

Enterprise Vault™ Setting up Microsoft Teams Archiving

14.5

Enterprise Vault™: Setting up Microsoft Teams Archiving

Last updated: 2023-09-05.

Legal Notice

Copyright © 2023 Veritas Technologies LLC. All rights reserved.

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

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

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

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

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

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

Veritas Technologies LLC, 2625 Augustine Drive, Santa Clara, CA 95054

<https://www.veritas.com>

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

<https://www.veritas.com/support>

You can manage your Veritas account information at the following URL:

<https://my.veritas.com>

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)

CustomerCare@veritas.com

Japan

CustomerCare_Japan@veritas.com

Before you contact Technical Support, run the Veritas Quick Assist (VQA) tool to make sure that you have satisfied the system requirements that are listed in your product documentation. You can download VQA from the following article on the Veritas Support website:

https://www.veritas.com/support/en_US/vqa

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

<https://www.veritas.com/docs/100040095>

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

evdocs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

<https://www.veritas.com/community>

Contents

Chapter 1	About this guide	5
	Introducing this guide	5
	Where to get more information about Enterprise Vault	6
	Enterprise Vault training modules	8
Chapter 2	Introducing Microsoft Teams Archiving	9
	About Enterprise Vault Microsoft Teams Archiving	9
	Microsoft Teams Archiving Overview	9
	Microsoft Teams Archiving Components	10
Chapter 3	Configuring Microsoft Teams Archiving	13
	Steps to configure Microsoft Teams archiving	13
	Roles-based administration (RBA) and Microsoft Teams Archiving	14
	Assigning the permissions required for exporting data from Microsoft Teams	14
	Preparing to configure a Microsoft 365 connection	16
	Collecting Merge1 information	18
	Configuring a Microsoft 365 connection	20
	Configuring a Microsoft Teams policy	23
	Configuring an Importer	25
	Managing Teams archives	32
	Managing Teams archiving tasks	34
	About Teams archiving task reports	36
	About Teams archiving tasks performance counters	37

About this guide

This chapter includes the following topics:

- [Introducing this guide](#)
- [Where to get more information about Enterprise Vault](#)

Introducing this guide

This guide describes how to set up Enterprise Vault Microsoft Teams archiving to archive conversations from Microsoft Teams.

This guide makes the following assumptions:

- You have already installed and configured Microsoft Teams.
For more information, refer to the [Microsoft Teams documentation](#).
- You have already installed and configured Veritas Merge1 in your environment to collect Microsoft Teams data.
- You have already created a Veritas Merge1 account for Microsoft connectors.
To create an account, contact [Veritas Customer Support](#).
- You have already registered Merge1 agent using a domain user.
- You are familiar with several Enterprise Vault features, including the Administration Console.
- You know how to administer your storage hardware.

Where to get more information about Enterprise Vault

Table 1-1 lists the documentation that accompanies Enterprise Vault. This documentation is also available in PDF and HTML format in the [Veritas Documentation Library](#).

Table 1-1 Enterprise Vault documentation set

Document	Comments
Veritas Enterprise Vault Documentation Library	<p>Includes all the following documents in Windows Help (.chm) format so that you can search across them all. It also includes links to the guides in Acrobat (.pdf) format.</p> <p>You can access the library in several ways, including the following:</p> <ul style="list-style-type: none"> ■ In Windows Explorer, browse to the <code>Documentation\language\Administration Guides</code> subfolder of the Enterprise Vault installation folder, and then open the <code>EV_Help.chm</code> file. ■ On the Help menu in the Administration Console, click Help on Enterprise Vault.
<i>Introduction and Planning</i>	Provides an overview of Enterprise Vault functionality.
<i>Deployment Scanner</i>	Describes how to check the required software and settings before you install Enterprise Vault.
<i>Installing and Configuring</i>	Provides detailed information on setting up Enterprise Vault.
<i>Upgrade Instructions</i>	Describes how to upgrade an existing Enterprise Vault installation to the latest version.
<i>Setting up Domino Server Archiving</i>	Describes how to archive items from Domino mail files and journal databases.
<i>Setting up Exchange Server Archiving</i>	Describes how to archive items from Microsoft Exchange user mailboxes, journal mailboxes, and public folders.
<i>Setting up File System Archiving</i>	Describes how to archive files that are held on network file servers.
<i>Setting up IMAP</i>	Describes how to configure IMAP client access to Exchange archives and Internet Mail archives.
<i>Setting up SharePoint Server Archiving</i>	Describes how to archive documents from Microsoft SharePoint servers.

Table 1-1 Enterprise Vault documentation set (*continued*)

Document	Comments
<i>Setting up Skype for Business Archiving</i>	Describes how to archive Skype for Business sessions.
<i>Setting up SMTP Archiving</i>	Describes how to archive SMTP messages from other messaging servers.
<i>Setting up Microsoft Teams Archiving</i>	Describes how to archive Microsoft Teams data.
<i>Classification using the Microsoft File Classification Infrastructure</i>	Describes how to use the classification engine that is built into recent Windows Server editions to classify all new and existing archived content.
<i>Classification using the Veritas Information Classifier</i>	Describes how to use the Veritas Information Classifier to evaluate all new and archived content against a comprehensive set of industry-standard classification policies. If you are new to classification with Enterprise Vault, we recommend that you use the Veritas Information Classifier rather than the older and less intuitive File Classification Infrastructure engine.
<i>Administrator's Guide</i>	Describes how to perform day-to-day administration procedures.
<i>PowerShell Cmdlets</i>	Describes how to perform various administrative tasks by running the Enterprise Vault PowerShell cmdlets.
<i>Auditing</i>	Describes how to collect auditing information for events on Enterprise Vault servers.
<i>Backup and Recovery</i>	Describes how to implement an effective backup strategy to prevent data loss, and how to provide a means for recovery in the event of a system failure.
<i>Reporting</i>	Describes how to implement Enterprise Vault Reporting, which provides reports on the status of Enterprise Vault servers, archives, and archived items. If you configure FSA Reporting, additional reports are available for file servers and their volumes.
<i>NSF Migration</i>	Describes how to import content from Domino and Notes NSF files into Enterprise Vault archives.
<i>PST Migration</i>	Describes how to migrate content from Outlook PST files into Enterprise Vault archives.

