

# Veritas SaaS Backup Administrator's Guide

For the Office 365, Dynamics 365, G  
Suite, and the Salesforce platforms

Version 4.0

# Contents

<b>Chapter 1</b>	<b>About SaaS Backup .....</b>	<b>6</b>
	SaaS Backup overview .....	6
	SaaS Backup features and functionalities .....	7
	SaaS Backup data centers .....	7
	System requirements .....	8
	Technical and documentation support .....	9
<b>Chapter 2</b>	<b>Getting started .....</b>	<b>11</b>
	Accessing SaaS Backup from your region .....	11
	Understanding administration interface .....	11
	Signing in to SaaS Backup .....	14
	Signing out from SaaS Backup .....	15
	Resetting a forgotten password .....	15
	Updating password and other account information .....	16
	Requesting a user license cancellation .....	18
	Upgrading the SaaS Backup subscription .....	20
<b>Chapter 3</b>	<b>Managing notifications .....</b>	<b>23</b>
	Viewing notifications .....	24
	Predefined email notifications .....	25
	Deleting multiple notifications .....	26
<b>Chapter 4</b>	<b>Managing users and roles .....</b>	<b>27</b>
	About users, user roles, and associated permissions .....	27
	Configuring access to connectors .....	31
	Creating user profiles .....	35
	Updating user profile details .....	37
	Deleting user profiles .....	38
<b>Chapter 5</b>	<b>Managing connectors .....</b>	<b>41</b>
	About connectors .....	41
	Common connector-specific operations .....	42
	Reactivating connectors .....	43

	Scheduling the data backup frequency .....	45
	About snapshots .....	47
<b>Chapter 6</b>	<b>Managing public share links .....</b>	<b>49</b>
	About public links .....	49
	Generating public share links for sharing data .....	50
	Deleting public share links .....	54
<b>Chapter 7</b>	<b>Monitoring backup and restore jobs .....</b>	<b>56</b>
	About backup and restore jobs monitoring .....	56
	Understanding the backup and restore job monitoring process .....	57
	Viewing backup and restore jobs and statistics .....	64
	Calculating the estimated time for a job completion .....	67
	Calculating the size of data you have in Office 365 .....	68
	Downloading job status report .....	71
<b>Chapter 8</b>	<b>Managing audit logs .....</b>	<b>73</b>
	About audit logs .....	73
	Viewing and downloading audit log reports .....	75
<b>Chapter 9</b>	<b>Managing cloud services for Office 365 .....</b>	<b>77</b>
	Office 365 cloud connectors overview .....	78
	Protected Office 365 data types .....	79
	Office 365 Throttling .....	81
	Preparing an Office 365 service account for SaaS Backup .....	82
	Adding Office 365 cloud connectors .....	85
	Deleting Office 365 connectors .....	90
	Restore a Microsoft 365 item .....	91
	Restore Exchange data using the Restore Wizard .....	94
	Restore OneDrive data using the Restore Wizard .....	101
	Monitoring jobs of Office 365 cloud connectors .....	107
	Sharing files and folders of Office 365 cloud connectors .....	109
	Downloading files and folders on Office 365 cloud connector .....	110
	About SharePoint backup data types .....	111
	Restrictions while restoring the SharePoint backups .....	114
	Reasons for smaller snapshot size than the actual data size in Office 365 .....	116
	Configuring SharePoint data backup .....	117
	About restoring SharePoint data .....	120
	Restore a SharePoint site .....	121
	Restoring SharePoint data in different scenarios .....	128

	Restoring SharePoint data across a tenant .....	137
	Restoring SharePoint data with an advanced backup configuration .....	138
	Restore SharePoint sites using the Restore Wizard .....	139
	About Groups and Teams data backup .....	145
	About Groups and Teams backup data types .....	147
	Restore Groups and Teams data using the Restore Wizard .....	154
	Adding global administrator to the Teams channel .....	161
	Restoring Teams channels data .....	162
<b>Chapter 10</b>	<b>Managing single sign-on (SSO) authentication in Office 365 .....</b>	<b>166</b>
	About single sign-on authentication .....	166
	Creating a single sign-on administrator profile .....	167
	Configuring single sign-on using Azure Active Directory .....	167
	Assigning users to single sign-on application in Azure Active Directory .....	170
	Configuring single sign-on using ADFS .....	175
	Configuring single sign-on in SaaS Backup .....	189
<b>Chapter 11</b>	<b>Managing cloud services for Dynamics 365 .....</b>	<b>193</b>
	Dynamics 365 cloud connectors overview .....	193
	Protected Dynamics 365 data types .....	194
	Adding Dynamics 365 cloud connectors .....	194
	Deleting Office 365 connectors .....	198
	Restoring files and folders from Dynamics 365 cloud connectors .....	199
	Monitoring jobs of Dynamics 365 cloud connectors .....	203
	Sharing files and folders of Dynamics 365 cloud connectors .....	204
	Downloading files and folders on Dynamics 365 cloud connector .....	205
<b>Chapter 12</b>	<b>Managing cloud services for Google Workspace .....</b>	<b>207</b>
	Google Workspace cloud connectors overview .....	207
	Protected Google Workspace components .....	208
	Preparing a Google Workspace service account for SaaS Backup .....	208
	Adding Google Workspace cloud connectors .....	210
	Deleting Google Workspace cloud connectors .....	213
	Restoring files and folders on Google Workspace cloud connectors .....	214
	Monitoring jobs of Google Workspace cloud connectors .....	216

Sharing files and folders of Google Workspace cloud connectors .....	217
Downloading files and folders from Google Workspace cloud connector .....	218

<b>Chapter 13</b>	<b>Managing cloud services for Salesforce .....</b>	<b>219</b>
	Salesforce cloud connectors overview .....	219
	Protected Salesforce data types .....	220
	About campaigns and campaign members backup .....	223
	Salesforce throttling and API request usage .....	224
	Adding Salesforce cloud connectors .....	225
	Deleting Salesforce cloud connectors .....	231
	Restoring records, files, and attachments on the Salesforce cloud connector .....	232
	Monitoring backup and restoring jobs of Salesforce cloud connectors .....	238
	Sharing files and folders of Salesforce cloud connectors .....	239
	Downloading files and folders from Salesforce cloud connector .....	240

# About SaaS Backup

This chapter includes the following topics:

- [SaaS Backup overview](#)
- [SaaS Backup features and functionalities](#)
- [SaaS Backup data centers](#)
- [System requirements](#)
- [Technical and documentation support](#)

## SaaS Backup overview

Veritas SaaS Backup (VSB) is a backup and recovery hosted service for SaaS application protection. It provides a cloud-to-cloud backup solution with secured and automated data protection across the SaaS based workloads. This solution is scalable from a small business to an enterprise level.

SaaS Backup enables you to backup and restore data on the following platforms:

- Office 365
- Dynamics 365
- G Suite
- Salesforce

You can create and monitor backup jobs, restore and download files and folders, generate public share links to share files and folders, restore cloud connectors, and use partial snapshots for backup. You can schedule a backup frequency, import data, and view the audit logs generated while running backup jobs.

# SaaS Backup features and functionalities

SaaS Backup provides simple workflows to speed up the routine backup and restore tasks. Its interface follows industry best practices and standards to provide an intuitive interaction.

- **Role-based access control:** Reasonable access to the workflows that are based on user roles and responsibilities.
- **Easy setup:** No need to purchase computer or storage, nothing to install or deploy.
- **Point-in-time restoration:** Find and restore the lost data quickly and easily.
- **Single sign-on (SSO) support:** Provides the centralized access management to its users
- **Multi-factor authentication (MFA) support:** Offers an increased security by asking users to prove identity during signing in.
- **Easy monitoring functions:** Monitor backup and restore status, view audit logs, receive email alerts, and set retention according to retention policy.
- **Reliable and secure infrastructure:** Automated backups, 99.9% uptime, 256-bit encryption at-rest, 1.2 TLS encryption in-flight, ISAE 3402.
- **Follows security standards:** Data centers meet the following security standards
  - **USA:** HIPAA, ISO 27001, SOC 2 Type 2, NIST 800-53/FISMA
  - **Europe:** ISAE 3402 Type 2, ISO 27001, SOC 2 Type 2
  - **Australia:** ISO 27001, SOC 2 Type 2

## SaaS Backup data centers

SaaS Backup data centers are operated from North America, Europe, and Asia-Pacific-Japan. Each serviced region operates two load-balanced data centers that are located in proximity of one another.

## Veritas SaaS Backup - Data Hosting Locations



Each regional pair of data centers is physically separated. Each facility is designed to run all the time, and employs various measures to help protect operations from power failure, physical intrusion, and network outages. Data is automatically replicated at the storage layer to help guard against unexpected hardware failures. Data centers ensure that the data is available when you need it. Four copies of data are available within a single region.

To troubleshoot the Azure Active Directory Conditional Access or other issues, you need the Veritas public IP addresses.

Veritas has two public gateway IP addresses for each region:

- **EU:** 212.97.158.49 and 212.97.158.53
- **US:** 216.170.117.4 and 216.170.117.5
- **AP:** 103.153.54.16 and 103.153.54.17
- **UK:** 185.221.244.16 and 185.221.244.17

## System requirements

SaaS Backup fully supports the following Internet browsers:



- Microsoft Edge
- Mozilla Firefox
- Opera
- Google Chrome
- Apple Safari

---

**Note:** SaaS Backup does not support mobile Web browsers.

---

## Technical and documentation support

Primary role of the support group is to respond to your specific queries about product features and functionalities. The support group also creates content for online documentation and the knowledge base. The support group collaboratively works with the other functional areas within the company to answer your questions in a minimum time.

The latest documentation is available on the following Veritas websites. Each document displays the date of the last update. Ensure that you have the current version of the documentation.

[www.veritas.com/support](http://www.veritas.com/support)

<https://sort.veritas.com/documents>

[https://www.veritas.com/content/support/en\\_US/dpp.SaaSBackup](https://www.veritas.com/content/support/en_US/dpp.SaaSBackup)

If you are already signed in to SaaS Backup, click the help icon shown in the following image to view the online help.



You can contact the support group for opening a new support case or managing your existing support cases.

**To create case:**

[https://www.veritas.com/content/support/en\\_US/manageCases/createCase.html](https://www.veritas.com/content/support/en_US/manageCases/createCase.html)

**To chat:** [https://www.veritas.com/content/support/en\\_US#](https://www.veritas.com/content/support/en_US#)

**To view phone directory:**

[https://www.veritas.com/content/support/en\\_US/contact-us.html](https://www.veritas.com/content/support/en_US/contact-us.html)

**To view support fundamentals:**

[https://www.veritas.com/content/support/en\\_US/terms/support-fundamentals.html](https://www.veritas.com/content/support/en_US/terms/support-fundamentals.html)

**To access SaaS Backup public API guide:**

[https://www.veritas.com/content/support/en\\_US/doc/SaaSBackup\\_API\\_Guide](https://www.veritas.com/content/support/en_US/doc/SaaSBackup_API_Guide)

SaaS Backup offers several functionalities to programmers through its accessible public APIs. PC backup client, iOS file access client and Web file access client can use these APIs for all operations on files as well as user settings. The SaaS Backup API is a RESTful API accessed over HTTPS. It is available at

<https://saasbackup.veritas.com>

# Getting started

This chapter includes the following topics:

- [Accessing SaaS Backup from your region](#)
- [Understanding administration interface](#)
- [Signing in to SaaS Backup](#)
- [Signing out from SaaS Backup](#)
- [Resetting a forgotten password](#)
- [Updating password and other account information](#)
- [Requesting a user license cancellation](#)
- [Upgrading the SaaS Backup subscription](#)

## Accessing SaaS Backup from your region

Depending on your working region or your choice at the provisioning, you can use the following links to access SaaS Backup User Interface.

**Europe-Middle East-Africa:** <https://eu.saasbackup.veritas.com>

**United Kingdom:** <https://uk.saasbackup.veritas.com>

**Americas:** <https://us.saasbackup.veritas.com>

**Asia-Pacific-Japan:** <https://ap.saasbackup.veritas.com>

## Understanding administration interface

After signing in to SaaS Backup, the administration console is displayed. It consists of the header with the notification icon, help icon, menu icon, and the user profile

icon. Below the header, the Connector page appears by default that displays all the added connectors with corresponding details such as the latest update time and the data size.

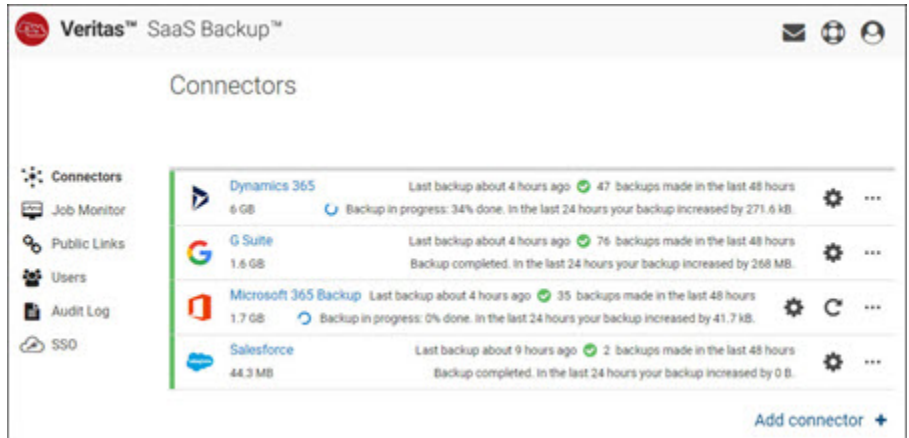













Table 2-1 explains the icons and their meaning in the SaaS Backup application.

**Table 2-1** SaaS Backup icons and description

Icons	Description
	<b>Notification icon</b> Click to view notifications sent to you in SaaS Backup.
	<b>Help icon</b> Click to view SaaS Backup help.
	<b>Menu icon</b> Click to view SaaS Backup menus.
	<b>User profile icon</b> Click to update account information and sign out from the SaaS Backup.
	<b>Share links icon</b> Click to view and copy the link of files and folders you want to share with others.
	<b>Job monitor icon</b> Click to monitor job status of connectors.

**Table 2-1** SaaS Backup icons and description (*continued*)

Icons	Description
 	<b>Edit icons</b> Click to update the corresponding details.
	<b>Delete icon</b> Click to delete selected items.
	<b>Manage access icon</b> Click to manage access to the connector and view a list of users with access.
	<b>Calender icon</b> Click to select a date.
	<b>Search icon</b> Click to get the search result.
	<b>Connectors icon</b> Click to go to the Connectors page.
	<b>Favorites icon</b> Click to add files and folders as a favorite. Use Favorites to keep your personal list of files and folders to access them quickly.
	<b>Audit icon</b> Click to view user wise audit log reports.
	<b>Users icon</b> Click to go to the Users page for adding, editing, and deleting users.
	<b>Single sign-on icon</b> Click to go to single sign-on (SSO) configuration page.

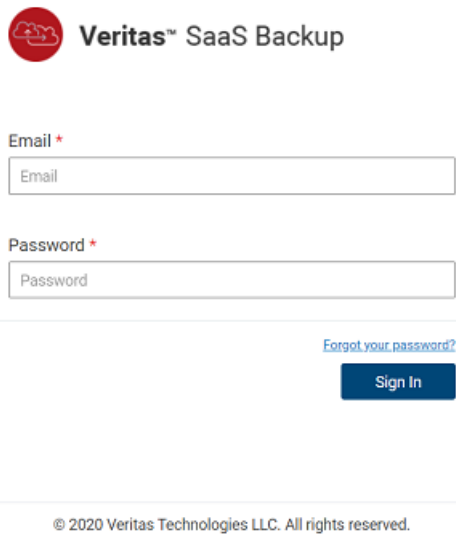
# Signing in to SaaS Backup

## To sign in to SaaS Backup

- 1 Enter the SaaS Backup URL in the internet browser.

See “[System requirements](#)” on page 8.

The authentication page appears.



The image shows the Veritas SaaS Backup authentication page. At the top, there is a red circular logo with a white cloud icon, followed by the text "Veritas™ SaaS Backup". Below this, there are two input fields: "Email \*" and "Password \*". The "Email \*" field has a placeholder text "Email". The "Password \*" field has a placeholder text "Password". To the right of the "Password \*" field, there is a link that says "Forgot your password?". Below the input fields, there is a blue button with the text "Sign In". At the bottom of the page, there is a copyright notice: "© 2020 Veritas Technologies LLC. All rights reserved."

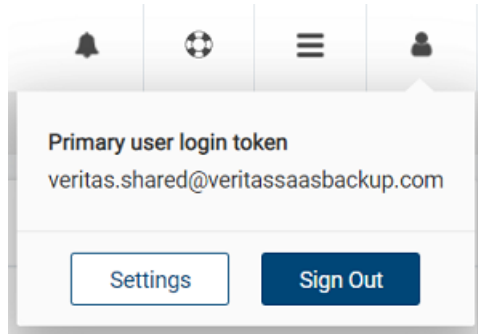
- 2 (Optional) Bookmark this URL in the SaaS Backup compatible internet browser.
- 3 Enter your user name and password in the authentication screen, and click **Sign In**.

After successful authentication, the SaaS Backup **Connectors** page appears.

# Signing out from SaaS Backup

To sign out from SaaS Backup

- 1 In the upper-right corner of the SaaS Backup console, click the user profile icon.



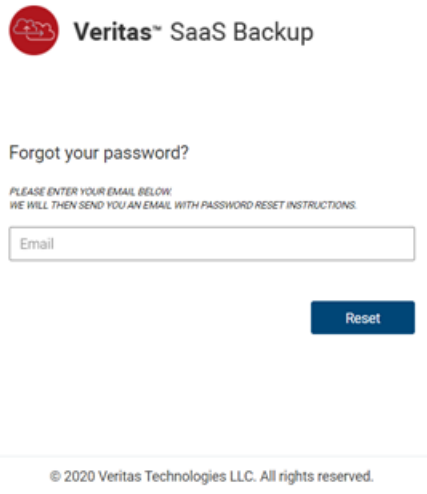
- 2 Click **Sign Out**.

## Resetting a forgotten password

If you forget your password and need help resetting it, SaaS Backup can help you by sending a link to your authenticated email address.

### To reset your forgotten password

- 1 In the authentication screen, click the **Forgot your password** link.  
The following page appears.



The screenshot shows the Veritas SaaS Backup password reset interface. At the top is the Veritas logo and the text 'Veritas™ SaaS Backup'. Below this is the heading 'Forgot your password?'. A subtext reads: 'PLEASE ENTER YOUR EMAIL BELOW. WE WILL THEN SEND YOU AN EMAIL WITH PASSWORD RESET INSTRUCTIONS.' There is a text input field labeled 'Email'. Below the field is a blue button labeled 'Reset'. At the bottom of the page, a footer line states: '© 2020 Veritas Technologies LLC. All rights reserved.'

- 2 In the **Email** field, provide your user email address.
- 3 Click **Reset**.

---

**Note:** SaaS Backup sends an email notification with the password resetting information on the provided email ID. If you do not receive a notification, check your spam or junk folder.

---

- 4 Click the reset password link in the received email.
- 5 Provide the requested information.

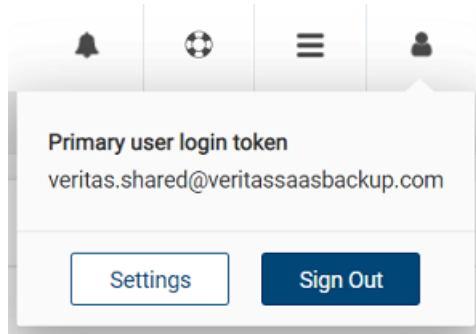
## Updating password and other account information

If you remember your password, but want to change it for a security reason, you can update it easily. In addition, you can update your email address, name, preferred language, password, and phone number.



## To update password and other account information

- 1 In the upper-right corner of the SaaS Backup console, click the user profile icon.



- 2 Click **Settings**.

The **Account information** dialog box appears.

The screenshot shows the "Account Settings" dialog box. The title "Account Settings" is at the top. The form is divided into three main sections: "Name", "Service Information", and "Billing and Invoices".

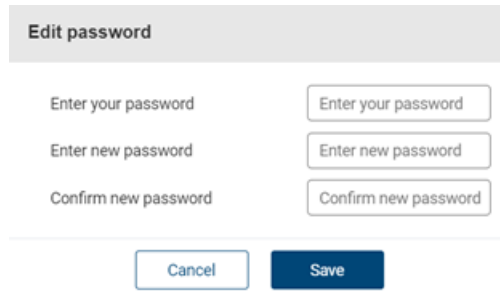
- Name:**
  - Name: larry.potter@veritas.com
  - Email: larry.potter@veritas.com
  - Language: English (with a dropdown arrow)
  - Password: (input field)
  - Confirm password: (input field)
- Service Information:**
  - Subscription: bvb13h-5cpzdi-a5qlx7
  - Service Expiration Date: unlimited
  - Licenses:**
    - Office 365: 20 of 10000 used
    - Salesforce: 6 of 10000 used
    - Sharepoint users: 19 of 10000 used
    - G Suite: 3 of 10000 used
    - Office 365 data retention: 1 months
    - Salesforce data retention: 1 months
    - G Suite data retention: 1 months
    - Dynamics 365 data retention: 1 months
  - Cancel subscription
  - Upgrade subscription
- Billing and Invoices:**
  - Product: Veritas\_Spearhead\_2020
  - Storage used: 9.3 GB
  - Sign out everywhere

At the bottom right, there are two buttons: "Back" and "Save".

- 3 Click the edit icon next to the item that you want to change.

- 4 Specify new information, and click **Save**.

For example, click the edit icon next to the Password, provide your existing password, specify a new password, rewrite the new password for confirmation, and click Save.



The screenshot shows a form titled "Edit password" in a light gray header. Below the header, there are three rows of input fields. The first row is labeled "Enter your password" and has a corresponding input box. The second row is labeled "Enter new password" and has a corresponding input box. The third row is labeled "Confirm new password" and has a corresponding input box. At the bottom of the form, there are two buttons: a light blue "Cancel" button and a dark blue "Save" button.

- 5 Click **Save**.

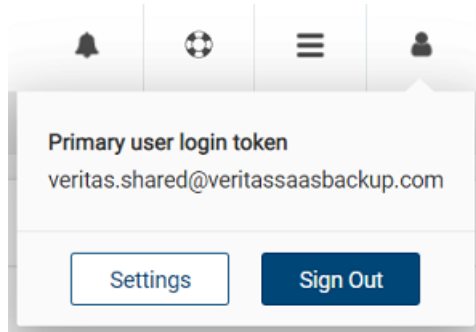
## Requesting a user license cancellation

Immediately after expiration or termination of services, you cannot access (sign in) the SaaS Backup administration console and perform new backup jobs.

For more information, see [SaaS Backup Licensing Guide](#)

## To request a user license cancellation

- 1 In the upper-right corner of the SaaS Backup console, click the user profile icon.



- 2 Click **Settings**.

The **Account information** dialog box appears.

### Account Settings

<p>Name larry.potter@veritas.com</p> <p>Email larry.potter@veritas.com</p> <p>Language English</p> <p>Password</p> <p>Confirm password</p>	<p><b>Service information</b></p> <p>Subscription: <b>bubt3h-5cpzdi-a5qlx7</b></p> <p>Service Expiration Date: <b>unlimited</b></p> <p><b>Licenses</b></p> <p>Office 365: <b>20 of 10000 used</b></p> <p>Salesforce: <b>6 of 10000 used</b></p> <p>Sharepoint users: <b>19 of 10000 used</b></p> <p>G Suite: <b>3 of 10000 used</b></p> <p>Office 365 data retention: <b>1 months</b></p> <p>Salesforce data retention: <b>1 months</b></p> <p>G Suite data retention: <b>1 months</b></p> <p>Dynamics 365 data retention: <b>1 months</b></p> <p><a href="#">Cancel subscription</a></p> <p><a href="#">Upgrade subscription</a></p>	<p><b>Billing and invoices</b></p> <p>Product: <b>Veritas_Spearhead_2020</b></p> <p>Storage used: <b>9.3 GB</b></p> <p><a href="#">Sign out everywhere</a></p>
--	---	--

Back Save

**3 Click **Request cancellation**.**

The application opens a request email in your Microsoft Outlook.

