

U S E R G U I D E



Globanet

Merge1 6.0

Address: Globanet Consulting Services
16501 Ventura Blvd, Suite 400
Encino, California 91436

Phone: 310-202-0757
Fax: 310-202-5452
www.globanet.com

Version: 6.20.0131

ME
RG
E 1
6.0



Possession, use, distribution, and decompilation is governed by license agreement from Globanet Consulting Services. Globanet Consulting Services makes no representations that the use of its products in the manner described in this publication will not infringe on existing or future patent rights, nor do the descriptions contained in this publication imply the granting of licenses to make, use, or sell software in accordance with the description. The information in this document may not be changed without the express written agreement of Globanet Consulting Services.

All trademarks are the property of their respective owners.

**© 2020 Globanet Consulting Services.
All rights reserved.**

TABLE CONTENT

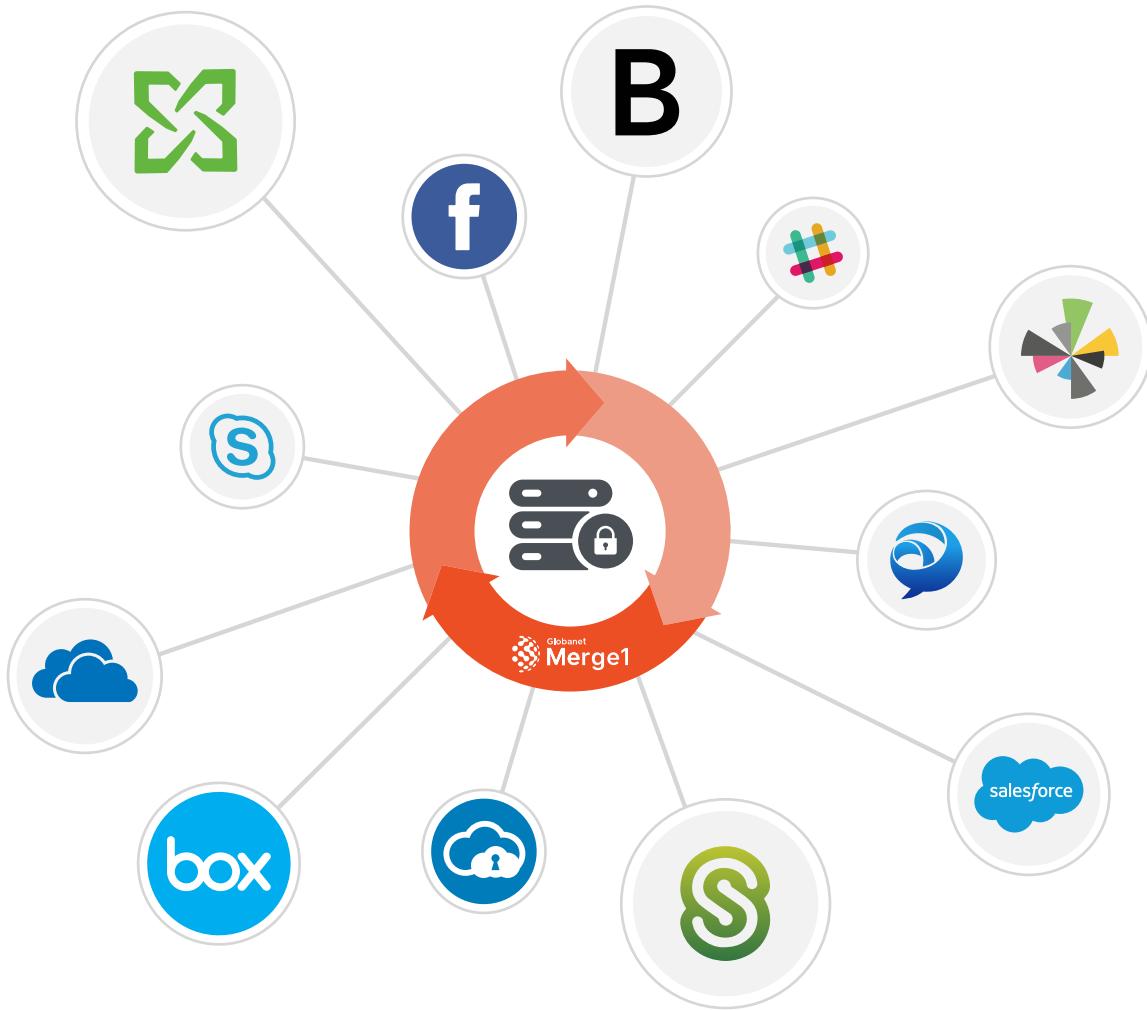
WELCOME	-----	4
KEY CONCEPTS	-----	6
SYSTEM REQUIREMENTS	-----	8
GETTING STARTED	-----	9
Pre-Installation Checklist	-----	10
Pre-Installation Steps	-----	12
Installation	-----	18
Database Configuration	-----	23
Signing in	-----	26
License Activation	-----	27
NAVIGATING MERGE1	-----	28
The Navigation Pane	-----	29
Account Settings	-----	30
DASHBOARD	-----	32
IMPORTERS	-----	35
The Configuration Wizard	-----	38
Monitored Users	-----	314
Filters	-----	320
Targets	-----	324
Importer Settings	-----	346
USERS & GROUPS	-----	361
REPORTS	-----	364
SETTINGS	-----	369
Database Configuration	-----	370
BRANDING	-----	372
LICENSING	-----	374
License Activation	-----	375
The Database Upgrade Wizard	-----	376
APPENDIX	-----	381

01

WELCOME TO MERGE1 6.0

- Key Concepts
- System Requirements

WELCOME TO MERGE1 6.0



Merge1 aids financial service firms in complying with SEC rule 17-a4, CFTC rule 1.31, Dodd-Frank requirements, FINRA and other regulatory agencies. It also greatly reduces legal risks by streamlining the discovery of e-communications data, aiding organizations across all verticals with internal investigations, lawsuits and audits. Merge1 offers excellent compatibility with Microsoft Exchange, Microsoft Office 365, IBM Domino, Veritas Enterprise Vault, Veritas Enterprise Vault.cloud and many other applications.

Merge1 6.0 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 little system resources.

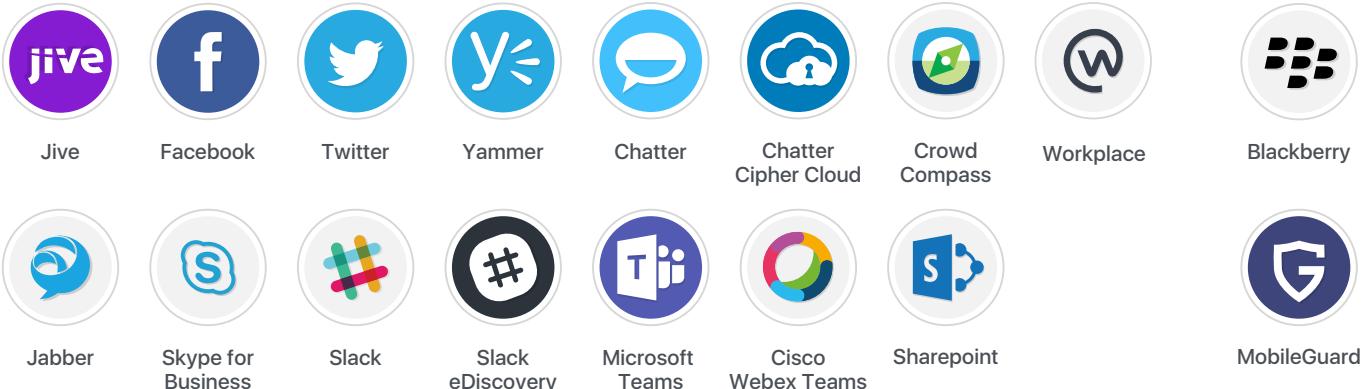
KEY CONCEPTS

SOURCES

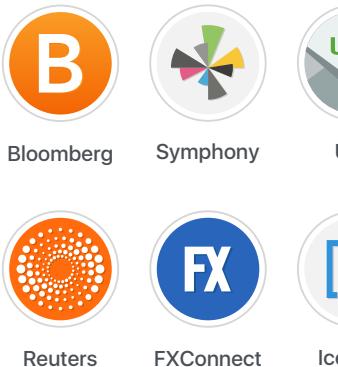
Merge1 collects data from an array of e-communication media. You can view all the sources supported in version 6.20.0131 below.

New Sources are frequently being added, feel free to contact Globanet Support concerning new additions or requests.

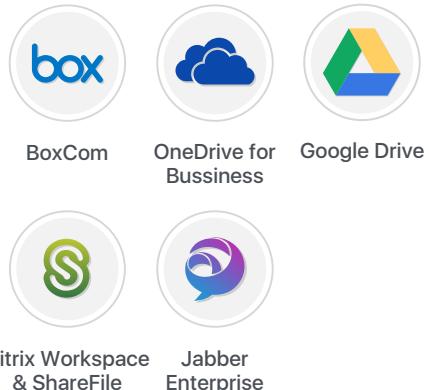
Enterprise Social



Financial Platforms



Enterprise Tools and File Sharing



Other



KEY CONCEPTS

MONITORED USERS

Monitored Users are the individuals whose data is collected by Merge1.:

FILTERS & TARGETS

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 via Active Directory.

Targets determine the means through which data is collected. Merge1 currently supports Enterprise Vault, Exchange Web Services, Office 365 EWS, NSF and SMTP.

For EV Targets:

- Symantec Enterprise Vault 2007 SP5 up to Enterprise Vault 12
- Enterprise Vault API Runtime 11 or 12

For EWS Targets:

- Microsoft Exchange Server 2007 SP1, 2010 (GA – SP3), 2013, or 2016

For NSF Targets:

- Domino Server 7.0.3, 8.0, or 8.5

For SMTP Targets:

- Domino Server 7.02 or higher
- Microsoft Exchange Server 2003, 2007, 2010, 2013, or 2016

IMPORTERS

Importers are where Sources, Monitored Users, Filters and Targets come together to perform data collection and delivery tasks.

SYSTEM REQUIREMENTS

MINIMUM HARDWARE REQUIREMENTS

- 2.4 GHz 64-bit dual-core processor
- 4 GB RAM
- 1 GB hard-disk space

Having more processor cores will ensure adequate performance in instances where multiple importers are consistently being run simultaneously.

SOFTWARE

- Windows 8.1 or later; Windows Server 2012 or later, x64-based
- Internet Information Services 7.0 or higher
- .NET Framework 3.5 & 4.7.2
- Microsoft Visual C++ 2017 (x64) Redistributable
- SQL Server 2012 or later

02

GETTING STARTED

- Preinstallation Checklist
- Installation
- Database Configuration
- Signing In
- Activating a License

PREINSTALLATION CHECKLIST

NOTE

Merge1 utilizes 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 defaults ports used for SSH Authentication by Bloomberg and IceChat are 30206 and 22 respectively. 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 dual-core processor with at least 4 GB RAM and 1 GB hard-disk space
- Windows 8.1 or later; Windows Server 2012 or later, x64-based
- Internet Information Services 7.0 or higher (please see Installing Internet Information Services in the Appendices)
- .NET Framework 3.5 & 4.7.2 (please see Verifying .NET Framework Requirements in the Appendices)
- Microsoft Visual C++ 2017 Redistributables
- SQL Server 2012 or later

Ensure that all relevant Target requirements are met:

EV Targets:

- Symantec Enterprise Vault 2007 SP5 up to Enterprise Vault 12
- Enterprise Vault API Runtime 11 or 12, (on the Merge1 host)*

EWS Targets:

- Microsoft Exchange Server 2007 SP1, 2010 (GA – SP3), 2013, or 2016

NSF Targets:

- Domino Server 7.0.3, 8.0, or 8.5

SMTP Targets:

- Domino Server 7.02 or higher
- Microsoft Exchange Server 2003, 2007, 2010, or 2013

* The EV API is required only if customer wants to write directly to the EV archive via binaries, instead of journaling.

The reason is that writing directly has the following drawback - it shortcuts Compliance Accelerator sampling, while it is preferred to send the items to a mailbox and use their regular Exchange journaling or smtp journaling method, like with any other type of mail.

PREINSTALLATION CHECKLIST

If your Merge1 version is earlier than 6.17.1129, uninstall it before the installation of the new version.

Note: Merge1 6.0 does not support MS Exchange Server targets as it did in previous versions, however, an EWS server may be used as an alternative. For more information see the Upgrade Wizard.

You can acquire the username and password of the administrator account on the host machine.

It is important to make a note of the address and authentication parameters of the SQL server that will host Merge1's databases.

Acquire an SSL certificate (please see Creating a Self-Signed Certificate in the Appendices)

SERVICE ACCOUNT PERMISSIONS

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

- Local Administrator
- Log on as Service rights
- Batch log on rights

PREINSTALLATION STEPS

INSTALLING INTERNET INFORMATION SERVICES

ON WINDOWS

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 and verify that the web server components listed below are enabled.

4. Click OK.

- Web Management Tools
 - IIS 6 Management Compatibility
 - IIS Metabase and IIS 6 configuration compatibility
 - IIS Management Console
 - IIS Management Scripts and Tools
 - IIS Management Service
- World Wide Web Services
 - Application Development Features
 - All .NET Extensibility Components
 - ISAPI Extensions
 - ISAPI Filters
- Security
 - Basic Authentication
 - Request Filtering
 - Windows Authentication

PREINSTALLATION STEPS

INSTALLING INTERNET INFORMATION SERVICES

ON WINDOWS SERVER

1. Click Start > Administrative Tools > Server Manager.

2. On the left panel of the Server Manager dialog box, click Roles.

- If IIS has not been enabled, click Add Roles on the Roles Summary panel. Click Next and enable Web Server (IIS) in the list. Then, click Next and select Role Services in the left panel.
- 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.

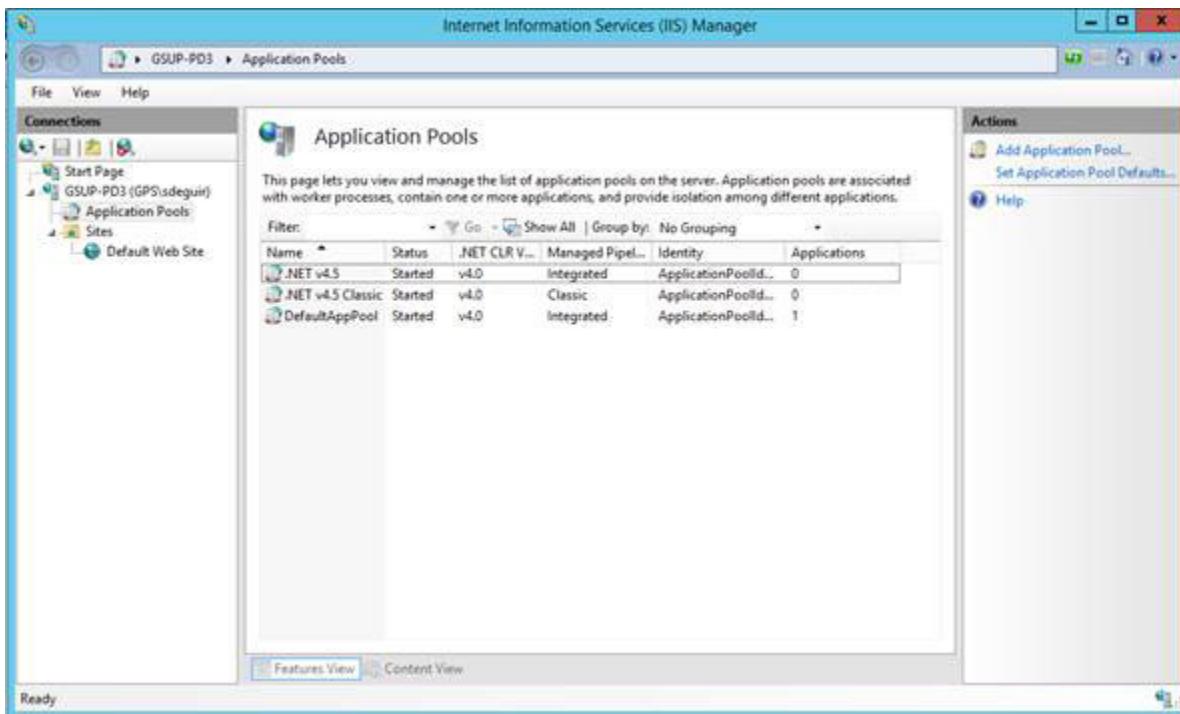
4. After enabling the required IIS components, click Next > Install.

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

PREINSTALLATION STEPS

VERIFYING .NET FRAMEWORK REQUIREMENTS

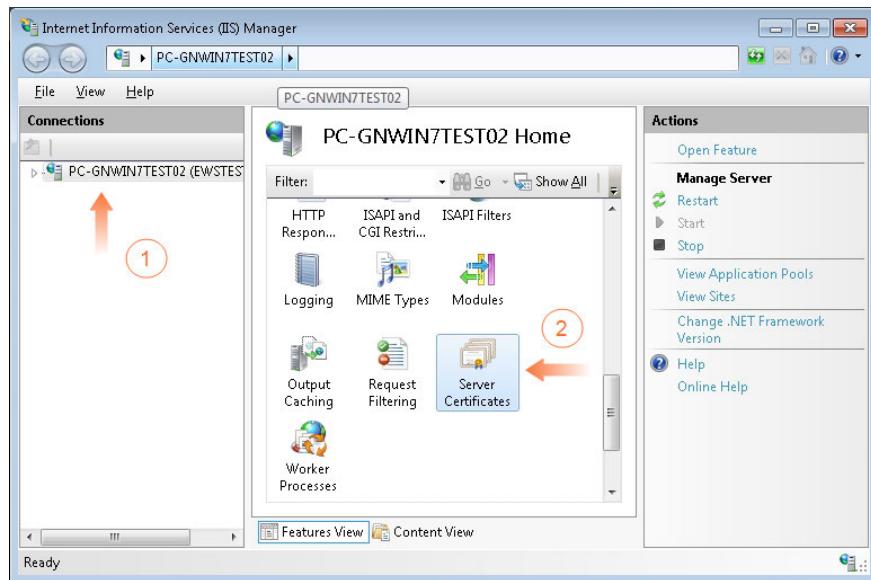
Internet Information Services must be installed prior to installing .NET Framework 4.7.2 in order for all the necessary framework components to be installed. Application pools can be viewed in IIS Manager (see image below). If the .NET v4.7.2 and .NET v4.7.2 Classic application pools do not appear in the list, please reinstall or repair .NET Framework 4.7.2 after installing Internet Information Services.



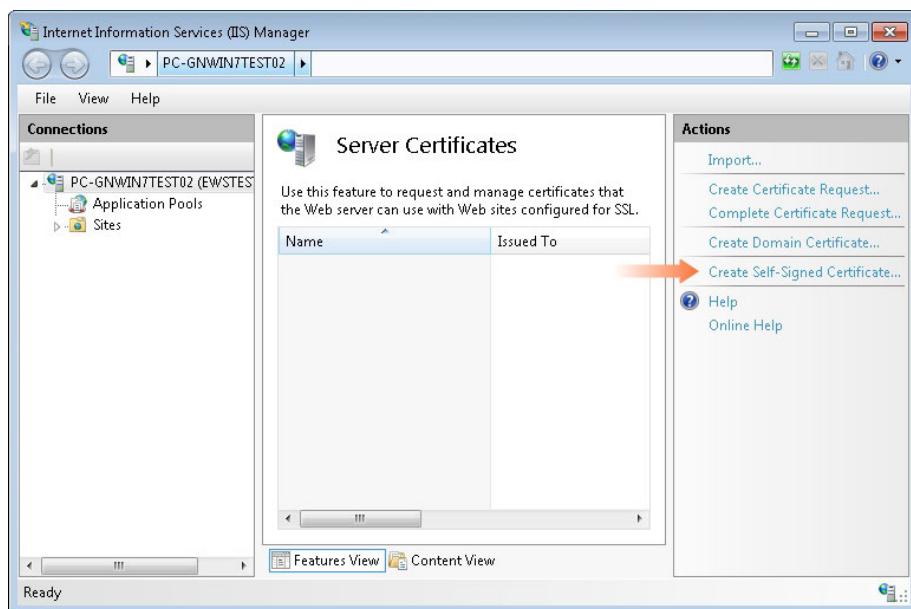
PREINSTALLATION STEPS

CREATING SELF-SIGNED CERTIFICATE

1. In Internet Information Services (IIS) Manager, click on the name of the host machine in the Connections the column on the left (1), then double-click on Server Certificates (2).

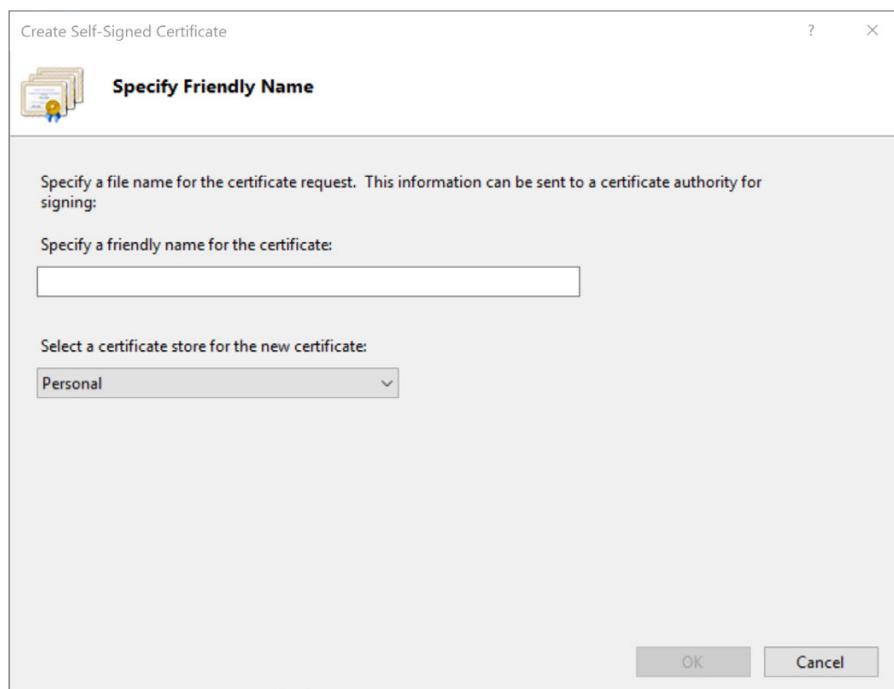


2. In the Actions column to the right, click Create Self-Signed Certificate.

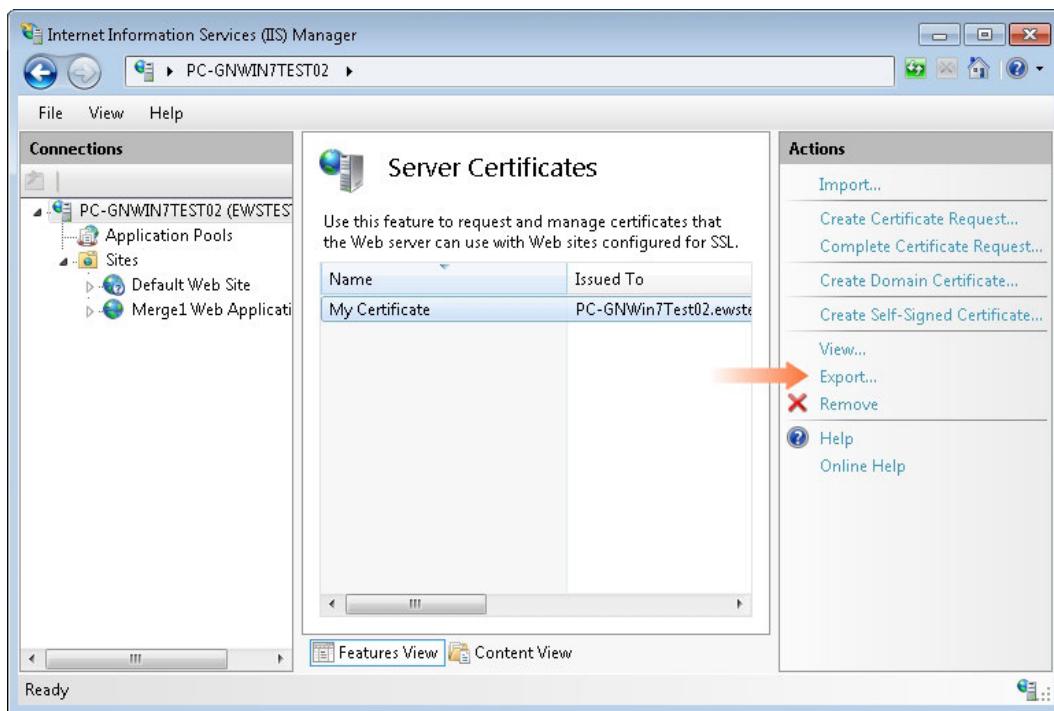


PREINSTALLATION STEPS

3. Enter a name and click OK.



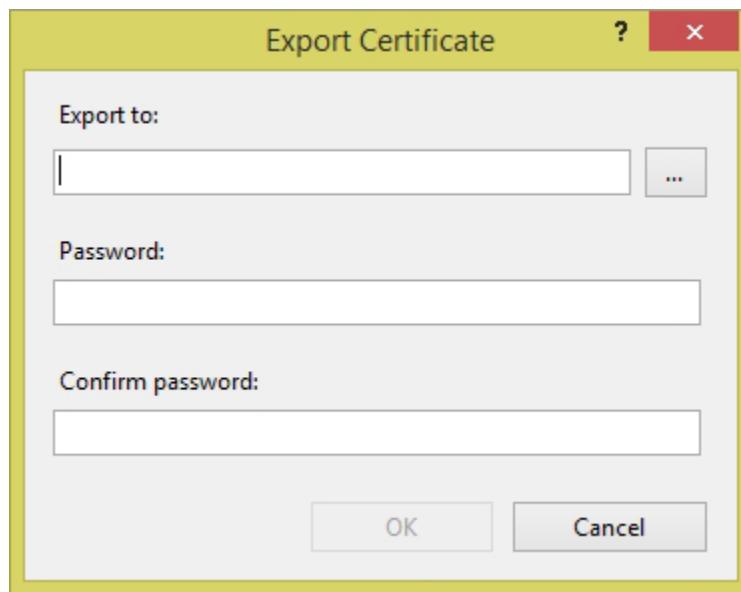
4. Select your certificate from the list and click Export in the Actions column to the right.



PREINSTALLATION STEPS

CREATING SELF-SIGNED CERTIFICATE

5. Specify an export location and password, then click Ok. The certificate location and password must be specified when installing Merge1.

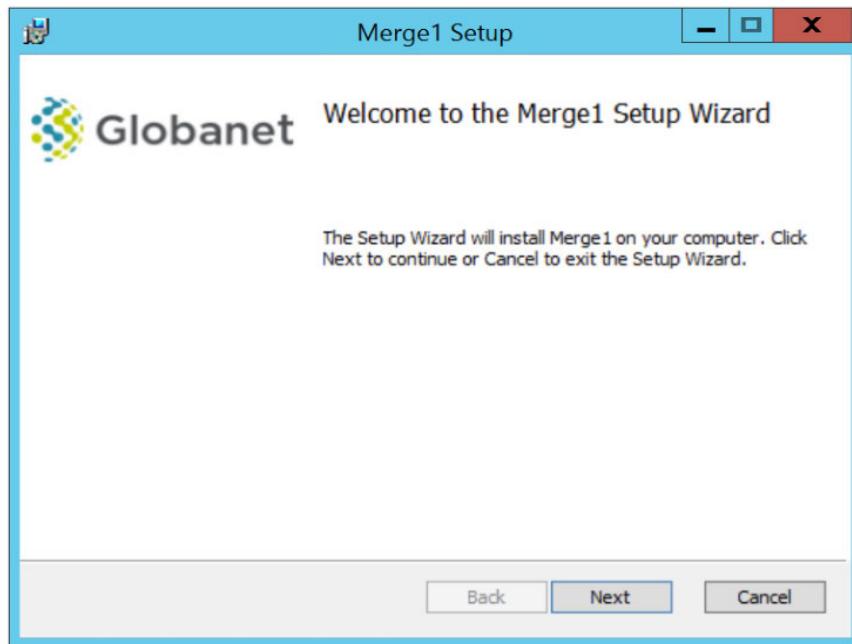


INSTALLATION

NOTE

Uninstall all previous versions of Merge1 (including Merge1 5.x and earlier versions) before attempting to install version 6.20.0131

1. Run the installer with administrator permissions and click Next.

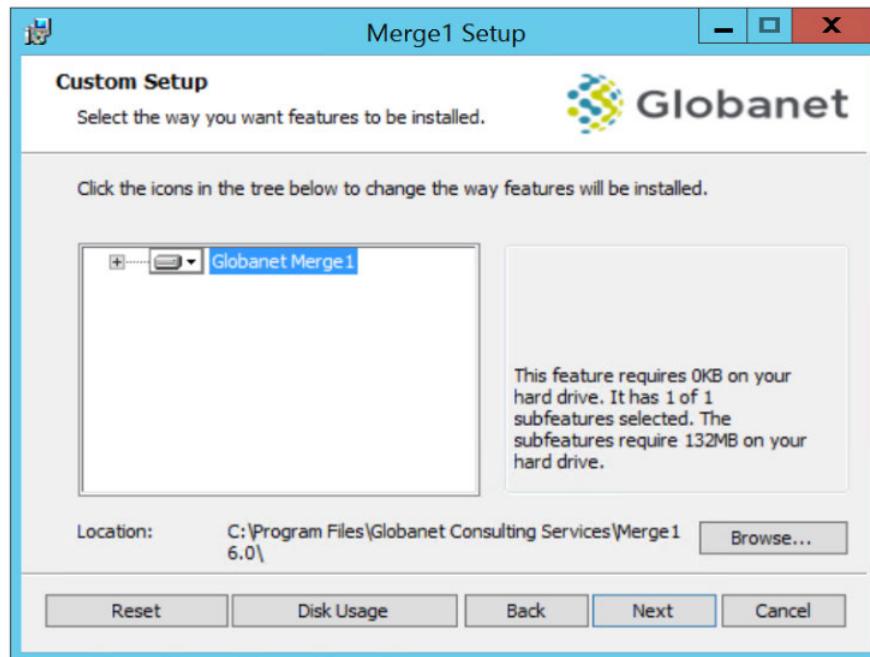


2. Read and accept the License Agreement.



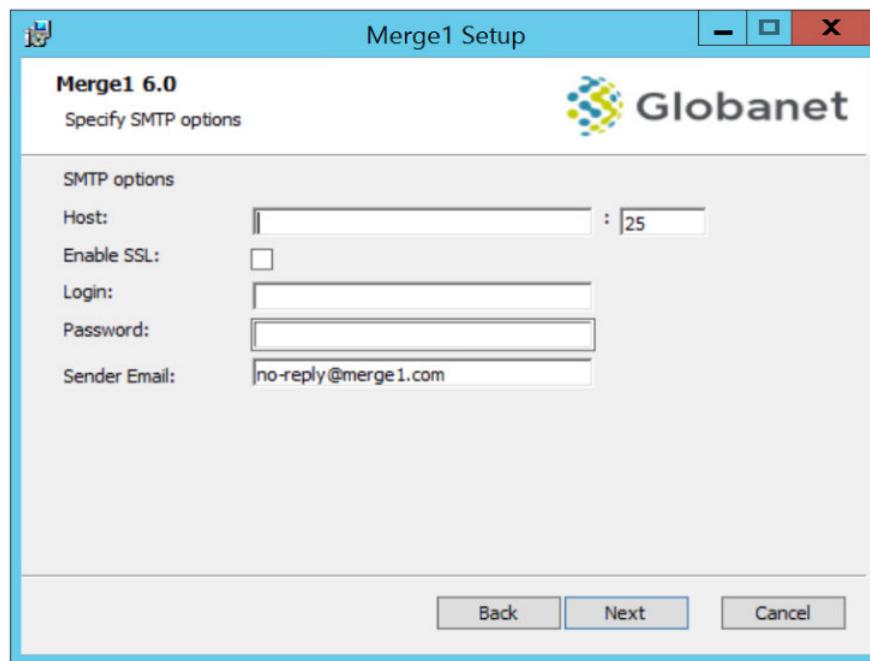
INSTALLATION

3. Select which features you would like to install.*



4. Specify an SMTP host.

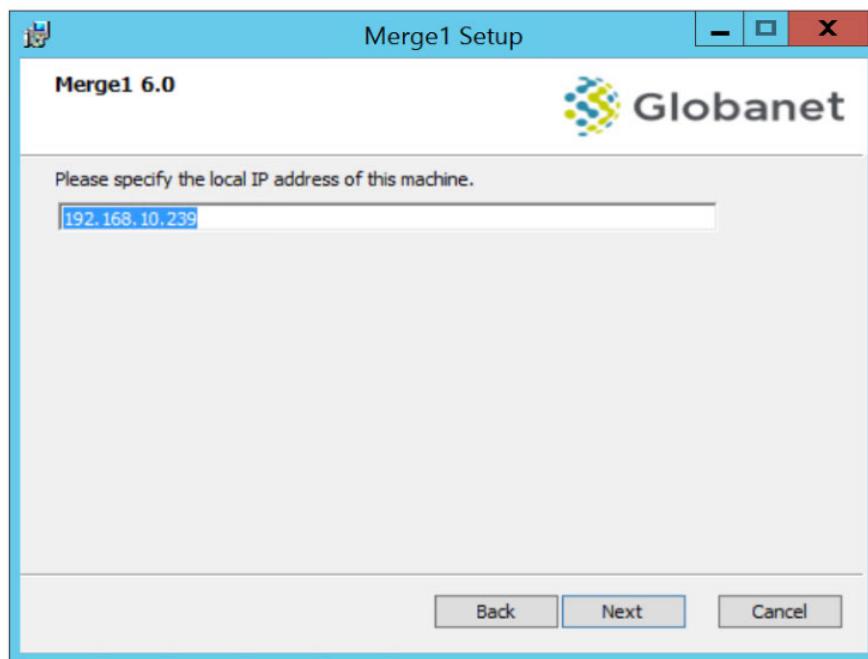
The Sender Email will appear in the From field when confirmation mail is sent to new users or when passwords are reset.



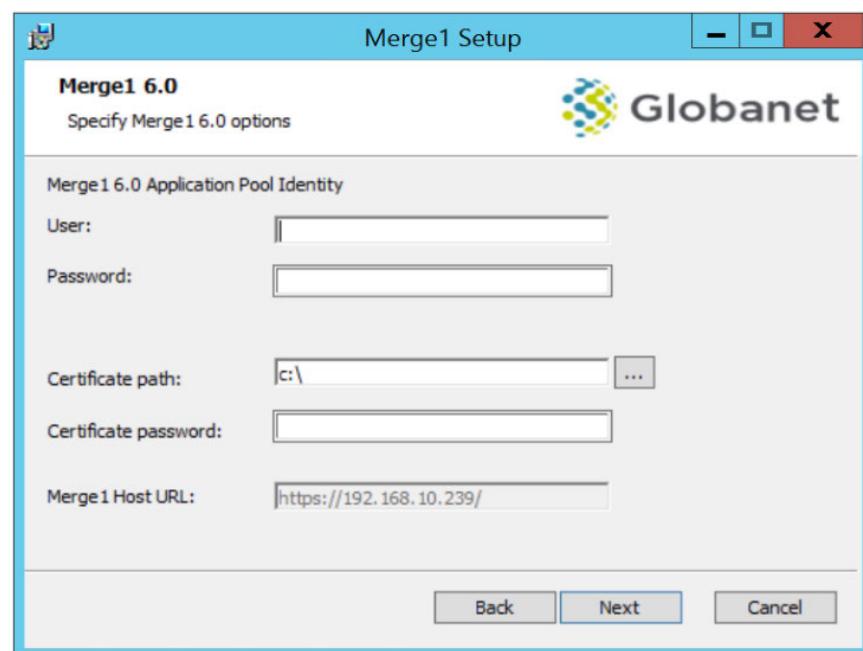
* There are no optional features in version 6.20.0131

INSTALLATION

5. Merge1 will automatically fetch the Host IP, then click **Next**.



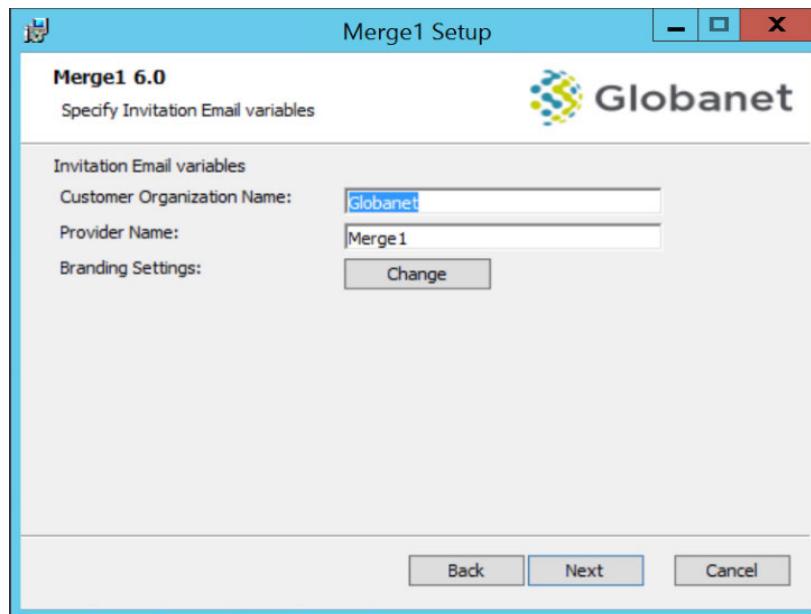
6. Enter the username & password of the administrator account of the host machine and specify a file path & password for an SSL certificate. Make a note of the **Host URL**, this URL is needed to access the Merge1 platform, click **Next**



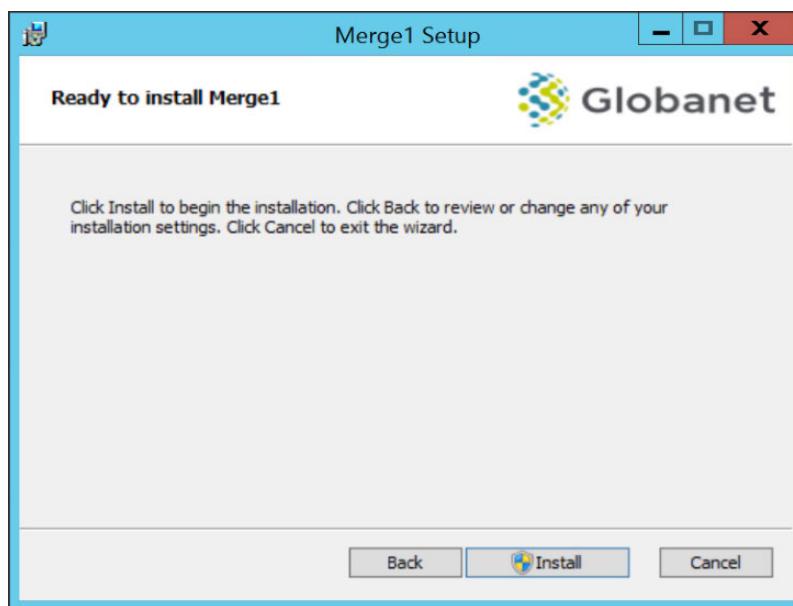
INSTALLATION

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

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



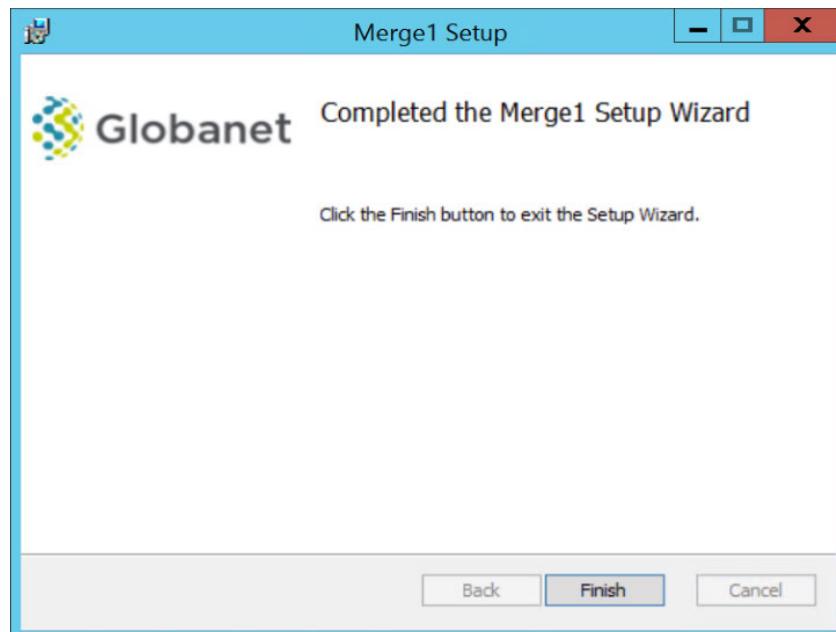
8. Click **Install** to begin the installation.



INSTALLATION

9. After the installation is complete, click Finish to exit the wizard.

Congratulations! You have successfully installed Merge1.



Please note:

You will have a 10-day free trial license period after the installation. Once the 10 days pass, contact us to prolong the license.

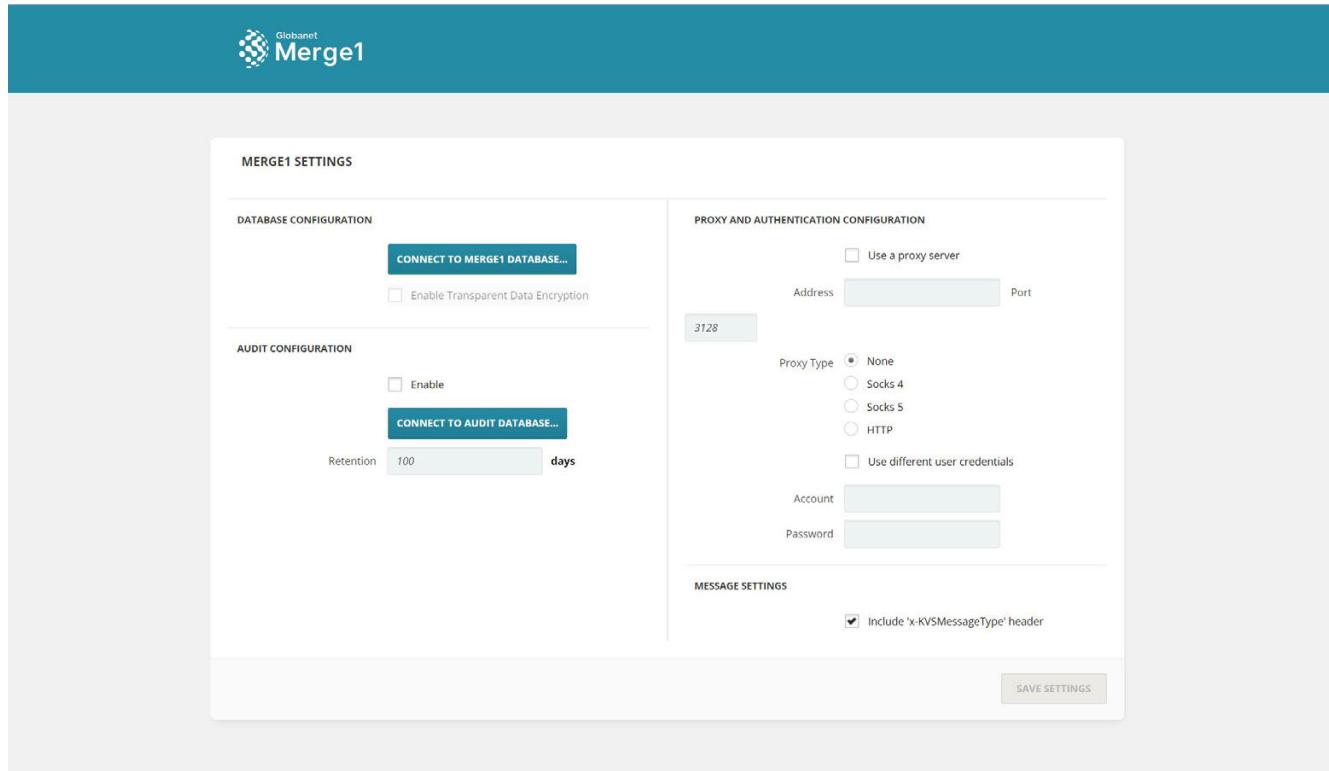
DATABASE CONFIGURATION

- Use the shortcut in the Start Menu to access the Merge1 portal or to navigate to the URL from the installation wizard (step 6) using a web browser of your choice. Merge1's configuration settings will appear.

Most browsers will display a security warning when a self-signed certificate is in use, this can be avoided by adding the certificate to the computer's list of Trusted Root Certification Authorities.

NOTE

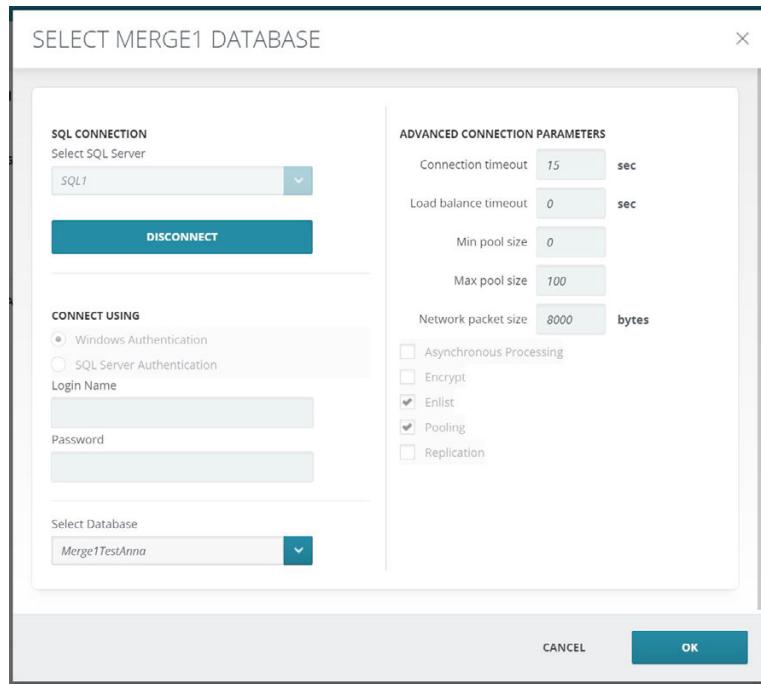
Never attempt to access or administer Merge1 using **localhost** in place of the URL, callback functions will not work properly and critical errors may occur.



To access Merge1 platform, let's start with Database Configuration. Click "**Connect to Merge1 Database**" button.

DATABASE CONFIGURATION

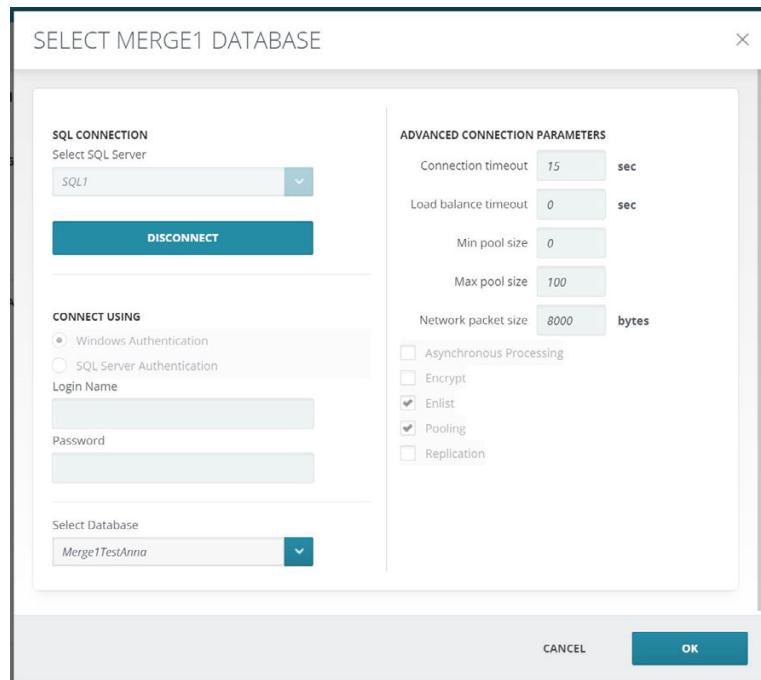
1. Select an SQL server using the drop-down menu or enter one in the same field.



2. Choose between **Windows** or **SQL Server Authentication** and enter the login & password.

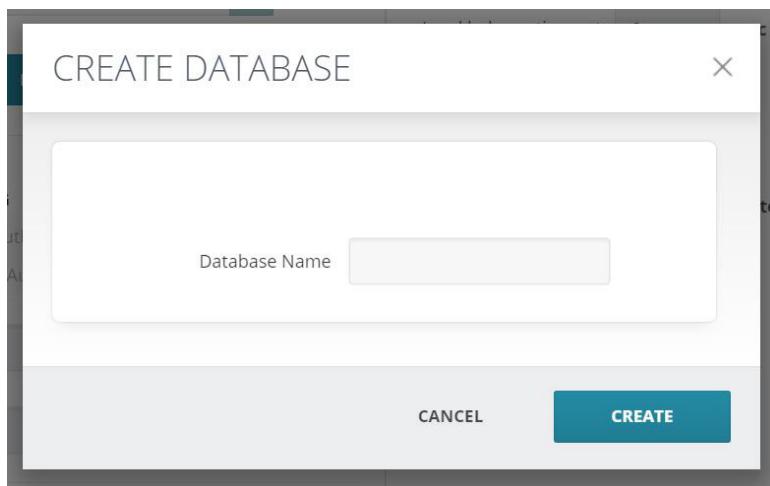
Note: When Windows Authentication is selected, Login Name and Password fields will be disabled because the credentials entered in step 6 (page 14) of INSTALLATION will be used.

3. Once you click **Connect**, the **Select Database** drop-down menu will become active.



DATABASE CONFIGURATION

4. Then, select **Create New** from the drop-down menu, a prompt will appear. Specify a name for the database and click **Create**, then click **OK**.



After configuring a database, click **Save Settings**.

Congratulations! You have successfully configured Merge1 Database. Now you will automatically be redirected to the **Merge1 Login Screen**.

AUDIT CONFIGURATION

Audit Database is used to log the activity performed in Merge1 UI, such as logging in, setting up a connector, running an import, etc.

To set up the Audit Database, click **Connect to Audit Database** and fill in the database information as shown in the previous steps.

Make sure that the **Enable** option is checked to record the audit logs in the database.

The Audit logs can be checked in the Reports section, by selecting **Audits** in the **Report Type** dropdown menu.

SIGNING IN

To sign in use the Start Menu shortcut to access the Merge1 portal.

Select the method to sign in:

- Merge1 Authentication. Use following credentials to enter Merge1:

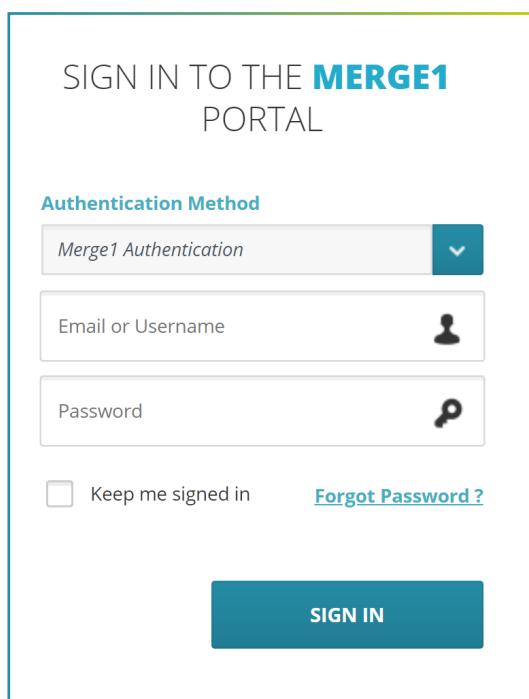
Email: **admin@merge1.com**

Password: **a**

- Windows Authentication. Enter using Windows Account Credentials.

This is the recommended option, as Merge1 Authentication will be discontinued in the future.

For the Windows Authentication use the SAM account name in the Username field.



The image shows a screenshot of the Merge1 Sign In Portal. The page title is "SIGN IN TO THE **MERGE1** PORTAL". Below the title, there is a section titled "Authentication Method" with a dropdown menu set to "Merge1 Authentication". There are two input fields: "Email or Username" and "Password", each with a corresponding icon (person and key). Below these fields are two buttons: a checkbox labeled "Keep me signed in" and a link "Forgot Password ?". At the bottom of the form is a large blue "SIGN IN" button.

Please note:

For new Merge1 installation, log in using admin@merge1.com and configure Windows Authentication administrator account from the User Profiles for the next logins.

LICENSE ACTIVATION

Upon logging in for the first time, navigate to the Licensing page for licensing.

Licenses are distributed for Sources and Target types individually. The **Activation Request Code** must be sent to support@globanet.com to activate a component(s) for use.

- Enter your **Activation Code** and click **Update**.

LICENSE DETAILS
Merge1 has a per-component licensing system for Connectors and Targets.

License Status: **Valid**

Merge1 Version: **6.18.0130**

Expiration date/time: **Permanent.**

Activation Request Code: **97D9-1CDA-E978-8000-0A1B-01D4-B1C**

Enter Activation Code: **UPDATE**

NAME	LICENSE COUNT	USER COUNT	LICENSE END DATE
Jive Connector	Unlimited	0	Never
Blackberry Connector	-	-	Never
Bloomberg Connector	-	-	Never
Symphony Connector	-	-	Never
EML Connector	-	-	Never

03

NAVIGATING MERGE1

- The Navigation Pane
- Account Settings

NAVIGATION PANE

The UI of Merge1 consists of two parts: Main screen and Navigation Pane.

The **Navigation Pane** is located on the left side of your screen. You can easily switch between the different sub-pages of the software through the Pane. Merge1 Navigation Pane consists of the following shortcuts: **Dashboard, Configuration, User Profiles, Reports, Settings, Branding Settings, and Administration.**

Dashboard

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

Configuration

Under Configuration, you can connect or remove company relevant Importers, configure targets and set filters.

User Profiles

The User Profiles allow you to view the basic information of all the users who are allowed to login the company's Merge1 account.

Reports

Reports lets you pull Export Optin and Audit reports of each connector in a PDF or CSV format. This feature also allows you to review failed messages and export them.

Settings

Merge1's settings give the user the capability to view and/or customize the database, audit, proxy and authentication configurations, as well as manage Message settings.

Branding Settings

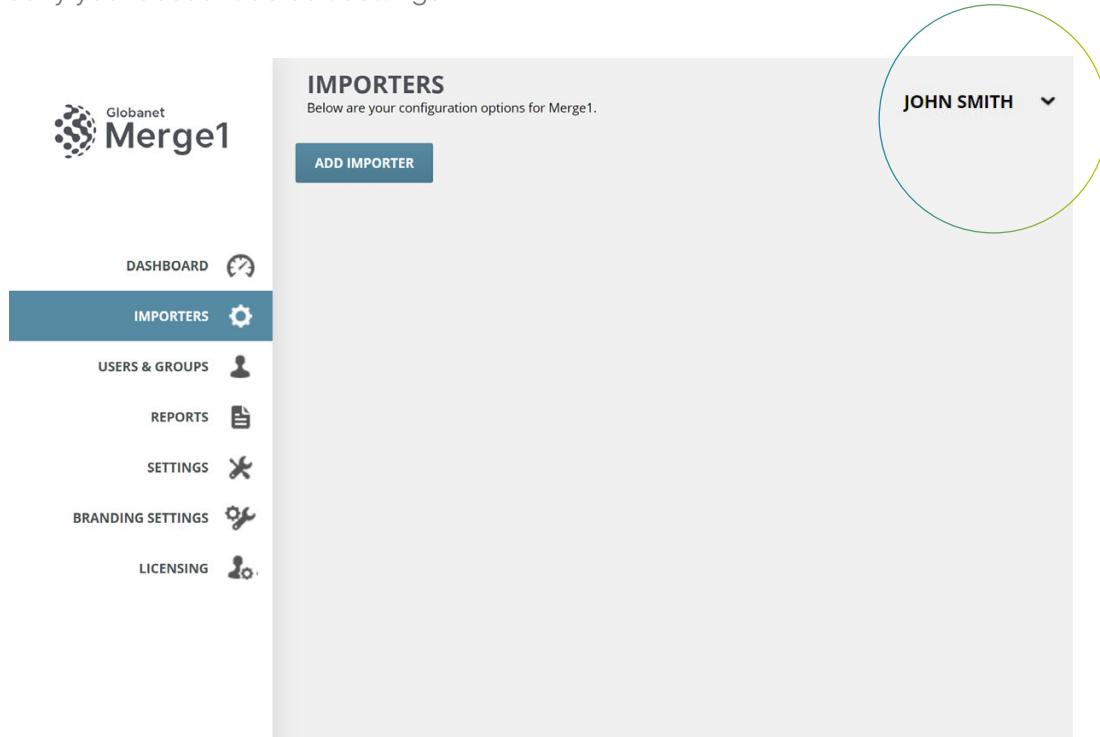
Make Merge1 your own! You have full control to change the overall look (Logo and colors) based on your company branding policies.

Administration

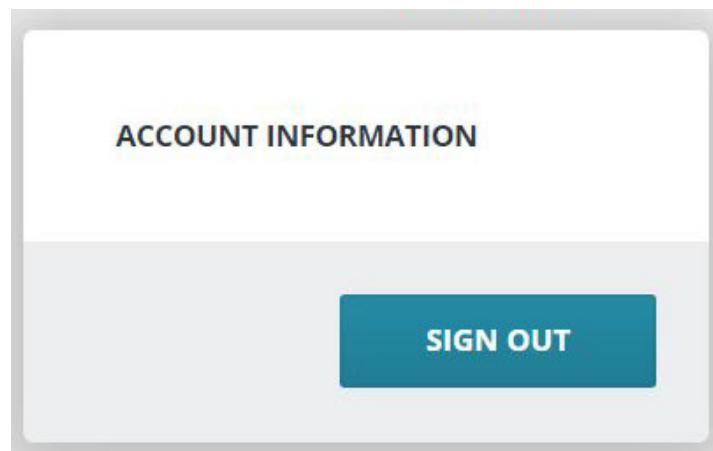
With the Administration button you can activate a license, view the version of your Merge1. You can also find the Merge1 Database upgrade wizard in this section.

ACCOUNT SETTINGS

On the top right corner of the Main Screen you can find your Account Settings which allow you to modify your account default settings.



To view your user Account Settings click on the arrow next to your username and then click Account Information.



ACCOUNT SETTINGS

In your Account Settings page, you can modify your default User Information, as well as change your password configurations. The following settings refer solely to your personal account and have no connection with general Merge1 Settings.

The screenshot shows the 'ACCOUNT INFORMATION' page. On the left, there's a sidebar with navigation links: DASHBOARD, IMPORTERS, USERS & GROUPS, REPORTS, SETTINGS, BRANDING SETTINGS, and LICENSING. The main area has a header 'ACCOUNT INFORMATION' and a dropdown 'JOHN SMITH'. It's divided into two sections: 'USER INFORMATION' and 'CHANGE PASSWORD'. The 'USER INFORMATION' section contains fields for First Name (John), Last Name (Smith), E-mail Address (admin@merge1.com), Phone Number, and Mobile Number. The 'CHANGE PASSWORD' section contains fields for Old Password, New Password, and Re-type. Each section has a 'SAVE' button at the bottom.

The Account Information screen consists of two parts: User Information and the Change Password Screen. User Information allows you to change your profile: first name, last name, email address, phone numbers.

CHANGE E-MAIL ADDRESS

1. Enter the new e-mail address in the E-mail Address field.
2. Click on Save under the User Information section. An email will be sent to the new e-mail address for confirmation.
3. Confirm the email change from the e-mail you received on the new address.

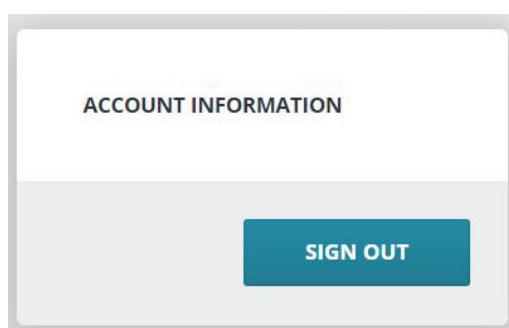
CHANGE PASSWORD

1. Enter the current password in the Old Password field.
2. Enter the new password in the New Password field.
3. Repeat the new password in the Re-type field.
4. Click on Save under the Change Password section..

Once you have made all the relevant changes, click **Save** and all the fields will be saved.

Please take note that your account information will be visible to everyone on your company's Merge1 account.

To log out from your Merge1 Account, click on the arrow next to your username and then click Sign Out Button.



04

DASHBOARD

DASHBOARD

The Merge1 Dashboard provides interactive visual modules that represent statistical and logical information about your Merge1 activity. You can download the information in PDF, JPG, PNG or SVG formats.

DASHBOARD

Below are some quick metrics regarding your Merge1 activity.

JOHN SMITH ▾

IMPORTER JOBS

DATE	IMPORTER	QUARANTINED SOURCES	IMPORTED MESSAGES	FAILED MESSAGES
08/21/2019	BoxCom Importer	0	54	0
07/18/2019	Text-Delimited Importer	0	0	0
07/18/2019	Text-Delimited Importer	0	1	0
07/18/2019	EWS Importer	0	4	0
07/18/2019	EWS Importer	0	4	0
07/18/2019	EWS Importer	0	0	0
07/18/2019	EWS Importer	0	0	0
07/12/2019	IceChat Importer	0	8	0
06/25/2019	IceChat Importer	0	8	0

« | < 1 > | » 20 items per page 1 - 11 OF 11 ITEMS

MONITORED USERS BY SOURCE TODAY

NO DATA TO DISPLAY

MESSAGES PROCESSED BY MERGE1 OVER LAST 7 DAYS

Messages

0

9/17 9/18 9/19 9/20 9/21 9/22 9/23

Imported Excluded Failed

NUMBER OF MESSAGES BY IMPORTER OVER LAST 7 DAYS

NO DATA TO DISPLAY

DASHBOARD

Merge1 Dashboard consists of four screens:

- **Importer Jobs**

In this section the history of the Merge1 runs is shown with the breakdown of quarantined sources, imported messages, and failed messages.

- **Monitored Users by Source**

In this screen you can view the number of the users for each source.

- **Messages Processed by Merge1**

The following module provides information on Imported, Excluded and Failed attempts.
The chart populates information from the last 7 days.

- **Number of Message per Importer**

Here you can find a pie chart that displays the total number of messages processed by Merge1 per source.



05

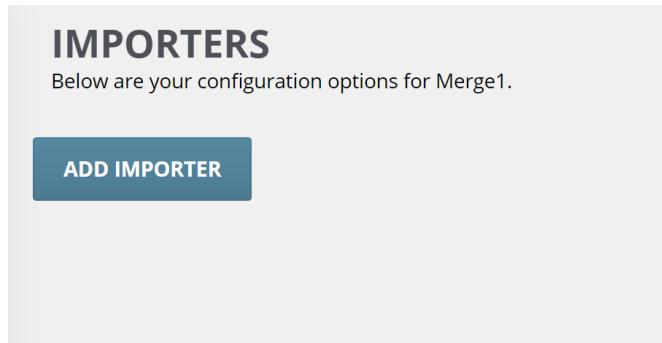
IMPORTERS

- The Configuration Wizard
- Monitored Users
- Filters
- Targets
- Importer Settings

IMPORTERS

The Configuration button in the Navigation Pane allows you to connect or remove company relevant Importers, configure targets and set filters.

You will find the Add Importer button on the top left corner of the screen:



If you already have configured Importers, you will see them in separate Importer Cards.

A screenshot of the Merge1 application showing a specific importer configuration. The card is titled 'BLOOMBERG IMPORTER' with a status of 'Stopped'. It includes sections for 'SOURCE' (Bloomberg logo), 'MONITORED USERS' (NOT APPLICABLE), and 'FILTERS & TARGETS' (Default target, Not Configured). Below this is an 'IMPORTER SETTINGS' section with tables for Service Account (LocalSystem), Schedule (Run Once), Logging Level (File: Info | Event: Error), Custom Headers (Not Configured), and Reporting Settings (Summary Report Only). Buttons for 'EDIT' and 'DELETE DATA' are at the bottom.

- Clone option copies the importer with all the configured settings.
- Edit option allows editing the settings of the connector.
- Rename option allows changing the name and the description of the importer.
- Delete option deletes the importer.

IMPORTERS

IMPORTER PANELS

When integrating an Importer, the Importer Panel is added to the Configuration Screen. Each Importer Panel consists of four static blocks:

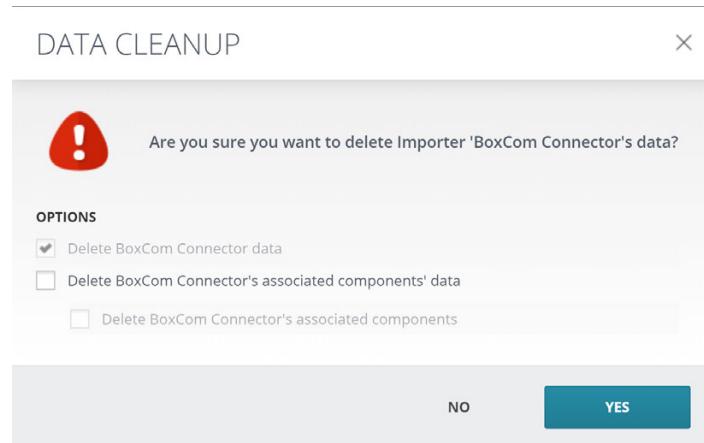
- Source, where you can find the name of the importer as well as edit it.
If you click on Source Block Configuration you will find a detailed explanation of the Source block and its configurations.
- Monitored Users, this is where you can find information about all the users of the connector monitors. The Monitored Users Block Configuration will give the user a better understanding of this block and its configurations.
- Filters and Targets, allow users to set up where the connector information is sent to.
- Importer Settings is where you can change all the importer configurations.
If you want to get more information on how to setup configurations click Importer Settings.

On the top part, next to the Importer name, you can see the Green button. This button is used to run or stop the importer.

- Drag Importer panels to re-arrange their order in the Merge1 UI.
- Double-click on the top part of the Importer panel and the Importer will collapse. These changes are specific to each Merge1 user.

CONNECTOR HISTORY DELETION

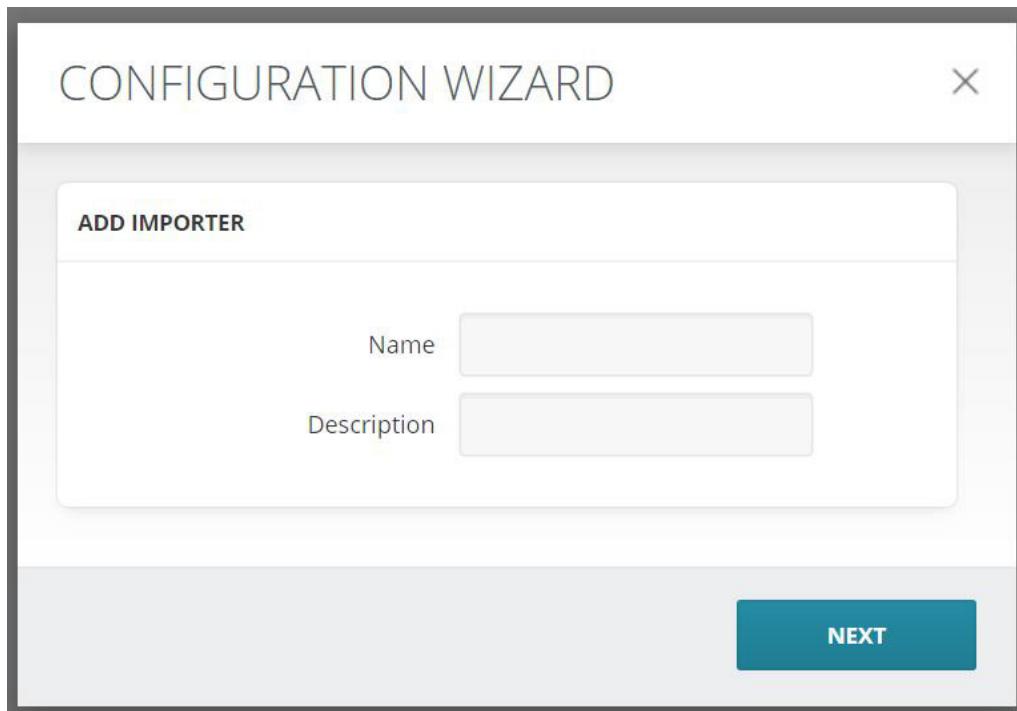
There are two ways of deleting the connector history. First one is to use **Delete Data** option under Source section. This removes all connector data history from the previous runs and processed data. Second way is to select **Delete Data** under Importer Settings. It will make a pop-up appear. It also removes all connector data history from the previous runs. However, if the **Delete "Connector Name"'s associated components' data** option is checked, all the failed messages and failed sessions are deleted from the database as well.



CONFIGURATION WIZARD

In this section, we will be providing detailed information on how to Add Importers through the Configuration Wizard. You can find the Wizard under the Configurations in the Navigation Pane.