Table 1-1 Enterprise Vault documentation set (*continued*)

Document	Comments
<i>Utilities</i>	Describes Enterprise Vault tools and utilities.
<i>Registry Values</i>	A reference document that lists the registry values with which you can modify many aspects of Enterprise Vault behavior.
<i>Help for Administration Console</i>	The online Help for the Enterprise Vault Administration Console.
Help for Enterprise Vault Operations Manager	The online Help for Enterprise Vault Operations Manager.

For the latest information on supported devices and versions of software, see the Enterprise Vault [Compatibility Charts](#).

Enterprise Vault training modules

Veritas Education Services provides comprehensive training for Enterprise Vault, from basic administration to advanced topics and troubleshooting. Training is available in a variety of formats, including classroom-based and virtual training.

For more information on Enterprise Vault training, curriculum paths, and certification options, see <https://www.veritas.com/services/education-services>.

Introducing Microsoft Teams Archiving

This chapter includes the following topics:

- [About Enterprise Vault Microsoft Teams Archiving](#)

About Enterprise Vault Microsoft Teams Archiving

Enterprise Vault enables you to archive Microsoft Teams instant messaging (IM) and channel communications. This in turn helps support the compliance requirements that are specified in industry and government regulations.

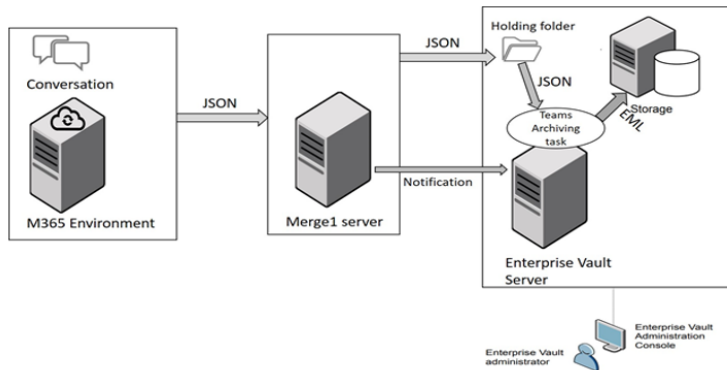
Enterprise Vault archives the following:

- Peer-to-peer chat conversations
- Private channel messages
- Public channel messages

Microsoft Teams Archiving Overview

Microsoft Teams Archiving with Enterprise Vault links the Microsoft 365 environment and Enterprise Vault using Merge1 server. Enterprise Vault assumes that archiving is enabled for individual or all users in the Microsoft 365 Domain and appropriate archiving policies have been applied. Enterprise Vault requires Microsoft 365 and Merge1 environment details to actively archive conversations to a file server. These conversations are then archived in the Enterprise Vault environment as EML files.

The following figure illustrates the process when archiving a conversation from Microsoft Teams.



The archiving process is as follows:

- A conversation takes place between Microsoft Teams users.
- Merge1 fetches the conversation JSON and sends them to the chat holding folder on the Enterprise Vault server.
- Merge1 notifies Enterprise Vault after every 50 messages.
- Enterprise Vault segregates the messages by date and chat room id in a chat segregated folder.
- Teams archiving task processes files in the chat segregated folder and creates EML files for each room id and day.
- Teams archiving task archives the item in a Teams archive. During processing, the task applies the retention category or retention plan that is specified in the target properties.

Microsoft Teams Archiving Components

The following table provides an overview of the main components of Microsoft Teams archiving. You can configure Microsoft Teams archiving using the Enterprise Vault Administration Console.

Table 2-1 Microsoft Teams Archiving components overview

Component	Description
Teams Archiving task	<p>The Teams Archiving task processes the JSON conversation files in the holding folder as follows:</p> <ul style="list-style-type: none"> ■ Creates EML files from the segregated JSON files. 1 EML per chat room, per day. ■ Stores the conversations in the archive that is associated with the importer. ■ Applies the target retention category or retention plan. ■ Deletes the conversation files from the holding folder by default, when archiving is completed successfully. If errors occur, the task does not delete the files.
Teams holding folder	<p>The Teams holding folder is a shared folder that is assigned to the Teams Archiving task. The folder location is in the Teams Importer properties. Conversation JSON files are placed in the folder for the archiving task to process.</p> <p>Conversations which the archiving task fails to archive are not deleted automatically from the holding folder. These conversations are placed in a Failed subfolder called <code>BrokenChatHolding</code>.</p>
Teams policies	<p>A Teams policy is assigned to a Importer. The policy defines rules based on which the Importer collects data from Microsoft Teams. The Teams policies are displayed in the Administration Console, under Policies > Microsoft 365 > Teams.</p>
Retention categories and retention plans	<p>Retention categories are assigned to conversations when the conversations are archived. This categorization makes it easier to retrieve conversations because it is possible to search by retention category. Users can select retention categories and assign them to Teams conversations.</p> <p>When Enterprise Vault archives a conversation, it is stored with the appropriate retention category. With a retention plan, you can associate a retention category with several other settings, such as a classification policy and the criteria for discarding expired conversations. All these settings can be applied to one or more archives.</p> <p>For more information, refer to the topic "Working with retention categories and retention plans" in the <i>Enterprise Vault Administrator's Guide</i>.</p>