**4 Provide the details, and send the email to [returnsandcancellations@veritas.com](mailto:returnsandcancellations@veritas.com).**

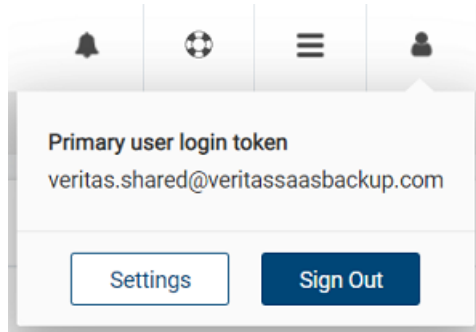
## Upgrading the SaaS Backup subscription

Upgrading the subscription lets you use the product licenses during a specified period of time. Licenses include access to the administration console, audit log, job monitor, single sign-on support, role-based access control, unlimited retention, and 24x7 support.

For more information, see [SaaS Backup Licensing Guide](#)

## To upgrade the SaaS Backup subscription

- 1 In the upper-right corner of the SaaS Backup console, click the user profile icon.



- 2 Click **Settings**.

The **Account information** dialog box appears.

### Account Settings

<p>Name larry.potter@veritas.com</p> <p>Email larry.potter@veritas.com</p> <p>Language English</p> <p>Password</p> <p>Confirm password</p>	<p><b>Service information</b></p> <p>Subscription: <b>bubt3h-5cpzdi-a5qlx7</b></p> <p>Service Expiration Date: <b>unlimited</b></p> <p><b>Licenses</b></p> <p>Office 365: <b>20 of 10000 used</b></p> <p>Salesforce: <b>6 of 10000 used</b></p> <p>Sharepoint users: <b>19 of 10000 used</b></p> <p>G Suite: <b>3 of 10000 used</b></p> <p>Office 365 data retention: <b>1 months</b></p> <p>Salesforce data retention: <b>1 months</b></p> <p>G Suite data retention: <b>1 months</b></p> <p>Dynamics 365 data retention: <b>1 months</b></p> <p><a href="#">Cancel subscription</a></p> <p><a href="#">Upgrade subscription</a></p>	<p><b>Billing and invoices</b></p> <p>Product: <b>Veritas_Spearhead_2020</b></p> <p>Storage used: <b>9.3 GB</b></p> <p><a href="#">Sign out everywhere</a></p>
--	---	--

Back
Save

**3 Click Upgrade subscription.**

The application opens a request email in your Microsoft Outlook.

**4 Provide the details, and send the email to [customercare@veritas.com](mailto:customercare@veritas.com).**

# Managing notifications

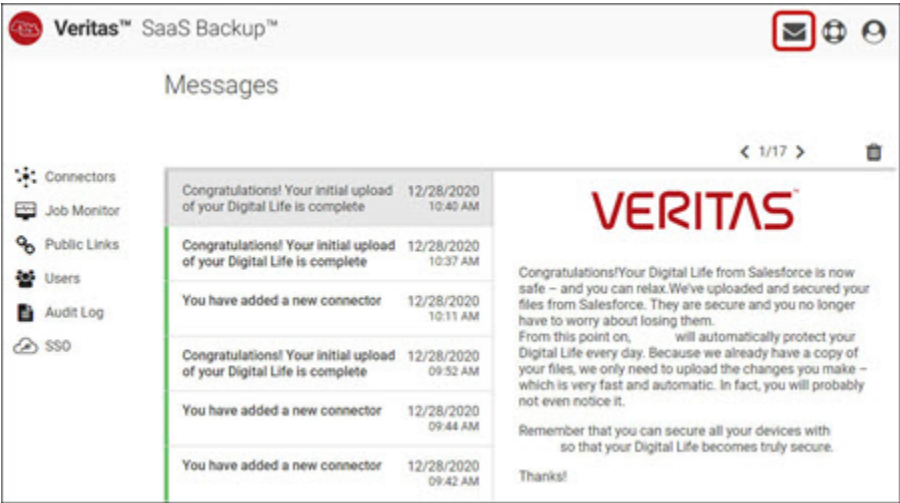
This chapter includes the following topics:

- [Viewing notifications](#)
- [Predefined email notifications](#)
- [Deleting multiple notifications](#)

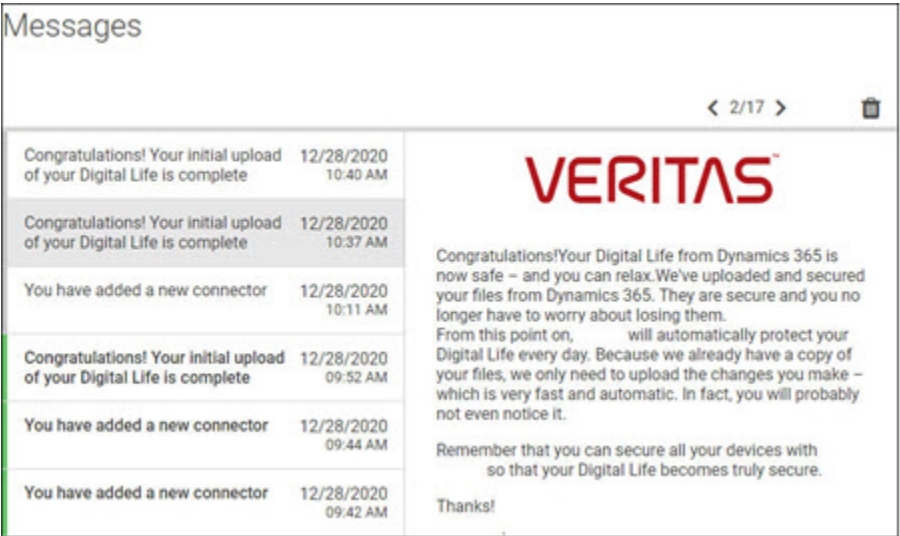
# Viewing notifications

## To view notifications

- 1
- In the upper-right corner of the SaaS Backup console, click the notification icon.



- 2
- Click on the message you want to read.
- The message preview appears.



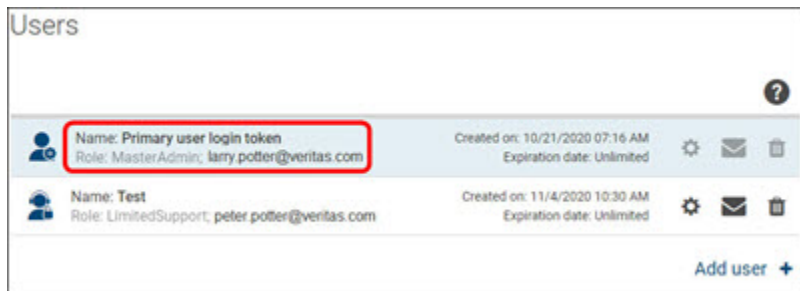
- 3
- Click **Delete** to delete the selected message from the list.



- 4 Click > to view the next message.
- 5 Click < to view the previous message.
- 6 To close the message board, click outside the message board.

## Predefined email notifications

SaaS Backup generates the following email messages, and sent these notifications to the Primary SaaS Backup Administrator from **no-reply@saasbackup.veritas.com** when required.

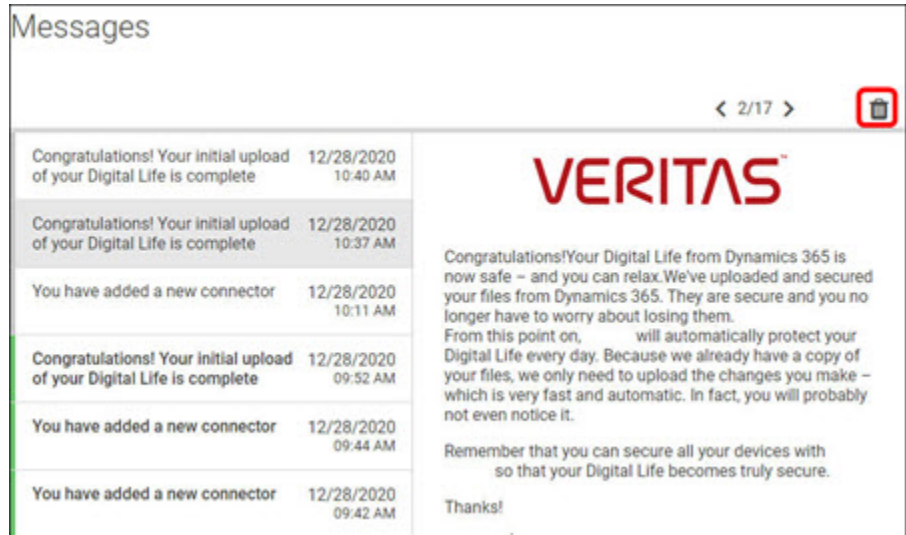


- Welcome to Veritas SaaS Backup
- Forgot Password
- Health changed (Connector Status changes to Critical)
- Approaching license limit (80% of your total purchased SaaS Backup licenses)
- Reached maximum license limit
- Approaching 30 days from subscription end date
- Approaching 60 days from subscription end date
- Approaching 90 days from subscription end date
- Account has expired
- Insufficient licenses to backup SharePoint/Google Sites/Salesforce

# Deleting multiple notifications

To delete multiple messages simultaneously

- 1 In the upper-right corner of the SaaS Backup console, click the notification icon



- 2 To remove all messages at a time, click the **Select** check-box and click **Delete selected messages**.
- 3 To remove specific messages at a time, click the check-boxes adjacent to those messages, and click **Delete selected messages**.

# Managing users and roles

This chapter includes the following topics:

- [About users, user roles, and associated permissions](#)
- [Configuring access to connectors](#)
- [Creating user profiles](#)
- [Updating user profile details](#)
- [Deleting user profiles](#)

## About users, user roles, and associated permissions

Figure 4-1 and Table 4-1 explain the predefined user roles and their permissions in SaaS Backup.

**Figure 4-1** User roles and associated permissions

Veritas Saas Backup - Administrator Roles							
	Master Administrator	Backup Administrator	Full Support	Standard Support	Limited Support	Audit	SSO
Create Connector	✓	✓					
Delete Connector	✓	✓					
Configure Connector	✓	✓					
Restore in Place	✓	✓	✓	✓			
Restore to Folder	✓	✓	✓	✓	✓		
Item Restore	✓	✓	✓	✓			
Import: Skip	✓	✓	✓	✓	✓		
Import: Overwrite	✓	✓	✓	✓			
Import: Rename	✓	✓	✓	✓	✓		
Preview Items	✓	✓	✓				
Download Items	✓	✓	✓				
Share	✓	✓	✓				
View Audit Log	✓					✓	
View Job Monitor	✓	✓	✓	✓			
Create User Roles	✓	✓					
Edit User Settings	✓	✓					
Manage access to connectors	✓	✓					
Configure SSO	✓						✓

**Table 4-1** User roles and associated permissions

User role	Associated permissions
Master administrator	<p>Create connectors</p> <p>Delete connector</p> <p>Configure connector</p> <p>Preview files</p> <p>Download files and folders</p> <p>Share files and folders</p> <p>Import files by using the <b>Skip duplicate files</b> method. Restore files across a connector to folder</p> <p>Import files by using the <b>Overwrite duplicate files</b> method. Restore files across a connector in place and to folder. User can perform an item restore.</p> <p>Import files by using the <b>Rename duplicate files</b> method</p> <p>View audit logs</p> <p>Configure Single sign-on</p> <p>Manage access to connectors</p>
Backup administrator	<p>Create connectors</p> <p>Delete connector</p> <p>Configure connector</p> <p>Preview files</p> <p>Download files and folders</p> <p>Share files and folders</p> <p>Import files by using the <b>Skip duplicate files</b> method. Restore files across a connector to folder</p> <p>Import files by using the <b>Overwrite duplicate files</b> method. Restore files across a connector in place and to folder. User can perform an item restore.</p> <p>Import files by using the <b>Rename duplicate files</b> method</p> <p>Manage access to connectors</p>

**Table 4-1** User roles and associated permissions (*continued*)

User role	Associated permissions
Full support user	Preview files Download files and folders Share files and folders Import files by using the <b>Skip duplicate files</b> method. Restore files across a connector to folder Import files by using the <b>Overwrite duplicate files</b> method. Restore files across a connector in place and to folder. User can perform an item restore. Import files by using the <b>Rename duplicate files</b> method
Standard support user	Import files by using the <b>Skip duplicate files</b> method. Restore files across a connector to folder Import files by using the <b>Overwrite duplicate files</b> method. Restore files across a connector in place and to folder. User can perform an item restore. Import files by using the <b>Rename duplicate files</b> method
Limited support user	Import files by using the <b>Skip duplicate files</b> method. Restore files across a connector to folder Import files by using the <b>Rename duplicate files</b> method
Audit user	View audit logs
Single sign-on administrator	Configure Single sign-on

These permissions are used to create administrators who can access the entire system. These administrators do not affect the licensing of the solution. Therefore, there can be indefinite users in each group.

By default, the first user who sign in to SaaS Backup, automatically becomes a Master Administrator. The Master Administrator profile cannot be edited or deleted. The master administrator can add, edit, and delete additional administrators and user roles.

Based on your roles and permissions, you can access specific connectors, configure connectors, manage users, monitor data backup jobs, access backup data, and restore it. This role-based access control capability of SaaS Backup ensures information safety and data protection of your tenant, which may be distributed over multiple connectors.

# Configuring access to connectors

Before you begin, ensure that you are aware of the following roles and have appropriate permissions to manage access to connectors.

- Master administrator has universal access to all connectors and can configure connector access for other users too. Master administrator can prevent customers from being locked out from connectors.
- Audit user has universal access to check the audit logs of every connector, but cannot configure connector access for other users.
- Backup administrators have access to the connectors that are created by them, but cannot configure connector access for other users.
- Single sign-on administrator has access to single sign-on configurations, but cannot configure connectors or data.

---

**Note:** Access rights of master administrator, audit user, backup administrator, and single sign-on administrator cannot be changed or deleted.

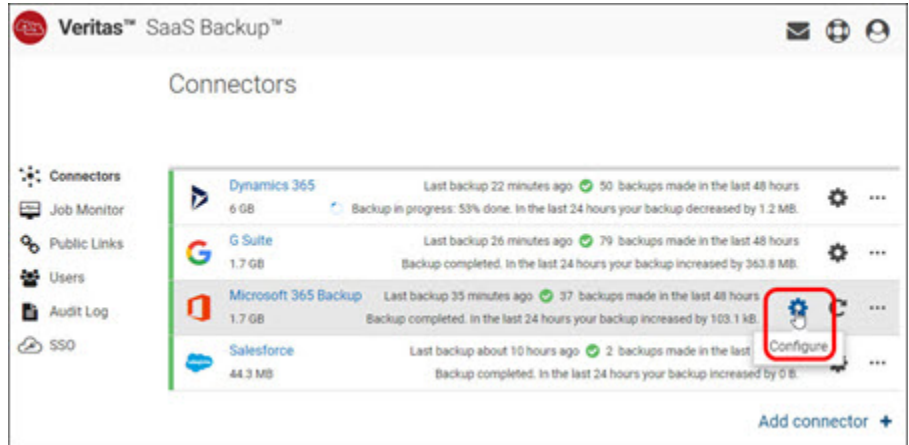
---

Unless the master or the backup administrator restricts the access, all the existing users can access the connectors that are created before the launch of SaaS Backup Q1 2020. Users with the restricted access cannot:

- View the unavailable connectors, their status, and the size
- Browse files and folders
- Restore backup

### To configure access to connectors

- 1 On the **Connectors** page, select the connector, and click the edit icon.











2 Click **Configure connector**.



Microsoft 365 Connector Configuration

Connector Name  
Microsoft 365 Backup




  
☒  
Exchange  
Backup enabled  
 [Configure](#)

  
☒  
OneDrive  
Backup enabled  
 [Configure](#)

  
☒  
SharePoint  
Backup enabled  
 [Configure](#)


  
☒  
Groups & Teams  
Backup enabled  
 [Configure](#)

**Save** **Cancel**


  

- 3 Click the manage access icon (lock icon) to view the **Access to Office 365** page.

Access to Microsoft 365 Connector



Here you can see a list of users that have access to your connector. It is not possible to change the access for Master Administrators, SSO Admins, or Audit users.



Users

Users whose access can be changed

☒ Test - LimitedSupport - larry.potter@veritas.com

Users whose access cannot be changed

☒ Primary user login token - MasterAdmin - larry.potter@veritas.com

Save selection

Cancel

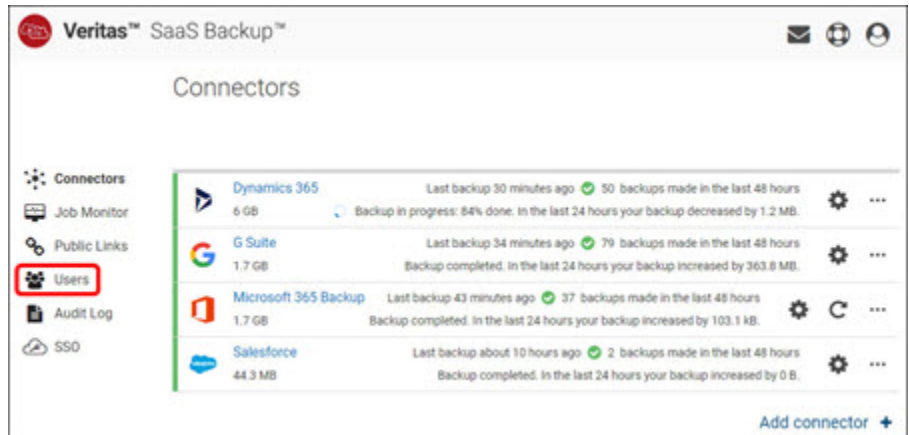
- 4 To provide access, select the check-boxes adjacent to users.
- 5 To revoke access, clear the check-boxes adjacent to users.
- 6 Click **Save**.

# Creating user profiles

You must have the master administrator role to add new user profiles in SaaS Backup.

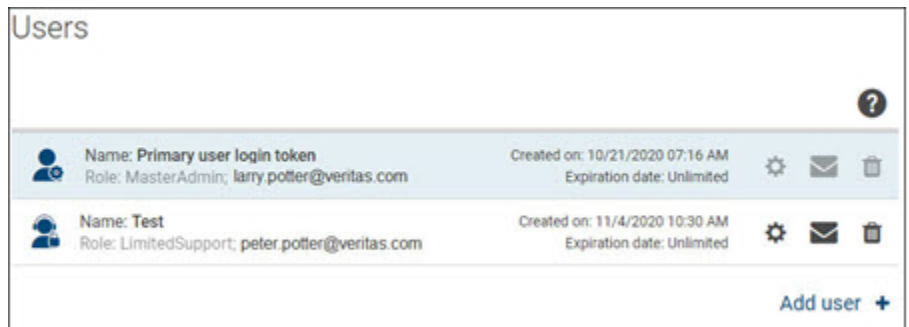
## To create a new user profile

- 1 In the upper-right corner of the SaaS Backup console, click the menu icon.



- 2 Click **Users**.

The **User List** page appears.



**3** Click **Create user**.

**4** In the **Create new user** dialog box, specify the following information.

Field	Description
Role	Select the user role that you want to assign to a user.  See <a href="#">“About users, user roles, and associated permissions”</a> on page 27.
Permissions	View the permissions associated with the selected user role.
Name	Enter name of a user.
Email	Enter email address of a user.
Send activation mail	Select this check-box to notify a user about its user profile activation.
Password	Provide a password to access a user profile.
Confirm password	Retype the same password to confirm its correctness.
Expire time	Specify the user profile expiry time.

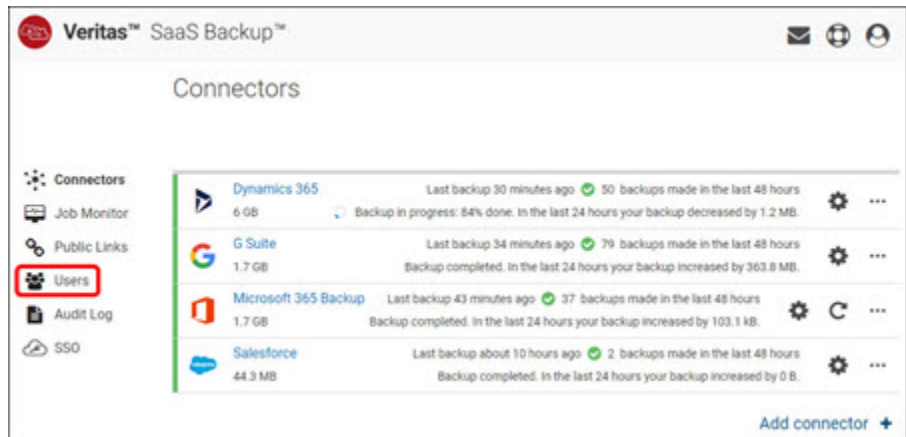
- 5 Click **Create user**.
- 6 Click **Done**.

## Updating user profile details

You must have the master administrator role to edit user profiles in SaaS Backup.

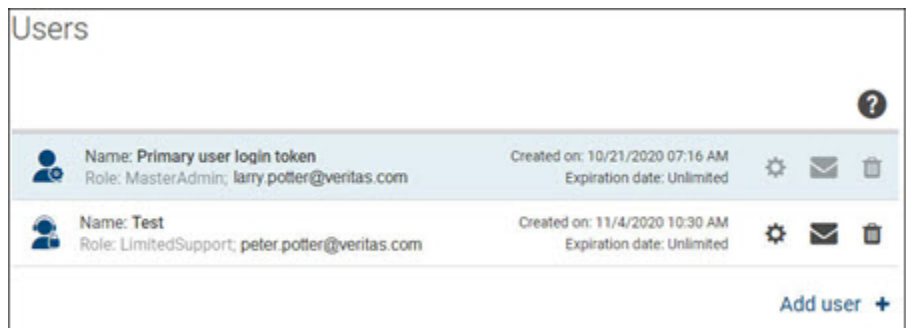
### To update a user profile

- 1 In the upper-right corner of the SaaS Backup console, click the menu icon.



- 2 Click **Users**.

The **User List** page appears.



- 3 Click the edit icon next to the user profile that you want to edit.

**4** Update the following information:

Field	Description
Role	Select the user role that you want to assign to a user. See <a href="#">“About users, user roles, and associated permissions”</a> on page 27.
Permissions	View the permissions associated with the selected user role.
Name	Enter name of a user.
Email	Enter email address of a user.
Password	Provide a password to access a user profile.
Confirm password	Retype the same password to confirm its correctness.
Expire time	Specify the user profile expiry time.

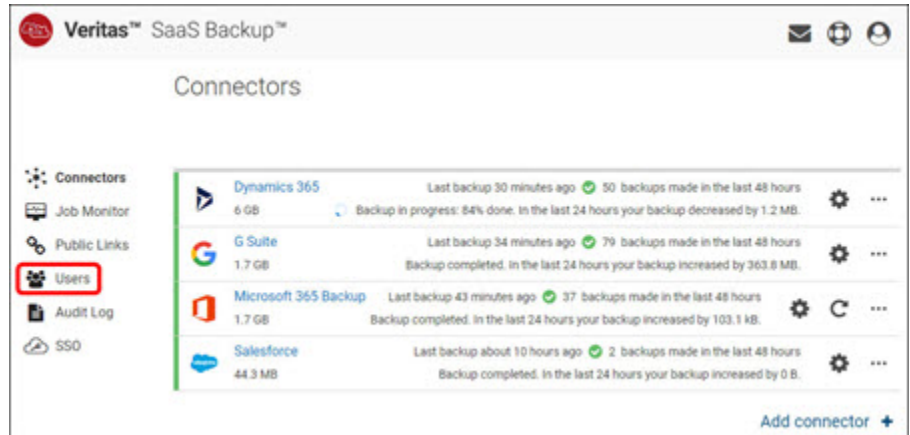
**5** Click **Update user**.

## Deleting user profiles

You must have the master administrator role to delete user profiles in SaaS Backup.