As a first time user, you will see a fully blank page when clicking on the Configuration. On the top right corner you will see an orange button, click on the button and the Wizard will launch.



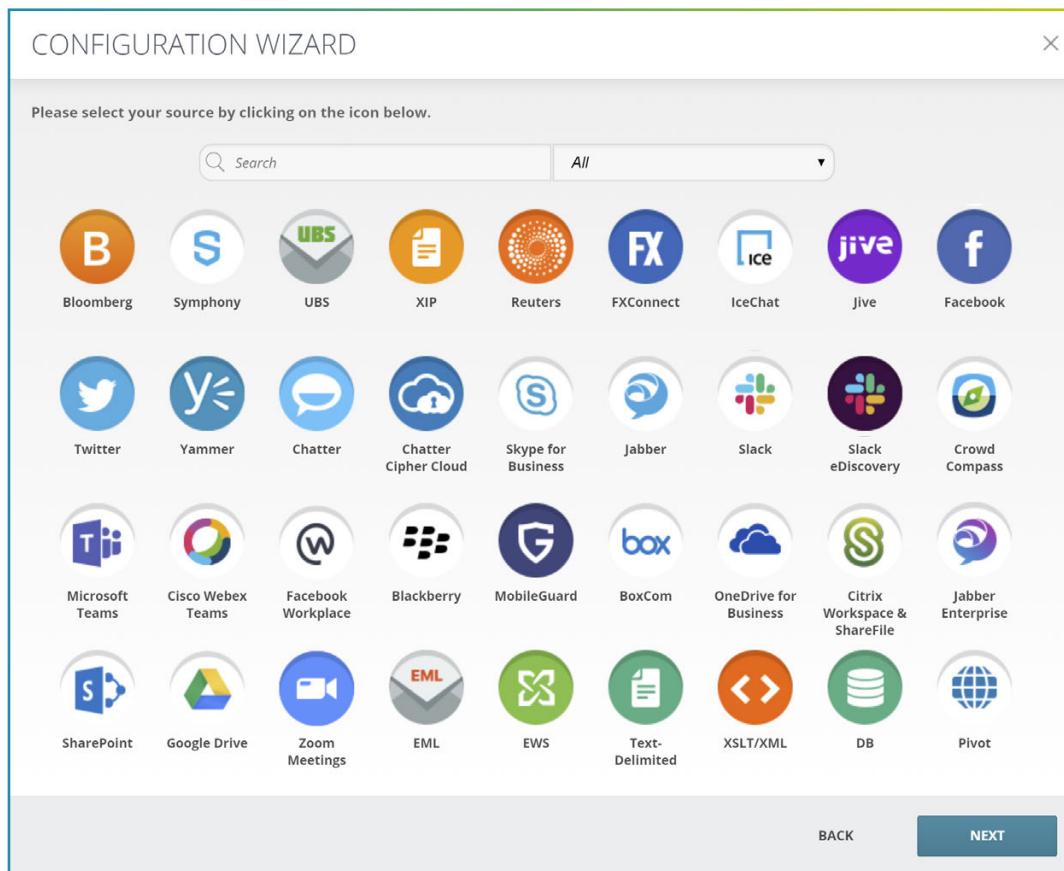
1. When the Wizard launches you will see a small screen where you will be asked to fill in the Importer name and description. This information will later be displayed on the Importers page.
2. Once you have filled in all the relevant information, click **Next**.

CONFIGURATION WIZARD

3. In the next screen, you will be prompted to choose the Source you want to import.

In order to make the search easier, we have grouped all the Importers based on their types:

- Financial Platforms
- Enterprise Social
- Social Media
- Mobile
- Enterprise tools and file sharing
- Custom



If you are not sure where to look for the exact Connector, next to the drop-down menu you will find a search bar. Simply type the connector name and it will show up.

CONFIGURATION WIZARD

4. Select the Importer, click **Next** and the Importer Configuration Wizard will open.

The screen consists of 5 tabs:

- Source
- Monitored Users
- Filters
- Targets
- Settings

CONFIGURATION WIZARD

SOURCE **MONITORED USERS** **FILTERS** **TARGETS** **SETTINGS**

Please provide your Bloomberg configuration data so that Merge1 can access your Bloomberg data.

FTP

Download files from FTP

FTP CONFIGURATION OPTIONS +

Execute script against source files

Script file * UPLOAD

PGP

Use PGP Decryption

PGP DECRYPTION OPTIONS +

ATTACHMENT VALIDATION

Replace all attachments with the following note:
This message contained the following attachments w/

Replace missing attachments with the following note:
This message contained the following attachments th

Fail messages with missing attachments. (default)

DISCLAIMER VALIDATION

Replace all disclaimers with the following note:
This message contained the following disclaimer but i

Replace missing disclaimers with the following note:
This message contained the following disclaimer that

BACK NEXT

5. When you fill in all the information as prompted by the Configuration Wizard, your Importer will be generated. Now you can view the importer under the Configuration Screen.

IMPORTERS

In Merge1 you can collect data from an array of e-communication media, which are known as Sources. Please view all the Sources of Merge1 version 6.20.0131 below. If you are interested in the specific Source, please click on it and you will be redirected to the relevant Source setup configurations page.

Enterprise Social



Jive



Facebook



Twitter



Yammer



Chatter

Chatter
Cipher CloudCrowd
Compass

Workplace

Mobile



Blackberry



Jabber

Skype for
Business

Slack

Slack
eDiscoveryMicrosoft
TeamsCisco
Webex Teams

Sharepoint



MobileGuard

Financial Platforms



Bloomberg



Symphony



UBS



XIP



BoxCom

OneDrive for
Business

Google Drive



Reuters



FXConnect



IceChat

Citrix Workspace
& ShareFileJabber
Enterprise

Other



EML



EWS

Text-
Delimited

XSLT/XML



DB



Pivot



Web Page

We are constantly updating Sources. If you cannot find the one required for your team, please contact Globanet Support team and send us your request.

BLOOMBERG



Bloomberg

ABOUT BLOOMBERG

Bloomberg delivers business and markets news, data, analysis, and video to the world, featuring stories from Businessweek and Bloomberg News.

Bloomberg Vault is a hosted end-to-end information management service that delivers compliance and IT solutions by leveraging the scalability and reliability of Bloomberg's global infrastructure. It provides secure digital storage for corporate clients of Bloomberg, primarily email and messaging content.

Merge1 imports and processes the following types of files from Bloomberg:

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

HOW TO SET UP THE BLOOMBERG IMPORTER

After selecting the Bloomberg icon in the Configuration Wizard and clicking **Next**, you will be redirected to the next screen of the Configuration. As mentioned earlier the Configuration Wizard Screen consists of 5 tabs. You will be prompted to start with Source Configuration.

The Bloomberg Source Configuration Screen has the following Bloomberg options (click on the name to open the relevant configuration information):

- FTP configurations
- PGP configurations
- Folders (required)
- Attachment Validation
- Disclaimer Validation
- Bloomberg Option
- Primary Address
- Misc Settings

SOURCES



Bloomberg

BLOOMBERG SFTP CONFIGURATIONS

Merge1 retrieves data from Bloomberg via **FTP** and stores it in the Import Folder for processing. Corrupt files are moved to the Quarantine Folder.

Please note that when SFTP is disabled, Merge1 attempts to retrieve the data directly from the Import Folder. This is useful when data is already in-hand or if the user wishes to acquire the data manually.

If you want to get data from Bloomberg through SFTP, check the **Download files from FTP box**. The SFTP Configuration options will automatically open.

SSH KEY AUTHENTICATION

The screenshot shows the 'SFTP Configuration Options' window with a yellow border. It includes sections for 'Use SSH Key Authentication' (checkbox), 'Connection' (Host: ftpcom.bloomberg.com, Port: 30206, Path: /), 'Authentication' (Username field, TEST CONNECTION button), 'Generate Keys' (Public Key field, GENERATE KEYS button), and 'Private Key' (Export/Import Private Key buttons: EXPORT PRIVATE KEY, IMPORT PRIVATE KEY).

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

2. Connection. 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 Bloomberg is 30206.

3. Authentication. Enter the username provided by Bloomberg and hit "Generate". The generated key must be provided to Bloomberg under the "Public Keys" tab at CCNS <Go>.

SOURCES



Bloomberg

BLOOMBERG SFTP CONFIGURATIONS

The screenshot shows the Bloomberg SFTP configuration interface. It is divided into several sections with numbered callouts:

- 1. CONNECTION:** Host: ftpcorn.bloomberg.com, Port: 30206, Path: /
- 2. AUTHENTICATION:** Anonymous Access selected.
- 3. FILE FILTER:** Include selected, filter: *
- 4. FILTER BY TIME:** None selected, Only download files modified within the last: 1 days
- 5. OPTIONS:** Maintain history of downloaded file for 5 days (0 = infinite), Download subdirectories recursively selected, Delete files on server after downloading selected

1. Connection. Enter the hostname of the remote SFTP server and the folder path in the Host and Path text boxes, respectively. The default port is 21. Choose SFTP connection type from the Connection type dropdown list. SFTP can run in either passive or active mode. Information about the connection type should be provided by the SFTP host. If you wish to use SFTP over SSL, select **Use SSL** check box and choose connection method: implicit or explicit.

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

3. File Filter. This filter is used to 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. This filter is used for separating 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 modified 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 time period.
- Server Time Zone specifies the time zone in which the SFTP sever is located to correctly determine the time stamp of downloadable files.

5. Options.

- Maintain history of downloaded file for X days. 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.

SOURCES



Bloomberg

USING SCRIPT AGAINST FILES

Execute script against source files allows the user to utilize alternative methods data download or acquisition methods other than SFTP. For example, batch script files that download information via an SFTP alternative and move it into the appropriate processing folder. The uploaded script files can also be downloaded.

The screenshot shows a 'FTP' configuration window. At the top is a checkbox for 'Download files from FTP'. Below it is a section titled 'FTP CONFIGURATION OPTIONS' with a '+' icon. Underneath is another checkbox for 'Execute script against source files'. This section contains a 'Script file *' input field, an 'UPLOAD' button, and a 'DOWNLOAD' button. The entire window is enclosed in a green border.

USING PGP CONFIGURATIONS

The screenshot shows a 'PGP' configuration window. At the top is a checkbox for 'Use PGP Decryption'. Below it is a section titled 'PGP DECRYPTION OPTIONS' with a '-' icon. This section contains fields for 'Username *', 'Password *', and 'Email *'. To the right of these fields is a 'GENERATE KEY' button. Further down is a 'Generated Public Key *' field with a 'EXPORT PUBLIC KEY' button to its right. At the bottom are two buttons: 'EXPORT PRIVATE KEY' and 'IMPORT PRIVATE KEY'. The entire window is enclosed in a green border.

Starting from June 30, 2016, Bloomberg requires its clients to use PGP keypair in order to encrypt customer files on the Bloomberg SFTP server.. Instructions to enable PGP encryption are presented below.

1. Click **Use PGP Decryption** and PGP Decryption Options open.
2. Specify a Username, Password, and Email, then click **Generate Key**. Once the key is generated you will see a green tick icon. *
3. Log into your Bloomberg CCNS control panel and enable PGP encryption by adding Merge1 Keys.
4. In your Bloomberg CCNS click **Add** and the Add Public Key window will appear. From the Key Type drop-down menu, select Encryption and paste the full contents of the public key (including the block header and footer) under the Public Keys tab at CCNS<Go> in your Bloomberg terminal.

5. Click the Decryption button. (The key appears in the Public Keys section). To save the PGP encryption key to your account click **Submit**.

* Use the Export Public / Private Key buttons to save the keys to a secure location on your device. This will enable you to restore the keys if they are lost or when moving the database to a new machine.

SOURCES



Bloomberg

BLOOMBERG FOLDER CONFIGURATION (REQUIRED*)

After successfully setting up the SFTP and PGP Configurations, you will have to change the folder configurations. In Merge1 you will have to specify the Import Folder, where you would like to store the data after retrieving it from Bloomberg, as well as Quarantine Folder where all the failed messages will be archived.

If you have sub-folders under your Import Folder, you can enable **Traverse Subdirectories** to maintain the sub-folder structure of imported data and include the data in your Bloomberg Merge1.

FOLDERS	
Import folder*	
<input type="text"/>	
<input type="checkbox"/> Traverse subdirectories	
Quarantine folder*	
<input type="text"/>	
AFTER SUCCESSFULL IMPORTING	
<input checked="" type="radio"/> Move original files into a subfolder of the Import folder.	
<input type="radio"/> Delete original files permanently.	

Under **After Successfully Importing** settings you can provide Merge1 what to do with the original files. If Move original files into a subfolder is selected, the files will be moved to a folder called _Import. If Delete original files permanently is selected, the files after being processed will be deleted. Please note, that if deleted it won't be possible to recover them.

Please note:

When the SFTP is disabled, Merge1 attempts to retrieve the data directly from the Import Folder. This is useful when data is already in-hand or if the user wishes to acquire the data manually.

BLOOMBERG OPTIONS

In Merge1 you have six Bloomberg options:

▪ Use Legacy Bloomberg Importer style of data processing

Merge1 will scan the date and time stamp of dump files and assume their time zones correspond with those of the machine on which Merge1 is running

* Merge1 Folder Option 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.

SOURCES



Bloomberg

(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, meaning that the selection under Attachment Validation (such as Fail messages with missing attachments) 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, meaning that the selection under Disclaimer Validation (such as Fail messages with missing attachments) will be ignored.

If disabled, the selection under Disclaimer Validation will be applied to the messages that are missing attachments.

▪ Generate RSMF Messages

If checked, the output message will be in RSMF format. However, checking this option is not enough. The output format (RSMF) should be selected in the Folder Target configuration section.

▪ Split IB Conversations by day

If checked, messages with the same UTC day will be imported in one message.

▪ For IB: use EndTime as SentTime instead of StartTime

The SentTime in the imported mesage of IB source files will be replaced with the EndTime of the message, instead of StartTime. See examples on the next page (if Split IB Messages by day is enabled, DateTimeUTC is prioritized).

BLOOMBERG OPTIONS	
<input type="checkbox"/>	Advanced Reprocessing
<input type="checkbox"/>	Use Legacy Bloomberg Importer style of date processing
<input checked="" type="checkbox"/>	Generate RSMF Messages
<input checked="" type="checkbox"/>	Full attachment validation
<input checked="" type="checkbox"/>	Full disclaimer validation
<input type="checkbox"/>	Split IB Conversations by day
<input type="checkbox"/>	For IB: use EndTime as SentTime instead of StartTime
<input type="checkbox"/>	For MSG: exclude TO, CC and BCC data from message body

SOURCES



Bloomberg

- **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 selected, Participant Entered and Participant Left events are shown in a separate table at the bottom of the message.

Note that in the below examples the timestamps in the body message are UTC, while the SentTime of the generated output is UTC +4. The SentTime of the message is adjusted according to the timezone of the device it is opened on.

Also note, that the mapping of SentDate (10:26 PM) can be changed using the "For IB: use EndTime as SentTime instead of StartTime" checkbox.

By default SentTime of the email is shown the same as StartTime:

The screenshot shows an email message from ANTON NORMAL (ATR FUND MANAGEMENT) <ANORMAL@bloomberg.net>. The message is a CHAT-2847039-2373595-113959354479953. The recipient is QUENTIN KNAPP. The message body contains a file attachment named tradequotes.txt (3 KB). Below the message, there is a table titled 'INTERACTION TYPE' showing the following data:

INTERACTION TYPE	DATE	USER INFO	CONTENT	DEVICE TYPE
Participant Entered	03/11/2008 14:25:34	ANTON NORMAL (ATR FUND MANAGEMENT) <ANORMAL@bloomberg.net>		
Participant Invited	03/11/2008 14:25:34	QUENTIN KNAPP (SOME BIG BANK) <QKNAPP@bloomberg.net>	ANORMAL - Good morning sir...Is there anything that I should be doing for you?	M
Participant Entered	03/11/2008 14:25:37	QUENTIN KNAPP (SOME BIG BANK) <QKNAPP@bloomberg.net>		
Message	03/11/2008 14:26:06	QUENTIN KNAPP (SOME BIG BANK) <QKNAPP@bloomberg.net>	Not for now, but by the end of the next week I might start looking at floaters. I will let you know...	
Message	03/11/2008 14:31:37	QUENTIN KNAPP (SOME BIG BANK) <QKNAPP@bloomberg.net>	Not for now, but by the end of the next week I might start looking at floaters. I will let you know...	
Message	03/11/2008 17:52:27	QUENTIN KNAPP (SOME BIG BANK) <QKNAPP@bloomberg.net>	No thanks	
Participant Left	03/11/2008 22:08:00	QUENTIN KNAPP (SOME BIG BANK) <QKNAPP@bloomberg.net>		
Participant Left	03/11/2008 22:15:56	ANTON NORMAL (ATR FUND MANAGEMENT) <ANORMAL@bloomberg.net>		
Attachment	03/11/2008 21:19:22	QUENTIN KNAPP (SOME BIG BANK) <QKNAPP@bloomberg.net>	tradequotes.txt	

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

The screenshot shows an email message from ANTON NORMAL (ATR FUND MANAGEMENT) <ANORMAL@bloomberg.net>. The message is a CHAT-2847039-2373595-113959354479953. The recipient is QUENTIN KNAPP. The message body contains a file attachment named tradequotes.txt (3 KB). Below the message, there is a table titled 'INTERACTION TYPE' showing the following data:

INTERACTION TYPE	DATE	USER INFO	CONTENT	DEVICE TYPE
Participant Entered	03/11/2008 14:25:34	ANTON NORMAL (ATR FUND MANAGEMENT) <ANORMAL@bloomberg.net>		
Participant Invited	03/11/2008 14:25:34	QUENTIN KNAPP (SOME BIG BANK) <QKNAPP@bloomberg.net>	ANORMAL - Good morning sir...Is there anything that I should be doing for you?	M
Participant Entered	03/11/2008 14:25:37	QUENTIN KNAPP (SOME BIG BANK) <QKNAPP@bloomberg.net>		
Message	03/11/2008 14:26:06	QUENTIN KNAPP (SOME BIG BANK) <QKNAPP@bloomberg.net>	Not for now, but by the end of the next week I might start looking at floaters. I will let you know...	
Message	03/11/2008 14:31:37	QUENTIN KNAPP (SOME BIG BANK) <QKNAPP@bloomberg.net>	Not for now, but by the end of the next week I might start looking at floaters. I will let you know...	
Message	03/11/2008 17:52:27	QUENTIN KNAPP (SOME BIG BANK) <QKNAPP@bloomberg.net>	No thanks	
Participant Left	03/11/2008 22:08:00	QUENTIN KNAPP (SOME BIG BANK) <QKNAPP@bloomberg.net>		
Participant Left	03/11/2008 22:15:56	ANTON NORMAL (ATR FUND MANAGEMENT) <ANORMAL@bloomberg.net>		
Attachment	03/11/2008 21:19:22	QUENTIN KNAPP (SOME BIG BANK) <QKNAPP@bloomberg.net>	tradequotes.txt	

SOURCES



Bloomberg

ADVANCED REPROCESSING: ATTACHMENT VALIDATION

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

If Full Attachment Validation is enabled and **Fail Messages with missing Attachments** is selected, the following happens:

In case attachment file is either missing or corrupted, Merge1 starts processing the source files and quarantines them due to missing attachment . When running the next import, on condition that the missing attachment is available now, Merge1 successfully processes all the files. This way Merge1 processes the messages previously quarantined just like any new complete file group.

BLOOMBERG OPTIONS

- Advanced Reprocessing
- Use Legacy Bloomberg Importer style of date processing
- Full attachment validation
- Full disclaimer validation
- Split IB Messages by day
- For IB: use EndTime as SentTime instead of StartTime
- For MSG: exclude TO, CC and BCC data from message body

If Full Attachment Validation is disabled the following happens:

In case attachment file is either missing or corrupted, Merge1 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're 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 condition that the missing attachment is available now, Merge1 reprocesses the failed messages.

BLOOMBERG OPTIONS

- Advanced Reprocessing
- Use Legacy Bloomberg Importer style of date processing
- Full attachment validation
- Full disclaimer validation
- Split IB Messages by day
- For IB: use EndTime as SentTime instead of StartTime
- For MSG: exclude TO, CC and BCC data from message body

SOURCES



Bloomberg

ADVANCED REPROCESSING: DISCLAIMER VALIDATION

If 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, Merge1 starts processing the source files and quarantines them due to missing attachment . When running the next import, on condition that the missing disclaimer is available now, Merge1 successfully processes all the files. This way Merge1 processes the messages previously quarantined just like any new complete file group.

BLOOMBERG OPTIONS

- Advanced Reprocessing
- Use Legacy Bloomberg Importer style of date processing
- Full attachment validation
- Full disclaimer validation
- Split IB Messages by day
- For IB: use EndTime as SentTime instead of StartTime
- For MSG: exclude TO, CC and BCC data from message body

If Full Disclaimer Validation is disabled:

In case disclaimer file is either missing or corrupted, Merge1 starts processing the source files. The messages that have available disclaimers are processed and sent to the target. The messages that have reference to missing disclaimers are not delivered to the target, they're 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, on condition that the missing disclaimer is available now, Merge1 reprocesses the failed messages.

BLOOMBERG OPTIONS

- Advanced Reprocessing
- Use Legacy Bloomberg Importer style of date processing
- Full attachment validation
- Full disclaimer validation
- Split IB Messages by day
- For IB: use EndTime as SentTime instead of StartTime
- For MSG: exclude TO, CC and BCC data from message body

SOURCES



Bloomberg

BLOOMBERG ATTACHMENT VALIDATION

Merge1 enables you to develop customized notes for attachment validation. The default setting is **Fail Messages with missing Attachments**, as a result of which the messages that do not have attachments are failed and can be viewed under the Reports. Note that Advanced Processing shouldn't be selected for this to happen.

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.

ATTACHMENT VALIDATION

- Replace all attachments with the following note:

This message contained the following attachments w/

- Replace missing attachments with the following note:

This message contained the following attachments th/

- Fail messages with missing attachments. (default)

SOURCES



Bloomberg

BLOOMBERG DISCLAIMER VALIDATION

Merge1 enables you to develop customized notes for disclaimer validation. The default setting is **Fail Messages with missing disclaimers**, as a result of which the messages that do not have disclaimers are failed and can be viewed under the Reports. Note that Advanced Processing shouldn't be selected for this to happen.

If you select the "Replace all the 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.

DISCLAIMER VALIDATION

Replace all disclaimers with the following note:
This message contained the following disclaimer but i

Replace missing disclaimers with the following note:
This message contained the following disclaimer that

Fail messages with missing disclaimers. (default)

SOURCES



BLOOMBERG PRIMARY ADDRESS

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

PRIMARY ADDRESS TO USE

- Bloomberg email address
- Corporate email address

IB MESSAGE BODY

In Bloomberg Connector you can choose from two IB message body options.

When you select Plain option (default) you will see the interactions below each other. If you enable Grid option, you will see the information in five following columns:

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

See the examples on the next page.

IB MESSAGE BODY

- Plain Mode
- Grid Mode

SOURCES



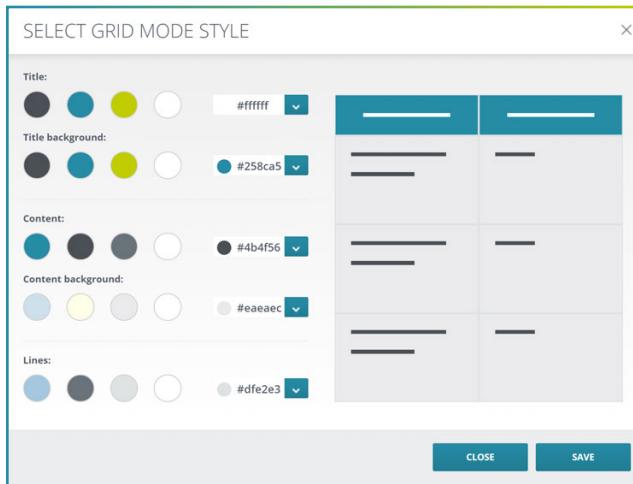
Bloomberg

Below are the examples of messages imported from Bloomberg source in two different modes: Grid Mode and Plain mode.

Plain mode displays the message in its basic form.

Grid mode allows to separate the data by sections and make it more readable.

The colors of the Grid mode are adjustable.



Grid Mode

A screenshot of a chat interface in Grid Mode. The top shows a message from AN (ANTON NORMAL) at 10:26 PM. Below is a table of interactions:

Plain Mode

A screenshot of the same chat session in Plain Mode. The top shows the message from AN. Below is the text content of the interactions:

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

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

Message 03/11/2008 14:31:37 QUENTIN KNAPP (SOME BIG BANK) <QKNAPP@bloomberg.net> Not for now, but by the end of the next week I might start looking at floaters. I will let you know...

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

SOURCES



BLOOMBERG MISCELLANEOUS 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 file-type with a vertical bar " | ". Simply write the name of the file (ex. bloomberg.ib) or use wildcards to import the whole file-type) (ex. *.txt | *.xml)

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.

MISC SETTINGS

Files to import: e.g.: *.txt | *.xml (separated by vertical bars)*

.

Subject prefix

HOW TO PROCESS BLOOMBERG FIRM-LEVEL FILES

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

This way, new account numbers can be discovered using the reporting feature in the Importer's settings (Reporting). 'Unconditional hit default target' and 'Process all filters' must be disabled (Filtering).

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

SOURCES



Bloomberg

HOW TO MANAGE QUARANTINE FILES

There are mainly two reasons that cause a file to become quarantined. The first occurs when a file cannot be parsed, or in simpler terms, the file format is incorrect. The second reason is caused by an IB (instant messages) or an MSG (email) file that is missing attachments or disclaimers. To address these quarantine files, the client will typically ask Bloomberg to resupply the ATT (attachments) or the DSCL (disclaimer) files. Once provided, the corrected file including the IB and MSG file (the file that was quarantined) will need to be added into the IMPORT folder (the name of this folder is decided at the time of configuration by the client – check the Connector Setting screen). Once the importer starts again, this information will be reprocessed. This is the way the reprocessing works if **Full Attachment/Disclaimer Validation** and **Advanced Reprocessing** are not enabled.

Another option is to ignore the missing attachments and disclaimers. Messages can be processed without attachments. For this, **Full Attachment/Disclaimer Validation** should be enabled and the default settings set to **Replace missing attachments/disclaimers with the following note**. This option is only set if there is no interest in the missing attachment/disclaimer of a message and only a reference to the missing file name is sufficient. Choosing this option will create a reference for the missing attachment within the messages once delivered to the target.

NEXT STEPS

After setting up the connector follow the appropriate links below to continue with configuration of Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users is not applicable to this connector.
- Filters
- Targets
- Importer Settings

EML



ABOUT EML CONNECTOR

EML connector is used to process EML type files from various sources. 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.

If EML connector is used for importing EML data from Symphony. Files with md5 extension should be excluded from the import, as content from Symphony is exported in a single Zip file containing EML files for each active conversation.

There are some drawbacks in using EML instead of Symphony connector for processing files from Symphony. They include:

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

MESSAGE MAPPINGS

- Participant names and email addresses in the To, From, CC, and BCC fields.
- Messages in the body of the output message.
- Attachments.
- Thread name in the message subject.

SOURCES



FTP CONFIGURATIONS

Merge1 retrieves data from the source **FTP** and stores it in the Import Folder for processing. Corrupt files are moved to the **Quarantine Folder**.

If you want to get data from the source through FTP, tick **Download files from FTP**. FTP Configuration options will automatically open.

A screenshot of the 'FTP' configuration dialog box. The interface is divided into several sections: 'FTP' at the top left, followed by 'FTP CONFIGURATION OPTIONS'. Section 1 ('CONNECTION') contains fields for 'Host' (with placeholder '/'), 'Port' (set to 21), and 'Connection Type' (dropdown menu). Section 2 ('AUTHENTICATION') includes 'Anonymous Access' checked, 'Username' and 'Password' fields, and a 'TEST CONNECTION' button. Section 3 ('FILE FILTER') has 'Include' selected and a wildcard entry '*'. Section 4 ('FILTER BY TIME') offers 'None', 'Only download files modified within the last: 1 days', 'Only download files modified: Later than [date] or Earlier Than [date]', and a 'Server Time Zone' dropdown set to 'UTC'. Section 5 ('OPTIONS') includes 'Maintain history of downloaded file for 5 days (0 = infinite)', 'Download subdirectories recursively', 'Delete files on server after downloading', and 'Execute script against source files' (with 'Script file' input and 'UPLOAD' and 'DOWNLOAD' buttons).

FTP

Download files from FTP

FTP CONFIGURATION OPTIONS

Use SSH Key Authentication

CONNECTION 1

Host * / Port * 21

Path * /

Connection Type

Use Security

Implicit SSL

Explicit SSL

SSH

AUTHENTICATION 2

Anonymous Access

Username *

Password *

TEST CONNECTION

FILE FILTER 3

Include

Exclude

*

FILTER BY TIME 4

None

Only download files modified within the last: 1 days

Only download files modified:

Later than [date]

Earlier Than [date]

Server Time Zone UTC

OPTIONS 5

Maintain history of downloaded file for 5 days (0 = infinite)

Download subdirectories recursively

Delete files on server after downloading

Execute script against source files 6

Script file *

Download script file

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 21. Choose FTP connection type from the Connection type dropdown list. FTP can run in either passive or active mode. Information about the connection type should be provided by the FTP host. If you wish to use FTP over SSL, select **Use SSL** check box and choose connection method: implicit or explicit.

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. This filter is used to 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. This filter is used for separating 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 modified within the mentioned days will be downloaded.
- Only download files modified earlier than/later than. When this option is selected, the data modified earlier than or later than the mentioned date will be downloaded. Both options can be selected simultaneously to choose a time period.
- Server Time Zone specifies the time zone in which the FTP sever is located to correctly determine the time stamp of downloadable files.

5. Options.

- Maintain history of downloaded file for X days. 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.

SOURCES



- 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.

6. Execute script against source files allows the user to utilize alternative methods of data download or acquisition methods other than FTP. For example, batch script files that download information via an FTP alternative and move it into the appropriate processing folder.

PGP CONFIGURATIONS

PGP DECRYPTION OPTIONS

Username *

Password *

Email *

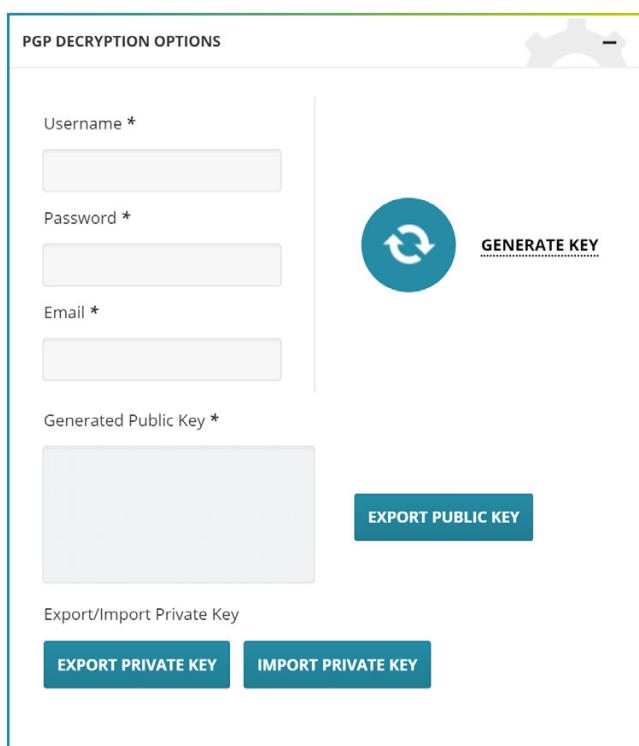
Generated Public Key *

EXPORT PUBLIC KEY

Export/Import Private Key

EXPORT PRIVATE KEY IMPORT PRIVATE KEY

GENERATE KEY



1. Click **Use PGP Decryption** and PGP Decryption Options open.
2. Specify a Username, Password, and Email, then click **Generate Key**. Once the key is generated you will see a green tick icon. **
3. Log into your source control panel and enable PGP encryption by adding Merge1 Keys.
4. In your source control panel click **Add** and the Add Public Key window will appear. From the Key Type drop-down menu, select Encryption and paste the full contents of the public key (including the block header and footer) under the Public Keys tab of the control panel in your terminal.
5. Click the Decryption button. (The key appears in the Public Keys section). To save the PGP encryption key to your account click **Submit**.

Please note:

When the FTP is disabled, Merge1 attempts to retrieve the data directly from the Import Folder. This is useful when data is already in-hand or if the user wishes to acquire the data manually.

* Please note that this password is required for configuring multiple connectors with the same PGP Key.

* Use the Export Public / Private Key buttons to save the keys to a secure location on your device. This will enable you to restore the keys if they are lost or when moving the database to a new machine.

SOURCES



FOLDER CONFIGURATION (REQUIRED*)

After successfully setting up the FTP and PGP Configurations, you will have to change the folder configurations. In Merge1 you will have to specify the Import Folder, where you would like to store the data after retrieving it from EML, as well as Quarantine Folder where all the failed messages will be archived.

If you have sub-folders under your Import Folder, you can enable **Traverse Subdirectories** to maintain the sub-folder structure of imported data and include the data in your EML Merge1.

FOLDERS

Import folder*

Traverse subdirectories

Quarantine folder*

AFTER SUCCESSFULL IMPORTING

Move original files into a subfolder of the Import folder.

Delete original files permanently.

Under **After Successfully Importing** settings you can provide Merge1 what to do with the original files. If Move original files into a subfolder is selected, the files will be moved to a folder called _Imported If Delete original files permanently is selected, the files after being processed will be deleted. Please note, that if deleted it won't be possible to recover them.

* Merge1 Folder Option 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.

SOURCES



MISCELLANEOUS SETTINGS

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

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.

MISC SETTINGS

Files to import: e.g.: *.txt | *.xml (separated by vertical bars)*

Subject prefix

Example of Output Message:

Tue 7/1/2003 1:53 PM

 Joe Q. Public <john.q.public@example.com>

To: Mary Smith; jdoe@example.org; Who?
Cc: boss@nil.test; Giant

Hi everyone.

NEXT STEPS

After setting up the connector follow the appropriate links below to continue with configuration of Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users is not applicable to this connector.
- Filters
- Targets
- Importer Settings

EWS



ABOUT EWS CONNECTOR

Exchange Web Services (EWS) is an application program interface (API) that allows programmers to access Microsoft Exchange items such as calendars, contacts and email.

EWS, which first became available in Exchange Server 2007, provides administrators with the flexibility to store, retrieve, move and modify email and related data for a single user, a group of users or an entire Exchange Server organization on an Exchange server. EWS can be useful for migrating Exchange data on-premises or to a third-party host in the cloud.

Merge1 retrieves data from Exchange servers via EWS and processes specific message classes from specific mailboxes. The EWS Source may also be configured to ingest data from Skype for Business Online. For that see **Enable Retention Policy** and **Enable In-Place Hold** sections of EWS Connector set up to configure Skype for Business Online.

ACTIVITIES CAPTURED

- One-on-one Chats
- Group Chats
- Messages sent from mobile devices

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 have to 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 isn't captured when you have an In-Place Hold set up in Exchange. Thus the data you would send via file transfer doesn't 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'll find the option for turning off non-archived features. You're supposed to "select this option if you're legally required to preserve electronically stored information."

SOURCES



PROVIDING NECESSARY PERMISSIONS TO THE ACCOUNT

1. Go to <https://portal.office.com/AdminPortal/Home>
2. Log into your account if you're not logged in yet
3. Open **Exchange Admin Center**

A screenshot of the Microsoft 365 admin center. The left sidebar shows various admin centers: Home, Customize your home, Search users, groups, settings or tasks, Admin centers (with Exchange highlighted and a red arrow pointing to it), Teams & Skype, SharePoint, OneDrive, Yammer, PowerApps, Flow, Security & Compliance, Azure Active Directory, and Microsoft Search. The main content area shows Billing (Total balance: \$0.00, Update payment details, View my bill), Support (New service request, View service requests), and a sidebar with Billing, Total balance: \$0.00, Update payment details, View my bill, Support, New service request, and View service requests.

4. Go to **Permissions**

A screenshot of the Exchange admin center. The left sidebar shows dashboard, recipients (with permissions highlighted and a red box around it), compliance management, organization, protection, mail flow, mobile, public folders, unified messaging, and hybrid. The main content area shows Welcome, recipients (mailboxes, groups, resources, contacts, shared, migration), organization (sharing, add-ins), and a sidebar with dashboard, recipients, compliance management, organization, protection, mail flow, mobile, public folders, unified messaging, hybrid, and a link to the Office 365 Admin center.

SOURCES



EWS

5. Double click on **Discovery Management** to open its settings

The screenshot shows the Exchange admin center interface. On the left, there's a sidebar with various links like dashboard, recipients, permissions (which is selected), compliance management, organization, protection, mail flow, mobile, public folders, unified messaging, and hybrid. The main area is titled "admin roles" and shows a list of role groups. One item, "Discovery Management", is highlighted with a red arrow pointing to it. The list includes: Compliance Management, ExchangeServiceAdmins_2103897041, Help Desk, HelpdeskAdmins_b19cf, Hygiene Management, Organization Management, Recipient Management, Records Management, RIM_MailboxAdmins0ba9b71288554c2f91a1f7e6cc2c5721, Security Administrator, Security Reader, TenantAdmins_c057d, UM Management, and View-Only Organization Management.

6. Click on + under **Roles** section to add roles

The screenshot shows the "Role Group - Google Chrome" window. The URL is https://outlook.office365.com/ecp/UsersGroups/EditAdminRoleGroup.aspx?Activit... The title is "Discovery Management".
Fields:

- *Name: Discovery Management
- Description: Members of this management role group can perform searches of mailboxes in the Exchange organization for data that meets specific criteria.
- Write scope: Default
- Roles: A list of available roles. An arrow points to the "+" button next to the list.
 - NAME
 - ApplicationImpersonation
 - Legal Hold
 - Mailbox Search
- Members: A list of users assigned to the role group. An arrow points to the "+" button next to the list.
 - NAME DISPLAY NAME
 - Michael Michael Krasner

Buttons at the bottom: Save and Cancel.

SOURCES



EWS

7. Add Legal Hold*, ApplicationImpersonation and Mailbox Import Export*

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**.

Please 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.

A screenshot of a web browser window titled 'Select a Role - Google Chrome'. The URL is https://outlook.office365.com/ecp/Pickers/ManagementRolePicker.aspx?ActivityCorrelationID=bedf2f7a-3... . The page lists various Exchange roles under 'DISPLAY NAME'. Two roles are highlighted with dark gray bars: 'Legal Hold' and 'Mailbox Import Export'. Below these, there is a list of other roles like 'Federated Sharing', 'Information Rights Management', 'Journaling', 'LegalHoldApplication', etc. At the bottom left is a red-bordered 'add ->' button. At the bottom right are 'OK' and 'Cancel' buttons, also with red borders around them. A status bar at the bottom indicates '2 selected of 53 total'.

8. Click on + under Members section to select the members of that role group

A screenshot of a web browser window titled 'Select Members - Google Chrome'. The URL is https://outlook.office365.com/ecp/Pickers/SecurityPrincipalPicker.aspx?ActivityCorrelationID=bedf2f7a-37... . The page lists users under 'NAME' and 'DISPLAY NAME'. One user, 'GlobanetShared', is highlighted with a dark gray bar. Below the list is a red-bordered 'add ->' button. At the bottom right are 'OK' and 'Cancel' buttons, also with red borders around them. A status bar at the bottom indicates '1 selected of 29 total'.

9. Click on Save changes in Discovery Management settings.

SOURCES



EWS

ENABLE RETENTION POLICY

1. Login to Microsoft Office 365 and navigate to
<https://protection.office.com/?rfr=AdminCenter#/retention>
2. From the **Data governance** drop down menu select **Retention**.

A screenshot of the Microsoft Office 365 Security & Compliance interface. The left sidebar shows a navigation menu with several options: Alerts, Permissions, Classifications, Data loss prevention, Data governance (which is expanded), Dashboard, Import, Archive, Retention (which is selected and highlighted in grey), Events, Dispositions, and Supervision. The main content area is titled 'Home' and features a section about GDPR compliance. Below it, there's a section titled 'Data governance' with a sub-section about threat management. A blue arrow points from the 'Retention' option in the sidebar to the 'Retention' section in the main content area.

3. Click the **+ Create** to create a new retention policy

A screenshot of the Microsoft Office 365 Security & Compliance interface, specifically the 'Retention' page. The left sidebar is identical to the previous screenshot. The main content area is titled 'Home > Retention'. It contains two sections: 'Labels' and 'Label policies'. The 'Labels' section has a description of what it does and a 'Create' button. A red arrow points to this 'Create' button. Below the 'Labels' section are search and filter fields for 'Name' and 'Created by'. The 'Label policies' section also has a description and its own 'Create' button.

SOURCES



EWS

4. Name your policy, provide a description and click **Next**.

This screenshot shows the 'Name your policy' step of a retention wizard. On the left, a sidebar lists steps: 'Name your policy' (selected), 'Settings', 'Choose locations', and 'Review your settings'. The main area has a title 'Name your policy' and fields for 'Name *' (containing 'Retention policy') and 'Description' (containing 'Description for retention policy'). A red box highlights the 'Next' button at the bottom.

5. Select the retention options based on your compliance requirements and click **Next**

This screenshot shows the 'Decide if you want to retain content, delete it, or both' step. It includes a sidebar with steps: 'Name your policy' (selected), 'Settings', 'Choose locations', and 'Review your settings'. The main area asks 'Do you want to retain content?' with a radio button selected for 'Yes, I want to retain it'. It shows retention settings ('For this long... 7 years') and deletion options ('Do you want us to delete it after this time? No'). A red box highlights the 'Next' button at the bottom.

6. Select the location on which content the policy should be applied and click **Next**.

If necessary, choose users or groups of the location you have chosen.

For Skype for Business Online select **Skype for Business** then click **Choose users**.

This screenshot shows the 'Choose locations' step. It includes a sidebar with steps: 'Name your policy' (selected), 'Settings', 'Choose locations', and 'Review your settings'. The main area lists locations with toggle switches: 'OneDrive accounts' (on), 'Office 365 groups' (on), 'Skype for Business' (on), and 'Exchange public folders' (off). For each location, there are 'CHOOSE SITES' and 'EXCLUDE SITES' buttons. A red box highlights the 'Next' button at the bottom.

SOURCES



EWS

7. Enable the check box that is at the top of the list to select all users or select the users that need to be monitored, then click **Choose**.

The screenshot shows the 'Edit locations' dialog box for Skype for Business. At the top, it says 'Edit locations' and has a close button. Below that is a section for 'Skype for Business' with a search bar. A red arrow points to the 'Users (13)' section under 'Added (13)'. In this section, there is a checkbox for 'Name' which is checked. Below it is a list of users with their names and emails. At the bottom of the list are 'Choose' and 'Cancel' buttons, with 'Choose' being highlighted by a red box.

8. Once the users have been added, click **Done** and then click **Next**.

9. Review your settings and click **Create this policy**.

The screenshot shows the 'Create a policy' wizard. On the left, a sidebar lists steps: 'Name your policy' (done), 'Settings' (done), 'Choose locations' (done), and 'Review your settings' (in progress). The main area is titled 'Review your settings' and contains a note about retention policy application. It shows settings for a policy named 'Retention policy' with a retention period of 1 day. It also lists locations where the policy applies: Exchange email, OneDrive accounts, SharePoint sites, Skype for Business, and Office 365 groups. At the bottom, there are 'Back', 'Save for later', 'Create this policy' (highlighted by a red box), and 'Cancel' buttons.

SOURCES



EWS

10. Note that at this point the Status should be **On (Pending)**, please allow up to 24 hours for the policy to be applied and the status changed to **On (Success)** at which point you can start running Merge1 to capture conversations.

A screenshot of a web-based retention policy configuration interface. The title bar says "Retention policy".

- Status:** On (Pending) (with a blue toggle switch)
- Policy name:** Retention policy
- Description:** Description for retention policy (with an "Edit" link)
- Applies to content in these locations:** Exchange email, OneDrive accounts, SharePoint sites, Office 365 groups (with an "Edit" link)

At the bottom are "Close" and "Feedback" buttons.

SOURCES



EWS

ENABLE IN-PLACE HOLD

Follow the steps of this section if you're using EWS Connector for Skype for Business Online.

1. Log in to the Microsoft Office 365 Admin Center (<https://outlook.office365.com/ecp>)

2. Go to **Compliance Management** section:

A screenshot of the Exchange admin center interface. The top navigation bar shows 'Office 365' and 'Admin'. The main title is 'Exchange admin center'. On the left, there's a sidebar with various links: dashboard, recipients, permissions, compliance management (which is highlighted with a red box), organization, protection, mail flow, mobile, public folders, unified messaging, and hybrid. To the right of the sidebar, under 'Welcome', there are three sections: 'recipients' (mailboxes, groups, resources, contacts, shared, migration), 'organization' (sharing, add-ins), and a note about 'We're still planning to remove the ability to create new In-Place eDiscovery Searches and holds in the EAC. We'll announce this when we have a firm date. Please start using Content search in the Office 365 Security & Compliance Center. In Exchange hybrid deployments, searches run from your on-premises organization won't be affected by this change. Learn more about content search and retention in the Security & Compliance Center.' At the bottom of the sidebar, there's a table with columns for NAME, HOLD STATUS, MODIFIED DATE, and CREATED BY, with a red '+' sign in the first column.

3. Under the **in-place eDiscovery & hold** tab, click the **+** (plus) sign

A screenshot of the 'in-place eDiscovery & hold' page. The top navigation bar has 'in-place eDiscovery & hold' selected. Below it, there's a search bar and a note about the removal of the feature. A table at the bottom allows for creating a new hold, with a red '+' sign highlighted. The table columns are NAME, HOLD STATUS, MODIFIED DATE, and CREATED BY.

Please note

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 holds please use Retention Policy described earlier in this guide.

SOURCES



EWS

4. Provide a suitable name and description, click **Next**.

The screenshot shows a web browser window titled 'In-Place eDiscovery & Hold - Google Chrome'. The URL is <https://outlook.office365.com/ecp/Reporting/NewDiscoveryHold.aspx?ActivityCorrelationID=4117c6f6-346d-860a-0607-fe...>. The page displays a search interface for 'new in-place eDiscovery & hold'. It includes fields for 'Name' and 'Description'. A note at the bottom states: 'In-Place Hold is a premium feature that requires an Exchange Online Plan 2 or Exchange Online Archiving'. At the bottom right are 'Next' and 'Cancel' buttons.

5. In-place Hold is not available if you select **Search all mailboxes**. Select **Specify mailboxes** to search and click the + (plus) sign. Add specific mailboxes (or distribution groups), then click **Next**.

The screenshot shows two overlapping windows. The background window is the 'In-Place eDiscovery & Hold' configuration page, which now shows 'Specify mailboxes' selected under 'Mailboxes'. The foreground window is a 'Select Mailbox' dialog titled 'Select Mailbox - Google Chrome'. It lists a single item: 'Archive Mailbox' with the email address 'ArchiveMailbox@globanetconsulting.com'. Below the list, it says '1 selected of 23 total'. At the bottom of the dialog are 'OK', 'Cancel', 'Back', 'Next', and 'Cancel' buttons. A note at the bottom of the main window states: 'In-Place Hold is a premium feature that requires an Exchange Online Plan 2 or Exchange Online Archiving to enable it for each user mailbox. [Learn more](#)'.

SOURCES



EWS

6. You can either choose to put all content In-Place Hold (not recommended) or define some criteria (recommended).

I. Select **Filter based on criteria**

II. Click **select message types...**

III. Click Select the message types to search and check the **Skype for Business** items checkbox.

IV. Click **Next**.

The screenshot shows two windows side-by-side. The left window is titled 'In-Place eDiscovery & Hold - Google Chrome' and contains fields for 'Search query', 'Specify start date' (set to 2018 October), 'Specify end date' (set to 2018 November), 'From:' (empty), and 'To/Cc/Bcc:' (empty). Below these is a section for 'Message types to search' with a 'select message types...' button. A tooltip at the bottom left of this window says: 'In-Place Hold is a premium feature that requires an Exchange Online Plan 2 or Exchange Online Archiving license to enable it for each user mailbox.' The right window is titled 'Message Types to Search - Google Chrome' and shows a list of message types: Email, Meetings, Tasks, Notes, Documents, Journal, Contacts, and Skype for Business items. The 'Skype for Business items' checkbox is checked. Both windows have 'OK', 'Cancel', 'Back', and 'Next' buttons at the bottom.

6. Select **Place content matching the search query in selected mailboxes on hold**, then select either:

- Hold indefinitely
- Specify number of days to hold items relative to their received date

The screenshot shows the 'In-Place eDiscovery & Hold' configuration page. It features an 'In-Place Hold settings' section with a checked checkbox for 'Place content matching the search query in selected sources on hold'. Below this are two radio buttons: 'Hold indefinitely' (selected) and 'Specify number of days to hold items relative to their received date'. A tooltip at the bottom left of this section says: 'In-Place Hold is a premium feature that requires an Exchange Online Plan 2 or Exchange Online Archiving license to enable it for each user mailbox.' At the bottom of the page are 'Back', 'Finish', and 'Cancel' buttons.

7. Click **Finish**.

SOURCES



EWS

HOW TO CONFIGURE EWS CONNECTOR SETTINGS

1. Specify the URL for EWS connector
2. Select the required Exchange version from the drop-down menu
3. Choose if the import should be done by last modification date (DateTimeModified) or by creation date (DateTimeCreated). The cut-off date options change accordingly.
4. Write down the Mailbox Folders from where the data should be imported.
If you have more than one Mailbox Folder, separate each name with a semicolon (";")
 - **Include subfolders**, if selected, processes data within the subfolders of the specified mailboxes.
 - **Load recoverable items**, if the Exchange Version is not Exchange2007Sp1 and if this option is selected, Merge1 searches for the mentioned mailbox folders in the recovery route folders.
5. Provide Impersonator name and Password.

Personal archive, if selected, processes only the archived information.

EWS CONFIGURATION

URL	<input type="text" value="https://outlook.office365.com"/>
Exchange Version	<input type="button" value="Exchange2013"/>
Import based on	<input type="button" value="DateTimeModified"/>
Mailbox Folders	<input type="text" value="Conversation History"/> separated by ':' <input type="checkbox"/> All folders <input type="checkbox"/> Include subfolders <input checked="" type="checkbox"/> Load recoverable items
Impersonator	<input type="text" value="michael@globanetconsulting."/>
Password	<input type="password" value="*****"/> <input type="checkbox"/> Personal archive
<input checked="" type="checkbox"/> Do not download data modified before: <input type="text" value="7/1/2019"/> <input type="button" value="Calendar"/>	
<input checked="" type="checkbox"/> Do not download data modified after: <input type="text" value="7/11/2019"/> <input type="button" value="Calendar"/>	

SOURCES



EWS

- 6.** Options **Do Not Download Data Modified/Created Before** and **Do Not Download Data Modified/Created After** allow to cut off data outside the set date range. If the Before date is set to 04/17/2016 and the After is set to 08/25/2018 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.

- 7.** Select the Message Class you would like Merge1 to import and then click **Next**.

A Message Class is an internal identifier that Microsoft Outlook and Microsoft Exchange utilize to locate and activate forms.

There are 12 Message Class types that Merge1 can import:

- Message (IPM.Note)
- Note (IPM.Post)
- Task (IPM.Task)
- Task Request (IPM.TaskRequest)
- Task Accept (IPM.TaskRequest.Accept)
- Task Decline (IPM.TaskRequest.Decline)
- Contact (IPM.Contact)
- Meeting Request (IPM.Schedule.Meeting.Request)
- Meeting Cancellation (IPM.Schedule.Meeting.Canceled)
- Appointment (IPM.Appointment)
- Document (IPM.Document)
- Message Recall (IPM.Outlook.Recall)
- Skype for Business (IPM.Note.Microsoft.Conversation)
- Skype for Business Archive (IPM.Note.Microsoft.Conversation.Archive)
- Skype for Business Missed (IPM.Note.Microsoft.Conversation.Missed)

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

Message Classes can be edited in Merge1.Connectors.Base.dll.config in the Bin folder within the Merge1 6.0 installation directory. Default path: **C:\Program Files\Globanet Consulting Services\Merge1 6.0\Bin\Merge1.Connectors.Base.dll.config**

SOURCES



EWS

PROGRESS COUNTER

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

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

EWS/ | STATUS: **Running (Importing)** | Acquiring monitored users list...

SOURCE
Below is where Merge1 should gather your data.

MONITORED USERS
Below is whose data Merge1 should gather.

USING EWS FOR SKYPE FOR BUSINESS ONLINE

If no retention policy is set, only Skype for Business and Skype for Business Missed message classes are captured, as they are not compliant.

When in-place hold is activated, a compliant copy of each message is saved in the Purges folder (in addition to a copy saved in the user's mailbox) and cannot be deleted from there. If Skype for Business Archived message class is selected, data is captured from Purges folder.

When all 3 Skype for Business messageclasses are selected, duplicates can be captured, as copies are kept both in the user mailbox and in the Purges folder.

The only use case to get compliant data from Skype for Business Online without duplicates is checking Skype for Business Missed and Skype for Business Archived.

HISTORY TRACKING

The message history tracking (and cut-off date filtering) itself is being done by LastModifiedTime or DateTimeCreated property (determined by the "Import Based On" setting of the connector) 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.

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 (see point 3 of previous section).

SOURCES



EWS

Example Sample Message

Sun 8/26/2018 10:26 PM

Michael Smith <Michael@example.com>

Conversation with John Smith

To Michael Smith; John Doe

Michael Smith 10:25 PM:
Hey

Michael Smith 10:25 PM:
This is from a mobile

John Smith 10:26 PM:
hey, how you doin

NEXT STEPS

After setting up the connector follow the appropriate links below to continue with configuration of Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users. Mailboxes must be specified using an LDAP Query. To do so, choose **Active Directory** in the Monitored Users tab in the Configuration Wizard.
- Filters (EWS works with all filters except **XML Filter**)
- Targets
- Importer Settings

JIVE



Jive

ABOUT JIVE CONNECTOR

Jive is the leading provider of communication and collaboration solutions for business. Inside companies, Jive Interactive Intranets dramatically improve employee engagement, alignment and productivity by providing one place to connect, communicate and collaborate. Externally, Jive Customer Communities activate and enhance every stage of the customer journey, from marketing engagement to support and brand advocacy. Millions of users and many of the world's most successful companies rely on Jive day in and day out to get work done, delight their customers and stay ahead of their competitors.

ACTIVITIES CAPTURED

- Questions are captured with attachments (everyone in CC), tags are included
- Group discussions
- One-on-one discussions
- Blog posts
- File Upload
- Polls
- Document collaboration
- Bookmark share and discuss is captured partly: shows activity but doesn't capture attachments
- Status updates
- Tasks
- Private Message are captured with attachments
- Videos

SOURCES



Jive

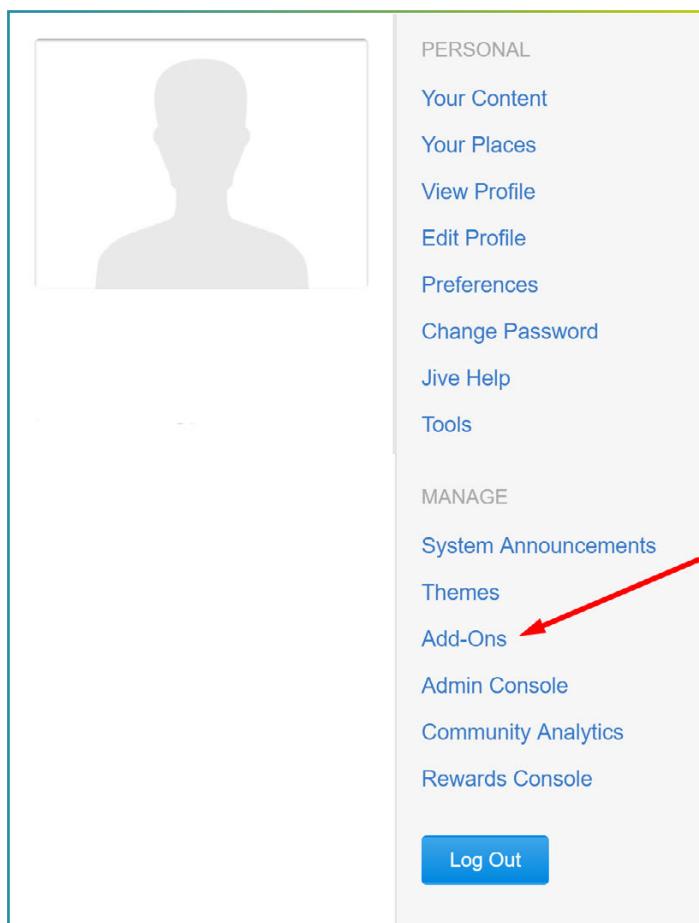
CREATING JIVE APPLICATION

To configure the connector, you must already have created an application in Jive. If you do not have an application created for Jive, please follow the steps below:

1. Create an add-on package. Instructions and samples can be found at <https://community.jivesoftware.com/docs/DOC-99941>.

When prompted for a redirect URL, set it to the URL of your local Merge1 environment with the following extension: "**/Configuration/OAuthCallback**". For example: <https://globanetlabs.com/Configuration/OAuthCallback/>
Please note, that only hostnames should be used in the Callback URL, IP addresses won't work.

2. Log into your Jive environment. You will need to be a community manager or have the ability to install add-ons for personal use on this Jive server. We suggest you use the Jive Developer Sandbox for testing.
3. Go to Add-Ons section of the account.



SOURCES



Jive

4. Click **Upload Package**.

The screenshot shows the Jive platform's Add-ons management interface. In the center, there's a section titled "All Add-ons: Installed". Below this, under "Storage Providers", there are three items: "API Services", "Analytics Services", and "All Add-ons". To the right of the "All Add-ons" item is a list of bullet points describing how add-ons extend the Jive Platform. At the bottom right of this section is a blue button labeled "Upload Package", which is highlighted with a red box.

5. Click **Choose File** and select the add-on package to upload.

This screenshot shows a modal dialog box titled "Upload Package". It asks if you want to upload your local .jive package to this community or preview it first. There is a red box around the "Choose File" button, which is labeled "file chosen". Below the button are three buttons: "Install now", "Preview", and "Cancel". At the bottom of the dialog, there is a note about previewing the service.

6. Once you've selected the file, click **Install now**.

7. When the package is installed, go to **All Add-ons: Installed**, click on the settings icon of the necessary add-on and go to **View Client ID and Secret**.

This screenshot shows a list of installed add-ons. The first two entries are "Merge1 Full Access" and "Merge1 Full Access", both by Globanet. The third entry is "Merge1 Dev" by Globanet. To the right of each entry are details like permissions (Read and write, Full Access) and the date of installation. For the "Merge1 Dev" entry, a context menu is open, with a red arrow pointing to the "View Client ID and Secret" option. Other options in the menu include "Settings", "Publish to Add-ons Registry", "Uninstall", and "Enable for External Contributors".

8. Copy the **Client ID** and **Client Secret**.

This screenshot shows a modal dialog box titled "View Client ID and Secret". It displays two fields: "Client ID" containing the value "f5y23go5swzmcds4co9tvmo3ph1gisq.i" and "Client Secret" containing the value "ckhqqlihi9yejs1oy7c4ol6fhlm5p4n1ef.s". At the bottom left is a "Done" button.



Jive

CONFIGURING JIVE CONNECTOR

1. Provide **Jive Instance URL** of your company
2. Fill in the **Application ID** field with the **Client ID** copied previously.
3. Enter the **Client Secret** in the **Application Secret/Key** field.
4. Click **Next**.

EDIT CONNECTOR

X

SOURCE MONITORED USERS FILTERS TARGETS SETTINGS

Please provide the following credentials to your company's Jive app so that Merge1 can be configured to access your monitored users' account data.

If you do not have an app created for Jive, please [click](#) for more information.

JIVE APPLICATION CONFIGURATION

Jive Instance URL

Application ID

Application Secret/Key

NEXT

Please note:

The highlighted click button in the configuration window will provide guiding information for setting up the connector.



Jive

COMMUNICATION CONFIGURATION OPTION

This option allows choosing what types of group chats from Jive will be imported.

When **Private Communication** is checked, only group chats of private type will be imported. When **Public Communication** is checked, only group chats of public type will be imported. Both options can be selected simultaneously.

Note that one-on-one messages will be imported regardless of these settings.

These options apply only to group chats.

COMMUNICATION CONFIGURATION OPTIONS

Private Communication

Public Communication

Private messages are captured regardless of the settings above.

ADVANCED CONFIGURATION OPTIONS

The “**Do not download data modified before**” check will ensure that old or irrelevant data is excluded. For example, if the date selected is 9/1/2017, it won’t retrieve any data modified before September 1 of 2017. Only the data after 9/1/2017 will be retrieved, archived, and imported.

ADVANCED CONFIGURATION OPTIONS

Do not download data modified before:





Jive

Example of Output Message:

Tue 7/3/2018 12:07 PM

John Doe <jdoe@example.com>

Test 1

To Tim Jones

Cc Anna Smith; Arthur Doe; David Davids; Jackie Jackson; Michael Smith

Content:

Test 1

Parent Place: John Doe (person)

Follower Count: 0

View Count: 1

Published: 7/3/2018 8:06:59 AM UTC

Updated: 7/3/2018 8:06:59 AM UTC

Status: published

Reply Count: 0

Likes Count: 0

Message Type: JIVE.UPDATE

NEXT STEPS

After setting up the connector follow the appropriate links below to continue with the configuration of Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users (preferred option for Jive is **All (Based on Native API)**, the users will be retrieved automatically)
- Filters (Jive works with all filters except **XML Filter**)
- Targets
- Importer Settings

FACEBOOK



Facebook

HOW TO SET UP FACEBOOK IMPORTER

A Facebook page is a public profile specifically created for businesses, brands, celebrities, causes, and other organizations. Unlike personal profiles, pages do not gain "friends," but "fans" - which are people who choose to "like" a page. Pages can gain an unlimited number of fans, differing from personal profiles, which has had a 5,000 friend maximum put on it by Facebook. Pages work similarly to profiles, updating users with things such as statuses, links, events, photos and videos. This information appears on the page itself, as well as in its fans' personal news feeds.

ACTIVITIES CAPTURED

- Posts
- Comments
- Replies to comments
- Pictures (as links)
- Shares
- Videos (as links)
- Posts from external users into the group
- Post edits

SOURCES



Facebook

FACEBOOK APPLICATION CREATION

1. Go to <https://developers.facebook.com/>
2. Log into your Facebook account.
3. From **My Apps** dropdown menu click **Add New App**.
4. Enter the **Display Name** and **Contact Email** address and click **Create App ID**:

Create a New App ID

Get started integrating Facebook into your app or website

Display Name
Sample App

Contact Email
sample@domain.com

By proceeding, you agree to the Facebook Platform Policies

Cancel Create App ID

5. Go to the **Dashboard** and click **Set Up** on Facebook Login section:

facebook for developers

Sample App APP ID: 328999324459552 Status: In Development View Analytics

Dashboard

Settings

Basic Advanced

Roles

Test Users

Alerts

Inbox Archived

App Review

Current Request My Permissions and Features Permissions and Features

PRODUCTS

Add a Product

Account Kit

Facebook Login

Audience Network

Analytics

Messenger

Webhooks

Read Docs Set Up Read Docs Set Up Read Docs Set Up

Read Docs Set Up Read Docs Set Up Read Docs Set Up

6. Select **Web** as an app platform:

Use the Quickstart to add Facebook Login to your app. To get started, select the platform for this app.

iOS

Android

Web

Other

SOURCES



Facebook

7. Enter a Site URL, click **Save** and then **Continue**.
8. Click **Next** on the rest of set up steps, until the pop-up closes.
9. Go back to the Apps page <https://developers.facebook.com/apps> and click on the created App in the previous steps.
10. Go to Facebook Login's settings page and add a Redirect URI "<https://yourdomain.com>" (for example, <https://globanet.com/Configuration/OAuthCallback>).
Click **Save Changes**.

The screenshot shows the 'Client OAuth Settings' page. It includes several configuration options with checkboxes:

- Client OAuth Login:** Yes (selected)
- Web OAuth Login:** Yes (selected)
- Enforce HTTPS:** Yes (selected)
- Force Web OAuth Reauthentication:** No
- Embedded Browser OAuth Login:** No
- Use Strict Mode for Redirect URIs:** Yes (selected)
- Valid OAuth Redirect URIs:** A text input field containing 'Valid OAuth redirect URLs'. A red arrow points to this field.
- Login from Devices:** No

At the bottom right are two buttons: 'Discard' and 'Save Changes' (highlighted with a blue box). Red arrows point from the text 'Valid OAuth redirect URLs.' to the input field and from the 'Save Changes' button to the button itself.

11. Go to the Basic section of the Settings and copy the **App ID** and **App Secret**.

The screenshot shows the 'Basic' section of the Facebook App Settings. The left sidebar has a 'Settings' tab selected, indicated by a red arrow. The main area displays the following fields:

- App ID:** 328999324459552 (highlighted with a red arrow)
- App Secret:** A masked string (highlighted with a red arrow)
- Display Name:** Sample App
- App Domains:** (empty)
- Namespace:** (empty)
- Contact Email:** shahinyan.mary@yahoo.com
- Privacy Policy URL:** Privacy policy for Login dialog and App Details
- Terms of Service URL:** Terms of Service for Login dialog and App Details
- App Icon (1024 x 1024):** A placeholder image (highlighted with a red arrow)
- Category:** Choose a Category

At the top, there is a status indicator 'OFF Status: In Development' and links for 'View Analytics' and 'Help'.

SOURCES



Facebook

FACEBOOK CONNECTOR CONFIGURATION

1. Paste **App ID** and **App Secret** copied in the previous steps into Application ID, and Application Secret/Key fields correspondingly. Click **Next**.

The screenshot shows the 'CONFIGURATION WIZARD' interface. At the top, there are tabs: SOURCE (which is selected), MONITORED USERS, FILTERS, TARGETS, and SETTINGS. Below the tabs, a note reads: 'Please provide the following credentials to your company's Facebook app so that Merge1 can be configured to access your monitored users' account data.' A section titled 'FACEBOOK APPLICATION CONFIGURATION' contains fields for 'Application ID' and 'Application Secret/Key', both with placeholder text. There is also a checkbox labeled 'I have Access Token'. At the bottom of the wizard are 'BACK' and 'NEXT' buttons.

NEXT STEPS

After setting up the connector follow the appropriate links below to continue with the configuration of the Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users is not applied to Facebook connector, as Pages are monitored, not Users.
- Filters (**XML**, **Active Directory**, **Mail** filters are not applicable)
- Targets
- Importer Settings

TWITTER



Twitter

ABOUT TWITTER CONNECTOR

Twitter is an online news and social networking site where people communicate in short messages called tweets.

Twitter requires opt-in from the users that are going to be monitored. The Twitter connector does not work with a proxy server.

ACTIVITIES CAPTURED

- GIFs are captured as links
- GIF post texts
- Attachments are captured as links
- Comments
- Shares
- Emojis
- Tweets to timelines
- The choosing options of polls are not captured, only the poll post note

Follows and direct messages are not captured.

SOURCES



Twitter

CREATING TWITTER APPLICATION:

If you do not have an application created for Twitter, please follow the steps below:

- 1.** Log in at "<https://developer.twitter.com/>".
- 2.** Click Create New App.
- 3.** Complete the form:
 - a.** Provide a name for the application, i.e. "Merge1 Twitter App".
 - b.** Provide a brief description for the application.
 - c.** Enter the URL of your organization's website.
 - d.** Enter the URL of your local Merge1 environment with the following extension:
/Configuration/OAuthCallback
 - e.** Agree to the terms of service.
- 4.** Click **Create**.
- 5.** Open the **Keys and Tokens** tab to view the **API Key** and **API Secret Key**.

TWITTER APPLICATION CONFIGURATION

To activate Twitter Importer, fill in the following information in the Configuration Wizard Source tab:

- 1.** Provide your Twitter Application ID
- 2.** Enter the Application Secret/Key
- 3.** Click **Next**.

Please note:

Twitter connector requires opt-in from the users that are going to be monitored. More information on how the opt-in works is given in the Reports section of this guide.

YAMMER



ABOUT YAMMER

Yammer is a collaboration tool that helps users and their teams stay on top of it all. They can start conversations, work together on files, and organize around projects. The Yammer app allows Merge1 to hook in and collect data.

ACTIVITIES CAPTURED

- Posts in a group
- Private Messages
- Attachments (excluding sharepoint files)
- Internal group members
- External group members
- Public posts
- Private posts
- Updates to posts
- Polls - Only the question of the poll and the replies
- Praise - Only the text of the praise and the replies
- Announcements - Only the text of the announcement and the replies
- Posts threading
- Personal messages threading
- Deleted Posts (including attachments) *
- Deleted Comments (including attachments) *
- Deleted Private Messages (including attachments) *

* The created message does not say it was deleted from Yammer. To capture the deletes the data retention setting needs to be set to Soft-Delete. See the instruction by following this link:

<https://docs.microsoft.com/en-us/yammer/manage-security-and-compliance/manage-data-compliance>

Some events of former members aren't captured due to limited permissions of admin-generated token

SOURCES



Yammer

HOW TO SET UP YAMMER CONNECTOR

1. Log into your Yammer account at https://www.yammer.com/client_applications.
Please note that the user needs to have Admin access.
2. Click on **Register New App**.