Table 2-1 Microsoft Teams Archiving components overview (*continued*)

Component	Description
Microsoft 365 Connection	Connection holds the authentication information to connect to Merge1 server and Microsoft 365 server. The Microsoft 365 Connections are displayed in the Administration Console, under Targets > Microsoft 365 > Connections.
Importer	<p>The Importer downloads Microsoft Teams data to Veritas Enterprise Vault.</p> <p>The importer properties contain following settings:</p> <ul style="list-style-type: none"> ■ A Microsoft 365 Connection. ■ A Teams Policy. ■ An archive. ■ A vault store. ■ A retention category or retention plan. ■ Teams holding folder. ■ Log folder. ■ Monitored users. ■ Date Range filter. ■ Schedule information to collect Microsoft Teams data. <p>The Importers are displayed in the Administration Console, under Targets > Microsoft 365 > Importers.</p>
Teams archives	A new Teams Archive is created for each importer. These are displayed in the Administration Console, under Archives > Teams.

Configuring Microsoft Teams Archiving

This chapter includes the following topics:

- [Steps to configure Microsoft Teams archiving](#)
- [Roles-based administration \(RBA\) and Microsoft Teams Archiving](#)
- [Assigning the permissions required for exporting data from Microsoft Teams](#)
- [Preparing to configure a Microsoft 365 connection](#)
- [Configuring a Microsoft 365 connection](#)
- [Configuring a Microsoft Teams policy](#)
- [Configuring an Importer](#)
- [Managing Teams archives](#)
- [Managing Teams archiving tasks](#)

Steps to configure Microsoft Teams archiving

The steps to configure Microsoft Teams archiving are as follows:

1. Configure a Microsoft 365 connection.
See [“Configuring a Microsoft 365 connection”](#) on page 20.
2. Configure a Microsoft Teams policy.
See [“Configuring a Microsoft Teams policy”](#) on page 23.
3. Configure an Importer.

See “[Configuring an Importer](#)” on page 25.

Note: You must configure Microsoft Teams archiving only from the Enterprise Vault Administration Console. For the importers you have created from the Enterprise Vault console, you are strongly discouraged from making importer-related configuration changes from the Merge1 server console.

Roles-based administration (RBA) and Microsoft Teams Archiving

To configure Microsoft Teams Archiving, you must log in to Enterprise Vault using the Vault Service account or an account that is assigned to the Microsoft 365 Administrator role.

The Microsoft 365 Administrator role is also included in the Power Administrator role.

For more information on roles-based administration, see the Administrator's Guide.

Assigning the permissions required for exporting data from Microsoft Teams

Creating the Microsoft application for Merge1 Importer

Perform the following steps on the Microsoft Azure portal to create the Microsoft application for the Merge1 importer:

Note: Only a Microsoft Office 365 or Microsoft Azure administrator of your organization can create the Microsoft application for the Merge1 importer.

1. Navigate to <https://portal.azure.com> and log on to your organization's Microsoft Azure account.
2. Click on **Azure Active Directory** and select **App registrations**.
3. In the command pane to the top, click on **New registration**.
4. In the opened **Register an Application** window fill in the **Name** and click the **Register** button.
5. Copy the **Application ID** and **Directory (tenant) ID** from the **Overview** section to later use them in the connection creation.

6. Navigate to the **Certificates and secret** section and upload the Merge1 server and Enterprise Vault server certificates. The thumbprint of the certificate will be later used for connection creation.
7. In the navigation pane to the left, under **Certificates & secrets**, click **API permissions**.
8. Add the following permissions:

Microsoft Graph

Channel

- Channel.ReadBasic.All

ChannelMember

- [ChannelMember.Read.All]

ChannelMessage

- ChannelMessage.Read.All

Chat

- Chat.Read.All
- Chat.ReadBasic.All

Files

- Files.Read.All

Group

- Group.Read.All

Team

- Team.ReadBasic.All

User

- User.Read.All

SharePoint

Sites

- Sites.Read.All

User

- User.Read.All

Grant all the above-referenced permissions.

Ensure that the Azure AppRegistration is granted with the additional privileges to access the Protected APIs from Microsoft. Click on the following link and access the **request form**. Fill up the details in the request form and submit to Microsoft:

<https://docs.microsoft.com/en-us/graph/teams-protected-apis>

Preparing to configure a Microsoft 365 connection

The **New Connection** wizard enables you to add a connection and perform the following actions:

- Connect to the Azure Active Directory
- Configure Importers for collection of Microsoft Teams data

Prerequisites: Information required from the Microsoft Azure administrator

Ensure that you have the following information available with you from your Microsoft Azure administrator:

- **Application ID** and **Tenant ID** which you have copied at **step 5** in [Assigning the permissions required for exporting data from Microsoft Teams](#).
- X509 certificate's thumbprint or X509 certificate and its password

Prerequisites: Information required from the Veritas Merge1 administrator

Ensure that you have the following information available with you from your Veritas Merge1 administrator:

Note: To learn how to collect the Merge1 information, see [Collecting Merge1 information](#).

- Merge1 instance URL
- API Client Application ID associated with the Merge1 server
- API Client Secret associated with the Merge1 server

Prerequisites: Acquiring a certificate thumbprint

Merge1 requires an SSL certificate to use in the authentication flow. This certificate must be generated by the customer and the certificate thumbprint must be entered in the "X509 Certificate Thumbprint" field of Connector Configuration.

Note: If you want to generate your own X.509 certificate, see [Steps to generate a self-signed certificate \(X.509\) for the Merge1 server](#).