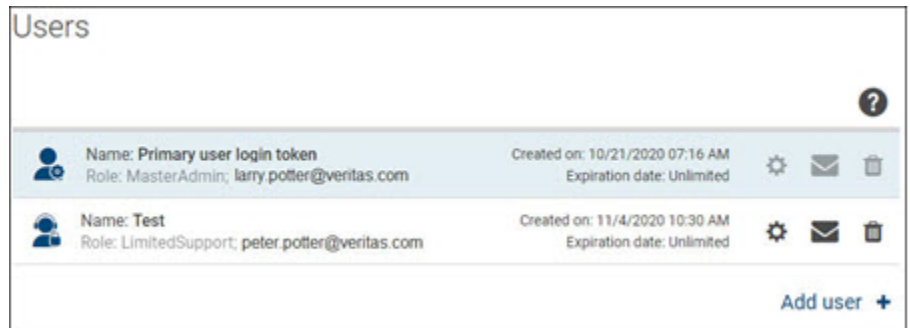
## To delete a user profile

- 1 In the upper-right corner of the SaaS Backup console, click the menu icon.



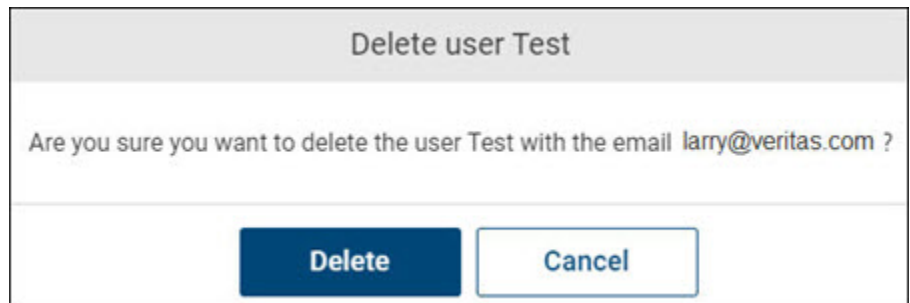
- 2 Click **Users**.

The **User List** page appears.



- 3 Click the delete icon next to the user profile that you want to delete.

The application prompts you to confirm that you want to perform the operation.



- 4** Click **Yes** to complete the operation or click **Cancel** to cancel it.
- 5** Click **Done**.



# Managing connectors

This chapter includes the following topics:

- [About connectors](#)
- [Common connector-specific operations](#)
- [Reactivating connectors](#)
- [Scheduling the data backup frequency](#)
- [About snapshots](#)

## About connectors

Connectors, also referred as cloud connectors, serve as a communication channel between the platform (Office 365, Dynamics 365, Google G suite, and Salesforce) and the SaaS Backup data centers. Cloud connectors represent the backup of a cloud service, and enable you to restore and share files and folders available on these platforms.

Master and backup administrator can create, configure, and delete the connectors. SaaS Backup generates connector-specific audit logs when connectors are created, updated, and deleted. Master administrator can access all the available connectors, and prevents customers from being locked out from the associated connectors. Other users such as support administrators and auditors can then back up, restore, download, and share the files and folders available on those connectors. Users with the restricted access cannot view connector status and size, and cannot browse or restore data.

To back up cloud services, you must first create and configure cloud connector services. Users need credentials to access the connector services. After creating a connector, SaaS Backup asks for permission for the first time, and then retains the permissions it needs for future.

Creating a separate connector for each workload is the best practice. For example, creating a separate connector for each workload such as Microsoft Exchange, OneDrive, and SharePoint leads to better back up performance as you can set different retention periods per connector.

After configuring connectors, the backup process starts immediately. However, it takes time to get pushed to the top of the queue of the scheduled backup jobs. You cannot manually schedule time to start backup jobs. There can be only one backup job in progress per connector.

SaaS Backup sends a notification to inform you when the health status of the connector changes to Critical.

## Common connector-specific operations

A cloud connector represents the backup of platforms services. Some operations are common across all these platforms. These operations are explained in detail in the chapters for managing respective platforms. The commonly used operations are as follows:

### **Adding cloud connectors**

You can add connectors for all the above-mentioned platforms. When you add a connector, you need to provide a unique name for the connector so that you can identify it easily. You need access to the corresponding platform APIs and administrative permissions to access all the data of their agents.

### **Deleting cloud connectors**

You can delete an expired or outdated cloud connector service. You need permissions to delete cloud connectors.

**Restoring files and folders on cloud connectors:** You can easily locate your data and restore the files and folders by using partial snapshots, indexed snapshots, or complete snapshot. You can restore the previous version of a file and folder.

### **Monitoring jobs of cloud connectors**

You can monitor the backup and restore job status and the job statistics.

### **Sharing files and folders of cloud connectors**

You can generate a public share link and share it with the authorized users so that these users can view, analyze, and download the files and folders.

### **Downloading files and folders cloud connector**

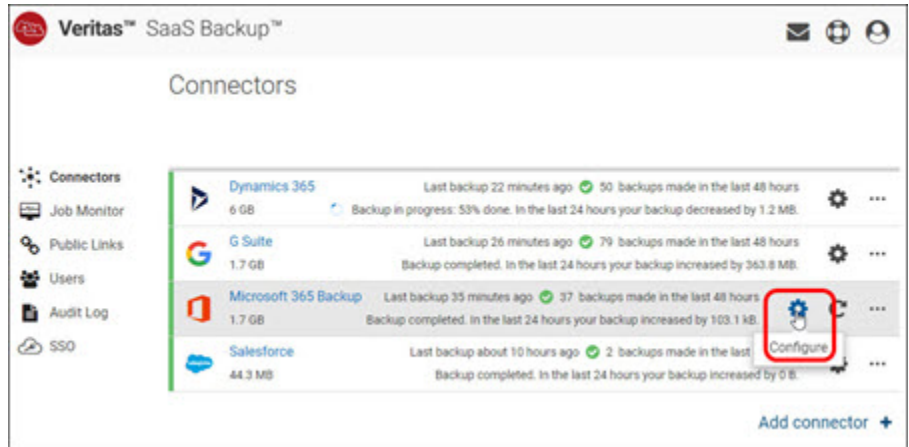
You can download the entire folder with the latest data or the specific version of files and folders within it.

## Reactivating connectors

You can reactivate the connector that is scheduled for deletion. It lets you access and collect data of such connectors until their retention period.

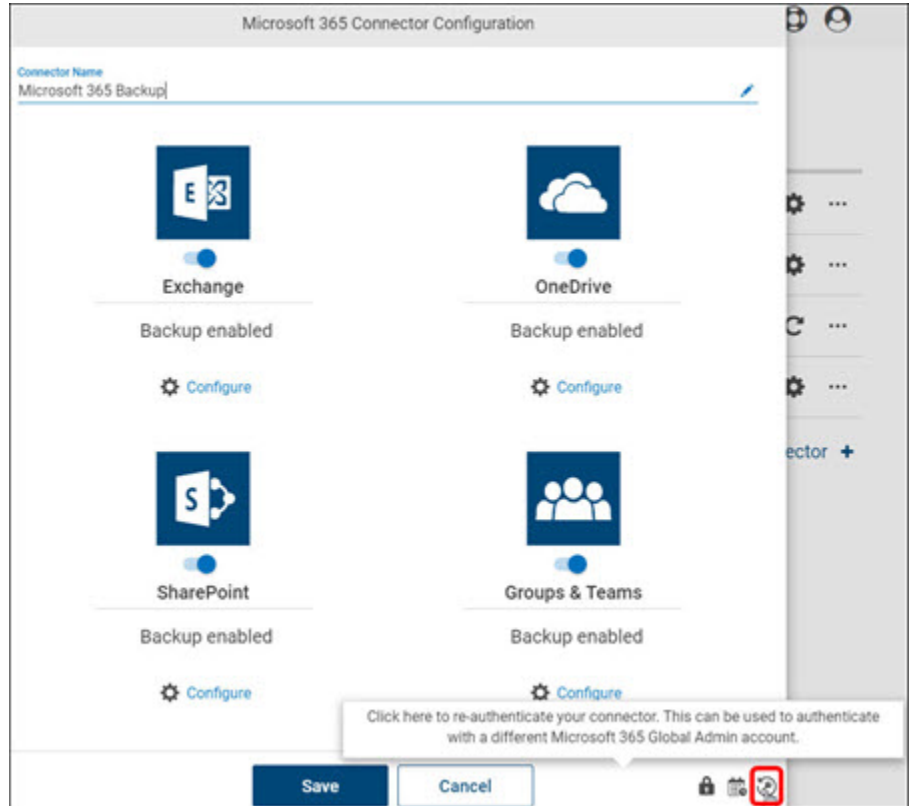
### To reactivate the connector that has scheduled for deletion

- 1 On the **Connectors** page, select the Office 365 cloud connector that is scheduled for deletion.



- 2 Click **Edit**, and select **Configure connector**.

The configuration dialog box appears.



- 3 Click the grayed-out open **Delete** icon.

The connector appears on the **Connectors** page with access to all its data.

## Scheduling the data backup frequency

SaaS Backup schedules two backup jobs per day by default. The backup jobs are scheduled automatically to run every 12 hours. The first backup starts immediately when you configure a connector. It takes some time to display it in the queue of scheduled backup jobs. You cannot manually schedule backup jobs at a specific time. There can be only one backup job in progress per connector.

You can understand the backup job schedule and frequencies through the following examples.

- If a backup job starts at 8:00 A.M. and lasts for less than 12 hours, the next backup job gets scheduled to start at 8:00 P.M.
- If a backup job starts at 8:00 A.M. and took more than 12 hours to complete, say 14 hours, then the next backup job starts immediately after the previous backup job completes. It means that the next backup job will start at 10:00 P.M. The next checkpoint for the following backup job will be 10:00 A.M., unless it took longer than 12 hours.

Customers can request to increase the back-up frequency for their account. In such situation, the SaaS Backup support team analyzes the backup performance of the customer account, understand customer environment, and determine the optimal approach. Sometimes increasing the backup frequency can affect the SaaS Backup performance due to API throttling limits. In such situation, the back-up frequency cannot be increased or decreased as per customer request.

The factors that can affect the back-up frequency are as follows:

### **Backup stages**

A backup has an initial stage and an incremental stage. The initial backup takes longer time and can last for several days or even weeks. Usually, there is one backup job over the whole period of onboarding. Incremental backups tend to run as defined by the environment configuration as the data changes are backed up during this stage.

### **Backup job duration**

When the duration of a backup job lasts for an extended period of time, there may be fewer backup jobs for that specific connector. SaaS Backup by default schedules two backup jobs per day, which on average each job takes not more than 12 hours. However, if the backup jobs last longer than 12 hours, there will be the fewer backup jobs that day.

### **Connector configuration changes**

After the onboarding stage is over, the customer can decide to add a new type of data to the connector. It means that the backup must again go through the initial stage for that data type. SaaS Backup continues to incrementally back up the previously selected data types. However, the overall duration of the backup changes.

### **External factors**

Several external factors, such as throttling, cloud service maintenance, errors on the side of the cloud service provider, migration of customer data, and customer setup, can affect the backup performance. Throttling is the most serious factors for backup job failure. It causes the backup job to take longer than usual time as following the best practices of a cloud service provider, the product allocates a certain number of retries to finally process the data.

### **Changes made to the data in the cloud**

Even if the customer has selected all data types for back up, some data might still remain in the migration process. Whenever a new job starts, there can be a lot of new data to be backed up even though the initial backup stage is over.

### **Data added to the backup**

Every customer has different data to be secured. Some customers have a lot of Exchange data, others may have more SharePoint data. While there are some mechanisms to improve the backup performance of Exchange data, there is no way for the product to influence the external factors that may slow down the backup. Number of files and their sizes can affect the job. The smaller items that are present in the customer tenant, the longer the backup job can take. It is because the product needs to process each file separately. In this case, the backup speed may seem to be slower than expected, even though the number of secured files increases quickly.

## **About snapshots**

In SaaS Backup, snapshot is a type of copied data at a specific time that is used to restore the files and folders of a particular cloud connector. A view history can contain multiple snapshots of the same connector.

### **Partial snapshots**

Until an entire backup has been completed, these partial snapshots are displayed in the SaaS Backup application, giving users access to the data that is currently in the backup. Users must remember that a partial snapshot might not contain the data they want to recover. After backing up the entire data, SaaS Backup does not show any partial snapshot. After restoring the complete backup, new partial snapshots appear again when new backup starts.

When SaaS Backup displays only partial snapshot, it is recommended to browse and ensure the availability of data in the connector. You can create a public link of a snapshot that restricts data to that specific snapshot.

### **Index snapshots**

The process of capturing the index snapshot is incremental. In the process, SaaS Backup analyses the list of the index files that are already stored on the connectors. SaaS Backup adds the files that are newly created or changed since the last snapshot.

### **Complete snapshots**

When the entire backup is completed, the completed snapshots are displayed in the SaaS Backup application. You can restore the complete data by using the completed snapshots.

When SaaS Backup displays the partial and the complete backup snapshot, it is recommended to import and restore from the complete snapshot to recover the entire data.



# Managing public share links

This chapter includes the following topics:

- [About public links](#)
- [Generating public share links for sharing data](#)
- [Deleting public share links](#)

## About public links

The master administrator, backup administrator, and the full support administrator can generate and share public links with other users. If you are one of them, you can generate public share links of the file or a folder available in the connectors. Users with the standard support, limited support, single sign-on administration, and the auditor roles cannot generate the links.

When the file is sent as a link, the user always receives the latest version of the file and the folder. Users do not require a SaaS Backup account to access the content of shared links. Users can directly browse and download the shared data.

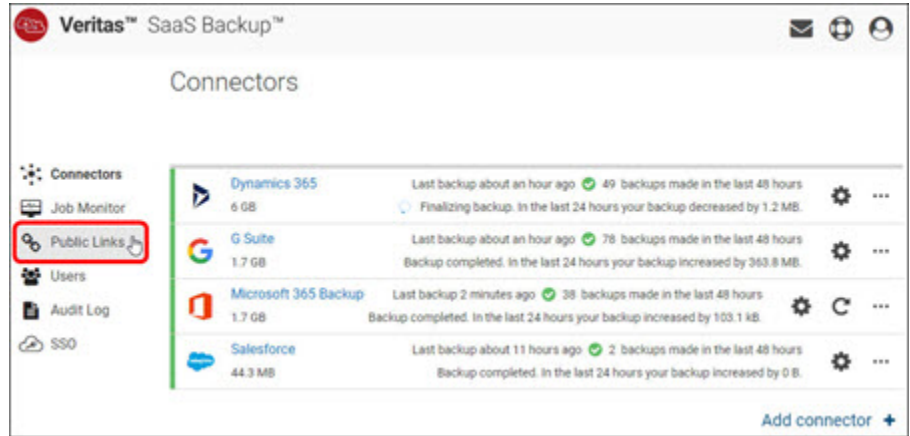
You can create a public link for a previous snapshot that restricts the public link to the content of that specific snapshot.

To ensure information safety, you can set a password for the public share link. Before opening the shared content, user needs to type the password. You can set an expiration date for the link. After the specified number of days, the public share link is not accessible.

# Generating public share links for sharing data

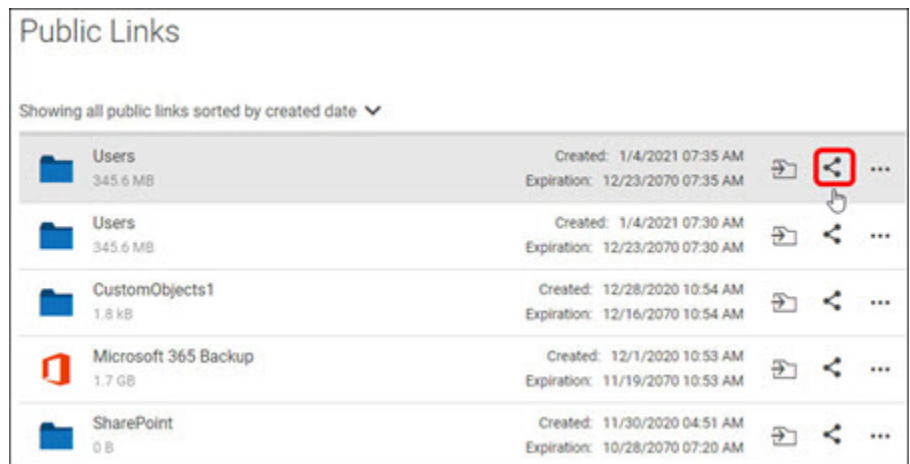
## Method 1: To generate a public share link

- 1 In the upper-right corner of the SaaS Backup console, click the menu icon.



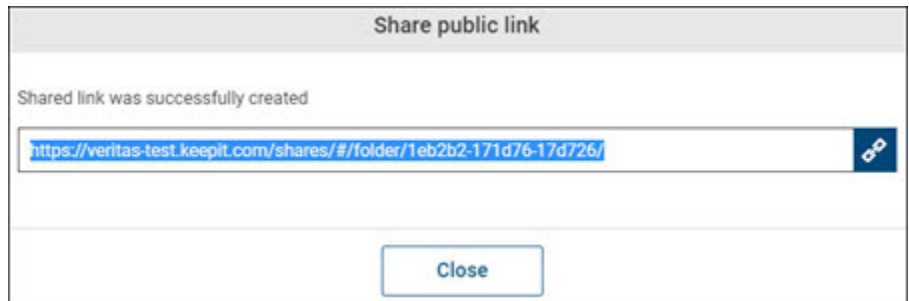
- 2 Click **Links**.

The application displays a list of available files and folders of all connectors.



- 3 Navigate to the file or the folder you want to share, and click the share icon in the same row.

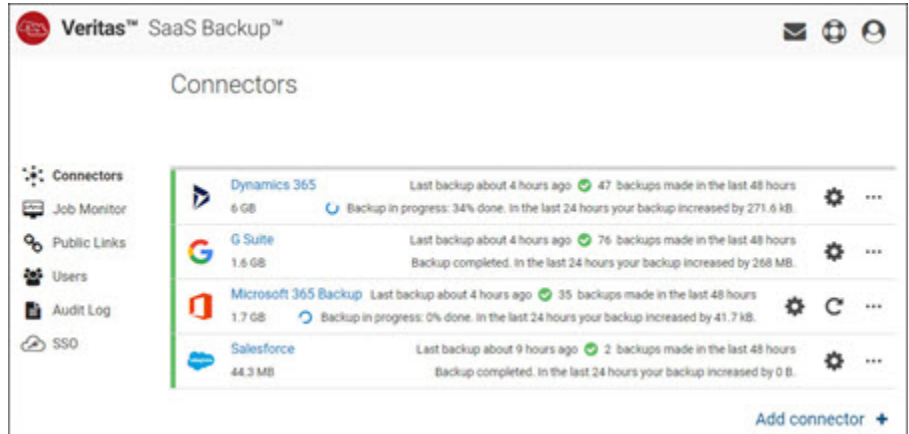
The application opens the **Share public link** page.



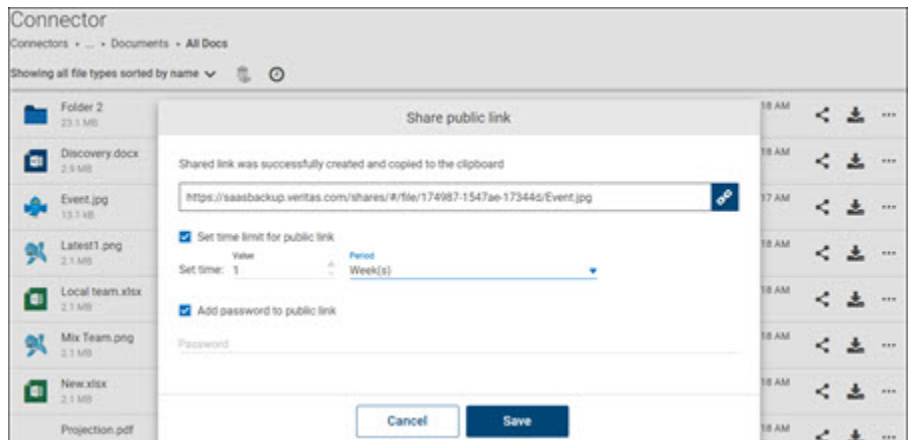
- 4 Copy the link to share with the user, and click **Close** to exit this page.

## Method 2: To generate a public share link from the Connectors page

- 1 On the **Connectors** page, click the appropriate cloud connector.



- 2 Navigate to the file or folder you want to share, and click the **Share** icon in the same row.



- 3 In the **Share public link** dialog box, specify the following information:

Field	Description
Time limit public link	Select this check-box to view the <b>Set expiration time</b> field.
Set expiration time	Set the expiration time of a public share link.
Password protect public link	Select this check-box to specify the password for user to access the shared content. You need to share this password with the user via email.

- 4 Click **Save**.

The application opens the **Share public link** page.

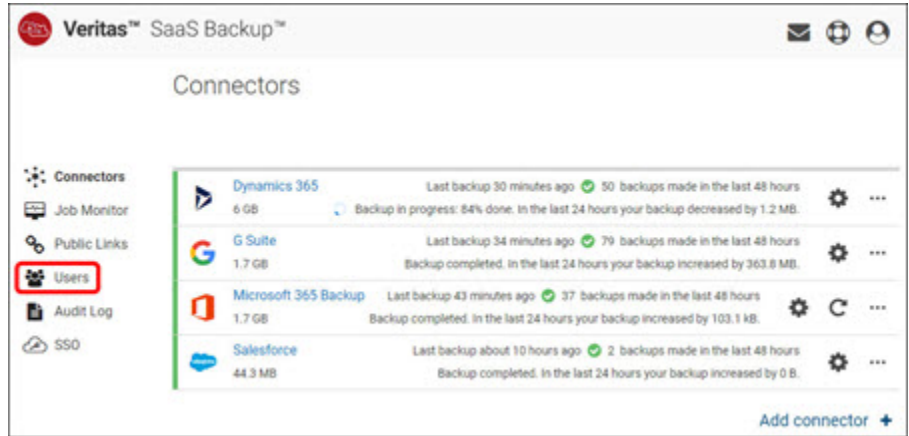


- 5 Copy the link to share with the user, and click **Close** to exit this page.

# Deleting public share links

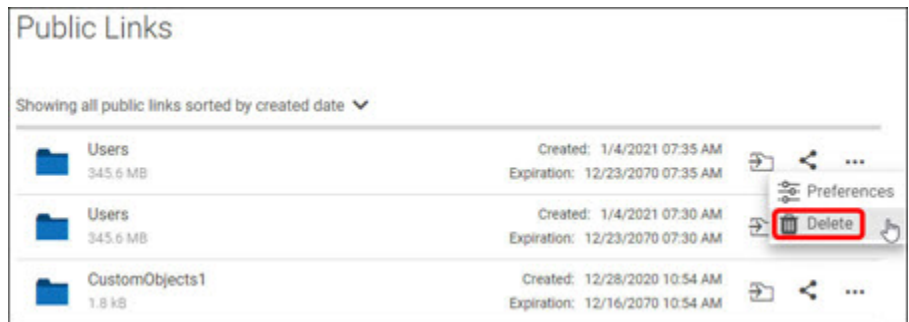
To delete a public share link

- 1 In the upper-right corner of the SaaS Backup console, click the menu icon.

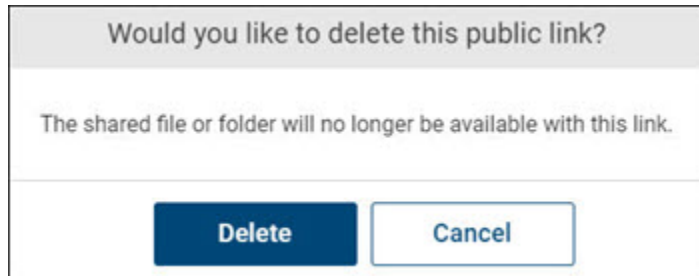


- 2 Click **Links**.

The application displays a list of available files and folders of all connectors.



- 3 Navigate to the file or folder you want to share, and click the delete icon in the same row.



- 4 Click **Yes** to complete the operation or click **Cancel** to cancel it.

# Monitoring backup and restore jobs

This chapter includes the following topics:

- [About backup and restore jobs monitoring](#)
- [Understanding the backup and restore job monitoring process](#)
- [Viewing backup and restore jobs and statistics](#)
- [Calculating the estimated time for a job completion](#)
- [Calculating the size of data you have in Office 365](#)
- [Downloading job status report](#)

## About backup and restore jobs monitoring

For improved operations and faster reporting, job monitoring provides visibility over all the important cloud connectors activities. Using the Job Monitor, you can perform the following tasks:

- Finding out the connector jobs that were run in the past
- Following up the current (in-progress) jobs and the scheduled jobs
- Monitoring the actions that are taken to perform data backup and restore
- Defining filters to narrow down the jobs for monitoring
- Searching for and filter-specific connector activities, job status, and job types
- Refreshing the information in the **Job Monitor** page by clicking **Refresh** manually
- Sorting the job information by clicking on a column heading in the **Job Monitor** page



- Viewing details such as number and size of the backed-up files, the restored files, and the failed to restore files
- Viewing details of items skipped during backups and restores. You can download a detailed CSV report to stay on top of backup and restore objectives.
- Generating and downloading job reports as a CSV file. The report shows the reasons for all the failed backup and restore jobs. It also provides information to troubleshoot the errors.

