS** TARGETS SETTINGS

Preview and confirm Monitored User entries.

ADD MONITORED USER DELETE SELECTED Search for User SEARCH

	CORP EMAIL ADDRESS	DISPLAY NAME	MONITOR	JABBER ENTERPRISE EM
<input type="checkbox"/>	jsmith@veritas.com	John Smith	<input checked="" type="checkbox"/>	jsmith@veritas.com

1 - 1 OF 1 ITEMS

BACK SAVE CHANGES NEXT

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.

The screenshot shows a 'CONFIGURATION WIZARD' window with a 'TARGETS' tab selected. The form contains the following fields and buttons:

- Target Name \*: M365 Ingestion Target (301)
- Target Type: M365 Ingestion Service
- Tenant ID: 74a05e7c-a8e5-4546-9f00-16
- MS Job ID: 74a05e7c-a8e5-4546-9f00-16
- TEST CONNECTION button
- BACK button
- NEXT button

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.

The screenshot shows a 'CONFIGURATION WIZARD' window with a close button (X) in the top right corner. Below the title bar are four tabs: 'SOURCE', 'MONITORED USERS', 'TARGETS', and 'SETTINGS' (which is highlighted in red). Below the tabs is a sub-header 'REPORTING & MESSAGE TRACKING' with a gear icon and a minus sign. Underneath, the 'REPORT LEVEL' section has three radio button options: 'Generate Summary Report Only' (selected), 'Generate Per-Source and Summary Report', and 'Generate Per-Message, Per-Source and Summary Report'. Below this are two input fields: 'Message Subject' with the value 'Merge1 Importer Report' and 'Recipient Email' with the value 'admin@merge1.com'. A red 'SEND TEST EMAIL' button is positioned to the right of the 'Recipient Email' field. At the bottom of the wizard, there is an 'ALERTING' section with a gear icon and a plus sign, and a footer with 'BACK' and 'SAVE & FINISH' buttons.

- 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.

The screenshot shows the 'CONFIGURATION WIZARD' interface with a navigation bar containing 'SOURCE', 'MONITORED USERS', 'TARGETS', and 'SETTINGS'. The 'SETTINGS' tab is active. Below the navigation bar, there is a section for 'REPORTING & MESSAGE TRACKING' and an 'ALERTING' section. The 'ALERTING' section is expanded, showing a checked 'ENABLE ALERTING' option. Under 'ALERTING LEVEL', the 'Error' radio button is selected, and the 'Warning' radio button is unselected. A 'Buffer Size' input field is set to '200'. At the bottom of the alerting section, there is a 'Recipient Email' input field containing 'admin@merge1.com' and a 'SEND TEST EMAIL' button. At the bottom of the wizard, there are 'BACK' and 'SAVE & FINISH' buttons.

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.

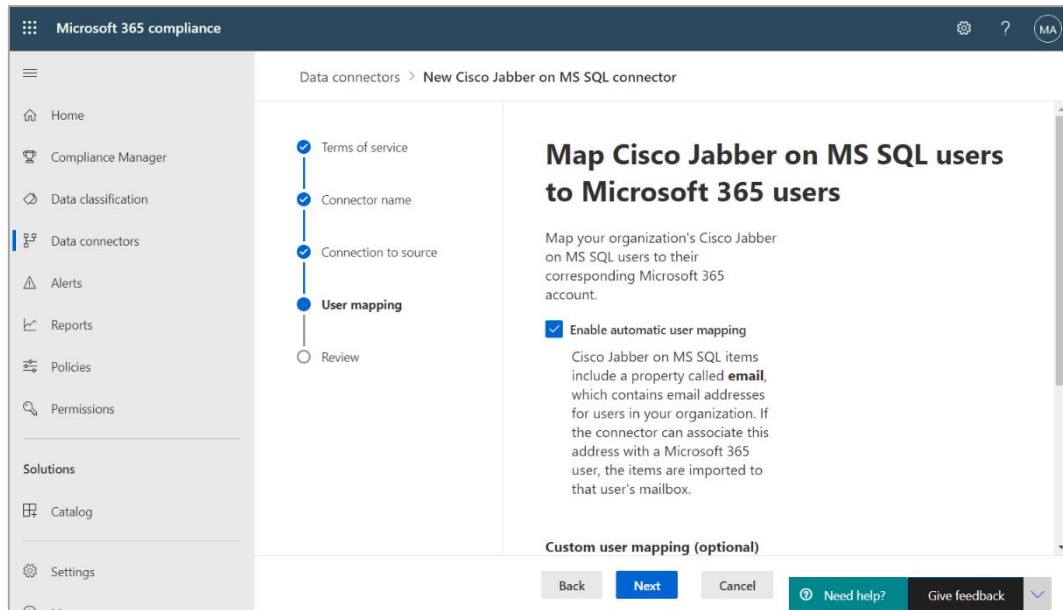
To configure the alerting, specify the **Buffer Size**.

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

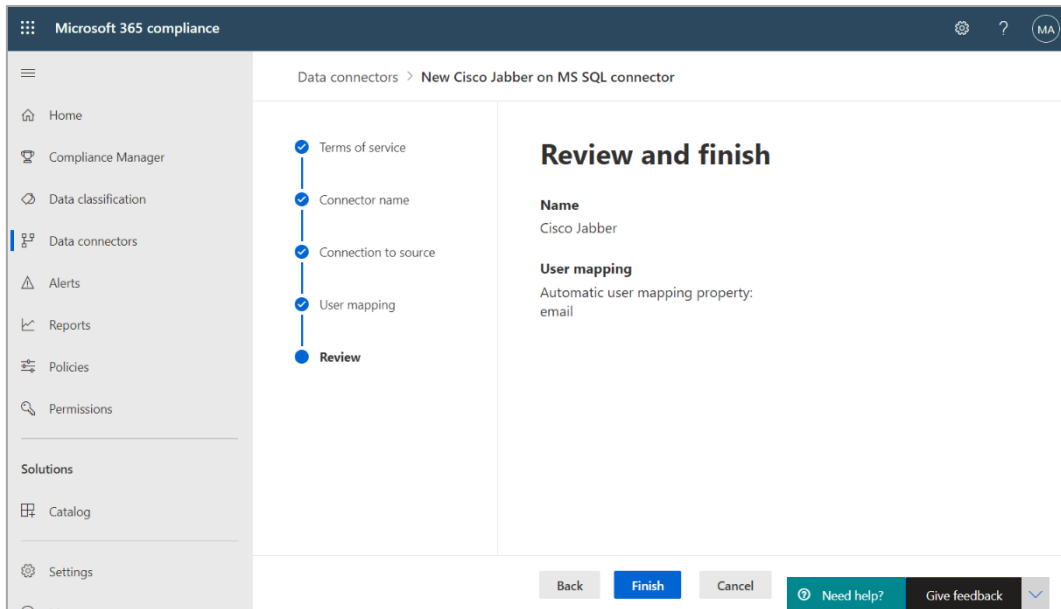
Provide the required user mapping.



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!