You can also use the same certificate used by Merge1 Web Application, to do this launch PowerShell and run the following command, which might return several certificates. Choose the one depending on your requirements and copy the thumbprint.

```
Get-ChildItem -path cert:\LocalMachine\My
```

Prerequisites: Setting up the Data Access Account

To be able to create a connection, the Data Access Account must be set on the Directory properties. You must create an Enterprise Vault anonymous user. For more information about creating an anonymous user, see https://www.veritas.com/support/en_US/article.100022472.

If you already have a Data Access Account user created, you can use the same account. You must re-enter the credentials associated with the account at **Directory properties > Data Access Account**, so that the user account is configured in the IIS Merge1WebHook application.

Prerequisites: Installing the Enterprise Vault site certificate from IIS on the Merge1 server

You must install the Enterprise Vault site certificate from IIS on the Merge1 server under **Trusted Root Certification Authorities**.

Prerequisites: Installing the Enterprise Vault site certificate from IIS on the Merge1 agent

You must install the Enterprise Vault site certificate from IIS on the Merge1 agent under **Trusted Root Certification Authorities**.

Prerequisites: Installing the Merge1 server certificate on the Merge1 agent

You must install the Merge1 server certificate from IIS on the Merge1 agent under the **Trusted Root Certification Authorities**.

Prerequisites: Installing the Merge1 server certificate on the Enterprise Vault server

Install the Merge1 server self-signed certificate or X509 certificate of the Merge1 server (uploaded on the Microsoft Azure portal) under the local machine's trusted root on the Enterprise Vault server.

Prerequisites: Installing the Merge1 agent certificate on the Enterprise Vault server

You must install the Merge1 agent certificate from IIS on the Enterprise Vault server.

Collecting Merge1 information

This topic contains information that enables you to collect the Merge1 information which is required for setting up Microsoft Teams archiving.

API Clients

This section describes the Merge1 API feature which allows managing Client Applications for having access to the Merge1 REST APIs.

Adding Importer Manager role in the system variable

1. Go to **System Properties > Environment Variables > System Variables**.
2. Click **Add new**.

The New system variable window opens.

3. Enter variable name as follows and **true** as the Variable value:
 Merge1:Customizations:AllowClientApplicationImporterManagerRole
4. Restart the Merge1 server virtual machine.

Managing API Clients

This section describes how to add an application.

Adding an Application

To add an application:

1. Go to the **API Client** section of the navigation pane.
2. Click **ADD APPLICATION**.
3. In the pop-up window, enter **Application Name** (maximum 64 characters length).
4. Select the **Agent Manager** and **Importer Manager** roles.
5. Click **ADD**.

The application consists of the following fields:

Table 3-1 Application fields

Component	Description
Name	The application name is specified.
Role	The level of accessibility is specified.
Application ID	The application ID is presented. You can copy the ID by clicking the Copy option.

Managing Secrets

This section describes how to add a secret.

To navigate to secrets, click **Go to Secrets** located on the left bottom corner of the application.

Adding a Secret

To add a secret:

1. Click **ADD SECRET**.
2. In the opened window, enter a **Description** (maximum 500 characters length) for the secret and select the **Expiration period**.

The specified expiration period is used to invalidate the secret.

Available periods are:

- Recommended: 6 months
- 3 months
- 12 months
- 18 months
- 24 months
- Custom

You can select one of the available periods from the drop-down list. Also, you can specify a custom expiration date by selecting the **Custom** option from the list and specifying the date.

The secret consists of the following fields:

Table 3-2 Secret fields

Component	Description
Description	The description of the secret.

Table 3-2 Secret fields (*continued*)

Component	Description
Client Secret	The client secret is specified. Note that the Client secret is displayed only when you create the secret. Copy the secret using the Copy option, and save it in a secure location for later usage.
Expires	The expiration date is specified.

Configuring a Microsoft 365 connection

To create the connection

- In the left pane of the Enterprise Vault Administration Console, click **Targets > Microsoft 365 > Connections**.
- To create a new connection, right-click on Connections and select **New > Connection**.
The **New Connection** wizard opens.
- Click **Next**.
- Enter the following details and click **Next**:
 - Name**: Enter a unique and appropriate name for the new connection.
 - Description**: Enter an appropriate description for the new connection.
- Enter the following connection details to connect to the Microsoft Azure Active Directory:
 - Application ID** and **Tenant ID** which you have copied at **step 5** in [Assigning the permissions required for exporting data from Microsoft Teams](#).
 - X509 Certificate Source**: If the X509 certificate source is on your local computer, select Local Machine and enter the X509 certificate thumbprint on the corresponding text box..
If you want to upload the X509 certificate as a PFX file, select **Upload File**. Navigate to the X509 certificate PFX file location and select the certificate. Enter the X509 certificate password on the corresponding text box.
- Click **Test** to validate the Microsoft Azure Active Directory connection. On successful validation, click **Next**.
- Enter the following Veritas Merge1 server details to connect to the Veritas Merge1 server:

- **Merge1 instance URL:** Enter the Merge1 server instance URL.
 The instance URL must be in the `https://hostname:port` format.
 It is recommended that you use the DNS alias for the Merge1 server instance URL.
 - **API Client Application ID:** Enter the API Client Application ID.
 - **API Client Secret:** Enter the API Client Secret.
8. Click **Test** to validate the Merge1 server connection. On successful validation, click **Next**.
 9. Review the details that you have entered for the connection.
 10. Click **Finish**.

To view and edit the connections

1. In the left pane of the Enterprise Vault Administration Console, click **Targets > Microsoft 365 > Connections**.
 The right pane of the Administration Console displays the available connections.
2. Right-click on a connection to perform the following actions:

Field	Actions
Delete	Allows you to delete a connection. If you want to delete a connection which has been configured to importers, you must first delete the associated Importers and then delete the connection.
Properties	Allows you to view and update the connection properties. You can double-click on a connection to view and update the properties. For more information, see the steps below.