## Understanding the backup and restore job monitoring process

You can monitor the jobs and troubleshoot its performance. Before you execute your jobs and collect performance statistics, you must understand the meaning of associated job types and statuses. You must understand reasons and possible resolutions for the failed jobs.

### Job types

[Table 7-1](#) explains various job types and their meaning.

**Table 7-1** Job types

Job types	Meaning
Backup	Performing a backup job. The result is a snapshot that contains copies of backed-up data.
Restore	Restoring a data area or the data areas across accounts. You can find the Importing activity under this job type.
Item restore	Restoring an individual item or a folder.

### Job statuses

You can view the real-time detailed status about the backup and restore jobs in SaaS Backup. When you specify parameters to search for the jobs, the application displays job details along with their status. [Table 7-2](#) explains various job statuses and their meaning.

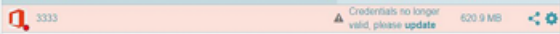
**Table 7-2** Job statuses

Job statuses	Meaning
Succeeded	<p>Job is completed successfully.</p> <p>A backup job is marked as succeeded when:</p> <ul style="list-style-type: none"><li>■ All items are successfully backed up.</li><li>■ Some items fail to be backed up, but the rest items are successfully backed up. The application marks these items as skipped and attempts to back them up during the next job.</li><li>■ Nothing changes from the last snapshot. In this case you will see 0 MB and 0 items backed up.</li></ul>
Failed	<p>Job is not completed successfully.</p> <p>A backup job is marked as failed when:</p> <ul style="list-style-type: none"><li>■ The entire backup attempt fails, and the description field shows N/A.</li><li>■ One item fails to restore, but the rest items are successfully restored. The failed items are shown in the statistics. If a restore job fails completely, the description field shows N/A.</li></ul>
In progress	Job is still being performed
Cancelled	Job that is cancelled by the technical support team at the request of a customer.
Scheduled	<p>Job is scheduled to run at a specific date and time.</p> <p>Restore and item restore jobs will be immediately displayed in the Job Monitor as they are scheduled.</p> <p><b>Note:</b> To view the scheduled backup jobs, set the <b>End date</b> one day ahead of the current date.</p>

**Reasons for the failed backup jobs****Table 7-3** Reasons for the failed backup jobs

Reasons	Meaning
Job aborted	When a backup job is aborted, you do not need to take any action in this case. The application automatically schedules a new job.
Error	When an error occurs, contact the support team to understand and rectify the error before executing the same job next time.

Table 7-3 Reasons for the failed backup jobs (continued)

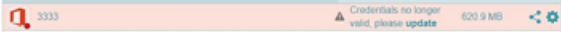
Reasons	Meaning
User not global admin	<p>The job fails if the account used for the backup is not a global admin account. If a global administrator is changed after you set up your backup, the new backup cannot begin. You need to assign your Office 365 service account with the global admin role, and authenticate the process again.</p> <p>See <a href="#">“Preparing an Office 365 service account for SaaS Backup”</a> on page 82.</p>
Authentication failed	<p>When the connector authentication fails, the backup job fails and the connector health status is critical. To authenticate your connector again, click <b>Credentials no longer valid, please update</b> next to your connector.</p>  <p>It happens when the authentication between SaaS Backup and Office 365 is invalid, the Office 365 session expires, or if you have conditional access enabled in Azure Active Directory.</p> <p>SaaS Backup uses an application and a user access token to authorize the backup of Office 365 data. When a user sets up conditional access, SaaS Backup does not get this access token, and displays this message. To ensure a stable backup for your connectors, it is recommended to disable the conditional access.</p>
API request usage limit reached	<p>The backup process do not start when the API request usage reaches its limit that is set for your Salesforce connector. If you want your backup to complete sooner, you can increase the percentage of API requests. However, it can affect performance.</p> <p>See <a href="#">“Salesforce throttling and API request usage”</a> on page 224.</p>
Configuration corrupted	<p>When your backup configuration is corrupted, contact the support team to fix the configuration and start backup again.</p>
Incident occurred	<p>When an incident occurs on the server, the support team immediately start fixing the issue. You do not need to contact support unless this issue reoccurs.</p>

Reasons for the failed restore jobs

**Table 7-4** Reasons for the failed restore jobs

Reasons	Meaning
At least one item skipped	<p>A restore job is marked as failed if one or more items were not restored. To see which exact items were skipped, download a skipped files report. If necessary, start a restore of these files individually.</p> <p>If many items were skipped, you can start the same restore again. If a limited number of items were skipped, you can restore these files individually.</p> <p>If you are restoring a SharePoint site, be aware that certain metadata, column and content types, or permissions may not restore. In most of these cases, your actual data is returned. Check in SharePoint and see if you have the necessary data.</p>
All items skipped	<p>A restore job is marked as failed if the job completed but no items were restored. Try to restore it again. If this continues to occur, contact the support team to understand and rectify the error before executing the same job next time.</p>
Job aborted	<p>When a restore job is aborted, you do not need to take any action in this case. The application automatically schedules a new job.</p>
Error	<p>When an error occurs, contact the support team to understand and rectify the error before executing the same job next time.</p>
User not Global admin	<p>The job fails if the account used for the restore is not a global admin account. If a global administrator is changed after you set up your restore, the new backup cannot begin. You need to assign your Office 365 service account with the global admin role, and authenticate the process again.</p> <p>See <a href="#">“Preparing an Office 365 service account for SaaS Backup”</a> on page 82.</p>

**Table 7-4** Reasons for the failed restore jobs (*continued*)

Reasons	Meaning
Authentication failed	<p>When the connector authentication fails, the restore job fails and the connector health status is critical. To authenticate your connector again, click <b>Credentials no longer valid, please update</b> next to your connector.</p>  <p>It happens when the authentication between SaaS Backup and Office 365 is invalid, the Office 365 session expires, or if you have conditional access enabled in Azure Active Directory.</p> <p>SaaS Backup uses an application and a user access token to authorize the restore of Office 365 data. When a user sets up conditional access, SaaS Backup does not get this access token, and displays this message. To ensure a stable restore for your connectors, it is recommended to disable the conditional access.</p>
API request usage limit reached	<p>The restore process do not start when the API request usage reaches its limit that is set for your Salesforce connector. If you want your restore to complete sooner, you can increase the percentage of API requests. However, it can affect performance.</p>
Invalid restore configuration	<p>When the restore configuration generated in the web client is invalid, contact the support team to fix the configuration and start your restore.</p>
Incident occurred	<p>When an incident occurs on the server, the support team immediately start fixing the issue. You do not need to contact support unless this issue reoccurs.</p>

### Backup job statistics

For all the in-progress backup jobs, the statistics information is updated every five minutes. You can refresh the page manually to update the statistics information.

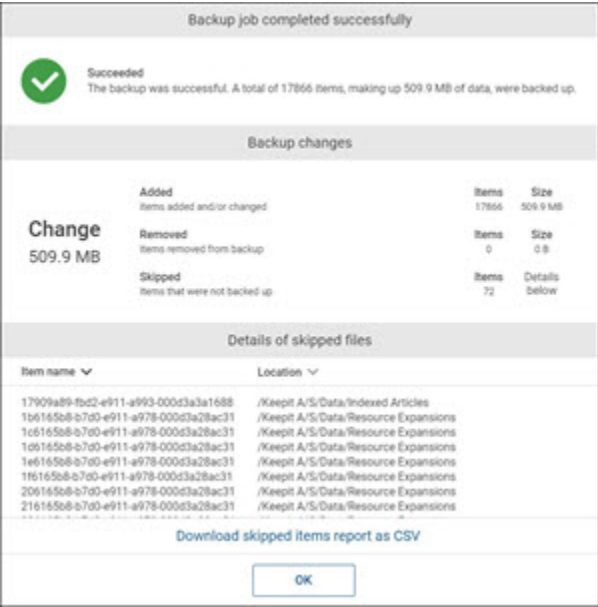


Table 7-5 explains the meaning of statistical parameters of backup jobs.

Table 7-5 Statistical parameters of backup jobs

Parameters	Description
Added to Snapshot	Displays the number of items and the total size (in MB) that are added or changed since the last backup.
Removed from snapshot	Displays the number of items and the total size (in MB) that are no longer exist on the tenant.  For example, if an email or a file is deleted, then it is removed from the current snapshot, but it exists in older snapshots.
Skipped items	Displays the number of items and the total size (in MB) that could not be added due to the throttling problem, API failures, or inaccessibility form Microsoft. SaaS Backup tags these files as failed, and try again to reach them during the next backup.

Restore job statistics

For all the in-progress restore jobs, the statistics information is updated every five minutes. You can refresh the page manually to update the statistics information.




Item restore job statistics			
	 Restored	 Deleted	 Failed to restore
Items	1	0	0
Size	3.4 MB	0 B	0 B
<div>OK</div>			

Table 7-6 explains the meaning of statistical parameters of restore jobs.

Table 7-6 Statistical parameters of restore jobs

Parameter	Description
Restored	Displays the number of items and the total size (in MB) that are successfully restored.
Deleted	Displays the number of items and the total size (in MB) that are deleted. SaaS Backup deletes the files that are found in the target location, but are not available in the snapshot you are trying to restore.
Failed to restore	The number and size of objects that failed to be restored due to such reasons as throttling, a bad request, or a bad token. The failed objects will be listed below and can be downloaded as a CSV file.

Skipped items

SaaS Backup lists skipped items for each backup and restore job. You can view the log of the skipped files, and download the report as a CSV file. If a file is skipped during a job, SaaS Backup backs it up or restores it in the next job.

In this report, you can check if the particular files are being skipped continuously, and troubleshoot the problem. You can compare the CSV files from multiple jobs to track such possible items.

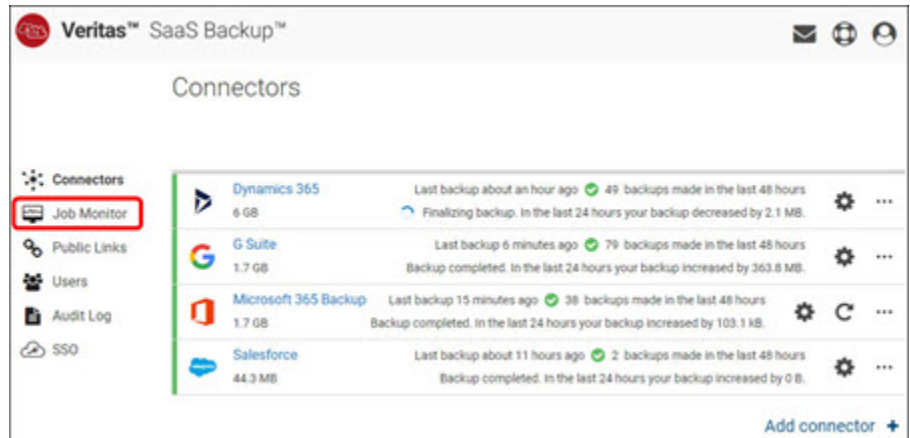
If more than 100 items are skipped during the backup or restore job, SaaS Backup does not display the list. Instead, you can download a CSV file to view the list of all skipped files.

**Note:** Skipped items list and its CSV file reports are available for only one month after the job completion.

# Viewing backup and restore jobs and statistics

To view status of backup and restore jobs and statistics

- 1 In the upper-right corner of the SaaS Backup console, click the menu icon.



- 2 Click **Job Monitor**.

The screenshot shows the Job Monitor page. At the top, there are filters for Connectors (All), Status (All), and Type (All types). Below these are filters for Time span (Last 24 hours), Start time (1/13/2021), and End time (1/14/2021). A 'Refresh' button is located to the right of the time filters. Below the filters is a 'Filter' input field and a 'Download as CSV' link. The main content is a table with columns: Connector, Type, Status, Description, Start time, and End time. The table contains four rows of job data.

Connector	Type	Status	Description	Start time	End time
Microsoft 365 B...	Restore	Succeeded	0 B restored in 0 it... <a href="#">Show more</a>	1/14/2021 04:...	1/14/2021 04:...
G Suite	Backup	Succeeded	0 B backed up in 0 ... <a href="#">Show more</a>	1/14/2021 04:...	1/14/2021 04:...
Microsoft 365 B...	Backup	Succeeded	748 kB backed up i... <a href="#">Show more</a>	1/14/2021 03:...	1/14/2021 03:...
G Suite	Backup	Succeeded	0 B backed up in 0 ... <a href="#">Show more</a>	1/14/2021 03:...	1/14/2021 03:...



- 3 On the **Job Monitor** page, specify the following information.

Field	Description
Connector	Select the connector for which you want to generate a job monitoring report.
Status	Select the job status from the drop-down list for which you want to generate a report.
Type	Select the job type from the drop-down list for which you want to generate a report.
Time span	Specify the time span of the report you want to generate a job monitoring report. Predefined options are available. However, you can customize duration of report as per your requirement.
Start date	If the time span value is selected as <b>Custom period</b> , specify the date from which you want to generate a job monitoring report.
End date	If the time span value is selected as <b>Custom period</b> , specify the date up to which you want to generate a job monitoring report.


- 4 To view the result, click **Refresh**.
- 5 To sort a column details, click the respective column header.

- 6 To further narrow down the result, type a keyword in the **Filter** field, and click the search icon.
- 7 To view the statistic of a specific item, click its **Show more** link in the **Description** column.

You can view a list of all the skipped items in completed backups. You can download a CSV report with items and error codes, which you can use for troubleshooting.

### Example of a successfully completed backup job summary

Backup job completed successfully



**Succeeded**  
The backup was successful. A total of 17866 items, making up 509.9 MB of data, were backed up.

Backup changes

	Added Items added and/or changed	Items 17866	Size 509.9 MB
<b>Change</b> 509.9 MB	<b>Removed</b> Items removed from backup	Items 0	Size 0 B
	<b>Skipped</b> Items that were not backed up	Items 72	Details Below

Details of skipped files


Item name	Location
17909a89-fbd2-e911-a993-000d3a28ac31	/Keepit A/S/Data/Indexed Articles
1b6165b8-b7d0-e911-a978-000d3a28ac31	/Keepit A/S/Data/Resource Expansions
1c6165b8-b7d0-e911-a978-000d3a28ac31	/Keepit A/S/Data/Resource Expansions
1d6165b8-b7d0-e911-a978-000d3a28ac31	/Keepit A/S/Data/Resource Expansions
1e6165b8-b7d0-e911-a978-000d3a28ac31	/Keepit A/S/Data/Resource Expansions
1f6165b8-b7d0-e911-a978-000d3a28ac31	/Keepit A/S/Data/Resource Expansions
206165b8-b7d0-e911-a978-000d3a28ac31	/Keepit A/S/Data/Resource Expansions
216165b8-b7d0-e911-a978-000d3a28ac31	/Keepit A/S/Data/Resource Expansions

Download skipped items report as CSV

OK

### Example of a failed backup job summary

Backup job failed



**Authentication failed**  
The backup could not start because authentication failed. Please re-authenticate your connector by selecting the "Credentials no longer valid, please update" message on your connector. [Read more](#)

# Calculating the estimated time for a job completion

If the connector is experiencing poor backup or restore performance, you can calculate the estimated time for a current job to complete. These instructions use a connector's backup speed during the last backup job to predict how quickly the next job (either backup or restore) will run.

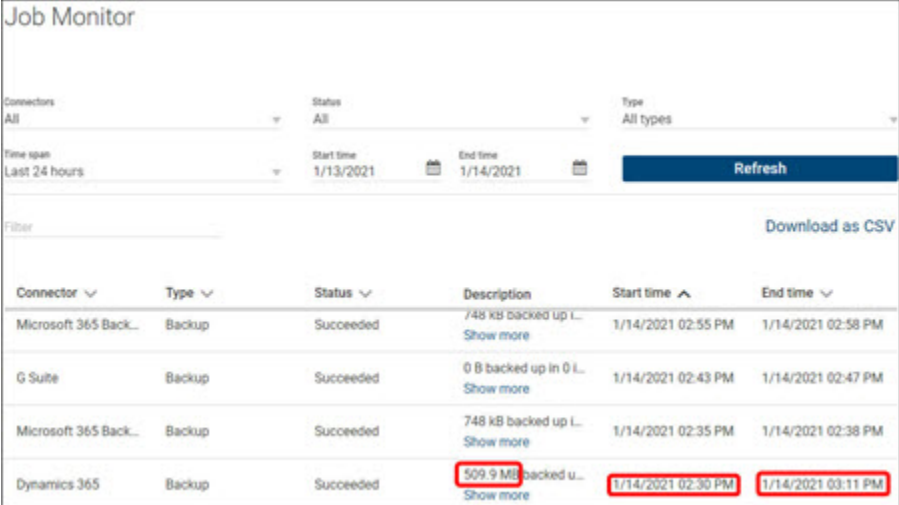
## To calculate the estimated time for a job completion

- 1 On the **Job Monitor** page, check the last succeeded backup job on the connector.
- 2 Calculate the number of hours of the job by finding the difference between the Start Time and End Time.

For example, 0.68 hrs in this case.

- 3 Check the size of data (in MB, GB, or TB) backed up during this job.

For example, 509.9 MB in this case.



Connectors All	Status All	Type All types	Time span Last 24 hours	Start time 1/13/2021	End time 1/14/2021	Refresh
Filter						Download as CSV
Connector	Type	Status	Description	Start time	End time	
Microsoft 365 Back...	Backup	Succeeded	748 kB backed up L... <a href="#">Show more</a>	1/14/2021 02:55 PM	1/14/2021 02:58 PM	
G Suite	Backup	Succeeded	0 B backed up in 0 L... <a href="#">Show more</a>	1/14/2021 02:43 PM	1/14/2021 02:47 PM	
Microsoft 365 Back...	Backup	Succeeded	748 kB backed up L... <a href="#">Show more</a>	1/14/2021 02:35 PM	1/14/2021 02:38 PM	
Dynamics 365	Backup	Succeeded	509.9 MB backed u... <a href="#">Show more</a>	1/14/2021 02:30 PM	1/14/2021 03:11 PM	

- 4 Calculate the speed (in Mbph/Gbph) of this job by dividing the size by the number of hours.

For example,  $509.9 / 0.68 = 749.85$  Mbph in this case.

- 5 Check your account to see size of data (in MB, GB, or TB) you were expecting to back up.

- To calculate Office 365 data size, See [“Calculating the size of data you have in Office 365”](#) on page 68..
  - If you already have a full backup, subtract the size that is already in SaaS Backup from the size you have currently in Office 365.  
For example, 1.7 GB in this case.
- 6 Calculate the estimated time by dividing the expected amount of data by the speed.

---

**Note:** During calculation, use the same units of measurement. In this case,  $1.7\text{GB}/0.74985=2.26\text{h}$ . It means the estimated time required for a job completion is 2.26 hours.

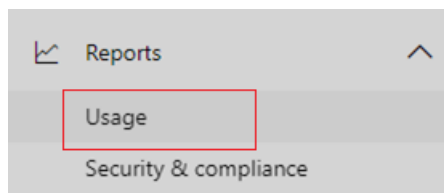
---

## Calculating the size of data you have in Office 365

To estimate size of data you need to back up, you can check the storage usage of different areas of your Microsoft tenant. However, the storage usage in Microsoft for OneDrive, SharePoint, and Groups & Teams may not reflect the amount of data that SaaS Backup backs up in these areas.

### To calculate the estimated time for a job completion

- 1 Access the Microsoft 365 admin center.
- 2 In the left navigation pane, select **Reports > Usage**.



- 3 Click **Select a report**.
  - For **Exchange** usage, select **Exchange > Mailbox usage**. Select the **Storage** tab.  
Look at the last day on the chart to see how much storage is used.
  - For **SharePoint** usage, select **Exchange > Site usage**. Select the **Storage** tab.  
Look at the last day on the chart to see how much storage is used.

---

**Note:** The size you see in Microsoft may differ significantly because VSB only backs up current versions of files in SharePoint.

---

- For **Groups** usage, select **Office 365 > Groups activity**. Select the **Storage** tab.  
Look at the last day to see the total storage used across all group mailboxes and group sites.

---

**Note:** This may not include all the data that SaaS Backup backs up under the Groups & Teams data area.

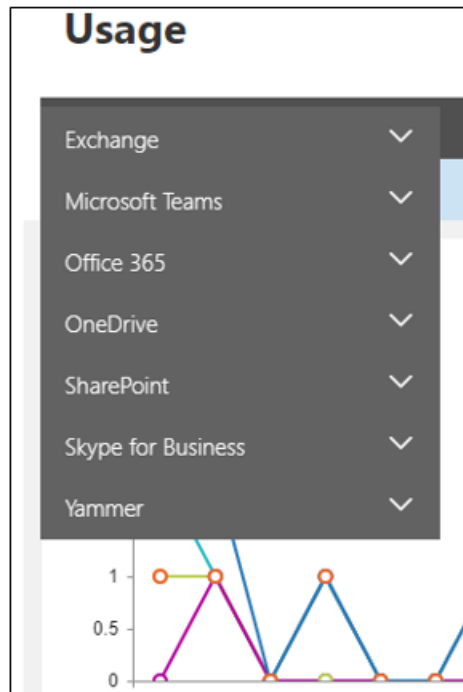
---

- For **OneDrive** usage, select **OneDrive > Usage**. Select the **Storage** tab.  
Look at the last day on the chart to see how much storage is used.

---

**Note:** The size in Microsoft may differ significantly from the size of OneDrive data that SaaS Backup backs up. This is because the size you see in Office 365 includes any versions and metadata associated with the files, while SaaS Backup backs up only the last versions of your files.

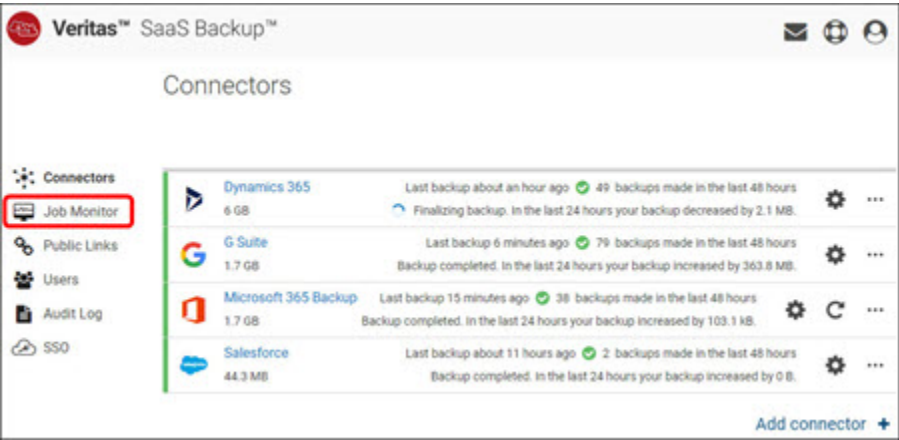
---



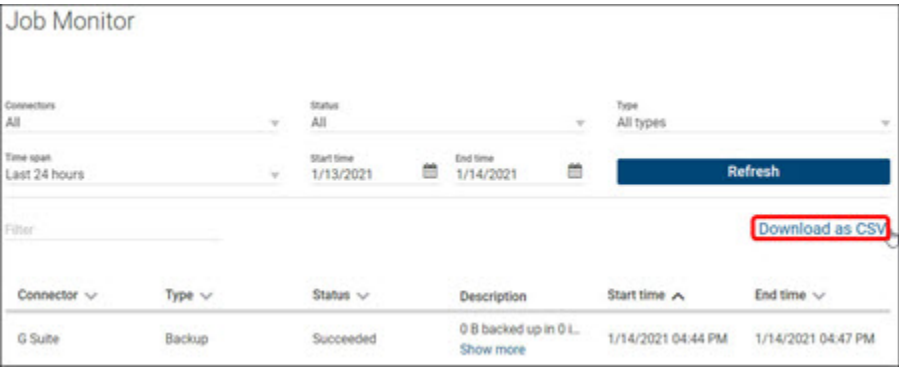
# Downloading job status report

To view backup and restore jobs and their statistics

- 1
- In the upper-right corner of the SaaS Backup console, click the menu icon.