The screenshot shows a portion of the Yammer dashboard. At the top, there are two application entries in a table:

MK-Consulting-Ya...	HPE-YAMMER	September 16, 2016	September 16, 2016	✓
MK-Consulting-Ya...		March 08, 2016	September 16, 2016	✓

Below the table is a green button labeled "Register New App". Underneath the button, there is a "Get help" section with three links:

- [API documentation](#)
- [Site issues](#)
- [Partner with Yammer](#)

3. Fill in the details. Provide an Application Name, fill in the Organization name, fill in the Support email, add a Website link, and add a Redirect URL in the following format:
https://<your_merge1_IP>/Configuration/OAuthCallback. Note that the IP address should be used.

The screenshot shows the "Register new App" dialog box. It has a header "Register new App" and a close button "x". A message "All fields are required." is displayed. There are five input fields with labels and question marks:

- Application Name
- Organization
- Support e-mail
- Website
- Redirect URI

Below the fields is a checkbox agreement: By checking this box, you agree that you have read and agree to the [Yammer API Terms of Service](#).

At the bottom are "Cancel" and "Continue" buttons.

4. Click on **Continue**.

SOURCES



Yammer

5. From the opened page, copy **Client ID** and **Client Secret**
6. Go to Merge1 and click on **Add Importer**.
7. Select **Yammer** from the list of connectors.
8. Fill in the **Name** (required) and **Description**.

CONFIGURATION WIZARD

ADD IMPORTER

Name: Importer

Description: Importers

NEXT

9. In the **Application ID** field add the **Client ID** copied in the previous steps, in the **Application Secret/Key** add the copied **Client Secret**.

CONFIGURATION WIZARD

SOURCE MONITORED USERS FILTERS TARGETS SETTINGS

Please provide the following credentials to your company's Yammer app so that Merge1 can be configured to access your monitored users' account data.

If you do not have an app created for Yammer, please [click](#) for more information.

YAMMER APPLICATION CONFIGURATION

Application ID:

Application Secret/Key:

BACK NEXT

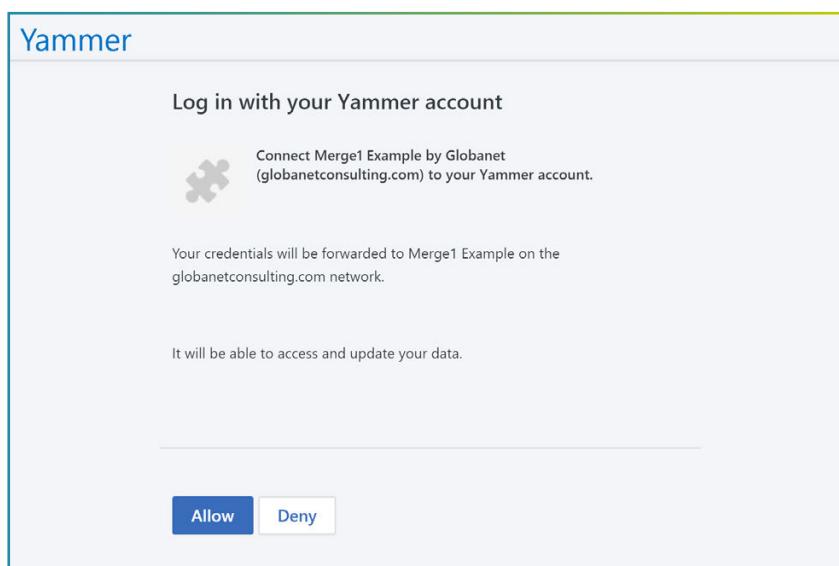
SOURCES



10. Click **Next**.

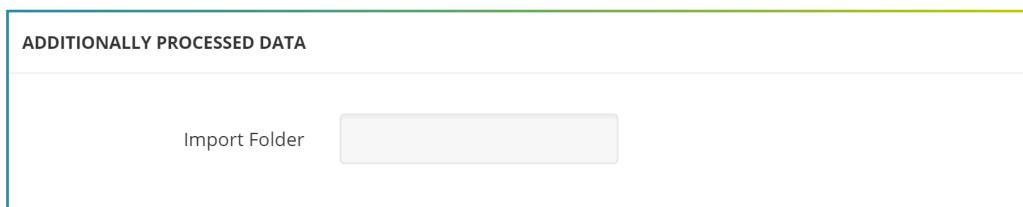
11. Allow logging in with the Yammer account to finalize the connector set up.

Make sure that the pop-ups are not blocked by the browser. You can check that from the top right corner of the browser address field.



ADDITIONALLY PROCESSED DATA

Merge1 needs an Import Folder to download, store and process data from Yammer. This is because Yammer's APIs are limited in their ability to send and receive data. The Import Folder must be empty for the importer to function properly.



ADVANCED CONFIGURATION OPTIONS

There are following advanced options when configuring the Yammer connection with Merge1.

- The **Merge messages by thread** combines all messages in a thread into a single message.
- The "**Do not download data modified before**" check will ensure that old or irrelevant data is excluded. For example, if the date selected is 9/1/2017, it won't retrieve any data modified before September 1 of 2017. Only the data after 9/1/2017 will be retrieved, archived, and imported.

SOURCES



Yammer

- 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.
- The **Message Body Type** specifies how the imported message will be displayed in the target. The Plain mode displays the message as simple text, and the HTML mode organizes the data. See the examples below.

ADVANCED CONFIGURATION OPTIONS

Merge messages by thread

Do not download data modified before:

Subject prefix

MESSAGE BODY TYPE

Plain

Html

TIMESTAMP FORMATTING & DATETIME FORMATS

In addition to the primary stamp, a second timestamp can be enabled with its own timezone. 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 three options in the Datetime Formats section.

TIMESTAMP FORMATTING

Primary Time Zone
 (UTC+04:00) Yerevan (CST)

Secondary Time Zone

DATETIME FORMATS

March 29 at 09:31 PM

Mar 29, 2019 21:31:11

29/03/2019 21:31:11

SOURCES



Yammer

EXCLUDE FILE TYPES

- 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 this 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 shouldn't be downloaded can be specified in the following format: ex. txt,png,xml. The comma is used to separate the file types.

EXCLUDE FILE TYPES

Do not download files greater than megabyte(s).

Custom Message This message will be inserted at the beginning of the email body text.
example: Files {0} are not imported, because they are greater than {1} megabytes
All the filenames that were excluded will be written instead of {0} symbol.
File size limit will be written instead of {1} symbol.

File Types

Custom Message This message will be inserted at the beginning of the email body text.
example: Files {0} are not imported.
All the filenames that were excluded will be written instead of {0} symbol.

SPLITTING MESSAGES

Splitting Messages option allows splitting big files. In the field the size of a split part of the message can be specified so that each part doesn't 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.

SPLITTING MESSAGES

Split messages

(MB) Max Size for each part of splitted message
Split size must be an integer

SOURCES



Yammer

Example of Plain Body Type:

Mon 10/1/2018 6:58 PM

MS Michael Smith <msmith@example.com>

Thread Id: 1160867420 | I got your message. Thank...

To John Smith; archivemailbox; dsfsfsdfds <dsfsfsdfds@mailru.ue>

group.png 286 bytes avatar.png 2 KB

Group Name: MaryTest
From: Michael Smith
Sent Date: 10/1/2018 6:57:56 PM
Message: I got your message. Thank you. Everything OK?

Example of HTML Body Type:

Mon 10/1/2018 6:58 PM

MS Michael Smith <msmith@example.com>

Thread Id: 1160867420 | I got your message. Thank...

To John Smith; archivemailbox; dsfsfsdfds <dsfsfsdfds@mailru.ue>

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

Group Name: MaryTest
 Michael Smith
October 01 at 06:57 PM

I got your message. Thank you. Everything OK?

NEXT STEPS

After setting up the connector follow the appropriate links below to continue with the configuration of the Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users (preferred option for Yammer is All (based on native API), so the connector can get all users automatically)
- Filters (Yammer works with all filters except **XML Filter**)
- Targets
- Importer Settings

CHATTER



Chatter

ABOUT CHATTER

Chatter is an enterprise collaboration platform from Salesforce, a cloud-based customer relationship management (CRM) vendor. Chatter can be used as a company intranet or employee directory.

Merge1 Chatter Connector does not use opt-in for the monitored users, it needs to log into the sales force with Admin and get user personal token to import data. Besides, triggers need to be published on Chatter site to be able to capture updates, deletes, and edits. The triggers will create a post in a channel and Merge1 will capture the information from the channel.

Merge1 supports Shield Platform Encryption without any additional configuration in Merge1, since the data is encrypted by Salesforce "At rest" and the API provides the data decrypted.

Use Chatter Cipher Cloud if you have a host domain.

ACTIVITIES CAPTURED

- Posts
- Files
- Comments
- Shares
- Deletes (Requires triggers)
- Edits (Requires triggers)
- Links
- Polls
- Private Chats
- Edits (Requires triggers)
- Group Chats
- Feedpoll Choices (If Modify all data permission is enabled)
- All online communication, including attachments and deleted information (if the triggers are set)

SOURCES



Chatter

CREATING SALESFORCE APPLICATION AND ACQUIRING A TOKEN

To perform the steps below you'll need a Salesforce account with System Administrator profile, if you do not have access to a System Administrator user, please contact your Salesforce admin and ask for the permissions required to perform the steps below in your Salesforce environment.

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're using the Lightning Experience).

The screenshot shows the Salesforce Lightning Experience interface. At the top, there's a navigation bar with tabs like Sales, Home, Opportunities, Leads, Tasks, Files, Accounts, and Contacts. Below the navigation is a chart titled 'Quarterly Performance' showing sales trends from October to December. To the right of the chart is a context menu with two options highlighted: 'Switch to Salesforce Classic' (option 1) and 'Add Username' (option 2). The URL in the browser address bar is px.globenetlabs-dev-ed.lightning.force.com/fng/switcher?dest....

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

The screenshot shows the Salesforce Setup interface. On the left, there's a sidebar with links like Home, Chatter, Libraries, Content, Subscriptions, and Administer. Under Administer, 'Manage Users' is selected and expanded, with 'Profiles' listed as an option. A context menu is open at the top right, with 'Switch to Lightning Experience' (option 1) and 'Content' (option 2) highlighted. The main content area displays sections like 'Getting Started' (with 'Build App' and 'Salesforce Lightning' buttons), 'System Overview' (with a message about messages), and 'Recent Items' (listing various objects like Merge Service, Insights, Collaboration, etc.).

SOURCES



Chatter

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

The screenshot shows the Salesforce 'Profiles' page. At the top, there's a navigation bar with links for Home, Chatter, Libraries, Content, Subscriptions, and a search bar. Below the navigation is a sidebar with links for Lightning Experience Transition Assistant, Salesforce Mobile Quick Start, Home, and Administer (Manage Users, Profiles). The main content area is titled 'Profiles' and shows a table of profiles. One row is highlighted with a blue border, indicating it is selected. The selected profile is 'Action 2 Profile Name: Read Only' with 'User License: Salesforce'. A blue circle with the number '1' is positioned above the table header. A blue circle with the number '2' is positioned next to the 'Edit | Clone' link for the 'Read Only' profile.

- Enter a name for the profile and click the **Save** button.

The screenshot shows the 'Clone Profile' dialog box. It has a title 'Clone Profile' and a sub-instruction 'Enter the name of the new profile.' Below this, it says 'You must select an existing profile to clone from.' There are two input fields: 'Existing Profile' (set to 'Read Only') and 'Profile Name' (containing 'Merge1'). A blue circle with the number '1' is positioned above the 'Profile Name' field. A blue circle with the number '2' is positioned next to the 'Save' button.

- Click **Edit**.

The screenshot shows the 'Profile Merge1' edit page. At the top, there's a navigation bar with links for Home, Chatter, Libraries, Content, Subscriptions, and a search bar. Below the navigation is a sidebar with links for Lightning Experience Transition Assistant, Salesforce Mobile Quick Start, Home, and Administer (Manage Users, Profiles). The main content area shows the 'Profile Detail' section for 'Merge1'. It includes fields for Name (Merge1), User License (Salesforce), Description, Created By (Hagop.Esfahani), and Modified By (Hagop.Esfahani). Below this is the 'Console Settings' section with a 'Console Layout' button. The 'Page Layouts' section lists various global and specific page layouts for different objects like Global, Email Application, Home Page Layout, Account, and Asset. A blue circle with the number '1' is positioned above the 'Edit' link in the 'Profile Detail' section.

SOURCES



Chatter

The required permissions for Merge1 are:

Administrative Permissions:

- API Enabled
- Select Files from Salesforce
- Manage Chatter Messages and Direct Messages
- View All Data
- Modify All Data (Only if capturing Feedpoll Choices is required, otherwise can be ignored but errors will be present in the connector log. This is a limitation from Salesforce).

Note that when you enable View All Data , Read and View All permissions will be selected for all Standard Object Permissions and other view only permissions ,do not disable these permissions.

6. Scroll down and click **Save**.

The screenshot shows the 'Session Settings' page in the Salesforce setup. It includes sections for 'Feedback Question Sets', 'Feedback Requests', 'Feedback Templates', 'Streaming Channels', and 'DmSync Integration Clients'. The 'Session Settings' section contains fields for 'Session Times Out After' (set to '2 hours of inactivity'), 'Session Security Level Required at Login' (set to 'None'), and various password policy settings. At the bottom right of the form, there is a red arrow pointing to the 'Save' button.

Step 2: Create a User (Service Account)

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

The screenshot shows the 'Users' page in the Salesforce Lightning Experience. On the left, there's a sidebar with 'Lightning Experience Transition Assistant' and 'Salesforce Mobile Quick Start'. The main area shows a list of users with columns for 'Action', 'Full Name', 'Alias', 'Username', 'Last Login', 'Role', 'Active', 'Profile', and 'Manager'. At the top of the user list, there are buttons for 'New User', 'Reset Password(s)', and 'Add Multiple Users'. A red arrow points to the 'New User' button.

SOURCES

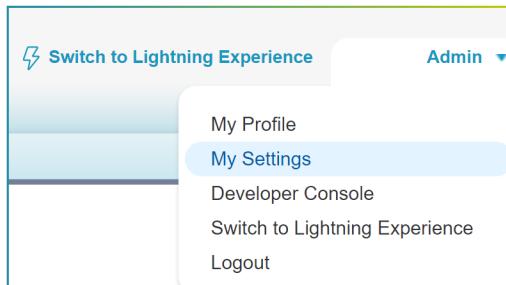


Chatter

2. Populate the required fields and select **Salesforce** as **User License**, and the profile created in step 1 (in this case the profile name is Merge1), then scroll down and click **Save**.

Step 3: Retrieving Access Token

1. Click on your username at the top right corner of the production environment and select **My Settings**.



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

SOURCES



Chatter

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. **Private** and **Broadcast Only** options are selected (as shown in the picture).

Group Edit
New Group

Basic Information

Group Name: Private Group
Owner: Owner

Description:

Automatic Archiving: Don't automatically archive this group.

Group Access

Public Everyone can see updates and join.
 Private Only members can see updates. Membership requires approval.
 Allow customers You can invite customers to this group.
 Broadcast Only Only group owners and managers can create new posts. Group members can comment on the posts.

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

https://eu8.salesforce.com/_ui/core/chatter/groups/GroupProfilePage?g=0F90N000000gPf8

Chatter > Groups > Private Group

Post File New Event More

Share with Private Group Share

Show All Updates

There are no updates.

3. Create new label named as "Private Group Id".

- Go to Setup > Custom Labels.
- Click "New Custom Label"

All

Custom Labels are custom text values, up to 1,000 characters, that can be accessed from Apex Classes or Visualforce Pages. If Translation Workbench has been enabled for your organization, these labels can then be translated into any of the languages salesforce.com supports. This allows developers to create true multilingual apps by presenting information to users - for example, help text or error messages - in their native language. You can create up to 5,000 custom labels.

View: All | Create New View

New Custom Label

Name	Categories	Short Description	Value	Language
No records to display.				

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | Other | All

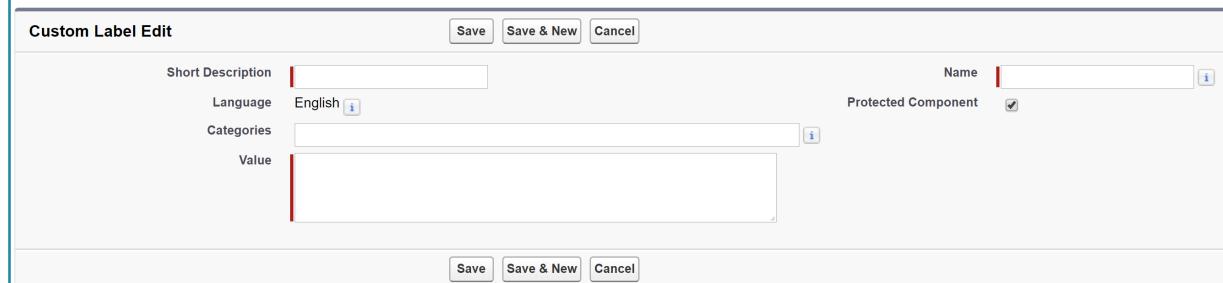
SOURCES



Chatter

- c. Short Description: "Private Group Id"
- d. Name: "Private_Group_Id"
- e. Value: Insert group Id of private group

New Custom Label



A screenshot of the 'Custom Label Edit' screen in Salesforce. The title bar says 'New Custom Label'. The form has fields for 'Short Description', 'Language' (set to English), 'Categories', 'Name' (unchecked), 'Protected Component' (checked), and 'Value'. There are 'Save', 'Save & New', and 'Cancel' buttons at the top and bottom.

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

SOURCES



Chatter

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. **Process messages in the last X days** allows specifying the timeline for messages to be processed.

The screenshot shows the 'CHATTER CONFIGURATION' dialog. It contains four input fields: 'Username' with the value 'michael@globanetconsulting', 'Password' with several dots, 'Security Token' with several dots, and 'Process messages in the last' with the value '20' followed by 'days'.

ADVANCED CONFIGURATION OPTIONS

- The **Auto Update** feature will ensure that the connector is updated to the latest version. Each time the Importer is run, it contacts Globanet server(s) and updates the connector if a newer version is available.
- 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.
- Options **Do Not Download Data Modified Before** and **Do Not Download Data Modified After** allow to cut off data outside the set date range. If the Before date is set to 04/17/2016 and the After is set to 08/25/2018 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.

The screenshot shows the 'ADVANCED CONFIGURATION OPTIONS' dialog. It includes a checkbox for 'Auto Update', a text field for 'Subject Prefix', and two date range filters. Each filter has a checkbox ('Do not download data modified before/' or 'Do not download data modified after'), a date input field, and a calendar icon.

When both **Process messages in the last X days** and **Do not download Data Modified Before/After** are set, the priority is given to the timeline set in Process messages in the last X days.

SOURCES



Chatter

Example of sample message:

A screenshot of a Chatter message feed. At the top, there's a profile picture of Michael Admin (MA) and the timestamp "Mon 11/5/2018 3:17 PM". Below that is the message text "Michael Admin <michael@example.com> Chatter test file". Underneath the message is a "To" field showing "Integration User; Chatter Expert; Security User". A file attachment is shown with the name "test.txt" and size "133 bytes". In the main message area, there's a reply from "MICHAEL ADMIN" at "November 5 at 11:17 AM" with the text "test file". At the bottom, it says "Post Type: ContentPost".

Mon 11/5/2018 3:17 PM

Michael Admin <michael@example.com>

Chatter test file

To Integration User; Chatter Expert; Security User

test.txt 133 bytes

MICHAEL ADMIN - November 5 at 11:17 AM

test file

Post Type: ContentPost

NEXT STEPS

After setting up the Source follow the appropriate links below to continue with the configuration of Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users (preferred option for Chatter is **All (Based on Native API)**, the users will be retrieved automatically)
- Filters (Chatter works with all filters except **XML Filter**)
- Targets
- Importer Settings

CHATTER CIPHER CLOUD



Chatter
Cipher Cloud

ABOUT CHATTER CIPHER CLOUD

Chatter is an enterprise collaboration platform from Salesforce, a cloud-based customer relationship management (CRM) vendor. Chatter can be used as a company intranet or employee directory.

Merge1 Chatter Connector does not use opt-in for the monitored users, it needs to log into the sales force with Admin and get user personal token to import data. Besides, triggers need to be published on Chatter site to be able to capture updates, deletes, and edits. The triggers will create a post in a channel and Merge1 will capture the information from the channel.

Merge1 supports Shield Platform Encryption without any additional configuration in Merge1, since the data is encrypted by Salesforce "At rest" and the API provides the data decrypted.

ACTIVITIES CAPTURED

- Posts
- Files
- Comments
- Shares
- Deletes (Requires triggers)
- Edits (Requires triggers)
- Links
- Polls
- Private Chats
- Edits (Requires triggers)
- Group Chats
- All online communication, including attachments and deleted information (if the triggers are set)

SOURCES



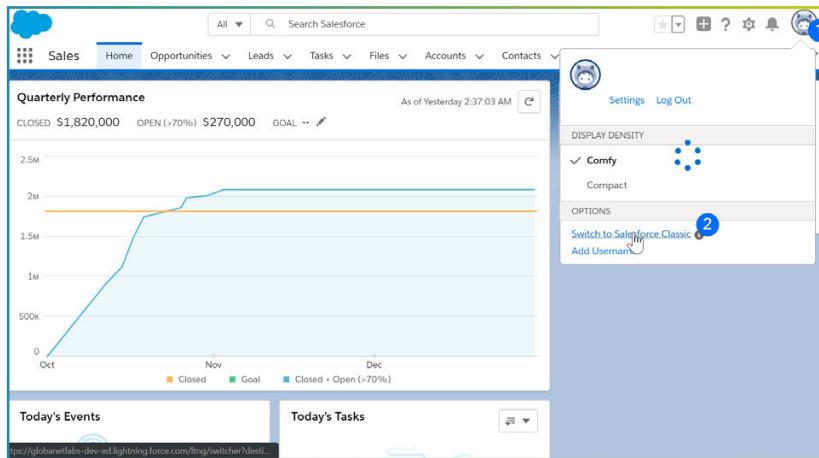
Chatter
Cipher Cloud

CREATING SALESFORCE APPLICATION AND ACQUIRING A TOKEN

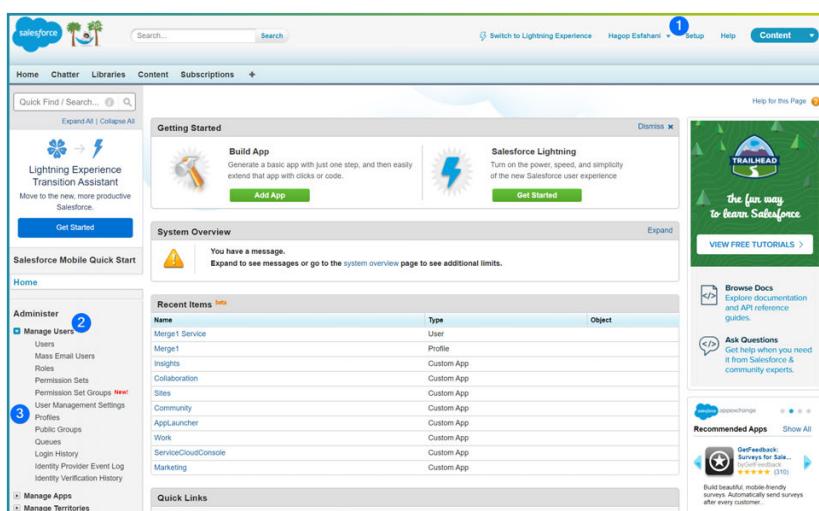
To perform the steps below you'll need a Salesforce account with System Administrator profile, if you do not have access to a System Administrator user, please contact your Salesforce admin and ask for the permissions required to perform the steps below in your Salesforce environment.

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're using the Lightning Experience).



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



SOURCES



Chatter
Cipher Cloud

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

The screenshot shows the Salesforce 'Profiles' page. At the top, there's a navigation bar with 'Home', 'Chatter', 'Libraries', 'Content', 'Subscriptions', and a search bar. Below it is a 'Quick Find / Search...' field. The main area is titled 'Profiles' with a sub-header 'All Profiles'. A table lists profiles: 'Action' (checkbox), 'Profile Name' (dropdown), 'User License' (checkbox), and 'Cust' (checkbox). One row is selected, highlighted with a blue border: 'Edit | Clone' (button) → 'ReadOnly' (Profile Name) → 'Salesforce' (User License). The 'ReadOnly' row has a checked 'Cust' checkbox. Other rows include 'Edit | Del.' and 'ReadOnly1'. At the bottom, there are pagination controls ('1 of 1') and a help link ('Help for this Page').

- Enter a name for the profile and click the **Save** button.

The screenshot shows the 'Clone Profile' dialog box. It has a title 'Clone Profile' and a sub-instruction 'Enter the name of the new profile.' Below this is a section 'You must select an existing profile to clone from.' It shows an 'Existing Profile' dropdown set to 'Read Only' and a 'User License' dropdown set to 'Salesforce'. A text input field 'Profile Name' contains 'Merge1' (marked with a blue circle 1). At the bottom are 'Save' and 'Cancel' buttons (marked with a blue circle 2).

- Click **Edit**.

The screenshot shows the 'Profile' edit page for 'Merge1'. The top navigation bar includes 'Home', 'Chatter', 'Libraries', 'Content', 'Subscriptions', and a search bar. The main content area starts with a 'Profile' header and a 'Merge1' sub-header. It displays a list of permissions and record types. Below this is a 'Profile Detail' section with fields: 'Name' (Merge1), 'User License' (Salesforce), 'Custom Profile' (checkbox checked), 'Created By' (Hagop.Esfahani, 11/8/2019, 2:03 AM), and 'Modified By' (Hagop.Esfahani, 11/8/2019, 2:03 AM). There are 'Edit', 'Clone', 'Delete', and 'View Users' buttons. The 'Console Settings' section shows 'Console Layout' with an '[Edit]' button. The 'Page Layouts' section lists various global and specific page layouts for different objects like Account, Asset, Case, etc., each with their respective 'View Assignment' status. At the bottom, there are 'Feed Item', 'Goal', 'Goal Link', 'Group', and 'Idea' sections with their own layout assignments.

SOURCES



Chatter
Cipher Cloud

The required permissions for Merge1 are:

Administrative Permissions:

- API Enabled
- Select Files from Salesforce
- Manage Chatter Messages and Direct Messages
- View All Data
- Modify All Data (Only if capturing Feedpoll Choices is required, otherwise can be ignored but errors will be present in the connector log. This is a limitation from Salesforce).

Note that when you enable View All Data , Read and View All permissions will be selected for all Standard Object Permissions and other view only permissions ,do not disable these permissions.

6. Scroll down and click **Save**.

The screenshot shows the 'Session Settings' page in the Salesforce setup. It includes sections for 'Feedback Question Sets', 'Feedback Requests', 'Feedback Templates', 'Streaming Channels', and 'DmSync Integration Clients'. The 'Session Settings' section contains fields for 'Session Times Out After' (set to '2 hours of inactivity'), 'Session Security Level Required at Login' (set to 'None'), and various password policy configurations. At the bottom right of the form, there is a red arrow pointing to the 'Save' button.

Step 2: Create a User (Service Account)

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

The screenshot shows the 'Users' page in the Salesforce Lightning Experience. On the left, there's a sidebar with 'Lightning Experience Transition Assistant' and 'Salesforce Mobile Quick Start' sections. The main area shows a table of users with columns for 'Action', 'Full Name', 'Alias', 'Username', 'Last Login', 'Role', 'Active', 'Profile', and 'Manager'. There are 5 users listed: 'Chatter_Expert', 'Esfahani_Haggar', 'Service_Merge1', 'User_Integration', and 'Winder_Grant'. Below the table are buttons for 'New User', 'Reset Password(s)', and 'Add Multiple Users'. A red arrow points to the 'New User' button.

SOURCES



Chatter
Cipher Cloud

2. Populate the required fields and select **Salesforce** as **User License**, and the profile created in step 1 (in this case the profile name is Merge1), then scroll down and click **Save**.

The screenshot shows the 'Edit User' page for a user named 'Merge1'. The 'User License' field is set to 'Salesforce'. The 'Profile' field is set to 'Merge1'. The 'Save' button at the bottom left is highlighted with a yellow box.

Step 3: Retrieving Access Token

1. Click on your username at the top right corner of the production environment and select **My Settings**.



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

The screenshot shows the 'Reset My Security Token' page. The 'Reset Security Token' button is highlighted with a red box.

SOURCES



Chatter
Cipher Cloud

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. **Private** and **Broadcast Only** options are selected (as shown in the picture).

The screenshot shows the 'Group Edit' screen for creating a new group named 'Private Group'. Under 'Basic Information', the 'Owner' is set to 'Owner'. Under 'Automatic Archiving', the radio button for 'Don't automatically archive this group' is selected. In the 'Group Access' section, 'Private' is selected, and 'Broadcast Only' is checked. The URL in the browser is https://eu8.salesforce.com/_ui/core/chatter/groups/GroupProfilePage?g=0F90N0000000gPf8.

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

The screenshot shows the 'Private Group' page in the Chatter interface. The URL in the browser is https://eu8.salesforce.com/_ui/core/chatter/groups/GroupProfilePage?g=0F90N0000000gPf8. The page displays a placeholder image for the group profile and a message stating 'There are no updates.'

3. Create new label named as "Private Group Id".

- Go to Setup > Custom Labels.
- Click "New Custom Label"

The screenshot shows the 'Custom Labels' page in the Salesforce Setup. A red arrow points to the 'New Custom Label' button at the top right of the main table area. The table has columns for Name, Categories, Short Description, Value, and Language. The URL in the browser is https://eu8.salesforce.com/setup/customlabels.

SOURCES



Chatter
Cipher Cloud

- c. Short Description: "Private Group Id"
- d. Name: "Private_Group_Id"
- e. Value: Insert group Id of private group

New Custom Label

Custom Label Edit

Save Save & New Cancel

Short Description	English	Name
Language	Categories	Protected Component
Value		<input checked="" type="checkbox"/>
Save Save & New Cancel		

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

SOURCES



Chatter
Cipher Cloud

CHATTER CONFIGURATION

1. Enter the Instance URL of your Chatter environment in the **Host** field.
2. Enter the **Username** and **Password** of the Chatter Admin account used for app creation.
3. Enter the previously copied **Security Token**.
4. **Process messages in the last X days** allows specifying the timeline for messages to be processed.

CHATTER CIPHER CLOUD CONFIGURATION

Host []

Username []

Password []

Security Token []

Process messages in the last days

ADVANCED CONFIGURATION OPTIONS

- The **Auto Update** feature will ensure that the connector is updated to the latest version. Each time the Importer is run, it contacts Globanet server(s) and updates the connector if a newer version is available.
- 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.
- 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 04/17/2016 and the After is set to 08/25/2018 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.

ADVANCED CONFIGURATION OPTIONS

Auto Update

Subject Prefix []

Do not download data modified before: []

Do not download data modified after: []

When both **Process messages in the last X days** and **Do not download Data Modified Before/After** are set, the priority is given to the timeline set in Process messages in the last X days.

SOURCES



Chatter
Cipher Cloud

Example of sample message:

Mon 11/5/2018 3:17 PM

Michael Admin <michael@example.com>

Chatter test file

To Integration User; Chatter Expert; Security User

 test.txt
133 bytes

MICHAEL ADMIN - November 5 at 11:17 AM

test file

Post Type: ContentPost

NEXT STEPS

After setting up the Source follow the appropriate links below to continue with the configuration of the Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users (preferred option for Chatter Cipher Cloud is **All (Based on Native API)**, the users will be retrieved automatically)
- Filters (Chatter Cipher Cloud works with all filters except **XML Filter**)
- Targets
- Importer Settings

SLACK



Slack

HOW TO SET UP THE SLACK IMPORTER

After selecting the Slack icon in the Configuration Wizard and clicking **Next** you will be redirected to the next screen of the Configuration. As mentioned earlier the Configuration Wizard Screen consists of 5 tabs. You will be prompted to start with Source Configuration.

Slack Source Configuration tab has the following Settings options (click on the name to open the relevant configuration information):

- Slack Application Configuration
- Optional Settings (visible only after you provide all the required information)

CONFIGURATION WIZARD

SOURCE MONITORED USERS FILTERS TARGETS SETTINGS

Please provide the following credentials to your company's Slack app so that Merge1 can be configured to access your monitored users' account data.

If you do not have an app created for Slack, please [click](#) for more information.

SLACK APPLICATION CONFIGURATION

Workspace URL	<input type="text" value="domain"/>	.slack.com
Application ID	<input type="text"/>	
Application Secret/Key	<input type="text"/>	

BACK **NEXT**

SOURCES



Slack

SLACK APPLICATION CONFIGURATION

1. Provide your corporate **Slack's Team Name** (usually it looks like this: companyname.slack.com).
2. Enter the Client ID in the Application ID field and the Client Secret/Key in the Application Secret/Key field..
3. When you provide all the mentioned information you will see Slack Optional Settings. Setup the Advanced Configuration Options for Merge1 Slack Importer.
 - The **Auto Update** setting will ensure that the latest message formats and bug fixes are updated within Merge1's architecture each time the Importer is run.
 - 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.
 - The **Do not download data modified before** check will ensure that old or irrelevant data is excluded.
4. When you are finished with the configuration click **Next**.

CONFIGURATION WIZARD

SOURCE	MONITORED USERS	FILTERS	TARGETS	SETTINGS
SLACK CONFIGURATION:				
Slack users were identified in your environment. You will have the option to add them to the Monitored Users list in the next section.				
ADVANCED CONFIGURATION OPTIONS				
<input type="checkbox"/> Auto Update Subject Prefix <input type="text"/> <input type="checkbox"/> Do not download data modified before: <input type="text"/> <input type="button"/>				
<input type="button" value="BACK"/>		<input type="button" value="NEXT"/>		

SOURCES



Slack

CREATING A SLACK APPLICATION:

In case you do not have a Slack application, you can carry out the following steps to create a Slack application to be used in Merge1.

- 1.** Log in to your Slack team's administrator account and navigate to "<https://api.slack.com/apps>".
- 2.** Click **Create New App**.
- 3.** Specify a **Name, Short Description** and **Long Description**.
- 4.** In the **Callback URI** field, enter the URL of your local Merge1 environment with the following extension: **/Configuration/OAuthCallback**.
- 5.** Click **Create App**.
- 6.** On the menu to the left, select **OAuth & Permissions** to view the Application ID & Secret.

Please note:

Slack connector requires opt-in from the users that are going to be monitored. More information on how the opt-in works is given in the Reports section of this guide.

SLACK eDISCOVERY



ABOUT SLACK eDISCOVERY CONNECTOR

Slack eDiscovery Connector 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 own team ID, its own directory of members, its own channels, conversations, files, and zeitgeist.

To set up the Slack eDiscovery connector you will be required to contact Globanet support at support@globanet.com with the redirect URL and within **24 hours** we will whitelist the IP and the server and send you a confirmation. In addition, Slack should be contacted at **exports@slack.com** and asked to enable **Discovery API** for your organization before finishing the connector set up.

ACTIVITIES CAPTURED & WORKSPACES

- Activities captured from all workspaces
- Direct Messages
- 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 text)
- Deletes (including the deleted message and the event itself)*
- Edits (including the message before and after it is edited)*
- Channel join
- Set Channel purpose
- Guest conversations
- File Deletes

* This depends 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.

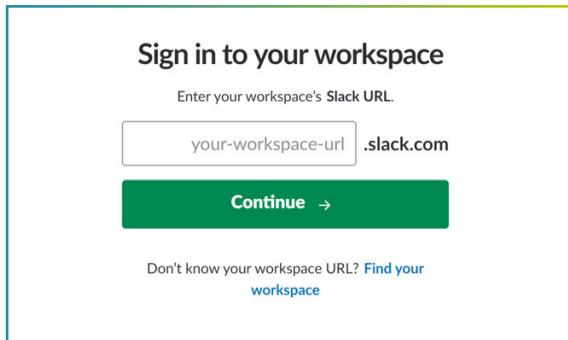
SOURCES



Slack
eDiscovery

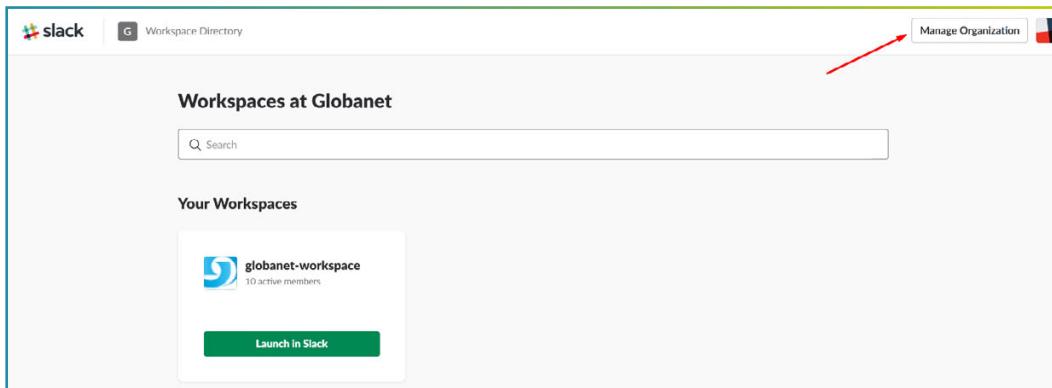
HOW TO SET UP THE SLACK eDISCOVERY CONNECTOR

1. Log into your Slack Enterprise workspace using the organization URL.
You should stay logged into your account when adding a Merge1 connector.



The screenshot shows the 'Sign in to your workspace' page. It has a text input field labeled 'Enter your workspace's Slack URL.' containing 'your-workspace-url.slack.com'. Below it is a green 'Continue →' button. At the bottom, there's a link 'Don't know your workspace URL? Find your workspace'.

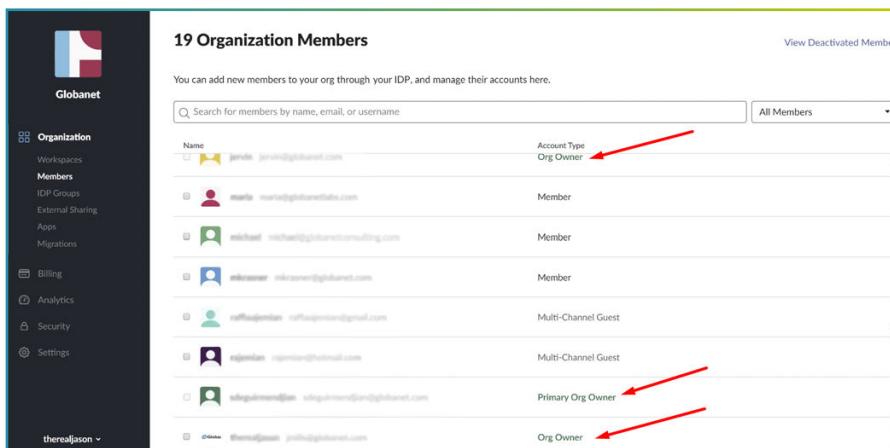
2. Click on **Manage Organizations** on the upper right corner.



The screenshot shows the 'Workspaces at Globanet' page. On the right side, there is a 'Manage Organization' button with a red arrow pointing to it. Below it, there is a section titled 'Your Workspaces' showing a workspace named 'globanet-workspace' with 10 active members and a 'Launch in Slack' button.

3. Enter the necessary workspace

4. Confirm that the account used for configuring Merge1 has the necessary permissions, e.g. is either a **Org. Owner** or a **Primary Org. Owner**. **Org. Owners** control the highest-level security and administrative settings, but only the **Primary Org. Owner** (usually the person who created the workspace) can delete it.



The screenshot shows the '19 Organization Members' page. On the left, there is a sidebar with 'Globanet' and various organization management options like 'Workspaces', 'Members', 'IDP Groups', etc. The main area shows a table of members:

Name	Account Type
jason_jason@globanet.com	Org Owner
maria_maria@globanetstatus.com	Member
michael_michael@globanetconsulting.com	Member
niko@niko@globanet.com	Member
raffaelraffael@globanet@gmail.com	Multi-Channel Guest
rajman_rajman@hotmail.com	Multi-Channel Guest
sdegalmed@sdegalmed@sdegalmed@globanet.com	Primary Org Owner
therealjason_@therealjason@therealjason@globanet.com	Org Owner

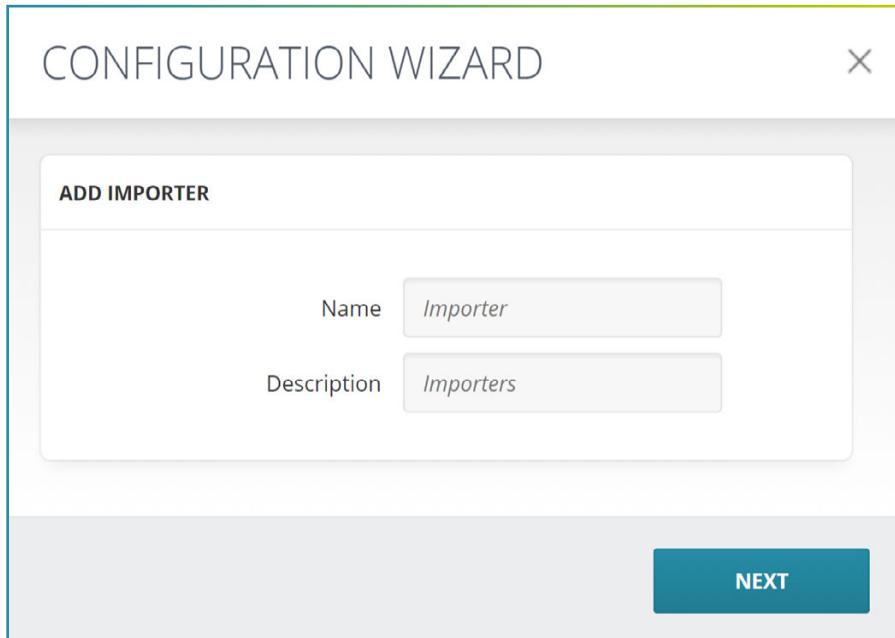
Red arrows point to the 'Org Owner' and 'Primary Org Owner' entries in the list.

SOURCES

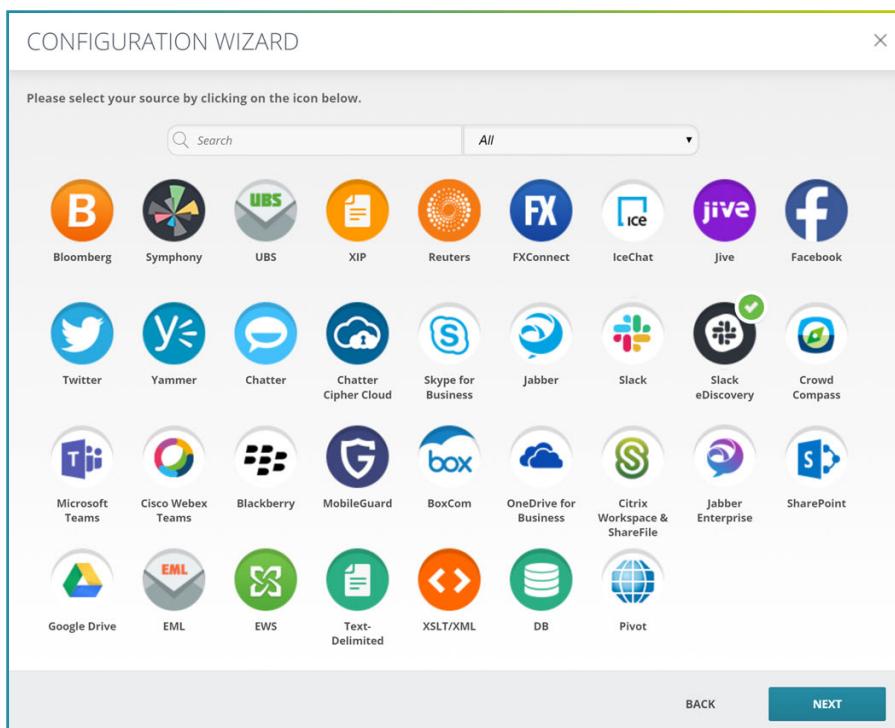


Slack
eDiscovery

5. Leave the window open.
6. Go to Merge1 Connector and add click on **Add Importer**.
7. Add a name to the importer and description. It is advised to use a name that will help you distinguish multiple Importers from one another if you're going to use the same source more than one time.



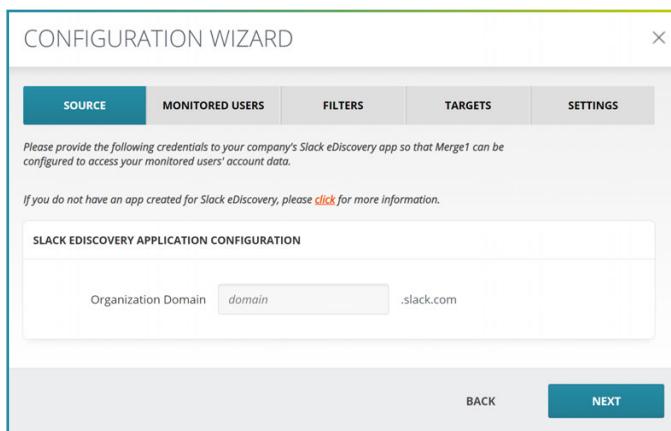
8. Select **Slack eDiscovery** from the options and click Next.



SOURCES

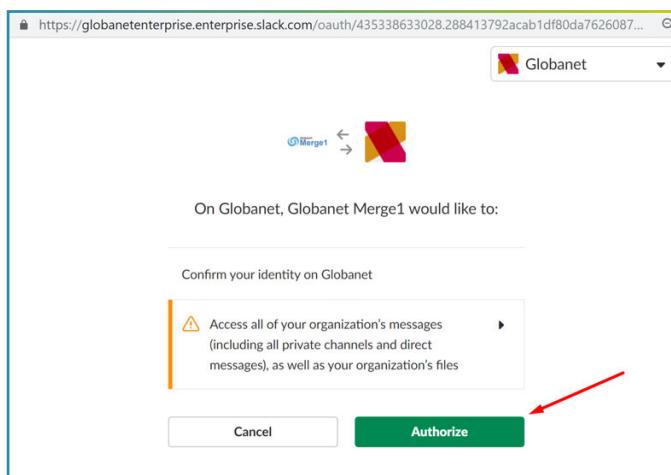


9. Send the Redirect URL "<https://yourdomain.com/Configuration/OAuthCallback>" (for example, <https://globanet.com/Configuration/OAuthCallback>) to **support@globanet.com** and wait 24 hours before configuring your Slack eDiscovery Connector. This is needed for us to whitelist the IP address and the server. As soon as it's done, you'll receive a confirmation from us.
10. After receiving a confirmation from us, contact **exports@slack.com** and ask to enable **Discovery API** for your organization.
11. 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 "globanet.enterprise.slack.com" should be filled in as "globanet".



12. Click **Next** to initialize the connection after the **Discovery API** is enabled. **Discovery API** allows use approved third-party apps (in this case Merge1) to export, archive, or meet other security and compliance obligations for any organization content.

13. Authorize the connection between Slack eDiscovery and Merge1.



9. Go to the next step to set up **Advanced Configuration Options**.

SOURCES



ADVANCED CONFIGURATION OPTIONS

There are following advanced options when configuring the connection with Merge1.

- The **Auto Update** feature will ensure that the connector is updated to the latest version. Each time the Importer is run, it contacts Globanet server(s) and updates the connector if a newer version is available.
- If the option **Single Message per Channel** is enabled, Merge1 retrieves the data from a channel and archives it as one message.
- The option **Split by Day** merges the messages from the same day into one email message. The time zone by which the messages are split can be selected from the drop-down menu. When Process Incomplete Days option is enabled, the messages of the days that haven't yet ended will be imported in a separate email as well. This option can be selected only if Single Message per Channel is selected.
- When the option **Import Archived Channel** is selected, Merge1 imports the data from archived 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.
- 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 04/17/2016 and the After is set to 08/25/2018 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.

When you are finished with the configuration click **Save**.

ADVANCED CONFIGURATION OPTIONS

Auto Update

Single Message per Channel

Split By Day

Message Time Zone
 ▼

Process Incomplete Days

Import Archived Channel

Subject Prefix

Do not download data modified before: ▼

Do not download data modified after: ▼

SOURCES



Slack
eDiscovery

Example of Single Message:

A screenshot of a Slack Direct Message interface. At the top left is a user icon for 'RJ' (represented by a grey circle with 'RJ' in white). To its right is the timestamp 'Thu 9/27/2018 2:14 PM'. Below the timestamp is the recipient's name 'jervin <jervin@globanet.com>' and the message subject '@jervin Direct Messages-DIRECT MESSAGES 2018-09-27...'. Underneath this, it says 'To michael'. The message body shows a single message from 'JERVIN' at 02:14 PM: 'single message'. Below the message is a light grey bar containing the text 'Channel: DIRECT MESSAGES' and 'Type: message'.

Example of Single Message per Channel:

A screenshot of a Slack channel interface. At the top left is a user icon for 'RJ'. To its right is the timestamp 'Tue 9/25/2018 8:03 AM'. Below the timestamp is the recipient's name 'jervin <jervin@globanet.com>' and the message subject 'Slack - @jervin Direct Messages-DIRECT MESSAGES 20...'. Underneath this, it says 'To'. The message body shows two messages from 'JERVIN': one at 08:03 AM labeled 'draft message' and another at 08:04 AM labeled 'another draft'. Below these messages is another message from 'JERVIN' at 10:13 AM with the text 'Type: message'. At the bottom of the message list is the number '1'.

NEXT STEPS

After setting up the Source follow the appropriate links below to continue with the configuration of the Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users (preferred option for Slack eDiscovery is **All (Based on Native API)**, the users will be retrieved automatically)
- Filters (Slack eDiscovery works with all filters except **XML Filter**)
- Targets
- Importer Settings

BLACKBERRY



Blackberry

HOW TO SET UP THE BLACKBERRY IMPORTER

After selecting the Blackberry icon in the Configuration Wizard and clicking **Next** you will be redirected to the next screen of the Configuration. As mentioned earlier the Configuration Wizard Screen consists of 5 tabs. You will be prompted to start with Source Configuration.

Blackberry Source Configuration tab has the following Settings options (click on the name to open the relevant configuration information):

- FTP configurations
- PGP configurations
- Folders (Required)
- Blackberry Options
- Blackberry Filtering
- Misc Settings

CONFIGURATION WIZARD

SOURCE MONITORED USERS FILTERS TARGETS SETTINGS

Please provide your Blackberry configuration data so that Merge! can access your Blackberry data.

FTP

Download files from FTP

FTP CONFIGURATION OPTIONS +

Execute script against source files

Script file *

PGP

Use PGP Decryption

PGP DECRYPTION OPTIONS +

BLACKBERRY OPTIONS

Connector Type

Source Time Zone

BLACKBERRY FILTERING

Filter by status types (separated by '|'):

Filter by status subtypes (separated by '|'):

Filter by commands (separated by '|'):

BACK

SOURCES



Blackberry

FTP CONFIGURATIONS

Merge1 retrieves data from Blackberry **FTP** and stores it in the Import Folder for processing. Corrupt files are moved to the **Quarantine Folder**.

If you want to get data from Blackberry through FTP, tick **Download files from FTP**. FTP Configuration options will automatically open.

FTP

Download files from FTP

FTP CONFIGURATION OPTIONS

Use SSH Key Authentication

CONNECTION 1

Host * Port *
Path *
Connection Type

Use Security
 Implicit SSL
 Explicit SSL
 SSH

AUTHENTICATION 2

Anonymous Access

Username *
Password *

FILE FILTER 3

Include
 Exclude
*

FILTER BY TIME 4

None
 Only download files modified within the last: days
 Only download files modified:
 Later than
 Earlier Than
Server Time Zone

OPTIONS 5

Maintain history of downloaded file for days (0 = infinite)
 Download subdirectories recursively
 Delete files on server after downloading

Execute script against source files **6**

Script file *

Download script file

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 21. Choose FTP connection type from the Connection type dropdown list. FTP can run in either passive or active mode. Information about the connection type should be provided by the FTP host. If you wish to use FTP over SSL, select **Use SSL** checkbox and choose connection method: implicit or explicit.

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 checkbox, which is the default setting.

3. File Filter. This filter is used to 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. This filter is used for separating 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 modified within the mentioned days will be downloaded.
- Only download files modified earlier than/later than. When this option is 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 of time.
- 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. 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.

SOURCES



Blackberry

- Download subdirectories recursively. If checked, files from the subdirectories of the mentioned path will be downloaded too.
- Delete files on server after downloading. If checked, the files downloaded will be deleted from the server.

6. Execute script against source files allows the user to utilize alternative methods of data download or acquisition methods other than FTP. For example, batch script files that download information via an FTP alternative and move it into the appropriate processing folder.

PGP CONFIGURATIONS

PGP DECRYPTION OPTIONS

Username *

Password *

Email *

Generated Public Key *

EXPORT PUBLIC KEY

Export/Import Private Key

EXPORT PRIVATE KEY IMPORT PRIVATE KEY

GENERATE KEY

1. Click **Use PGP Decryption** and PGP Decryption Options open.
2. Specify a Username, Password, and Email, then click **Generate Key**. Once the key is generated you will see a green tick icon. **
3. Log into your Blackberry control panel and enable PGP encryption by adding Merge1 Keys.
4. In your Blackberry control panel click **Add** and the Add Public Key window will appear. From the Key Type drop-down menu, select Encryption and paste the full contents of the public key (including the block header and footer) under the Public Keys tab at control panel in your terminal.
5. Click the Decryption button. (The key appears in the Public Keys section). To save the PGP encryption key to your account click **Submit**.

* Please note that this password is required for configuring multiple connectors with the same PGP Key.

* Use the Export Public / Private Key buttons to save the keys to a secure location on your device. This will enable you to restore the keys if they are lost or when moving the database to a new machine.

SOURCES



Blackberry

FOLDER CONFIGURATION (REQUIRED*)

After successfully setting up the FTP and PGP Configurations, you will have to change the folder configurations. In Merge1 you will have to specify the **Import Folder**, where you would like to store the data after retrieving it from Blackberry, 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 Blackberry Merge1.

FOLDERS
Import folder*
<input type="text"/>
<input type="checkbox"/> Traverse subdirectories
Quarantine folder*
<input type="text"/>
AFTER SUCCESSFULL IMPORTING
<input checked="" type="radio"/> Move original files into a subfolder of the Import folder.
<input type="radio"/> Delete original files permanently.

Under **After Successfully 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. Please note that once deleted, the files cannot be recovered.

Please note:

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.

* Merge1 Folder Option 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.

SOURCES



Blackberry

OPTIONS

The Blackberry source can only process one format at a time. You have four **Connector Types** to choose from:

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

BLACKBERRY OPTIONS	
Connector Type	P2P
Source Time Zone	Local Timezone

Once you have selected the Connector Type, you can also provide the **Source Time Zone** information. Merge1 assumes that the messages in the source file are of the set timezone and based on that data the dates in the messages are processed to UTC timezone. 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 will be imported. Separate each name with the following symbol " | ". Please note, that wildcards are NOT supported for the following field.

Each source type has different filtering options. P2P type can be filtered with status types and commands. SMS sources can be filtering by all displayed options. Messenger type can be filtered only by commands. VideoChats can not be filtered at all.

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

BLACKBERRY FILTERING

Filter by status types (separated by '|'):

Filter by status subtypes (separated by '|'):

Filter by commands (separated by '|'):

SOURCES



Blackberry

MISCELLANEOUS SETTINGS

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

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.

MISC SETTINGS

Files to import: e.g.: *.txt|*.xml (separated by vertical bars)*

*.CSV

Subject prefix

Example of SMS Message:

Mon 7/1/2013 7:46 PM

 John.Doe@example.com

Got it!

To +19177789123

(i) We removed extra line breaks from this message.

NYC-BES10A_sms_1.0_20130701_0001.CSV

Name#ID: NYC.example.COM/JDoe

Email Address: John.Doe@example.com

Type of Message: Outgoing

To: +19175365750

From:

Callback Phone Number:

Body: Got it!

Sent/Received Date: 7/1/2013 3:45:30 PM UTC Server Log Date: 7/1/2013 11:46:56 AM UTC Message Status: Tx_Sent

Command: -

UID: -

SOURCES



Blackberry

Example of VideoChat Message:

Mon 7/1/2013 7:39 PM
2B00A445
BBM Video Chat Record

To NYC.example.COM/MSmith
(i) We removed extra line breaks from this message.

Name.ID: NYC.example.COM/MSmith
Type of Call: Incoming
Media Type: Video
Name: John Doe
SIP Address: 2B00A445@sip.voip.blackberry.com Start Date: 2013/07/01 19:39:00 Elapsed Time: 45 Server Log Date: 2013/07/01 15:43:49 EDT

NEXT STEPS

After setting up the connector follow the appropriate links below to continue with the configuration of the Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users is not applicable to this connector.
- Filters (all filters except **XML filter**)
- Targets
- Importer Settings

SYMPHONY



ABOUT SYMPHONY CONNECTOR

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.

Symphony connector works with XML format only. Make sure that the files are in the correct format.

Symphony connector can also process zipped XML files, it's not necessary to unzip them.

There are following mappings of XML tags to emails:

- <initiator> = From
- <sentTo> = To
- <readBy> = CC

ACTIVITIES CAPTURED

- Post Date
- From
- Message Content
- Record Type
- Message ID
- Attachment
- Downloaded By
- Event Action
- Read By

SOURCES



Symphony

FTP CONFIGURATIONS

Merge1 retrieves data from Symphony **FTP** and stores it in the Import Folder for processing. Corrupt files are moved to the **Quarantine Folder**.

If you want to get data from Symphony through FTP, tick **Download files from FTP**. FTP Configuration options will automatically open.

The screenshot shows the 'FTP' configuration page with the following sections:

- CONNECTION (1):** Host: *, Port: 21, Connection Type: Active.
- AUTHENTICATION (2):** Anonymous Access checked, Username: [redacted], Password: [redacted].
- FILE FILTER (3):** Include selected, Filter: *.
- FILTER BY TIME (4):** Only download files modified within the last: 1 days.
- OPTIONS (5):** Maintain history of downloaded file for 5 days (0 = infinite), Download subdirectories recursively, Delete files on server after downloading.
- EXECUTE SCRIPT (6):** Execute script against source files, Script file: [redacted], UPLOAD, DOWNLOAD.

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 21. Choose FTP connection type from the Connection type dropdown list. FTP can run in either passive or active mode. Information about the connection type should be provided by the FTP host.

If you wish to use FTP over SSL, select **Use SSL** checkbox and choose connection method: implicit or explicit.

2. Authentication. To authenticate an FTP connection, enter the appropriate information in the Username and Password textboxes, respectively. To enable anonymous FTP connections, select the Anonymous Access checkbox, which is the default setting.

3. File Filter. This filter is used to 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. This filter is used for separating 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 modified within the mentioned days will be downloaded.
- Only download files modified earlier than/later than. When this option is selected, the data modified earlier than or later than the mentioned date will be downloaded. Both options can be selected simultaneously to choose a time period.
- Server Time Zone specifies the time zone in which the FTP sever is located to correctly determine the timestamp of downloadable files.

5. Options.

- Maintain history of downloaded file for X days. 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.

SOURCES



Symphony

- 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.

6. Execute script against source files allows the user to utilize alternative methods of data download or acquisition methods other than FTP. For example, batch script files that download information via an FTP alternative and move it into the appropriate processing folder.

PGP CONFIGURATIONS

PGP DECRYPTION OPTIONS

Username *

Password *

Email *

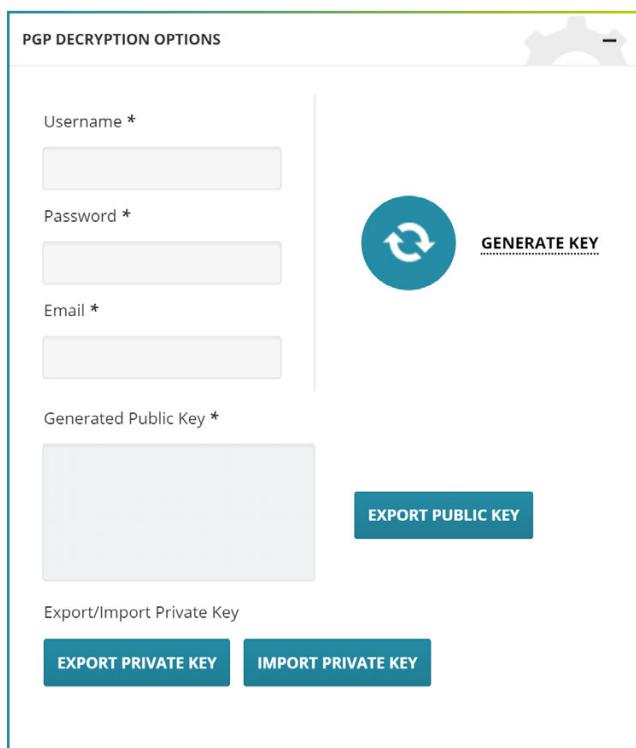
Generated Public Key *

EXPORT PUBLIC KEY

GENERATE KEY

Export/Import Private Key

EXPORT PRIVATE KEY IMPORT PRIVATE KEY



1. Click **Use PGP Decryption** and PGP Decryption Options open.
2. Specify a Username, Password, and Email, then click **Generate Key**. Once the key is generated you will see a green tick icon. **
3. Log into your Symphony control panel and enable PGP encryption by adding Merge1 Keys.
4. In your Symphony control panel click **Add** and the Add Public Key window will appear. From the Key Type drop-down menu, select Encryption and paste the full contents of the public key (including the block header and footer) under the Public Keys tab at the control panel in your terminal.
5. Click the Decryption button. (The key appears in the Public Keys section). To save the PGP encryption key to your account click **Submit**.

* Please note that this password is required for configuring multiple connectors with the same PGP Key.

* Use the Export Public / Private Key buttons to save the keys to a secure location on your device. This will enable you to restore the keys if they are lost or when moving the database to a new machine.

SOURCES



Symphony

FOLDER CONFIGURATION (REQUIRED*)

After successfully setting up the SFTP and PGP Configurations, you will have to change the folder configurations. In Merge1 you will have to specify the Import Folder, where you would like to store the data after retrieving it from Symphony, as well as Quarantine Folder where all the failed messages will be archived.

If you have sub-folders under your Import Folder, you can enable **Traverse Subdirectories** to maintain the sub-folder structure of imported data and include the data in your Symphony Merge1.

FOLDERS
Import folder*
<input type="text"/>
<input type="checkbox"/> Traverse subdirectories
Quarantine folder*
<input type="text"/>
AFTER SUCCESSFULL IMPORTING
<input checked="" type="radio"/> Move original files into a subfolder of the Import folder.
<input type="radio"/> Delete original files permanently.

Under the **After Successfully Importing** settings you can decide what Merge1 will do with the original files. You can either Move the original fines in a subfolder in Importer Folder or you can Delete the files. Please note that once Deleted you can not recover them.

Please note:

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.

MISCELLANEOUS SETTINGS

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

MISC SETTINGS
Subject prefix
<input type="text"/>

* Merge1 Folder Option is a Required Setting Option. If you do not fill in the information, you will not be allowed to proceed to the next screen.

SOURCES



Symphony

ATTACHMENT VALIDATION

Merge1 enables you to develop customized notes for attachment validation. The default setting is **Fail Messages with missing Attachments**, as a result of which the messages that do not have attachments are failed and can be viewed under the Reports.

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 under the Reports you will see only the custom message that you have entered.

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.

ATTACHMENT VALIDATION

Replace all attachments with the following note:
This message contained the following attachments w/

Replace missing attachments with the following note:
This message contained the following attachments th/

Fail messages with missing attachments. (default)

Auto Update

Merge Messages by Thread

Use the timestamp of the first record as message timestamp

Grid Mode | [Select Style](#)

Process messages with "IsArchived" tag

Ignore readyby messages

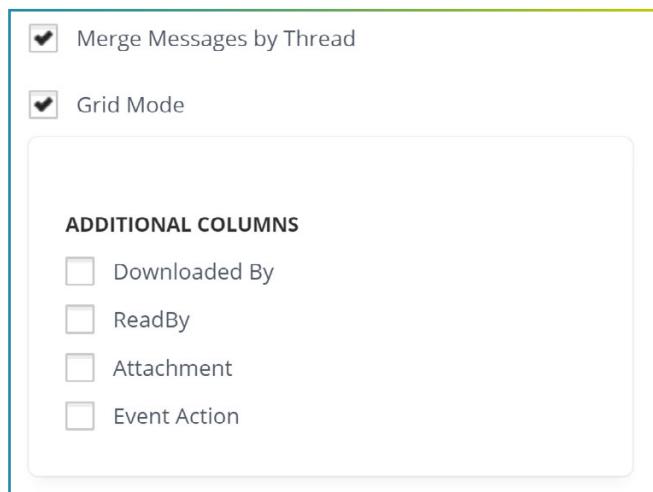
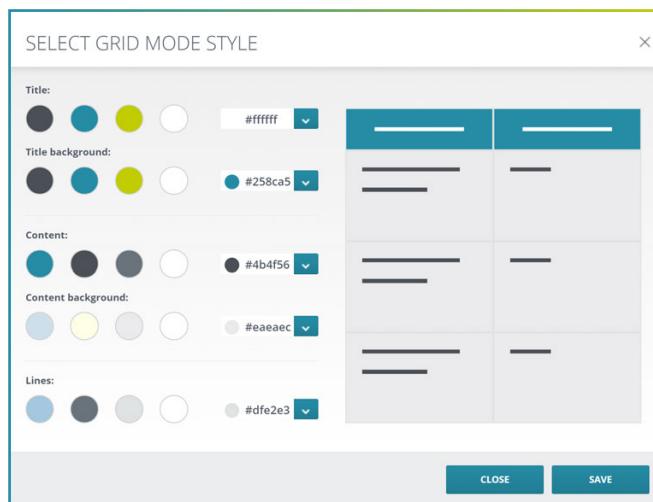
- The **Auto Update** feature, when selected, automatically updates Symphony connector based on the recent changes in Symphony environment before running the import.
- When **Merge Messages by Thread** option is selected, messages with identical thread IDs are grouped into individual emails (as opposed to receiving a separate email per message). It's possible to select additional fields (Downloaded By and Read By) to be added to the merged message (see examples at the end of the connector set up information).
- The **Use the timestamp of the first record as message timestamp** feature can be selected only when Merge Messages by Thread is selected. When enabled, it uses the timestamp of the first Symphony message as a message timestamp, instead of the one of the last message.

SOURCES



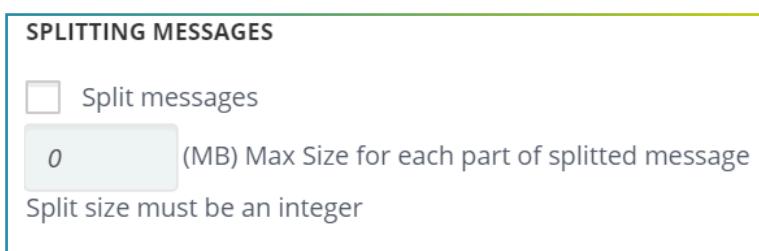
Symphony

- The **Grid Mode** option is activated only when Merge Messages by Thread is selected. It allows viewing the email content in a compact grid format. When Grid Mode is selected additional checkboxes will appear that can activate extra columns in the grided message. The Grid mode color scheme can also be customized.



- When **Process messages with "IsArchived" tag** is checked, messages that have the "IsArchived" tag are processed as well.
- When **Ignore readyby messages** is checked, messages with ReadBy field in them will be ignored.

SPLIT MESSAGE



SOURCES



Symphony

Splitting Messages option allows splitting big files. In the field the size of a split part of the message can be specified so that each part doesn't 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.

Please note:

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.

INCLUDE RECORD TYPE

In this section the types of records that should be processed from Symphony can be specified. At least one type should be selected. There are three types of records from Symphony that can be selected:

- Social Messages
- Event
- Email Notification

INCLUDE RECORD TYPES

- Social Message
- Event
- Email Notification

EXAMPLES

Example of a part of the message from email when Merge Messages by Thread is selected. On the right the message is shown when additional options to show Downloaded By and Readyby are selected.

The screenshot displays two side-by-side email messages from the 'warcicd qa6' account. Both messages are dated Friday, October 26, 2018, at 4:06 PM. The left message shows the standard 'Merge Messages by Thread' behavior. The right message shows the behavior when 'Downloaded By' and 'Readyby' options are selected.

Left Message (Standard Thread Merging):

- From:** warcicd qa6 (companyNameSix) <warcicd-qa6@warcicd.com>
- To:** warcicd qa6 (companyNameSix)
- Cc:** warcicd qa6 (companyNameSix)
- Subject:** warcicd qa6 (companyNameSix) read message :- Content:** warcicd qa6 (companyNameSix) read message :- RecordType:** SOCIALMESSAGE
- MessageId:** BGLP1GvpM0Bneqj1V8cTTn//pnpr5Q8bQ--
- Scope:** PRIVATE
- ConversationScope:** internal
- OwningCompany:** companyNameSix
- SocialMessageType:** CHATROOM
- PostDate:** 10/26/2018 12:07:24 PM

Right Message (With Downloaded By and Readyby):

- From:** warcicd qa6 (companyNameSix) <warcicd-qa6@warcicd.com>
- To:** warcicd qa6 (companyNameSix)
- Cc:** warcicd qa6 (companyNameSix)
- Subject:** warcicd qa6 (companyNameSix) read message :- Content:** warcicd qa6 (companyNameSix) read message :- RecordType:** SOCIALMESSAGE
- MessageId:** BGLP1GvpM0Bneqj1V8cTTn//pnpr5Q8bQ--
- Scope:** PRIVATE
- ConversationScope:** internal
- OwningCompany:** companyNameSix
- SocialMessageType:** CHATROOM
- PostDate:** 10/26/2018 12:07:24 PM
- DownloadedBy:** warcicd-qa6@warcicd.com
- ReadyBy:** warcicd-qa6@warcicd.com

SOURCES



Symphony

Example of email with Grid Mode enabled.