3. If you want to update a connection, double-click on the connection. The connection properties dialog box is displayed and contains the following tabs:

Note: If you want to update a connection which has been configured with the importers, you must first disable the importers on which the connection has been configured. After updating the connection, enable the importers for data collection.

Tab

General

Microsoft 365

Merge1

Details

- **Name:** View the connection name.
- **Description:** Enter an appropriate description for the connection.
- **Application ID:** Enter the application ID associated with Microsoft Teams.
- **Tenant ID:** Enter the tenant ID associated with Microsoft Teams.
- **X509 Certificate Source:** If the X509 certificate source is on your local computer, select **Local Machine** and enter the X509 certificate thumbprint on the corresponding text box. If you want to upload the X509 certificate as a PFX file, select **Upload File**. Navigate to the X509 certificate PFX file location and select the certificate. Enter the X509 certificate password on the corresponding text box.

Click **Test** to validate the Microsoft Azure Active Directory connection.

- **Merge1 instance URL:** Enter the Merge1 server instance URL. The instance URL must be in the `https://hostname:port` format. It is recommended that you use the DNS alias for the Merge1 server instance URL.
- **API Client Application ID:** Enter the API Client Application ID associated with the Merge1 server.
- **API Client Secret:** Enter the API Client Secret associated with the Merge1 server.

Click **Test** to validate the Merge1 server connection.

4. Click **Apply > OK**.

Configuring a Microsoft Teams policy

The Teams policies are the set of rules based on which the Importer collects data from Microsoft Teams.

To add a new Teams policy

1. In the left pane of the Enterprise Vault Administration Console, click **Policies > Microsoft 365**.
2. Click **Teams**.
3. Right-click on Teams and select **New > Policy**.
The **New Teams Policy** wizard opens.
4. Click **Next**.
5. Enter the following details in the corresponding text boxes and click **Next**:
 - Enter an appropriate name for the new Teams policy.
 - Enter an appropriate description for the new Teams policy.
6. Configure the Teams policy as follows:
 - **Conversation areas to capture**: Select the conversation areas to capture. If you select **All areas**, conversation is captured from Chats or Channels. If you select certain areas, you can select between Chats or Channels.
 - **Attachment configuration**: To specify the maximum size of an attachment that can be downloaded, select the **Do not download files greater than** check box and enter the size in MB in the text box.
If you want to exclude certain file types from being downloaded, select the **Exclude file types** check box and specify the file types in a comma separated format and without any space in between (such as, txt,jpg,png) in the text box.
 - **Participant configuration**: To specify the number of participants for whom you want to capture the conversation, select the required operator from the **Match messages that have** dropdown list and enter the number of participants in the check box.
 - Click **Next**.
7. Review the new Teams Policy configurations and click **Finish**.

To view and update a Teams policy

1. In the left pane of the Enterprise Vault Administration Console, click **Policies > Microsoft 365**.

2. Click **Teams**.

The right pane of the Administration Console displays the available Teams policies. **Default Teams Policy** is the default Veritas Enterprise Vault Teams policy.

3. Right-click on a policy to perform the following actions:

Field	Actions
Copy Policy	<p>Allows you to copy an existing policy.</p> <ol style="list-style-type: none"> 1 Click on Copy Policy. 2 In the Copy Policy dialog box, enter a unique policy name and a policy description in the appropriate text boxes. 3 Click OK.
Delete	<p>Allows you to delete a policy.</p> <p>If you want to delete a policy which has been applied on a Importer, you must first delete the associated Importer and then delete the policy.</p>
Properties	<p>Allows you to view and update the policy properties. You can double-click on a policy to view and update the properties. For more information, see the step below.</p>

4. If you want to update a Teams policy, double-click on the policy.

The Teams policy properties dialog box is displayed.

Note: If you want to update a policy which has been applied on Importers, you must first disable the importers on which the policy has been applied. After updating the policy, enable the Importers for data collection.

5. The **General** tab displays the following, which you can update:

- Policy name
- Policy description

6. The **Configuration** tab displays the following, which you can update:

- **Conversation areas to capture:** The conversation areas to capture. If you select **All areas**, conversation is captured from Chats or Channels. If you select certain areas, you can select between Chats or Channels.
 - **Attachment configuration:** The maximum size of an attachment that can be downloaded. Select the **Do not download files greater than** check box and enter the size in MB in the text box.
If you want to exclude certain file types from being downloaded, select the **Exclude file types** check box and specify the file types in a comma separated format and without any space in between (such as, txt,jpg,png) in the text box.
 - **Participant configuration:** The number of participants for whom you want to capture the conversation. Select the required operator from the **Match messages that have** dropdown list and enter the number of participants in the check box.
7. If you have updated the Teams policy, click **Apply > OK**.

Configuring an Importer

The importer downloads Microsoft Teams data to Veritas Enterprise Vault.

Prerequisite

- Ensure that the Teams domain is added to the list of internal SMTP domains for marking the correct message direction (internal or external). Navigate to **Site Properties > Advance > SMTP > List of internal SMTP domains** to add the Teams domain.
- Ensure that the connection to configure the importer is available in Enterprise Vault under **Targets > Microsoft 365 > Connections**.
- Ensure that the **Merge1WebHookPool** application pool identity is set as Enterprise Vault Service Account under **IIS Manager > Application Pools** on the Enterprise Vault server.
- Ensure that **Anonymous Authentication** is enabled for the **Merge1WebHook** application under **IIS Manager > Default Web Site > EnterpriseVault > Merge1WebHook > Authentication** on the Enterprise Vault server.
- Be aware of the Vault Store you want to use for the importer.
- Be aware of the log folder path of the Merge1 server where the Merge1 importer logs are written. The log folder path must be a local path on the Merge1 server.
- Ensure that the Merge1 agent is registered using the domain user in the same domain. It is recommended that you use the Enterprise Vault Service Account

to register the Merge1 agent. However, if you already have registered Merge1 agent with a non-Enterprise Vault Service Account, you can continue using this account, provided it is the same domain user.