- 2
- Click Job Monitor.



3 On the **Job Monitor** page, specify the following information.

Field	Description
Connector	Select the connector for which you want to generate a job monitoring report.
Status	Select the job status from the drop-down list for which you want to generate a report.
Type	Select the job type from the drop-down list for which you want to generate a report.
Time span	Specify the time span of the report you want to generate a job monitoring report. Predefined options are available. However, you can customize duration of report as per your requirement.
Start date	If the time span value is selected as <b>Custom period</b> , specify the date from which you want to generate a job monitoring report.
End date	If the time span value is selected as <b>Custom period</b> , specify the date up to which you want to generate a job monitoring report.

- 4 To view the result, click **Refresh**.
- 5 To sort a column details, click the respective column header.
- 6 To further narrow down the result, type a keyword in the **Filter** field, and click the search icon.
- 7 To download a job status report, click **Download as CSV**.



# Managing audit logs

This chapter includes the following topics:

- [About audit logs](#)
- [Viewing and downloading audit log reports](#)

## About audit logs

generates and records audit logs as a proof of compliance. It captures the changes to a system configuration, detects issues in the workflows, and maintains an administrator activity log to record changes to the data. These logs are important to troubleshoot issues with the backup and restore process.

You can generate audit log reports to monitor and review all the activities that are mentioned in [Table 8-1](#). You can download the audit log report as a CSV file.

**Table 8-1** Activities for which audit log is generated

Event category	Activities
User events	Successful sign in Failed sign in Create a user profile Edit a user profile Delete a user profile Updating credentials Update a role Update expiration time of another user

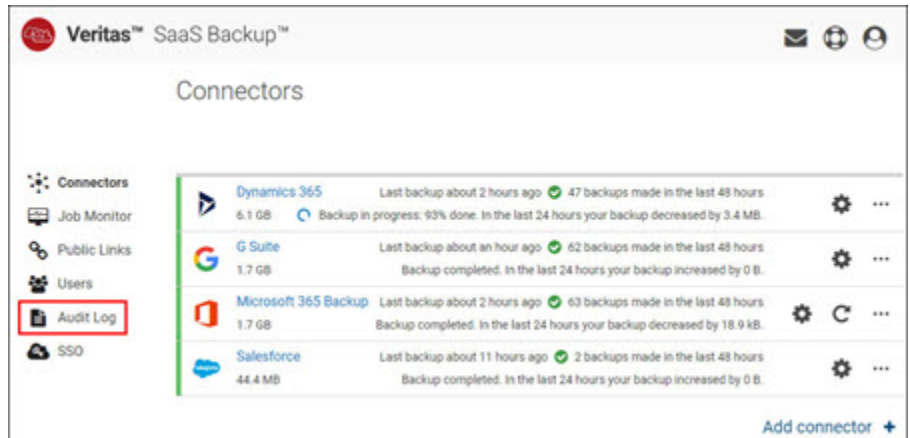
**Table 8-1** Activities for which audit log is generated (*continued*)

Event category	Activities
Connector events	Create a new connector Update a connector Delete a connector
Backup and restore events	Schedule a backup Schedule a restore (includes import) Schedule a selective restore
Miscellaneous events	Create a new single sign-on configuration Create, update, or delete a shared link Download a file Download a folder as a .zip file Preview a file Browse data Browse a shared folder

# Viewing and downloading audit log reports

To view and download audit log

- 1 From the Right Menu Bar of the SaaS Backup console, click **Audit Log**.



- 2 Use the different filtering options to find the events you are interested in. You can filter by user, area, type of action, time span, specified dates, or by the free text filter.

The available area types are User events, Connector events, Backup/Restore, and Misc.

---

**Note:** The actions of deleted users are also shown in the logs. To see these actions, select **All users under the User** filter.

---

- 3 To view the audit log, click **Refresh**.

---

**Note:** Entries highlighted in red indicate denied actions. These display actions that the user did not have permission to perform.

---

- 4 To sort a column details, click the column header.
- 5 To download an audit log report, click **Download as CSV**.

Audit Log				
User	Area	Show actions		
All users	All areas	All actions		
Time span	Start date	End date	Refresh	
Last 10 days	1/17/2021	1/27/2021		
Filter			Download as CSV	
User	Area	Action	IP	Time
demo_theme_s@kee...	User events	Signed in	165.225.34.158	1/27/2021 04:39:37 ...
demo_theme_s@kee...	Miscellaneous	Viewed data are...	165.225.222.153	1/26/2021 11:53:57 ...
demo_theme_s@kee...	Miscellaneous	Viewed data are...	165.225.222.153	1/26/2021 11:53:54 ...
demo_theme_s@kee...	Miscellaneous	Entered folder / ...	165.225.222.153	1/26/2021 11:53:29 ...

# Managing cloud services for Office 365

This chapter includes the following topics:

- [Office 365 cloud connectors overview](#)
- [Protected Office 365 data types](#)
- [Office 365 Throttling](#)
- [Preparing an Office 365 service account for SaaS Backup](#)
- [Adding Office 365 cloud connectors](#)
- [Deleting Office 365 connectors](#)
- [Restore a Microsoft 365 item](#)
- [Restore Exchange data using the Restore Wizard](#)
- [Restore OneDrive data using the Restore Wizard](#)
- [Monitoring jobs of Office 365 cloud connectors](#)
- [Sharing files and folders of Office 365 cloud connectors](#)
- [Downloading files and folders on Office 365 cloud connector](#)
- [About SharePoint backup data types](#)
- [Restrictions while restoring the SharePoint backups](#)
- [Reasons for smaller snapshot size than the actual data size in Office 365](#)
- [Configuring SharePoint data backup](#)

- [About restoring SharePoint data](#)
- [Restore a SharePoint site](#)
- [Restoring SharePoint data in different scenarios](#)
- [Restoring SharePoint data across a tenant](#)
- [Restoring SharePoint data with an advanced backup configuration](#)
- [Restore SharePoint sites using the Restore Wizard](#)
- [About Groups and Teams data backup](#)
- [About Groups and Teams backup data types](#)
- [Restore Groups and Teams data using the Restore Wizard](#)
- [Adding global administrator to the Teams channel](#)
- [Restoring Teams channels data](#)

## Office 365 cloud connectors overview

Microsoft Office 365 is a suite of various cloud-based components. SaaS Backup lets you back up, restore backup, download data, share data, and monitor your Office 365 specific jobs.

### Components

SaaS Backup provides a complete, flexible data protection solution for the following components of the Office 365 platform.

**Table 9-1** Components of Office 365 platform

Exchange	OneDrive	SharePoint	Groups	Teams
Calendar	Files	Lists	Calendar	Calendar
Contacts	Folders	Libraries	Conversations	Channels
Mailboxes		Permissions	Files	Files
Shared Mailboxes		Sites	Notebook	Private Chats
Tasks			Planner	
			SharePoint Team Site	

To view the updated list of SaaS Backup supported Office 365 Workloads, [https://www.veritas.com/support/en\\_US/article.100045238](https://www.veritas.com/support/en_US/article.100045238).

### System requirements

System requirements and limitations for SaaS Backup to work with Office 365 are as follows:

- Microsoft O365 Exchange Online: See <xxx>
- Microsoft O365 SharePoint Online: See <xxx>

You must use the incognito (private) mode of supported browser to avoid cached credentials.

### Required APIs

SaaS Backup uses the following APIs to backup and restore Office 365 data.

- **Exchange Web Services (EWS) API** is used to back up Exchange (Mail, Calendar, Contacts, Tasks, In-Place Archive) and Public Folders.
- **SharePoint REST + CSOM API** is used to process OneDrive, Sites (Legacy), and some parts of the new SharePoint.
- **Microsoft Graph API** is used to back up Office 365 Groups (Calendar, Conversations, Channels, Planner, Files) and parts of SharePoint.

SaaS Backup consists of several services to collaborate with each other to process, store, and show backed up data to the user. SaaS Backup communicates with Office 365 through a gateway, which is also part of system. To back up and restore Office 365 data, SaaS Backup make HTTPS calls to the Microsoft public APIs, and save the data to secured storage systems.

The data is stored in a special encoded format, and it cannot be displayed to the user as it is. SaaS Backup uses other internal services for data transformation, indexing, and the search function. This ability of SaaS Backup improves user experience and makes it more flexible and robust.

## Protected Office 365 data types

The following Microsoft (Office) 365 data can be backed up:

### Exchange Online

- Mail (Outlook)
- Contacts
- Tasks
- Calendar

- In-Place Archives (also known as Online Archives)
- Public Folders
  - All email messages in Public Folders including email messages in sub-folders, but not items that are posted in the Public Folders
  - User Permissions (which are automatically restored together with content)

**OneDrive** (not including My Site Host Sites)

- Documents
- Form Templates
- Style Library

**SharePoint**

- Customization
- Document Libraries
- Lists
- Pages
- Permissions
- Site Columns
- Site Content Types
- Subsites

See [“About SharePoint backup data types”](#) on page 111.

**Groups and Teams**

- Conversations
- Calendar
- Planner
- Files
- Channels
  - Team channel posts and replies
  - Wiki pages (backed up but cannot be restored, recoverable only by copy-pasting data out or downloading raw files)
- SharePoint
  - Team sites



- Notebooks

---

**Note:** Backup of Channel posts may not work for some customers. SaaS Backup supports the backup of Teams channels posts, but please note that this may not apply to all customers. The reason for this is because Keepit uses the Graph API beta version for the backup and restore of Teams channels, since the Graph API 1.0 currently has limitations on supporting channels. We are following the development of the Graph API closely and we expect to remove these limitations in the future.

---

For more information about the Groups and Teams backup:

See [“About Groups and Teams backup data types”](#) on page 147.

## Office 365 Throttling

Throttling is a security mechanism that keeps server healthy and responsive. It is called "throttling" because it limits the workload coming through the server by regulating network traffic and minimizing bandwidth congestion.

Microsoft uses throttling to manage Office 365 operations and ensures that all customers receive a quality service. Microsoft offers a limited bandwidth to its Office 365 customers. Applications installed by these customers cannot exceed the allocated bandwidth limit.

Throttling limit can affect the SaaS Backup application performance. It can slow down the speed of backup and restore process. All Microsoft Office 365 components deal with the throttling issue. This issue cannot be completely resolved by modifying an application configuration or a regular troubleshooting.

To avoid slow performance, avoid running other data intensive solutions against your Microsoft Office 365 tenant, such as synchronization or secondary backup services. You can contact Microsoft support to increase the throttling limits for the following parameters of the Office 365 Exchange data.

- EwsMaxBurst: Unlimited
- EwsRechargeRate: Unlimited
- EwsCutoffBalance: Unlimited
- EWSMaxConcurrency: highest limit

Microsoft can temporarily change a setting that improves SaaS Backup performance of Office 365 Exchange data. This is helpful during the initial full back up or the on-boarding process. This capability can be used up to 90 days.

### **Additional Details**

The EwsMaxBurst parameter specifies the amount of time that an Exchange Web Services user can consume an elevated amount of resources before being throttled. This is measured in milliseconds. This value is set separately for each component.

The EwsRechargeRate parameter specifies the rate at which an Exchange Web Services user's budget is charged (budget grows by) during the budget time. The EwsCutoffBalance parameter specifies the resource consumption limits for an Exchange Web Services user before that user is completely blocked from performing operations on a specific component.

The EwsMaxConcurrency parameter specifies how many concurrent connections an Exchange Web Services user can have against an Exchange server at one time. A connection is held from the moment a request is received until a response is sent in its entirety to the requestor. If users attempt to make more concurrent requests than their policy allows, the new connection attempt fails. However, the existing connections remain valid. The EwsMaxConcurrency parameter has a valid range from **0** through **2147483647** inclusive. The default value is 10. To indicate that the number of concurrent connections should be unthrottled (no limit), this value should be set to **\$null**.

The SaaS Backup connector auto scaling strategy is all about threads, number of items, and number of mailboxes you hit at the time. This strategy is tailored to auto scale based on the number of mailboxes which works well in "normal exchange" environments as it spreads the load over many mailboxes and as a result less impact on a particular user.

When you have multiple mailboxes, you can restrict the default number of requests to two per mailbox.

## **Preparing an Office 365 service account for SaaS Backup**

Before you back up data of the Office 365 component, you need to prepare an Office 365 service account.

### **To prepare an Office 365 service account**

- 1** Create a new Office 365 service account for backup.
  - Set up a dedicated service account to handle Office 365 data backup. If the employee responsible for managing backup jobs is unavailable for any reason, the job can be easily passed on to another employee.
  - Provide a unique and descriptive account name and an email ID. For example, **SaaS Backup/SaaS\_Backup@company.com**. This avoids a

confusion as this user becomes a member of all Teams and Groups being backed up.

**2** Assign the Global Administrator permissions.

After creating a new service account, assign the Office 365 Global Administrator role to it.

The global administrator has full access to data and can include all the data in the backup file, specially SharePoint, Groups, and Teams. The Office 365 global administrator becomes a member of all Teams and Groups that are being backed up. When this service account is added to an Office 365 Group, it becomes a member of the Group site. If it is not needed, global administrator can manually remove the service account from the Group. However, after the next backup or restore, the SaaS Backup application again adds this service account as a member. The service account never becomes a member of a Communication Site that is created by the user after the backup of Sites.

### 3 Assign a license to the Office 365 Global Administrator.

Assign a license to Global Administrator to provide access to the Groups and the Teams data. This user becomes a member of all Office 365 Teams and Groups. This step is important as SaaS Backup can only back up Office 365 Groups that the Global Administrator is a part of.

SaaS Backup supports the following Office 365 license plans:

Business	Enterprise	Education	Firstline Workers	Government
Essential	E1	A1		G1
Premium	E3	A3	F3	G3
	E5	A5		G5

When you create an Office 365 connector with the Global administrator credentials, the application directs you to the Microsoft link to grant permissions to Veritas. After you approve Veritas request, you are redirected to Veritas SaaS Backup with an authorization code (token). It allows Veritas to access the data it needs to back up. When you provide a Veritas access to Office 365 with a global admin account, SaaS Backup uses the token that is provided to back up the data. Veritas does not receive, store, or use the global administrator account. The credentials remain secured to provide a secured environment when you restore Office 365 data.

Veritas uses all the Office 365 APIs (Graph/REST/EWS/SP) to backup Office 365 data at a granular level. These APIs quickly restore entire workloads like mailboxes, SharePoint sites, and individual items like email messages, files, folders, chats, and Wiki pages.

### 4 Create Active Directory (AD) backup user groups.

This activity is optional, but it is recommended to create an Active Directory backup user group.

Create a dedicated group of users from your Active Directory (your company directory in Microsoft). While selecting the accounts that needs to be backed up, choose these Active Directory groups in the SaaS Backup configuration. This way, you can configure the backup of multiple users simultaneously.

SaaS Backup supports the backup of individual accounts in Office 365 Groups (also known as Unified Groups), Security Groups, and Distribution Lists. See [Compare Groups](#).

In Office 365, select Groups in the left navigation pane, and click Add a group. See [Create a group in the Microsoft 365 admin center](#).

## Adding Office 365 cloud connectors

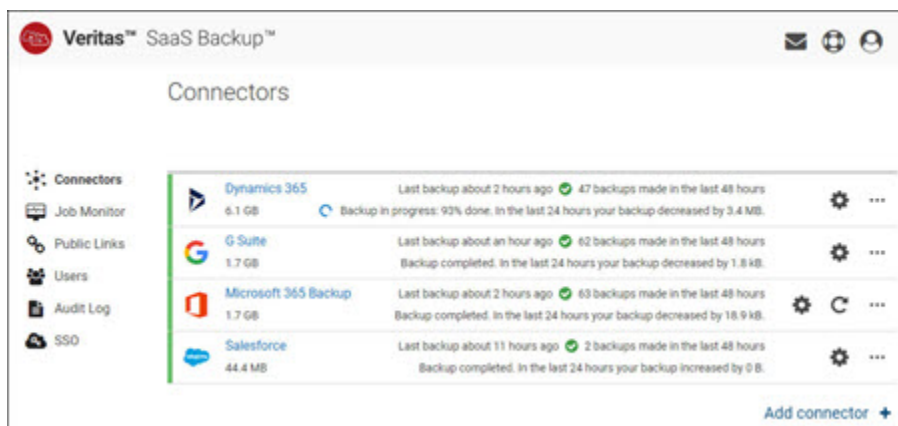
An Office 365 cloud connector represents the backup of an Office 365 cloud service. You need to create an Office 365 cloud connector to back up Office 365 cloud services.

To manage the Office 365 cloud services, you need valid credentials. Ensure that you have a Global administrator account in Office 365.

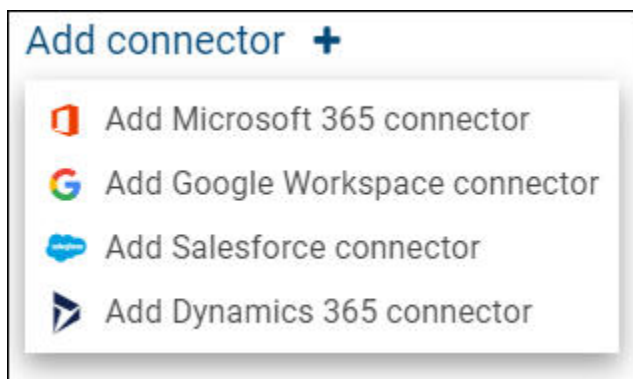
## To add an Office 365 cloud connector

- 1 Sign in to SaaS Backup.

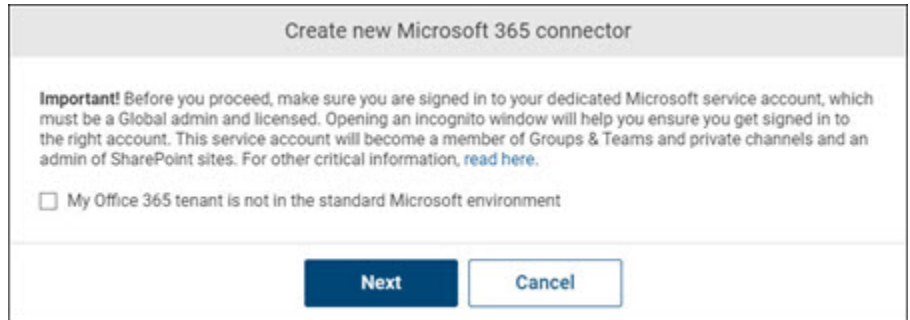
**Note:** The **Connector** page appears by default. If you are on working on any other page (Links, Job Monitor, Audit, and so on), you can click Connectors from the menu icon. This page lets you view a list of connectors, the last updated date, side of data on connector, and the action icons.



- 2 On the **Connectors** page, click **Add**.



- 3 Read and confirm the requirements for creating a new Microsoft 365 connector. If your M365 tenant is not in the standard Microsoft environment, please specify the environment.



**Create new Microsoft 365 connector**

**Important!** Before you proceed, make sure you are signed in to your dedicated Microsoft service account, which must be a Global admin and licensed. Opening an incognito window will help you ensure you get signed in to the right account. This service account will become a member of Groups & Teams and private channels and an admin of SharePoint sites. For other critical information, [read here](#).

☐ My Office 365 tenant is not in the standard Microsoft environment

Next
Cancel

- 4 Click **Next**.
- 5 You will be forwarded to the M365 site and asked to enter the M365 Global Administrator credentials.

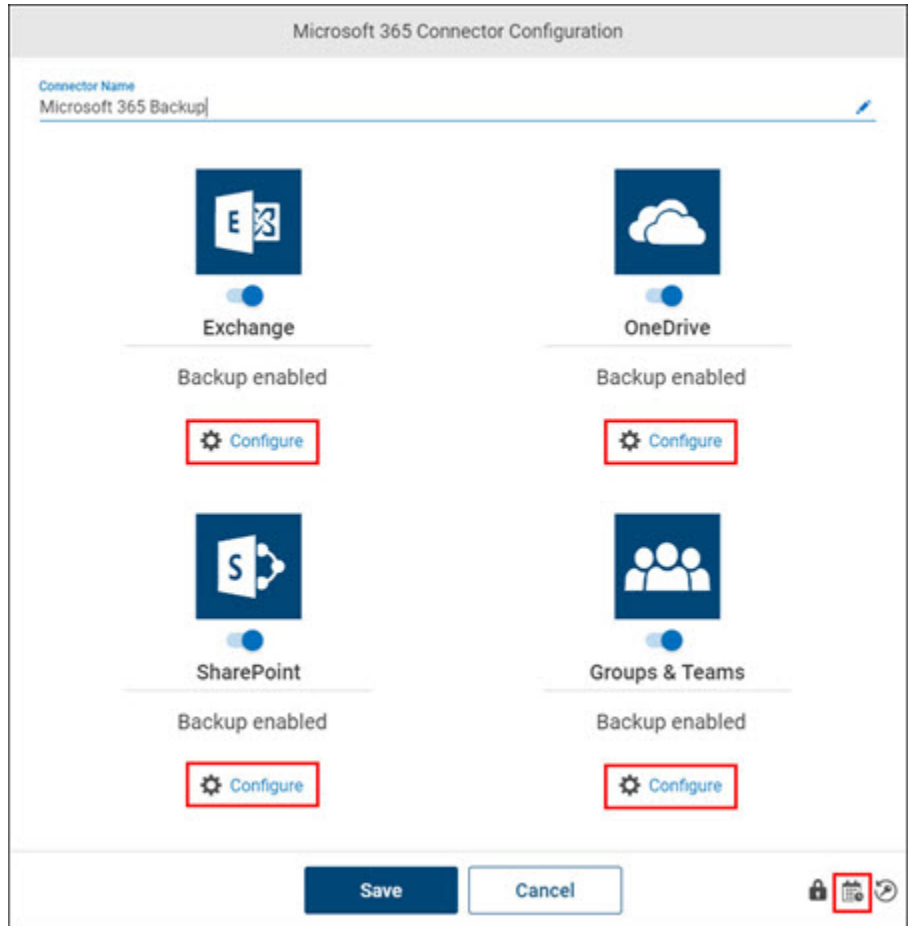
---

**Note:** Veritas SaaS Backup never has access to the Global Admin account nor is any data about the Global Admin account stored in Veritas SaaS Backup.

---

- 6 The configuration dialog box appears.

Enter a unique Office 365 connector name and configure the individual M365 workloads.




- 7 Click the **Exchange Configure Icon** and assign users (accounts) / user groups for this cloud connector.
- 8 Click the **OneDrive Configure Icon** and assign users (accounts) / user groups for this cloud connector.
- 9 Click the **SharePoint Configure Icon** and de-/select the SharePoint sites for this cloud connector.




- 10 Click the **Groups & Teams Configure Icon** and de-/select the Groups for this cloud connector.
- 11 To select a custom snapshot period for this connector click the calendar icon in the bottom right corner for this connector.

Enable the Limit retention period and set the retention period as required and click **Update**.

Connector Snapshot Retention



Here you can change the retention period for your connector. Remember that decreasing the retention period may result in a loss of data.



Change Snapshot Retention

Current connector retention period - 1 month

☒ Limit retention period

Set new retention period: Value: 1 Period: Months

Update

Cancel

- 12 Click **Save**.

# Deleting Office 365 connectors

You can delete an expired or outdated Office 365 cloud connector. Ensure that you have permissions to delete a cloud connector.

## To delete a Office 365 cloud connector

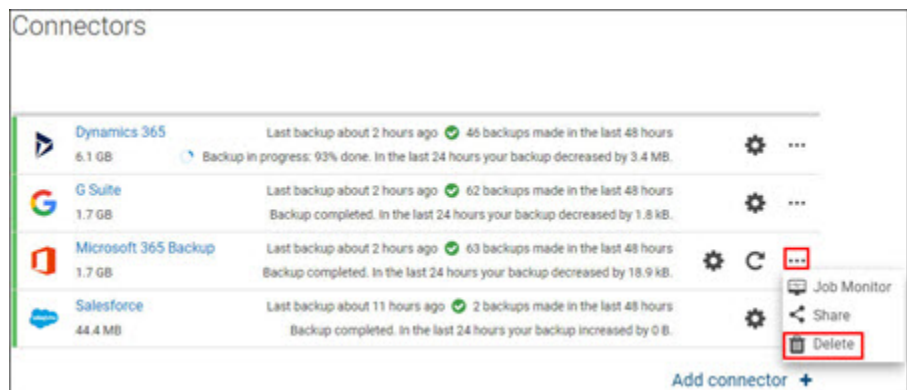
- 1 Sign in to SaaS Backup.