POSTDATE	FROM	MESSAGECONTENT	RECORDTYPE	MESSAGEID
10/26/2018 12:07:24 PM	warcicd qa6 (companyNameSix) <warcicd-qa6@warcicd.com>	warcicd qa6 (companyNameSix) read message : dsadas	SOCIALMESSAGE	BGLPiGvpNd08nqkVVXTTn//pnpy5Q8bQ==
10/26/2018 12:07:24 PM	warcicd qa6 (companyNameSix) <warcicd-qa6@warcicd.com>	warcicd qa6 (companyNameSix) read message : dsadasa	SOCIALMESSAGE	rSSPejW6nyPRFKHEmtNH//pnk1sd0bQ==
10/26/2018 12:07:24 PM	warcicd qa6 (companyNameSix) <warcicd-qa6@warcicd.com>	warcicd qa6 (companyNameSix) read message : DADSA	SOCIALMESSAGE	TAlD/Fg29CgnxO6muu3//pl454QbQ==
10/26/2018 12:07:24 PM	warcicd qa6 (companyNameSix) <warcicd-qa6@warcicd.com>	warcicd qa6 (companyNameSix) read message : test	SOCIALMESSAGE	FJAGRAJXlb2mX+UWcqmden//plie7w8bQ==
10/26/2018 12:07:24 PM	warcicd qa6 (companyNameSix) <warcicd-qa6@warcicd.com>	warcicd qa6 (companyNameSix) read message : test room	SOCIALMESSAGE	k04IcaOLPEH3WTrdN8Wkfhh//plTf7MLbQ==
10/26/2018 12:05:44 PM	warcicd qa6 (companyNameSix) <warcicd-qa6@warcicd.com>	test	SOCIALMESSAGE	FyUEk2ygrTPakd3FIMln//plPu+bMjQ==

Example of email with Grid Mode enabled with additional options checked (DownloadedBy, Readby, Attachment, EventAction, Ready)

POSTDATE	FROM	MESSAGECONTENT	RECORDTYPE	MESSAGEID	ATTACHMENT	DOWNLOADEDBY	EVENTACTION	READY
10/26/2018 12:07:24 PM	warcicd qa6 (companyNameSix) <warcicd-qa6@warcicd.com>	warcicd qa6 (companyNameSix) read message : dsadas	SOCIALMESSAGE	BGLPiGvpNd08nqkVVXTTn//pnpy5Q8bQ==		warcicd-qa6@warcicd.com		
10/26/2018 12:07:24 PM	warcicd qa6 (companyNameSix) <warcicd-qa6@warcicd.com>	warcicd qa6 (companyNameSix) read message : dsadasa	SOCIALMESSAGE	rSSPejW6nyPRFKHEmtNH//pnk1sd0bQ==		warcicd-qa6@warcicd.com		
10/26/2018 12:07:24 PM	warcicd qa6 (companyNameSix) <warcicd-qa6@warcicd.com>	warcicd qa6 (companyNameSix) read message : DADSA	SOCIALMESSAGE	TAlD/Fg29CgnxO6muu3//pl454QbQ==		warcicd-qa6@warcicd.com		
10/26/2018 12:07:24 PM	warcicd qa6 (companyNameSix) <warcicd-qa6@warcicd.com>	warcicd qa6 (companyNameSix) read message : test	SOCIALMESSAGE	FJAGRAJXlb2mX+UWcqmden//plie7w8bQ==		warcicd-qa6@warcicd.com		
10/26/2018 12:07:24 PM	warcicd qa6 (companyNameSix) <warcicd-qa6@warcicd.com>	warcicd qa6 (companyNameSix) read message : test room	SOCIALMESSAGE	k04IcaOLPEH3WTrdN8Wkfhh//plTf7MLbQ==		warcicd-qa6@warcicd.com		

NEXT STEPS

After setting up the connector follow the appropriate links below to continue with the configuration of the Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users is not applicable to this connector.
- Filters
- Targets
- Importer Settings

TEXT-DELIMITED



Text Delimited

ABOUT TEXT-DELIMITED

Merge1 Text Delimited Connector is designed to allow to rapidly develop text delimited file processing. The objective of the connector is to map the text delimited fields to email required format. The mapping is done based on the uploaded XML template. The mapping varies from source to source, it has to be written separately. Contact our support at support@globanet.com for more details on the mapping corresponding to the source you're going to use it for.

ACTIVITIES CAPTURED

- Participants: From, To, CC, and BCC
- Start Time
- End Time
- Body Message
- Custom mappings
- Attachments

Please note:

In order to process the attachments please add the full path to the attachment in the CSV document. In order to prevent files with similar names we recommend creating attachments with folder structure to avoid clash of files with similar name shared on different days and in different conversations.

SOURCES

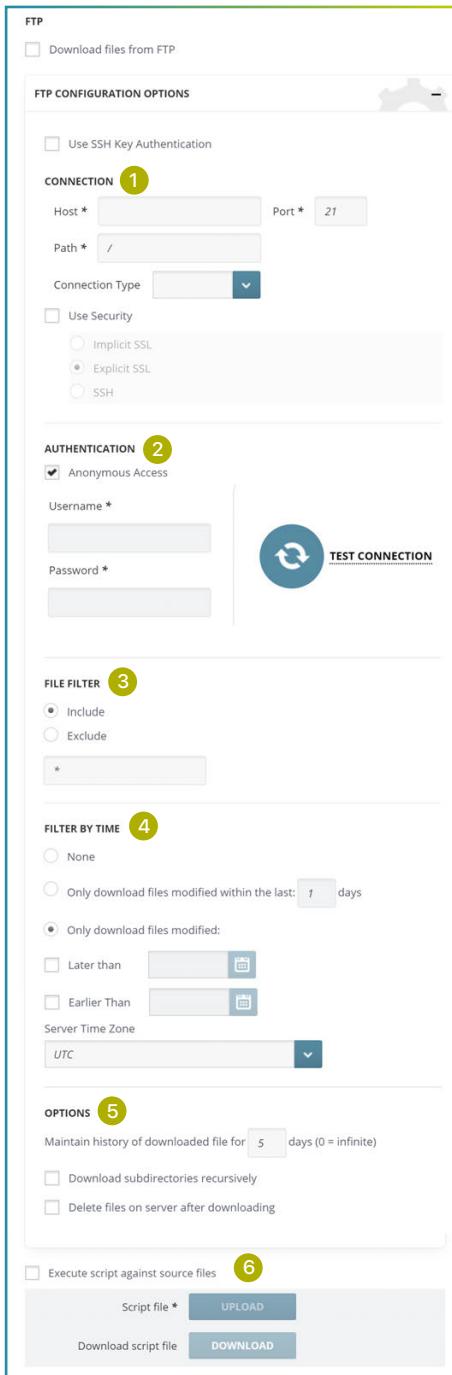


Text Delimited

FTP CONFIGURATIONS

Merge1 retrieves data from the source **FTP** and stores it in the Import Folder for processing. Corrupt files are moved to the **Quarantine Folder**.

If you want to get data from the source through FTP, tick **Download files from FTP**. FTP Configuration options will automatically open.



The screenshot shows the 'FTP CONFIGURATION OPTIONS' page. It includes sections for Connection (Host: *, Port: 21, Connection Type dropdown), Authentication (Anonymous Access checked, Username and Password fields, TEST CONNECTION button), File Filter (Include selected, wildcard *), Filter by Time (None selected, Only download files modified within the last 1 day, Later than and Earlier Than date pickers, Server Time Zone set to UTC), Options (Maintain history of downloaded file for 5 days, Download subdirectories recursively, Delete files on server after downloading, Execute script against source files checked, Script file input field, UPLOAD and DOWNLOAD buttons), and a bottom section for Download script file and its corresponding UPLOAD and DOWNLOAD buttons.

1. Connection. Enter the hostname of the remote FTP server and the folder path in the Host and Path textboxes, respectively. The default port is 21. Choose FTP connection type from the Connection type dropdown list. FTP can run in either passive or active mode. Information about the connection type should be provided by the FTP host. If you wish to use FTP over SSL, select **Use SSL** check box and choose connection method: implicit or explicit.

2. Authentication. To authenticate an FTP connection, enter the appropriate information in the Username and Password textboxes, respectively. To enable anonymous FTP connections, select the Anonymous Access checkbox, which is the default setting.

3. File Filter. This filter is used to 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. This filter is used for separating 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 modified within the mentioned days will be downloaded.
- Only download files modified earlier than/later than. When this option is 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 of time.
- 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. 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.

SOURCES



Text Delimited

- Download subdirectories recursively. If checked, files from the subdirectories of the mentioned path will be downloaded too.
- Delete files on the server after downloading. If checked, the files downloaded will be deleted from the server.

6. Execute script against source files allows the user to utilize alternative methods of data download or acquisition methods other than FTP. For example, batch script files that download information via an FTP alternative and move it into the appropriate processing folder.

PGP CONFIGURATIONS

The screenshot shows the 'PGP DECRYPTION OPTIONS' section of a configuration interface. It includes fields for 'Username *', 'Password *', and 'Email *'. A large blue button labeled 'GENERATE KEY' with a circular arrow icon is positioned next to these fields. Below this, there is a text area labeled 'Generated Public Key *' and a 'EXPORT PUBLIC KEY' button. At the bottom, there are two buttons: 'EXPORT PRIVATE KEY' and 'IMPORT PRIVATE KEY'.

1. Click **Use PGP Decryption** and PGP Decryption Options open.
2. Specify a Username, Password, and Email, then click **Generate Key**. Once the key is generated you will see a green tick icon. **
3. Log into your source control panel and enable PGP encryption by adding Merge1 Keys.
4. In your source control panel click **Add** and the Add Public Key window will appear. From the Key Type drop-down menu, select Encryption and paste the full contents of the public key (including the block header and footer) under the Public Keys tab at the control panel in your terminal.
5. Click the Decryption button. (The key appears in the Public Keys section). To save the PGP encryption key to your account click **Submit**.

* Please note that this password is required for configuring multiple connectors with the same PGP Key.

* Use the Export Public / Private Key buttons to save the keys to a secure location on your device. This will enable you to restore the keys if they are lost or when moving the database to a new machine.

SOURCES



Text Delimited

FOLDER CONFIGURATION (REQUIRED*)

After successfully setting up the SFTP and PGP Configurations, you will have to change the folder configurations. In Merge1 you will have to specify the **Import Folder**, where you would like to store the data after retrieving it from the source, as well as Quarantine Folder where all the failed messages will be archived. If you have sub-folders under your Import Folder, you can enable **Traverse Subdirectories** to maintain the sub-folder structure of imported data and include the data in your Text Delimited Merge1.

FOLDERS
Import folder*
<input type="text"/>
<input type="checkbox"/> Traverse subdirectories
Quarantine folder*
<input type="text"/>
AFTER SUCCESSFULL IMPORTING
<input checked="" type="radio"/> Move original files into a subfolder of the Import folder.
<input type="radio"/> Delete original files permanently.

Under **After Successfully Importing** settings you can provide Merge1 what to do with the original files. If **Move original files into a subfolder** is selected, the files will be moved into a folder _Import inside the Import folder. If **Delete original files permanently** is selected, the files after being processed will be deleted. Please note, that if deleted it won't be possible to recover them.

Please note:

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.

* Merge1 Folder Option 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.

SOURCES



Text Delimited

TEXT BASED CONNECTOR OPTIONS

Upload an XML template and select the relevant time zone. Merge1 will attempt to retrieve the correct time zone from the source automatically.

TEXT BASED CONNECTOR OPTIONS

Choose XML Template File *

Source Time Zone

The XML file should contain the information about the file itself. It should specify if the file contains headers, the number of columns, delimiter type and the text qualifier. Next part of the XML file should assign column names, identify data types, and indicate if the columns are optional. Lastly, it should map the columns to the expected data fields: "From", "To", "Subject", "Date", and "Body". You can see an example of XML template on the next page.

If you want to manually set up the Source Time Zone select the relevant one from the dropdown menu.

Please note:

That the Source Timezone setting will attempt to retrieve the timezone from the data itself automatically.

MISCELLANEOUS SETTINGS

If you want to import specific files or filetypes, note them in the Files to Import form. You can separate each file or filetype with a vertical bar " | ". Simply write the name of the file (ex. blackberry.txt) or use wildcards to import the whole filetype (ex. *.txt | *.xml). The default setting is *.txt as Text Delimited parses only text 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.

MISC SETTINGS

Files to import: e.g.: *.txt|*.xml (separated by vertical bars)*

Subject prefix

SOURCES



Text Delimited

XML TEMPLATE SAMPLE CONFIGURATION GUIDELINE

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

```
<version>TD_2.0</version>
<options>
    <containsHeader>No</containsHeader>
    <maxCols>5</maxCols>
    <delimiter>","</delimiter>
    <text_qualifier>"</text_qualifier>
</options>
```

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

```
<columns>
    <column>
        <order>1</order>
        <name>COLUMN_FROM</name>
        <datatype>String</datatype>
    </column>
    <column>
        <order>2</order>
        <name>COLUMN_TO</name>
        <datatype>String</datatype>
    </column>
    <column>
        <order>3</order>
        <name>COLUMN SUBJECT</name>
        <datatype>String</datatype>
    </column>
    <column>
        <order>4</order>
        <name>COLUMN_MESSAGE_BODY</name>
        <datatype>String</datatype>
    </column>
    <column>
        <order>5</order>
        <name>COLUMN_SENT_RECEIVED_DATE</name>
        <datatype>DateTime</datatype>
        <datatype_options>
            <format>XX/DD/YYYY HH:MM</format>
        </datatype_options>
    </column>
</columns>
```

SOURCES



Text Delimited

3. The last part of the XML file maps the columns to the expected data fields:
"From", "To", "Subject", "Date", "Body"

```
<mappings>
  <mapping can_be_empty = "Yes">
    <property>From</property>
    <items>
      <item>COLUMN_FROM</item>
    </items>
  </mapping>
  <mapping can_be_empty = "Yes">
    <property>To</property>
    <items>
      <item>COLUMN_TO</item>
    </items>
  </mapping>
  <mapping can_be_empty = "Yes">
    <property>Subject</property>
    <items>
      <item>COLUMN SUBJECT</item>
    </items>
  </mapping>
  <mapping can_be_empty = "Yes">
    <property>Body</property>
    <items>
      <item>COLUMN_MESSAGE_BODY</item>
    </items>
  </mapping>
  <mapping can_be_empty = "Yes">
    <property>Date</property>
    <items>
      <item>COLUMN_SENT_RECEIVED_DATE</item>
    </items>
  </mapping>
  <mapping can_be_empty = "Yes">
    <property>X-KVS-MessageType</property>
    <items>
      <string>"Twitter"</string>
    </items>
  </mapping>
</mappings>
```

SOURCES



Text Delimited

Example of source .txt file:

```
chatreport-2011-05-05 - Notepad
File Edit Format View Help
HOST MEMBER;HOST USER;GUEST MEMBER;GUEST USER;START TIME;END TIME;TEXT_SOURCE;TEXT
M.GLOBANET;sales@globanet.com;CONTRA;dev@globanet.com;2011-05-05 15:54:07;2011-05-05
15:54:14;Host;Submitted Ticket
M.GLOBANET;products@globanet.com;CONTRA;support@globanet.com;2011-05-05 12:49:13;2011-05-05
12:49:38;Guest;Submitted case closed
M.GLOBANET;sales@globanet.com;CONTRA;mmc@globanet.com;2011-05-05 10:20:23;2011-05-05
10:20:40;Guest;Submitted bug report
M.GLOBANET;dev@globanet.com;CONTRA;products@globanet.com;2011-05-05 14:43:49;2011-05-05 14:43:54;Guest;Done
for now.
M.GLOBANET;mmc@globanet.com;CONTRA;dev@globanet.com;2011-05-05 12:37:11;2011-05-05 12:37:34;Host;Submitted
Done.
```

Parsed output:

Thu 5/5/2011 8:54 PM
S sales@globanet.com
SessionID - Submitted Ticket
To dev@globanet.com

HOST MEMBER: M.GLOBANET
HOST USER: sales@globanet.com
GUEST MEMBER: CONTRA
GUEST USER: dev@globanet.com
START TIME: May 05, 2011 15:54:07
END TIME: May 05, 2011 15:54:14
TEXT SOURCE: Host
TEXT: Submitted Ticket

NEXT STEPS

After setting up the connector follow the appropriate links below to continue with the configuration of the Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users is not applicable to this connector.
- Filters
- Targets
- Importer Settings

MOBILE GUARD



MobileGuard

ABOUT MOBILE GUARD

MobileGuard is a mobile communication monitoring and retention owned by Smarsh. Merge1 processes the Mobile Guard files from CSV format. The data should be exported from Mobile Guard in "Simple CSV with MMS" format. A Zip file can be provided as well.

Merge1 maps the columns of the CSV file with the fields in the output message. Please note, that message participants by default are imported in Mobile Guard Connect User ID format unless their email address is given in the CSV file. If you want to map them to the users' email addresses, each email address and corresponding Mobile Guard User ID should be added in User Mappings section of the connector set up (please check Next Steps for more information).

ACTIVITIES CAPTURED

- Participants: To, From, CC, and BCC
- Sent Time
- GIFs
- Attachments
- Emojis*

* Emoticons not found within the EmojiOne library are not supported. For emoticons not found in the EmojiOne library: all content types besides Slack will display the Unicode version of the emoticon (e.g., "U+1F642"); for Slack, the custom emoticon will display as the Slack "short name" for the emoticon (e.g., ":slightly_smiling_face:"). Custom mobile emoticon keyboards are not supported. Emoticons are not supported within attachments, or the print view. Emoticons are not searchable within the archive.

SOURCES



MobileGuard

FTP CONFIGURATIONS

Merge1 retrieves data from Mobile Guard **FTP** and stores it in the Import Folder for processing. Corrupt files are moved to the **Quarantine Folder**.

If you want to get data from Mobile Guard through FTP, tick **Download files from FTP**. FTP Configuration options will automatically open.

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 21. Choose FTP connection type from the Connection type dropdown list. FTP can run in either passive or active mode. Information about the connection type should be provided by the FTP host.

If you wish to use FTP over SSL, select **Use SSL** checkbox and choose connection method: implicit or explicit.

2. Authentication. To authenticate an FTP connection, enter the appropriate information in the Username and Password textboxes, respectively. To enable anonymous FTP connections, select the Anonymous Access checkbox, which is the default setting.

3. File Filter. This filter is used to 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. This filter is used for separating 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 modified within the mentioned days will be downloaded.
- Only download files modified earlier than/later than. When this option is 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 of time
- Server Time Zone specifies the time zone in which the FTP sever is to correctly determine the timestamp of downloadable files.

5. Options.

- Maintain history of downloaded file for X days. 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.

SOURCES



MobileGuard

- Download subdirectories recursively. If checked, files from the subdirectories of the mentioned path will be downloaded too.
- Delete files on server after downloading. If checked, the files downloaded will be deleted from the server.

6. Execute script against source files allows the user to utilize alternative methods of data download or acquisition methods other than FTP. For example, batch script files that download information via an FTP alternative and move it into the appropriate processing folder.

PGP CONFIGURATIONS

PGP DECRYPTION OPTIONS

Username *

Password *

Email *

Generated Public Key *

EXPORT PUBLIC KEY

Export/Import Private Key

EXPORT PRIVATE KEY IMPORT PRIVATE KEY

A screenshot of the PGP Decryption Options interface. It shows fields for Username, Password, and Email, and a Generated Public Key area. There are buttons for EXPORT PUBLIC KEY and IMPORT PRIVATE KEY. A large blue GENERATE KEY button with a circular arrow icon is prominently displayed.

1. Click **Use PGP Decryption** and PGP Decryption Options open.
2. Specify a Username, Password, and Email, then click **Generate Key**. Once the key is generated you will see a green tick icon. **
3. Log into your Mobile Guard control panel and enable PGP encryption by adding Merge1 Keys.
4. In your Mobile Guard control panel click **Add** and the Add Public Key window will appear. From the Key Type drop-down menu, select Encryption and paste the full contents of the public key (including the block header and footer) under the Public Keys tab at the control panel in your Bloomberg terminal.
5. Click the Decryption button. (The key appears in the Public Keys section). To save the PGP encryption key to your account click **Submit**.

* Please note that this password is required for configuring multiple connectors with the same PGP Key.

* Use the Export Public / Private Key buttons to save the keys to a secure location on your device. This will enable you to restore the keys if they are lost or when moving the database to a new machine.

SOURCES



MobileGuard

FOLDER CONFIGURATION (REQUIRED*)

After successfully setting up the FTP and PGP Configurations, you will have to change the folder configurations. In Merge1 you will have to specify the **Import Folder**, where you would like to store the data after retrieving it from MobileGuard, 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 MobileGuard Merge1.

FOLDERS
Import folder*
<input type="text"/>
<input type="checkbox"/> Traverse subdirectories
Quarantine folder*
<input type="text"/>
AFTER SUCCESSFULL IMPORTING
<input checked="" type="radio"/> Move original files into a subfolder of the Import folder.
<input type="radio"/> Delete original files permanently.

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

Please note:

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.

* Merge1 Folder Option 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.

SOURCES



MobileGuard

MOBILEGUARD CONNECTOR OPTIONS

If you want to manually set up the Source Time Zone select the relevant one from the dropdown menu.

MOBILE GUARD CONNECTOR OPTIONS

Source Time Zone

UTC



Define User Mappings List

Please define User Mappings list on next step to tell us how you want Merge1 to map users.

Once you have selected the Connector Type, you can also provide the **Source Time Zone** information. Merge1 assumes that the messages in the source file are of the set timezone and based on that data the dates in the messages are processed to UTC timezone. By default, Merge1 sets the **Source Time Zone** as UTC.

Please note:

The Source Timezone setting will attempt to retrieve the timezone from the data itself automatically.

MISCELLANEOUS SETTINGS

If you want to import specific files or filetypes, note them in the Files to Import form. You can separate each file or filetype with a vertical bar " | ". Simply write the name of the file (ex. blackberry.txt) or use wildcards to import the whole filetype (ex. *.txt | *.xml). The default setting is *.csv because Blackberry files are parsed in CSV format.

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.

MISC SETTINGS

Files to import: e.g.: *.txt|*.xml (separated by vertical bars)*

*.CSV

Subject prefix

SOURCES



MobileGuard

Example Output Message:

Thu 7/13/2017 7:44 PM
yuriy.ross@example.com <David.davidson@example.com>
Testing qa 4-way SMS with attachment _Please confirm delivery

To t.adams@example.com; john.doe@example.com; adam.smith1@example.com

 ms-nHKlq1.gif
166 KB

7/13/2017 3:43:55 PM
Testing qa 4-way SMS with attachment
Please confirm delivery

NEXT STEPS

After setting up the connector follow the appropriate links below to continue with the configuration of the Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users - to map user IDs from Mobile Guard to the email addresses of the users, use Add User Mapping Manually option. System ID and Corporate Email Address should be input manually to display the emails in the output message. The list of added mapped users can then be edited Edit Existing List section of User Mappings.
- Filters (Mobile Guard works with all filters except **XML Filter**)
- Targets
- Importer Settings

UBS



UBS

HOW TO SET UP UBS CONNECTOR

After selecting the UBS icon in the Configuration Wizard and clicking **Next** button you will be redirected to the next screen of the Configuration.

As mentioned earlier the Configuration Wizard Screen consists of 5 tabs. You will be prompted to start with Source Configuration.

The UBS Connector Source Configuration Screen has the following Settings options (click on the name to open the relevant configuration information):

- FTP configurations
- PGP configurations
- Folders (Required)
- UBS Options
- Misc Settings

CONFIGURATION WIZARD

SOURCE MONITORED USERS FILTERS TARGETS SETTINGS

Please provide your UBS configuration data so that Merge1 can access your UBS data.

FTP

Download files from FTP

FTP CONFIGURATION OPTIONS +

Execute script against source files

Script file *

PGP

Use PGP Decryption

PGP DECRYPTION OPTIONS +

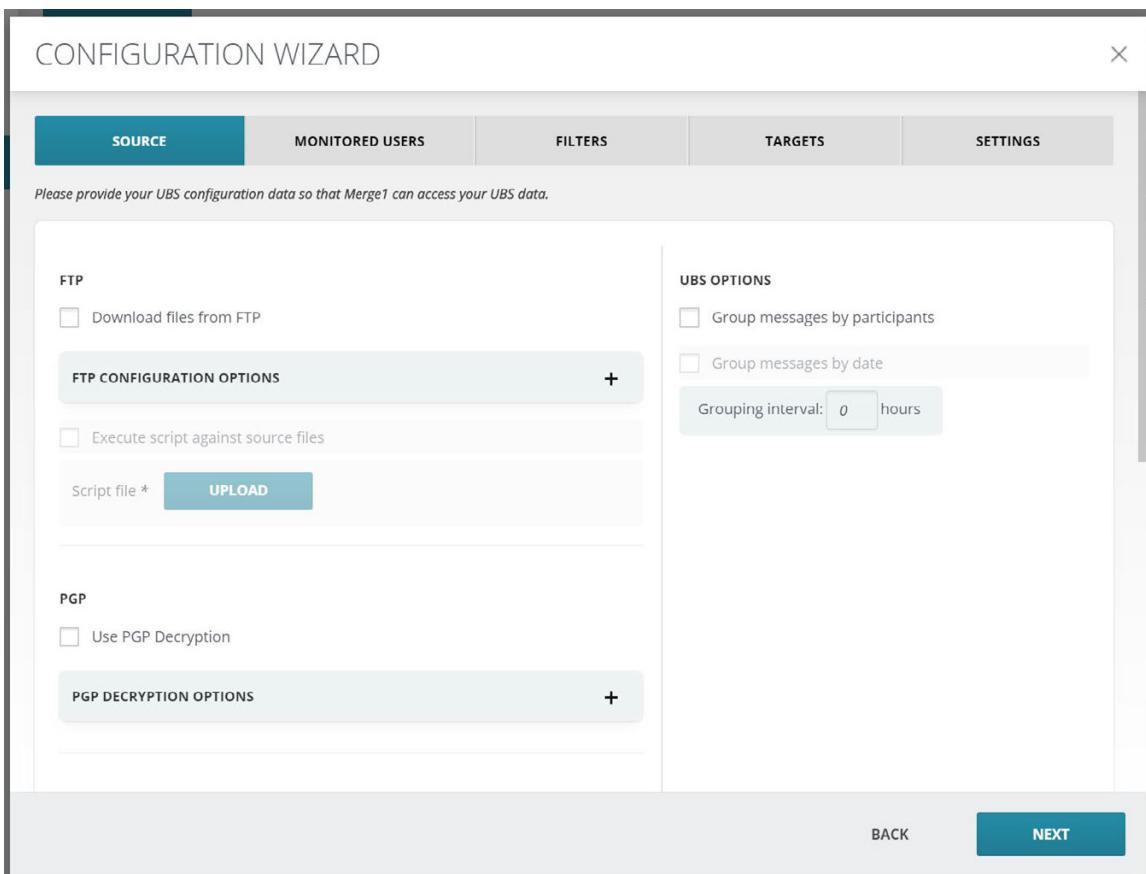
UBS OPTIONS

Group messages by participants

Group messages by date

Grouping interval: 0 hours

BACK



SOURCES



FTP CONFIGURATIONS

Merge1 retrieves data from UBS **FTP** and stores it in the Import Folder for processing. Corrupt files are moved to the **Quarantine Folder**.

If you want to get data from UBS through FTP, tick **Download files from FTP**. FTP Configuration options will automatically open.

A screenshot of the 'FTP Configuration Options' dialog box. The interface is divided into several sections: 1. Connection: Host (text box), Port (dropdown menu set to 21). 2. Authentication: Username (text box), Password (text box), TEST CONNECTION button. 3. File Filter: Include (radio button selected), Exclude (radio button), wildcard filter (*). 4. Filter by Time: None (radio button), Only download files modified within the last (dropdown menu set to 1 days), Only download files modified (radio button selected), Later than (button), Earlier Than (button), Server Time Zone (dropdown menu set to UTC). 5. Options: Maintain history of downloaded file for (dropdown menu set to 5 days), Download subdirectories recursively, Delete files on server after downloading. 6. Execute script against source files: Script file (text box), UPLOAD and DOWNLOAD buttons.

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 21. Choose FTP connection type from the Connection type dropdown list. FTP can run in either passive or active mode. Information about the connection type should be provided by the FTP host.

If you wish to use FTP over SSL, select **Use SSL** checkbox and choose connection method: implicit or explicit.

2. Authentication. To authenticate an FTP connection, enter the appropriate information in the Username and Password textboxes, respectively. To enable anonymous FTP connections, select the Anonymous Access checkbox, which is the default setting.

3. File Filter. This filter is used to 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. This filter is used for separating 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 modified within the mentioned days will be downloaded.
- Only download files modified earlier than/later than. When this option is 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 of time.
- Server Time Zone specifies the time zone in which the FTP sever is to correctly determine the time stamp of downloadable files.

5. Options.

- Maintain history of downloaded file for X days. 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.

SOURCES



- Download subdirectories recursively. If checked, files from the subdirectories of the mentioned path will be downloaded too.
- Delete files on server after downloading. If checked, the files downloaded will be deleted from the server.

6. Execute script against source files allows the user to utilize alternative methods of data download or acquisition methods other than FTP. For example, batch script files that download information via an FTP alternative and move it into the appropriate processing folder.

PGP CONFIGURATIONS

PGP DECRYPTION OPTIONS

Username *

Password *

Email *

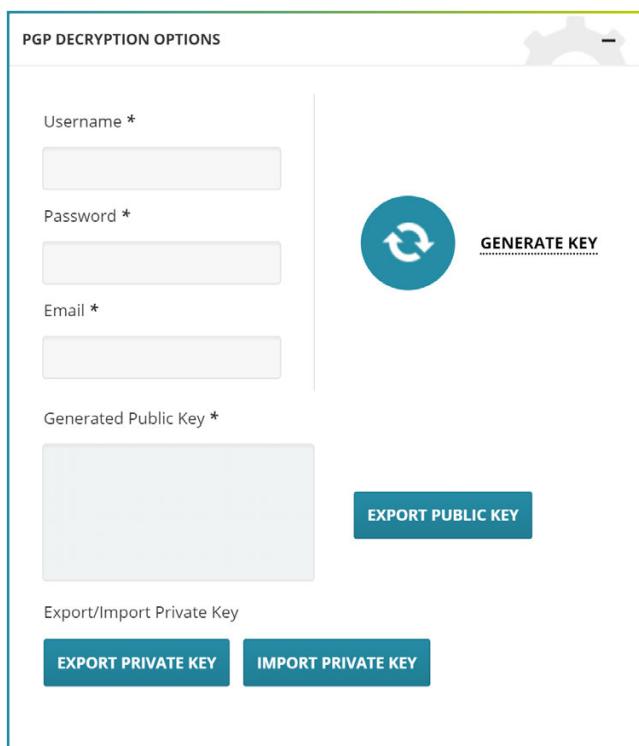
Generated Public Key *

EXPORT PUBLIC KEY

GENERATE KEY

Export/Import Private Key

EXPORT PRIVATE KEY IMPORT PRIVATE KEY



1. Click **Use PGP Decryption** and PGP Decryption Options open.
2. Specify a Username, Password, and Email, then click **Generate Key**. Once the key is generated you will see a green tick icon. **
3. Log into your UBS control panel and enable PGP encryption by adding Merge1 Keys.
4. In your UBS control panel click **Add** and the Add Public Key window will appear. From the Key Type drop-down menu, select Encryption and paste the full contents of the public key (including the block header and footer) under the Public Keys tab at the control panel in your terminal.
5. Click the Decryption button. (The key appears in the Public Keys section). To save the PGP encryption key to your account click **Submit**.

Please note:

When FTP is disabled, Merge1 attempts to retrieve the data directly from the Import Folder. This is useful when data is already in-hand or if the user wishes to acquire the data manually.

* Please note that this password is required for configuring multiple connectors with the same PGP Key.

* Use the Export Public / Private Key buttons to save the keys to a secure location on your device. This will enable you to restore the keys if they are lost or when moving the database to a new machine.

SOURCES



UBS

FOLDER CONFIGURATION (REQUIRED*)

After successfully setting up the FTP and PGP Configurations, you will have to change the folder configurations. In Merge1 you will have to specify the **Import Folder**, where you would like to store the data after retrieving it from UBS, 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 MobileGuard Merge1.

FOLDERS

Import folder*

Traverse subdirectories

Quarantine folder*

AFTER SUCCESSFULL IMPORTING

Move original files into a subfolder of the Import folder.

Delete original files permanently.

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

Please note:

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.

* Merge1 Folder Option 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.

SOURCES



UBS

UBS OPTIONS

Merge1 enables you to validate the UBS attachments. You can either group all messages based on participants or you can group messages by date.

UBS OPTIONS

Group messages by participants

Group messages by date

Grouping interval: hours

You can also set grouping interval. The time is calculated in hours.

MISCELLANEOUS SETTINGS

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

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.

MISC SETTINGS

Files to import: e.g.: *.txt | *.xml (separated by vertical bars)*

*.xml

Subject prefix

SOURCES



UBS

Example Output Message:

Mon 6/13/2011 11:59 PM

DJ Doe, John(Example Company) <John.s.Doe@example.com>
UBS Chat Conversation from Doe, John(Example Company)

To Michael, Smith(Example)

(6/13/2011 6:59:24 PM UTC) Doe, John(Example Company) says: see the IPXL
(6/13/2011 6:59:44 PM UTC) Doe, John(Example Company) says: complete
(6/13/2011 6:59:49 PM UTC) Michael, Smith(Example) says: k

Participant: Doe, John(Example Company) <John.s.Doe@example.com>
Participant: Michael, Smith(Example) (Smithro) <Michael.Smith@example.com>

NEXT STEPS

After setting up the connector follow the appropriate links below to continue with the configuration of Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users is not applicable to this connector.
- Filters
- Targets
- Importer Settings

XSLT/XML



XSLM/XML

ABOUT XSLT/XML CONNECTOR

Merge1 XML/XSLT connector allows our customers to rapidly transform XML file using XSLT to a predefined format. Once XML is transformed Merge1 can process the XML by generating the required mapping "From" "To" "Subject" "Date" "body" fields to appropriate elements of the XML file.

The mapping varies from source to source, it has to be written separately. Contact our support at support@globanet.com for more details on the mapping corresponding to the source you're going to use it for.

ACTIVITIES CAPTURED

- Participants: From, To, CC, and BCC
- Start Time
- End Time
- Body Message
- Device Used

SOURCES



XSLM/XML

FTP CONFIGURATIONS

Merge1 retrieves data from the source **FTP** and stores it in the Import Folder for processing. Corrupt files are moved to the **Quarantine Folder**.

If you want to get data from the source through FTP, tick **Download files from FTP**. FTP Configuration options will automatically open.

The screenshot shows the 'FTP Configuration Options' dialog box. It includes fields for Host, Port, Connection Type, Username, Password, File Filter, Time Filter, and various Options like maintaining history, recursive download, and executing scripts.

- 1 CONNECTION: Host, Port, Connection Type dropdown.
- 2 AUTHENTICATION: Username, Password, TEST CONNECTION button, Anonymous Access checkbox (checked).
- 3 FILE FILTER: Include/Exclude radio buttons, wildcard filter field (*).
- 4 FILTER BY TIME: None, Only download files modified within the last 1 day, Only download files modified, Later than/Earlier Than date pickers, Server Time Zone dropdown (UTC).
- 5 OPTIONS: Maintain history of downloaded file for 5 days, Download subdirectories recursively, Delete files on server after downloading.
- 6 EXECUTE SCRIPT: Execute script against source files checkbox, Script file input, UPLOAD and DOWNLOAD buttons.

1. Connection. Enter the hostname of the remote FTP server and the folder path in the Host and Path textboxes, respectively. The default port is 21. Choose FTP connection type from the Connection type dropdown list. FTP can run in either passive or active mode. Information about the connection type should be provided by the FTP host. If you wish to use FTP over SSL, select **Use SSL** checkbox and choose connection method: implicit or explicit.

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. This filter is used to 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. This filter is used for separating 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 modified within the mentioned days will be downloaded.
- Only download files modified earlier than/later than. When this option is only the data modified earlier than or later than the mentioned date will be downloaded. Both options can be selected simultaneously to choose a time period.
- Server Time Zone specifies the timezone in which the FTP sever is to correctly determine the timestamp of downloadable files.

5. Options.

- Maintain history of downloaded file for X days. 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.

SOURCES



XSLM/XML

- 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.

6. Execute script against source files allows the user to utilize alternative methods of data download or acquisition methods other than FTP. For example, batch script files that download information via an FTP alternative and move it into the appropriate processing folder.

PGP CONFIGURATIONS

PGP DECRYPTION OPTIONS

Username *

Password *

Email *

Generated Public Key *

EXPORT PUBLIC KEY

GENERATE KEY

Export/Import Private Key

EXPORT PRIVATE KEY IMPORT PRIVATE KEY

1. Click **Use PGP Decryption** and PGP Decryption Options open.
2. Specify a Username, Password, and Email, then click **Generate Key**. Once the key is generated you will see a green tick icon. **
3. Log into your source control panel and enable PGP encryption by adding Merge1 Keys.
4. In your source control panel click **Add** and the Add Public Key window will appear. From the Key Type drop-down menu, select Encryption and paste the full contents of the public key (including the block header and footer) under the Public Keys tab at the control panel in your terminal.
5. Click the Decryption button. (The key appears in the Public Keys section). To save the PGP encryption key to your account click **Submit**.

Please note:

That when FTP is disabled, Merge1 attempts to retrieve the data directly from the Import Folder. This is useful when data is already in-hand or if the user wishes to acquire the data manually.

* Please note that this password is required for configuring multiple connectors with the same PGP Key.

* Use the Export Public / Private Key buttons to save the keys to a secure location on your device. This will enable you to restore the keys if they are lost or when moving the database to a new machine.

SOURCES



XSLM/XML

FOLDER CONFIGURATION (REQUIRED*)

After successfully setting up the FTP and PGP Configurations, you will have to change the folder configurations. In Merge1 you will have to specify the **Import Folder**, where you would like to store the data after retrieving it from MobileGuard, 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 MobileGuard Merge1.

FOLDERS
Import folder*
<input type="text"/>
<input type="checkbox"/> Traverse subdirectories
Quarantine folder*
<input type="text"/>
AFTER SUCCESSFULL IMPORTING
<input checked="" type="radio"/> Move original files into a subfolder of the Import folder.
<input type="radio"/> Delete original files permanently.

Under **After Successfully Importing** settings you can provide Merge1 what to do with the original files. You can either Move the original files to a subfolder in the Importer Folder or you can Delete the files. Please note that once Deleted you can not recover them.

Please note:

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.

* Merge1 Folder Option 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.

SOURCES



XSLM/XML

XSLT/XML CONNECTOR OPTIONS

Upload the XSLT template from Merge1 6.0 folder. You can find the templates in the Templates folder of the Merge1 Installation file.

XSLT CONNECTOR OPTIONS

Choose XSLT file: *

UPLOAD

The XSLT 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 XSLT 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: "From", "To", "Subject", "Date", and "Body". You can see an example of XSLT template on the next page.

MISCELLANEOUS SETTINGS

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

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.

MISC SETTINGS

Files to import: e.g.: *.txt | *.xml (separated by vertical bars)*

**.xml*

Subject prefix

SOURCES



XSLM/XML

Example Output Message:

Wed 10/5/2016 4:34 PM
raj.nagi@ozcap.com
YJ 2016-10-05
To raj.nagi@ozcap.com; syed.shah@ozcap.com

[2016-10-05 16:34:17]: [rnagi@yjenergy.com](#) [raj.nagi@ozcap.com](#) joined conversation.
[2016-10-05 16:34:17]: [sshah9@yjenergy.com](#) [syed.shah@ozcap.com](#) joined conversation.

[2016-10-05 16:34:17]: [rnagi@yjenergy.com](#) : whats up Syed
[2016-10-05 16:34:26]: [sshah9@yjenergy.com](#) : test message
[2016-10-05 16:34:35]: [sshah9@yjenergy.com](#) : test 12:34 with RAJ
[2016-10-05 16:34:50]: [rnagi@yjenergy.com](#) : received test
[2016-10-05 16:34:53]: [sshah9@yjenergy.com](#) : why you are not replying .:

[2016-10-05 16:34:53]: [rnagi@yjenergy.com](#) left conversation.
[2016-10-05 16:34:53]: [sshah9@yjenergy.com](#) left conversation.

NEXT STEPS

After setting up the connector follow the appropriate links below to continue with the configuration of the Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users is not applicable to this connector.
- Filters
- Targets
- Importer Settings



XIP

HOW TO SETUP THE XIP CONNECTOR

After selecting the XIP icon in the Configuration Wizard and clicking **Next** you will be redirected to the next screen of the Configuration. As mentioned earlier the Configuration Wizard Screen consists of 5 tabs. You will be prompted to start with Source Configuration.

The XIP Connector Source Configuration Screen has the following Setting options (click on the name to open the relevant configuration information):

- FTP configurations
- PGP configurations
- Folders (Required)
- XIP Connector Options
- Misc Settings

CONFIGURATION WIZARD

X

SOURCE	MONITORED USERS	FILTERS	TARGETS	SETTINGS
--------	-----------------	---------	---------	----------

Please provide your XIP configuration data so that Merge1 can access your XIP data.

FTP

Download files from FTP

FTP CONFIGURATION OPTIONS +

Execute script against source files

Script file * UPLOAD

PGP

Use PGP Decryption

PGP DECRYPTION OPTIONS +

XIP CONNECTOR OPTIONS

Source Time Zone Local Timezone

BACK
NEXT

SOURCES



XIP

FTP CONFIGURATIONS

Merge1 retrieves data from the source **FTP** and stores it in the Import Folder for processing. Corrupt files are moved to the **Quarantine Folder**.

If you want to get data from the source through FTP, tick **Download files from FTP**. FTP Configuration options will automatically open.

1. Connection. Enter the hostname of the remote FTP server and the folder path in the Host and Path textboxes, respectively. The default port is 21. Choose FTP connection type from the Connection type dropdown list. FTP can run in either passive or active mode. Information about the connection type should be provided by the FTP host. If you wish to use FTP over SSL, select **Use SSL** checkbox and choose connection method: implicit or explicit.

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

3. File Filter. This filter is used to 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. This filter is used for separating 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 modified within the mentioned days will be downloaded.
- Only download files modified earlier than/later than. When this option is only the data modified earlier than or later than the mentioned date will be downloaded. Both options can be selected simultaneously to choose a time period.
- Server Time Zone specifies the time zone in which the FTP sever is to correctly determine the time stamp of downloadable files.

5. Options.

- Maintain history of downloaded file for X days. 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.

SOURCES



XIP

- Download subdirectories recursively. If checked, files from the subdirectories of the mentioned path will be downloaded too.
- Delete files on server after downloading. If checked, the files downloaded will be deleted from the server.

6. Execute script against source files allows the user to utilize alternative methods of data download or acquisition methods other than FTP. For example, batch script files that download information via an FTP alternative and move it into the appropriate processing folder.

PGP CONFIGURATIONS

PGP DECRYPTION OPTIONS

Username *

Password *

Email *

Generated Public Key *

EXPORT PUBLIC KEY

Export/Import Private Key

EXPORT PRIVATE KEY IMPORT PRIVATE KEY

GENERATE KEY

1. Click **Use PGP Decryption** and PGP Decryption Options open.
2. Specify a Username, Password, and Email, then click **Generate Key**. Once the key is generated you will see a green tick icon. **
3. Log into your source control panel and enable PGP encryption by adding Merge1 Keys.
4. In your source control panel click **Add** and the Add Public Key window will appear. From the Key Type drop-down menu, select Encryption and paste the full contents of the public key (including the block header and footer) under the Public Keys tab at the control panel in your terminal.
5. Click the Decryption button. (The key appears in the Public Keys section). To save the PGP encryption key to your account click **Submit**.

Please note:

That when FTP is disabled, Merge1 attempts to retrieve the data directly from the Import Folder. This is useful when data is already in-hand or if the user wishes to acquire the data manually.

* Please note that this password is required for configuring multiple connectors with the same PGP Key.

* Use the Export Public / Private Key buttons to save the keys to a secure location on your device. This will enable you to restore the keys if they are lost or when moving the database to a new machine.

SOURCES



XIP

FOLDER CONFIGURATION (REQUIRED*)

After successfully setting up the FTP and PGP Configurations, you will have to change the folder configurations. In Merge1 you will have to specify the **Import Folder**, where you would like to store the data after retrieving it from MobileGuard, 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 MobileGuard Merge1.

FOLDERS

Import folder*

Traverse subdirectories

Quarantine folder*

AFTER SUCCESSFULL IMPORTING

- Move original files into a subfolder of the Import folder.
- Delete original files permanently.

Under **After Successfully Importing** settings you can provide Merge1 what to do with the original files. You can either Move the original files to a subfolder in the Importer Folder or you can Delete the files. Please note that once Deleted you can not recover them.

Please note:

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.

* Merge1 Folder Option 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.

SOURCES



XIP

XIP CONNECTOR OPTIONS

If you want to manually set up the Source Time Zone select the relevant one from the dropdown menu.

XIP CONNECTOR OPTIONS

Source Time Zone



Once you have selected the Connector Type, you can also provide the **Source Time Zone** information. Merge1 assumes that the messages in the source file are of the set timezone and based on that data the dates in the messages are processed to UTC timezone. By default, Merge1 sets the **Source Time Zone** as the Local Timezone.

MISCELLANEOUS SETTINGS

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

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.

MISC SETTINGS

Files to import: e.g.: *.txt|*.xml (separated by vertical bars)*

Subject prefix

SOURCES



Example Output Message:

Thu 6/24/2010 10:21 AM

Anil Ohri <AnilOhri>

nem - sag; t upto sag

To Jane Doe

Hello World!

NEXT STEPS

After setting up the connector follow the appropriate links below to continue with the configuration of the Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users is not applicable to this connector.
- Filters
- Targets
- Importer Settings

SKYPE FOR BUSINESS



Skype
for Business

ABOUT SKYPE FOR BUSINESS CONNECTOR

Skype for Business is an instant messaging client used with Skype for Business Server or with Skype for Business Online. Skype for Business is 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 contain 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

SOURCES



Skype
for Business

DB CONFIGURATION

Merge1 retrieves data from Lync / Skype for Business directly from its database(s).

Select the System Type from the dropdown menu. (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).

The screenshot shows a user interface titled "DB CONFIGURATION". It lists three database types: "Archive Database", "Persistent Chat Database", and "Compliance Database", each with a "CONFIGURE" button. Below these is a dropdown menu labeled "Source System Type" with the value "Lync2007" selected. The interface has a clean, modern design with a light gray background and white cards for each database type.

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 database name.

SOURCES



Skype
for Business

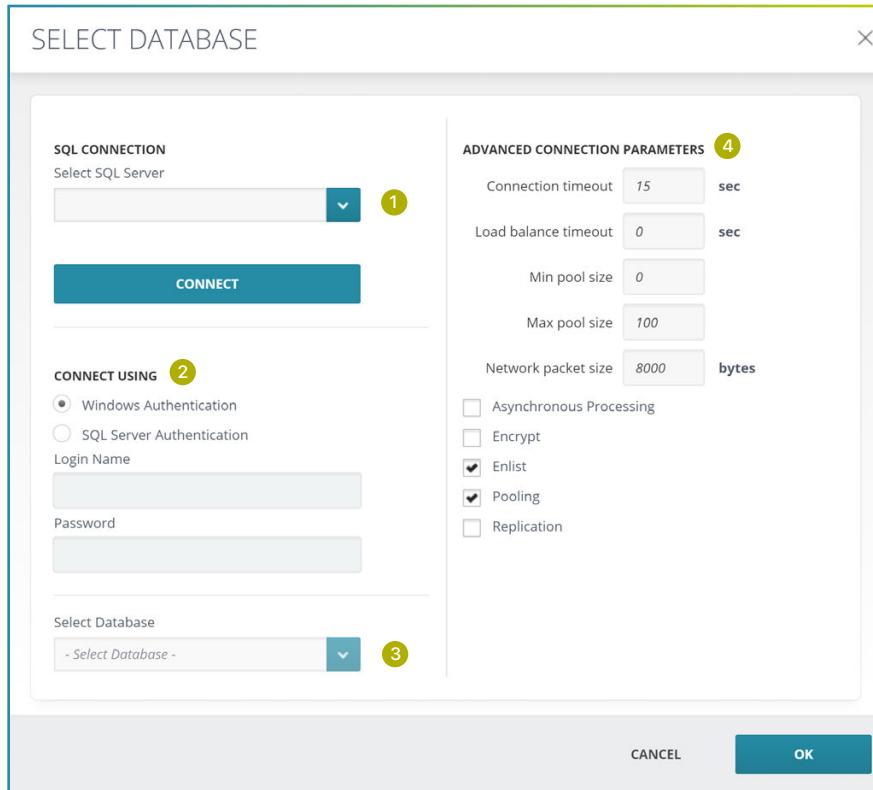
ALL THREE TYPES OF DATABASES ARE CONFIGURED AS FOLLOWS:

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's 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 menu 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 having 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.

SOURCES



Skype
for Business



OTHER OPTIONS

- The **Auto Update** feature will ensure that the connector is updated to the latest version. Each time the Importer is run, it contacts Globanet server(s) and updates the connector if a newer version is available.
- 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 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.

SOURCES



Skype
for Business

- Options **Do Not Download Data Modified Before** and **Do Not Download Data Modified After** allow to cut off data outside the set date range. If the Before date is set to 04/17/2016 and the After is set to 08/25/2018 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.
- **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 amount 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.

The screenshot shows the 'OTHER OPTIONS' configuration screen in Merge1. It includes the following settings:

- Subject Prefix:** Pfx
- Message Grouping:** Single Message per Conversation Contributor (selected)
- Download Date Filters:**
 - Do not download data modified before: [date input]
 - Do not download data modified after: [date input]
- Message Chunking:**
- IMs per Chunk:** 5000
- Archiving Delay Check:**
Delay(Hours): 24
- Use With Caution:** A note explaining the Delayed Archive feature and its purpose to mitigate a problem caused by a perceived deficiency in Skype for Business.
- Add User SMTP Address in Subject and Report:**
- Persistent Chat Identifier:** For persistent chats use prinUri as user identifier

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. Merge1 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 Merge1 will have to do. Globanet recommends choosing a minimal look back period only when necessary and to never exceed 72 hours.

SOURCES



Skype
for Business

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 connector only one time a day on a non-working hour.

Example of Single Message per Conversation:

Wed 6/25/2014 10:35 PM
msmith@gps.local
SkypeForBusiness Lync User#1 Chat 2014-06-25 @ 22:34:34.220#1 (Conversation)
To: msmith@gps.local; meyers-a@gps.local

[file:///vmsmith@gps.local/](#)
Click or tap to follow link.

msmith@gps.local [6/25/2014 10:34:34 PM]: Hi Albert.
From account: msmith
Local username: Jackie Ervin
Corp Email: msmith@gps.local ([file:///msmith@gps.local/](http://msmith@gps.local/))
msmith@gps.local [6/25/2014 10:39:05 PM]:
I got your meeting invite.
From account: msmith
Local username: Michael Smith
Corp Email: msmith@gps.local

Example of Single Message per Conversation Contributor:

Tue 8/13/2013 10:12 PM
jervin@gps.local
SkypeForBusiness Lync User#1 Chat 2013-08-13 @ 22:12:17.993#1 (ConversationContributor)
To: jervin@gps.local; msmith@gps.local

jervin@gps.local [8/13/2013 10:12:17 PM]: here is the file.
[mhopkins@gps.local](#) [8/13/2013 10:13:12 PM]:
thanks!:)

Tue 8/13/2013 10:12 PM
msmith@gps.local
SkypeForBusiness Lync User#3 Chat 2013-08-13 @ 22:12:17.993#1 (ConversationContributor)
To: jervin@gps.local; msmith@gps.local

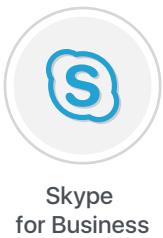
jervin@gps.local [8/13/2013 10:12:17 PM]: here is the file.
[mhopkins@gps.local](#) [8/13/2013 10:13:12 PM]:
thanks!:)

Example of Single Message per Conversation Contributor in Bloomberg Vault Format:

Tue 7/30/2013 2:57 PM
meyers-a@gps.local
SkypeForBusiness Lync User#5 Chat 2013-07-30 @ 14:56:58.467#1 (ConversationContributor)
To: jervin@gps.local; meyers-a@gps.local

```
<?xml version="1.0"?><chatTranscript><sessionId>0</sessionId><startTime>2013-07-30T14:56:58+00:00</startTime><endTime>2013-07-30T14:57:16+00:00</endTime><participants><buddyName>jervin@gps.local</buddyName><networkName>MS Lync</networkName><email>jervin@gps.local</email><displayName>jervin@gps.local</displayName></participant><s><participants><buddyName>meyers-a@gps.local</buddyName><networkName>MS Lync</networkName><email>meyers-a@gps.local</email></participants><events><sequenceNumber>0</sequenceNumber><eventType>post</eventType><eventOwner>jervin@gps.local</eventOwner><buddyName>jervin@gps.local</buddyName><networkName>MS Lync</networkName><email>jervin@gps.local</email><displayName>jervin@gps.local</displayName></eventOwner><eventTime>2013-07-30T14:56:58+00:00</eventTime><content><text><html><contentType>text</html><contentType>text</content></text></content></event><events><events><sequenceNumber>0</sequenceNumber><eventType>post</eventType><eventOwner>jervin@gps.local</eventOwner><buddyName>meyers-a@gps.local</buddyName><networkName>MS Lync</networkName><email>meyers-a@gps.local</email><displayName>meyers-a@gps.local</displayName></eventOwner><eventTime>2013-07-30T14:57:16+00:00</eventTime><content><text><html><contentType>text</html><contentType>text</content></text></content></event></events></events></chatTranscript>
```

SOURCES



Example of Single Message per IM:

Tue 7/30/2013 2:45 PM
msmith@gps.local
SkypeForBusiness Lync User#3 Chat 2013-07-30 @ 14:44:55.590#1 (IM)
To jervin@gps.local; msmith@gps.local

msmith@gps.local [7/30/2013 2:44:55 PM]:
got this message

Example of Single Message per User (Combine all conversations):

Tue 7/30/2013 5:53 AM
jdoe@gps.local

To jdoe@gps.local; ajohnson@gps.local; msmith@gps.local; ddavids@gps.local; ameiers@gps.local

jdoe@gps.local [7/30/2013 5:52:58 AM]: **this is a test**
jdoe@gps.local [7/30/2013 5:52:59 AM]: this is a test
jdoe@gps.local [7/30/2013 5:53:14 AM]: hey Matt, just testing Lync
jdoe@gps.local [7/30/2013 5:53:14 AM]: hey Matt, just testing Lync
jdoe@gps.local [7/30/2013 5:53:28 AM]: Hi Cat. testing Lync
jdoe@gps.local [7/30/2013 5:53:28 AM]: Hi Cat. testing Lync
jdoe@gps.local [7/30/2013 2:44:04 PM]: testing lync
jdoe@gps.local [7/30/2013 2:45:08 PM]:
fantastic

NEXT STEPS

After setting up the connector follow the appropriate links below to continue with the configuration of the Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users. We advise to upload a CSV file with the data of the users that should be monitored. Please check CSV File option in the Monitored Users section.
- Filters
- Targets
- Importer Settings

DB



DB

ABOUT DB CONNECTOR

Merge1 DB connector is designed as an open SDK platform to allow our customers to rapidly import a table or part of the table from an MS SQL or Oracle Database. With the DB source you can collect and process data from a table from any MS SQL database. The objective of the connector is to map the columns of the table to specific email required fields format. We are looking to map the "From", "To", "Subject", "Date", "Body" fields to appropriate columns in the text delimited file. Merge1 keeps a history of data imported to make sure the same data is not re-imported (note multiple columns could be added to the body of the email).

SOURCES



DB

With the DB source you can collect and process data from any database. To do so, use **XML mapping** (see the sample below). Upload the **XML** file containing your formatting preferences and click Next.

Configuration XML file *

SELECT

XML MAPPING SAMPLE

```
<?xml version="1.0" encoding="utf-16"?>
<DBConnectorMapping xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsdd="http://www.w3.org/2001/XMLSchema">
<Version>1.0</Version>
<ConnectionString>{Database Connection String}</ConnectionString>
<TableName>{Source Table Name}</TableName>
<Columns>
    <ColumnMetaInfo>
        <Name>{Column Name}</Name>
        <DataType>{Column Type}</DataType> (optional)
        <Nullable>{true/false}</Nullable> (optional)
    </ColumnMetaInfo>
    <ColumnMetaInfo>
        ...
    </ColumnMetaInfo>
    ...
</Columns>
<ColumnMaps>
    <ColumnMapping>
        <CanBeEmpty>{true/false}</CanBeEmpty> (optional)
        <MessagePropertyName>{Message Field Name}</MessagePropertyName>
        <ColumnNames>
            <string>{Column Name from above}</string>
            <string>...</string>
        </ColumnNames>
    </ColumnMapping>
    <ColumnMapping>
        ...
    </ColumnMapping>
    ...
</ColumnMaps>
</DBConnectorMapping>
```

SOURCES



DB

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.

Please note:

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:

- From: One value, must be a valid SMTP email address.
- To: One or more values, each must be a valid SMTP email addresses.
- CC: One or more values, each must be a valid SMTP email addresses.
- BCC: One or more values, each must be a valid SMTP email addresses.
- Subject: One or more values.
- Date: One value, must be a valid DateTime value.
- Body: One or more values.

SOURCES



DB

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.

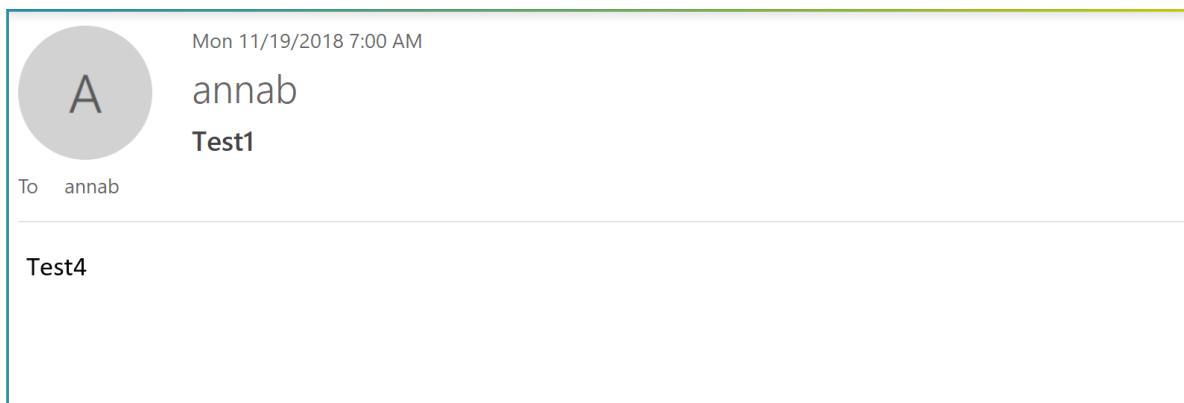
Merge1 DB Connector supports the following data type values that can be collected from the database: varchar, nvarchar, ntext, int, tinyint, longint, and datetime.

Please note:

From, 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.

Example Output Message:



A screenshot of an email message window. The message is as follows:

Mon 11/19/2018 7:00 AM
annab
Test1
To annab

Test4

NEXT STEPS

After setting up the connector follow the appropriate links below to continue with the configuration of the Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users is not applicable to this connector.
- Filters
- Targets
- Importer Settings

REUTERS



Reuters

ABOUT REUTERS

Reuters.com brings user the latest news from around the world, covering breaking news in markets, the business, politics, entertainment, technology, video.

Merge1 Reuters Connector processes data from Eikon Messenger and SI Dealing . Eikon Messenger is captured and delivered to clients either via a daily XML posted to FTP (External Feed) or hosted archiving (Global Relay). The Eikon Messenger instant messaging network is based on an individual's user-ID + firm name and is captured/recognized as such.

Contact our support at support@globanet.com for more details on the mapping corresponding to the source you're going to use Reuters connector for.

ACTIVITIES CAPTURED

- Person to Person messages
- Group Chats
- Attachments
- Disclaimers

SOURCES



Reuters

FTP CONFIGURATIONS

Merge1 retrieves data from Reuters **FTP** and stores it in the Import Folder for processing. Corrupt files are moved to the **Quarantine Folder**.

If you want to get data from Reuters through FTP, tick **Download files from FTP**. FTP Configuration options will automatically open.

1. Connection. Enter the hostname of the remote FTP server and the folder path in the Host and Path textboxes, respectively. The default port is 21. Choose FTP connection type from the Connection type dropdown list. FTP can run in either passive or active mode. Information about the connection type should be provided by the FTP host.

If you wish to use FTP over SSL, select **Use SSL** checkbox and choose connection method: implicit or explicit.

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. This filter is used to 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. This filter is used for separating 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 modified within the mentioned days will be downloaded.
- Only download files modified earlier than/later than. When this option is only the data modified earlier than or later than the mentioned date will be downloaded. Both options can be selected simultaneously to choose a time period.
- Server Time Zone specifies the timezone in which the FTP sever is to correctly determine the timestamp of downloadable files.

5. Options.

- Maintain history of downloaded file for X days. 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.

SOURCES



Reuters

- Download subdirectories recursively. If checked, files from the subdirectories of the mentioned path will be downloaded too.
- Delete files on server after downloading. If checked, the files downloaded will be deleted from the server.

6. Execute script against source files allows the user to utilize alternative methods of data download or acquisition methods other than FTP. For example, batch script files that download information via an FTP alternative and move it into the appropriate processing folder.

PGP CONFIGURATIONS

PGP DECRYPTION OPTIONS

Username *

Password *

Email *

Generated Public Key *

EXPORT PUBLIC KEY

Export/Import Private Key

EXPORT PRIVATE KEY IMPORT PRIVATE KEY

GENERATE KEY

1. Click **Use PGP Decryption** and PGP Decryption Options open.
2. Specify a Username, Password, and Email, then click **Generate Key**. Once the key is generated you will see a green tick icon. **
3. Log into your Reuters control panel and enable PGP encryption by adding Merge1 Keys.
4. In your source control panel click **Add** and the Add Public Key window will appear. From the Key Type drop-down menu, select Encryption and paste the full contents of the public key (including the block header and footer) under the Public Keys tab at the control panel in your terminal.
5. Click the Decryption button. (The key appears in the Public Keys section). To save the PGP encryption key to your account click **Submit**.

Please note:

When the FTP is disabled, Merge1 attempts to retrieve the data directly from the Import Folder. This is useful when data is already in-hand or if the user wishes to acquire the data manually.

* Please note that this password is required for configuring multiple connectors with the same PGP Key.

* Use the Export Public / Private Key buttons to save the keys to a secure location on your device. This will enable you to restore the keys if they are lost or when moving the database to a new machine.

SOURCES



Reuters

FOLDER CONFIGURATION (REQUIRED*)

After successfully setting up the FTP and PGP Configurations, you will have to change the folder configurations. In Merge1 you will have to specify the **Import Folder**, where you would like to store the data after retrieving it from Reuters, 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 Reuters Merge1.t

FOLDERS
Import folder*
<input type="text"/>
<input type="checkbox"/> Traverse subdirectories
Quarantine folder*
<input type="text"/>
AFTER SUCCESSFULL IMPORTING
<input checked="" type="radio"/> Move original files into a subfolder of the Import folder.
<input type="radio"/> Delete original files permanently.

Under the **After Successfully Importing** settings you can provide Merge1 what to do with the original files. You can either Move the original files in a subfolder in Importer Folder or you can Delete the files. Please note that once files are deleted, they can not be recovered.

Please note:

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.

* Merge1 Folder Option 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.

SOURCES



Reuters

ATTACHMENT VALIDATION

Merge1 enables you to develop customized notes for attachment validation. The default setting is **Fail Messages with missing Attachments**, as a result of which the messages that do not have attachments are failed and can be viewed under the Reports. Note that Advanced Processing shouldn't be selected for this to happen.

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.

ATTACHMENT VALIDATION

Full Attachment Validation:

Replace all attachments with the following note:
This message contained the following attachments w/

Replace missing attachments with the following note:
This message contained the following attachments th/

Fail messages with missing attachments. (default)

MESSAGE BODY

In Reuters Connector you can choose from two IB message body options.

When you select Plain option (default) you will see the interactions below each other. If you enable Grid option, you will see the information in the five following columns:

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

SOURCES



Reuters

REUTERS OPTION

Split Messages by Day option merges all messages sent in one day into one email. The date is determined by the UTC timezone, so the messages are split based on their sent time in UTC.

REUTERS OPTIONS

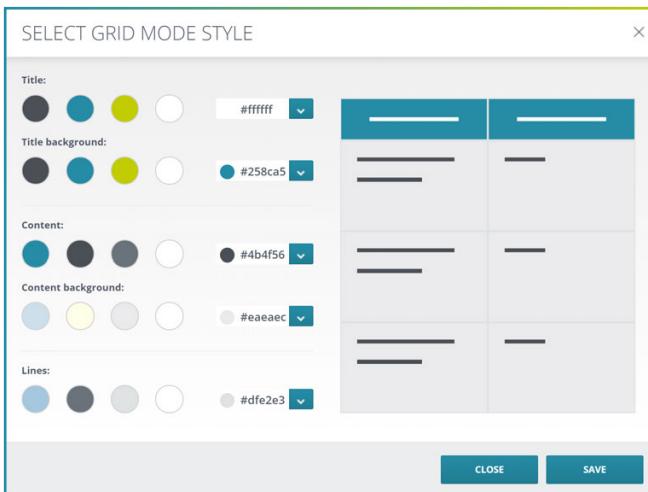
Split Messages by day

MESSAGE BODY

Plain Mode

Grid Mode | [Select Style](#)

It's possible to change the color scheme of the grid mode by clicking on the Select Style.



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

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.

SOURCES



Reuters

MISC SETTINGS

Files to import: e.g.: *.txt | *.xml (separated by vertical bars)*

Subject prefix

EXAMPLES

Plain Mode:

Mon 11/28/2011 6:00 PM
bob Smith <bob@company.com>

To: dave@company.com; bob Smith; bob Smith; bob Smith
Cc: bob Smith

Top5Picks.xls 8 KB Screenshot.png 906 KB

ChatIdentifier: 29edwnjewii39
ChatTopic:
ChatDisclaimer:
Participants:
User: [bob@company.com](#)
User: [dave@company.com](#)
User: [charles@company.com](#)
User: [sam@company.com](#)
User: [simon.company.com@thomsonreuters.com](#)

EventType: Join
EventUser: [bob@company.com](#)
EventUtcTime: 11/28/2011 6:00:20 PM

EventType: Join
EventUser: [dave@company.com](#)
EventUtcTime: 11/28/2011 6:00:20 PM

EventType: Send
EventUser: [bob@company.com](#)
EventUtcTime: 11/28/2011 6:00:20 PM
Content: Hi dave

Grid Mode:

Mon 11/28/2011 6:00 PM
bob Smith <bob@company.com>

To: dave@company.com; bob Smith; bob Smith; bob Smith
Cc: bob Smith

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

Top5Picks.xls 8 KB Screenshot.png 906 KB

ChatIdentifier: 29edwnjewii39
ChatTopic:
ChatDisclaimer:
Participants:
User: [bob@company.com](#)
User: [dave@company.com](#)
User: [charles@company.com](#)
User: [sam@company.com](#)
User: [simon.company.com@thomsonreuters.com](#)

UTC Time Stamp	User Info	Content	Event Type	Message ID	Attachment
11/28/2011 6:00:20 PM	bob@company.com		Join		
11/28/2011 6:00:20 PM	dave@company.com		Join		
11/28/2011 6:00:20 PM	bob@company.com	Hi dave	Send	239238	

SOURCES



Reuters

Split Messages by Day:

Mon 11/28/2011 6:00 PM

bob Smith <bob@company.com>

To: dave@company.com; bob Smith; bob Smith; bob Smith
Cc: bob Smith

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

Top5Picks.xls 8 KB Screenshot.png 906 KB

UTC TIME STAMP	USER INFO	CONTENT	EVENT TYPE	MESSAGE ID	ATTACHMENT
11/28/2011 6:00:20 PM	bob@company.com		Join		
11/28/2011 6:00:20 PM	dave@company.com		Join		
11/28/2011 6:00:20 PM	bob@company.com	Hi dave	Send	239238	
11/28/2011 6:00:20 PM	charles@company.com	That's correct	Send	239300	

NEXT STEPS

After setting up the connector follow the appropriate links below to continue with the configuration of the Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users is not applicable to this connector.
- Filters
- Targets
- Importer Settings

FXCONNECT



FXConnect

ABOUT FXCONNECT CONNECTOR

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

The data from FX Connect should be imported to Merge1 in CSV format. Merge1 maps the columns of the CSV file with the fields in the output message. Please note, that message participants by default are imported in FX Connect User ID format. If you want to map them to the users' email addresses, each email address and corresponding FX Connect User ID should be added in User Mappings section of connector set up (please check Next Steps for more information). Merge1 Connector automatically merges messages with the same session ID into one output message.