You must add the Merge1 agent user to the following security policies on the Merge1 agent server:

- Log on as Service rights
- Log on as a batch job right
- Ensure that the Merge1 agent user account has been added to the local Administrators group on the Merge1 server.
- Ensure that the Merge1 agent user account has been assigned the **db_owner** permissions on the Merge1 database.
- Ensure that the Enterprise Vault server administrator (Vault Service account, Power Administrator, Microsoft 365 Administrator, and RBA role member) account has been added to the local Administrators group on the Merge1 server.
- Ensure that the Teams holding folder in the Enterprise Vault server is available to receive the Microsoft Teams data. The holding folder path can be a local or remote path to the Enterprise Vault server. The holding folder must be a shared folder so that the Merge1 server and the Enterprise Vault server can access it.
- Ensure that the Vault Service account has **Full control** security permission on the Teams holding folder.
- Ensure that the Enterprise Vault server administrator (Vault Service account, Power Administrator, Microsoft 365 Administrator, and RBA role member) account has the **Change, Read** sharing permissions on the Teams holding folder.
- Ensure that the Merge1 agent user account has the **Change, Read** sharing permissions on the Teams holding folder.
- Ensure that the Merge1 agent user account has the **Modify** security permission on the Teams holding folder.
- While creating an importer in the Enterprise Vault Administration Console, enter the shared folder path by copying and pasting it into the Holding folder field.

Note: For collecting legacy data and daily data, it is recommended that you create two separate importers. The administrator must manually start the Teams Archiving Task to collect both legacy and daily data. For legacy data collection, the administrator must allow the importer to download data for a few days and then start the Teams Archiving Task either in the Run now or Schedule mode. See Managing Teams archiving tasks for more information about the Run now and Schedule modes.

About Holding Folder

The holding folder is the folder where Merge1 will dump the Microsoft Teams data and Enterprise Vault pick that data for the archiving.

The holding folder path must comply with the following conditions:

- The folder is recommended to be on a local drive to the EV Server.
- The folder should be excluded from virus scanning. Scanning the holding folder can cause the corruption of items, performance issues, and data loss.
- The folder must be a shared folder and must be specified in UNC path format where-ever asked.
- The maximum permitted length of folder path is (140 - importer's Name length) characters.
- Ensure that the Enterprise Vault server administrator (Vault Service Account/Power Administrator/Microsoft 365 Administrator RBA role member) account has the 'Change, Read' sharing permissions on the Teams holding folder.
- Ensure that the Merge1 agent user account has the 'Change, Read' sharing permissions on the Teams holding folder.
- Ensure that Vault Service Account has the 'Full control' security permission on the Teams holding folder.
- Ensure that the Merge1 agent user account has the 'Modify' security permission on the Teams holding folder.

Configure holding folder on a server other than the Enterprise Vault server

- The machine to be configured for holding Teams chat data must be in the same domain as the Enterprise Vault server.
- While creating Importer in the Enterprise Vault Administration Console, enter the shared folder path by copying and pasting it into the Holding folder field.

This configuration allows notification requests to be received correctly from the Merge1 server to the Enterprise Vault server and the chat items segregation process is triggered successfully.

To create an importer

1. In the left pane of the Enterprise Vault Administration Console, click **Targets > Microsoft 365 > Importers**.
2. To create a new importer, right-click on **Importers** and select **New > Importers**.
3. In the **New Importer** wizard, click **Next**.
4. Enter the following details in the corresponding text boxes and click **Next**:
 - Enter an appropriate and unique name for the new importer.
 - Enter an appropriate description for the new importer.
5. Select the following and click **Next**:
 - **Microsoft 365 connection**: From the dropdown list, select connection.
 - **Holding folder**: Select the Microsoft Teams holding folder path to receive the Microsoft Teams data
 - **Log folder**: Select the location of the log folder of the Merge1 server where the Merge1 importer logs are written.
6. Specify the users whose data will be collected by the importer:
 - To collect data for all users, select **All users**.
 - To collect data for specific users, select **Manually maintain the list**.
To manually enter email IDs and display names of specific users, click **Add** and enter the user details. Click **OK**.
To import specific users from a CSV file, click **Import** and select the CSV file. Click **Open**.
Entries in the CSV file should be present in the following format:
<Email Address1>,<Username1>
<Email Address2>,<Username2>
...
...
7. Click **Next**.
8. Specify the Date Range for which importer will collect the Microsoft Teams data.
 - **All Time**: Select this option to collect the Microsoft Teams data for all the time without any date filter criteria. It will continuously keep on collecting the Microsoft Teams data whenever data is available.

- **Date Based:** Select this option to collect the Microsoft Teams data for the specific date range. If you select this option, you must select at least one of the checkboxes - **Collect data generated after** and **Do not collect data generated after** - to specify the date range for data collection.
- **Collect data generated after:** Select this option to collect the Microsoft Teams data from a specific date only. Team data prior to this date will not be collected.
- **Do not collect data generated after:** Select this option to collect the Microsoft Teams data up to a specific date only. Microsoft Teams data after this date will not be collected.