---

### Note:

The **Connector** page appears by default. If you are on working on any other page (Links, Job Monitor, Audit, and so on), you can click **Connectors** from the menu icon. This page lets you view a list of connectors, the last updated date, side of data on connector, and the action icons.

---



- 2 Search for and select the Office 365 cloud connector you want to delete and click the **More Options** icon and click the **Delete** icon.

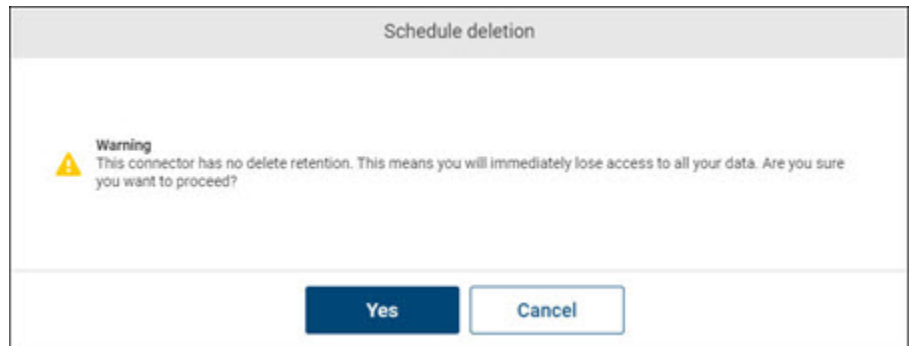
- 3 The application prompts you to confirm that you want to perform the operation.

---

**Note:** SaaS Backup schedules the deletion of the selected connector. The connector is deleted after the retention period is over. If you remove a Microsoft 365 connector, entire data that is associated with the connector is deleted. You cannot revert the changes.

---

- 4 Click **Yes** to complete the operation or click **Cancel** to cancel it.



## Restore a Microsoft 365 item

All Microsoft 365 files and folders can be restored in place.

Outlook, Calendar, In-Place Archive, and OneDrive folders can also be restored to folder. This means that the data will be restored to a newly created separate folder in Microsoft 365.

When you restore in place, what will happen to duplicate items depends on what data you restore.

### In-place restore

By default, all items are restored in place. Certain items can also be restored to folder.

#### Will items be deleted?

When performing an Item Restore, items present in Microsoft but not in the snapshot you are restoring from will not be deleted.

#### Exchange

Modified items (same item but with different timestamps) will be added to Exchange. These items will not be renamed because they have their own unique IDs and receive new IDs each time they are restored. Important: If you are restoring an email from the Sent Items folder, the timestamp in the Outlook web app on the restored email will reflect the date and time that the email was restored, NOT the date and time that the email was sent. The reason for it is that for Sent items, the Outlook web app uses the create date timestamp instead of the sent date, despite the fact that the metadata contains the correct information. In the Outlook desktop app, the timestamp on the restored email will reflect the date and time the email was sent.

### **OneDrive**

Modified items (same item but with different timestamps) will be overwritten.

### **SharePoint**

Restoring in place brings the SharePoint site back to its original location by overwriting the original site.

#### **SharePoint site items**

- If files (including site pages) in your Document Library or Views of Lists and Document Libraries with the same name already exist in SharePoint, they will be overwritten with the data in the snapshot.
- If items in your Lists with the same ID (regardless if the names are the same or different) already exist in SharePoint, they will be overwritten with the data in the snapshot.
- If a subsite ID in SharePoint differs from the subsite ID in the snapshot (for example, if the subsite was previously lost and created), the subsite will be skipped.
- If the quick launch menu of a site in SharePoint differs from the one in the snapshot, it will be overwritten by the menu in the snapshot.

### **Groups and Teams**

Files: Modified files (same item but with different timestamps) will be overwritten.

Calendar events: Modified events (same item but with different timestamps) will be added to the Calendar.

Plan tasks: Modified items (same item but with different timestamps) will be skipped.

Group Conversations: Modified items (same item but with different timestamps) will be skipped.

Channel posts: Modified posts (same item but with different timestamps) will be added to Teams.

## To new folder

Mail, Calendar, In-Place Archives, and OneDrive folders can also be restored to folder. This means that the data will be restored to a newly created separate folder in Microsoft 365. If you select to restore To new folder, a new folder will be created where all the data will be restored.

The folder will be found at the root level of your Mail, Calendar, In-Place Archive, or OneDrive and named `Keepit_Restore_[date of restore]`.

### Will items be deleted?

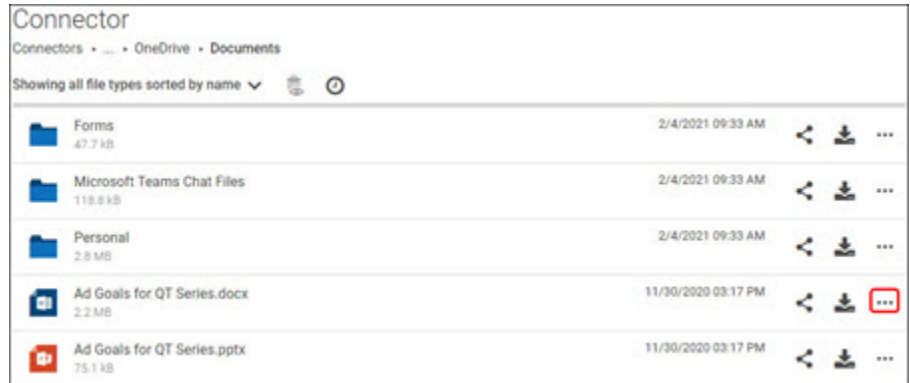
Items present in OneDrive but not in the snapshot you are restoring from will not be deleted.

### To restore a file or folder

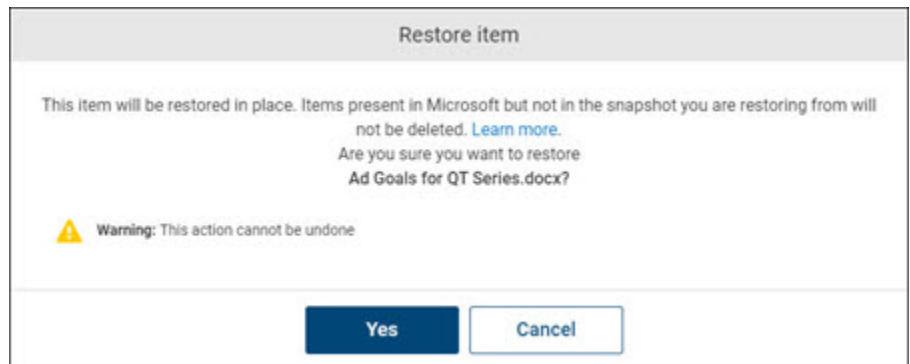
- 1 Select the connector from which you want to restore.
- 2 Find the item you want to restore.
- 3 (Optional) If you want to restore an older version of the item, select the Snapshots Viewer icon, and then select an earlier snapshot. You will now be viewing data from that particular time.

4 Select ... > **Restore**.

**Note:** If you are restoring a single file, select the file to open the File Previewer and verify you have found the correct item. Then restore the file by selecting the Restore icon in the upper-left corner.



5 To confirm the restore, select **Yes**.



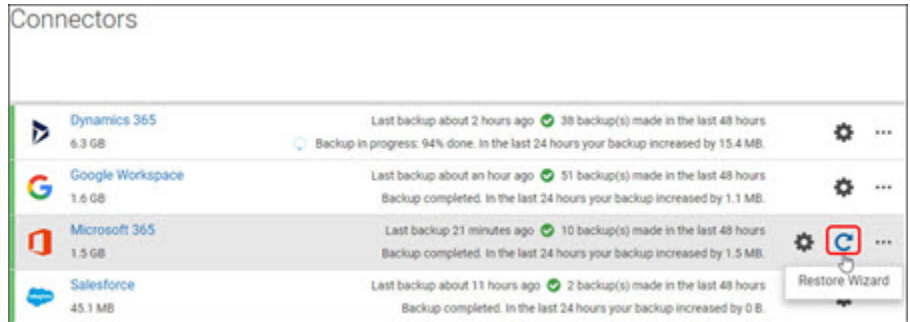
## Restore Exchange data using the Restore Wizard

If you want to restore large amounts of Exchange data or more than one user at a time, use the Restore Wizard.

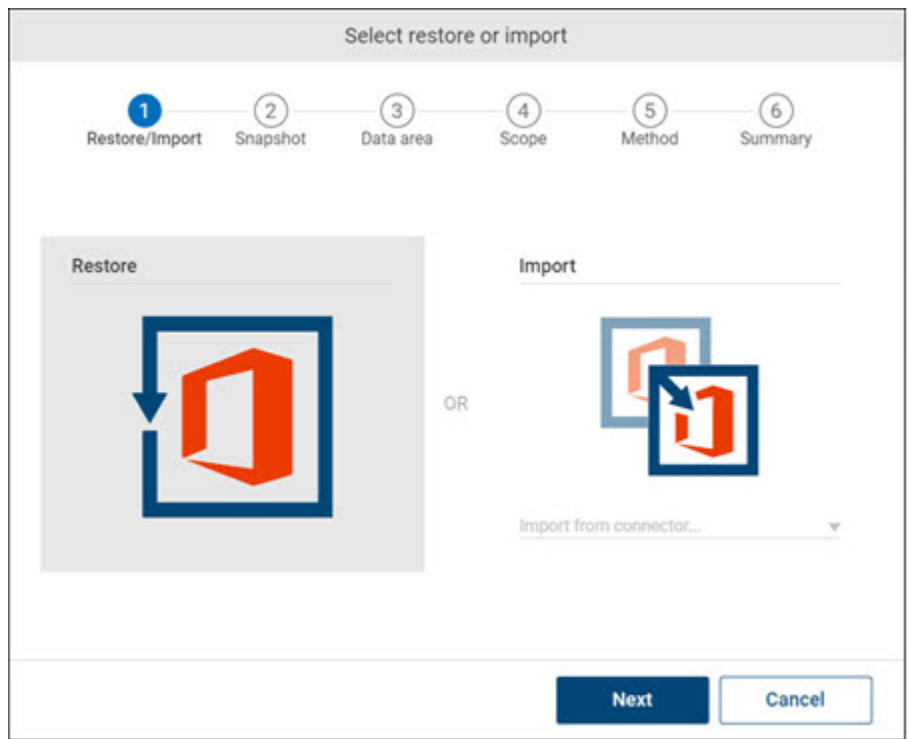
You can restore one Exchange data item.

## To restore Exchange data

- 1 To open the Restore Wizard, to the right of your connector select the **Restore** icon.



- 2 Select **Restore**, and then select **Next**.



- 3 Select a snapshot from the time you want to restore, and then select **Next**.

Select snapshot to restore

1

Restore/Import
 

2

Snapshot
 

3

Data area
 

4

Scope
 

5

Method
 

6

Summary

2/16/2021

6 Feb

9 Feb

12 Feb

15 Feb

Snapshots

February ▾	77 snapshots
16 - Tuesday ▾	3 snapshots
04:14:39 PM ●	1.5 GB
12:10:36 PM ●	1.5 GB
06:10:06 AM ●	1.5 GB
15 - Monday >	6 snapshots
14 - Sunday >	4 snapshots

Back

Next


Cancel



4 Select **Exchange**, and then **Next**.


Select data area to restore

1 Restore/Import 2 Snapshot 3 Data area 4 Scope 5 Method 6 Summary




**Exchange**

- Mail
- Calendar
- Tasks
- Contacts
- Public folders




**OneDrive**

- Files



**SharePoint**

- Sites
- Subsites
- Team sites



**Groups & Teams**

- Conversations
- Files & Plans
- Calendar
- Sites & Channels

Back Next Cancel

- 5 Select users you want to restore and what data areas you want to restore, and/or select public folders to restore, then select **Next**.

---

**Note:** If you select users, you must also select at least one data type to restore. If you select users and public folders, but no data types, only the public folders will be restored.

---

Select how much data to restore

1 Restore/Import   
 2 Snapshot   
 3 Data area   
 4 Scope   
 5 Method   
 6 Summary

**Select users to restore**

Filter users

- ☐ Select all
- ☒ Miriam Graham - MiriamG@M365x378256.OnMicrosoft.com
- ☐ Joni Sherman - JoniS@M365x378256.OnMicrosoft.com
- ☐ Conf Room Hood - Hood@M365x378256.OnMicrosoft.com
- ☐ Johanna Lorenz - JohannaL@M365x378256.OnMicrosoft.co...
- ☐ Patti Fernandez - PattiF@M365x378256.OnMicrosoft.com
- ☐ Diego Sicilliani - DiegoS@M365x378256.OnMicrosoft.com
- ☐ Christie Cline - ChristieC@M365x378256.OnMicrosoft.com
- ☐ Debra Berger - DebraB@M365x378256.OnMicrosoft.com
- ☐ Conf Room Stevens - Stevens@M365x378256.OnMicrosoft...

Select what to restore

- ☒ Mail
- ☒ Calendar
- ☒ Contacts
- ☒ Tasks
- ☒ In-Place Archive

Select public folders to restore

Back
Next
Cancel

- 6 Select a restore method.
  - If you select **To new folder**, then select **Next**.

---

**Note:** This is available only for Mail, Calendar, and In-Place Archive. SAAS BACKUP will create a new folder where all the data will be restored to.

---

- If you select **In-place**, select how to handle duplicate items, and then select **Next**.  
 You have two options:

**Skip duplicate items:** Modified items (same item but with different timestamps) will be skipped.

**Rename duplicate items:** Modified items (same item but with different timestamps) will be added to Exchange. These items will not be renamed because they have their own unique IDs and receive new IDs each time they are restored.

Select how to restore the data

1

Restore/Import

2

Snapshot

3

Data area

4

Scope

5

Method

6

Summary

How should we restore your data?

To new folder

In-place

Clean existing data

How should we handle duplicates?

Skip duplicate items

Rename duplicate items

Overwrite existing items

BackNextCancel

**7** Review the summary, and then select **Restore**.

Items present in Exchange but not in the snapshot will be deleted.

**Restore summary**

1 2 3 4 5 6  
 Restore/Import   Snapshot   Data area   Scope   Method   Summary

**Warning:** Selecting Restore below will start the restore job. This action cannot be undone.

**Restore summary**

- Restoring Exchange data from snapshot dated 2/16/2021 04:14 PM
- 1 Exchange user(s) selected for restore including Mail, Calendar, Contacts, Tasks, In-Place Archive
- Selected restore method: In-place restore handling duplicates by skipping duplicate items

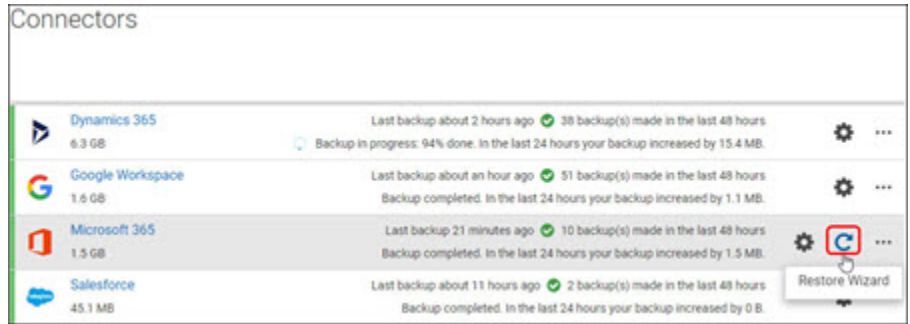
## Restore OneDrive data using the Restore Wizard

If you want to restore the entire OneDrive of a user, or the OneDrives of more than one user at a time, use the Restore Wizard.

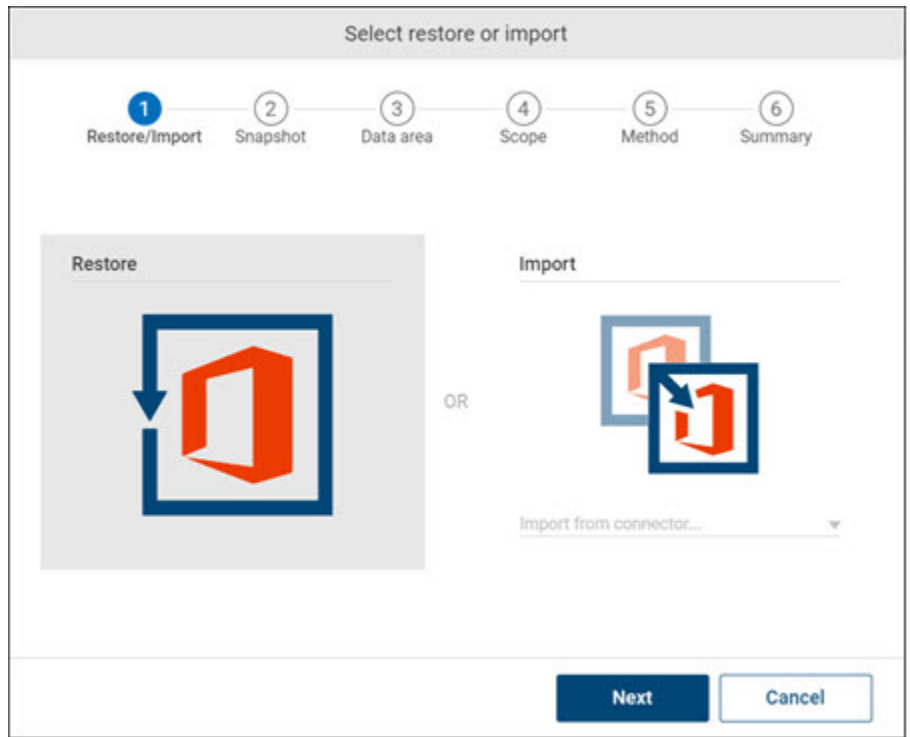
You can restore one OneDrive file.

## To restore OneDrive data

- 1 To open the Restore Wizard, to the right of your connector select the **Restore** icon.



- 2 Select **Restore**, and then select **Next**.



- 3** Select a snapshot from the time you want to restore, and then select **Next**.

Select snapshot to restore

1

Restore/Import
 

2

Snapshot
 

3

Data area
 

4

Scope
 

5

Method
 

6

Summary

2/16/2021

6 Feb

9 Feb

12 Feb

15 Feb

Snapshots

February ▾	77 snapshots
16 - Tuesday ▾	3 snapshots
04:14:39 PM ●	1.5 GB
12:10:36 PM ●	1.5 GB
06:10:06 AM ●	1.5 GB
15 - Monday >	6 snapshots
14 - Sunday >	4 snapshots

Back


Next

Cancel

4 Select **OneDrive**, and then **Next**.


Select data area to restore

1 Restore/Import 2 Snapshot 3 Data area 4 Scope 5 Method 6 Summary




Exchange

- Mail
- Calendar
- Tasks
- Contacts
- Public folders




OneDrive

- Files



SharePoint

- Sites
- Subsites
- Team sites



Groups & Teams

- Conversations
- Files & Plans
- Calendar
- Sites & Channels

Back Next Cancel



- 5 Select users you want to restore, and then select **Next**.

Select how much data to restore

1 Restore/Import   
 2 Snapshot   
 3 Data area   
 4 Scope   
 5 Method   
 6 Summary

**Select users to restore**

Filter users

- ☐ Select all
- ☒ Miriam Graham - MiriamG@M365x378256.OnMicrosoft.com
- ☐ Joni Sherman - JoniS@M365x378256.OnMicrosoft.com
- ☐ Johanna Lorenz - JohannaL@M365x378256.OnMicrosoft.com
- ☐ Patti Fernandez - PattiF@M365x378256.OnMicrosoft.com
- ☐ Diego Siciliani - DiegoS@M365x378256.OnMicrosoft.com
- ☐ Christie Cline - ChristieC@M365x378256.OnMicrosoft.com
- ☐ Debra Berger - DebraB@M365x378256.OnMicrosoft.com
- ☐ Alex Wilber - AlexW@M365x378256.OnMicrosoft.com
- ☐ Pradeep Gupta - PradeepG@M365x378256.OnMicrosoft.com
- ☐ Grady Archie - GradyA@M365x378256.OnMicrosoft.com
- ☐ MOD Administrator - admin@M365x378256.onmicrosoft.com

Back
Next
Cancel

- 6 Select a restore method.
  - If you select **To new folder**, then select **Next**.
  - If you select **In-place**, select how to handle duplicate items, and then select **Next**.

You have three options:

**Skip duplicate items:** Modified items (same item but with different timestamps) will be skipped.

**Rename duplicate items:** Modified items (same item but with different timestamps) will be added to Exchange. These items will not be renamed because they have their own unique IDs and receive new IDs each time they are restored.

**Overwrite existing items:** Modified items (same item but with different timestamps) will be overwritten.

Select how to restore the data

1Restore/Import

2Snapshot

3Data area

4Scope

5Method

6Summary

How should we restore your data?

To new folder

In-place

Clean existing data

How should we handle duplicates?

Skip duplicate items

Rename duplicate items

Overwrite existing items

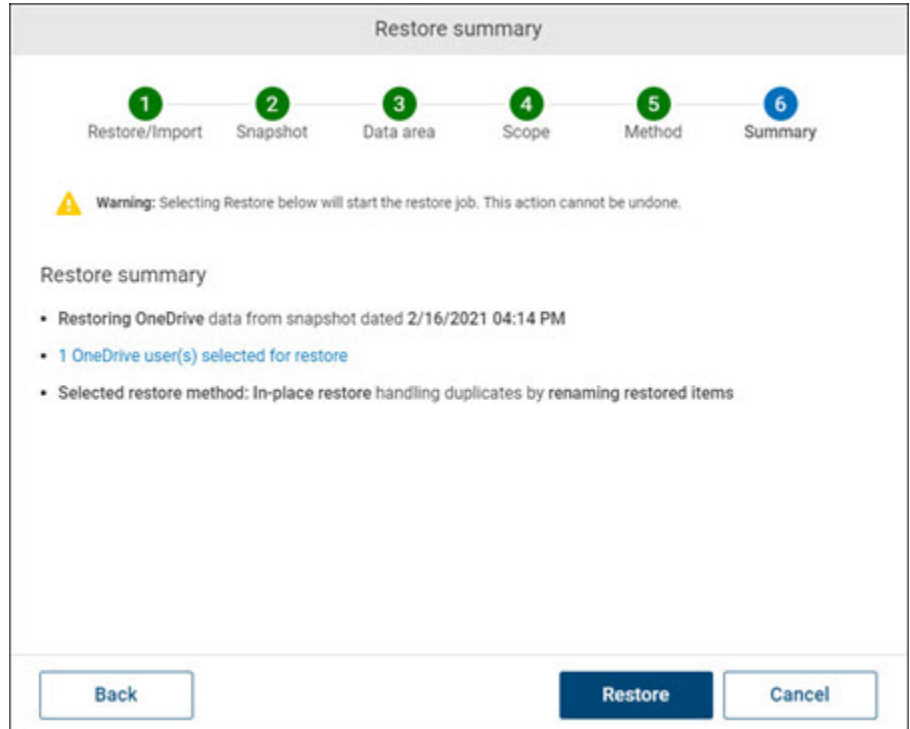
Back

Next

Cancel

7 Review the summary, and then select **Restore**.

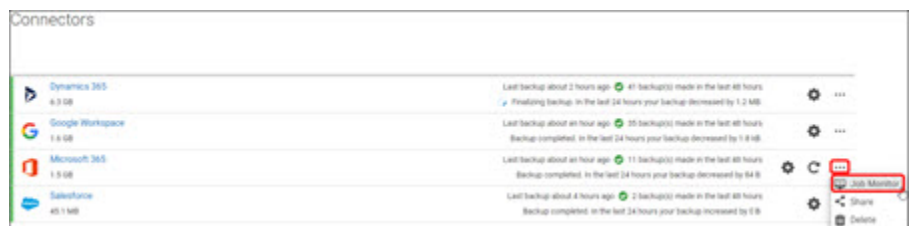
Items present in OneDrive but not in the snapshot will be deleted.