ACTIVITIES CAPTURED

- Session ID
- Trade participants
- Messages
- Time Stamps

SOURCES



FXConnect

FTP CONFIGURATIONS

Merge1 retrieves data from FXConnect **FTP** and stores it in the Import Folder for processing. Corrupt files are moved to the **Quarantine Folder**.

If you want to get data from FXConnect through FTP, tick **Download files from FTP**. FTP Configuration options will automatically open.

The screenshot shows the 'FTP' configuration dialog with the following sections:

- CONNECTION (1):** Host: *, Port: 21, Connection Type dropdown.
- AUTHENTICATION (2):** Anonymous Access checked, Username and Password fields, TEST CONNECTION button.
- FILE FILTER (3):** Include selected, wildcard filter: *.
- FILTER BY TIME (4):** None selected, Only download files modified within the last: 1 days, Only download files modified: Later than and Earlier Than date pickers, Server Time Zone: UTC.
- OPTIONS (5):** Maintain history of downloaded file for 5 days (0 = infinite), Download subdirectories recursively, Delete files on server after downloading.
- EXECUTE SCRIPT (6):** Execute script against source files checked, Script file input field, UPLOAD and DOWNLOAD buttons.

1. Connection. Enter the hostname of the remote FTP server and the folder path in the Host and Path textboxes, respectively. The default port is 21. Choose FTP connection type from the Connection type dropdown list. FTP can run in either passive or active mode. Information about the connection type should be provided by the FTP host.

If you wish to use FTP over SSL, select **Use SSL** checkbox and choose connection method: implicit or explicit.

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. This filter is used to 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. This filter is used for separating 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 modified within the mentioned days will be downloaded.
- Only download files modified earlier than/later than. When this option is only the data modified earlier than or later than the mentioned date will be downloaded. Both options can be selected simultaneously to choose a time period.
- Server Time Zone specifies the time zone in which the FTP sever is to correctly determine the time stamp of downloadable files.

5. Options.

- Maintain history of downloaded file for X days. 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.

SOURCES



FXConnect

- Download subdirectories recursively. If checked, files from the subdirectories of the mentioned path will be downloaded too.
- Delete files on server after downloading. If checked, the files downloaded will be deleted from the server.

6. Execute script against source files allows the user to utilize alternative methods of data download or acquisition methods other than FTP. For example, batch script files that download information via an FTP alternative and move it into the appropriate processing folder.

PGP CONFIGURATIONS

PGP DECRYPTION OPTIONS

Username *

Password *

Email *

Generated Public Key *

EXPORT PUBLIC KEY

Export/Import Private Key

EXPORT PRIVATE KEY IMPORT PRIVATE KEY

GENERATE KEY

1. Click **Use PGP Decryption** and PGP Decryption Options open.
2. Specify a Username, Password, and Email, then click **Generate Key**. Once the key is generated you will see a green tick icon. **
3. Log into your FXConnect control panel and enable PGP encryption by adding Merge1 Keys.
4. In your FXConnect control panel click **Add** and the Add Public Key window will appear. From the Key Type drop-down menu, select Encryption and paste the full contents of the public key (including the block header and footer) under the Public Keys tab at the control panel in your FXConnect terminal.
5. Click the Decryption button. (The key appears in the Public Keys section). To save the PGP encryption key to your account click **Submit**.

Please note:

When the FTP is disabled, Merge1 attempts to retrieve the data directly from the Import Folder. This is useful when data is already in-hand or if the user wishes to acquire the data manually.

* Please note that this password is required for configuring multiple connectors with the same PGP Key.

* Use the Export Public / Private Key buttons to save the keys to a secure location on your device. This will enable you to restore the keys if they are lost or when moving the database to a new machine.

SOURCES



FXConnect

FOLDER CONFIGURATION (REQUIRED*)

After successfully setting up the FTP and PGP Configurations, you will have to change the folder configurations. In Merge1 you will have to specify the **Import Folder**, where you would like to store the data after retrieving it from FXConnect, 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 FXConnect Merge1.

The screenshot shows the 'Folders' configuration section of the FXConnect Merge1 interface. It includes fields for 'Import folder*' (with a placeholder 'C:\Temp\Import'), a checkbox for 'Traverse subdirectories', and a field for 'Quarantine folder*' (with a placeholder 'C:\Temp\Quarantine'). Below this, there's a section titled 'AFTER SUCCESSFULL IMPORTING' with two radio button options: 'Move original files into a subfolder of the Import folder.' (selected) and 'Delete original files permanently.'

Under the **After Successfully Importing** settings you can input what you want Merge1 to do with the original files. You can either Move the original files in a subfolder in Importer Folder or you can Delete the files. Please note that once deleted, the files can't be recovered.

Please note:

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.

* Merge1 Folder Option 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.

SOURCES



FXConnect

FXCONNECT CONNECTOR OPTIONS

If you want to manually set up the Source Time Zone select the relevant one from the dropdown menu.

FXCONNECT CONNECTOR OPTIONS

Source Time Zone

▼

Define User Mappings List

⚠ *Please define User Mappings list on next step to tell us how you want Merge1 to map users.*

Once you have selected the Connector Type, you can also provide the **Source Time Zone** information. Merge1 assumes that the messages in the source file are of the set timezone and based on that data the dates in the messages are processed to UTC timezone. By default, Merge1 sets the **Source Time Zone** as UTC.

DEFINE USER MAPPINGS LIST

Merge1 can match FXUserID with the user's SMTP address via the feature called "Match Email Address" in Importer Settings (see the corresponding section in the User Guide). This is normally used to switch an old SMTP address with a new one, however, it can also be used to switch the FXID with an SMTP address. Create a CSV file with the following 5 columns per user:

- LastName
- FirstName
- CompanyName
- FXUserID
- SMTP address

Select **Change the SMTP address** and point to the location of the CSV. You can click Preview to see how it looks and click Save.

MISCELLANEOUS SETTINGS

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

MISC SETTINGS

Files to import: e.g.: *.txt|*.xml (separated by vertical bars)*

Subject prefix

SOURCES



FXConnect

The **Subject Prefix** is added to the subject line of imported emails. For example, if the subject prefix "FxConnect" is entered, the subject line of the message will look as in the example below. This is useful for organizing imported data, i.e. when multiple sources share a common target

Thu 6/24/2010 10:58 AM

D dondavo.lol.pijamo

FxConnect FXConnect Chat – 06/24/2010 - Trade ID: 24704921

To globstar.loi.turnament

Example of sample source file:

A	B	C	D	E	F
1 SELLTRIAD	BUYTRIAD	SESSIONID MESSAGE		MSGTIMESTAMP	MSGCREATEDBY
2 bbq.netc.painter	globstar.loi.cppjava	24252431 [2010-06-10 12:44:35] hey Jatin		44:27.7 SERVER	
3 bbq.netc.painter	globstar.loi.cppjava	24252431 [2010-06-10 17:45:14] hurry up		44:36.1 bbq.netc.painter	
5 bbq.netc.painter	globstar.loi.cppjava	24252431 [2010-06-10 17:45:19] hehe		45:14.7 globstar.loi.cppjava	
6 bbq.netc.painter	globstar.loi.cppjava	24252431 [2010-06-10 17:45:24] test order		45:20.0 globstar.loi.cppjava	
7 bbq.netc.painter	globstar.loi.cppjava	24252431 [2010-06-10 12:45:24] trader working it at best		45:24.5 globstar.loi.cppjava	
8 bbq.netc.painter	globstar.loi.cppjava	24252431 [2010-06-10 17:45:28] hahahahaha		45:24.7 bbq.netc.painter	
9 bbq.netc.painter	globstar.loi.cppjava	24252431 [2010-06-10 12:45:28] half done		45:28.4 globstar.loi.cppjava	
10 bbq.netc.painter	globstar.loi.cppjava	24252431 [2010-06-10 17:45:34] dont front run me dude!		45:28.8 bbq.netc.painter	
11 dondavo.loi.pijamo	globstar.loi.cppjava	24329781 Trader loi.dondavo.pijamo picked up new trade session from loi.globstar.cppjava; Trade Session Id: GLOBSTAR-24329781		45:34.7 globstar.loi.cppjava	
12 duteacher.loi.schema	globstar.loi.gogsmo	24330491 Trader loi.duteacher.schema picked up new trade session from loi.globstar.gogsmo; Trade Session Id: GLOBSTAR-24330491		02:24.2 SERVER	
13 barcode.loi.mrichards	globstar.loi.gogsmo	24330811 Trader loi.barcode.mrichards picked up new trade session from loi.globstar.gogsmo; Trade Session Id: GLOBSTAR-24330811		18:30.2 SERVER	
14 dondavo.loi.pijamo	globstar.loi.turnament	24333921 Trader loi.dondavo.pijamo picked up new trade session from loi.globstar.turnament; Trade Session Id: GLOBSTAR-24333921		22:45.3 SERVER	
15 dondavo.loi.pijamo	globstar.loi.turnament	24333921 [2010-06-14 15:02:58] pls price at mkt		02:39.7 SERVER	
16 dondavo.loi.pijamo	globstar.loi.turnament	24333921 [2010-06-14 15:03:00] ha		02:59.2 globstar.loi.turnament	
17 fbcmbf.lo.brooklyn	globstar.loi.gogsmo	24337171 Trader loi.fbcmbf.brooklyn picked up new trade session from loi.globstar.gogsmo; Trade Session Id: GLOBSTAR-24337171		03:01.3 globstar.loi.turnament	
18 fbcmbf.lo.brooklyn	globstar.loi.gogsmo	24337171 [2010-06-15 15:44:59] 4pm fixing order		37:56.9 SERVER	
19 fbcmbf.lo.brooklyn	globstar.loi.turnament	24370161 Trader loi.fbcmbf.brooklyn picked up new trade session from loi.globstar.turnament; Trade Session Id: GLOBSTAR-24370161		45:00.0 globstar.loi.gogsmo	
20 dondavo.loi.kwright	globstar.loi.turnament	24375411 Trader loi.dondavo.kwright picked up new trade session from loi.globstar.turnament; Trade Session Id: GLOBSTAR-24375411		27:03.3 SERVER	
21 bbq.lo.shameonyou	globstar.loi.gogsmo	24382061 Trader loi.bbq.shameonyou picked up new trade session from loi.globstar.gogsmo; Trade Session Id: GLOBSTAR-24382061		46:01.3 SERVER	
22 bbq.lo.shameonyou	globstar.loi.gogsmo	24382061 [2010-06-15 15:00:44] hello		00:29.6 SERVER	
23 bbq.lo.shameonyou	globstar.loi.gogsmo	24382061 [2010-06-15 15:00:49] ab pls		00:45.0 globstar.loi.gogsmo	
24 bbq.lo.shameonyou	globstar.loi.gogsmo	24382061 [2010-06-15 10:00:54] sure		00:50.0 globstar.loi.gogsmo	
25 urban.lo.sanfrancisco	globstar.loi.gogsmo	24382571 Trader loi.urban.sanfrancisco picked up new trade session from loi.globstar.gogsmo; Trade Session Id: GLOBSTAR-24382571		00:55.4 bbq.lo.shameonyou	
				06:00:2 SERVER	

Example of output message:

Thu 6/10/2010 5:44 PM

B bbq.netc.painter

FxConnect FXConnect Chat – 06/10/2010 - Trade ID: 24252431

To globstar.loi.cppjava

We removed extra line breaks from this message.

SERVER 12:44:27> [2010-06-10 12:44:27] Trader netc.bbq.painter picked up new trade session from loi.globstar.cppjava; Trade Session Id: GLOBSTAR-24252431 bbq.netc.painter 12:44:36> [2010-06-10 12:44:36] hey Jatin globstar.loi.cppjava 12:45:14> [2010-06-10 12:45:14] [2010-06-10 12:45:14] [2010-06-10 17:45:14] hurry up globstar.loi.cppjava 12:45:20> [2010-06-10 12:45:20] [2010-06-10 17:45:19] hehe globstar.loi.cppjava 12:45:24> [2010-06-10 12:45:24] [2010-06-10 17:45:24] test order bbq.netc.painter 12:45:24> [2010-06-10 12:45:24] [2010-06-10 12:45:24] trader working it at best globstar.loi.cppjava 12:45:28> [2010-06-10 12:45:28] [2010-06-10 17:45:28] hahahahaha bbq.netc.painter 12:45:28> [2010-06-10 12:45:28] [2010-06-10 17:45:28] half done globstar.loi.cppjava 12:45:34> [2010-06-10 12:45:34] [2010-06-10 17:45:34] dont front run me dude!

NEXT STEPS

After setting up the connector follow the appropriate links below to continue with the configuration of the Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users - not applicable
- Filters (FX Connect works with all filters except **XML Filter**)
- Targets
- Importer Settings

BOXCOM



BoxCom

ABOUT BOXCOM CONNECTOR

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

ACTIVITIES CAPTURED

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

Please note:

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

SOURCES



BoxCom

CREATING BOXCOM APPLICATION

1. Go to developer.box.com, sign in to an existing account or create a new one.
2. Click on **Create New App**

A screenshot of the 'My Apps' section of the Box Developers website. On the left, there's a sidebar with links like 'My Apps', 'SDKs', 'API Docs', and 'Support'. The main area shows a list of apps under 'My Apps'. At the bottom of this list is a large button with a plus sign and the text 'Create New App'. A red arrow points from the top right towards this button.

3. Choose **Custom App** and click **Next**

A screenshot of the 'CREATE A NEW BOX APP' wizard. The title bar says 'CREATE A NEW BOX APP'. Below it, a question asks 'Let's get started. What type of app are you building?'. Three options are shown: 'Custom App', 'Enterprise Integration', and 'Partner Integration'. The 'Custom App' option is highlighted with a blue box. At the bottom right of the screen, there are 'Cancel' and 'Next' buttons, with the 'Next' button being highlighted by a red box.

SOURCES



BoxCom

4. Use **Standard OAuth 2.0 Authentication Method** and click **Next**

CREATE A NEW BOX APP

Authentication Method

We've recommended an authentication method based on the type of app you've chosen.
You may change the authentication method below. [Learn more.](#)

RECOMMENDED FOR CUSTOM APP:

OAuth 2.0 with JWT (Server Authentication)
Allows your app to authenticate directly to Box using a digitally signed JSON Web Token instead of user credentials. For use with Service Accounts and App Users.

OTHER AVAILABLE AUTHENTICATION METHODS:

App Token (Server Authentication)
Provides API functionality scoped to previewing content in your application. This will NOT allow you to create and manage users in Box. Please read our documentation on New Box View and make sure that it fits your application's requirements before proceeding.

Standard OAuth 2.0 (User Authentication)
Requires Box users to log in with a username and password to authorize your app to access content in their account.

[Back](#) [Next](#)

5. Give a name to the app and click **Create App**

CREATE A NEW BOX APP

What would you like to name your app?

Don't worry—you can change this later.

By clicking 'Create App', you agree to the terms of the [Box Developer Agreement](#) and the [Box Privacy Policy](#).

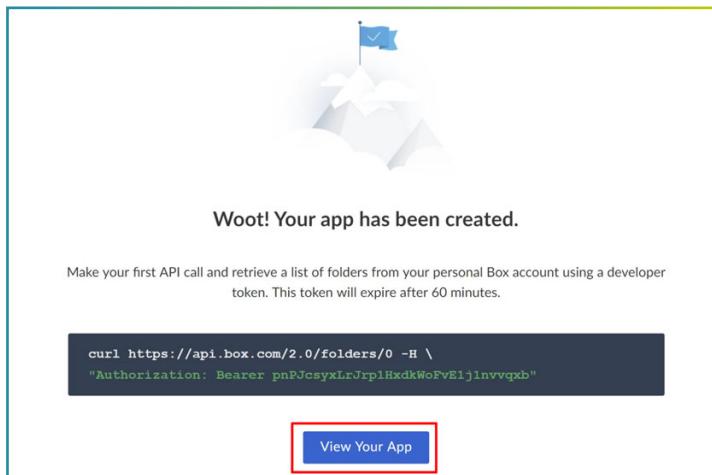
[Back](#) [Create App](#)

SOURCES



BoxCom

6. After the creation of the app you'll receive this message. Click on **View Your App**.



7. Go to the **Configuration** section, copy and save **Client ID** and **Client Secret**

Configuration
Configure the authentication and permissions for your app to begin using the Box APIs. Check out our [Getting Started Guide](#) for a walkthrough of these settings.

OAuth 2.0 Credentials
Credentials for using OAuth 2.0 as your Authentication type.

Client ID	74qp03xwh12kz90b8ntmt15k6qu0fs9	COPY
Client Secret	*****	COPY

Reset

8. Add Merge1 IP address to Redirect URI and Save Changes:

<https://Merge1IPaddress/Configuration/OAuthCallback>

Configuration
Configure the authentication and permissions for your app to begin using the Box APIs. Check out our [Getting Started Guide](#) for a walkthrough of these settings.

OAuth 2.0 Redirect URI
The redirect URI is the URL within your application that will receive OAuth 2.0 credentials.

Redirect URI
https://192.168.10.69/Configuration/OAuthCallback

Save Changes

SOURCES



BOXCOM APPLICATION CONFIGURATION

1. Go to Merge1, click on **Add Importer**
2. Enter a **Name** and a Description (optional) for the connector.

The screenshot shows the 'CONFIGURATION WIZARD' window with the title 'ADD IMPORTER'. It contains two input fields: 'Name' with the value 'Importer' and 'Description' with the value 'Importers'. A large 'NEXT' button is visible at the bottom right.

3. In the field of the **Application ID** add the **Client ID** copied previously, and in the field of **Application Secret/Key** enter copied **Client Secret**, click **Next**.

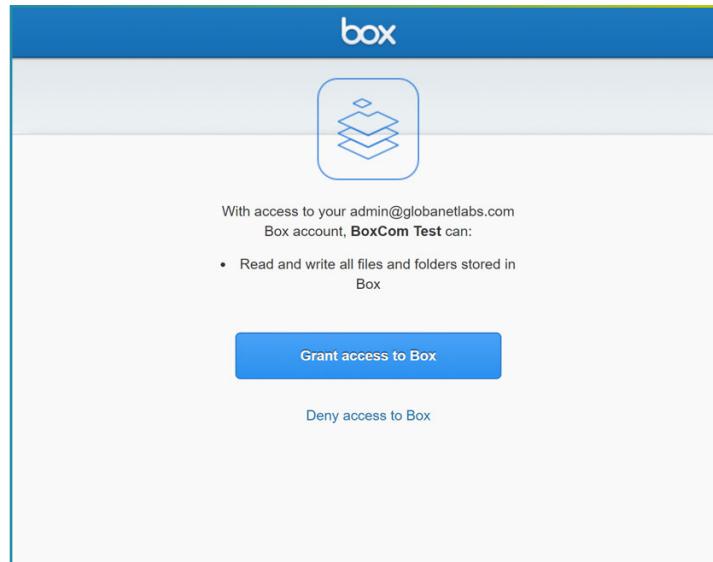
The screenshot shows the 'CONFIGURATION WIZARD' window with the title 'BOX APPLICATION CONFIGURATION'. It includes tabs for SOURCE, MONITORED USERS, FILTERS, TARGETS, and SETTINGS. The SOURCE tab is selected. A note at the top says: 'Please provide the following credentials to your company's Box app so that Merge1 can be configured to access your monitored users' account data.' Below this, a link says: 'If you do not have an app created for Box, please [click](#) for more information.' There are two input fields: 'Application ID' and 'Application Secret/Key'. At the bottom, there are 'BACK' and 'NEXT' buttons.

SOURCES



BoxCom

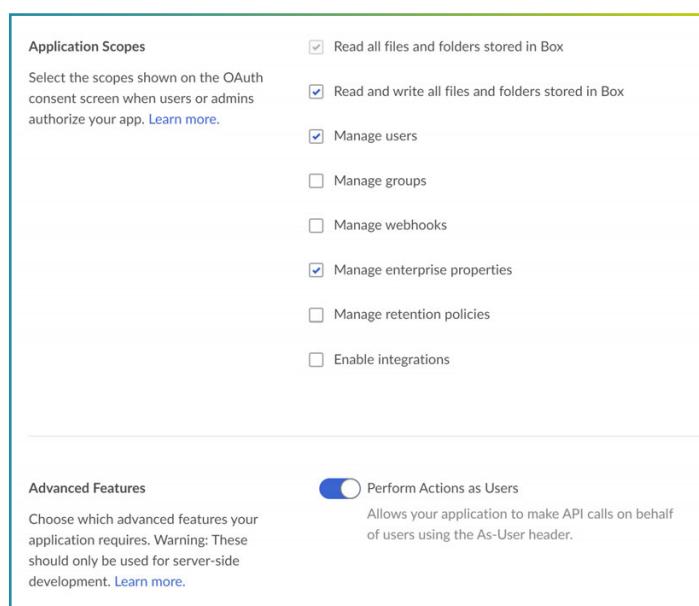
4. Grant Access to Box in the opened pop-up window. Make sure that pop-ups are not blocked by your browser.



BOXCOM APPLICATION PERMISSION SCOPES

The BoxCom application should have the following permissions:

- Application Scopes
 - Read all files and folders stored in Box
 - Read and write all files and folders stored in Box
 - Manage users
 - Manage enterprise properties
- Advanced Features: Perform Actions as Users



SOURCES



BoxCom

ADDITIONALLY PROCESSED DATA

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

- The **Auto Update** feature will ensure that the connector is updated to the latest version. Each time the Importer is run, it contacts Globanet server(s) and updates the connector if a newer version is available.
- **Process File Downloads**, if checked processes the download file events from the events feed in BoxCom.
- To ignore the downloads done by the connected to the Merge1application, add the application ID in the "**Skip downloads initiated by service**" field. Follow these steps to retrieve the ID:
 1. Log in to Box and navigate to "https://developers.box.com/".
 2. At the top right corner, click **My Apps**.
 3. Select your application to navigate to its details page.
 4. Copy the last number from the URL. in the browser address field e.g.
(<https://<yourdomain>.app.box.com/developers/console/app/THIS-NUMBER>)

The screenshot shows a configuration interface for 'ADDITIONALLY PROCESSED DATA'. It includes two checkboxes: 'Auto Update' and 'Process File Downloads'. Below these is a text input field labeled 'Skip downloads initiated by service' containing the placeholder 'https://<yourdomain>.app.box.com/developers/console/app/THIS-NUMBER'. To the right of the input field is a link 'How to get service id'.

ADVANCED CONFIGURATION OPTIONS

- The **Do not download data modified before** check will ensure that old or irrelevant data is excluded. For example, if the date selected is 9/1/2017, it won't retrieve any data modified before September 1 of 2017. Only the data after 9/1/2017 will be retrieved, archived, and imported.
- The **Choose file types to extract text** allows choosing the types of files that will be extracted as txt files.

The screenshot shows a configuration interface for 'ADVANCED CONFIGURATION OPTIONS'. It features a checkbox 'Do not download data modified before:' followed by a date input field. Below this is a section labeled 'Choose file types to extract text' with a corresponding input field.

SOURCES



BoxCom

Example of output message:

Mon 10/22/2018 12:16 PM

Admin <admin@example.com>

Re: FXConnect.png (UPLOAD)

To Admin

comment to an old post

>From: Admin admin@example.com
>To: Admin admin@example.com
>Subject: Re: FXConnect.png (UPLOAD)
>Sent: 22/10/2018 12:15
>File size: 945550 bytes
>Folder path: All Files
>URL to file: N/A
>File tags:

NEXT STEPS

After setting up the connector follow the appropriate links below to continue with the configuration of the Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users (preferred option for BoxCom is **All (Based on Native API)**, the users will be retrieved automatically)
- Filters (BoxCom works with all filters except **XML Filter**)
- Targets
- Importer Settings

JABBER



Jabber

ABOUT JABBER

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 process it.

Please use Jabber Enterprise connector if you want to import data from multiple databases.

ACTIVITIES CAPTURED

- Messages between individuals
- Groups chats

SOURCES



Jabber

DB CONFIGURATION

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

- Postgres
- Microsoft SQL Server
- Oracle Database

In the **Command Timeout** field time can be set after which if the SQL query still runs, it will yield a timeout. The timeout is specified in seconds.

Select the database that you want to connect to and click **Configure**.

DB CONFIGURATION

DATABASE TYPE

Postgres
 Microsoft SQL Server
 Oracle databases

CONFIGURE

Command Timeout

POSTGRESS CONNECTION

1. Enter the server name or IP address and the Port.
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's set upon. If Postgres Server Authentication is chosen it can be connected to with the Postgres server credentials.

3. Select the database, where Jabber files are stored, from the drop-down menu after connecting to the server,
4. Add the name of the scheme in the Select Scheme field.

5. 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.

SOURCES



Jabber

- **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 having 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.

POSTGRESQL CONNECTION

Select SQL Server Select Port
5432 ①

CONNECT

CONNECT USING ②

Windows Authentication
 Postgres Server Authentication

Login Name

Password

Select Database - Select Database - ③

Select Scheme

ADVANCED CONNECTION PARAMETERS ⑤

Connection timeout 15 sec

Load balance timeout 0 sec

Min pool size 0

Max pool size 100

Network packet size 8000 bytes

Asynchronous Processing

Encrypt

Enlist

Pooling

Replication

SOURCES



Jabber

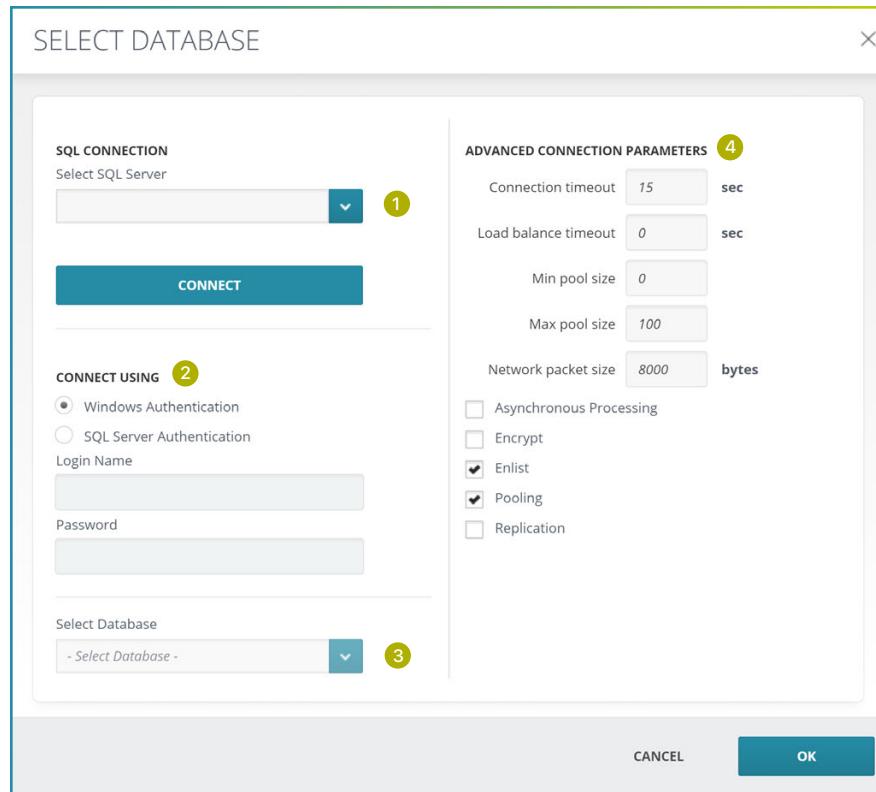
MICROSOFT SQL SERVER

- 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's 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.
- 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 having 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.

SOURCES



Jabber



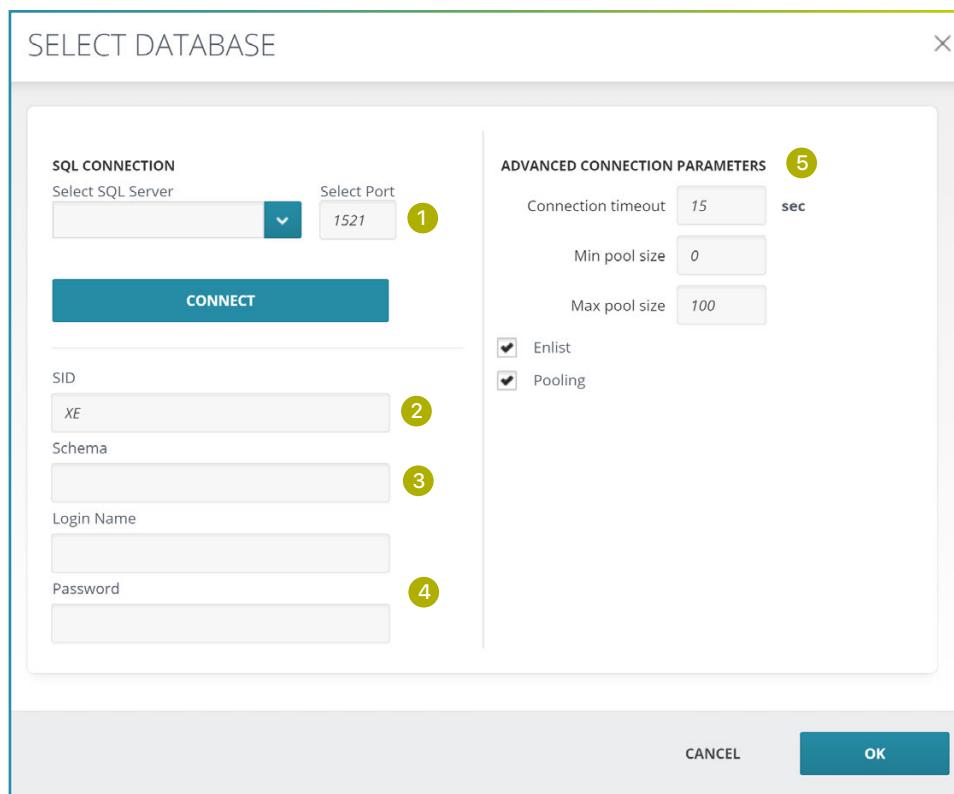
ORACLE DATABASE

1. Select the server from the drop-down menu or enter it manually, and add the Port number.
2. In the SID field add your Oracle SID, the unique name that uniquely identifies your instance/database.
3. Add the name of your database schema in the Schema.
4. Login Name and Password
5. 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.
 - **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.
 - **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 having to create another one.

SOURCES

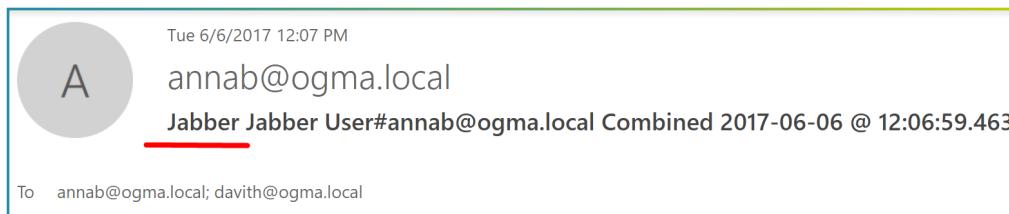


Jabber



ADVANCED CONFIGURATION

- The **Auto Update** feature will ensure that the connector is updated to the latest version. Each time the Importer is run, it contacts Globanet server(s) and updates the connector if a newer version is available.
- The **Subject Prefix** is added to the subject line of imported emails. For example, if the subject prefix "Jabber" is entered, the subject line of the message will look as in the example below. 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 name. You can enable **Bloomberg Vault Format** to enable Bloomberg archive formatting.

SOURCES



Jabber

- 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.
- The **Do not download data modified before** check will ensure that old or irrelevant data is excluded. For example, if the date selected is 9/1/2017, it won't retrieve any data modified before September 1 of 2017. Only the data after 9/1/2017 will be retrieved, archived, and imported.
- **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 amount of hours, you can enable **Archiving Delay Check**.

OTHER OPTIONS

Auto Update:

Subject Prefix

Single Message per Conversation

Single Message per Conversation Contributor

Single Message per IM

Single Message per User (Combine all conversations)

Do not download data modified before:

Enable Message Chunking

IMs per Chunk

Enable Archiving Delay Check

Delay(Hours)

SOURCES



Jabber

Example of Single Message per Conversation:

Fri 6/2/2017 12:14 PM
davith@ogma.local
Jabber Jabber User#davith@ogma.local Conference 2017-06-02 @ 12:14:15.483 ThreadID:chat284812036020360@
To annab@ogma.local; davith@ogma.local

[davith@ogma.local](#) [6/2/2017 12:14:15 PM]: test message to group chat
[davith@ogma.local](#) [6/2/2017 12:15:27 PM]: asdfasf asf jka sjkdfhas f asfasf multiline
[annab@ogma.local](#) [6/2/2017 12:16:14 PM]: Aram Karapetyan OK

Example of Single Message per Conversation Contributor:

Fri 6/2/2017 12:14 PM
davith@ogma.local
Jabber Jabber User#davith@ogma.local Conference 2017-06-02 @ 12:14:15.483 ThreadID:chat284812036020360@
To annab@ogma.local; davith@ogma.local

[davith@ogma.local](#) [6/2/2017 12:14:15 PM]: test message to group chat
[davith@ogma.local](#) [6/2/2017 12:15:27 PM]: asdfasf asf jka sjkdfhas f asfasf multiline
[annab@ogma.local](#) [6/2/2017 12:16:14 PM]: Aram Karapetyan OK

Fri 6/2/2017 12:14 PM
annab@ogma.local
Jabber Jabber User#annab@ogma.local Conference 2017-06-02 @ 12:14:15.483 ThreadID:chat284812036020360@
To annab@ogma.local; davith@ogma.local

[davith@ogma.local](#) [6/2/2017 12:14:15 PM]: test message to group chat
[davith@ogma.local](#) [6/2/2017 12:15:27 PM]: asdfasf asf jka sjkdfhas f asfasf multiline
[annab@ogma.local](#) [6/2/2017 12:16:14 PM]: Aram Karapetyan OK

Example of Single Message per Conversation Contributor (Bloomberg Vault Format):

Sun 6/4/2017 10:24 AM
davith@ogma.local
Jabber Jabber User#davith@ogma.local Conference 2017-06-04 @ 10:24:19.293 ThreadID:connect23416 #1 (Conversation)
To davith@ogma.local; aramk@ogma.local

<?xml version="1.0"?><chatTranscript><sessionId>connect23416</sessionId><startTime>2017-06-04T10:24:19+00:00</startTime><endTime>2017-06-04T10:24:19+00:00</endTime><participants><buddyName>davith@ogma.local</buddyName><email>davith@ogma.local</email><display Name>davith@ogma.local</display Name></participants><participants><buddyName>aramk@ogma.local</buddyName><email>aramk@ogma.local</email><display Name>aramk@ogma.local</display Name></participants><events><sequenceNumber>connect23416</sequenceNumber><eventType>post</eventType><eventOwner><buddyName>davith@ogma.local</buddyName><networkName>Cisco Jabber</networkName><email>davith@ogma.local</email><display Name>davith@ogma.local</display Name></eventOwner><eventTime>2017-06-04T10:24:19+00:00</eventTime><content><contentType>text_plain</contentType><text>message on 06/04 - 2</text></content></events><messageSize>38</messageSize><documentType>im</documentType></chatTranscript>

SOURCES



Jabber

Example of Single Message per IM:

Tue 6/6/2017 12:07 PM
annab@ogma.local
Jabber Jabber User#annab@ogma.local Chat 2017-06-06 @ 12:06:59.463 ThreadID:connect18000 #1 (IM)
To annab@ogma.local; davith@ogma.local

[annab@ogma.local](#) [6/6/2017 12:06:59 PM]: here we go

NEXT STEPS

After setting up the connector follow the appropriate links below to continue with the configuration of the Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users. For Jabber it's possible to Filter Accounts using Active Directory, CSV file, or Manually Maintain the users for filtering.
- Filters (Jabber works with all filters except **XML Filter**)
- Targets
- Importer Settings

PIVOT



Pivot

HOW TO SET UP THE PIVOT IMPORTER

After selecting the Pivot icon in the Configuration Wizard and clicking **Next** you will be redirected to the next screen of the Configuration. As mentioned earlier the Configuration Wizard Screen consists of 5 tabs. You will be prompted to start with Source Configuration.

The Pivot Source Configuration tab has the following Settings options (click on the name to open the relevant configuration information):

- FTP configurations
- PGP configurations
- Folders (Required)
- Misc Settings

CONFIGURATION WIZARD

SOURCE **MONITORED USERS** **FILTERS** **TARGETS** **SETTINGS**

Please provide your Pivot configuration data so that Merge1 can access your Pivot data.

FTP

Download files from FTP

FTP CONFIGURATION OPTIONS +

Execute script against source files

Script file * UPLOAD

PGP

Use PGP Decryption

PGP DECRYPTION OPTIONS +

BACK NEXT

SOURCES



Pivot

FTP CONFIGURATIONS

Merge1 retrieves data from Pivot **FTP** and stores it in the Import Folder for processing. Corrupt files are moved to the **Quarantine Folder**.

If you want to get data from Pivot through FTP, tick **Download files from FTP**. FTP Configuration options will automatically open.

The screenshot shows the 'FTP CONFIGURATION OPTIONS' dialog box. It includes sections for Connection, Authentication, File Filter, Filter by Time, Options, and Execute Script. Callouts numbered 1 through 6 point to various configuration fields:

- CONNECTION (1):** Host, Port, Connection Type dropdown.
- AUTHENTICATION (2):** Use Security checkboxes for Implicit SSL, Explicit SSL, and SSH; Anonymous Access checkbox.
- FILE FILTER (3):** Include/Exclude radio buttons, wildcard filter input.
- FILTER BY TIME (4):** None, Only download files modified within the last 1 day, Only download files modified, Later than/Earlier Than date pickers, Server Time Zone dropdown.
- OPTIONS (5):** Maintain history of downloaded file for 5 days, Download subdirectories recursively, Delete files on server after downloading.
- EXECUTE SCRIPT (6):** Execute script against source files checkbox, Script file input, UPLOAD and DOWNLOAD buttons.

1. Connection. Enter the hostname of the remote FTP server and the folder path in the Host and Path textboxes, respectively. The default port is 21. Choose FTP connection type from the Connection type dropdown list. FTP can run in either passive or active mode. Information about the connection type should be provided by the FTP host. If you wish to use FTP over SSL, select **Use SSL** checkbox and choose connection method: implicit or explicit.

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. This filter is used to 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. This filter is used for separating 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 modified within the mentioned days will be downloaded.
- Only download files modified earlier than/later than. When this option is only the data modified earlier than or later than the mentioned date will be downloaded. Both options can be selected simultaneously to choose a time period.
- Server Time Zone specifies the timezone in which the FTP sever is to correctly determine the timestamp of downloadable files.

5. Options.

- Maintain history of downloaded file for X days. 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.

SOURCES



Pivot

- Download subdirectories recursively. If checked, files from the subdirectories of the mentioned path will be downloaded too.
- Delete files on server after downloading. If checked, the files downloaded will be deleted from the server.

6. Execute script against source files allows the user to utilize alternative methods of data download or acquisition methods other than FTP. For example, batch script files that download information via an FTP alternative and move it into the appropriate processing folder.

PGP CONFIGURATIONS

PGP DECRYPTION OPTIONS

Username *

Password *

Email *

Generated Public Key *

EXPORT PUBLIC KEY

Export/Import Private Key

EXPORT PRIVATE KEY IMPORT PRIVATE KEY

GENERATE KEY

1. Click **Use PGP Decryption** and PGP Decryption Options open.
2. Specify a Username, Password, and Email, then click **Generate Key**. Once the key is generated you will see a green tick icon. **
3. Log into your Pivot control panel and enable PGP encryption by adding Merge1 Keys.
4. In your Pivot control panel click **Add** and the Add Public Key window will appear. From the Key Type drop-down menu, select Encryption and paste the full contents of the public key (including the block header and footer) under the Public Keys tab at the control panel in your terminal.
5. Click the Decryption button. (The key appears in the Public Keys section). To save the PGP encryption key to your account click **Submit**.

Please note:

When FTP is disabled, Merge1 attempts to retrieve the data directly from the Import Folder. This is useful when data is already in-hand or if the user wishes to acquire the data manually.

* Please note that this password is required for configuring multiple connectors with the same PGP Key.

* Use the Export Public / Private Key buttons to save the keys to a secure location on your device. This will enable you to restore the keys if they are lost or when moving the database to a new machine.

SOURCES



Pivot

FOLDER CONFIGURATION (REQUIRED*)

After successfully setting up the FTP and PGP Configurations, you will have to change the folder configurations. In Merge1 you will have to specify the **Import Folder**, where you would like to store the data after retrieving it from Pivot, 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 Pivot Merge1.

FOLDERS	
Import folder*	<input type="text"/>
<input type="checkbox"/> Traverse subdirectories	
Quarantine folder*	<input type="text"/>
AFTER SUCCESSFULL IMPORTING	
<input checked="" type="radio"/> Move original files into a subfolder of the Import folder.	
<input type="radio"/> Delete original files permanently.	

Under the **After Successfully Importing** settings you can input what you want Merge1 what to do with the original files. You can either Move the original fines in a subfolder in Importer Folder or you can Delete the files. Please note that once Deleted you can not recover them.

Please note:

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.

* Merge1 Folder Option 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.

SOURCES



Pivot

MISCELLANEOUS SETTINGS

If you want to import specific files or filetypes, note them in the Files to Import form.

You can separate each file or filetype with a vertical bar " | ". Simply write the name of the file (ex. pivot.xml) or use wildcards to import the whole filetype) (ex. *.txt | *.xml).

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.

MISC SETTINGS

Files to import: e.g.: *.txt|*.xml (separated by vertical bars)*

Subject prefix

PRIMARY ADDRESS TO USE

Choose the email address type you would like Merge1 to prioritize when processing data from users that have both their corporate email address and their corporate email address registered on Pivot.

PRIMARY ADDRESS TO USE

Pivot email address

Corporate email address

SOURCES



Pivot

Example of an output message:

Mon 1/8/2018 6:32 PM
csmith@example.net <clark.smith@example.com>

To Default example test-6a3174ef-d8ab-44a0-9413-0ec0c55d58f2 Chatroom Listener; csmith@example.net; clark.smith@cmepivot.im

ParticipantEntered: Default example test-6a3174ef-d8ab-44a0-9413-0ec0c55d58f2 Chatroom Listener
DateTimeUTC: [2018-01-08 18:32:04]
InternalFlag:
CorporateEmailID: [chatroomlistener@pivot3.example.net](#)

ParticipantEntered: [csmith@example.net](#)
DateTimeUTC: [2018-01-08 18:32:04]
InternalFlag:
CorporateEmailID: [clark.smith@example.com](#)

ParticipantEntered: [clark.smith@cmepivot.im](#)
DateTimeUTC: [2018-01-08 18:32:04]
InternalFlag:
CorporateEmailID: [clark.smith@example.com](#)

MessageBy: [clark.smith@example.net](#)
DateTimeUTC: [2018-01-08 18:32:04]
Message: testing 123

MessageBy: [clark.smith@example.net](#)
DateTimeUTC: [2018-01-08 18:42:46]
Message: testing room

NEXT STEPS

After setting up the connector follow the appropriate links below to continue with the configuration of the Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users is not applicable.
- Filters
- Targets
- Importer Settings

ICECHAT



IceChat

ABOUT 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 ICE Chat users can react to trade opportunities in real-time with features including quote and trade recognition logic, blast messages and a marketplace directory connecting over 80,000 market participants.

ACTIVITIES CAPTURED

- Room ID
- Start Time
- Message Content
- Participants
- Participants Entered
- Message Date

SOURCES



IceChat

FTP CONFIGURATIONS

Merge1 retrieves data from IceChat **FTP** and stores it in the Import Folder for processing. Corrupt files are moved to the **Quarantine Folder**.

If you want to get data from IceChat through FTP, tick **Download files from FTP**. FTP Configuration options will automatically open.

The screenshot shows the 'FTP CONFIGURATION OPTIONS' dialog box. It includes the following sections:

- Connection (1):** Host: *, Port: 21, Connection Type: Passive.
- Authentication (2):** Anonymous Access checked, Username: [redacted], Password: [redacted].
- File Filter (3):** Include selected, Filter: *.
- Filter by Time (4):** Only download files modified within the last: 1 days.
- Options (5):** Maintain history of downloaded file for 5 days (0 = infinite), Download subdirectories recursively, Delete files on server after downloading.
- Script (6):** Execute script against source files, Script file: [redacted], UPLOAD and DOWNLOAD buttons.

1. Connection. Enter the hostname of the remote FTP server and the folder path in the Host and Path textboxes, respectively. The default port is 21. Choose FTP connection type from the Connection type dropdown list. FTP can run in either passive or active mode. Information about the connection type should be provided by the FTP host. If you wish to use FTP over SSL, select **Use SSL** checkbox and choose connection method: implicit or explicit.

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. This filter is used to 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. This filter is used for separating 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 modified within the mentioned days will be downloaded.
- Only download files modified earlier than/later than. When this option is only the data modified earlier than or later than the mentioned date will be downloaded. Both options can be selected simultaneously to choose a time period.
- Server Time Zone specifies the time zone in which the FTP sever is to correctly determine the time stamp of downloadable files.

5. Options.

- Maintain history of downloaded file for X days. 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.

SOURCES



IceChat

- Download subdirectories recursively. If checked, files from the subdirectories of the mentioned path will be downloaded too.
- Delete files on server after downloading. If checked, the files downloaded will be deleted from the server.

6. Execute script against source files allows the user to utilize alternative methods of data download or acquisition methods other than FTP. For example, batch script files that download information via an FTP alternative and move it into the appropriate processing folder.

PGP CONFIGURATIONS

PGP DECRYPTION OPTIONS

Username *

Password *

Email *

Generated Public Key *

EXPORT PUBLIC KEY

Export/Import Private Key

EXPORT PRIVATE KEY IMPORT PRIVATE KEY

A circular button with a white circular arrow icon inside, labeled 'GENERATE KEY' below it.

1. Click **Use PGP Decryption** and PGP Decryption Options open.
2. Specify a Username, Password, and Email, then click **Generate Key**. Once the key is generated you will see a green tick icon. **
3. Log into your IceChat control panel and enable PGP encryption by adding Merge1 Keys.
4. In your IceChat control panel click **Add** and the Add Public Key window will appear. From the Key Type drop-down menu, select Encryption and paste the full contents of the public key (including the block header and footer) under the Public Keys tab at the control panel in your terminal.
5. Click the Decryption button. (The key appears in the Public Keys section). To save the PGP encryption key to your account click **Submit**.

Please note:

When FTP is disabled, Merge1 attempts to retrieve the data directly from the Import Folder. This is useful when data is already in-hand or if the user wishes to acquire the data manually.

* Please note that this password is required for configuring multiple connectors with the same PGP Key.

* Use the Export Public / Private Key buttons to save the keys to a secure location on your device. This will enable you to restore the keys if they are lost or when moving the database to a new machine.

SOURCES



IceChat

FOLDER CONFIGURATION (REQUIRED*)

After successfully setting up the FTP and PGP Configurations, you will have to change the folder configurations. In Merge1 you will have to specify the Import Folder, where you would like to store the data after retrieving it from IceChat, as well as **Quarantine Folder** where all the failed messages will be archived. If you have sub-folders under your Import Folder, you can enable **Traverse Subdirectories** to maintain the sub-folder structure of imported data and include the data in your IceChat Merge1.

FOLDERS

Import folder*

Traverse subdirectories

Quarantine folder*

AFTER SUCCESSFULL IMPORTING

Move original files into a subfolder of the Import folder.

Delete original files permanently.

Under **After Successfully Importing** settings you can provide Merge1 what to do with the original files. If **Move original files into a subfolder is selected**, the files will be moved into a folder _Import inside the Import folder. If **Delete original files permanently** is selected, the files after being processed will be deleted. Note, that if deleted files can't be recovered.

Please note:

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.

* Merge1 Folder Option 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.

SOURCES



IceChat

OPTIONAL SETTINGS

- The **Auto Update** feature, when selected, automatically updates IceChat connector based on the recent changes in IceChat environment before running the import.
- When **Bloomberg Vault Format** is selected, the imported messages are displayed in Bloomberg Vault format (see the example on the next page).

- Auto Update
 Bloomberg Vault Format

MISCELLANEOUS SETTINGS

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

The **Subject Prefix** is added to the subject line of imported emails. For example, if the subject prefix "IceChat" is entered, the subject line of the message will look as in the example below. This is useful for organizing imported data, i.e. when multiple sources share a common target

Mon 1/9/2017 11:44 PM



msh9@globanet.com <msh11@globanetconsulting.com>

IceChat QARoom|2017-01-09

To msh9@globanet.com; hs@globanet.com

MISC SETTINGS

Files to import: e.g.: *.txt|*.xml (separated by vertical bars)*

Subject prefix

SOURCES



IceChat

Example of standard processed message from IceChat:

Wed 10/5/2016 8:33 PM

gs@globanet.com <gs1@globanetconsulting.com>
IceChat QARoom 2016-10-05

To gs@globanet.com; systemAlerts@globanet.com

[2016-10-05 20:33:22]: [gs@globanet.com](#) [gs1@globanetconsulting.com](#) joined conversation.
[2016-10-05 20:33:22]: [systemAlerts@globanet.com](#) joined conversation.

[2016-10-05 20:33:22]: [systemAlerts@globanet.com](#) : ICE Chat account msh9 has requested to add you as a contact. To accept the request visit the Incoming Requests group in your Contact List

[2016-10-05 20:33:22]: [gs@globanet.com](#) left conversation.
[2016-10-05 20:33:22]: [systemAlerts@globanet.com](#) left conversation.

Example of a processed message in Bloomberg Vault Format:

Wed 10/5/2016 8:33 PM

gs@globanet.com <gs1@globanetconsulting.com>
IceChat QARoom 2016-10-05

To gs@globanet.com; systemAlerts@globanet.com

<?xml version="1.0"?><chatTranscript><sessionId>0</sessionId><startTime>2016-10-05T20:33:22+04:00</startTime><endTime>2018-11-12T14:44:58+04:00</endTime><participants><buddyName>gs@globanet.com</buddyName><networkName>IceChat</networkName><email>gs@globanetconsulting.com</email><displayName>gs@globanet.com</displayName></participants><participants><buddyName>systemAlerts@globanet.com</buddyName><networkName>IceChat</networkName><email>systemAlerts@globanet.com</email><displayName>systemAlerts@globanet.com</displayName></participants><events><sequenceNumber>0</sequenceNumber><eventType>enter</eventType><eventOwner><buddyName>gs@globanet.com</buddyName><networkName>IceChat</networkName><email>gs@globanetconsulting.com</email><displayName>gs@globanet.com</displayName></eventOwner><eventTime>2016-10-05T20:33:22+04:00</eventTime></events><events><sequenceNumber>0</sequenceNumber><eventType>leave</eventType><eventOwner><buddyName>gs@globanet.com</buddyName><networkName>IceChat</networkName><email>gs@globanetconsulting.com</email><displayName>gs@globanet.com</displayName></eventOwner><eventTime>2016-10-05T20:33:22+04:00</eventTime></events><events><sequenceNumber>0</sequenceNumber><eventType>leave</eventType><eventOwner><buddyName>systemAlerts@globanet.com</buddyName><networkName>IceChat</networkName><email>systemAlerts@globanet.com</email><displayName>systemAlerts@globanet.com</displayName></eventOwner><eventTime>2016-10-05T20:33:22+04:00</eventTime></events><events><sequenceNumber>0</sequenceNumber><eventType>post</eventType><eventOwner><buddyName>systemAlerts@globanet.com</buddyName><networkName>IceChat</networkName><email>systemAlerts@globanet.com</email><displayName>systemAlerts@globanet.com</displayName></eventOwner><eventTime>2016-10-05T20:33:22+04:00</eventTime></events><content><contentType>text_plain</contentType><content>ICE Chat account msh9 has requested to add you as a contact. To accept the request visit the Incoming Requests group in your Contact List</content></content></events><serverName>GeneratedIceChat_2016</serverName><messageSize>274</messageSize><documentType>im</documentType></chatTranscript>

NEXT STEPS

After setting up the connector follow the appropriate links below to continue with the configuration of the Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users is not applicable.
- Filters
- Targets
- Importer Settings

ONEDRIVE FOR BUSINESS



OneDrive
for Business

ABOUT ONEDRIVE FOR BUSINESS

OneDrive is a file-hosting service operated by Microsoft as part of its suite of online services. It allows users to store files as well as other personal data like Windows settings or BitLocker recovery keys in the cloud. OneDrive connector's features include Monitored Users management, it's possible to specify which users' Microsoft OneDrive accounts should be captured. Microsoft OneDrive source data is retrieved via API and each time is downloaded one time per modification.

OneDrive metadata is used to create Merge1 email file. The metadata includes document creator (author in the Merge1 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
- Move to events with the file
- Copy to events with the file
- Copy link with the file
- Share link with the file
- Delete event without the file
- New created documents via browser with the file

SOURCES



OneDrive
for Business

MICROSOFT AZURE APP CREATION

1. Create an O365 account.
2. Open the **Azure Portal** (<https://portal.azure.com/>) using the same credentials as for O365 (Global Admin).
3. Navigate to **Azure Active Directory** icon on the left-hand toolbar.

The screenshot shows the Microsoft Azure portal interface. On the left, there is a dark sidebar with various service icons and names. One of the icons is 'Azure Active Directory', which is highlighted with a red arrow pointing towards it. The main content area is titled 'Панель мониторинга' (Monitoring Dashboard) and displays a message: 'All resources All subscriptions' and 'No resources to display'. It also features a 'Create DevOps Project' button and sections for 'Quickstarts + tutorials', 'Windows Virtual Machines', 'Linux Virtual Machines', and 'App Service'.

4. Click on the **App Registration**.

The screenshot shows the 'Globanet - Overview' page within the Azure Active Directory section. The left sidebar is identical to the previous screenshot. The main content area has a header 'Home > Globanet - Overview' and 'Globanet - Overview' under 'Azure Active Directory'. Below this, there is a search bar and a navigation menu with several items: 'Overview', 'Getting started', 'Manage', 'Users', 'Groups', 'Organizational relationships', 'Roles and administrators', 'Enterprise applications', 'Devices', 'App registrations', 'Application proxy', 'Licenses', and 'Azure AD Connect'. The 'App registrations' item is highlighted with a red arrow.

SOURCES



OneDrive
for Business

5. Click on the **+ New Registration** button.

The screenshot shows the 'Globanet - App registrations' page in the Azure Active Directory. A red arrow points to the '+ New registration' button in the top navigation bar. The page includes a search bar, navigation links for Overview, Getting started, Manage (Users, Groups, Organizational relationships), and tabs for All applications and Owned applications. A note at the top right mentions the transition from Legacy App registrations.

6. Enter a **Name** for the application, select "**Web**" under Redirect URI(optional), and enter the URL of your local Merge1 environment with the following extension: **"/Configuration/OAuthCallback"**. Then click on the **Register** button.

The screenshot shows the 'Register an application' form. It includes fields for Name (Sample Application), Supported account types (Accounts in this organizational directory only (Globanet)), Redirect URI (optional) (Web, https://globanetlabs.com/Configuration/OAuthCallback), and a checkbox for Microsoft Platform Policies. A red arrow points to the 'Register' button at the bottom left.

7. Find your **Application (client) ID**. Make a note of the Application (client) ID, this is needed for configuring the OneDrive Source in Merge1.

SOURCES



OneDrive
for Business

8. In the navigation pane to the left go to **Certificates & secrets**.

The screenshot shows the 'Sample Application' page in the Azure portal. On the left, the navigation pane lists several sections: Overview, Quickstart, Manage (Branding, Authentication, Certificates & secrets, API permissions, Expose an API, Owners, Manifest), Support + Troubleshooting (Troubleshooting, New support request), and Call APIs. A red arrow points from the text in step 8 to the 'Certificates & secrets' link in the Manage section. The main content area displays basic application details: Display name (Sample Application), Application (client) ID, Directory (tenant) ID, and Object ID. Below this is a welcome message and a 'View API Permissions' button.

9. Click on **New client secret**, enter a Description, specify a **Duration** and click **Add**.

Make a note of the new client secret value, this is needed for configuring the OneDrive for Business Source in Merge1.

The screenshot shows the 'Certificates & secrets' sub-page for the 'Sample Application'. The left sidebar has the same navigation as the previous screenshot. The main area shows a form to add a new client secret: 'Description' (Secret), 'Expires' (radio buttons for 'In 1 year', 'In 2 years', and 'Never' - the latter is selected), and two buttons: 'Add' (highlighted with a red arrow) and 'Cancel'. Below this is a table titled 'Client secrets' with one row: '+ New client secret'. A red arrow points from the text in step 9 to the '+ New client secret' button. The table also includes columns for 'DESCRIPTION', 'EXPIRES', and 'VALUE'.

SOURCES



OneDrive
for Business

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

The screenshot shows the 'Certificates & secrets' blade for a sample application. The left sidebar has 'API permissions' selected. The main area displays sections for 'Certificates' and 'Client secrets'. A red arrow points to the 'API permissions' link in the sidebar.

11. Click on Microsoft Graph, in the opened pane select **Application permissions**.

The screenshot shows the 'Request API permissions' pane. The left sidebar has 'API permissions' selected. The main area shows two sections: 'Delegated permissions' and 'Application permissions'. A red arrow points to the 'Application permissions' section, which is described as running as a background service or daemon without a signed-in user. The 'Select permissions' section lists various Microsoft Graph permissions, and the 'ADMIN CONSENT REQUIRED' column is shown for some of them.

SOURCES



OneDrive
for Business

Grant the following permissions:

- **Files:** Files.Read.All
- **Directory:** Directory.Read.All
- **User:** User.Read.All
- **Applications:** Applications.Read.All
- **Applications:** Applications.ReadWrite.All*

Once you have selected all three checkboxes, click **Update Permissions**.

The screenshot shows the 'Request API permissions' dialog for a sample application. On the left, there's a sidebar with navigation links like Overview, Quickstart, Manage, Support + Troubleshooting, and Troubleshooting. The main area is titled 'Sample Application - API permissions' and shows the 'API permissions' section. It lists 'API / PERMISSIONS NAME' and 'DESCRIPTION'. Under 'Microsoft Graph (1)', it shows 'Domain', 'EduAdministration', 'EduAssignments', 'EduRoster', and 'Files (1)'. In 'Files (1)', there are two permissions: 'Files.Read.All' (checked) and 'Files.ReadWrite.All' (unchecked). A red arrow points from the bottom of the sidebar towards the 'Update permissions' button at the bottom right of the dialog.

* Only required if the certificate has not been already uploaded to the Azure App.
Check Appendix for certificate management.

SOURCES



OneDrive
for Business

12. Get back to API permissions section, click **+ Add a permission** and select **Sharepoint API with Application permissions**. These are the permissions you need to grant:

- **Sites**: Sites.FullControl.All; Sites.Read.All
- **User**: User.Read.All
- **TermStore**: TermStore.Read.All

Once you have selected all three checkboxes, click **Update Permissions**.

The screenshot shows the 'Request API permissions' dialog in the Microsoft Azure portal. On the left, the navigation menu includes 'Overview', 'Quickstart', 'Manage' (with 'Branding', 'Authentication', 'Certificates & secrets', 'API permissions' selected), 'Expose an API', 'Owners', 'Manifest', 'Support + Troubleshooting', and 'New support request'. The main area displays the 'Request API permissions' dialog for a SharePoint application named 'https://microsoft.sharepoint-df.com/ Docs'. It shows a warning about SharePoint APIs being available via Microsoft Graph instead. It asks 'What type of permissions does your application require?' with options for 'Delegated permissions' (selected) and 'Application permissions' (highlighted with a red arrow). Below, under 'Select permissions', there's a search bar and a table of permissions grouped by category. The 'Sites' category is expanded, showing two permissions: 'Sites.FullControl.All' (checked) and 'Sites.ReadAll' (checked). Both have 'Yes' under 'ADMIN CONSENT REQUIRED'. At the bottom are 'Add permissions' and 'Discard' buttons.

SOURCES



OneDrive
for Business

SETTING UP THE CONNECTOR IN MERGE1

1. Open **Merge1 Configuration** section, click **Add Importer**, specify **Name** for the new importer and click **Next** (**Description** is optional).

The screenshot shows the 'CONFIGURATION' section of the Merge1 interface. A red arrow points to the 'ADD IMPORTER' button. A modal window titled 'CONFIGURATION WIZARD' is open, showing the 'ADD IMPORTER' step. It has two input fields: 'Name' (set to 'Importer') and 'Description' (set to 'Importers'). A 'NEXT' button is at the bottom right of the modal.

2. Select **OneDrive for Business** and click **Next**.

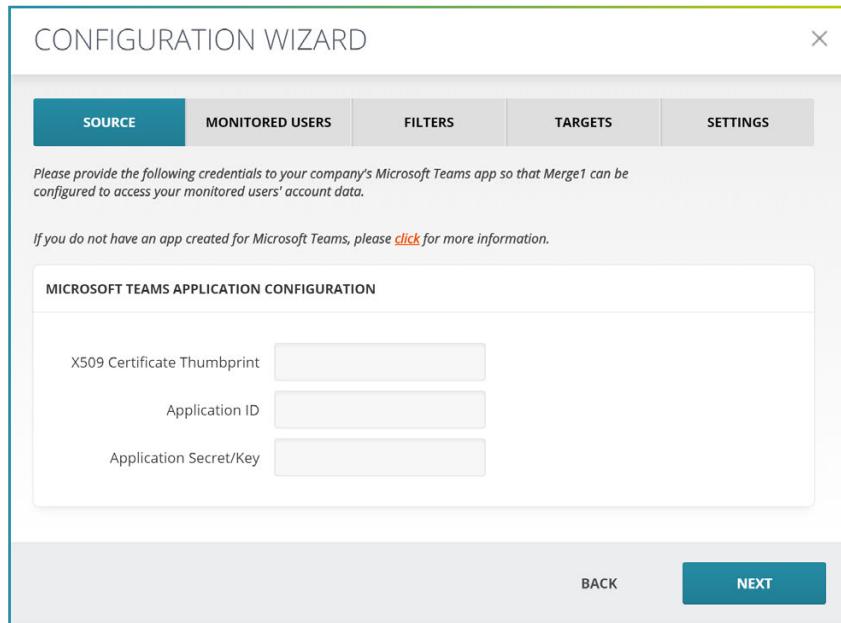
The screenshot shows the 'CONFIGURATION WIZARD' with the heading 'Please select your source by clicking on the icon below.' A red arrow points to the 'OneDrive for Business' icon in the grid of available sources. Another red arrow points to the 'NEXT' button at the bottom right of the wizard.

SOURCES



OneDrive
for Business

3. In the new window you need to add **X509 Certificate Thumbprint**, **Application ID**, and **Application Secret/Key**.



- 4.1 To get the **Certificate Thumbprint** open the PowerShell on the Merge1 server and use the **Get-ChildItem -path cert:\LocalMachine\My** command (please note that as a result you can have more than one thumbprint, therefore, you should use the thumbprint of the Self-Signed Certificate that you have used during Merge1 installation).