Note: Once data for the specific date range is collected we cannot collect the data prior to this date range by modifying it from the importer's properties. Importer will always collect the data from the date where it last collected the data.

9. Click **Next**.
10. Select the following:
 - The Teams policy that you want to apply on the importer.
 - The retention category that you want to use for the importer.
11. Click **Next**.
12. Select the Vault Store that you want to use for the importer.

Note: The Microsoft Teams Archive and the Teams Archiving Task for the importer are created on the same machine where the Vault Store is present.

13. Review the new importer configurations and click **Finish**.

To view and update importers

1. In the left pane of the Enterprise Vault Administration Console, click **Targets > Microsoft 365 > Importers**.
The right pane of the Administration Console displays the available importers.
2. Right-click on an importer to perform the following actions:
 - **Enable:** Allows you to enable the importer.
 - **Disable:** Allows you to disable the importer. This is needed to modify the importer's properties and to delete the importer.

- **Run Now:** Allows you to run the importer, which will collect the Microsoft Teams data.
 - **Delete** Allows you to delete the importers. Importer should be in the disabled state to perform this operation.
 - **Properties:** Allows you to view and update the importer properties. You can double-click on an importer to view and update the properties. For updating the importer properties, importer must be in disabled state. For more information, see the steps below.
3. To update an importer, double-click on it.

Note: If you want to update an importer, ensure that the importer is in the disabled state.

The importer properties dialog box is displayed and contains the following tabs:

- **General:** The **Details** section displays the importer name, description, status, and the Teams archiving task associated with the importer.
The **Settings** section displays the Teams archive name and the Teams policy applied on the importer. You can update the settings, if required.
The **Retention** section displays the retention category. You can update the retention category settings, if required.
- **Connection and Folders:** The **Connection** section displays the available connections with the Merge1 server on which the importer has been created. You can update the connection, if required.
The **Holding folder** section displays the path of the Microsoft Teams holding folder which receives the Microsoft Teams data from the Merge1 server. You can update the holding folder path, if required. Before updating the holding folder location for the importer, perform the following steps:
Step 1: In the Enterprise Vault Administration Console, stop the importer's Teams Archiving task.
Step 2: Copy the existing content of the current holding folder tree to the new location.
The **Log folder** section displays the path of the log folder of the Merge1 server where the Merge1 importer logs are stored. You can update the log folder path, if required.
- **Monitored Users:** Specify the users whose data will be collected by the importer:
 - To collect data for all users, select **All users**.
 - To collect data for specific users, select **Manually maintain the list**.

To manually enter email IDs and displays names of specific users, click **Add** and enter the user details. Click **OK**.

To import specific users from a CSV file, click **Import** and select the CSV file. Click **Open**.

Entries in the CSV file should be present in the following format:

<Email Address1>,<Username1>

<Email Address2>,<Username2>

...

...

- **Date Range:** Specify the Date Range for which importer will collect the Microsoft Teams data.
 - **All Time:** Select this option to collect the Microsoft Teams data for all the time without any date filter criteria. It will continuously keep on collecting the Microsoft Teams data whenever data is available.
 - **Date Based:** Select this option to collect the Microsoft Teams data for the specific date range. If you select this option, you must select at least one of the checkboxes - **Collect data generated after** and **Do not collect data generated after** - to specify the date range for data collection.
 - **Collect data generated after:** Select this option to collect the Microsoft Teams data from a specific date only. Team data prior to this date will not be collected.
 - **Do not collect data generated after:** Select this option to collect the Microsoft Teams data up to a specific date only. Microsoft Teams data after this date will not be collected.

Note: Importer will always collect the data from the date where it last collected the data.

- **Schedule:** The configurations to schedule running of the importer. The Interval section allows you to select 1 hour or 15 minutes to schedule running of the importer. You can also select specific time slots on specific days of the week to schedule running of the importer by clicking on the time scheduler at the bottom of the dialog box.
- **Advanced:** Displays the batch size of the Merge1 notifications. The batch size of the number of copied files initiates Merge1 to send notifications to Enterprise Vault. The default batch size is 50. Click **Modify** if you want to change the existing batch.

4. Click **Apply > OK**.
5. If you have updated the holding folder location, perform one of the following actions:
 - Recycle the Merge1WebHookPool in the IIS Manager application pools.
Or,
 - Restart the IIS server.
6. Enable the importer.
7. Start the corresponding Teams Archiving task.

Managing Teams archives

1. In the left pane of the Enterprise Vault Administration Console, click **Archives > Teams**.

The right pane of the Administration Console displays the available Teams archives. By default, the name of the Teams archive has the same name as the Importer name.

2. Right-click on an archive to perform the following actions:

Field	Actions
Search archive	Allows you to search for archived Teams items.
View expiry report	Allows you to view the expiry report of archived Teams items.
Delete	Allows you to delete an archive.
Properties	Allows you to view and update the archive properties. You can double-click on an archive to view and update the properties. For more information, see the step below.

3. If you want to update a Teams archive, double-click on the archive.

The Teams archive properties dialog box is displayed and contains the following tabs:

Tab

General

Details

Allows you to:

- View and rename the Teams archive.
- View the details of the Teams archive, such as site, vault store, and so on.
- The Administrative note sections allows you to add any note.

Permissions

Allows you to:

- Control access of users and groups to the archive.
- Select users and groups to which permission is to be granted or denied for accessing the archive.

Indexing

Allows you to:

- Select indexing level of the archive.
- View configured archiving dates.

Advanced

Allows you to:

- View and set archive deletion settings.
- View the archive ID.
- View the archive type ID.

Archive Usage limit

Allows you to control the maximum size of the archive. You can set a limit for the archive, inherit the setting from the site properties, or the Vault Store properties.