## Monitoring jobs of Office 365 cloud connectors

To monitor backup and restoring jobs of Office 365 cloud connectors

1 Select the Office 365 connector for which you want to monitor jobs.



2 Click **Job Monitor**.

- 3 On the **Job Monitor** page, specify the following information.

Field	Description
Connector	Displays the connector name for which you want to generate a job monitoring report.
Status	Select the job status from the drop-down list for which you want to generate a report.
Type	Select the job type from the drop-down list for which you want to generate a report.
Time span	Specify the time span of the report you want to generate a job monitoring report. Predefined options are available. However, you can customize duration of report as per your requirement.
Start date	If the time span value is selected as <b>Custom period</b> , specify the date from which you want to generate a job monitoring report.
End date	If the time span value is selected as <b>Custom period</b> , specify the date up to which you want to generate a job monitoring report.

- 4 To view the result, click **Refresh**.
- 5 To sort a column details, click the respective column header.
- 6 To further narrow down the result, type a keyword in the **Filter** field, and click the search icon.
- 7 To view the statistic of a specific item, click its **Show more** link in the **Description** column.

# Sharing files and folders of Office 365 cloud connectors

## To share files and folders of Office 365 cloud connectors

- 1 Select the Office 365 connector for which you want to share the data.

Connectors			
Cloud Connectors		Last Update	Size
	Dynamics 365 - Don't change any setting at ALL	about 6 hours ago	1.4 GB
	G Suite Demo - Don't change any setting at ALL	42 minutes ago	1.8 GB
	Office 365 Demo - Don't change any setting at ALL	about 9 hours ago	62.8 GB
	Salesforce Demo - Don't change any setting at ALL	about 7 hours ago	1.3 MB
	test_o365	First backup scheduled	-

- 2 To share entire connector data, click **Share folder** on the **Connectors** page.  
The application opens the **Share public link** page.

## Share public link

Clicking Share will make the data available for anyone who receives this link:

Shared data: test\_o365

☒ Time limit public link

Set expiration time:

☐ Password protect public link

Close

Share

3 In the **Share public link** dialog box, specify the following information:

Field	Description
Time limit public link	Select this check-box to view the <b>Set expiration time</b> field.
Set expiration time	Set the expiration time of a public share link.
Password protect public link	Select this check-box to specify the password for user to access the shared content. You need to share this password with the user via email.

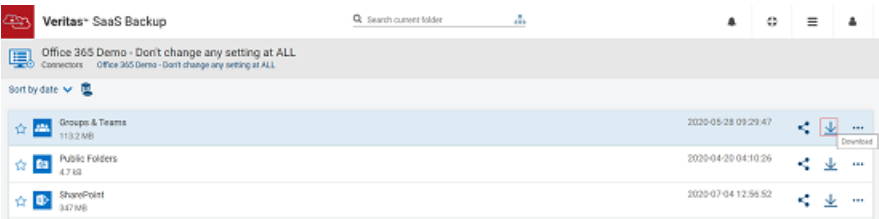
- 4 Click **Share**.
- The application opens the **Share public link** page.
- 5 Copy the link to share with the user, and click **Close** to exit this page.

# Downloading files and folders on Office 365 cloud connector

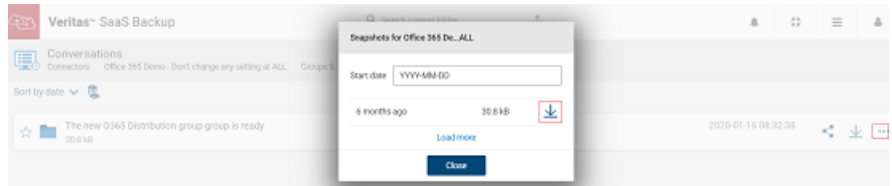
You can download the entire folder with the latest data or the specific version of files and folders within it.

## To download the entire folder with the latest data

- 1 Select the Office 365 connector, and navigate to the file or folder.
- 2 To download the entire folder with the latest data, click **Download**.



- 3 To download the specific version of the file, click the **More options** icon.



- 4 Select the point in time from which you want to download, and click **Download**.

## About SharePoint backup data types

The advanced SharePoint configuration lets you improve SharePoint backup performance. You can select the specific SharePoint data you want to include in your Office 365 backup. You can exclude individual SharePoint sites or domains you do not want to include in your Office 365 backup.

You can back up all the following SharePoint data, by default.

### Site Collection Lists:

- List (with inherited permissions)
  - Items
  - Columns
  - Content Types
  - Views
  - Permissions (link to parent Site Permissions folder)
- List (with unique permissions)
  - Items
  - Columns
  - Content Types
  - Views
  - Assignments
- List (with an item that has unique permissions)
  - Items
  - Items permissions

- Columns
- Content Types
- Views
- Permissions (Link to parent Permissions folder)

### **Document Libraries**

- Document Library (with inherited permissions)
  - Content
  - Columns
  - Content Types
  - Views
  - Permissions (Link to parent Permissions folder)
- Document Library (with unique permissions)
  - Content
  - Columns
  - Content Types
  - Views
  - Assignments
- Document Library (with an item that has unique permissions)
  - Content
  - Items permissions
  - Columns
  - Content Types
  - Views
  - Permissions (Link to the parent Permissions folder)
- List Template Gallery (this is document library where templates of the List and Document library are saved)
- Solution Gallery (document library where templates of sites are saved)

### **Site Content Types**

### **Site Columns**

### **Permissions**



- Groups
- Assignments
- Permission Levels
- Site Administrators

### **Customization**

- Quick launch navigation menu

---

**Note:** SaaS Backup does not backup the quick launch navigation menu for the site templates, namely: Business Intelligence Center, Enterprise Wiki, Enterprise Search Center, Publishing Portal, Basic Search Center.

---

### **Pages**

---

**Note:** This link is not available for the Site Templates, namely: Basic Search Center, Blog, Community Portal, Document Center, eDiscovery Center, Project site, Record Center, Visio Process Repository.

---

### **Sub-Sites**

- Sub-Site (with inherited permissions) Lists
  - Lists
  - Document Libraries
  - Site Content Types
    - Link to parent Site Content Type folder
    - List of own Content Types
  - Site Columns
    - Link to parent Site Columns folder
    - List of own Site Columns
  - Permissions (Link to parent Site Permissions folder)
- Sub-Site (with unique permissions)
  - Permissions
    - Assignments (permissions for the site)
    - SharePoint Groups

- Permission Levels
- Sub-Sites

**Sites (Legacy)** formerly called Sites.

---

**Note:** This is only available for users who had this enabled in versions older than 2.0. This checkbox will eventually be phased out (est. early 2020).

---

- Document Libraries of Classic Sites
- Document Libraries of Communication Sites

SaaS Backup does not back up the following data types:

- Personal Views of Lists and Document Libraries
- External Lists
- Footer navigation menu
- Top link bar
- Sites themes
- SharePoint IRM (Information Right Management)
- Project Online (SaaS Backup supports the backup of site collections with Web App Part, but do not support the backup of projects)
- SharePoint workflows

## Restrictions while restoring the SharePoint backups

SaaS Backup does not back up the following items:

- Personal Views of Lists and Document Libraries
- External Lists
- Web part page types of Site Collections
- SharePoint IRM (Information Right Management)
- SharePoint workflows
- Project Online

---

**Note:** SaaS Backup supports the backup of site collections with Web App Part, but does not support the backup of projects.

---

You can restore most of the SharePoint data including metadata and configuration settings. However, if parent content or configurations (such as views, permissions, etc.) are missing from SharePoint, SaaS Backup cannot restore the data. Without these details, SaaS Backup cannot find the right place to restore data, and SharePoint cannot display it.

You cannot restore the user-specific data, metadata, permissions, and assignments if the user is deleted from the Microsoft Active Directory.

You cannot restore a Subsite or the data from a Subsite if the Subsite in SharePoint has a different ID. For example, if a Subsite was previously lost and created, the application skips the Subsite and items.

The following are some specific cases when SaaS Backup does not restore objects at all or restore with some missing elements.

### **Site Content Type**

You cannot restore the Site Content if the Site Column or parent Content Type is not present in SharePoint.

### **Group of people**

You cannot restore the users that are deleted from the Office 365 account. All other users can be restored normally.

### **User Assignments**

Site Content Type You cannot restore User Assignments its User Role is not present in SharePoint.

### **List Content Type**

You cannot restore the List Content Type if the parent Content Type is not present in the SharePoint Site and the required List Column is not present in the List.

### **List Item**

If the List Content Type of the List Item is not present in SharePoint, SaaS Backup restores the item with the default content type.

If the List Column of the List Item is not present in SharePoint, SaaS Backup restores item without the column properties.

If the List metadata columns have symbols, special characters including Danish letters), or spaces in its names, SaaS Backup restores cannot restores List items.

### **List View**

If the List Column of the List View is not present in the List, SaaS Backup restores View without the column.

#### **Item Permission**

You cannot restore the Item Permission if the Site, Subsite, Permission Level, Group Role, User Role, List or Document Library, or List Item or Document Library file are not present in SharePoint.

#### **List Permission**

You cannot restore a List Permission if the Permission Level, Group Role, or User Role is not present in SharePoint.

## **Reasons for smaller snapshot size than the actual data size in Office 365**

There are several reasons why a snapshot size can be smaller in comparison to the data usage you see in the Microsoft admin panel, especially when it comes to OneDrive and SharePoint. However, the most common reasons are:

#### **SaaS Backup do not cover versioning of files**

This reason applies to OneDrive and SharePoint that have the file versioning system. SaaS Backup backs up only the current versions of files. For example, if you have a file that has three versions, each of which takes up about 100Mb, then in Microsoft you can see 300Mb size. Whereas SaaS Backup shows only latest file of 100Mb.

#### **Skipped files due to Microsoft throttling or lost connection**

Due to the internet network outage or throttling settings, SaaS Backup is unable to access and back up some files. However, SaaS Backup attempts to back up those skipped files in the next backup jobs.

#### **SaaS Backup may not cover certain data types or metadata**

The amount of data you see in Microsoft is not always an accurate representation of the data you have selected to back up. Certain metadata that is stored in Microsoft as well as certain data types may not be covered by SaaS Backup. For more information on data types protected in Office 365, See [“Protected Office 365 data types”](#) on page 79.

# Configuring SharePoint data backup

## To configure SharePoint data backup

- 1 On the **Connectors** page, select the Office 365 cloud connector for which you want to back up the SharePoint data.

Select data area to restore

1 Restore/Import 2 Snapshot 3 Data area 4 Scope 5 Method 6 Summary

**Exchange**

- Mail
- Calendar
- Tasks
- Contacts
- Public folders

**OneDrive**

- Files

**SharePoint**

- Sites
- Subsites
- Team sites

**Groups & Teams**

- Conversations
- Files & Plans
- Calendar
- Sites & Channels

Back Next Cancel

- 2 Click **Edit**, and select **Configure connector**.

The configuration dialog box appears.

Select how much data to restore

1 2 3 4 5 6  
Restore/Import Snapshot Data area Scope Method Summary

Select sites to restore

Filter sites

- ☐ All sites
- ☒ https://m365x378256.sharepoint.com/sites/askhr (1/1 sites selected)
- ☐ https://m365x378256.sharepoint.com/portals/hub
- ☐ https://m365x378256.sharepoint.com/sites/give
- ☐ https://m365x378256.sharepoint.com
- ☐ https://m365x378256.sharepoint.com/sites/safety
- ☐ https://m365x378256.sharepoint.com/sites/Retail
- ☐ https://m365x378256.sharepoint.com/sites/Contoso
- ☐ https://m365x378256.sharepoint.com/portals/Community
- ☐ https://m365x378256.sharepoint.com/sites/operations
- ☐ https://m365x378256.sharepoint.com/sites/leadership
- ☐ https://m365x378256.sharepoint.com/sites/allcompany

Back Next Cancel

- 3 In the configuration dialog box, ensure that the check-box for the SharePoint component is selected. If it is not selected, select the check-box for the SharePoint component, and click **Configure**.

The Advanced SharePoint configuration dialog box appears.

**Restore summary**

1 2 3 4 5 6  
 Restore/Import   Snapshot   Data area   Scope   Method   Summary

**Warning:** Selecting Restore below will start the restore job. This action cannot be undone.

**Restore summary**

- Restoring SharePoint data from snapshot dated 2/16/2021 04:14 PM
- 1 SharePoint site(s) selected for restore
- Selected restore method: In-place restore handling duplicates by skipping duplicate items

- 4 In the **Advanced SharePoint configuration** dialog box, select one or more check-boxes.
  - Select the **Library files** check-box to include library files during backup.
  - Select the **List items** check-box to include list items during backup.
  - Select the **Metadata** check-box to include metadata during backup.

---

**Note:** You can select the **Metadata** check-box if you have selected the **Library files** and the **List items** check-box or both.

---

- 5 To exclude SharePoint sites or domains, enter the URL of the site or domain in the **Exclude individual SharePoint sites or domains** field.

---

**Note:** You can exclude more than one sites and domains. The application can save only valid URLs.

---

Example of a site URL: `https://veritasdemo.sharepoint.com/sites/communication`

Example of a domain URL: `https://veritasdemo.sharepoint.com`

If you enter a domain, the application excludes all the sites and the subsites that use this domain. If you enter URLs to exclude from the backup, you must also select which data you include in the above step. Else, you cannot save the configuration.

- 6 Click **Save**.

This configuration setting becomes effective when the next backup begins. You do not need click **Save** on the main configuration window to save your advanced SharePoint configuration changes. However, if you make other changes to your backup configuration on the main configuration window, you must click **Save** to update the configuration.

- 7 To ensure that you have customized the configuration, confirm that an asterisk sign appears near the SharePoint data area on the main configuration window.

## About restoring SharePoint data

The SharePoint data is restored in the SharePoint folder. SaaS Backup recovers your SharePoint data along with its configurations and metadata. It is recommended to restore data at the highest appropriate level. If you lose specific data items or configuration settings, you can restore these as individual items.

In certain cases, you may not be able to restore data if parent content or configurations (such as views, permissions, etc.) are missing from SharePoint. Restoring process fails if the List metadata columns contain symbols, special characters (including Danish letters), or spaces in its names.

You can restore a SharePoint data to its original location or site, or to a new location. SaaS Backup does the following:

- Overwrites the existing data, if you restore the backup to its original location.
- Creates a new SharePoint site to restore the backup, if you restore the backup to a new location, SaaS Backup. The existing data remains unchanged.
- Retains (do not delete) the Sites that are found in the SharePoint location, but not available in the snapshot.



- Skips the Subsite if a Subsite ID in SharePoint differs from the Subsite ID in the snapshot (for example, if the Subsite was previously lost and created).
- Overwrites the items in your Lists with the same ID.
- Creates a location for new items.  
For example, if you restore an item from a Document Library that was deleted, SaaS Backup creates a Document Library with the default column settings. However, in such situation, it is recommended to restore the entire Document Library.

### **Structure of your SharePoint data in SaaS Backup**

Every Site and Subsite folder contains:

- **Data** of your Site (Lists and Document Libraries)
- **Configurations** (Site Columns, Site Content Types, and Permissions)
- **Subsites** (if applicable)

Every List and Document Library folder contains:

- **Data** (Items in Lists and Content in Document Libraries)
- **Configurations** (Columns, Content Types, Views, Item Permissions, and Assignments)

## **Restore a SharePoint site**

### **What can be restored?**

SaaS Backup backs up all three SharePoint site pages types: Modern, Web Part, and Wiki, but can only restore Modern and Wiki types.

### **Methods**

A SharePoint site or subsite can be restored using two different methods:

- In place overwriting the original site
- As a new site with a new URL

Both methods of restore work for all types of sites.

### **In Place**

Restoring in place brings the site back to its original location by overwriting the original site.

## As a New Site

Restoring as a new site creates a new site with a new URL in parallel with the existing source site. The site will work like the original site - all users and permissions will also be restored.

You can restore a site as a new site only if the original site still exists in SharePoint. If the site no longer exists, you will only not be presented with the option to select a restore method.

### To restore a SharePoint site in place

- 1 Navigate to the site or subsite you want to restore.

---

**Note:** If you want to restore a site or subsite from an earlier point in time, select the **Snapshots Viewer** icon and then select the appropriate snapshot.

---

- 2 To the right of your site, select **...** > **Restore**.



- 3 Select **Restore in place (overwrite existing site)**, and then select **Next**.


Restore

1

Restore

2

Summary

 Restoring in place brings the site back to its original location by overwriting the original site. Items in the site that are not present in the snapshot you are restoring but that are present in SharePoint will not be deleted.

Are you sure you want to restore **All Company**?

Select method:

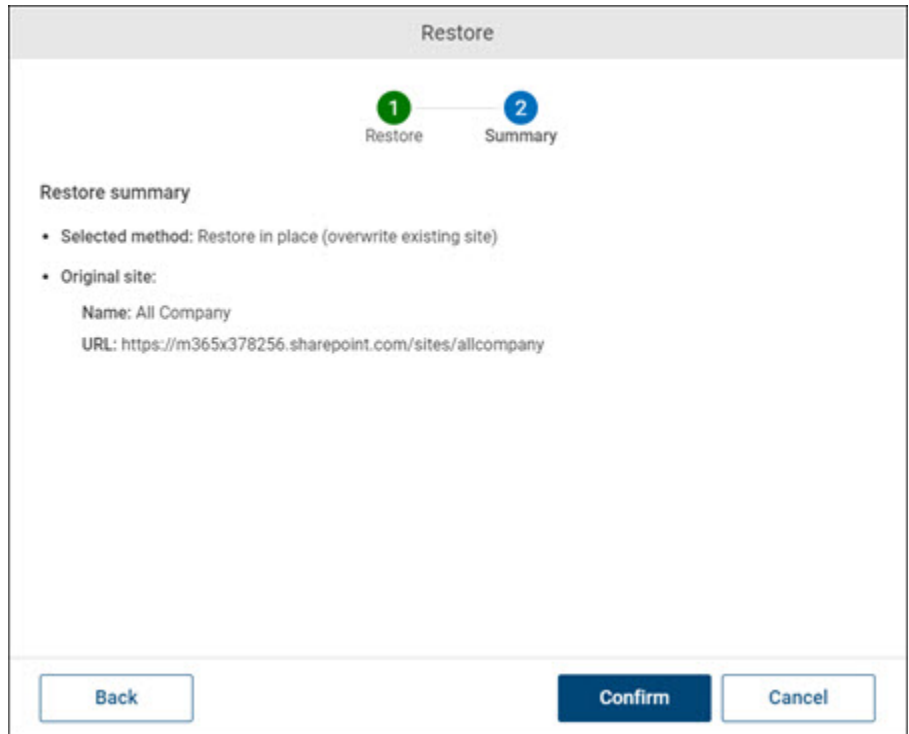
☒ Restore in place (overwrite existing site)

☐ Restore site as a new site (with new URL)

Next

Cancel

- 4 Review the restore summary and select Confirm. The site will be returned to its original location.



#### To restore a SharePoint site as a new site

- 1 Navigate to the site or subsite you want to restore.

---

**Note:** If you want to restore a site or subsite from an earlier point in time, select the **Snapshots Viewer** icon and then select the appropriate snapshot.

---

- 2 To the right of your site, select **...** > **Restore**.



- 3** Select **Restore site as a new site (with new URL)** and then select **Next**.

**Restore**

1 — 2 — 3  
Restore — Configure — Summary

**i** Restoring as a new site creates a new site with a new URL in parallel with the existing source site. The site will work like the original site. All users and permissions will also be restored.

Are you sure you want to restore **All Company**?

**Select method:**

☐ Restore in place (overwrite existing site)

☒ Restore site as a new site (with new URL)

**Original site:**

**Name:** All Company

**URL:** https://m365x378256.sharepoint.com/sites/allcompany

**Next** **Cancel**

- 4** In the field **New site**, enter a new name for your site. A new URL ending will automatically be added and the new site URL will be displayed.

---

**Note:** The URL must be unique and cannot contain special characters. If URL already exists in SharePoint you will see the error message **New SharePoint site URL is required**.

---

- 5** (Optional) You can edit the new URL ending if you want it to differ from the name of the new site.

**6** Select **Next**.

Restore

1

Restore

2

Configure

3

Summary

Selected method: Restore site as a new site (with new URL)

New site:

New site name

allcompany V2

New URL ending

allcompanyV2

New site URL: https://m365x378256.sharepoint.com/sites/allcompanyV2

Back

Next

Cancel

- 7 Review the restore summary and select **Confirm**. The site will be restored and will appear in the same location in the hierarchy in SharePoint.

Restore

1

Restore



2

Configure



3

Summary

**Restore summary**

- **Selected method:** Restore site as a new site (with new URL)
- **Original site:**

Name: All Company

URL: <https://m365x378256.sharepoint.com/sites/allcompany>
- **New site:**

Name: allcompany V2

URL: <https://m365x378256.sharepoint.com/sites/allcompanyV2>

Back

Confirm

Cancel

## What happens to SharePoint site items when I restore sites?

If items in your Lists with the same ID (regardless if the names are the same or different) already exist in SharePoint, they will be overwritten with the data in the snapshot.

If a subsite ID in SharePoint differs from the subsite ID in the snapshot (for example, if the subsite was previously lost and created), the subsite will be skipped.

If the quick launch menu of a site in SharePoint differs from the one in the snapshot, it will be overwritten by the menu in the snapshot.

If a file with a sensitivity label still exists in SharePoint, the restore of the file's content will fail because of a lack of permissions. Only the metadata will be overwritten and the restore job will be marked as failed.

# Restoring SharePoint data in different scenarios

SaaS Backup allows you to recover your SharePoint data along with its configurations and metadata - the data that defines your content, how it is displayed, and who has access to it.

It is recommended that you restore data at the highest appropriate level so that data is always restored intact, together with these configurations and metadata.

If you lose specific data items or configuration settings, you can restore these as individual items. However, it is only recommended if you know what exactly you lost.

## Requirements (only for older snapshots)

This is only necessary if you want to restore from a snapshot that was made before July 23, 2020 (the release of SAAS BACKUP 4.0). No action required if you want to restore a Communication Site page from a snapshot after July 23.

From the side of your SharePoint, you will not need to take any actions before you restore your SharePoint data, except when restoring Communication Site pages. To restore deleted pages, you need to set extra settings to your Site Collection, which can be done via PowerShell using:

```
Set-SPOsite -Identity <SiteURL> -DenyAddAndCustomizePages 0
```

For more information, see Microsoft's instructions.

<https://docs.microsoft.com/en-us/sharepoint/permissions/permissions#permissions>

## What happens to my data when I restore?

When you restore your SharePoint data, it will be created in your SharePoint.

If you have a custom SharePoint configuration, See “[Restoring SharePoint data with an advanced backup configuration](#)” on page 138.

In certain cases, you may not be able to restore data if parent content or configurations (such as views, permissions, etc.) are missing from SharePoint.

Please also note that List items cannot be restored if List metadata columns have symbols, special characters (including Danish letters), or spaces in its names.

## Structure of your SharePoint data in SAAS BACKUP

Every Site and Subsite folder contains:

- The data of your Site (Lists and Document Libraries)
- Your configurations (Site Columns, Site Content Types, Permissions, Customization)



- Subsites (if applicable)

Every List and Document Library folder contains:

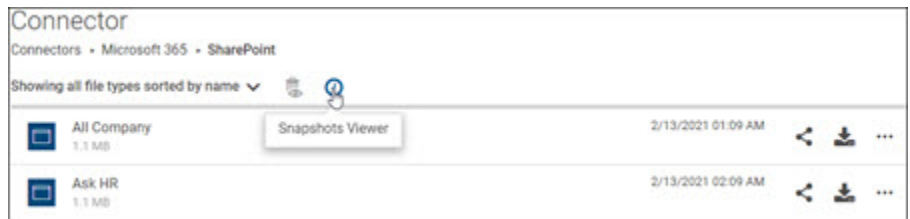
- Your data ("Items" in Lists and "Content" in Document Libraries)
- Your configurations (Columns, Content Types, Views, Item Permissions, and Assignments)

For a more detailed structure of your SharePoint data, See [“About SharePoint backup data types”](#) on page 111.

## Restore from Correct Snapshot

Before you restore data, remember to always find a snapshot from a time before your data was lost or damaged.

Select your connector, select the Snapshots Viewer icon, and then select the appropriate snapshot.



You will see a message showing you what snapshot you are viewing.



## Restore Scenarios

Depending on what data you want to recover, there are different ways to bring back your SharePoint data.