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32> Get-ChildItem -path cert:\LocalMachine\My

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

Thumbprint                               Subject
-----                               -----
5095E64932B0F8D073C1B34D426EC5C37486324E CN=WMSvc-SHA2-DESKTOP-DR3LPRO
35B0BDD6CA12AD86D316691C78ED034C96CFFCD8 CN=DESKTOP-DR3LPRO

PS C:\WINDOWS\system32>
```

SOURCES



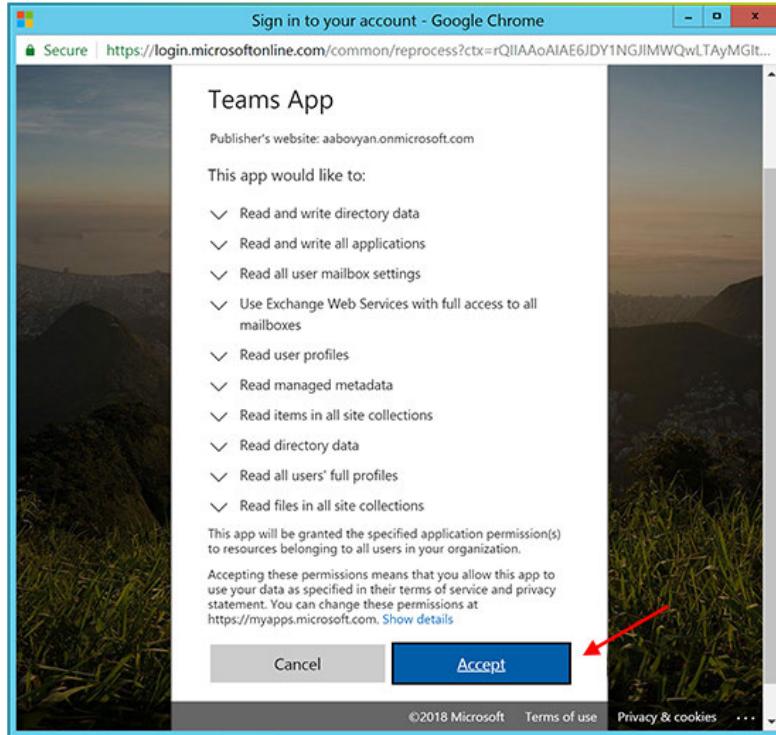
OneDrive
for Business

- 4.2 You can copy the **Application ID** from the Azure Active Directory -> App Registrations -> <your app name> section.

The screenshot shows the 'Globanet - App registrations' page in the Azure portal. On the left, there's a sidebar with 'Overview', 'Getting started', 'Manage' (selected), 'Users', 'Groups', 'Organizational relationships', 'Roles and administrators', 'Enterprise applications', 'Devices', and 'App registrations'. The main area has tabs for 'New application registration', 'Endpoints', and 'Troubleshoot'. A search bar at the top says 'Search by name or AppID' and dropdowns show 'My apps'. Below is a table with columns 'DISPLAY NAME', 'APPLICATION TYPE', and 'APPLICATION ID'. One row is shown for 'Globanet' (Web app / API) with the Application ID highlighted in red: `f2832761-307e-445c-adb3-b12b2aa2f262`.

- 4.3 Refer to Point 14 in the Microsoft Azure App Creation section. Enter the **Application Secret/Key** that you have saved before.

5. After clicking **Next** a pop-up window should appear where you should provide the O365 Global Admin user credentials (please note that usually the pop-up is being blocked by the browser so pay attention to the top right corner of the browser if the popup is not appearing). In the next window click **Accept** to grant the permissions.



SOURCES



OneDrive
for Business

ADDITIONAL CONFIGURATION

- With the **Do not download files greater than X megabyte(s)** option the size of the files that should be downloaded can be specified. For example, if the size is set to 10 MB, files that are greater than 10MB won't be downloaded.
- The "**Do not download data modified before**" check will ensure that old or irrelevant data is excluded. For example, if the date selected is 9/1/2017, it won't retrieve any data modified before September 1 of 2017. Only the data after 9/1/2017 will be retrieved, archived, and imported.

A screenshot of a configuration interface. At the top, it says "MAXIMUM FILE SIZE TO BE DOWNLOADED". Below that is a checkbox labeled "Do not download files greater than" followed by a text input field containing "megabyte(s)". Underneath this is a section titled "ADVANCED CONFIGURATION OPTIONS" which contains another checkbox labeled "Do not download data modified before:" followed by a date picker button.

Example output message:

A screenshot of an email message from Michael Smith. The message header shows "Fri 5/25/2018 11:55 AM" and the recipient as Michael Smith <Michael@example.com>. The subject is "Quick Notes.one (UPLOAD MODIFIED)". The message body includes a file attachment named "Quick Notes.one" (132 KB). Below the attachment, there is a detailed file information block:
File size: 134330 bytes
Folder path: root//Notebooks/Michael @ Work File Url: https://exampleservices-my.sharepoint.com/personal/michael_example_com/_layouts/15/WopiFrame.aspx?sourcedoc=%7BE694F6AB-C2DC-40E8-B749-5001BD8A4B94%7D&file=Quick%20Notes.one&action=default&wdorigin=sharepoint
File ID: 01L6DTP2VL62KONXGC5BALOSKQAG6YUS4U

NEXT STEPS

After setting up the connector follow the appropriate links below to continue with the configuration of the Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users (preferred option for Cisco Webex Teams is **All (Based on Native API)**, the users will be retrieved automatically)
- Filters
- Targets
- Importer Settings

CROWD COMPASS



Crowd Compass

ABOUT CROWD COMPASS CONNECTOR

CrowdCompass creates custom-branded mobile event apps for coming events or conferences. Event managers can communicate with Attendees.

Merge1 captures data from the Crowd Compass using an API. The connection is established using an Access Token. The access token provided by Crowd Compass support corresponds to an Event Center user. The token will be able to access any event that the user does.

So, for example, if you are an event admin for the Sandbox event only, and can't see any other events in the account, your access token will not be able to make API calls to the other events in the account.

ACTIVITIES CAPTURED

- From details
- To details
- Invitations
- Event IDs
- Messages

SOURCES



RETRIEVING ACCESS TOKEN

Contact Crowd Compass Support to request an Access Token for your organization's Crowd Compass environment.

Crowd Compass

CONFIGURING CROWD COMPASS CONNECTOR

Fill in the Access-Token for your Crowd Compass environment.

CROWD COMPASS CONFIGURATION

Access-Token

ADVANCED CONFIGURATION OPTIONS

- The **Auto Update** feature will ensure that the connector is updated to the latest version. Each time the Importer is run, it contacts Globanet server(s) and updates the connector if a newer version is available.
- 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.
- The "**Do not download data modified before**" check will ensure that old or irrelevant data is excluded. For example, if the date selected is 9/1/2017, it won't retrieve any data modified before September 1 of 2017. Only the data after 9/1/2017 will be retrieved, archived, and imported.

ADVANCED CONFIGURATION OPTIONS

Auto Update

Subject Prefix

Do not download data modified before:



SOURCES



Crowd Compass

Example of Login activity message:

Thu 10/18/2018 5:10 PM

 support@example.com

Meeting Invite Event - 2018 Conference

To: jane doe

```
created_at: 2018-10-18T13:09:31Z
email: jane.doe@example.com
first_name: jane
last_name: doe
suffix:
status: delivered
delivery_requested: False
delivery_requested_at:
registration_code: JZNHD6WPX7V
oid: vCZ16UmgKF
ref: 78EF0A97-4188-4777-BED3-16E225CD6885
source: CORE
source_url:
job_title: Vice President
organization_name: Example
bio:
address_street_1:
address_street_2:
address_city:
address_state:
address_zipcode:
address_country:
phone_work: 412-234-8960
phone_mobile: 724-678-9936
website:
website_2:
linkedin_url:
twitter_url:
facebook_url:
show_email_in_profile: true
visible_on_attendee_list: true
phone_other_type:
phone_other:
is_moderator: false
delivered_at: 2018-10-31T21:15:38Z
remote_avatar_url:
ident: 84ad828a-0ab2-4e6b-8fb2-abebed586966
```

NEXT STEPS

After setting up the connector, follow the appropriate links below to continue with the configuration of the Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users
- Filters (Crowd Compass works with all filters except **XML Filter**)
- Targets
- Importer Settings

CITRIX WORKSPACE & SHAREFILE



Citrix Workspace &
ShareFile

ABOUT CITRIX WORKSPACE & SHAREFILE CONNECTOR

Citrix Workspace & ShareFile provides secure file sharing, storage, sync and more – all built for business.

Merge1 Citrix Workspace & ShareFile connector does not capture ShareFile activities for clients. The connector requires a service account to create the API. The Service account content will not be captured.

ACTIVITIES CAPTURED

- File upload
- File download
- File delete
- File move
- File share
- Folder create
- Folder delete
- Check in /Check out
- Login info
- File Share (Public/Private)
- Private Messages
- file_Comment (Public/Private)
- channel_join (Public/Private)
- message_deleted (Public/Private)
- channel_purpose (Public/Private)

SOURCES



Citrix Workspace &
ShareFile

CITRIX WORKSPACE & SHAREFILE APP CREATION

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 on **Get an API Key**.

Welcome to the ShareFile API

Integrate with other services and build tools and applications on top of ShareFile

Get an API Key A red arrow points to this button.

Browse the documentation

Get Help

Get started right away - request your API key.

Learn how the API works and what it can do.

Stuck somewhere? Check out our developers' forum.

4. Fill in the **Application Name**.
5. In the Redirect URI field add the URL of your local Merge1 environment with the following extension:
https://<your_merge1_domain>/Configuration/OAuthCallback
6. Click Generate API Key.

API Key Generator

Application Name*
Do not include "ShareFile" or any other Citrix product name

Description

Redirect URI (with an https:// protocol)
Note: The redirect URI provided should match exactly what is sent as part of the authorization flow, including host, port, path, and query.

I don't know or will not use a Redirect URI

Generate API Key By Submitting this form you agree to the [ShareFile API Terms of Service](#).

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

Your API Keys

Application	Client Id	Client Secret	Redirect URI
Merge1 Example	uYdmg2Q7N7UzHm2XJpyUrmv9dXx2VRoG	ZE3KfjJIW6eF0PwhTYr2XocXDHEQC1XECvxdMrn7ASJIPzT	https://globanetlabs.com/Configuration/OAuthCallback

SOURCES



Citrix Workspace &
ShareFile

CONFIGURING CITRIX WORKSPACE & SHAREFILE CONNECTOR

1. In the **Application ID** field copy the Client Id.
2. In the **Application Secret/Key** field copy the Client Secret.
3. Add subdomain of the Sharefile workspace into the **SubDomain** field.
(Subdomain is located under admin settings> Company info > Edit company Branding)

The screenshot shows a 'EDIT CONNECTOR' dialog box. At the top, there are tabs: SOURCE (which is selected), MONITORED USERS, FILTERS, TARGETS, and SETTINGS. Below the tabs, there is a note: 'Please provide the following credentials to your company's Citrix Workspace & ShareFile app so that Merge1 can be configured to access your monitored users' account data.' Another note below it says: 'If you do not have an app created for Citrix Workspace & ShareFile, please [click](#) for more information.' The main section is titled 'CITRIX WORKSPACE & SHAREFILE APPLICATION CONFIGURATION' and contains three input fields: 'Application ID' (empty), 'Application Secret/Key' (empty), and 'SubDomain' (empty). At the bottom right of the dialog is a blue 'NEXT' button.

4. In the popped up window 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.

The screenshot shows a ShareFile login page. At the top, the ShareFile logo is displayed. Below it, a message reads: 'Globanet Consulting Services Merge1 Example has requested access to your ShareFile account.' There are two input fields: 'Email' and 'Password' (with dots showing the length). Below these is a large blue 'Sign In' button. At the bottom of the page, there are links: 'Log in with my company credentials', 'Forgot Password?', and 'Privacy Policy'. The Citrix logo is at the very bottom center.

SOURCES



Citrix Workspace &
ShareFile

ACTIVITIES TO BE CAPTURED

It's possible to choose which activities Merge1 processes from Citrix Workspace & ShareFile.

- Archive only ShareFile Shared Items. Only shared items are imported.
- Archive all activity in Sharefile. All activities are captured and imported.
- Archive only a certain selection of activity in ShareFile. Activities to be captured and imported can be selected separately.

ACTIVITIES TO BE PROCESSED

ACTIVITIES

Archive only ShareFile Shared Items
 Archive all activity in ShareFile
 Archive only a certain selection of activity in ShareFile

Upload
 Download/View
 Folder create
 Check In/Check Out
 Delete/Archive
 Login
 Move
 File share

ADVANCED CONFIGURATION 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 04/17/2016 and the After is set to 08/25/2018 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.

ADVANCED CONFIGURATION OPTIONS

Subject Prefix

Do not download data modified before:

Do not download data modified after:

SOURCES



Citrix Workspace &
ShareFile

Example of Login activity message:

Fri 11/16/2018 5:55 PM

Product example <product@example.com>
Citrix - Login | product@example.com ShareFile AP...

To

Date: 11/16/2018 8:54:32 AM
ItemName: [product@example.com](#) ShareFile API Documentation
Activity: Login
User: Product example
Email: [product@example.com](#)
Company:
IPAddress: 212.42.198.68
Location: US, Ashburn, Virginia
EventID: 0baf2444-e55a-47cf-8fdf-02c47e339526
ReportType: Activity
EventDate: 11/16/2018 5:54:32 PM
EventType: Login

Example of Upload activity message:

Wed 9/26/2018 4:41 PM

Product example <product@example.com>
Citrix - Upload | /product@example.com/Workflows/...

To

 .pdf 125 KB

Date: 9/26/2018 8:41:21 AM
ItemName: [/product@example.com/Workflows/Cisco_IMP_ExtDB_WP.pdf](#)
Activity: Upload
User: Product example
Email: [product@example.com](#)
Company:
IPAddress: 35.153.16.199
Location: US, Ashburn, Virginia
EventID: fi9725c5-258c-f93f-d317-38572ab81f9e
ReportType: Activity
EventDate: 9/26/2018 4:41:21 PM
EventType: Upload

SOURCES



Citrix Workspace &
ShareFile

Example of Create Folder activity message:

Mon 10/8/2018 10:28 AM

JD John Doe <jdoe@example.com>
Citrix - Create Folder | /jdoe@example...

To

Creator: jdoe@example.com
Date: 10/8/2018 2:27:49 AM
ItemName: [/jdoe@example.com](#)
Activity: Create Folder
User: Steve Deguir
Email: jdoe@example.com
Company: example
IPAddress: 212.42.198.68
Location: US, Ashburn, Virginia
EventID: fohc4b45-8499-485b-a8d1-dca4dd4ed54b
ReportType: Activity
EventDate: 10/8/2018 10:27:49 AM
EventType: CreateFolder
===== Additional Info =====
Creator: jdoe@example.com | John Doe
CreationDate: 10/8/2018 10:27:54 AM
ExpirationDate: 12/31/9999 11:59:59 PM

Example of Upload activity message:

Wed 9/26/2018 9:36 PM

PE Product example <product@example.com>
Citrix - Download | /jdoe@example.com/Log...

To

LogFile to Send.txt
12 KB

Date: 9/26/2018 1:35:43 PM
ItemName: [/jdoe@example.com/LogFile](#) to Send.txt
Activity: Download
User: Product example
Email: product@example.com
Company:
IPAddress: 212.42.198.68
Location: US, Ashburn, Virginia
EventID: fi9dfbd9f-796f-da17-c21e-cd4768970e60
ReportType: Activity
EventDate: 9/26/2018 9:35:43 PM
EventType: Download

SOURCES



Citrix Workspace &
ShareFile

EXCLUDE FILES

- 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 this 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 shouldn't be downloaded can be specified in the following format: ex. *.txt | *.xml. The vertical bar is used to separate the file types.

The screenshot shows the 'EXCLUDE FILES' configuration screen. It includes fields for specifying file size limits and file types, along with examples of how these settings will appear in the email body.

EXCLUDE FILES	
<input type="checkbox"/> Do not download files greater than	megabyte(s).
Custom Message	This message will be inserted at the beginning of the email body text. example: Files {0} are not imported, because they are greater than {1} megabyte All the filenames that were excluded will be written instead of {0} symbol. File size limit will be written instead of {1} symbol.
File Types	
Custom Message	This message will be inserted at the beginning of the email body text. example: Files {0} are not imported. All the filenames that were excluded will be written instead of {0} symbol.

NEXT STEPS

After setting up the Source follow the appropriate links below to continue with the configuration of the Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users (preferred option for Citrix Workspace &ShareFile is **All (Based on Native API)**, the users will be retrieved automatically)
- Filters (Citrix Workspace &ShareFile works with all filters except **XML Filter**)
- Targets
- Importer Settings

MICROSOFT TEAMS



Microsoft Teams

ABOUT MICROSOFT TEAMS CONNECTOR

Microsoft Teams is a chat-based workspace in Office 365 that integrates with the apps and services teams use to get work done together. The Microsoft Teams developer platform makes it easy for you to integrate your service, whether you develop custom apps for your enterprise or SaaS applications for teams around the world.

Microsoft Teams provides the enterprise security and compliance features you expect from Office 365, including broad support for compliance standards, and eDiscovery and legal hold for channels, chats, and files. Tooltip about the availability of legal features Microsoft Teams encrypts data at all times, at-rest and in-transit, and includes multi-factor authentication to enhance identity protection.

ACTIVITIES CAPTURED

- One-on-one Chats*
- Group Conversations*
- Private & Public channel communications
- Private channel edits and deletes**
- Files shared by third-party integration
- Apps and bots
- Combines chats into easy to read threads
- Archives attachments
- Messages generated by third party integration apps and bots
- Files shared by third-party integration apps and bots
- Combines chats into easy-to-read threads
- Archives attachments
- Preserves metadata, original message time, and other data for accurate search and retrieval during eDiscovery
- Mentions (only the latest version)

* Hybrid and on-prem environments are not supported

** Edits and deletes of messages in chats and public channels are not captured

SOURCES



Microsoft Teams

IMPORTANT INFORMATION



Each team in Microsoft Teams has a team site in SharePoint Online, and each channel in a team gets a folder within the default team site document library. Files shared within a conversation are automatically added to the document library, and permissions and file security options set in SharePoint are automatically reflected within Teams+.

Private chat files are stored in the sender's OneDrive for the Business folder, and permissions are automatically granted to all participants as part of the file-sharing process.

If you don't have SharePoint Online enabled in your tenant, Microsoft Teams' users can't share files in teams. Users in private chat also can't share files because OneDrive for Business (which is tied to the SharePoint license) is required for that functionality.

By storing the files in the SharePoint Online document library and OneDrive for Business, all compliance rules configured at the tenant level will be followed.

You can use a retention policy to retain chats and channel messages in Teams. Teams chats are stored in a hidden folder in the mailbox of each user included in the chat, and Teams channel messages are stored in a similar hidden folder in the group mailbox for the team. However, it's important to understand that Teams uses an Azure-powered chat service that also stores this data, and by default, this service stores the data forever. For this reason, we strongly recommend that you use the Teams location to retain and delete Teams data. Using the Teams location will permanently delete data from both the Exchange mailboxes and the underlying Azure-powered chat service. For more information, see more here: <https://docs.microsoft.com/en-us/MicrosoftTeams/security-compliance-overview>

Note that Teams chats and channel messages are not affected by retention policies applied to the user or group mailboxes in the Exchange or Office 365 groups locations. Even though Teams chats and channel messages are stored in Exchange, they're affected only by a retention policy that's applied to the Teams location

Please see more on retention policy here: <https://docs.microsoft.com/en-us/office365/security-compliance/retention-policies>

Please note:

If a message is deleted and then the deletion was undone, all the other actions done on that message won't be captured due to the fact that the message is absent from the mailbox.

SOURCES



Microsoft Teams

MICROSOFT AZURE APP CREATION

1. Create an O365 account.
2. Open the **Azure Portal** (<https://portal.azure.com/>) using the same credentials as for O365 (Global Admin).
3. Navigate to **Azure Active Directory** icon on the left-hand toolbar.

The screenshot shows the Microsoft Azure portal's main dashboard. On the left, there's a sidebar with various service icons like App Services, Function Apps, and Storage accounts. At the bottom of this sidebar, the 'Azure Active Directory' icon is highlighted with a red arrow. The main central area shows a message 'No resources to display' and a 'Create resources' button. To the right, there's a promotional section for 'Azure getting started made easy!' featuring 'Create DevOps Project' and several quickstart options: Windows Virtual Machines, Linux Virtual Machines, and App Service.

4. Click on the **App Registration**.

This screenshot shows the 'Globanet - Overview' page within the Azure Active Directory section. The left sidebar remains the same as the previous screenshot. In the main content area, under the 'Manage' heading, there's a list of items: Users, Groups, Organizational relationships, Roles and administrators, Enterprise applications, Devices, Application proxy, Licenses, and 'App registrations'. The 'App registrations' link is also highlighted with a red arrow.

SOURCES



Microsoft Teams

5. Click on **+ New Registration** button.

The screenshot shows the 'Globanet - App registrations' page in the Azure Active Directory. The top navigation bar includes a search bar, a back arrow, and links for 'New registration', 'Endpoints', 'Troubleshooting', and 'Feedback'. Below the bar, a welcome message is displayed, followed by a note about learning how it's changed from App registrations (Legacy). The main area shows tabs for 'All applications' and 'Owned applications', with a search bar below them. On the left, a sidebar titled 'Manage' lists 'Overview', 'Getting started', 'Users', 'Groups', and 'Organizational relationships'.

6. Enter a **Name** for the application, select "**Web**" under Redirect URI(optional), and enter the URL of your local Merge1 environment with the following extension: **"/Configuration/OAuthCallback"**. Then click on the **Register** button.

The screenshot shows the 'Register an application' form. It starts with a field for the '*** Name**' (display name) containing 'Sample Application'. Below that is a section for '**Supported account types**' with three options: 'Accounts in this organizational directory only (Globanet)' (selected), 'Accounts in any organizational directory', and 'Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)'. There is also a 'Help me choose...' link. The next section is '**Redirect URI (optional)**' with a dropdown set to 'Web' and a text input field containing 'https://globanetlabs.com/Configuration/OAuthCallback'. At the bottom, there is a link 'By proceeding, you agree to the Microsoft Platform Policies' and a blue '**Register**' button.

7. Find your **Application (client) ID**. Make a note of the Application (client) ID, this is needed for configuring the Microsoft Teams Source in Merge1.

SOURCES



Microsoft Teams

8. In the navigation pane to the left go to **Certificates & secrets**.

The screenshot shows the Microsoft App registrations interface for a 'Sample Application'. The left sidebar has 'Certificates & secrets' selected. A red arrow points to this selection. The main area displays basic application details like Display name, Application (client) ID, and Directory (tenant) ID. Below this is a welcome message and a 'Call APIs' section with various service icons. At the bottom is a 'View API Permissions' button.

9. Click on **New client secret**, enter a Description, specify a **Duration** and click **Add**.

Make a note of the new client secret value, this is needed for configuring the Microsoft Teams Source in Merge1.

The screenshot shows the 'Certificates & secrets' creation dialog for the 'Sample Application'. It includes fields for 'Description' (set to 'Secret'), 'Expires' (set to 'Never'), and two 'Add' and 'Cancel' buttons. A red arrow points to the 'Add' button. Below this is a 'Client secrets' table with a 'New client secret' button. Another red arrow points to this button. The table currently shows 'No client secrets have been created for this application.'

SOURCES



Microsoft Teams

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

The screenshot shows the 'Certificates & secrets' section of the Microsoft Teams API permissions page. The left sidebar has 'API permissions' selected. The main area shows a message about client secrets and a table for certificates. A red arrow points to the 'API permissions' link in the sidebar.

11. Click on Microsoft Graph, in the opened pane select **Application permissions**.

The screenshot shows the 'Application permissions' section of the Microsoft Graph API permissions page. The left sidebar has 'API permissions' selected. The main area shows two sections: 'Delegated permissions' and 'Application permissions'. A red arrow points to the 'Application permissions' section. Below it, a table lists various permissions with checkboxes for 'ADMIN CONSENT REQUIRED'.

Grant the following permissions:

- **Files:** Files.Read.All
- **Directory:** Directory.Read.All
- **User:** User.Read.All
- **Applications:** Applications.Read.All
- **Applications:** Applications.ReadWrite.All*

* Only required if the certificate has not been already uploaded to the Azure App.
Check Appendix for more information.

SOURCES



Microsoft Teams

Once you have selected all three checkboxes, click **Update Permissions**.

The screenshot shows the Microsoft Teams 'API permissions' section. On the left, there's a sidebar with options like Overview, Quickstart, Manage, Support + Troubleshooting, and Troubleshooting. The 'API permissions' section is selected. On the right, a 'Request API permissions' dialog is open. It lists several API permissions under 'Microsoft Graph (1)'. Under 'Files (1)', two checkboxes are checked: 'Files.Read.All' (Read files in all site collections) and 'Files.ReadWrite.All' (Read and write files in all site collections). At the bottom of the dialog, there are 'Update permissions' and 'Discard' buttons.

12. Get back to API permissions section, click **+ Add a permission** and select **Sharepoint API** with **Application permissions**. These are the permissions you need to grant:

- **Sites:** Sites.FullControl.All; Sites.Read.All
- **User:** User.Read.All
- **TermStore:** TermStore.Read.All

Once you have selected all three checkboxes, click **Update Permissions**.

The screenshot shows the Microsoft SharePoint 'API permissions' section. On the left, there's a sidebar with options like Overview, Quickstart, Manage, Support + Troubleshooting, and Troubleshooting. The 'API permissions' section is selected. On the right, a 'Request API permissions' dialog is open. It shows 'SharePoint' selected under 'All APIs'. A note says 'SharePoint APIs are available via the Microsoft Graph API. You may want to consider using Microsoft Graph instead.' Under 'Delegated permissions', it says 'Your application needs to access the API as the signed-in user.' Under 'Select permissions', there are two sections: 'PERMISSION' and 'ADMIN CONSENT REQUIRED'. The 'Sites (2)' section contains four checkboxes:

- Sites.FullControl.All (Have full control of all site collections)
- Sites.Manage.All (Read and write items and lists in all site collections)
- Sites.Read.All (Read items in all site collections)
- Sites.ReadWrite.All (Read and write items in all site collections)

At the bottom of the dialog, there are 'Add permissions' and 'Discard' buttons.

SOURCES



Microsoft Teams

13. Get back to API permissions section, click **+ Add a permission** and select **Exchange API with Application permissions**. These are the permissions that you need to grant:

- Activate **full_access_as_app**
- **MailboxSettings**: MailboxSettings.Read

Once you have selected all three checkboxes, click **Add Permissions**.

The screenshot shows the 'Request API permissions' dialog in the Microsoft Azure portal. On the left, the 'Sample Application - API permissions' blade is visible, showing various API permissions like Azure Active Directory, Microsoft Graph, and SharePoint. The 'API / PERMISSIONS NAME' dropdown is set to 'Exchange'. In the main dialog, the 'Application permissions' section is selected, and the 'full_access_as_app' checkbox is checked. At the bottom, the 'Add permissions' button is highlighted with a red arrow.

SOURCES



Microsoft Teams

SETTING UP THE CONNECTOR IN MERGE1

1. Open **Merge1 Configuration** section, click **Add Importer**, specify **Name** for the new importer and click **Next (Description** is optional).

The screenshot shows the 'CONFIGURATION' screen for Merge1. At the top left is a circular icon with a blue 'T' and a white 'i'. Below it is the text 'Microsoft Teams'. In the center, there's a 'BLOOMBERG' entry with a status of 'Stopped'. A red arrow points to the 'ADD IMPORTER' button. A modal window titled 'CONFIGURATION WIZARD' is open, showing the 'ADD IMPORTER' step. It has fields for 'Name' (set to 'Importer') and 'Description' (set to 'Importers'), with a 'NEXT' button at the bottom.

2. Select **Microsoft Teams** and click **Next**.

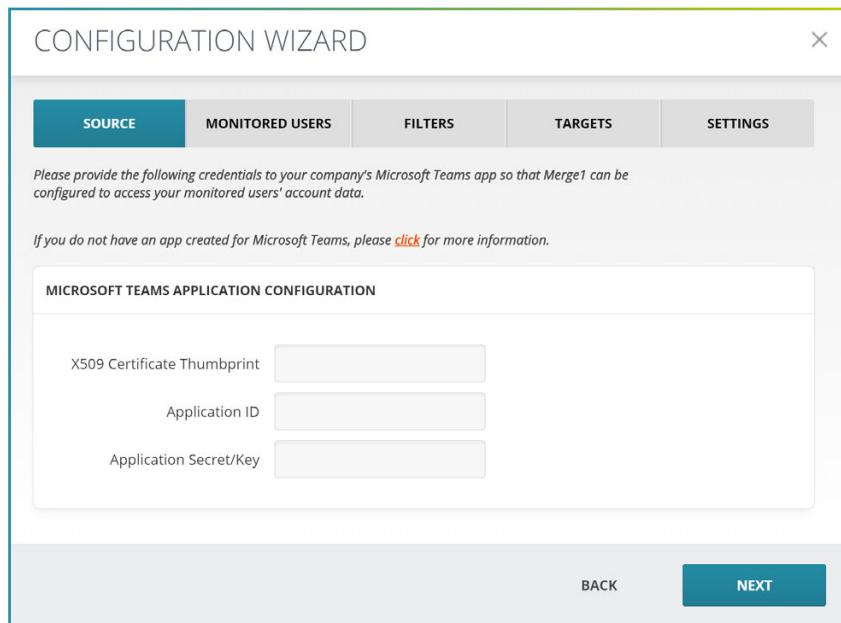
The screenshot shows the 'CONFIGURATION WIZARD' source selection screen. It displays a grid of various data sources with their icons and names. A red arrow points to the Microsoft Teams icon, which has a green checkmark next to it. Another red arrow points to the 'NEXT' button at the bottom right of the screen.

SOURCES



Microsoft Teams

3. In the new window you need to add **X509 Certificate Thumbprint**, **Application ID**, and **Application Secret/Key**.



- 4.1 To get the **Certificate Thumbprint** open the PowerShell on the Merge1 server and use the **Get-ChildItem -path cert:\LocalMachine\My** command (please note that as a result you can have more than one thumbprint, therefore, you should use the thumbprint of the Self-Signed Certificate that you have used during Merge1 installation).

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32> Get-ChildItem -path cert:\LocalMachine\My

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

Thumbprint          Subject
-----          -----
5095E64932B0F8D073C1B34D426EC5C37486324E CN=MSvc-SHA2-DESKTOP-DR3LPRO
35B0BDD6CA12AD86D316691C78ED034C96CFFCD8 CN=DESKTOP-DR3LPRO

PS C:\WINDOWS\system32>
```

SOURCES



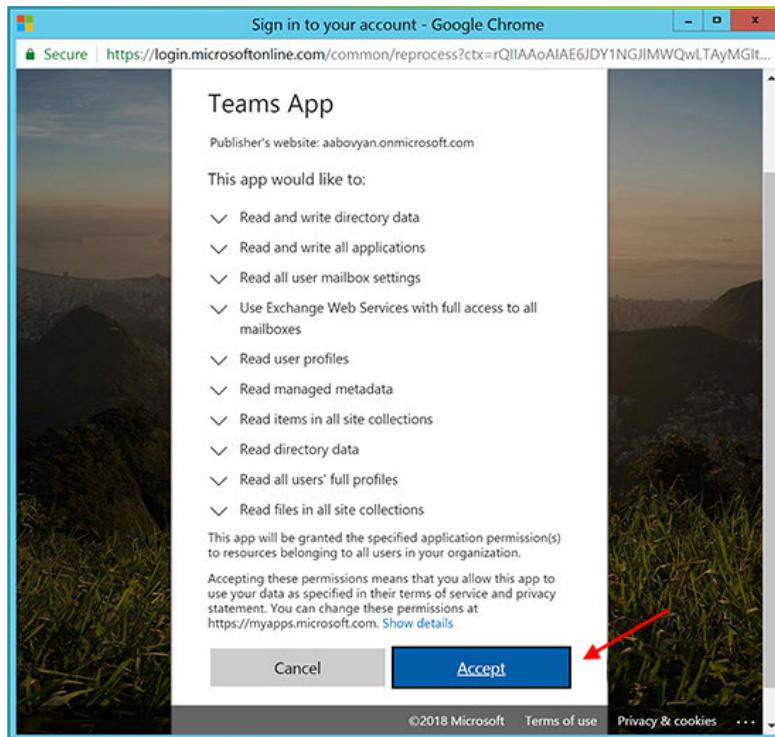
Microsoft Teams

- 4.2** You can copy the **Application ID** from the Azure Active Directory -> App Registrations -> <your app name> section.

The screenshot shows the 'App registrations' section of the Azure portal. On the left, there's a sidebar with links like Overview, Getting started, Manage (Users, Groups, etc.), and App registrations. The main area displays a table with columns: DISPLAY NAME, APPLICATION TYPE, and APPLICATION ID. A single row is shown for 'Globanet', which is a Web app / API. The APPLICATION ID column contains the value 'f2832761-307e-445c-adb3-b12b2aa2f262', which is highlighted with a red box.

- 4.3** Refer to Point 14 in Microsoft Azure App Creation section. Enter the **Application Secret/Key** that you have saved before.

- 5.** After clicking **Next** a pop-up window should appear where you should provide the O365 Global Admin user credentials (please note that usually the pop-up is being blocked by the browser so pay attention to the top right corner of the browser if the popup is not appearing). In the next window click **Accept** to grant the permissions.



SOURCES



Microsoft Teams

SETTING UP SECURITY AND COMPLIANCE FOR MICROSOFT 365

1. Navigate to <https://protection.office.com/?rfr=AdminCenter#/retention>.
2. Click **Create** to start the setup wizard.

The screenshot shows the Microsoft 365 Admin Center interface under the 'Retention' section. On the left, there's a sidebar with 'Home', 'Threat management', and 'Service assurance'. The main area has a heading 'Email, documents, Skype and Teams conversations. Your users generate a lot of content every day. Take control of it by setting up retention policies you don't.' followed by a link 'Learn more about retention'. Below this are two sections: 'Labels' and 'Label policies'. The 'Labels' section contains a description of what labels are used for (classifying and retaining content) and a 'Create' button. The 'Label policies' section contains a description of what label policies do (publishing or automatically applying labels) and a 'Create' button. At the bottom, there are filters for 'Name', 'Created by', and 'Last modified', and a message 'No data available'.

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

The screenshot shows the 'Name your policy' step of the setup wizard. On the left, there's a sidebar with steps: 'Name your policy' (selected), 'Settings', 'Choose locations', and 'Review your settings'. The main area has a heading 'Name your policy' and a 'Name *' input field with a placeholder 'Enter a friendly name'. Below it is a 'Description' input field with a placeholder 'Enter a friendly description for your policy'. At the bottom are 'Next' and 'Cancel' buttons. Red arrows point from the text 'Add a Name for the policy' in the previous slide to the 'Name' input field and the 'Description' input field.

SOURCES



Microsoft Teams

4. In 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**.

The screenshot shows the Microsoft Teams retention policy creation interface. On the left, a sidebar lists steps: 'Name your policy' (selected), 'Settings', 'Choose locations' (selected), and 'Review your settings'. The main panel title is 'Decide if you want to retain content, delete it, or both'. It asks 'Do you want to retain content?' with a radio button for 'Yes, I want to retain it'. Below it, 'Retain the content based on' is set to 'when it was created'. It also asks 'Do you want us to delete it after this time?' with a radio button for 'No'. A 'Need more options?' section includes a radio button for 'Use advanced retention settings'. At the bottom are 'Back', 'Next', and 'Cancel' buttons.

5. 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** or select **Let me choose specific locations** and apply them to specific applications. You should select the second option and activate last two options **Teams channel messages** and **Teams chats**. There is also an opportunity to choose specific **Teams/Users** or **Exclude** them.

Once you choose the locations where the retention policy applies, click "Next"

The screenshot shows the 'Choose locations' step of the retention policy creation. The sidebar shows 'Name your policy', 'Settings', 'Choose locations' (selected), and 'Review your settings'. The main panel lists application locations with toggle switches: 'Office 365 groups' (selected), 'Skype for Business', 'Exchange public folders', 'Teams channel messages' (selected), and 'Teams chats' (selected). For 'Teams channel messages', options are 'All' (selected) and 'Choose teams'. For 'Teams chats', options are 'All' (selected) and 'Choose users'. At the bottom are 'Back', 'Next', and 'Cancel' buttons.

SOURCES



Microsoft Teams

4. The next screen offers to review the settings that you have chosen.
If everything is correct click **Create this Policy**. Please note that it would take up to 1 day to apply the retention policy to the locations you chose.

Create a policy to retain what you want and get rid of what you don't.

Name your policy Microsoft Teams

Settings Retention period
Keep content for 7 years

Choose locations

Review your settings

Review your settings

It will take up to 1 day to apply the retention policy to the locations you chose.

Policy name [Edit](#)
Microsoft Teams

Description [Edit](#)

Applies to content in these locations [Edit](#)

Settings [Edit](#)

Retention period
Keep content for 7 years

Back Save for later **Create this policy** Cancel Feedback

Example output message:

Tue 9/25/2018 12:24 PM

John Doe <JDoe@example.com>

Teams Private Chat: IM

To Michael Smith

John Doe - September 25 at 12:23 PM

What is Lorem Ipsum? Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged.

MessageType: Chat Message

SOURCES



Microsoft Teams

ACTIVITIES CAPTURED

You can specify activities to capture by the connector if not events are needed. Chats are always captured, whether meetings/calls and mentioned are captured can be specified in this option.

ACTIVITIES TO CAPTURE

Capture all activities
 Capture certain activities

Chats
 Meetings / Calls
 Mentions

TIMESTAMP FORMATTING & DATETIME FORMATS

In addition to the primary stamp, a second timestamp can be enabled with its timezone. 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 Datetime Format dropdown menu.

TIMESTAMP FORMATTING

Primary Time Zone

Secondary Time Zone

DateTime Format

SOURCES



Microsoft Teams

ADVANCED CONFIGURATION OPTIONS

There are following advanced options when configuring the connection with Merge1.

- 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 04/17/2016 and the After is set to 08/25/2018 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.
- The **Merge Message by Thread** if checked combines messages by threads rather than sending them one by one.
- The option **Split by Day** merges the messages from the same day into one email message. The time zone by which the messages are split can be selected from the drop-down menu. When Process Incomplete Days option is enabled, the messages of the days that haven't yet ended will be imported in a separate email as well. This option can be selected only if Merge Messages by Thread is selected.
- The **Include detailed user information in the body of the message** feature searches Azure AD for user principal name and then add user display name and mail address from the Azure Active Directory.

When you are finished with the configuration click **Save**.

The screenshot shows the 'Advanced Configuration Options' section for a Microsoft Teams connection. It includes fields for 'Subject Prefix' (containing 'pus'), date range filters ('Do not download data modified before:' and 'Do not download data modified after:' with calendar icons), and checkboxes for 'Merge Messages by Thread' (checked), 'Split By Day' (unchecked), 'Include detailed user information in the body of the message' (unchecked), and 'Process Incomplete Days' (unchecked). A 'Message Time Zone' dropdown is set to '(UTC+01:00) Casablanca (MST)'.

SOURCES



Microsoft Teams

EXCLUDE FILE TYPES

- 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 this 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 shouldn't be downloaded can be specified in the following format: ex. txt,png,xml. The comma is used to separate the file types.

The screenshot shows the 'EXCLUDE FILES' section of a configuration interface. It includes two main sections: 'Do not download files greater than' and 'File Types'.

- Do not download files greater than:** A checkbox labeled 'Do not download files greater than' followed by a text input field containing 'megabyte(s)'.
- Custom Message:** A text area labeled 'Custom Message' with the placeholder text 'This message will be added to the email body.' Below it is an example message: 'example: Files {0} are not imported, because of greater than {1} megabyte All the filenames that were excluded will be written instead of {0} symbol. File size limit will be written instead of {1} symbol.'
- File Types:** A text input field labeled 'File Types' followed by a text area labeled 'Custom Message' with the placeholder text 'This message will be added to the email body.' Below it is an example message: 'Example: Files {0} are not imported. All the filenames that were excluded will be written instead of {0} symbol. File types will be written instead of {1} symbol.'

NEXT STEPS

After setting up the Source follow the appropriate links below to continue with the configuration of the Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users (preferred option for Microsoft Teams is **All (Based on Native API)**, the users will be retrieved automatically)
- Filters (Microsoft Teams works with all filters except **XML Filter**)
- Targets
- Importer Settings

CISCO WEBEX TEAMS



Cisco
Webex Teams

ABOUT CISCO WEBEX TEAMS

Cisco Webex Teams enables people to meet, message, share, whiteboard, and call in a secure way, that meets legal, regulatory, and compliance mandates, and provides comprehensive business insights.

Cisco Webex Teams brings people together to collaborate, discuss, and make decisions in instant and scheduled meetings. In-app audio and video calling pulls the people in your space together for a huddle, with one tap. Meetings powered by Cisco WebEx provide an even more productive meeting environment. All Cisco Webex Teams Meetings allow screen sharing and a variety of tools for interactive creative work.

ACTIVITIES CAPTURED

- One-on-one Messages
- Group chats
- Persistent chats and channels
- Group members in a group or persistent chat
- Attachments
- Emojis
- Deleted messages
- Deleted attachments
- Conversations related to all newly added users
- Messages threading /post threading / Group chats threading

SOURCES



Cisco
Webex Teams

CISCO WEBEX TEAMS APP CREATION

1. Go to <https://developer.ciscospark.com/apps.html> and log into your account. Note that the account should have Full Administrative Privileges and be a Compliance Officer. Permissions can be checked at <https://admin.webex.com/users> -> Select User -> Roles and Security.

The screenshot shows the 'Roles and Security' section of the Cisco Webex developer portal. Under 'Administrator Roles', the 'Full administrator privileges' option is selected. Under 'Compliance', the 'Compliance Officer' checkbox is checked. Both sections have a help icon (info symbol) next to their respective descriptions.

2. Click **Create New App**

The screenshot shows the Cisco Webex for Developers homepage. At the top, there's a navigation bar with 'Cisco Webex for Developers', 'Documentation', 'Blog', and 'Support'. Below the navigation bar, there's a 'My Apps' section and a prominent blue 'Create a New App' button. A red arrow points to this button.

3. Choose **Create an Integration**.

The screenshot shows the 'Create a New App' page with three options: 'Integration', 'Bot', and 'Guest Issuer'. The 'Integration' option is highlighted with a red arrow pointing to its 'Create an Integration' button. Each option has a brief description and a 'Learn More' link below its respective button.

SOURCES



Cisco
Webex Teams

4. Fill in 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:

<input checked="" type="checkbox"/> spark:all Full access to your Webex Teams account
<input type="checkbox"/> spark:memberships_read List people in the rooms you are in
<input type="checkbox"/> spark:memberships_write Invite people to rooms on your behalf
<input type="checkbox"/> spark:messages_read Read the content of rooms that you are in
<input type="checkbox"/> spark:messages_write Post and delete messages on your behalf
<input type="checkbox"/> spark:people_read Read your users' company directory
<input type="checkbox"/> spark:rooms_read List the titles of rooms that you are in
<input type="checkbox"/> spark:rooms_write Manage rooms on your behalf
<input type="checkbox"/> spark:team_memberships_read List the people in the teams your user belongs to
<input type="checkbox"/> spark:team_memberships_write Add people to teams on your users' behalf
<input type="checkbox"/> spark:teams_read List the teams your user's a member of
<input type="checkbox"/> spark:teams_write Create teams on your users' behalf
<input checked="" type="checkbox"/> spark-admin:licenses_read Access to read licenses available in your user's organizations
<input checked="" type="checkbox"/> spark-admin:organizations_read Access to read your user's organizations
<input checked="" type="checkbox"/> spark-admin:people_read Access to read your user's company directory
<input type="checkbox"/> spark-admin:people_write Access to write to your user's company directory
<input type="checkbox"/> spark-admin:resource_group_memberships_read Access to read your organization's resource group memberships
<input type="checkbox"/> spark-admin:resource_group_memberships_write Access to update your organization's resource group memberships
<input type="checkbox"/> spark-admin:resource_groups_read Access to read your organization's resource groups
<input checked="" type="checkbox"/> spark-admin:roles_read Access to read roles available in your user's organization
<input checked="" type="checkbox"/> spark-compliance:events_read Access to read events in your user's organization
<input checked="" type="checkbox"/> spark-compliance:memberships_read Access to read memberships in your user's organization
<input type="checkbox"/> spark-compliance:memberships_write Access to create/update/delete memberships in your user's organization
<input checked="" type="checkbox"/> spark-compliance:messages_read Access to read messages in your user's organization
<input type="checkbox"/> spark-compliance:messages_write Post and delete messages in all spaces in your user's organization
<input checked="" type="checkbox"/> spark-compliance:rooms_read Access to read rooms in your user's organization
<input checked="" type="checkbox"/> spark-compliance:team_memberships_read Access to read team memberships in your user's organization
<input type="checkbox"/> spark-compliance:team_memberships_write Access to update team memberships in your user's organization
<input checked="" type="checkbox"/> spark-compliance:teams_read Access to read teams in your user's organization

- 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_read
- spark-compliance:team_memberships_read
- spark-compliance:teams_read

7. Copy the **Client ID** and **Client Secret**.

SOURCES



CONFIGURING CISCO 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**.

A screenshot of the "CONFIGURATION WIZARD" window. The "SOURCE" tab is selected. A message at the top says: "Please provide the following credentials to your company's Cisco Webex Teams app so that Merge1 can be configured to access your monitored users' account data." Below this, a note says: "If you do not have an app created for Cisco Webex Teams, please [click](#) for more information." A section titled "CISCO WEBEX TEAMS APPLICATION CONFIGURATION" contains fields for "Application ID" and "Application Secret/Key", both with placeholder text. There is also a checkbox labeled "I have Access Token". At the bottom are "BACK" and "NEXT" buttons.

MISCELLANEOUS SETTINGS

- The **Subject Prefix** is added to the subject line of imported emails. This is useful for organizing imported data, i.e. when multiple sources share a common target.
- If the option **Merge Messages by Thread** is enabled, Merge1 retrieves the data from a thread and archives it as one message.
- Options **Do Not Download Data Modified Before** and **Do Not Download Data Modified After** allow to cut off data outside the set date range. If the Before date is set to 04/17/2016 and the After is set to 08/25/2018 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.

A screenshot of the "MISC SETTINGS" configuration screen. It includes fields for "Subject prefix" (with a placeholder box), a checked checkbox for "Merge Messages by Thread", and two date range selection boxes for "Do not download data modified before" and "Do not download data modified after", each with a calendar icon.

SOURCES



Cisco
Webex Teams

Example of Merge Messages by Thread output:

Fri 11/2/2018 1:57 PM

John Doe <jdoe@example.com>
Michael Smith | Room Id: Y2IzY29zcGFyazovL3VzL1J...
To John Doe; Michael Smith

test.txt 133 bytes

jdoe@example.com 11/2/2018 1:56:47 PM
Hello Micael

jdoe@example.com 11/2/2018 1:56:55 PM
this is test

jdoe@example.com 11/5/2018 12:21:07 PM
12345678

jdoe@example.com 11/5/2018 12:21:07 PM
12345678

jdoe@example.com 11/5/2018 12:21:08 PM
23456789876543

jdoe@example.com 11/5/2018 12:21:11 PM
34587654589098765490-098765

jdoe@example.com 11/5/2018 12:21:22 PM

NEXT STEPS

After setting up the connector follow the appropriate links below to continue with the configuration of the Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users (preferred option for Cisco Webex Teams is **All (Based on Native API)**, the users will be retrieved automatically)
- Filters
- Targets
- Importer Settings

JABBER ENTERPRISE



Jabber
Enterprise

ABOUT JABBER

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 process it.

ACTIVITIES CAPTURED

- Messages between individuals
- Groups chats

DB CONFIGURATION

Merge1 retrieves data directly from the following databases.

- Oracle database
- MS SQL database

You need to add all databases, from where to retrieve the data. Use the "+" button to add the databases.

SOURCES



Jabber
Enterprise

CONNECTING TO JABBER'S DATABASE THROUGH ORACLE SQL SERVER:

1. Specify a friendly "Configuration Name".
 2. Specify Oracle Server IP address and port.
 3. In the SID field add your Oracle SID, the unique name that uniquely identifies your instance/database. Or choose to add a ServiceName of the Oracle Database instead.
 4. Add the name of your database schema in the Schema field.
 5. Add the Login and Password.
6. 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.
 - **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.
 - **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 having to create another one.

The screenshot shows a configuration dialog for connecting to an Oracle database via SQL Server. The interface is divided into two main sections: 'SQL CONNECTION' on the left and 'ADVANCED CONNECTION PARAMETERS' on the right.

SQL CONNECTION fields include:

- Configuration Name (empty input field)
- Oracle Server (empty input field)
- Port (empty input field)
- CONNECT button (blue)
- SID radio button (selected) and input field (empty)
- ServiceName radio button and input field (empty)
- Schema input field (empty)
- Login Name input field (empty)
- Password input field (empty)

ADVANCED CONNECTION PARAMETERS fields include:

- Connection timeout: 15 sec
- Min pool size: 1
- Max pool size: 100
- Enlist checkbox (unchecked)
- Pooling checkbox (unchecked)

SOURCES



Jabber
Enterprise

- 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's 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.
- 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 having 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.

SOURCES



Jabber
Enterprise

SELECT DATABASE

SQL CONNECTION
Select SQL Server

CONNECT

CONNECT USING Windows Authentication SQL Server Authentication
Login Name
Password

Select Database 3

ADVANCED CONNECTION PARAMETERS 4

Connection timeout	15	sec
Load balance timeout	0	sec
Min pool size	0	
Max pool size	100	
Network packet size	8000	bytes

Asynchronous Processing
 Encrypt
 Enlist
 Pooling
 Replication

CANCEL **OK**

OTHER OPTIONS

- The **Auto Update** feature will ensure that the connector is updated to the latest version. Each time the Importer is run, it contacts Globanet server(s) and updates the connector if a newer version is available.
- The “**Do not download data modified before**” check will ensure that old or irrelevant data is excluded. For example, if the date selected is 9/1/2017, it won’t retrieve any data modified before September 1 of 2017. Only the data after 9/1/2017 will be retrieved, archived, and imported.

OTHER OPTIONS

Auto Update

Do not download data modified before:

SOURCES



Jabber
Enterprise

Example output message:

Tue 11/6/2018 11:15 AM
forrestgramacy@mig2.local
User#[forrestgramacy@mig2.local](#) 2018-11-06 @ 11:14:44.135 (PrivateChat)

To [gilbertedockal@mig2.local](#)

[forrestgramacy@mig2.local](#) [11/6/2018 11:14:44 AM]
Ut ex et sed aliqua, ipsum fugiat est labore.
[forrestgramacy@mig2.local](#) [11/6/2018 11:14:44 AM]
Ut ex et sed aliqua, ipsum fugiat est labore.

NEXT STEPS

After setting up the connector follow the appropriate links below to continue with the configuration of the Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users (all options except All (based on the API) work with **Jabber Enterprise** connector)
- Filters
- Targets
- Importer Settings

SHAREPOINT



Sharepoint

ABOUT SHAREPOINT CONNECTOR

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 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

Merge1 SharePoint connector captures data from SharePoint Online.

ACTIVITIES CAPTURED

- Newsfeed Posts
- Newsfeed Comments
- Site Page Comments

SOURCES



Sharepoint

MICROSOFT AZURE APP CREATION

1. Create an O365 account.
2. Open the **Azure Portal** (<https://portal.azure.com/>) using the same credentials as for O365 (Global Admin).
3. Navigate to **Azure Active Directory** icon on the left-hand toolbar.

A screenshot of the Microsoft Azure portal's monitoring dashboard. The left sidebar shows various service icons, and the 'Azure Active Directory' icon is highlighted with a red arrow. The main panel displays a message: 'No resources to display' and 'Try changing your filters if you don't see what you're looking for.' A 'Create resources' button is visible. On the right, there's a promotional section for 'Azure getting started made easy!' featuring 'Create DevOps Project' and several quickstart options like 'Windows Virtual Machines' and 'App Service'.

4. Click on the **App Registration**.

A screenshot of the 'Globanet - Overview' page in the Azure Active Directory section. The left sidebar is identical to the previous screenshot. In the main content area, under the 'Manage' heading, the 'App registrations' option is highlighted with a red arrow. Other manage options listed include 'Users', 'Groups', 'Organizational relationships', 'Roles and administrators', 'Enterprise applications', 'Devices', 'Application proxy', 'Licenses', and 'Azure AD Connect'.

SOURCES



Sharepoint

5. Click on **+ New Registration** button.

The screenshot shows the 'Globanet - App registrations' page in the Azure Active Directory. The top navigation bar includes 'Home', 'Globanet - App registrations', 'Azure Active Directory', 'Search (Ctrl+)', and 'New registration' (highlighted by a red arrow). Below the navigation is a welcome message: 'Welcome to the new and improved App registrations (now Generally Available). See what's new →'. A note below it says: 'Looking to learn how it's changed from App registrations (Legacy)? Learn more. Still want to use App registrations (Legacy)? Go back and tell us why.' The main content area has tabs for 'All applications' (selected) and 'Owned applications'. At the bottom are filters for 'DISPLAY NAME' and 'APPLICATION (CLIENT) ID'.

6. Enter a **Name** for the application, select "**Web**" under Redirect URI(optional), and enter the URL of your local Merge1 environment with the following extension: **"/Configuration/OAuthCallback"**. Then click on the **Register** button.

The screenshot shows the 'Register an application' form. It starts with a field for the '*** Name**' (Sample Application) and a note about the user-facing display name. The next section is 'Supported account types' with three options: 'Accounts in this organizational directory only (Globanet)' (selected), 'Accounts in any organizational directory', and 'Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)'. There is also a 'Help me choose...' link. The 'Redirect URI (optional)' section shows 'Web' selected and the URL 'https://globanetlabs.com/Configuration/OAuthCallback'. At the bottom is a note about agreeing to Microsoft Platform Policies and a blue '**Register**' button (highlighted by a red arrow).

7. Find your **Application (client) ID**. Make a note of the Application (client) ID, this is needed for configuring the SharePoint Source in Merge1.

SOURCES



Sharepoint

8. In the navigation pane to the left go to **Certificates & secrets**.

The screenshot shows the 'Sample Application' page in the Azure portal. On the left, the navigation pane includes 'Overview', 'Quickstart', 'Manage' (with 'Branding', 'Authentication', 'Certificates & secrets' selected), 'API permissions', 'Expose an API', 'Owners', and 'Manifest'. Under 'Support + Troubleshooting', there are 'Troubleshooting' and 'New support request'. The main content area displays the application's details: Display name (Sample Application), Application (client) ID, Directory (tenant) ID, and Object ID. A red arrow points to the 'Certificates & secrets' link in the navigation pane. Below the details, a welcome message and a 'Call APIs' section are visible.

9. Click on **New client secret**, enter a Description, specify a **Duration** and click **Add**.

Make a note of the new client secret value. This is needed for configuring the SharePoint Source in Merge1.

The screenshot shows the 'Certificates & secrets' blade for the 'Sample Application'. The left sidebar lists 'Overview', 'Quickstart', 'Manage' (selected), 'API permissions', 'Expose an API', 'Owners', and 'Manifest'. Under 'Support + Troubleshooting', there are 'Troubleshooting' and 'New support request'. The main area has a heading 'Add a client secret' with fields for 'Description' (set to 'Secret') and 'Expires' (set to 'Never'). A red arrow points to the 'Add' button. Below this, a 'Client secrets' table is shown with a single row: '+ New client secret'. Another red arrow points to this button. The table columns are 'DESCRIPTION', 'EXPIRES', and 'VALUE'. A note at the bottom states 'No client secrets have been created for this application.'

SOURCES



Sharepoint

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

The screenshot shows the 'Certificates & secrets' blade for a sample application in the Azure portal. The left sidebar lists various management options like Overview, Quickstart, Manage, Authentication, Certificates & secrets (which is selected and highlighted), API permissions, Expose an API, Owners, Manifest, Support + Troubleshooting, Troubleshooting, and New support request. The main content area has sections for 'Certificates' and 'Client secrets'. A red arrow points to the 'API permissions' link in the sidebar.

11. Click on Microsoft Graph, in the opened pane select **Application permissions**.

Grant the following permissions:

- **Files:** Files.Read.All
- **Directory:** Directory.Read.All
- **User:** User.Read.All
- **Applications:** Applications.Read.All
- **Applications:** Applications.ReadWrite.All*

Once you have selected all three checkboxes, click **Update Permissions**.

The screenshot shows the 'Request API permissions' dialog for Microsoft Graph. The left sidebar shows the 'API permissions' blade with the 'Microsoft Graph (1)' section selected. The right pane shows the 'Request API permissions' dialog with sections for 'Contacts', 'Device', 'Directory (1)', 'Domain', 'EduAdministration', 'EduAssignments', 'EduRoster', 'Files (1)', 'Group', 'IdentityRiskEvent', 'IdentityRiskyUser', and 'InformationProtectionPolicy'. Under 'Directory (1)', 'Directory.Read.All' is checked. Under 'Files (1)', 'Files.Read.All' is checked. At the bottom, there are 'Update permissions' and 'Discard' buttons, with 'Update permissions' highlighted by a red arrow.

* Only required if the certificate has not been already uploaded to the Azure App. Check Appendix for more information.

SOURCES



Sharepoint

- 12.** Get back to API permissions section, click **+ Add a permission** and select **Sharepoint API with Application permissions**. These are the permissions you need to grant:

- **Sites**: Sites.FullControl.All; Sites.Read.All
- **User**: User.Read.All
- **TermStore**: TermStore.Read.All

Once you have selected all three checkboxes, click **Update Permissions**.

The screenshot shows the 'Request API permissions' dialog box. On the left, the 'API permissions' section is expanded, showing 'Delegated permissions' and 'Application permissions'. Under 'Application permissions', it says 'Your application runs as a background service or daemon without a signed-in user.' In the 'Select permissions' table, under the 'Sites' category, there are four checkboxes:

- Sites.FullControl.All**: Have full control of all site collections. (Yes)
- Sites.Manage.All**: Read and write items and lists in all site collections. (Yes)
- Sites.Read.All**: Read items in all site collections. (Yes)
- Sites.ReadWrite.All**: Read and write items in all site collections. (Yes)

At the bottom of the dialog, there are 'Add permissions' and 'Discard' buttons. A blue box highlights the 'Add permissions' button, and two red arrows point from the text in the previous step to the 'Application permissions' section and the 'Add permissions' button.

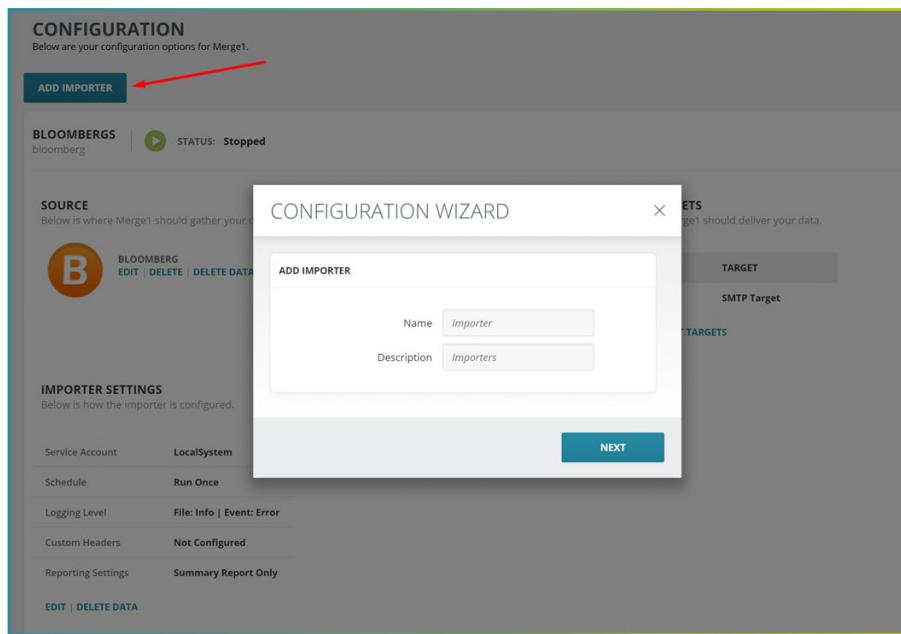
SOURCES



Sharepoint

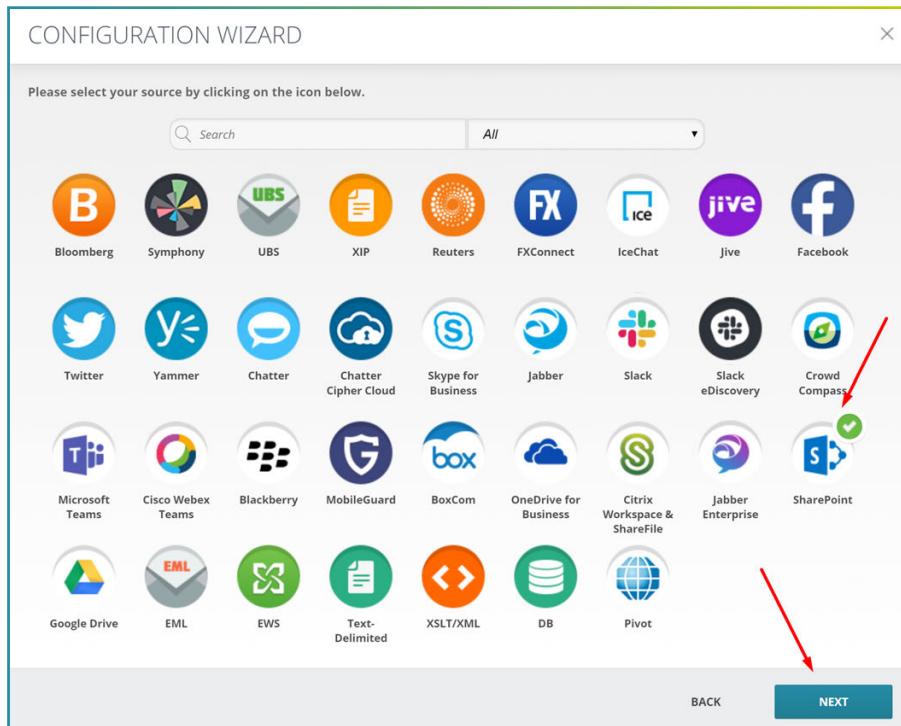
SETTING UP THE CONNECTOR IN MERGE1

1. Open **Merge1 Configuration** section, click **Add Importer**, specify **Name** for the new importer and click **Next (Description** is optional).



The screenshot shows the 'CONFIGURATION' screen for Merge1. A red arrow points to the 'ADD IMPORTER' button. A modal window titled 'CONFIGURATION WIZARD' is open, showing the 'ADD IMPORTER' step. It has two input fields: 'Name' (set to 'Importer') and 'Description' (set to 'Importers'). A 'NEXT' button is at the bottom right of the modal.

2. Select **Sharepoint** and click **Next**.



The screenshot shows the 'CONFIGURATION WIZARD' screen. A red arrow points to the SharePoint icon (a blue circle with a white 'S') in the grid of available sources. Another red arrow points to the 'NEXT' button at the bottom right of the wizard.

SOURCES



Sharepoint

3. In the new window you need to add **X509 Certificate Thumbprint**, **Application ID**, and **Application Secret/Key**.

EDIT CONNECTOR

SOURCE MONITORED USERS FILTERS TARGETS SETTINGS

Please provide the following credentials to your company's SharePoint app so that Merge1 can be configured to access your monitored users' account data.

If you do not have an app created for SharePoint, please [click](#) for more information.

SHAREPOINT APPLICATION CONFIGURATION

X509 Certificate Thumbprint

Application ID

Application Secret/Key

NEXT

- 4.1 To get the **Certificate Thumbprint** open the PowerShell on the Merge1 server and use the **Get-ChildItem -path cert:\LocalMachine\My** command (please note that as a result you can have more than one thumbprint, therefore, you should use the thumbprint of the Self-Signed Certificate that you have used during Merge1 installation).

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32> Get-ChildItem -path cert:\LocalMachine\My

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

Thumbprint                               Subject
-----                               -----
5095E64932B0F8D073C1B34D426EC5C37486324E CN=MSvc-SHA2-DESKTOP-DR3LPRO
35B0BDD6CA12AD86D316691C78ED034C96CFFCD8 CN=DESKTOP-DR3LPRO