Index Volumes

Allows you to:

- View the available index volumes.
- View the health of the index volumes.
- Upgrade, verify, synchronize, rebuild, and change location of the index volumes for the Enterprise Vault archives.

Deleted Items

Allows you to recover items marked for deletion from the archive.

4. Click **Apply > OK**.

Managing Teams archiving tasks

1. In the left pane of the Enterprise Vault Administration Console, click **Enterprise Vault Servers > Tasks**.

The right pane of the Administration Console displays the available Teams archiving tasks.

2. Right-click on an archive to perform the following actions:

Field	Actions
Start	Allows you to start the Teams archiving task.
Stop	Allows you to stop the Teams archiving task.
Restart	Allows you to restart the Teams archiving task.
Pause	Allows you to pause the Teams archiving task.
Resume	Allows you to resume a paused Teams archiving task.
Run Now	Allows you to immediately run the Teams archiving task.
Delete	Allows you to delete the Teams archiving task.
Properties	Allows you to view and update the archiving task properties. You can double-click on an archiving task to view and update the properties. For more information, see the step below.

3. If you want to update a Teams archiving task, double-click on the task.
 The Teams archiving task properties dialog box is displayed and contains the following tabs:
 - **General:** The **Details** section allows you to:
 - View the archiving task site name.
 - View the name of the machine on which the archiving task exists.

The **Settings** section allows you to view and update the archiving task startup type. The available startup options are:

- Automatic
- Manual
- Disabled

The **Administrative note** sections allows you to add any note.

- **Scheduled:** The configurations to schedule running of the archiving task. Select the **Use site setting** checkbox to schedule running of the archiving task based on the site setting. Selecting the checkbox, disable other scheduling settings. By default, the **Use site setting** checkbox is not selected.

If you want to schedule running of the archiving task based on configurations other than the site settings, clear the **Use site setting** checkbox.

In the **Run** section:

- Select **Never** to prohibit the archiving task to run on its own. Click **Run Now** to immediately run the archiving task.
- Select **At selected times** to configure running of the archiving task at specific intervals, in specific days and time-slots. Configure the settings from the **Interval** section and time and date picker section. Click **Run Now** to immediately run the archiving task.

4. **Reports:** Allows you to configure the archiving report settings.

See [“About Teams archiving task reports”](#) on page 36.

5. **Advanced:** Allows you to configure the following archiving task advanced settings

- **Converted chat folder path for Teams archiving task:** Path of the converted chat folder. Path must be a valid folder path.
- **Broken chat folder path for Team archiving task:** Path of the broken chat folder. Path must be a valid folder path.
- **Ignore items in the current date folder when processing items from the segregation folder:** Determines if the current date folder must be processed or not when processing items from the segregation folder. By default, the Teams archiving task ignores the current date folders.
 - **1:** Ignore current date folders in the segregation folder.
 - **0:** Do not ignore current date folders in the segregation folder.

6. Click **Apply > OK**.

Updating the converted chat or broken chat folder path

You can update the converted chat or broken chat folder path if required. Perform the following actions to update the converted chat or broken chat folder path:

1. From the Enterprise Vault Administration Console, stop the importer and the Teams archiving task corresponding to the importer.
2. Copy the existing content of the current holding folder tree to the new location.
3. Set the new folder path in the Teams Archiving Task Properties: Advanced page.
4. Perform one of the following actions:
 - Recycle the Merge1WebHookPool in the IIS Manager application pools.
Or,
 - Restart the IIS server.
5. Start the importer and Teams archiving task corresponding to the importer.

About Teams archiving task reports

When a Teams archiving task runs as per its schedule, or with the **Run Now** option, it creates a report with the details of the run.

Teams archiving task reports are created at following location:

```
<Enterprise Vault Install Path>\Enterprise Vault\Reports\Teams Archiving
```

Following is a sample of the Teams archiving task report:

```
Archive run started at 11/11/2021 3:26:04 PM for the Teams archiving task 'TEAMS ARCHIVING TASK FOR IMPORTER NAME'
```

```
Task Started : 11/11/2021 3:26:04 PM
```

```
Task Finished : 11/11/2021 3:26:20 PM
```

```
Elapsed Time : 00:10:15 (hh:mm:ss)
```

```
Total number of TeamsRoomChat in the segregation folder: 92318
```

```
Total number of TeamsRoomChat processed: 10
```

```
Total number of TeamsRoomChat archived: 10
```

```
Total Number of TeamsRoomChat failed to convert: 0
```

```
Total number of TeamsRoomChat failed to archive: 0
```

```
Total number of TeamsRoomChat marked as broken: 0
```

Total KB archived: 9867 KB

Note: If the Teams archiving task run does not find any files to process and archive, then it adds following note in the report.

NOTE: The Teams archiving task did not find any files to process and archive in the `\\SERVERNAME\c$\HoldingSharedFolder\ImporterName\ChatSegregated`. This could happen when there is no data available from Microsoft Teams for archiving. Ensure that the Merge1Webhook under the Veritas Enterprise Vault website is running and the Importer is dumping data into the holding folder.

About Teams archiving tasks performance counters

The task provides following counters to monitor the performance of the archiving process.

Counter	Description
Teams Room Chat Archived	Number of chat rooms data converted from .json to .eml and archived successfully.
Teams Room Chat Failed To Archive	Number of chat rooms data converted from .json to .eml but failed to archive.
Teams Room Chat Failed To Convert	Number of chat rooms data that failed to convert from .json to .eml.
Teams Room Chat Items In Queue	Number of chat items yet to be processed.
Teams Room Chat Marked As Broken	Number of chat rooms data successfully converted from .json to .eml and added to BrokenChatHolding folder.
Teams Room Chat Processed	Number of chat room processed.