PS C:\WINDOWS\system32>
```

SOURCES



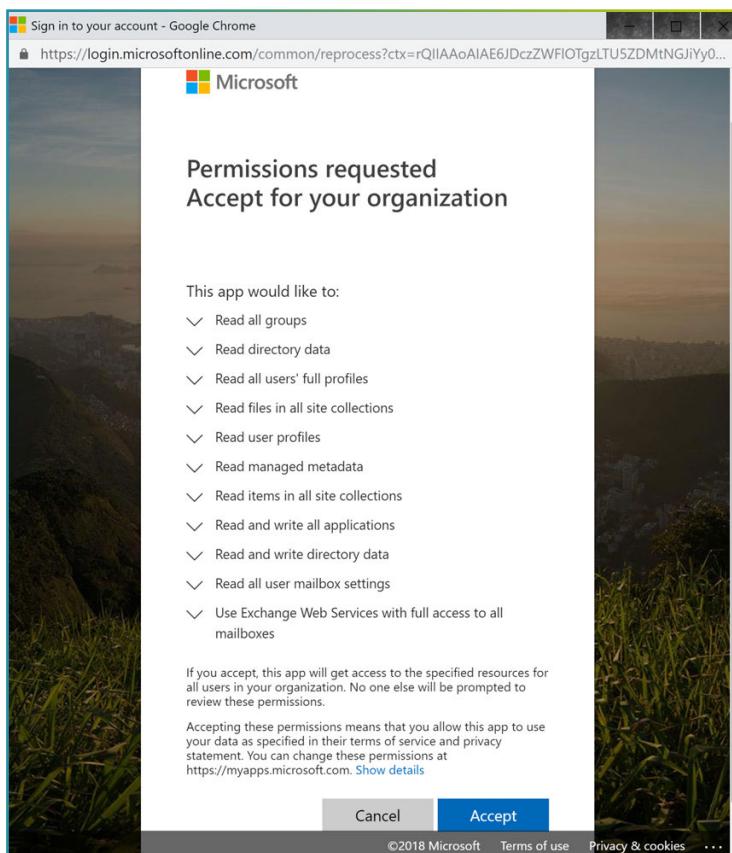
Sharepoint

- 4.2** You can copy the **Application ID** from the Azure Active Directory -> App Registrations -> <your app name> section.

The screenshot shows the 'App registrations' section of the Azure Active Directory portal. On the left, there's a sidebar with links like Overview, Getting started, Manage (Users, Groups, etc.), and App registrations. The main area shows a table with one row for 'Globalnet'. The columns are DISPLAY NAME, APPLICATION TYPE, and APPLICATION ID. The APPLICATION ID column contains the value 'f2832761-307e-445c-adb3-b12b2aa2f262', which is highlighted with a red box. The URL in the browser is 'https://aad.portal.azure.com/#blade/Microsoft_AAD_B2B/ApplicationsBlade/~/registrations/Globalnet'.

4.3 Refer to Point 14 in Microsoft Azure App Creation section. Enter the **Application Secret/Key** that you have saved before.

- 5.** After clicking **Next** a pop-up window should appear where you should provide the O365 Global Admin user credentials (please note that usually the pop-up is being blocked by the browser so pay attention to the top right corner of the browser if the popup is not appearing). In the next window click **Accept** to grant the permissions.



SOURCES



Sharepoint

SETTING UP SECURITY AND COMPLIANCE FOR SHAREPOINT

1. Navigate to <https://protection.office.com/?rfr=AdminCenter#/retention>.
2. Click **Create** to start the setup wizard.

The screenshot shows the 'Retention' page in the SharePoint Admin Center. The left sidebar has 'Home', 'Threat management', and 'Service assurance'. The main area shows two sections: 'Labels' and 'Label policies'. The 'Labels' section has a description: 'Create labels to let users manually classify and retain their own content (email, docs, folders, and more). You can also automatically apply labels to specific content.' It includes a 'Create' button. The 'Label policies' section has a description: 'Create label policies to publish or automatically apply existing labels to your users apps (Outlook, SharePoint, OneDrive, and more.)'. Below these are search and filter options ('Name', 'Created by', 'Last modified') and a message 'No data available'.

3. Click **Create** to start the setup wizard.

The screenshot shows the 'Name your policy' step of the setup wizard. On the left, a sidebar lists steps: 'Name your policy' (selected), 'Settings', 'Choose locations', and 'Review your settings'. The main area has a title 'Name your policy' and fields for 'Name' (with a red arrow pointing to it) and 'Description' (with a red arrow pointing to it). At the bottom are 'Next' and 'Cancel' buttons, and a 'Feedback' link at the bottom right.

SOURCES



Sharepoint

4. In 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**.

The screenshot shows a 'Create a policy to retain what you want and get rid of what you don't.' interface. On the left, there are tabs: 'Name your policy' (selected), 'Settings', 'Choose locations' (selected), and 'Review your settings'. The main content area is titled 'Decide if you want to retain content, delete it, or both'. It asks 'Do you want to retain content?' with a radio button for 'Yes, I want to retain it' (selected). It then specifies 'For this long... 7 years'. Below that, it asks 'Do you want us to delete it after this time?' with a radio button for 'No' (selected). It also has an option 'No, just delete content that's older than 1 year'. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons, and a 'Feedback' link.

5. 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** or select **Let me choose specific locations** and apply them to specific applications.

Once you choose the locations where the retention policy applies, click "Next"

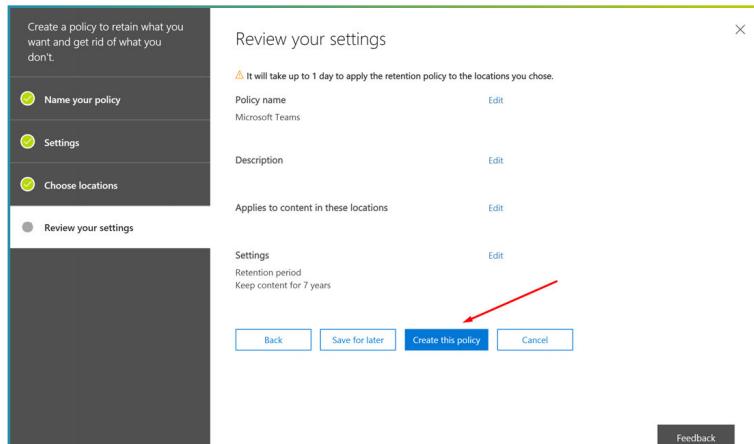
The screenshot shows the 'Edit retention policy' screen. On the left, there are tabs: 'Edit retention policy' (selected), 'Policy name' (disabled), and 'Policy settings' (disabled). The main content area is titled 'Retention policy' and 'Editing Locations applied'. It lists five locations with toggle switches: 'SharePoint sites' (selected), 'OneDrive accounts' (selected), 'Office 365 groups' (selected), 'Skype for Business' (selected), and 'Exchange public folders' (disabled). For each location, there are three options: 'All' (selected), 'Choose sites/accounts/groups/users' (link), and 'None' (selected). At the bottom, there are 'Save' and 'Cancel' buttons, and a 'Feedback' link.

SOURCES



Sharepoint

4. The next screen offers to review the settings that you have chosen. If everything is correct click **Create this Policy**. Please note that it would take up to 1 day to apply the retention policy to the locations you chose.



ADVANCED CONFIGURATION OPTIONS

ADVANCED CONFIGURATION OPTIONS

Subject Prefix

Do not download data modified before:

Do not download data modified after:

Auto Update

PROCESSING MODE

Single message per event

Single Message per comment and its replies/sub-comments

Single Message per Site

There are following advanced options when configuring the connection with Merge1.

- 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 04/17/2016 and the After is set to 08/25/2018 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.

SOURCES



Sharepoint

- The **Auto Update** feature will ensure that the connector is updated to the latest version. Each time the Importer is run, it contacts Globanet server(s) and updates the connector if a newer version is available.

PROCESSING MODE

- 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 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.

Example output message:

Tue 11/27/2018 3:32 PM
Marcus Smith <MSmith@example.com>
Globanet Team Site-Marcus Smith replied...
To: Dave Roberts; Kevin Jones; Marcus Smith; Merge1 Test; John Doe; Products

redkite50498.jpg - 7 KB

Marcus Smith - November 27 at 03:31 PM
reply to John's post
on 11/27 @ 3:30PM+4

Site: Globanet Team Site
Place: Newsfeed
MessageId: 45f3d97d-3ec5-4834-b761-4f9886dc1fe2
Attachment: redkite50498.jpg

NEXT STEPS

After setting up the connector follow the appropriate links below to continue with the configuration of the Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users (preferred option for Sharepoint is **All (Based on Native API)**, the users will be retrieved automatically)
- Filters (Sharepoint works with all filters except **XML Filter**)
- Targets
- Importer Settings

GOOGLE DRIVE



Google Drive

ABOUT GOOGLE DRIVE CONNECTOR

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
- Conversations and comments around shared documents

Please note:

While the SMTP addresses are unique in the To and From field of the generated message, the content inside the body of the message can have duplicate display names. It is the user's responsibility is to ensure that best practices are followed and there are no users with the same display name.

SOURCES



Google Drive

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.

1. Open the **Service accounts** page. If prompted, select a project.

<https://console.developers.google.com/iam-admin/serviceaccounts>

To view this page, select a project.

SELECT CREATE

2. Click **Create service account**.

Email	Status	Name	Description	Key ID	Actions
env-data-har	✓				⋮
env-helper	✓		Service Account for Gmail - GVault Target		⋮

SOURCES



Google Drive

3. In the **Create service account** window, type a name for the service account. The next two steps are optional and don't need to be filled in.

The screenshot shows the 'Create service account' dialog box. At the top, there are three tabs: 1 Service account details (selected), 2 Grant this service account access to project (optional), and 3 Grant users access to this service account (optional). The 'Service account details' section contains fields for 'Service account name' (Sample), 'Display name for this service account' (Sample), 'Service account ID' (sample@merge1.iam.gserviceaccount.com), and 'Service account description' (Describe what this service account will do). At the bottom are 'CREATE' and 'CANCEL' buttons.

4. Once the service account is created, open it. In its settings click Edit, open the Show Domain-wide Delegation menu and check Enable G Suite Domain-Wide Delegation.

The screenshot shows the 'Sample' service account details page. At the top, there are 'EDIT' and 'DELETE' buttons. Below is the 'Service account details' section with fields for 'Name' (Sample), 'Description', 'Email' (sample@merge1.iam.gserviceaccount.com), and 'Unique ID' (103959411903845318055). Under 'Disable service account', it says 'Account currently active' (checked) and 'Enabled' (checked). Under 'Enable G Suite Domain-wide Delegation', there is a checked checkbox with a descriptive text about delegation. At the bottom are 'HIDE DOMAIN-WIDE DELEGATION', '+ CREATE KEY', 'SAVE', and 'CANCEL' buttons. Red arrows point to the 'EDIT' button, the 'Enable G Suite Domain-wide Delegation' checkbox, and the 'HIDE DOMAIN-WIDE DELEGATION' link.

5. In the same window copy the Email and the Unique ID of the service account.

SOURCES



Google Drive

6. Click on Create Key to create a private key for the service account.

The screenshot shows the 'Service account details' section of the Google Cloud Platform interface. It includes fields for Name (Sample), Description, Email (sample@merge1.iam.gserviceaccount.com), and Unique ID (103959411903845318055). Below this, the 'Disable service account' section is shown with 'Account currently active' checked and 'Enabled' set. Under 'Enable G Suite Domain-wide Delegation', there is a checkbox that is checked. A red arrow points to the '+ CREATE KEY' button at the bottom left of the screen. At the bottom right are 'SAVE' and 'CANCEL' buttons.

7. Select the key type JSON and click Create.

The screenshot shows a modal dialog titled 'Create private key for "Sample"'. It contains instructions about storing the file securely. Under 'Key type', the 'JSON' option is selected (radio button is filled) and labeled 'Recommended'. The 'P12' option is also available with a note about backward compatibility. At the bottom are 'CANCEL' and 'CREATE' buttons, with a red arrow pointing to the 'CREATE' button.

8. Your new public/private key pair is generated and downloaded to your machine; it serves as the only copy of this key. You are responsible for storing it securely.

SOURCES



Google Drive

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 have to be performed by an administrator of the G Suite domain:

1. Go to your G Suite domain's Admin console <https://admin.google.com/>.
2. Select Security from the list of controls. If you don't see Security listed, select More controls from the gray bar at the bottom of the page, then select Security from the list of controls.

The screenshot shows the Google Admin console interface. At the top, there's a blue header bar with the title 'Google Admin' and a search bar. Below it is a white navigation bar with the text 'Admin Console' and a link 'Set up Admin Console: Click here to get started'. The main area contains several control cards arranged in a grid. The 'Security' card, which has a shield icon and the text 'Configure security settings', is highlighted with a red box. Other visible cards include 'Dashboard', 'Users', 'Groups', 'Organizational units', 'Buildings and resources', 'Devices', 'Apps', 'Reports', 'Billing', 'Company profile', 'Admin roles', 'Domains', and 'Data migration'.

3. Select Advanced settings from the list of options.

The screenshot shows the 'Security' section of the Google Admin console. On the left, there's a sidebar with the word 'Security'. The main content area lists several options: 'Advanced Protection Program (Beta)', 'Context-Aware Access (Beta)', 'Google session control', and 'Advanced settings'. The 'Advanced settings' card, which has a lock icon and the text 'Manage advanced security features such as authentication, and integrating G Suite with internal services.', is highlighted with a red box. Below it are other sections: 'Security and privacy resources' and 'API Permissions'.

SOURCES



Google Drive

4. Select Manage API client access in the Authentication section.

The screenshot shows the 'Advanced settings' page in Google Cloud Platform. The 'Authentication' section is highlighted with a red arrow. It contains the following text:
Authentication
Manage API client access
Allows admins to control access to user data by applications that use OAuth protocol.

5. Paste the Unique ID into the Client Name field.

The screenshot shows the 'Manage API client access' page. In the 'Authorized API clients' section, the 'Client Name' field contains the value '1173975812142269240'. A red arrow points to this field. The 'One or More API Scopes' field contains 'https://www.googleapis.com/auth/gmail.insert'. The 'Authorize' button is visible next to the scopes field.

6. In the One or More API Scopes field enter the list of scopes that your application should be granted access to (see image below). For example if you need domain-wide access to Users and Groups enter: `https://www.googleapis.com/auth/admin.directory.user.readonly`, `https://www.googleapis.com/auth/drive.file`

7. Click the Authorize button.

The screenshot shows the 'Manage API client access' page. In the 'Authorized API clients' section, the 'Client Name' field contains '1173975812142269240'. The 'One or More API Scopes' field contains 'https://www.googleapis.com/auth/admin.directory.user.readonly'. The 'Authorize' button is highlighted with a red box.

Your service account now has domain-wide access to the Google Admin SDK Directory API for all the users of your domain. You are ready to instantiate an authorized Admin SDK Directory service object on behalf of your G Suite domain's users.

Please 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.

SOURCES



Google Drive

CREATING ADMINISTRATIVE ROLE FOR THE USER MANAGER SERVICE ACCOUNT

1. Go to <https://admin.google.com> and click on Admin roles.

The screenshot shows the Google Admin console interface. It features a grid of 12 icons arranged in three rows of four. Each icon has a title and a brief description below it. A red arrow points from the text 'Admin roles' in step 2 to the 'Admin roles' icon in the bottom right corner of the grid.

Dashboard See relevant insights about your organization	Users Add or manage users	Groups Create groups and mailing lists	Organizational units Add, remove, rename, move or search for an organizational unit
Apps Manage apps and their settings	Security Configure security settings	Reports Monitor usage across your organization	Billing Manage subscriptions and billing
Domains Manage your domains	Data migration Manage migration	Buildings and resources Manage and monitor buildings, rooms and resources	Devices Secure corporate data on devices

2. Click CREATE A NEW ROLE.

The screenshot shows the 'Admin roles' page. At the top left, there is a button labeled 'CREATE A NEW ROLE' with a red arrow pointing to it. Below this, a section titled 'System Roles' lists several roles: Super Admin, User Management Admin (which is highlighted in red), Services Admin, Help Desk Admin, Groups Admin, and Mobile Admin. To the right of the roles, there are tabs for 'Admins' and 'Privileges'. Under the 'Admins' tab, there are two buttons: 'ASSIGN ADMIN' and 'UNASSIGN ADMIN'. Below these buttons is a checkbox labeled 'Administrators'. At the bottom of the page, there is a section titled 'User Created Roles'.

3. Name the New Role and click CREATE.

The screenshot shows a modal dialog box titled 'Create New Role'. Inside the dialog, there is a 'Name' field containing 'UserManagerReadOnly'. Below the name field is a 'Description' field which is currently empty. At the bottom of the dialog, there are two buttons: 'CANCEL' and 'CREATE'.

SOURCES



Google Drive

4. Expand Users, select Read and click SAVE.

The screenshot shows the 'CREATE A NEW ROLE' page. The role name is 'UserManagerReadOnly'. Under 'System Roles', 'Super Admin' is selected. Under 'User Created Roles', there is a list of roles. In the 'Privileges' section, the 'Admins' tab is selected. Under 'Admin Console Privileges', the 'Read' checkbox is checked. Under 'User Privileges', the 'Users' section has its 'Read' checkbox checked. At the bottom right, the 'SAVE' button is highlighted.

5. To assign the role to a user, go to <https://admin.google.com> and click Users, then click on the user that you want to assign the role to.

The screenshot shows the 'Users' page in the Google Admin console. It lists users with columns for Name, Email, Status, Last sign in, and Email usage. A red arrow points to the user 'Hagop Esfahani'.

6. Scroll down to Admin roles and privileges and click ASSIGN ROLES.

The screenshot shows the 'Admin roles and privileges' page for user 'James'. It displays a message: 'James doesn't have any admin roles or privileges.' Below this is a blue 'ASSIGN ROLES' button, which is highlighted with a red arrow.

7. Assign the role and click SAVE.

The screenshot shows the 'Roles' page for user 'James'. It lists various roles with their descriptions and assignment status. The 'UserManagerReadOnly' role is selected and assigned to 'All organizational units'. At the bottom right, the 'SAVE' button is highlighted.

SOURCES



Google Drive

CONNECTOR AUTHENTICATION

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.

AUTHENTICATION

Credentials JSON file *

Source mailbox *

3. The download button is only active when there is a JSON file uploaded.

AUTHENTICATION

Credentials JSON file *

Source mailbox *

ADVANCED CONFIGURATION OPTIONS

- The **Auto Update** feature will ensure that the connector is updated to the latest version. Each time the Importer is run, it contacts Globanet server(s) and updates the connector if a newer version is available.

ADVANCED CONFIGURATION OPTIONS

Auto Update

Subject Prefix

Do not download data modified before:

Do not download data modified after:

SOURCES



Google Drive

- 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.
- 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 04/17/2016 and the After is set to 08/25/2018 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.

Example output message:

The screenshot shows an email message from Hagop Esfahani (he) to himself. The subject is "Google Drive Test". The message body contains the following information:

Hagop Esfahani
DateTimeCreated: June 20 at 09:17 PM CST
DateTimeModified: August 28 at 02:53 PM CST
Uploaded File

File Name: Google Drive Test
File Version: 45
Size in bytes:
Created Time: June 20 at 09:17 PM CST
Modified Time: August 28 at 02:53 PM CST
Trashed: No
WebViewLink: https://docs.google.com/document/d/1aiX104WBjijE17N4-7h1YFbB_Ii52PRCb22B891jK5A/edit?usp=drivesdk

Replies:

- Hagop Esfahani
DateTimeCreated: August 28 at 12:54 PM CST
DateTimeModified: August 28 at 12:54 PM CST

pxik

Resolved: No
Deleted: No

NEXT STEPS

After setting up the connector follow the appropriate links below to continue with the configuration of the Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users (preferred option for Google Drive is **All (Based on Native API)**, the users will be retrieved automatically)
- Filters (Google Drive works with all filters except **XML Filter**)
- Targets
- Importer Settings

ZOOM MEETINGS



ABOUT ZOOM CONNECTOR

Zoom

Zoom is the leader in modern enterprise video communications, with an easy, reliable cloud platform for video and audio conferencing, chat, and webinars.

The Zoom account used for the Merge1 Zoom Connector needs to be on Pro or Business plan to gain access to the API. The Pro plan has access to all the features of the API except voice transcription that is only available in the Business subscription plan.

ACTIVITIES CAPTURED

- Meeting Metadata
- Meeting Recording Files
- Meeting Chat

Please note:

Only meetings from the last 6 months can be captured. The option to select a longer cut-off date in the Merge1 UI has also been disabled.

If a message was sent privately to one of the meeting participants, it is not added to the recording file, as the Zoom API doesn't provide that option. We recommend disabling the private messages to be SEC compliant by following this link: <https://zoom.us/account/setting>

Private chat



Allow meeting participants to send a private 1:1 message to another participant.

SOURCES



Zoom

ZOOM APP CREATION

1. Go to Zoom Marketplace: <https://marketplace.zoom.us/>
2. Select Develop -> Build App.

A screenshot of the Zoom App Marketplace homepage. At the top, there's a search bar, a 'Develop' dropdown menu, and 'Sign In' and 'Sign Up' buttons. Below the header, there's a section titled 'Find apps that enhance your Zoom experience' with a sub-section about power-ups. A red arrow points from the text 'Select Develop -> Build App.' in the previous step to the 'Build App' button in the screenshot. To the right of the button is 'Documentation', 'Developer Blog', 'Community Forum', and 'Team Drives'. The main area shows a grid of various app icons.

3. Sign In if prompted to.
4. Choose **OAuth** application type.

A screenshot of the 'Choose your app type' screen. It has three options: 'JWT', 'OAuth', and 'Chatbot'. The 'OAuth' option is highlighted with a red box around its 'Create' button. Below each option is a brief description and a 'Learn more' link. The 'OAuth' section also includes a note that says 'Your account already has JWT credentials.'

5. Choose **Account-level app** and disable publishing to Marketplace.

A screenshot of the 'Create an OAuth app' configuration screen. It starts with an 'App Name' field containing 'Merge1'. Below it is a 'Choose app type' section where 'Account-level app' is selected (indicated by a red arrow). The description for 'Account-level app' states: 'This app must be installed by admin and can manage all users in the account'. The 'User-managed app' option is also listed with its description. At the bottom, there's a question 'Would you like to publish this app on Zoom App Marketplace?' with a toggle switch. A red arrow points to the switch, which is turned off, indicating that publishing is disabled. There are 'Cancel' and 'Create' buttons at the bottom right.

SOURCES



Zoom

6. Under Redirect URL for OAuth enter the URL of your local Merge1 environment with the following extension: **"/Configuration/OAuthCallback"**. Copy the Client ID and the Client Secret. They will be used later to configure the Merge1 Zoom connector.

Click **Continue**.

The screenshot shows the 'Merge1' app configuration interface. The 'App Credentials' section is active. It displays the Client ID ('lItf5jbFQXu7akdTMTYxw') and Client Secret ('.....'), each with a 'Copy' button. Below these fields is the 'Redirect URL for OAuth' input field, which contains the URL 'https://globanetlabs.com/Configuration/OAuthCallback'. At the bottom right of the screen, there is a 'Saved' indicator and a prominent blue 'Continue' button.

8. In the Information section fill in the following information:

Short Description
Long Description
Developer Name
Developer Email Address

SOURCES



Zoom

9. Go to **Scopes** and click on **Add Scopes**.

The screenshot shows the 'Merge1' application settings page. At the top, there is a large 'UPLOAD' button with a plus sign. Below it, a sidebar lists categories: App Credentials, Information, Feature, **Scopes** (which has a red arrow pointing to it), and Install. The main area is titled 'Add Scopes' and contains a note about scopes defining API methods and restrictions. It includes a search bar and a '+ Add Scopes' button. A table below shows 'No Data'. At the bottom, there are 'Back', 'Saved' (with a green checkmark), and 'Continue' buttons.

10. Add following scopes to the application:

Meeting -> View all user meetings

Recording -> View all user recordings

User -> View all user information

Dashboard -> View Dashboard Data

Click **Done**.

The screenshot shows the 'Add scopes' dialog. It has a search bar and a list of scope types: Meeting, Webinar, Recording, User, Account, Billing, Contacts, **Dashboard** (which is highlighted with a blue background and has a red arrow pointing to it), Group, and Devices (H323). On the right, two checkboxes are shown: 'View sub account's Dashboard data' (unchecked) and 'View Dashboard data' (checked). At the top right, it says '4 Added'. At the bottom right is a 'Done' button.

SOURCES



Zoom

11. Go to **Install** section and click **Install**.

The screenshot shows the Merge1 app configuration page. At the top, there's a large 'UPLOAD' button with a plus sign. Below it, a sidebar lists several sections: 'App Credentials', 'Information', 'Feature', 'Scopes' (which is checked), and 'Install' (which is selected). The main area is titled 'Merge1' and shows the following details:

- 'Intent to publish: No'
- 'Account-level app'
- 'OAuth app'

Install your app

A blue 'Install' button is highlighted with a red box. Below it is an 'Installation URL' field containing a long URL, with a 'Copy' button next to it.

Share your app with others

An 'Enable Publishing' link is followed by a note: 'This app cannot be shared outside of your account or on the Zoom App Marketplace. If you wish to share this app with the Zoom community, please click the button below. Once changed, you will be able to submit your app for approval to be included in the Zoom App Marketplace.' A 'Change Now' button is present.

12. In order to enable Merge1 to download meeting recordings, the Admin must enable "Cloud recording downloads" setting and Do Not prevent non-host downloads:

The screenshot shows the 'Cloud recording downloads' settings. It includes two options:

- Allow anyone with a link to the cloud recording to download** (selected, indicated by a blue toggle switch)
- Only the host can download cloud recordings** (not selected, indicated by an empty checkbox)

SOURCES



Zoom

CONNECTOR CONFIGURATION

1. Enter Client ID in the Application ID field.
2. Enter Client Secret in the Application Secret/Key field. Click Next.

CONFIGURATION WIZARD

SOURCE MONITORED USERS FILTERS TARGETS SETTINGS

Please provide the following credentials to your company's Zoom Meetings app so that Merge1 can be configured to access your monitored users' account data.

If you do not have an app created for Zoom Meetings, please [click](#) for more information.

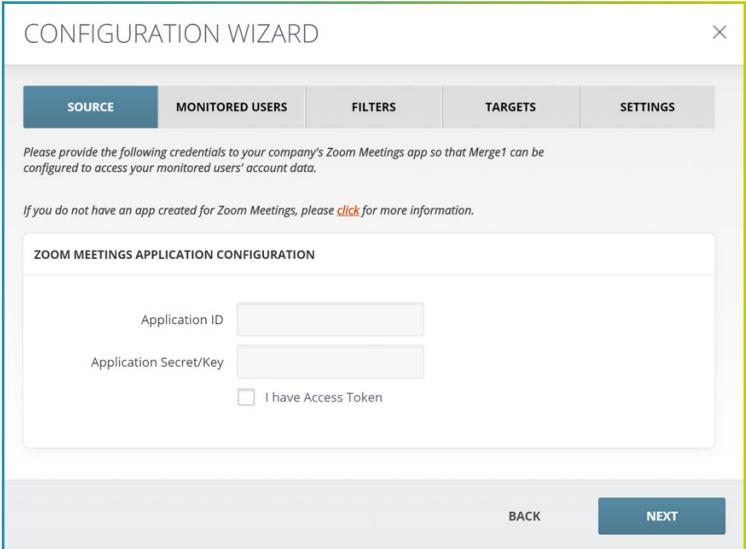
ZOOM MEETINGS APPLICATION CONFIGURATION

Application ID

Application Secret/Key

I have Access Token

BACK NEXT



3. In the opened pop-up confirm the application connection. Make sure that the pop-ups are not disabled in the browser window.

TIMESTAMP FORMATTING

In addition to the primary stamp, a second timestamp can be enabled with its timezone.

From the drop-down menu you can choose the time zone of the timestamp.

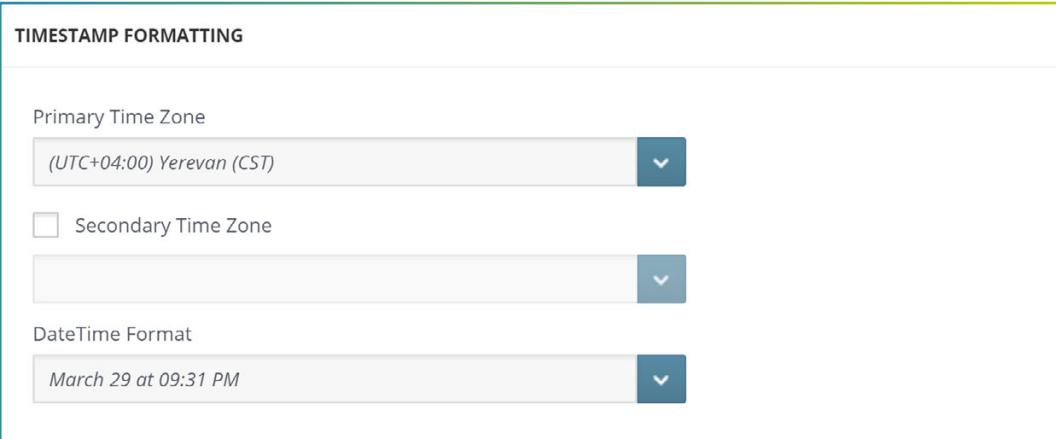
The format of the timestamp in the output message can also be specified from the six options in the Datetime Format dropdown menu.

TIMESTAMP FORMATTING

Primary Time Zone

Secondary Time Zone

Datetime Format



SOURCES



Zoom

MEETING FILE DOWNLOAD OPTIONS

- 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** option specifies how the chat file is added to the imported message: in the body of the message or attached to the message as a separate file.
- **Include Transcript File** option specifies how the chat file is added to the imported message: in the body of the message or attached to the message as a separate file.
- **Meeting Recordings** option specifies whether video with audio or only audio are included in the imported message.

MEETING FILE DOWNLOAD OPTIONS

Do not download files greater than megabyte(s).

INCLUDE CHAT FILE

In the Body
 As Attachment

INCLUDE TRANSCRIPT FILE

In the Body
 As Attachment

MEETING RECORDINGS

Video with audio
 Audio only

ADVANCED CONFIGURATION OPTIONS

SOURCES



Zoom

ADVANCED CONFIGURATION OPTIONS

Subject Prefix

Do not download data modified before:

Do not download data modified after:

Auto Update

Example output message:

zz - Hasmik's:VvspFLpaSeC4xW9k1mn2jw==

 admin admin <admin@globanetlabs.onmicrosoft.com>
To: Hasmik; Mariam

admin admin
Meeting Start Time: 17/10/2019 12:05:28.000 CST
Meeting Start Time: 17/10/2019 06:05:28.000 UTC-02
Meeting End Time: 17/10/2019 12:14:50.000 CST
Meeting End Time: 17/10/2019 06:14:50.000 UTC-02
Meeting Id: VvspFLpaSeC4xW9k1mn2jw==
Topic: Hasmik's
Participants: 3
Duration: 09:22
Screen Share: No
Has Recording: Yes
Download Url Of shared_screen_with_speaker_view: <https://api.zoom.us/recording/download/WHFyxKF7oFW3M5neHYguGx8WGcJFt5e4sfk-m7RYdV1khLmeGx6jzNVqzDuj2B1>
Download Url Of audio_only: https://api.zoom.us/recording/download/K5U6bvNqU97dRs6ix2twP-epXo6P-HaTtYKy9yznW2E5uhNwSGGjW0Z7_d1qc7
Download Url Of chat_file: <https://api.zoom.us/recording/download/MWPnrylHKvzlnI4r2EznW13m6b4rWWAv7UY4iTcb1KjnGMWTPFXpPSZRdlLxyV3i>

NEXT STEPS

After setting up the connector follow the appropriate links below to continue with the configuration of the Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users (preferred option for Zoom Meetings is **All (Based on Native API)**, the users will be retrieved automatically)
- Filters (Zoom Meetings works with all filters except **XML Filter**)
- Targets
- Importer Settings

FACEBOOK WORKPLACE



ABOUT FACEBOOK WORKPLACE CONNECTOR

Workplace

Workplace is an enterprise connectivity platform developed by Facebook, Inc. and featuring tools like groups, instant messaging and News Feed.

- Workplace allows third parties to fetch data from its APIs for Compliance and eDiscovery purposes - this is achieved by using Custom Integrations. Custom Integrations are not available in the free Workplace plans, customers who need to meet Compliance and eDiscovery must have a Premium plan.

ACTIVITIES CAPTURED

- One-on-one Chats
- Group Chats
- Attachments in the chats
- Deleted messages in the chats (if only one chat participant has deleted the message)
- Deleted attachments in the chats (if only one chat participant has deleted the attachment)
- Emojis
- Deleted messages (if the message was deleted by one participant of the chat)
- Deleted attachments (if the attachment was deleted by one participant of the chat)
- Posts (except multi-company groups, and main posts of buy & sell groups)
- Polls (w/o attachments)
- GIFs
- Comments and replies (w/o attachments)
- Likes & reactions to posts
- Photos
- Format with Markdown posts (w/o formatting)
- Descriptions to albums and photos in albums
- Create Doc posts in txt format (w/o image)
- Create Events (only image)
- Live Videos
- Post edits
- Group leave event
- Group chat add event
- Comments & replies to photos in albums
- Previous versions of posts (except attachments)

SOURCES



Workplace

CUSTOM INTEGRATION CREATION IN WORKPLACE BY FACEBOOK

1. Login to workplace using a System Administrator account.
2. Navigate to <https://my.workplace.com/work/admin/apps/>
3. Sign In if prompted to.

4. Click **Create Custom Integration**.

The screenshot shows the Workplace Admin Panel's sidebar with various options like Home, Notifications, Chats, Admin Panel, and Integrations selected. The main area is titled 'Integrations' and shows a list of 'Custom Integrations' including 'NEW', 'M1-L Development', 'Merge1POC', and 'HexTese'. A prominent red box highlights the blue 'Create Custom Integration' button at the top right of the integration list.

5. Enter a name for the Integration and click **Create**.

The dialog box has fields for 'Name' (containing 'Sample') and 'Description' (containing 'Describe what your integration does'). Below the fields is a note about API terms. At the bottom are 'Cancel' and 'Create' buttons, with 'Create' being highlighted.

6. Copy the **App ID** and the **App Secret**. Click **Create Access Token** and copy the generated token.

The screenshot shows the 'Integration Details' page for 'Merge1 Sample'. It displays the 'Name' (Merge1 Sample), 'App ID' (466735440619587), 'App Secret' (redacted), 'Description' (Describe what your integration does), 'Enabled' (Yes), and 'Discoverable' (Yes) settings. A red arrow points from the 'App Secret' field to the 'Access Token' section at the bottom, which includes a 'Create Access Token' button.

SOURCES



Workplace

7. If **Discoverable** is set to **Yes**, change it to **No**. This is not required but it's best practice to make sure the users are not aware of existence of the application.

Integration Details
You can update details about this integration.

 Update Logo	Name Sample 249	App ID 435264643858898	Enabled Yes
Description Describe what your integration does	App Secret Show	Access Token Create Access Token	Discoverable No

8. Under **Integration Permissions**, enable the following permissions:

- Read group content
- Read user timeline
- Read all messages
- Read user email
- Read group membership

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.

Integration Permissions
Choose the permissions your integration will need access to.

<input checked="" type="checkbox"/> Read group content See content in groups, including files and posts	<input checked="" type="checkbox"/> Read user email See any group member's email address
<input checked="" type="checkbox"/> Read user timeline See posts made by group members on a user's timeline	<input checked="" type="checkbox"/> Read group membership See list of members in a group and list of groups for a user
<input type="checkbox"/> Manage user timeline Post and comment on any group member's timeline	<input type="checkbox"/> Mention Bot When mentioned in a post, see the post and reply to comments
<input type="checkbox"/> Manage group content Post and comment in groups	<input type="checkbox"/> Manage groups Add and remove group members
<input type="checkbox"/> Manage accounts Add and remove people from this Workplace community <input type="checkbox"/> Automatically invite people to Workplace as soon as they're added using this integration	<input type="checkbox"/> Message any member Send messages to any group member <input type="checkbox"/> Allow this integration to work in group chats.
<input checked="" type="checkbox"/> Read all messages See messages sent to anyone in the community	<input type="checkbox"/> Delete chat messages Delete messages from Workplace Chat
<input type="checkbox"/> Read security logs See security events such as login attempts and password requests	<input type="checkbox"/> Logout Log members out of all active sessions
<input type="checkbox"/> Create link previews See links added to posts in order to display previews for certain domains	<input type="checkbox"/> Read work profile See any group member's complete profile, including phone number, department and location
<input type="checkbox"/> Read org chart Check a group member's profile to see who they report to and anyone who reports them	<input type="checkbox"/> Manage work profiles Update any group member's profile details, including changing their manager
<input type="checkbox"/> Provision user accounts Add and remove people from Workplace, and delete any unused accounts	

Automatically remove unused permissions
To help keep your Workplace community secure we automatically review & remove permissions on an ongoing basis. Disable this if you don't want to automatically remove permissions for this integration.
[Learn more](#)

Off

SOURCES



Workplace

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 the certain groups.

Give Integration Access to Groups
The permissions you've selected above will apply to the groups you select.

All groups
This will install your integration in all groups on Workplace.

Let group admins enable for their groups
This will allow your integration to be installed in all groups on Workplace.

Specific groups
Select only certain groups on Workplace that will have access to this integration.

Search groups by name

9. Following best security practices, enable **Require App Secret Proof** and whitelist the public IP addresses of your Merge1 server(s), gateways and/or proxy server(s).

Security Settings
Additional settings that relate to security of the integration.

Require App Secret Proof
 Require app secret proof and app secret time for all API calls. It is recommended to enable this.

Server IP Whitelist
This enforces that all API calls must come from one of the whitelisted ip addresses. It is highly encouraged to configure this for sensitive apps.
[Empty input field]

SOURCES



FACEBOOK WORKPLACE CONNECTOR CONFIGURATION

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.

The screenshot shows the 'CONFIGURATION WIZARD' interface. At the top, there are tabs: SOURCE (which is selected), MONITORED USERS, FILTERS, TARGETS, and SETTINGS. Below the tabs, a note reads: 'Please provide the following credentials to your company's Facebook Workplace app so that Merge1 can be configured to access your monitored users' account data.' Another note below it says: 'If you do not have an app created for Facebook Workplace, please [click](#) for more information.' A section titled 'FACEBOOK WORKPLACE APPLICATION CONFIGURATION' contains three input fields: 'Application ID', 'Application Secret/Key', and 'Access Token'. At the bottom right of the wizard are 'BACK' and 'NEXT' buttons.

2. Click **Next**.

TIMESTAMP FORMATTING

In addition to the primary stamp, a second timestamp can be enabled with its timezone. 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 Datetime Format dropdown menu.

The screenshot shows the 'TIMESTAMP FORMATTING' configuration screen. It includes three main sections: 'Primary Time Zone' (set to '(UTC+04:00) Yerevan (CST)'), 'Secondary Time Zone' (checkbox is unchecked), and 'DateTime Format' (set to 'March 29 at 09:31 PM'). Each section has a dropdown arrow to its right.

SOURCES



Workplace

EXCLUDE FILE TYPES

- 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 this 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 shouldn't be downloaded can be specified in the following format: ex. txt,png,xml. The comma is used to separate the file types.

The screenshot shows the 'EXCLUDE FILES' configuration screen. It includes two main sections: 'Do not download files greater than' and 'File Types'. Each section has a 'Custom Message' field containing examples of how the messages will appear in the email body.

Do not download files greater than:

- Custom Message: This message will be added to the email body.
- Example: Files {0} are not imported, because they are greater than {1} megabyte
All the filenames that were excluded will be written instead of {0} symbol.
File size limit will be written instead of {1} symbol.

File Types:

- Custom Message: This message will be added to the email body.
- Example: Files {0} are not imported.
All the filenames that were excluded will be written instead of {0} symbol.
File types will be written instead of {1} symbol.

ADVANCED CONFIGURATION OPTIONS

- The **Subject Prefix** is added to the subject line of imported emails. For example, if entered subject prefix is "Facebook Workplace", the subject line will look as in the example below. This is useful for organizing imported data, i.e. when multiple sources share a common 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 04/17/2016 and the After is set to 08/25/2018 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.
- The **Auto Update** feature will ensure that the connector is updated to the latest version. Each time the Importer is run, it contacts Globanet server(s) and updates the connector if a newer version is available.

SOURCES



Workplace

Subject Prefix

Do not download data modified before:

Do not download data modified after:

Auto Update

Example output message:

Conversation:t_2291286460950612

John Doe <John2@domain.com>
To: ○ John Doe; ○ Ani LastName; ○ Jane; ○ Jadon Sancho

195 bytes

Thu 5/16/2019 12:37 PM

Yes No

John Doe
Created Date Time: May 16 at 12:36 PM CST
John created the group.

John Doe
Created Date Time: May 16 at 12:36 PM CST
John changed the group photo.

John Doe
Created Date Time: May 16 at 12:48 PM CST
Hi! Let's use Workplace chat to get work done, have quick discussions or keep in touch on the go.

Jane
Created Date Time: May 16 at 12:48 PM CST
Jane joined the group.

Jane
Created Date Time: May 16 at 12:49 PM CST
Hey - I'm online now, checking out Workplace.

NEXT STEPS

After setting up the connector follow the appropriate links below to continue with the configuration of the Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users (preferred option for Facebook Workplace is **All (Based on Native API)**, the users will be retrieved automatically)
- Filters (Facebook Workplace works with all filters except **XML Filter**)
- Targets
- Importer Settings

WEB PAGE CAPTURE



Web Page

ABOUT WEB PAGE CAPTURE CONNECTOR

Merge1 Web page capture connector captures the web pages. It captures a specific web page and the links on the page at a configurable through the connector 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

Please note:

Heavy pages with the depth of capture more than 1 may be captured not fully, as all the pages may not be loaded completely by the time of the capture.

SOURCES



Web Page

URLS CONFIGURATION

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 a JSON file specified in PhantomJS format should be uploaded.
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 connector captures the filled in website URL and all the pages that open from that URL and have the same URL in their URLs.

URLS CONFIGURATION

+ ADD CONFIGURATION GROUP

URLS GROUP -

Group Name *

Output Format * PDF file (.pdf)

URLS

WebSite URL

Capture Mode Full Domain

Depth 1

+

SOURCES



Web Page

MESSAGE CONSTRUCTION

As the messages generated by the Web Page Capture connector don't 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 connector is a mailbox

MESSAGE CONSTRUCTION

From Email Address *

To Email Address *

TIMESTAMP FORMATTING

In addition to the primary stamp, a second timestamp can be enabled with its timezone. 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 Datetime Format dropdown menu.

TIMESTAMP FORMATTING

Primary Time Zone

(UTC+04:00) Yerevan (CST)

Secondary Time Zone

Date Time Format

March 29 at 09:31 PM

SOURCES



Web Page

ADVANCED CONFIGURATION OPTIONS

- The **Subject Prefix** is added to the subject line of imported emails. For example, if entered subject prefix is "Web Page Capture", the subject line will look as in the example below. This is useful for organizing imported data, i.e. when multiple sources share a common target.
- The **Auto Update** feature will ensure that the connector is updated to the latest version. Each time the Importer is run, it contacts Globanet server(s) and updates the connector if a newer version is available.

ADVANCED CONFIGURATION OPTIONS

Subject Prefix

Auto Update

Example output message:

030304 - Donald Trump - Wikipedia

hex@mig2.local To vazg@m.g

Page.pdf 6 MB

Send as Adobe Document Cloud link Yes No

Mon 12/9/2019 11:23 AM

hex@mig2.local hex@mig2.local
Capture Date: 09/12/2019 11:22:43.439 CST
Capture Date: 09/12/2019 05:22:43.439 MST
Title: Donald Trump - Wikipedia
https://en.wikipedia.org/wiki/Donald_Trump

NEXT STEPS

After setting up the connector follow the appropriate links below to continue with the configuration of the Monitored Users, Filters, Targets, and Importer Settings.

- Monitored Users (not available for Web Page Capture)
- Filters
- Targets
- Importer Settings

MONITORED USERS

Monitored Users are individuals whose data is collected by Merge1.

There are four User Sources from where Monitored Users can be added to the Connector.

- **All (Based on Native API)**
- **Active Directory**
- **CSV File**
- **Manually Maintain the List**

ALL (BASED ON NATIVE API)

This option automatically imports the users of the Connector using its API. This works for Sources, that are connected to Merge1 by the API, like Slack eDiscovery.

EDIT MONITORED USERS X

SOURCE	MONITORED USERS	FILTERS	TARGETS	SETTINGS
ACCOUNT FILTER				
USER SOURCE CONFIGURATION				
<input checked="" type="radio"/> All (based on native API) <input type="radio"/> Active Directory <input type="radio"/> CSV File <input type="radio"/> Manually Maintain The List				
FILTER TYPE CONFIGURATION				
<input type="checkbox"/> Include 1 <input type="checkbox"/> Exclude 2				
<i>Now that you have told us where to gather your data, tell us whose data you want Merge1 to gather.</i>				
			CLOSE	SAVE

1. Include is used for providing a path to a CSV file with a list of users that haven't been retrieved via API for any reason and should be included in the Monitored Users.

2. Exclude is used for providing a path CSV file with the users that should not be monitored as opposed to "Include".

MONITORED USERS

ACTIVE DIRECTORY

Active Directory (AD) is a directory service that Microsoft developed for the Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services. If the users that need to be monitored are in AD and need to be added to the **Monitored List**, this is the option to choose. Active Directory option allows to retrieve a user list using LDAP. Once you choose that option, click on **Configure Active Directory** to set it up.

AD SEARCH X

LDAP PROPERTIES

Server Name	1
Base Domain	2
Port	3
User Name	4
Password	5
Search Scope	6
Search Filter	7 (ObjectClass=User)

SEARCH

SEARCH RESULTS

CANCEL **SAVE**

Here are the steps for setting up LDAP Server in order to import users.

1. In the **Server Name** field fill in the name of the LDAP Server.

MONITORED USERS

2. In the **Base Domain** field add the section of the directory where the search should begin.

For example: ou=finance,dc=example,dc=com.

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. 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.

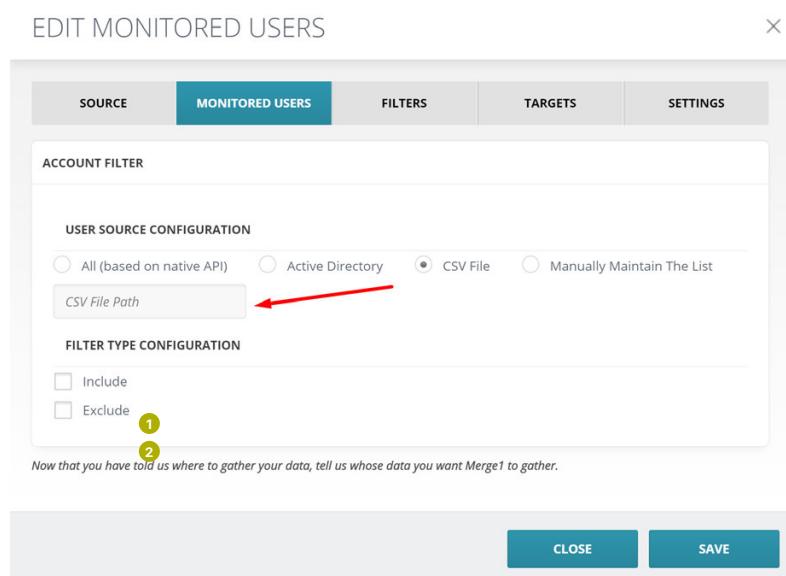
7. In **Search Filter** field add filters that can be used to restrict the number of users or groups

that are permitted to access an application.

Users who do not have the selected attribute or a Display Name will not be returned by the LDAP query.

CSV FILE

"CSV" file option allows to add our own CSV file based on which the monitored users will be added. The path to the CSV file should be added to the highlighted field.



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.

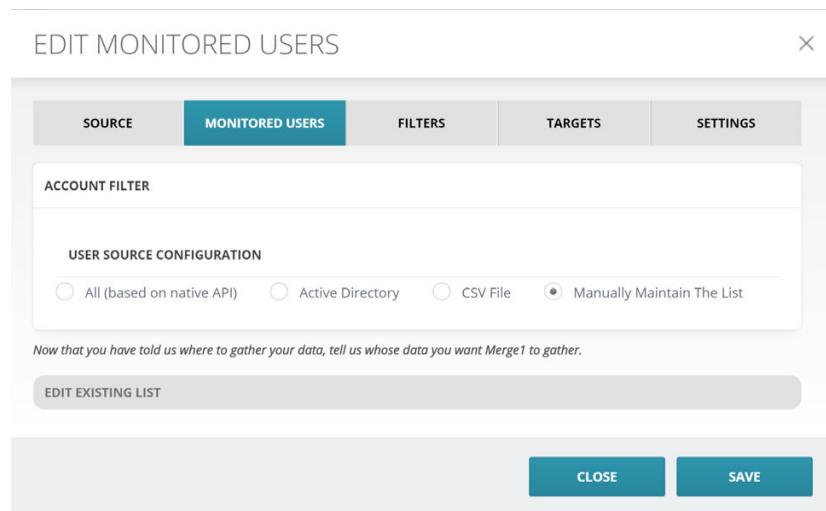
MONITORED USERS

1. Include is used for providing a path to a CSV file with a list of users that haven't been retrieved via API for any reason and should be included in the Monitored Users.

2. Exclude is used for providing a path CSV file with the users that should not be monitored as opposed to "Include".

MANUALLY MAINTAIN THE LIST

Manually Maintain the List allows to manually add and manage users.



After selecting this option, click on **Edit Existing List** to add and edit the settings of monitored users. Please note, that if previously another option for monitoring users was chosen, the new configuration should be Saved after switching to Manually Maintain the List.

	CORP EMAIL ADDRESS	DISPLAY NAME	MONITOR	SLACK EMAIL/ID
<input type="checkbox"/>	jsmith@globanet.com	Jsmith	<input checked="" type="checkbox"/>	jsmith@globanet.com

MONITORED USERS

1. **Add Monitored User** opens a window where you can add details of a user to be monitored.
2. **Delete Selected** removes selected users from the monitored list.
3. Conducts search in the list of existing users.
4. Select the user and click on **Delete Selected**. This will remove user/users the connector Monitored Users list.
5. Selects users.
6. Edits the information about an existing user.
7. If checked, monitors the user, if not, the user is not monitored.

To add a monitored user, click on Add Monitored User and fill in the necessary information. The same information can then be edited by clicking on Edit Monitored User.

EDIT MONITORED USERS

Please enter the information of the Monitored User that you would like to add.

SOURCE	MONITORED USERS	FILTERS	TARGETS	SETTINGS
--------	------------------------	---------	---------	----------

Corp Email Address

Display Name

Connector Email/ID

Monitor this user

+ ADD ANOTHER MONITORED USER

BACK **SAVE**

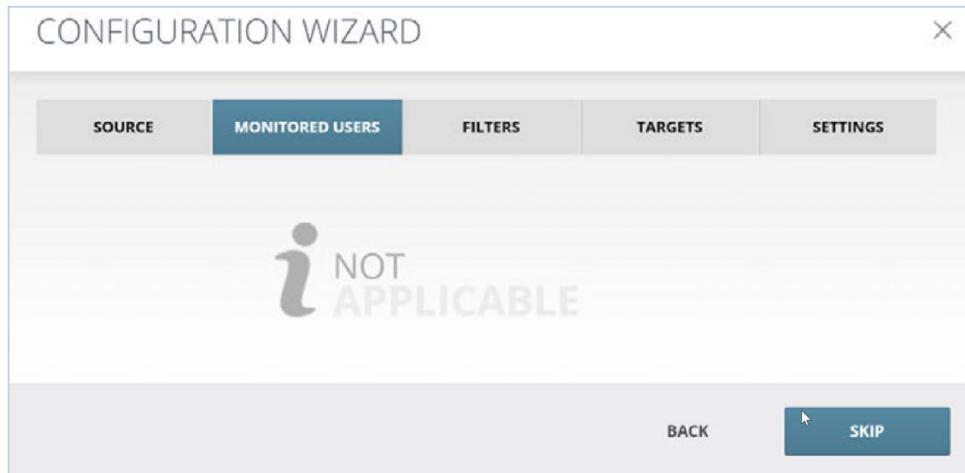
- **Corp Email Address** is a required field for the corporate email address of the user.
- **Display Name** is the name that will be displayed in the Monitored Users list.
- **Connector Email/ID** field is for the email or id of the user's Connector account.
- **Monitor This User** option if checked monitors the user and vice versa.

MONITORED USERS

SKIP MONITORED USERS

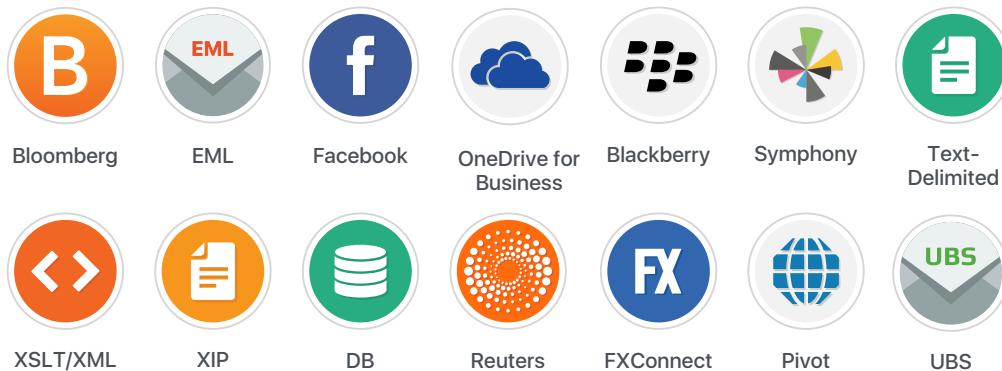
Please note:

Some of the Connectors 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**.

BELOW ARE THE CONNECTORS THAT DON'T HAVE MONITORED USERS



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.

1. Click on Add Filter

EDIT FILTERS X

SOURCE	MONITORED USERS	FILTERS	TARGETS	SETTINGS
--------	-----------------	----------------	---------	----------

Configure any needed data filters here.

+ **ADD FILTER**

2. Choose a **Filter Name** and **Filter Type**. Merge1 has five filter types:

- Active Directory Filter
- Keyword Filter
- Mail Filter
- XML Filter
- Message Size Filter

EDIT FILTERS X

SOURCE	MONITORED USERS	FILTERS	TARGETS	SETTINGS
--------	-----------------	----------------	---------	----------

NEW FILTER

Filter Name *

Filter Type * ▼

BACK ADD

Further you can find the detailed description of how to install each filter.

FILTERS

ACTIVE DIRECTORY FILTER

Please note:

That 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.

EDIT FILTERS

Active Directory Filter Configuration

SOURCE	MONITORED USERS	FILTERS	TARGETS	SETTINGS
Filter Rules				
Search Base	1			
Search Scope	2			
Search Filter	3	(<i>&(ObjectClass=User) (sAMAccountName=_PLACEHOLDER_)</i>)		
<input type="checkbox"/> User address search pattern	4			
Regular Expression	5	User address search pattern regular expression		
<input checked="" type="checkbox"/> Replace user address with LDAP attribute	6			
Replacement Attribute	7			
LDAP Properties				
LDAP Server	8			
Port	9	389		
User Name	10			
Password	11			
Caching Properties				
<input type="checkbox"/> Enable Caching	12			
Cached query count	13			
Cache update interval	14			
BACK		NEXT		

FILTERS

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 recordset (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 to skip 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 timeperiod 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.

FILTERS

KEYWORD FILTER

Keyword filter allows you to retrieve and refine the data by mentioned keywords and collect it in the specified target.

The screenshot shows the 'EDIT FILTERS' interface with the 'FILTERS' tab active. The 'Keyword Filter Configuration' section includes a 'Filter Name' field with the value 'Filter', a 'Filter Type' field set to 'Keyword Filter', and a 'Keywords (Comma separated)' field containing '1'. A 'Case Sensitive' checkbox is checked. Navigation buttons 'BACK' and 'NEXT' are at the bottom.

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" won't be filtered.

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 Merge1 can be static and dynamic.

Static Filter allows to upload a CSV file with email addresses that will be used for filtering. Click on 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.

The screenshot shows the 'EDIT FILTERS' interface with the 'FILTERS' tab active. The 'Mail Filter Configuration' section includes a 'Filter Name' field with the value 'Mail Filter', a 'Filter Type' field set to 'Mail Filter', and a 'FILTER TYPE' section with a 'Static' radio button selected. It also features an 'user@domain.com' input field with a '+' button and an 'ADD FROM CSV' button. Navigation buttons 'BACK' and 'NEXT' are at the bottom.

FILTERS

Dynamic Filter is used to specify email addresses dynamically from an LDAP server or from a CSV file. 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.

The screenshot shows the 'Edit Filters' interface with the 'FILTERS' tab selected. The 'Mail Filter Configuration' screen is displayed. The 'FILTER TYPE' section is active, showing the following fields:

- LDAP Server (1)
- Port (2)
- Account (3)
- Password (4)
- Search Base (5)
- Search Scope (6) - dropdown menu set to 'Base'
- Search Filter (7) - input field containing '(ObjectClass=User)'

At the bottom are 'BACK' and 'NEXT' buttons.

Here are the steps for setting up LDAP Server in order to set up Dynamic Filter.

1. In the **LDAP Server** field fill in the name of the LDAP Server.
2. In the **Port** field define the Port of the LDAP Server.
3. In the **Account** field add the username of the LDAP account.
4. In the **Password** field fill in the corresponding password to the LDAP account for signing in.
5. **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.
6. **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.
7. 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.

FILTERS

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.

EDIT FILTERS

SOURCE	MONITORED USERS	FILTERS	TARGETS	SETTINGS
--------	-----------------	----------------	---------	----------

Mail Filter Configuration

Filter Name * Filter Type

FILTER TYPE

Static Dynamic Active Directory CSV

FILTER BASED ON THE FOLLOWING FIELD(S)

From To
 CC BCC

BACK **NEXT**

MESSAGE SIZE FILTER

Message Size Filter allows filtering messages to a different target based on their size. If the message size exceeds the set size in the Message Size Filter the messages will be sent to a selected corresponding target.

EDIT FILTERS

SOURCE	MONITORED USERS	FILTERS	TARGETS	SETTINGS
--------	-----------------	----------------	---------	----------

Message Size Filter Configuration

Filter Name * Filter Type

Filter messages larger than MB

BACK **NEXT**

In the Filter messages larger than field the size of messages should be entered, in order for the messages that exceed that size will be filtered.

FILTERS

XML FILTER

XML filter allows to filter through XML source data with tags and their specific values.

EDIT FILTERS

Xml Filter Configuration

Filter Name * Filter Type

ADD TAG AND VALUE

1 + 2 **ADD FROM CSV**

HEADER

3 REMOVE ALL

BACK **NEXT**

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 on the activated Plus button.
2. If you don't want to input each tag and its value manually, upload a CSV file that includes tags and their values. Click on **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 "MessageOrigin Country - USA". See example below:

HEADER

MessageOriginCountry USA REMOVE ALL

Please 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.

Please note:

This filter works only with XML Sources, like Bloomberg, Symphony, and others.

TARGETS

After filling in all the information related to the Filters, click **Next** and you will be redirected to Targets tab. You can either fill in the Targets or skip it and fill later from the Importer Panel under the Configurations.

EDIT TARGETS

SOURCE **MONITORED USERS** **FILTERS** **TARGETS** **SETTINGS**

Please tell us where you want Merge1 to deliver your data.

ADD DEFAULT TARGET

Click **Add Default Target** and you will be redirected to the Target screen:

SOURCE **MONITORED USERS** **FILTERS** **TARGETS** **SETTINGS**

NEW TARGET

Target Name *

Target Type *

Fill in the Target Name and select the target type from the drop-down menu.

Please note:

These are mandatory fields.

When you have selected the exact target you wish to configure click **Next**.

TARGETS

Merge1 offers ten types of targets:

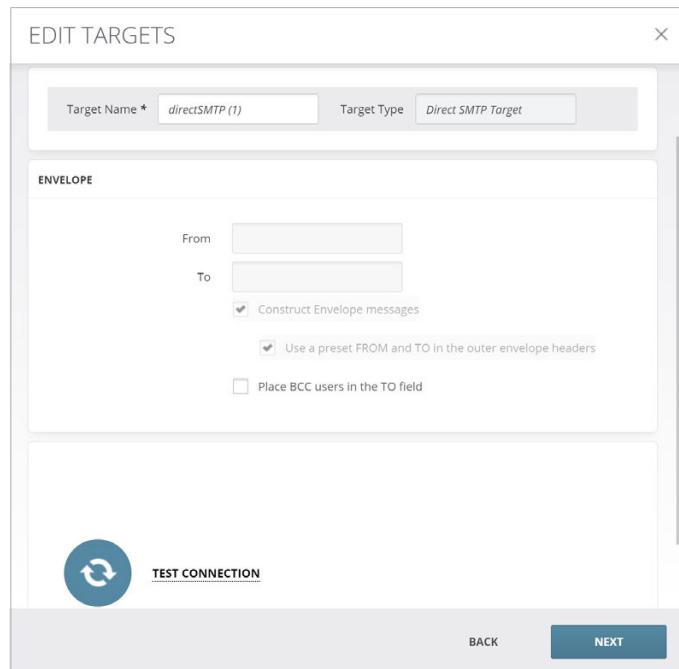
- **Direct SMTP Target**
Delivers data to an SMTP server address directly from the server.
- **EV Server**
Archives data in an Enterprise Vault archive.
- **EWS Server**
Delivers data to an Exchange Web Services server.
- **Failed Target**
Lists all imports as failed delivery attempts.
- **Folder Target**
Delivers data in EML or MSG format to specified folder.
- **Ignored Target**
Ignored target is used to mark all items sent to it as Ignored.
- **NSF Server**
Delivers data to a Domino Server in Notes State Facility format.
- **Office 365 EWS**
Delivers data to an Exchange Web Services server.
- **Report Target**
Prints the output of the data inside the log file, usually used for diagnostics.
- **SMTP Target**
Delivers data to an **SMTP** server address using a relay.
- **Google Vault Target**
Delivers data to **Google Vault**.

TARGETS

DIRECT SMTP TARGET

Direct SMTP Target allows Merge1 to deliver the processed messages directly to the recipient's SMTP server without requiring to relay 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 Connector.



1. Specify the sender SMTP address that you want to use in the **From** field. It is advisable to use an existing email address so the emails won't be spammed.
2. Specify a destination email address in the **To** field.
3. When you have filled in all the fields click **Next** button.
3. When Place BCC users in the TO field is selected, the BCC emails of the message will be added to the TO field.

Congratulations! You have successfully setup the Direct SMTP target.

TARGETS

ENTERPRISE VAULT TARGET

The EV Target requires the Enterprise Vault API Runtime (11 or above) installed on the machine hosting Merge1. The EV server's administrator account must be provided as the Log On Account in the [Importer's settings](#).

The screenshot shows the 'EV PROPERTIES' configuration screen. At the top, there is a field for 'SQL Server' with a 'CONNECT' button below it. Below this are dropdown menus for 'Site', 'Destination Server', 'Destination Vault Store', 'Destination Archive', and 'Retention Category'. At the bottom, there is an 'INDEX PROPERTIES' section with three input fields: 'Set', 'Name', and 'Value', and a 'REMOVE ALL' button.

1. To set up an EV target enter the instance name or IP address of the server that hosts your EV Directory SQL Database 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:
 - Site
 - Destination Server
 - Vault Store
 - Archive
 - Retention Category

Please note:

Merge1 6.0 officially supports Domino Journal, Journal Archive and SMTP archives, however, most other archive types are usually compatible as well.

3. When you have filled in all the fields click **Next**.

Congratulations! You have successfully setup the EV target.

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.

NOTE

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-KVSMimeType header, find and enable the option on the Settings page (not to be confused with [Importer Settings](#)).

TARGETS

EXCHANGE WEB SERVER TARGET

If you choose EWS Target Merge1 will deliver the data to the Exchange Web Services server you have chosen. Below you can find information on how to setup the EWS Target for your Connector.

The screenshot shows the 'DESTINATION MAILBOX' configuration interface. It includes fields for SMTP Address, Impersonator, Password, and a checkbox for 'Use Exchange Personal Archive'. Below these are fields for Default Sender (set to 'Merge1') and Timeout (set to 0 ms). A large blue 'CONNECT' button is centered. At the bottom, there's a dropdown for Target folder (set to 'Inbox') and a checkbox for 'Construct envelope messages'.

1. Enter the SMTP address in the relevant field.
2. Provide the Impersonator information and password of the target Exchange Web Services account.
3. Specify a Default Sender address for emails with empty **FROM** fields (EWS rejects such emails).
4. Click **Connect** to get the folder list.
5. Specify a Target folder for imported data.
6. When you have filled in all the fields click **Next**.

Please note

When checking the **Use Exchange Personal Archive** check-box you will enable Merge1 to import data to the Personal Archive folder of the Target folder.

When checking the **Construct Envelope Message** box you will enable Merge1 to import data in MS Exchange journal report format (the X-MS-journal-report header is also added)

Congratulations! You have successfully setup the EWS target.

TARGETS

MICROSOFT OFFICE 365 EWS TARGET

If you choose Office 365 EWS Target, Merge1 will deliver the data to EWS in Microsoft Office 365 (in the cloud). Below you can find information on how to setup the Office 365 EWS Target for your Connector.

DESTINATION MAILBOX

UserName

Password

Use Exchange Personal Archive

Default Sender

1. Enter the Username and Password of the target Exchange Web Services account.
2. Specify a Default Sender address for emails with empty FROM fields (EWS rejects such emails).
3. When you have filled in all the fields click the **Next** button.

Please note:

When checking the Use Exchange Personal Archive box you will enable Merge1 to import data to the Personal Archive folder of the Target folder.

Congratulations! You have successfully setup the Microsoft Office 365 EWA target.

TARGETS

SMTP TARGET

If you choose a SMTP Target, Merge1 will deliver the data to an SMTP server address you provide. Below you can find information on how to setup the SMTP Target for your Connector.

The screenshot shows the configuration interface for an SMTP Target. It consists of three main sections:

- ENVELOPE**: Contains fields for "From" and "To", and checkboxes for "Construct Envelope messages" (checked), "Use a preset FROM and TO in the outer envelope headers" (unchecked), and "Place BCC users in the TO field" (unchecked).
- MAIN SETTINGS**: Contains fields for "SMTP Server" and "Port" (set to 25, with a note "Default: 25").
- AUTHENTICATION ENCRYPTION**: Contains checkboxes for "Use SSL Encryption" (unchecked), "Implicit" (unchecked), "Use TLS Encryption" (unchecked), and "Supply username and password" (unchecked). It also includes fields for "Username" and "Password" and a "TEST CONNECTION" button.

1. Specify a destination email address in the To field and a return address in the From field.

2. Enter the SMTP Server address and port. (the default port number is 25).

3. Click **Test Connection** to check the connection and to insure that your settings are accurate.

4. When you have filled in all the fields click the **Next button**.

Note: SMTP Target is not recommended for delivering messages to Exchange Online Mailboxes, due to various throttling policies set by Microsoft, also Exchange Online does not accept Journal Envelope messages , this can result in loss of original message time stamps and other metadata.

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.

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.

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.

Please note:

- When checking the Construct Envelope Messages box you will enable Merge1 to import data in MS Exchange journal report format (the X-MS-Journal header also be added).
- When checking the Place BCC users in the TO field box you will enable Merge1 to move all BCC recipients to the TO field.
- **Encryption:** SSL and TLS encryption settings should match those of the target SMTP server.

TARGETS

REPORT TARGET

The Report Target is used to check whether or not data can be analyzed successfully. The Importer will list certain details for viewing in its activity logs. The complete header option includes subject lines, and everything includes complete headers as well as the messages themselves.

LEVEL

- None
- Subject only
- Complete header
- Everything

1. Select the relevant level

2. Click Next.

Congratulations! You have successfully setup the Report target.

TARGETS

FOLDER TARGET

If you choose Folder Target, Merge1 will deliver the data to the specified folder in EML or MSG formats. Below you can find information on how to setup the Folder Target for your Connector.

OUTPUT FOLDER

The screenshot shows the 'OUTPUT FOLDER' configuration for a 'Folder Target'. At the top, there are two input fields: 'Target Name *' containing 'Folder' and 'Target Type' containing 'Folder Target'. Below these, under the heading 'OUTPUT FOLDER', there is an 'Output Folder' field containing 'C:\Users\Christina\Desktop\M' and a checked checkbox for 'Create Folder Per Session'. Under the heading 'FILE FORMAT', there are two radio buttons: 'EML' (which is selected) and 'MSG'.

1. Select the output folder, to where the exported messages will be sent.
2. Specify the format of the exported message, EML or MSG. See the difference between two file types below.

EML	MSG
EML is the extension supported by multiple e-mail clients like Outlook Express, Thunderbird, Windows Live mail.	MSG is the extension supported by Microsoft Outlook.
.eml file can be read by its E-mail client along with other. Like Outlook can read .eml files.	.msg file can only be saved for e-mails and messages.
.eml files can be opened in a text editor as are similar to text files.	.msg files can only be opened by MAPI based applications.

TARGETS

You can easily convert your .msg file into an .eml file as there could be possibilities where you want to view an .msg file but you do not have MS Outlook to open it. MSG files are client dependent because they are a proprietary message for Outlook whereas, EML is a text based file representing a message. Therefore, having single messages stored in EML rather than an MSG file proves more beneficial for the users, due to its flexibility.

3. Create Folder Per Session if checked will create a separate folder for each time the Importer is run, named after the date and time of the run.

Name	Date modified	Type	Size
2018-10-25_12.29.45	10/25/2018 12:29	File folder	
2018-10-25_13.45.22	10/25/2018 1:45 P	File folder	

Congratulations! You have successfully setup the EWS target.

Please note:

The service account that runs the service should have read/write permission for the specified folder.

ENVELOPE

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.

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.

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.

ENVELOPE

From	<input type="text"/>
To	<input type="text"/>
<input checked="" type="checkbox"/> Construct Envelope messages	
<input type="checkbox"/> Use a preset FROM and TO in the outer envelope headers	
<input type="checkbox"/> Place BCC users in the TO field	

TARGETS

DOMINO (NSF) SERVER

If you choose a Domino (NSF) Target, Merge1 will deliver the data to a Domino Server in Notes State Facility format. Below you can find information on how to set up the Domino Target for your Connector.

NOTES DATABASE CONFIGURATION

Domino Server

Database Name

Password

CONNECT

Folder ▾

Temporary Folder

- 1.** Enter the Domino Server Name.
- 2.** Next, provide Database Name and Password of the target database.
- 3. Connect.** After successfully connecting you will be able to see the Folder list.
- 4.** Choose the folder for imported data.
You can also provide a file path for the **Temporary Folder**. Merge1 will process message attachments here and delete them later.
- 5.** When you have filled in all the fields click **Next**.

Congratulations! You have successfully setup the NSF Server target.

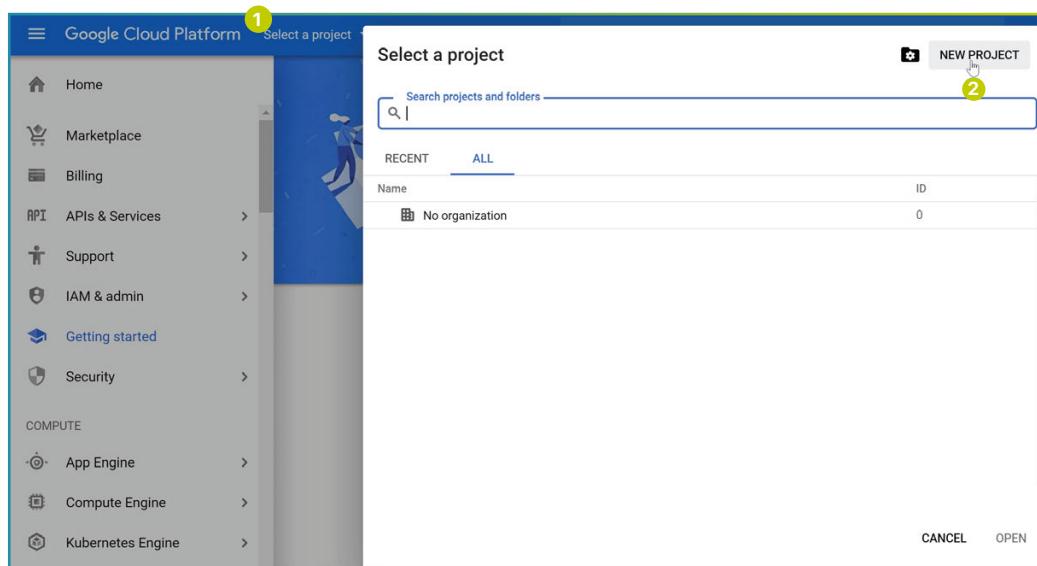
TARGETS

GOOGLE VAULT TARGET

Before configuring the Google Vault Target in the Merge1 UI, 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**.



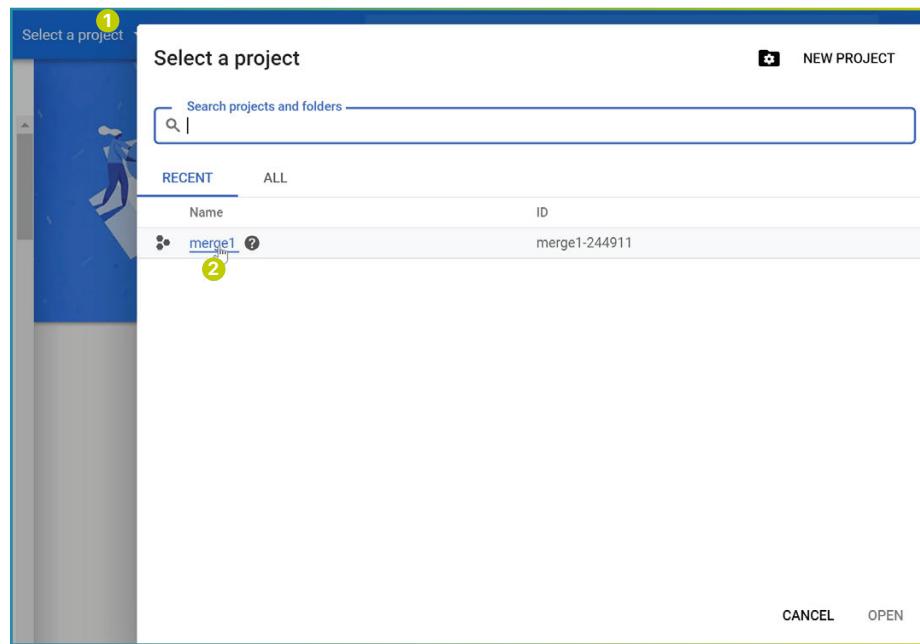
2. Enter a name for the project (example: merge1) and click **CREATE**.

The screenshot shows the 'New Project' dialog box. At the top left is the title 'New Project'. Inside the dialog:

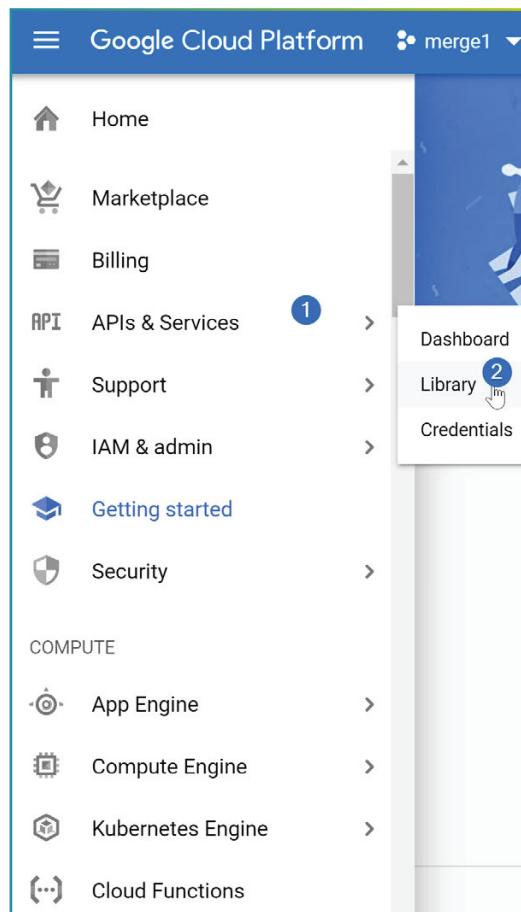
- A yellow warning icon with the text: 'You have 12 projects remaining in your quota. Request an increase or delete projects. [Learn more](#)'.
- A 'MANAGE QUOTAS' link.
- A 'Project name *' field containing 'merge1'.
- A note below the project name: 'Project ID: merge1-244911. It cannot be changed later. [EDIT](#)'.
- A 'Location *' section with a 'No organization' dropdown and a 'BROWSE' button.
- A note below the location: 'Parent organization or folder'.
- At the bottom are two buttons: a blue 'CREATE' button with a hand cursor icon, and a white 'CANCEL' button.

TARGETS

3. Once the Project is created click **Select a project**, then click on the project name (example: merge1).

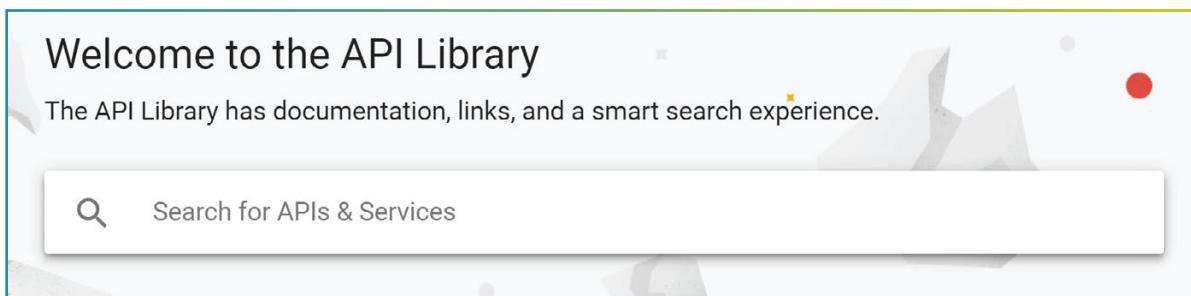


4. Mouseover **APIs & Services** then click on **Library**.

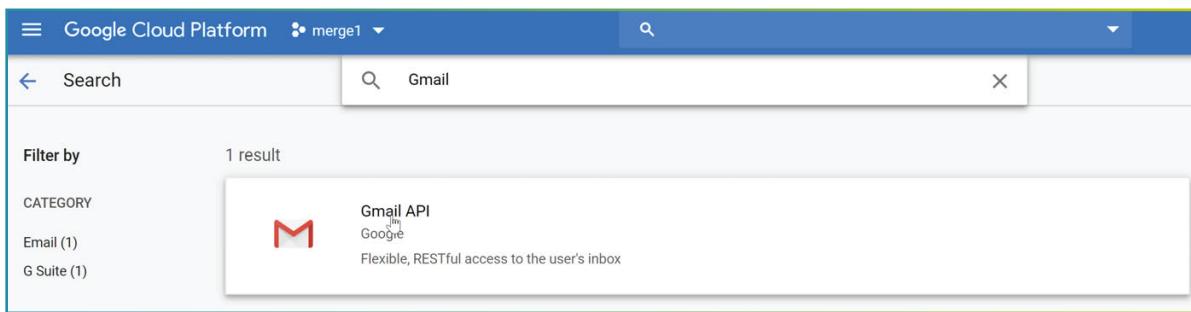


TARGETS

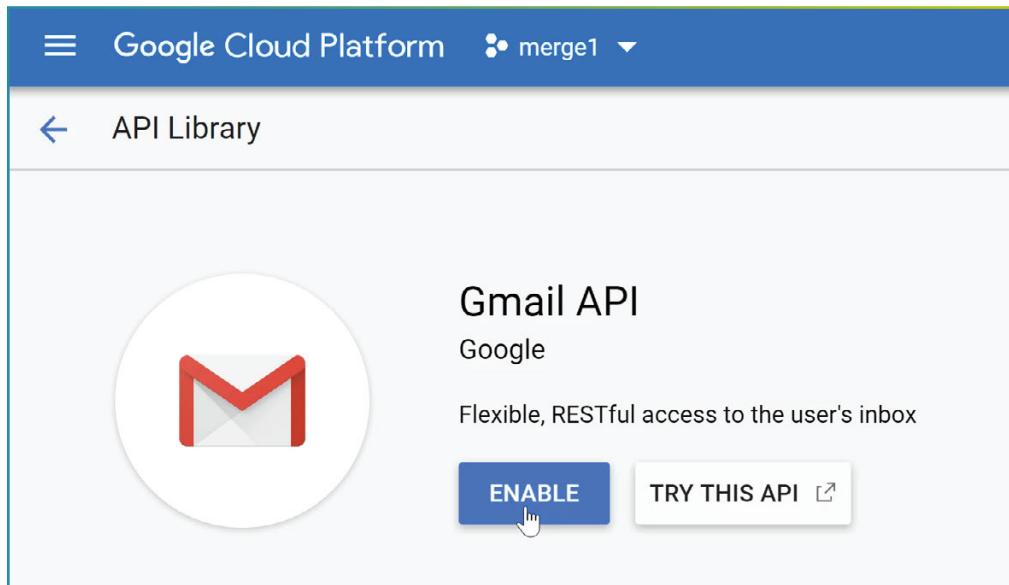
5. In the **Search for APIs & Services** search box type **Gmail**.



6. Click on **Gmail API**.

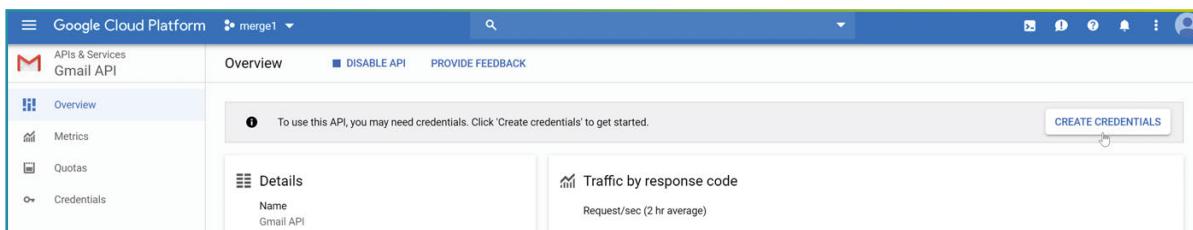


7. Once you're in the Gmail API page, click **ENABLE**.

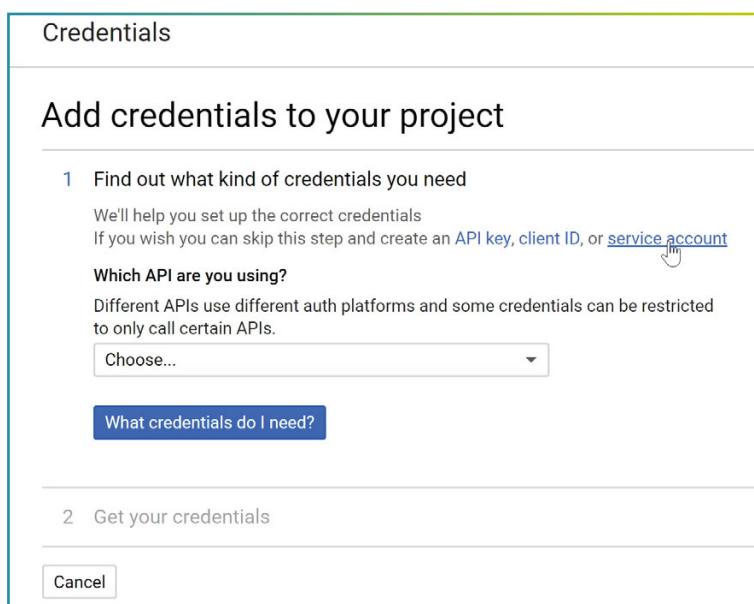


TARGETS

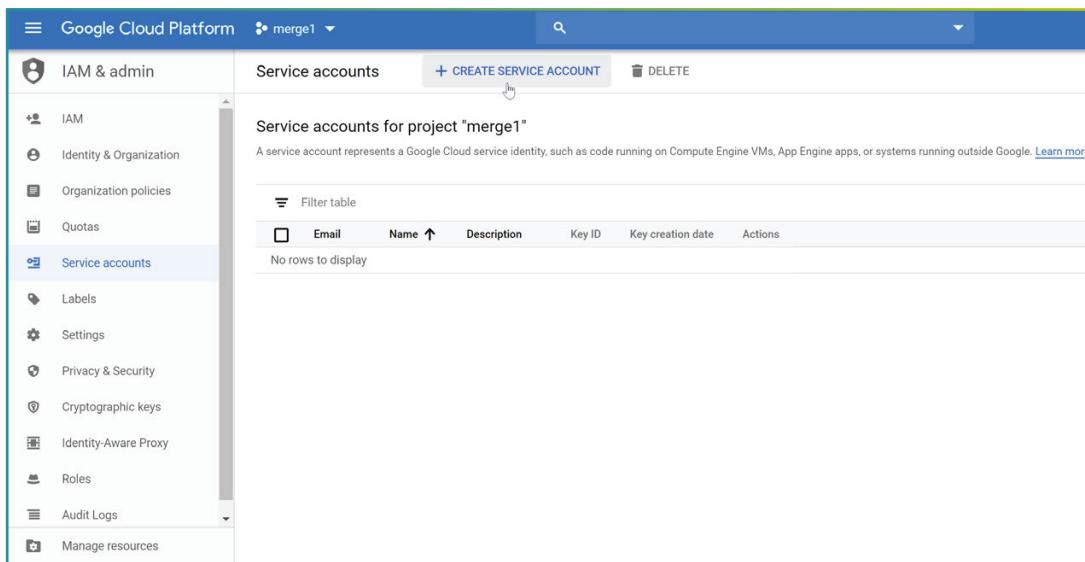
8. Click **Create Credentials**.



9. Click **Service account**.

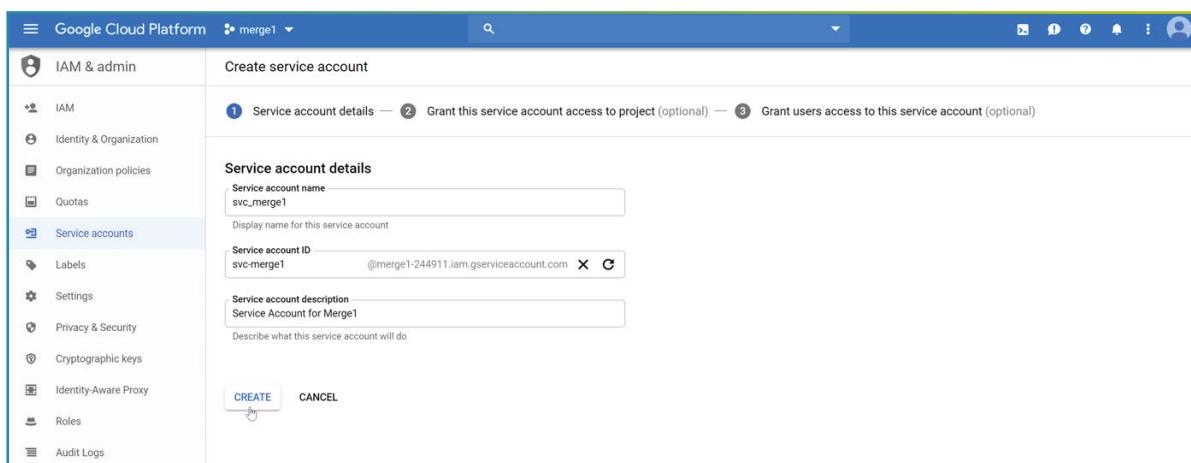


10. Click **+ CREATE SERVICE ACCOUNT**.

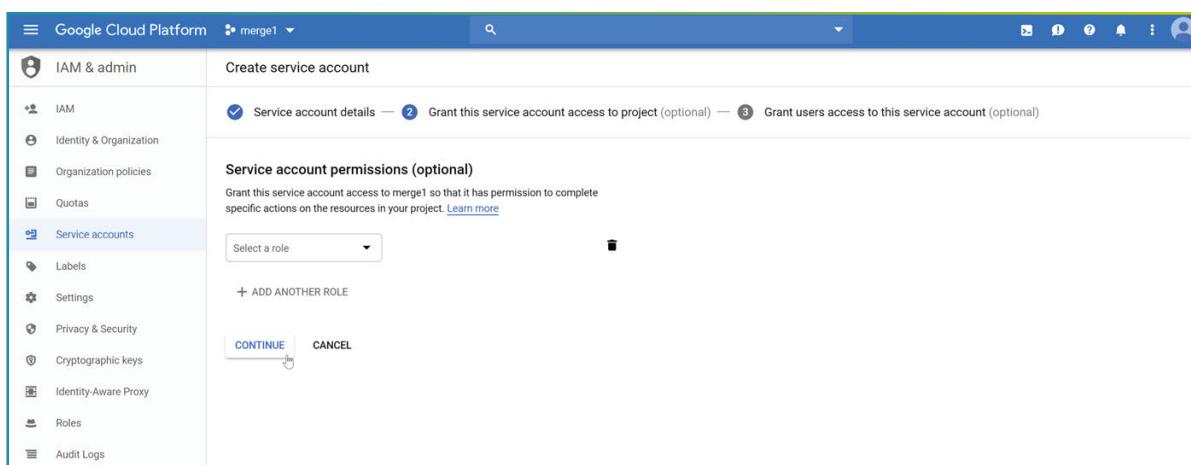


TARGETS

11. Click **Create Credentials**.



12. Click **+ CREATE SERVICE ACCOUNT**.



TARGETS

13. Click **CREATE KEY**.

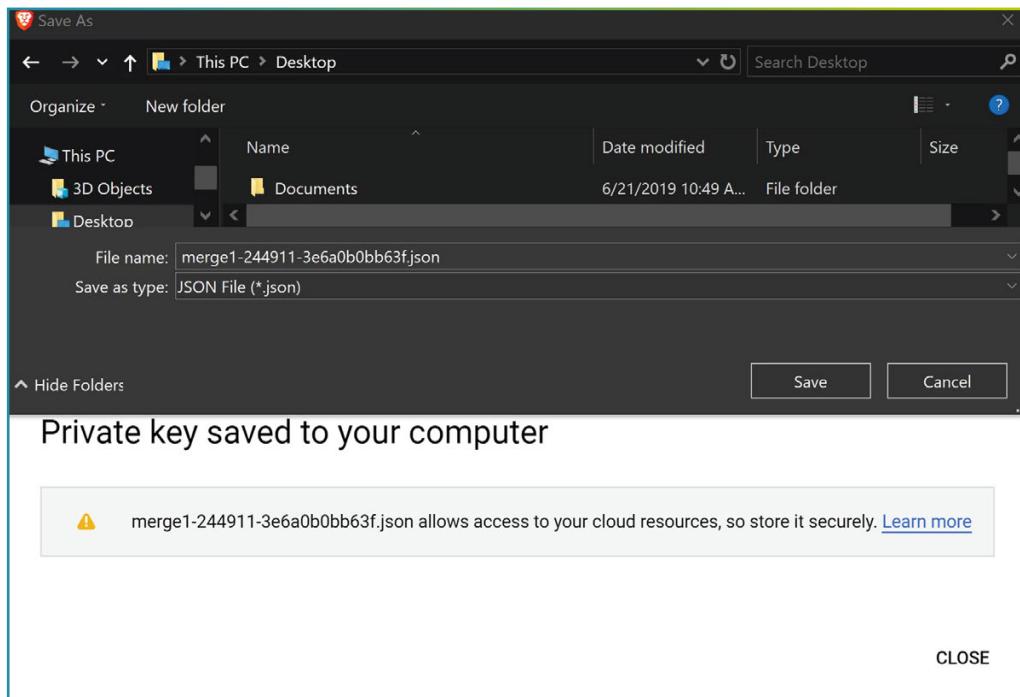
The screenshot shows the Google Cloud Platform interface. The top navigation bar includes the 'Google Cloud Platform' logo, a dropdown for 'merge1', and a search bar. On the left, a sidebar under 'IAM & admin' lists various services: IAM, Identity & Organization, Organization policies, Quotas, Service accounts (which is selected and highlighted in blue), Labels, Settings, Privacy & Security, Cryptographic keys, Identity-Aware Proxy, Roles, and Audit Logs. The main content area is titled 'Create service account' with a sub-section 'Grant users access to this service account (optional)'. It contains two roles: 'Service account users role' (with a description 'Grant users the permissions to deploy jobs and VMs with this service account') and 'Service account admins role' (with a description 'Grant users the permission to administer this service account'). Below these is a section titled 'Create key (optional)' with a note about storing the private key securely. A blue button labeled '+ CREATE KEY' is visible, with a hand cursor icon indicating it is clickable. At the bottom of the form are 'DONE' and 'CANCEL' buttons.

14. Select **JSON** and click **CREATE**.

The dialog box is titled 'Create key (optional)'. It contains a note about downloading the private key and storing it securely. Two radio buttons are shown for 'Key type': 'JSON' (selected and highlighted with a yellow circle labeled '1') and 'P12' (with a note 'For backward compatibility with code using the P12 format'). At the bottom are 'CREATE' and 'CANCEL' buttons, with a hand cursor icon over the 'CREATE' button, indicating it is the next step to be clicked. A yellow circle labeled '2' is placed over the 'CREATE' button.

TARGETS

15. Once the key is created, you should get prompted to save the file on your computer, save it somewhere secure, you'll need it when configuring Merge1.

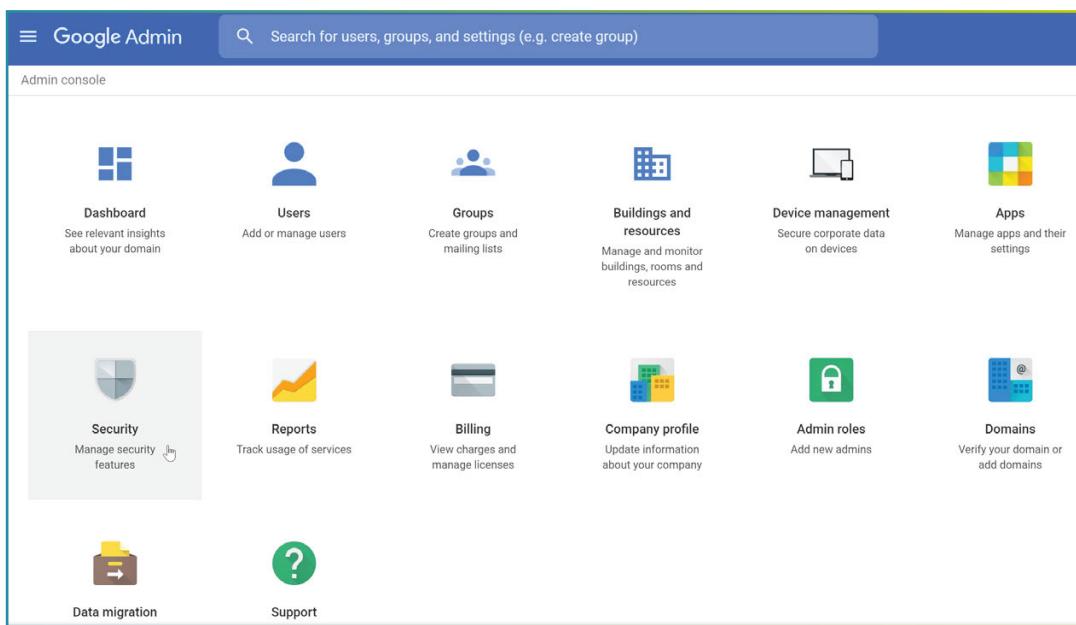


16. Click **DONE**.

A screenshot of the Google Cloud Platform 'IAM & admin' service account creation interface. On the left, there is a sidebar with options: IAM, Identity & Organization, Organization policies, Quotas, Service accounts (which is selected), Labels, Settings, Privacy & Security, Cryptographic keys, Identity-Aware Proxy, and Roles. The main area is titled 'Create service account' and contains a section for 'Create key (optional)' with a note about storing the private key securely. It shows a 'Key ID' field containing '3e6a0b0bb63f6dad09be43ed9cc0245eb7793615' and a '+ CREATE KEY' button. At the bottom, there are 'DONE' and 'CANCEL' buttons.

TARGETS

17. To grant permissions to the application, go to <https://admin.google.com> and click **Security**.



18. Scroll down and click **Advanced settings**.

A screenshot of the "Advanced settings" section in the Google Admin console. The section is titled "Set up single sign-on (SSO)" and includes a description: "Setup user authentication for web based applications (like Gmail or Calendar)". Below this is the "Context-Aware Access (Beta)" section, which includes a description: "Use device and user identification to manage access levels and enforce access policies for G Suite applications". Next is the "Google session control" section, with a description: "Set session duration for Google core and additional services, such as Gmail and Docs". Then comes the "Advanced settings" section, with a description: "Manage advanced security features such as authentication, and integrating G Suite with internal services". A small "Edit" icon is shown next to this section. Finally, there are two more sections: "Security and privacy resources" (with a description: "Get more information about security and privacy") and "API Permissions" (with a description: "Manage scope for API permissions").

TARGETS

19. Click **Manage API client access**.

The screenshot shows the 'Advanced settings' section of the Google Admin interface. Under the 'Authentication' tab, the 'Manage API client access' option is selected. A tooltip for this option states: 'Allows admins to control access to user data by applications that use OAuth protocol.' The entire screenshot is enclosed in a green border.

20. Open the key file that you saved in step 15 and copy the value of **client_id**, then paste it in the **Client Name** box shown below.

One or More API Scopes enter <https://www.googleapis.com/auth/gmail.insert>, then click **Authorize**.

The screenshot shows the 'Manage API client access' page. It displays a table with one row. The first column is 'Client Name' with the value '108805779875109015153'. The second column is 'One or More API Scopes' with the value 'https://www.googleapis.com/auth/gmail.insert'. The third column is 'Authorize' with a button. A tooltip for the 'One or More API Scopes' field says: 'Example: http://www.google.com/calendar/feeds/ (comma-delimited)'. The entire screenshot is enclosed in a green border.

21. That's it, you can now start configuring Merge1's Google Vault target.

The screenshot shows the 'Manage API client access' page after changes have been saved. A yellow banner at the top right says 'Your settings have been saved.' The table now has two rows. The first row is identical to the previous screenshot. The second row is for '108805779875109015153'. The 'One or More API Scopes' field now contains 'Email (Insert/Import messages)' followed by 'https://www.googleapis.com/auth/gmail.insert'. The 'Authorize' button is present in this row. A tooltip for the 'One or More API Scopes' field says: 'Example: http://www.google.com/calendar/feeds/ (comma-delimited)'. The entire screenshot is enclosed in a green border.

TARGETS

GOOGLE VAULT CONFIGURATION

1. Upload JSON file saved in the step 15 of the previous section by clicking on **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 on **Send Test Email** to test the connection to the target.

SERVICE ACCOUNT KEY

Credentials JSON file*	<input type="button" value="SELECT"/>	<input type="button" value="DOWNLOAD"/>
Destination mailbox*	<input type="text"/>	
Mark messages as deleted	<input type="checkbox"/>	
<input type="button" value="SEND TEST EMAIL"/>		

5. You can download the uploaded JSON file by clicking on **Download**. It is active only when there is a JSON file to download.

SERVICE ACCOUNT KEY

Credentials JSON file*	<input type="button" value="SELECT"/>	<input type="button" value="DOWNLOAD"/>
Destination mailbox*	<input type="text"/>	
Mark messages as deleted	<input type="checkbox"/>	
<input type="button" value="SEND TEST EMAIL"/>		

TARGETS

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 button Default. Click on it and your Alternative Target will become your default and it will be listed under the Alternative Targets.

EDIT TARGETS

Please tell us where you want Merge1 to deliver your data.

SOURCE	MONITORED USERS	FILTERS	TARGETS	SETTINGS
DEFAULT TARGET EVServer X				
ADD ALTERNATIVE TARGET				
NSF Server X				
Microsoft Office 365 EWS X				
SMTP Targe X				
ReportTarget X				

After filling in all the information related to the Targets, please click **Next** and you will be redirected to Importer Settings tab.

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:

- Log on account
- Reporting
- Message Header
- Logging
- Alerting
- Importer Schedule
- Filtering
- Processing
- Advanced Config Options

LOG ON ACCOUNT

Importer requires the host's or server's Service Account for certain permissions (such as EV administrator permissions). The service account username and password must be specified here.

LOG ON ACCOUNT (EMPTY FOR LOCALSYSTEM)

Service Account

Password

SAVE

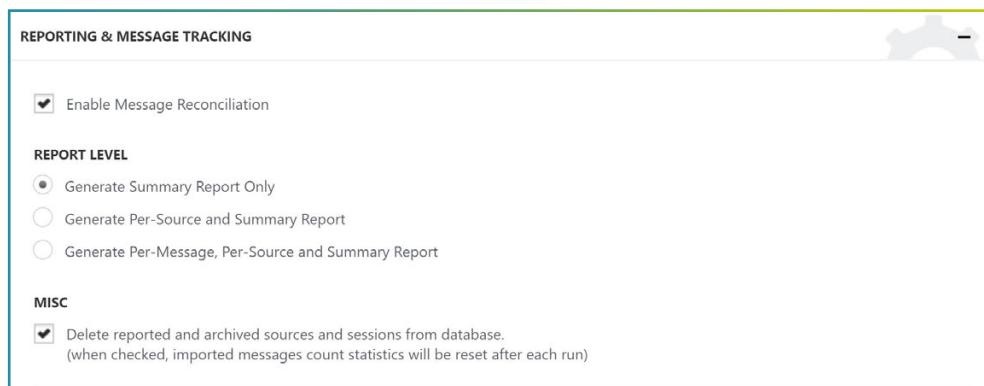
1. Provide Service account name and password

2. Click **Save**.

IMPORTER SETTINGS

REPORTING & MESSAGE TRACKING

The following section of the Importer Settings refers to email reports, which may be used to deliver statistical information (also viewable on the Dashboard) via email.



ENABLE MESSAGE RECONCILIATIONS

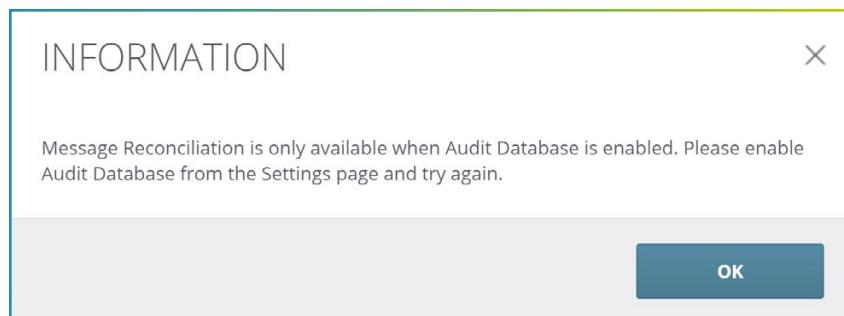
Merge1 imported messages have headers that can be found in message properties. When this option is enabled two following message headers are added to the generated message:

X-Merge1-Reconciliation-Id. This header is provided by the connectors and corresponds to the id of the message in the source. In case of EWS connector it is the ID retrieved from Exchange server mailboxes. Currently, only EWS connector sets this header. If the Reconciliation Id is not set by the connector, this header clones the Message-ID header value, which, in turn is generated by Merge1 for each unique message.

X-MessageSource. Each connector sets its own value for this header. For example, EWS connector sets the value of mentioned header using the user mailbox and mailbox folder name in the following format: Mailbox:Foldername.

These headers are both in an embedded message and in an enveloped message. Enveloped message has a different Message-ID from the embedded message. The Reconciliation Id remains the same for both an embedded message and an enveloped message.

The Enable Message Reconciliation can be enabled only when Audit DB is configured. Otherwise, the following pop-up will appear:



IMPORTER SETTINGS

REPORT LEVEL

A. 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 include the number of unprocessed, quarantined, failed, and imported sources. Message Statistics include 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, such as Bloomberg, Symphony, IceChat, Text-Delimited, and others. The per message report in addition to the reports described above is generated only in case a message has failed.

Detailed reports are longer and take more time to read. Reports exceeding 5 MB are shortened.

Reports are different from connector to connector, based on the activities that can be captured from them.

B. MISC: By enabling the **Delete Reported and Archived Sources and Sessions From Database** option, information will be deleted from the database when reports are sent. Deleted figures will no longer appear in the Reports section of the Dashboard.

The screenshot shows the 'EMAIL REPORT SETTINGS' configuration page. It includes fields for SMTP Server (25), Server Authentication (Username and Password inputs), SSL options (Use SSL, Implicit), and basic message fields (Sender Name, Message Subject, Sender Email, Recipient Email). A prominent blue button labeled 'SEND TEST EMAIL' is located at the bottom right.

C. Email Report Settings: Enable reporting by providing an SMTP server address.

D. Message Subject: Enter the subject for the report message.

E. Sender Name/Email: This information will appear in the FROM field when viewing emailed reports.

F. Recipient Email: Enter an email address for delivering reports.

IMPORTER SETTINGS

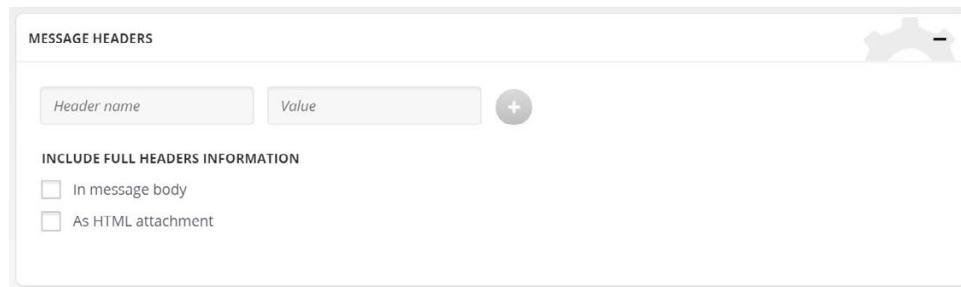
MESSAGE HEADERS

Message headers are custom headers that are used for labeling and sorting messages.

NOTE

Filters are not applied to headers generated by these settings.

These settings do not apply to the EML source.



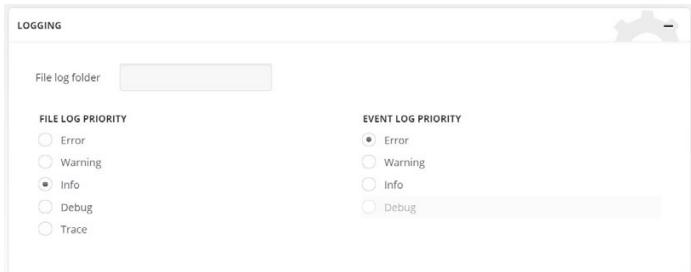
1. Fill in the Header Name and Value fields and click **+**.

You can include the full header information either in the **Message Body** (with metadata separators in between) or as **HTML attachment** (as Metadata.HTML attachment).

IMPORTER SETTINGS

LOGGING

Enter a file path in file log folder field. File logs are typically used for troubleshooting purposes. This field is required.



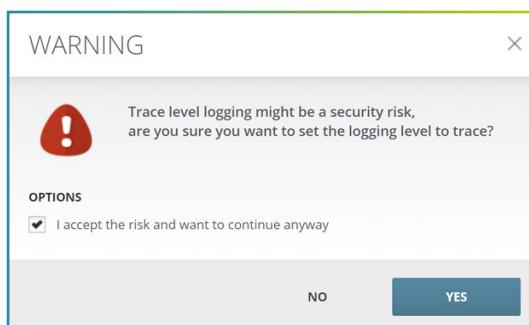
Please note

- **File Log Priority:** Saves the logs in a separate log file.
- **Event Log Priority:** Event Logs are stored in the Windows Event Viewer. Is used in order to avoid third-party tools in Windows. Helps to customize logging process and facilitate monitoring based on particular requirements.

A. 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. 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.
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.



IMPORTER SETTINGS

LOG FILE SIZE CONFIGURATION

The log files don't have a size limit, which means they can grow up to couple of GBs. Files that large can't be opened. Therefore a log file size limit needs to be set. The log file size can't be configured through Merge1 UI. However, it is possible to do by adding appropriate appender to the log config file in the Merge1 installation folder. It is done the following way:

1. Go to **C:\Program Files\Globanet Consulting Services\Merge1 6.0\Bin** path in the Merge1 installation folder.

2. Open **Merge1.Logging.config**

3. Add the following appender to the file before the root element at the end:

```
<appender 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> -->
```

4. Specify the size of the log file in the `<maximumFileSize value="1KB" />` field. For example, 10MB limit should be specified as `<maximumFileSize value="10MB" />`

5. Save the file.

Please note

As Merge1 is multi-threaded, always allow a +30% threshold between size you set in config file and actual file size you will see.

IMPORTER SETTINGS

ALERTING

In this section the option to alert on errors the connector 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 are registered in the logs.

To configure the alerting, enter the following information:

- Add the **SMTP Server**.
- Fill in the **SMTP Port**.
- Enable Server Authentication if required.
- Fill in Username and Password to authenticate to the server.
- Specify the buffer size.

The screenshot shows a configuration window titled 'ALERTING'. At the top, there is a checked checkbox labeled 'ENABLE ALERTING'. Below it, under 'ALERTING LEVEL', there are two radio buttons: 'Error' (selected) and 'Warning'. Under 'EMAIL ALERT SETTINGS', there is a 'SMTP Server' input field containing '25'. A checkbox for 'Server Authentication' is followed by 'Username' and 'Password' input fields. Below these are checkboxes for 'Use SSL' and 'Implicit'. A 'Buffer Size' input field contains '200'. At the bottom, there are three input fields for 'Sender Name', 'Sender Email', and 'Recipient Email'. To the right of these fields is a blue 'SEND TEST EMAIL' button.

You can test the connection by entering Sender Name, Sender Email (preferably an existing one in order to avoid the alert being sent to the Spam folder), and the Recipient Email. Click Send Test Email.

IMPORTER SETTINGS

IMPORTER SCHEDULE

In Merge1 you can setup the Bloomberg Import schedule, the default is only run once. This option is used to run the Importer manually from the configuration page when needed.

IMPORTER SCHEDULE

The screenshot shows a user interface for setting an importer schedule. At the top left is a title 'IMPORTER SCHEDULE'. Below it are three radio button options: 'Run Once' (selected), 'Selected Times', and 'Do not import upon startup'. To the right of these options is a large grey button labeled 'RUN IMPORTER NOW'.

You also have the option to choose the Selected Times importer schedule option. This enables you to set a weekly automated option. Increments are at 15-minute intervals.

IMPORTER SCHEDULE

The screenshot shows a user interface for setting an importer schedule using a weekly grid. At the top left is a title 'IMPORTER SCHEDULE'. Below it are three radio button options: 'Run Once' (unchecked), 'Selected Times' (selected), and 'Do not import upon startup' (unchecked). To the right of these options is a large grey button labeled 'RUN IMPORTER NOW'. The main area is a grid where each row represents a day of the week (Sunday through Saturday) and each column represents a 15-minute interval. A small moon icon is located in the top-left corner of the grid. The grid has vertical lines at 3 am and 6 am, and horizontal lines for each hour of the day. The days of the week are listed vertically on the left side of the grid.

Please note

- **Do not import upon startup:** The Importer will always run once when the service is started irrespective of the schedule. This can be avoided by enabling this option.
- **Run Importer Now:** Initiate an import manually when scheduling is enabled.

IMPORTER SETTINGS

FILTERING

Filters will not be applied unless filtering is enabled. To enable the filter click on the checkbox next to Enable filtering to configure their behavior.

- **Unconditional hit default target:** If selected, all data will be delivered to the default target, even if an alternative target is set.
- **Process all filters:** When checked, applies filters to the relevant target. In case Match any is selected, even if one filter matches to a message, the latter is sent to the set Target. If Match all is checked, all filters must match the message to be sent to the specified Target. For example, there are two Keyword Filters set with the following names: "Date - February", "No Attachment". If Match any is selected, a message that has only "Date-February" keyword will be filtered and sent to the target. If Match all is selected, only "Date-February" keyword won't suffice, the message should correspond to the second filter, "No Attachment", as well.

The screenshot shows the 'FILTERING' configuration screen. At the top, there is a blue header bar with the title 'FILTERING' and a gear icon. Below it is a light blue section labeled 'ENABLE FILTERING' with a checked checkbox. Underneath are several configuration options:

- A checkbox for 'Unconditional hit default target' which is unchecked.
- A checked checkbox for 'Process all filters'.
- Two radio buttons for 'Match any' (selected) and 'Match all'.
- A 'Target' dropdown menu.
- At the bottom, there are two dropdown menus labeled 'Filter' and 'Target' with a '+' button between them.

In the bottom fields, select the filter name and choose the target from the drop-down menu where the corresponding messages should be sent. Make sure to click on the activated **+** button to add the filtering setting, otherwise it won't be saved.

IMPORTER SETTINGS

PROCESSING

Processing Options

This option is mostly used for the troubleshooting purpose.

It is advised to use Process Failed Messages Only when there is a big number of failed messages.

If there are problems with connection which lead to failed messages, Process All Messages is the preferred choice.

If necessary, change this setting to process new segments or failed segments exclusively.

Attachment is missing

This line is added to the first line of the reprocessed segments with references to missing attachments.

Disclaimer is missing

This line is added to the first line of the reprocessed segments with references to missing disclaimers.

Strip Group Address Info

This option is selected by default and applies to the EML connector. 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

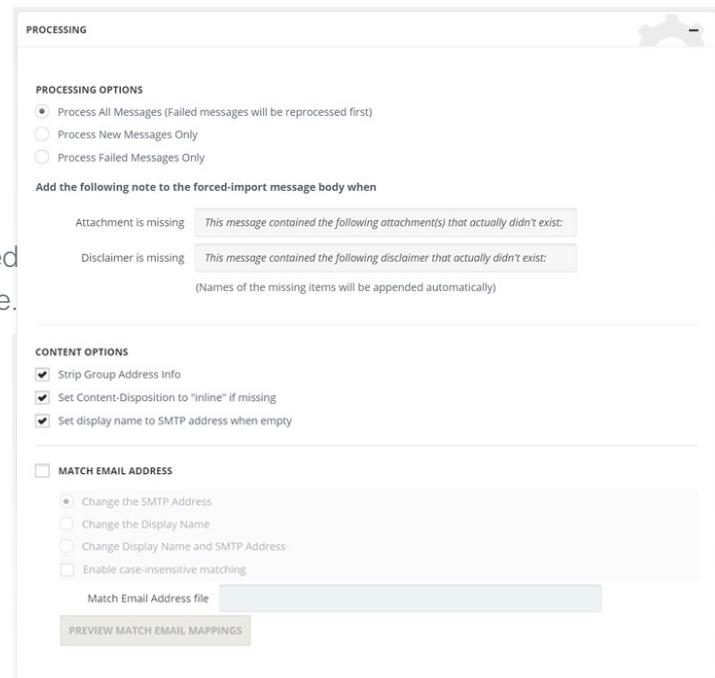
This option applies only to the EML source. When processing EML files that have image attachments, Merge1 will insert any missing ContentDisposition header fields and set their disposition type to inline so that images will appear in the message body when they are viewed in applications such as Microsoft Outlook.

Set display name to SMTP address when empty

Fill empty Display Name fields with the SMTP address (see below).

Match Email Address

The Match Email Address option can match the existing ID or SMTP Address and replace 1) SMTP Address; 2) Display Name; 3) 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).



IMPORTER SETTINGS

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.

In order to adjust the Importer's thread pool and optimize it for performance on certain systems you can use the files **Queues and Threads**.

Additionally, you can set the number of **Max target errors**, which indicates how many delivery attempts should fail before the Importer stops.

ADVANCED CONFIGURATION OPTIONS

ENABLE IMPORT THROTTLING

Chunk size	0	records
Delay	0	milliseconds

QUEUES AND THREADS

Thread pool sizes	3	Threads/Connections
Max queue size	44	MB
Max queue size	1173	messages

SET TO DEFAULTS

MISC

Max target errors	0	(0 to disable)
-------------------	---	----------------

IMPORTER SETTINGS

After you have filled in all the fields in the five tabs you will have to click Save & Finish.

Congratulations you have successfully set up the Importer!

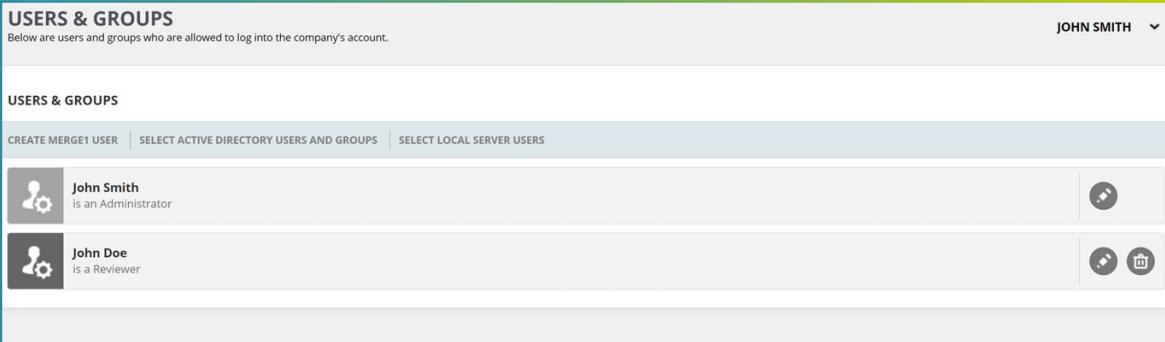
In case you want to make changes in the Wizard, click back and you will be redirected to the last screen (Importer Settings).

06

USERS & GROUPS

USERS & GROUPS

In order to manage Merge1 user accounts, click on User Profile on the navigation pane located on the left side.



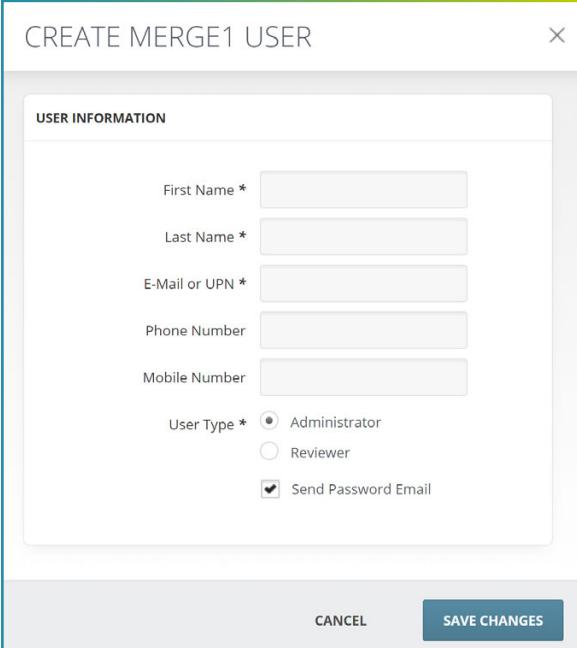
The screenshot shows the 'Users & Groups' section of the Merge1 interface. At the top right, it says 'JOHN SMITH'. Below that, there's a header 'USERS & GROUPS' and three tabs: 'CREATE MERGE1 USER', 'SELECT ACTIVE DIRECTORY USERS AND GROUPS', and 'SELECT LOCAL SERVER USERS'. Underneath, there are two user entries. Each entry includes a small profile icon, the username, a description ('is an Administrator' or 'is a Reviewer'), and edit (pencil) and delete (trash can) icons.

Users can be added to Merge1 in three ways:

Create Merge1 User

With this option a user can be created directly in the Merge1 environment.

1. Click on **Create Merge1 User** to add a new account.
2. You can edit user information and passwords if you click on the pencil icon next to the username.
3. You can easily delete the user account by clicking on the trash can.



The dialog box is titled 'CREATE MERGE1 USER'. It has a 'USER INFORMATION' section with fields for First Name, Last Name, E-Mail or UPN, Phone Number, and Mobile Number. There are also dropdowns for User Type (Administrator, Reviewer) and a checkbox for 'Send Password Email'. At the bottom are 'CANCEL' and 'SAVE CHANGES' buttons.

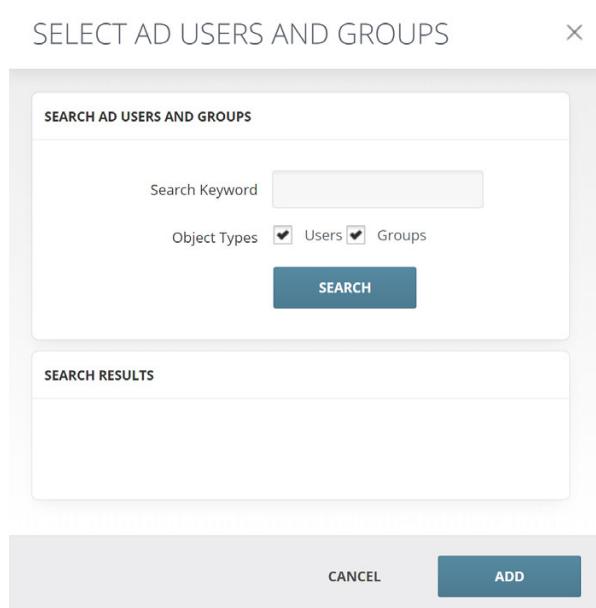
To create new user:

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 and you have now created a user account.

USERS & GROUPS

Select AD User Account (Recommended per industry best practice)

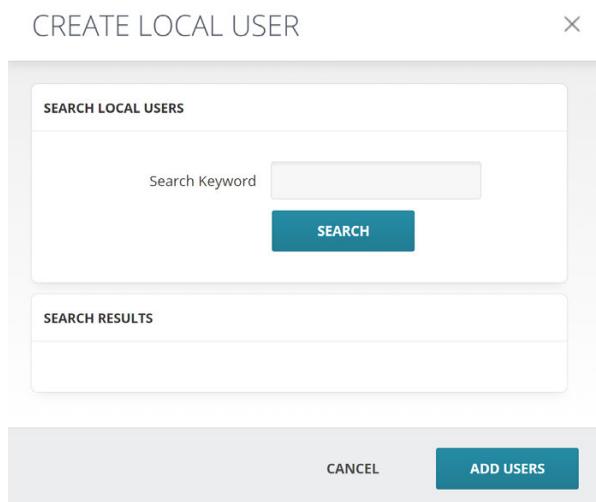
This option allows picking a user directly from the Active Directory of the Windows server the device is part of.



- 1.** Click on **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 on **Add Users**.
- 4.** Select the type of the user (Administrator or Reviewer).

Select Local Server User Account

This option allows picking a user directly from the users on the device Merge1 is installed on.



- 1.** Click on **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 on **Add Users**.
- 4.** Select the type of the user (Administrator or Reviewer).

07

REPORTS

REPORTS

To view and extract detailed information about the Merge1 user activity, optin requests and delivery failures, click on Reports Navigation pane.

- **Audit:** View Merge1 user activity. Many important actions that users make such as logging in, configuring importers or sending optin requests are listed.
- **Optin:** View completed or pending optin requests.
- **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.

2. After selecting the report type choose the connector type and which reports you would like to review.
3. Finally, you can export the report information either in a PDF or CSV format.

The screenshot shows a report table with the following columns: NAME, CORP EMAIL ADDRESS, and COMPLETED OPT-IN. The rows list users and their email addresses, with all entries marked as 'Yes' in the 'Completed Opt-in' column. The top navigation bar includes dropdowns for 'Report types' (set to 'Optin') and 'Connector types' (set to 'Yammer'), and checkboxes for 'Monitored' and 'Opt-in accepted'. At the bottom right are 'EXPORT PDF' and 'EXPORT CSV' buttons. A note at the bottom indicates there are 1 - 6 of 6 items.

NAME	CORP EMAIL ADDRESS	COMPLETED OPT-IN
Armen Aboyan	armen@globanetlabs.onmicrosoft.com	Yes
Hagop Esfahani	hagop@globanetlabs.onmicrosoft.com	Yes
Kevin Jones	kjones@globanetconsultingservices.onmicrosoft.com	Yes
Marcus Smith	msmith@globanetconsulting.com	Yes
Michael Krasner	michael@globanetconsulting.com	Yes
Sally Prescott	spprescott@globanetconsulting.com	Yes

NOTE

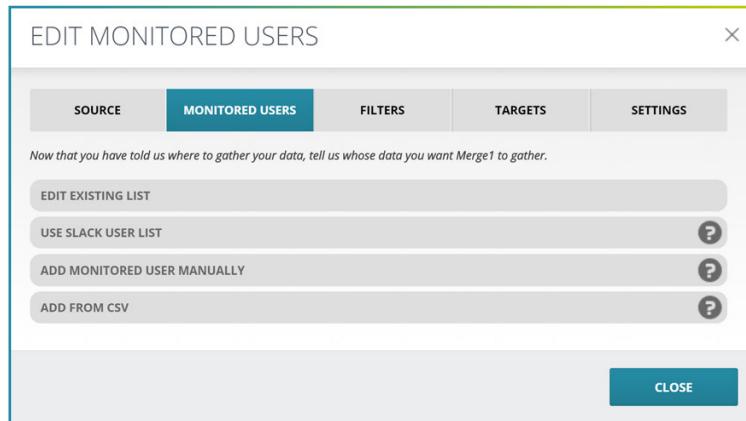
Click **Actions** at the top right corner of the page when viewing failed messages to see the reprocessing options.

Click **Export Messages** to dump all failed messages into a specified folder.

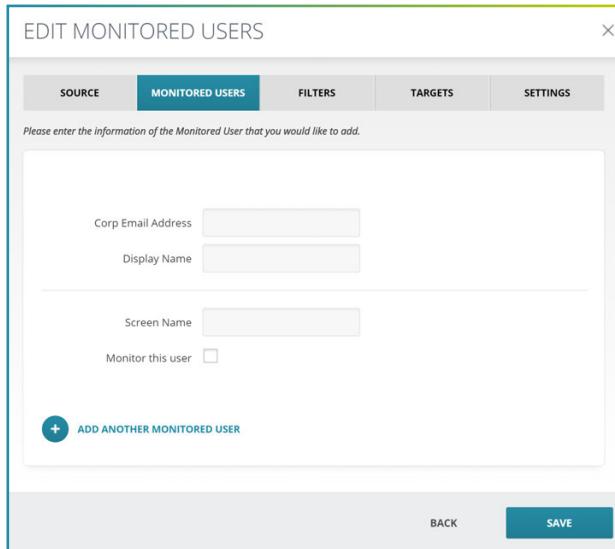
REPORTS

OPT-IN

Merge1 Twitter and Slack Regular connectors require an Opt-in from the users, that are going to be monitored. The opt-in works in the following way:



2. When Add Monitored User Manually is chosen, the following pop-up opens up, where the Corporate Email Address (email address of the Monitored User) should be entered, and the Display name of the user:



The Screen Name is added automatically when the user confirms the opt-in, and Merge1 gets the Screen Name automatically. If the user should be monitored, the Monitor this user option can be checked through here

3. If the users are added through a CSV file, the file path to the CSV should be inserted in the field. Each row should contain an email address and display name respectively, comma-separated.

REPORTS

EDIT MONITORED USERS

SOURCE MONITORED USERS FILTERS TARGETS SETTINGS

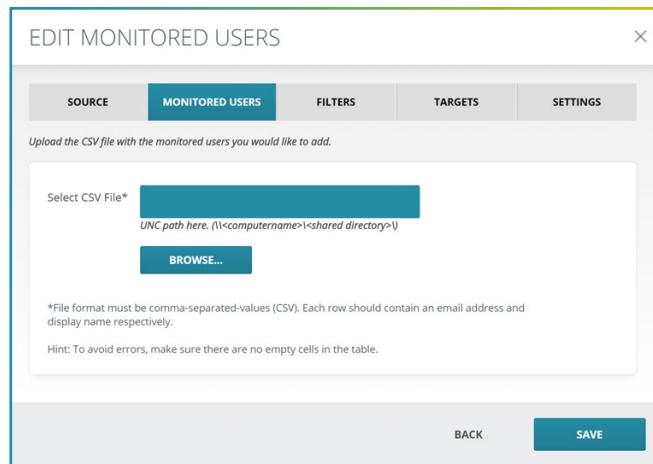
Upload the CSV file with the monitored users you would like to add.

Select CSV File* UNC path here. (\<computername>\shared directory\)

BROWSE...

*File format must be comma-separated-values (CSV). Each row should contain an email address and display name respectively.
Hint: To avoid errors, make sure there are no empty cells in the table.

BACK SAVE



4. Once the users are added, check the ones that should be monitored in the checkboxes of the Monitor column and click Save Changes:

EDIT MONITORED USERS

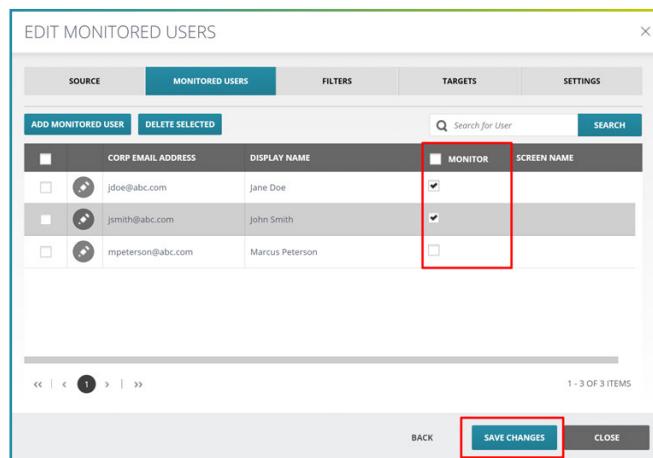
SOURCE MONITORED USERS FILTERS TARGETS SETTINGS

ADD MONITORED USER DELETE SELECTED SEARCH

	CORP EMAIL ADDRESS	DISPLAY NAME	MONITOR	SCREEN NAME
<input type="checkbox"/>	jdoe@abc.com	Jane Doe	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	jsmith@abc.com	John Smith	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	mpeterson@abc.com	Marcus Peterson	<input type="checkbox"/>	

1 - 3 OF 3 ITEMS

BACK **SAVE CHANGES** CLOSE



5. Then click on the Close or Next to send the opt-in:

EDIT MONITORED USERS

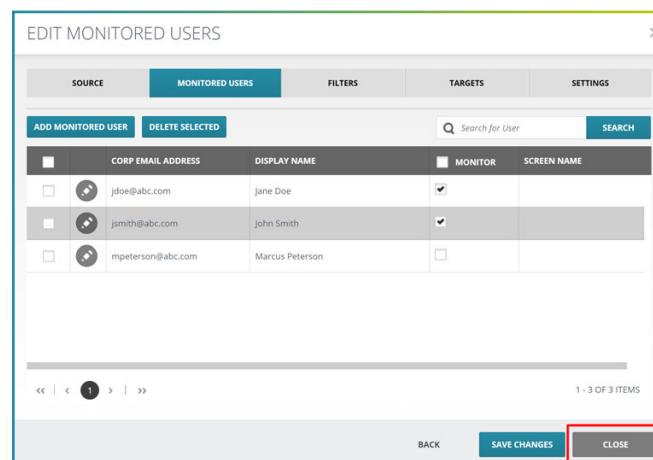
SOURCE MONITORED USERS FILTERS TARGETS SETTINGS

ADD MONITORED USER DELETE SELECTED SEARCH

	CORP EMAIL ADDRESS	DISPLAY NAME	MONITOR	SCREEN NAME
<input type="checkbox"/>	jdoe@abc.com	Jane Doe	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	jsmith@abc.com	John Smith	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	mpeterson@abc.com	Marcus Peterson	<input type="checkbox"/>	

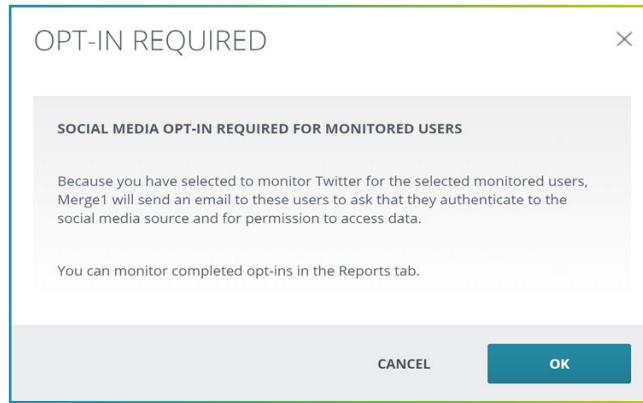
1 - 3 OF 3 ITEMS

BACK **SAVE CHANGES** **CLOSE**



REPORTS

The following pop-up will appear:

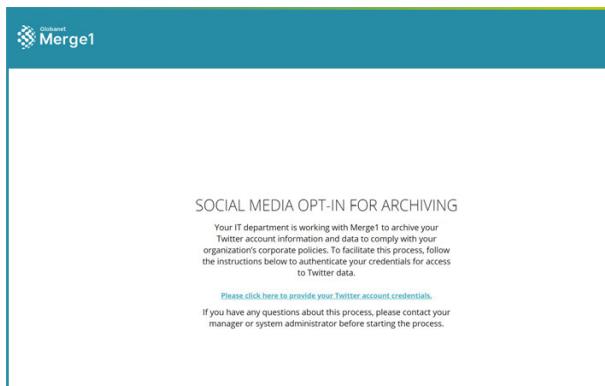


6. In the Reports section of Merge1 environment, select Report type – Optin, Connector types – Twitter or Slack. The status of the sent opt-ins, if they were accepted or not, will appear there:

A screenshot of the Merge1 Reports page. The top navigation bar shows "REPORTS" and a dropdown for "JOHN SMITH". The search filters are set to "Report types: Optin" and "Connector types: Twitter". The main table lists three users: John Smith, Jane Doe, and Marcus Peterson, along with their corporate email addresses. To the right of each user, there are two columns: "COMPLETED OPT-IN" and "RESEND EMAIL". All three entries show "No" in the "COMPLETED OPT-IN" column, and each has a "Click to Resend" link. The bottom right corner of the table area indicates "1 - 3 OF 3 ITEMS".

The Opt-ins can be resent from the Reports page as well, if they haven't been received or have expired.

7. In the received email the link for opt-in confirmation leads the following page:



When the highlighted link is clicked, the user will be redirected to log into their Twitter account and give the permission to be monitored.

The user who confirms the opt-in should be in an environment where Merge1 host server is accessible, be on the same network.

08

SETTINGS

SETTINGS

To view or configure Merge1 database proxy settings, click on Settings the navigation pane.

The screenshot shows the 'MERGE1 SETTINGS' page with the following sections:

- DATABASE CONFIGURATION**: Contains a 'CONNECT TO MERGE1 DATABASE...' button and a checkbox for 'Enable Transparent Data Encryption'. A yellow circle with the number '1' is positioned next to the 'CONNECT' button.
- AUDIT CONFIGURATION**: Contains a 'CONNECT TO AUDIT DATABASE...' button and a checkbox for 'Enable'. Below it is a 'Retention' field set to '100 days'.
- PROXY AND AUTHENTICATION CONFIGURATION**: Contains fields for 'Address' (with port 3128), 'Proxy Type' (set to 'None'), and 'Account' and 'Password' fields. It also includes checkboxes for 'Use a proxy server' and 'Use different user credentials'. A yellow circle with the number '2' is positioned next to the 'Proxy Type' section.
- MESSAGE SETTINGS**: Contains a checkbox for 'Include 'x-KVSMimeType' header' which is checked. A yellow circle with the number '3' is positioned next to this checkbox.

At the bottom right of the page is a 'SAVE SETTINGS' button.

1. When clicking Connect to a Merge1 Database you will be able to protect the data, encrypt databases on your hard drive and consequently on backup media by ticking the Enable Transparent Data Encryption box.

2. If your organization uses a proxy server, make sure the address and port information match those of your browser's proxy settings.

3. The x-KVSMimeType header is used for e-discovery tasks associated with Veritas™ Compliance Accelerator and Discovery Accelerator.

SETTINGS

DATABASE CONFIGURATIONS

Click **Connect** to Merge1 Database or Connect to Audit Database to view the database configuration menu.

1. Select an SQL server with the drop-down or enter one in the same field.
2. Choose between Windows or SQL Server Authentication and enter the login & password.
3. Click **Connect**, the **Select Database** drop-down will become active.
4. Select an existing database or create a new one, then click **OK**.

The screenshot shows the 'Database Configuration' settings page. On the left, under 'SQL CONNECTION', a dropdown menu is open with 'SQL1' selected. A green circle with the number '1' is placed over this dropdown. Below it is a large teal 'DISCONNECT' button. A green circle with the number '3' is placed over this button. Underneath is a section titled 'CONNECT USING' with two radio buttons: 'Windows Authentication' (selected) and 'SQL Server Authentication'. A green circle with the number '2' is placed over the 'Windows Authentication' button. Below these are fields for 'Login Name' and 'Password'. At the bottom is a 'Select Database' dropdown menu containing 'Merge1TestAnna'. A green circle with the number '4' is placed over this dropdown. On the right, under 'ADVANCED CONNECTION PARAMETERS', there are several input fields and checkboxes:

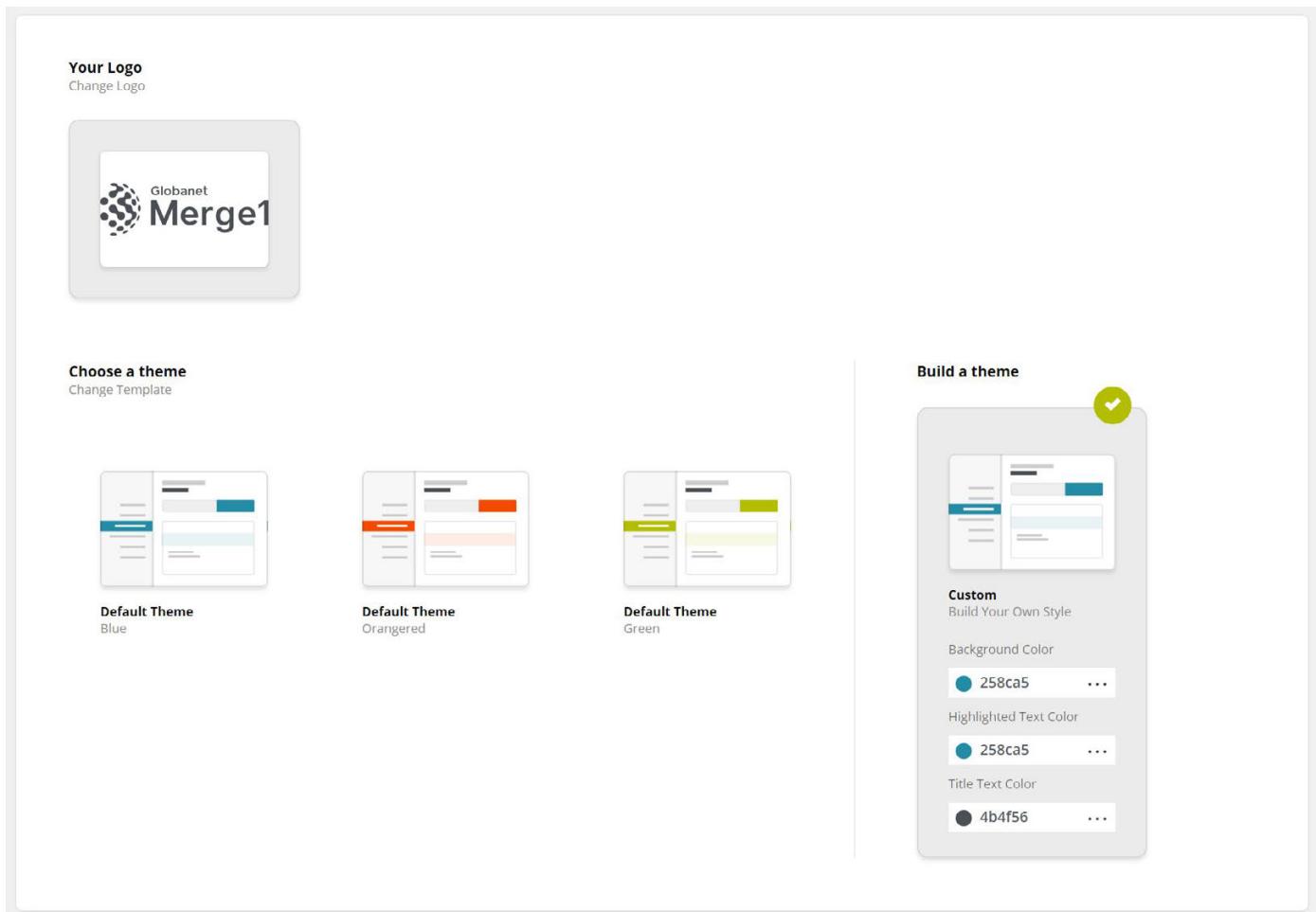
- 'Connection timeout': 15 sec
- 'Load balance timeout': 0 sec
- 'Min pool size': 0
- 'Max pool size': 1000
- 'Network packet size': 8000 bytes
- Checkboxes: Asynchronous Processing (unchecked), Encrypt (unchecked), Enlist (checked), Pooling (checked), Replication (unchecked)

09

BRANDING

BRANDING SETTINGS

Globanet Merge1 partners can change the overall interface look to make it closer to their corporate colors. You can change the color palette as well as the logo by clicking on Branding Settings in Navigation pane.



10

LICENSING

LICENSING

If you want to activate a license or upgrade the Merge1 5.x database to Merge1 6.0 click on Licensing in the Navigation Pane.

LICENSE ACTIVATION

License Status: **License has been marked as inactive on this computer. Please request Globanet for a new valid License Key.**

Licenses are distributed for Sources and Target types individually. To activate a component or components, please send the Activation Request Code to support@globanet.com.

You can view all License related information under License Details:

LICENSE DETAILS

Merge1 has a per-component licensing system for Connectors and Targets.

License Status: **Valid**

Merge1 Version: **6.18.0223**

Expiration date/time: **Permanent**.

Activation Request Code: **97D9-1CDA-E978-8000-0A1B-01D4-B1C;**

Enter Activation Code:

UPDATE

1. In case you fail to see the License Status marked as **Valid**, contact the Globanet Support team to activate your license.
2. Merge1 Verison will indicate the verison you are currenting using.
3. Also, you can change the expiration of your licesne to permanent or set to a specific date.
4. The license details will also show you your Activation Request Code.
5. Enter the alternative activation code and click on **Update**.

Please note:

If you go over the limit of the license of the API-based connectors, Bloomberg, Reuters, a warning message will be generated in the logs. Please make sure to contact us for a new license in that case.

LICENSING

THE DATABASE UPGRADE WIZARD

By clicking Launch Upgrade Wizard on the bottom of the page you will be redirected to a page that consists 5 tabs:

- 5.x Database Connection
- Importer Selection
- Pre- Upgrade
- Confirmation
- Results

UPGRADE WIZARD X

5.X DATABASE CONNECTION **IMPORTER SELECTION** **PRE-UPGRADE** **CONFIRMATION** **RESULTS**

SQL CONNECTION

Select SQL Server

CONNECT

CONNECT USING

Windows Authentication

SQL Server Authentication

Login Name

Password

Select Database

ADVANCED CONNECTION PARAMETERS

Connection timeout sec

Load balance timeout sec

Min pool size

Max pool size

Network packet size bytes

Asynchronous Processing

Encrypt

Enlist

Pooling

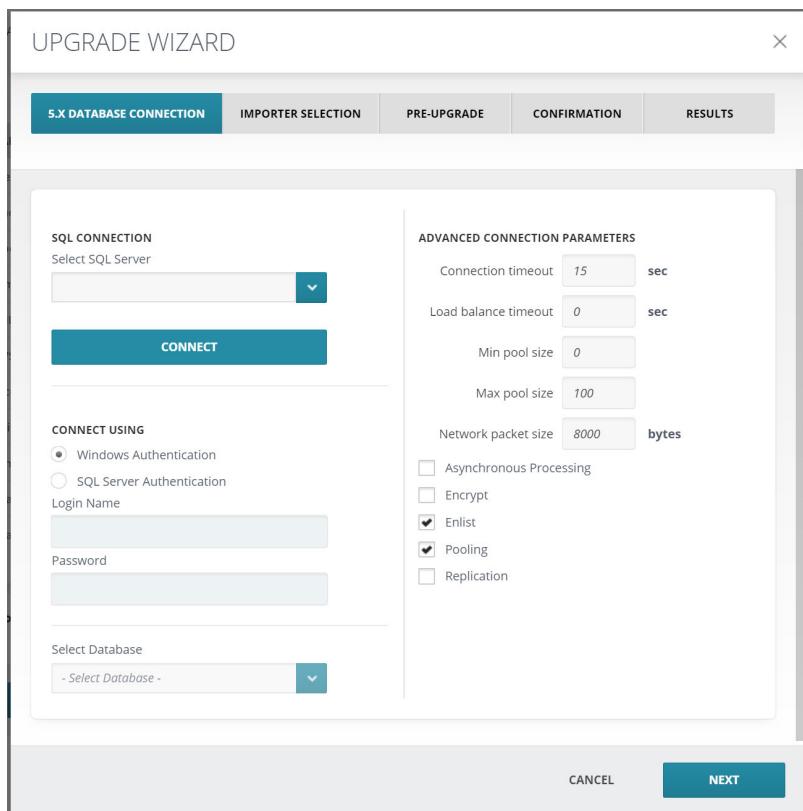
Replication

CANCEL **NEXT**

LICENSING

DATABASE UPGRADE

1. Select the SQL server from the drop-down menu, or manually enter the server name in the same field.
2. Choose between Windows or SQL Server Authentication and enter the login & password.
3. Click Connect, the **Select Database** drop-down will become active.
4. Select an existing database or create a new one, then click **OK**.
5. You can also configure Advanced Connection Parameters.
6. Once you have carried out all the required steps click **Next**.



Under the Importer Selection tab you can choose the selectors you want to upgrade.



NOTE

- Any components that are not associated with an Importer will not be upgraded.
- The MS Exchange Server Target is not supported in Merge1 6.0, all such targets will be replaced with an EWS Target during the upgrade process and will have to be reconfigured.

LICENSING

DATABASE UPGRADE

Orphan components can be upgraded by linking them to an importer. Sources can only be linked to importers that do not already have one.

The screenshot shows a 'IMPORTER SELECTION' interface. At the top, a message says 'Please Select the Importer services to upgrade to 6.16'. Below this, there are two main sections: 'JIVE' and 'BLOOMBERG'. The 'JIVE' section contains a list with 'UPGRADE' checked, which is highlighted in yellow. Underneath are 'Jive Connector' and 'EWS for jive'. The 'BLOOMBERG' section has a '+' button. Below these is a section titled 'COMPONENTS NOT ASSOCIATED WITH AN IMPORTER' containing 'jive Orphan' with a 'LINK TO IMPORTER' button.

After clicking on Link to Importer you will see the pop-up screen below. Choose the relevant Importer from the list and click **Link**.

The screenshot shows a 'LINK TO IMPORTER' dialog box. It has a dropdown menu labeled 'Available Importer *' with a blue arrow icon. At the bottom, there are 'CANCEL' and 'LINK' buttons.

LICENSING

DATABASE UPGRADE

All the Importers that fail validation will appear in the "Pre-Upgrade" tab. After troubleshooting any failed validation attempts click **Next**.

5.X DATABASE CONNECTION	IMPORTER SELECTION	PRE-UPGRADE	CONFIRMATION	RESULTS
-------------------------	--------------------	-------------	--------------	---------

PRE-UPGRADE

All selected components have been validated. Please hit next.

Review the Importers and components that will not be upgraded, then click **Start**.

5.X DATABASE CONNECTION	IMPORTER SELECTION	PRE-UPGRADE	CONFIRMATION	RESULTS
-------------------------	--------------------	-------------	--------------	---------

CONFIRMATION

The following components will not be migrated.

 **COMPONENTS NOT ASSOCIATED WITH AN IMPORTER**

- Jive Orphan
- Blackberry Orphan
- Active Directory Filter orphan
- MS Exchange Server orphan

LICENSING

DATABASE UPGRADE

To view the outcome click **Results** tab:

5.X DATABASE CONNECTION IMPORTER SELECTION PRE-UPGRADE CONFIRMATION **RESULTS**

RESULTS

The following components were successfully migrated.

 **JIVE (2)**

- Jive Connector (4)
- EWS for jive (2)

 **BLOOMBERG (1)**

- Bloomberg Connector (4)
- EWS for bloomberg (1)

 **SYMPHONY (2)**

- Symphony Connector (4)
- EWS for symphony (1)

11

APPENDIX

APPENDIX

MICROSOFT CERTIFICATE MANAGEMENT

Option 1: Request a certificate from a trusted certificate authority Please contact your IT team for more information about this method.

Option 2: Generate a new Self-Signed certificate
ps New-SelfSignedCertificate -DnsName "GlobanetMSConnectors" -CertStoreLocation "cert:\LocalMachine\My"

Copy the thumbprint returned by the previous command and use it in the command below.

```
```ps
$cert = Get-ChildItem -Path cert:\LocalMachine\My\CertificateThumbprint
Export-Certificate -Cert $cert -FilePath C:\Merge1Certificate.cer
````
```

Option 3: Use an existing certificate (For example the certificate used for Merge1 Web Application).

```
```ps
Get-ChildItem -Path cert:\LocalMachine\My
```

Copy the thumbprint of the certificate that you need to export and run the following commands.

```
```ps
$cert = Get-ChildItem -Path cert:\LocalMachine\My\CertificateId
Export-Certificate -Cert $cert -FilePath C:\Merge1Certificate.cer
````
```

After the certificate is generated or selected, you can either grant Application.ReadWrite.All permission to the Azure app created for Merge1 and allow Merge1 to upload the certificate Or upload the certificate manually without granting additional permissions.

### Upload the SSL Certificate Manually.

The screenshot shows the 'Certificates & secrets' blade for a new application named 'new APP'. The left sidebar has a 'Certificates & secrets' section highlighted. The main area has a heading 'Certificates' with a sub-section 'Upload certificate'. A button labeled 'Upload certificate' is visible. Below it, a message says 'No certificates found in this application.' There is a table with columns 'Thumbprint', 'Start Date', and 'Expires'.