To help you find the appropriate level to restore, please find the scenario that applies to you

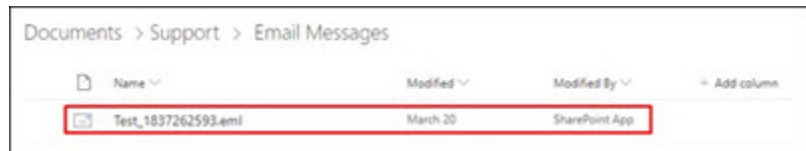
## 1 I lost files from a List or a Document Library

If you have lost files from a List or Document Library, restore either the folder that contains the items or content or the individual items.

**> SharePoint > Site Collection > Lists/DocLibs > List/DocLib > Items/Content**



When you restore a single item or folder, you restore the content along with the column properties and permissions (if applicable).



## 2 A List or Document Library or it was severely damaged

If a List or Document Library was severely damaged, restore the whole List or Document Library. This will restore everything -- both the content along with all other data including permissions, columns, content types, views, etc.

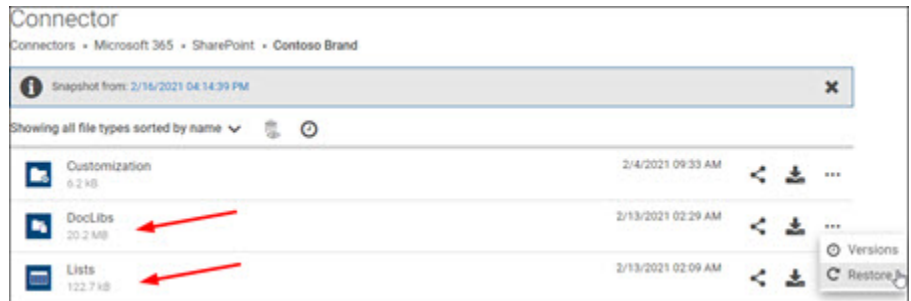
**> SharePoint > Site Collection > Lists/DocLibs > List/DocLib**



### 3 I lost my Lists or Document Libraries

If you lost all or many of your Lists or Document Libraries, restore the folder with all the Lists or Document Libraries.

#### > SharePoint > Site Collection

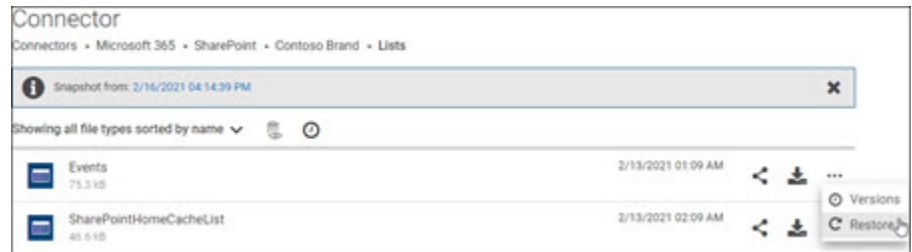


#### 4 I lost the configuration settings of my List or Document Library

If you lost all or most of your configurations (item permissions, columns, content types, views, assignments, permissions), we recommend you restore the whole List or Document Library. This will bring back not only the configurations but also the data that it applies to. This is the best way to ensure that all your data will be intact.

**Note:** Views and Items that were lost will have new IDs when they are restored.

##### SharePoint > Site Collection > Lists/DocLibs



If you lost or damaged only the permissions for a List or Document Library (those that have unique permissions), you can recover them by restoring the Assignments folder.

##### > SharePoint > Site Collection > Lists/DocLibs > List/DocLib



If you lost a specific content type or column, you can restore it as an individual item.

##### > SharePoint > Site Collection > Lists/DocLibs > List/DocLib > Columns



## 5 I lost a whole Site/Subsite or a Site/Substie was damaged

If you lost a whole Site or Subsite, restore the whole Site or Subsite. This will bring back both the data and all the metadata and configurations.

---

**Note:** If a Teams site is restored without a relevant group, it will be restored as a Communication site.

---

If a Site or Subsite was damaged (for example, if you lost both data and configurations, or you are uncertain what exactly was lost), restore the whole Site or Subsite.

---

**Note:** If the Site or Subsite still exists in SharePoint, you have the option of restoring in place by overwriting the original site or restoring to a new location.

---

Remember that when you restore a Site, all Subsites are also restored.

---

**Note:** Sites and Subsites will have new IDs when restored.

---

### > SharePoint

























### > SharePoint > Site Collection



Connector

Connectors • Microsoft 365 • SharePoint • All Company

Snapshot from: 2/16/2021 04:14:39 PM

Showing all file types sorted by name

	Customization 2.2 KB	2/4/2021 09:33 AM			...
	DocLibs 603.1 KB	2/13/2021 01:09 AM			...
	Lists 0 B	2/4/2021 09:33 AM			...
	Pages Link - Clicking here will take you to another location in the backup	2/4/2021 09:33 AM			
	Permissions 7.7 KB	2/4/2021 09:33 AM			...
	SiteColumns 404.8 KB	2/4/2021 09:33 AM			...
	SiteContentTypes 120.8 KB	2/4/2021 09:33 AM			...
	Subsites 0 B	2/4/2021 09:33 AM			...

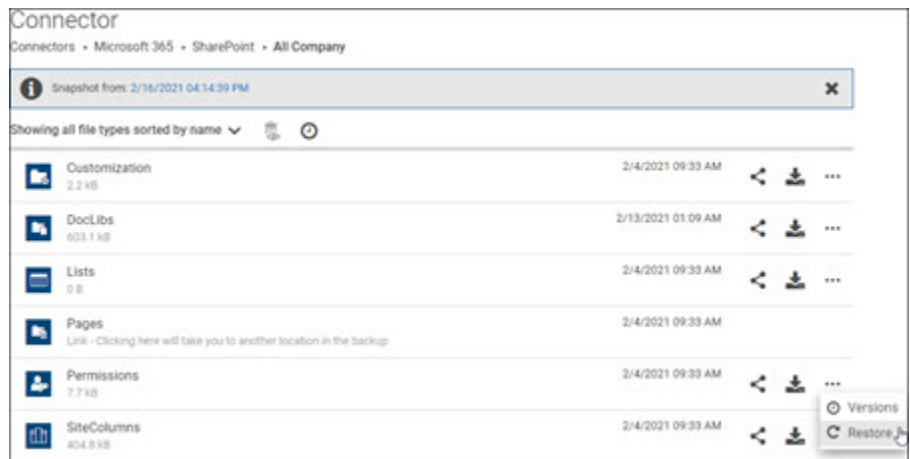
 Versions  
 Restore

If you know exactly what was lost or damaged, you can restore single items. Find the appropriate level so you don't have to do multiple restores.

## 6 I lost configurations to a whole Site/Subsite

If you lost configurations (permissions, Site Columns, or Site Content Types) you can restore these folders at the Site or Subsite level. However, please remember that when you restore configurations at this level, it will affect all Subsites, Lists, and Document Libraries that inherit permissions from the parent Site.

### > SharePoint > Site Collection



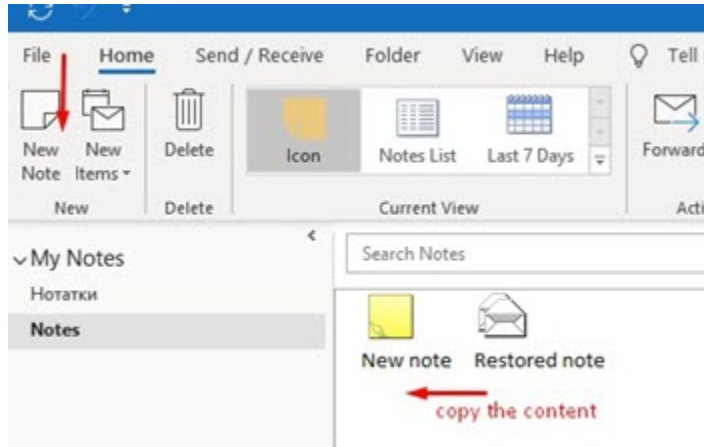
## Recover Outlook Notes

SaaS Backup backs up and restores Outlook Notes (desktop version) as EML files. After you restore, you may want to create a new note and copy the text of the restored file. This will make it easier to continue working with the file.

### Recreate the note from restored file:

1. Restore the note from SaaS Backup. It will appear in your Notes as an EML file.
2. Open the EML file.
3. Copy the content of the file.
4. Create a new note.
5. Paste the content from the restored file to the new one.





Now you will be able to edit the note and continue working with it.

After you have created the new note and saved the copied content, you can delete the EML file.

## Restoring SharePoint data across a tenant

SharePoint data can only be restored in place to its original location. You can use the General Restore function to restore all your SharePoint Sites data from the root level even if your SharePoint Sites have been damaged or lost. This function recovers your SharePoint data along with its configurations and metadata.

---

**Note:** : Use the **General Restore** function with caution as certain data may be overwritten.

---

### To restore an individual file or a folder

- 1 Open the connector to view files and folders of which you want to restore a snapshot.
- 2 Navigate to the file or a folder you want to restore.
- 3 Click the **More Options** icon, and select **Restore**.  
The application prompts you to confirm that you want to perform the operation.
- 4 Click **Yes** to complete the operation or click **Cancel** to cancel it.

# Restoring SharePoint data with an advanced backup configuration

Restoring a SharePoint backup is affected if you exclude SharePoint data types such as library files, list items, or metadata from your backup. Restoring inappropriate snapshots lead to major data loss. Therefore, it is important to understand what happens to your data when you restore it.

## Only Library files and metadata included in SharePoint backup

If you have lost a document library:

- Restoring the document library restores the document with all metadata.
- Restoring the whole site restores the document library with all metadata. Existing lists do not get deleted.
- Restoring the site as a new site with a new URL restores the site with document libraries and metadata.

## Only List items and metadata included in SharePoint backup

If you have lost a list:

- Restoring the list restores the list with all metadata.
- Restoring the whole site restores the list with all metadata. Existing document libraries do not get deleted.
- Restoring the site as a new site with a new URL restores the site with lists and metadata.

## Only List items included in SharePoint backup

If you have lost a list:

- Restoring the list restores the list with attachments, but without metadata.
- Restoring the whole site restores the list with all items and attachments. Existing document libraries and metadata do not get deleted.
- Restoring the site as a new site with a new URL restores the site with lists with its items and attachments. Default site metadata is restored.

## Only Library files included in SharePoint backup

If you have lost a document library:

- Restoring the document library restores the document library with its files. Custom metadata is not restored.
- Restoring the whole site restores the document library and its files without any custom metadata. Existing site data and metadata do not get deleted.

- Restoring the site as a new site with a new URL restores the site with document libraries and its files. Default site metadata is restored.

## Restore SharePoint sites using the Restore Wizard

If you want to restore all or several SharePoint sites at a time, use the Restore Wizard.

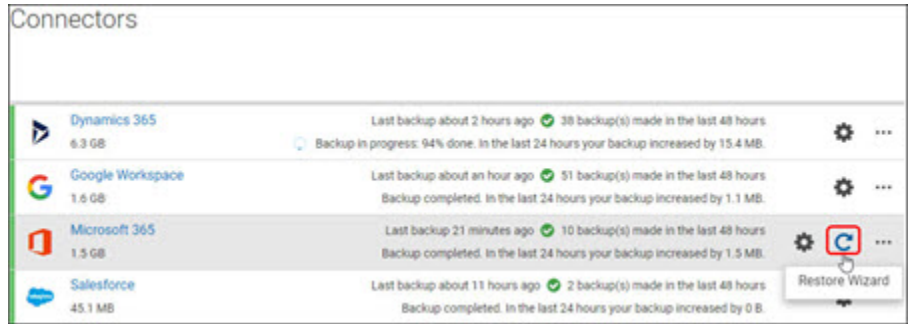
You can restore a SharePoint site as a new site with a new URL.

See [“About restoring SharePoint data”](#) on page 120.

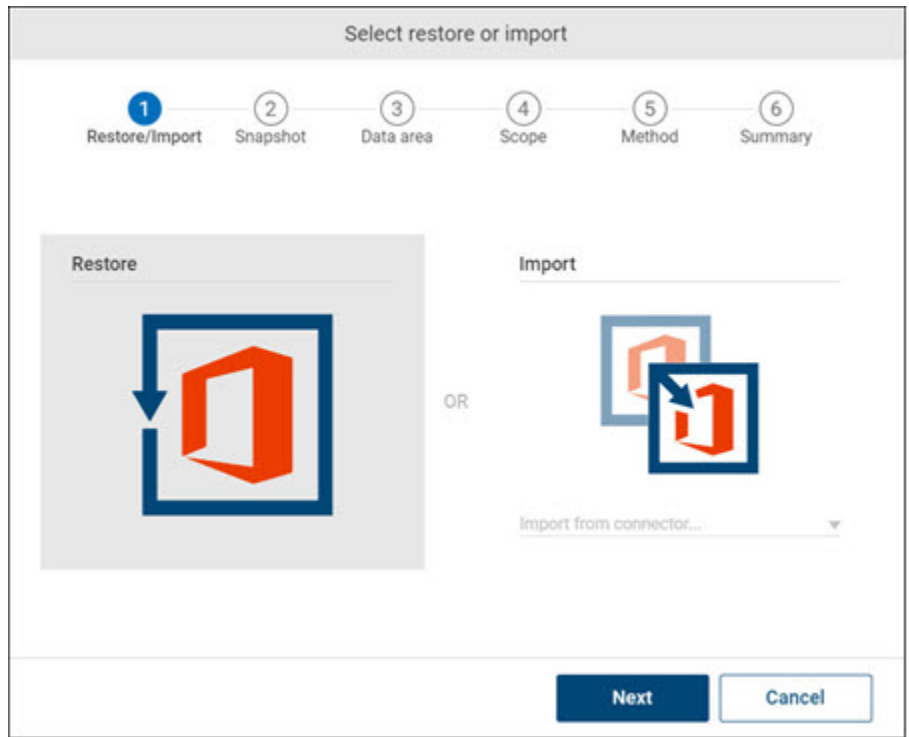
You can restore one item of your SharePoint site.

## To restore SharePoint sites

- 1 To open the Restore Wizard, to the right of your connector select the **Restore** icon.



- 2 Select **Restore**, and then select **Next**.



- 3 Select a snapshot from the time you want to restore, and then select **Next**.

Select snapshot to restore

1Restore/Import

2Snapshot

3Data area

4Scope

5Method

6Summary

2/16/2021

6 Feb

9 Feb

12 Feb

15 Feb

Snapshots

February ▾77 snapshots

16 - Tuesday ▾3 snapshots

04:14:39 PM ●1.5 GB

12:10:36 PM ●1.5 GB

06:10:06 AM ●1.5 GB

15 - Monday >6 snapshots

14 - Sunday >4 snapshots

Back





Next

Cancel

- 4 Select SharePoint, and then select **Next**.

Select data area to restore

1 Restore/Import 2 Snapshot 3 Data area 4 Scope 5 Method 6 Summary

	<b>Exchange</b> <ul style="list-style-type: none"><li>• Mail</li><li>• Calendar</li><li>• Tasks</li><li>• Contacts</li><li>• Public folders</li></ul>		<b>OneDrive</b> <ul style="list-style-type: none"><li>• Files</li></ul>
	<b>SharePoint</b> <ul style="list-style-type: none"><li>• Sites</li><li>• Subsites</li><li>• Team sites</li></ul>		<b>Groups &amp; Teams</b> <ul style="list-style-type: none"><li>• Conversations</li><li>• Files &amp; Plans</li><li>• Calendar</li><li>• Sites &amp; Channels</li></ul>

Back Next Cancel

- 5 Select the sites you want to restore, and then select **Next**.

Select how much data to restore

1 Restore/Import 2 Snapshot 3 Data area 4 Scope 5 Method 6 Summary

Select sites to restore

Filter sites

- ☐ All sites
- ☒ https://m365x378256.sharepoint.com/sites/askhr (1/1 sites selected)
- ☐ https://m365x378256.sharepoint.com/portals/hub
- ☐ https://m365x378256.sharepoint.com/sites/give
- ☐ https://m365x378256.sharepoint.com
- ☐ https://m365x378256.sharepoint.com/sites/safety
- ☐ https://m365x378256.sharepoint.com/sites/Retail
- ☐ https://m365x378256.sharepoint.com/sites/Contoso
- ☐ https://m365x378256.sharepoint.com/portals/Community
- ☐ https://m365x378256.sharepoint.com/sites/operations
- ☐ https://m365x378256.sharepoint.com/sites/leadership
- ☐ https://m365x378256.sharepoint.com/sites/allcompany

Back Next Cancel

- 6 Select how to handle duplicate items, and then select **Next**.

---

**Note:** When restoring SharePoint sites through the Restore Wizard, sites are automatically restored in-place to their original locations.

---

You have two options:

- **Skip duplicate items:** Modified items (same item but with different timestamps) will be skipped.
- **Overwrite existing items:** If an item already exists in SharePoint, it will be overwritten with the item from the snapshot. All items not found in SharePoint will be added.

Select how to restore the data

1

Restore/Import

2

Snapshot

3

Data area

4

Scope

5

Method

6

Summary

How should we restore your data?

To new folder

In-place

Clean existing data

How should we handle duplicates?

Skip duplicate items

Rename duplicate items

Overwrite existing items

Back

Next

Cancel



## 7 Review the summary, and then select **Restore**.

Sites or items present in SharePoint but not in the snapshot you are restoring from will not be deleted.

Restore summary

1

Restore/Import
 

2

Snapshot
 

3

Data area
 

4


Scope
 

5

Method
 

6

Summary


**Warning:** Selecting Restore below will start the restore job. This action cannot be undone.

Restore summary

- Restoring SharePoint data from snapshot dated 2/16/2021 04:14 PM
- 1 SharePoint site(s) selected for restore
- Selected restore method: In-place restore handling duplicates by skipping duplicate items

Back

Restore

Cancel

## About Groups and Teams data backup

Office 365 Groups, Teams, and SharePoint team sites are closely related and often contain overlapping data. Every Office 365 Group has a team site in SharePoint. A group can include a team in Teams, which needs to be created manually. Every Team that is created automatically creates an Office 365 Group, which in turn creates a team site in SharePoint.

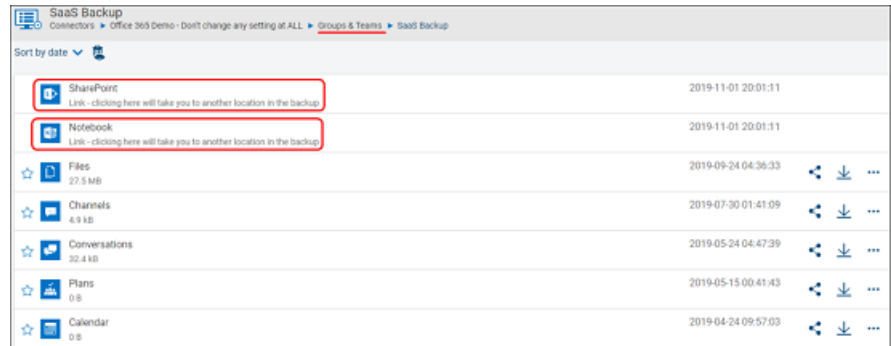
The data of groups and teams is backed up in the Groups & Teams backup. Team sites are backed up in the SharePoint backup. If you want to back up a team site and its notebook, the SharePoint backup must be enabled in addition to the Groups & Teams backup.

Teams private channels are not backed up by default. To back up Teams channel, the channel owner needs to add global administrator to the Teams channel.

SaaS Backup backs up the following Groups & Teams data:

- Group Conversations
- Calendar
- Planner
- Files
- Team channels including channel posts and replies
  - Wiki pages (backed up but cannot be restored, only recovered by copy-pasting data out or downloading raw files)
- Notebook (only if SharePoint backup is enabled)
- Team sites (only if SharePoint backup is enabled)

**If SharePoint is enabled**, you can back up team sites and associated notebooks. You can view the links to SharePoint (team sites) and notebook in your Groups & Teams backup.



SaaS Backup		
Connectors > Office 365 Demo - Don't change any setting at ALL > Groups & Teams > SaaS Backup		
Sort by date		
SharePoint	Link - clicking here will take you to another location in the backup	2019-11-01 20:01:11
Notebook	Link - clicking here will take you to another location in the backup	2019-11-01 20:01:11
Files	27.5 MB	2019-09-24 04:36:33
Channels	4.9 KB	2019-07-30 01:41:09
Conversations	32.4 KB	2019-05-24 04:47:39
Plans	0 B	2019-05-15 00:41:43
Calendar	0 B	2019-04-24 09:57:03

**If SharePoint is not enabled**, you cannot back up team sites and their associated notebooks. You cannot view the links to SharePoint (team sites) and notebook.

Snapshot from: 4.6963.880		
Sort by date ▼		
SharePoint	Link - clicking here will take you to another location in the backup	2019-11-01 20:01:11
Notebook	Link - clicking here will take you to another location in the backup	2019-11-01 20:01:11
Files	27.5 MB	2019-09-24 04:36:33 < > ⌵ ⋮
Channels	4.9 KB	2019-07-30 01:41:09 < > ⌵ ⋮
Conversations	32.4 KB	2019-05-24 04:47:39 < > ⌵ ⋮
Plans	0 B	2019-05-15 00:41:43 < > ⌵ ⋮
Calendar	0 B	2019-04-24 09:57:03 < > ⌵ ⋮

## About Groups and Teams backup data types

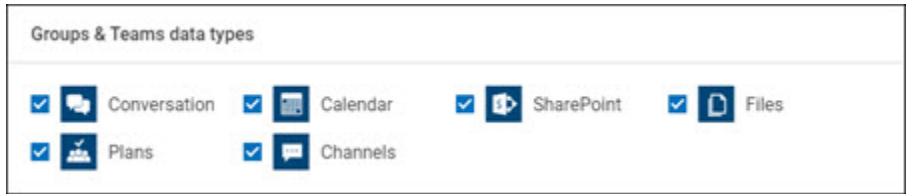
Available Groups & Teams data types

- Conversation
- Calendar
- Planner
- Files
- Channels
  - Team channel posts and replies (Conversations)
  - Wiki pages (backed up but cannot be restored, recoverable only by copy-pasting data out or downloading raw files)
- SharePoint
  - Team sites
  - Notebooks

---

**Note:** Teams private channels have their own team sites and the private channel's files are backed up not in the Files folder in Groups and Teams, but in the SharePoint folder. To find these files in SaaS Backup, go to **SharePoint > the team's channel site > DocLibs > Documents > Content**.

---



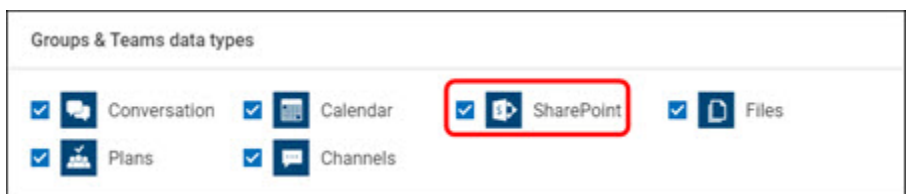
## Understanding how Groups & Teams and SharePoint are related

Microsoft 365 groups, teams, and SharePoint team sites are closely related and often contain overlapping data. Every Microsoft 365 Group has a team site in SharePoint. A group can also have a team in Teams, which is either manually or automatically created depending on Microsoft settings. For every team that is created, a Microsoft 365 group is automatically created, which in turn creates a team site in SharePoint.

In SaaS Backup, groups and teams data is backed up in the Groups and Teams folder, while the group's team site and notebook are backed up in the SharePoint folder.



However, to backup a group's team site and its notebook, you do not need to enable the SharePoint data area but can select the SharePoint checkbox in the Groups & Teams advanced backup settings.




Where to find team sites and notebooks?

## SharePoint data type selected


If the SharePoint data type is selected, a SharePoint folder with the team sites will be created in SaaS Backup – even if the SharePoint data area is disabled on the main Microsoft 365 configuration window. Links to the SharePoint team site and to the notebook will be found in **Groups & Teams > group name**.

This remains true even if a group is included in the backup in Groups & Teams, but the its team site is excluded from the backup in the SharePoint settings.

Groups & Teams Backup Settings



Here you can see all Microsoft 365 groups and data types that are included in your backup. You can customize your backup, but we recommend you include all groups and data types so that all your data is covered.



Select Microsoft 365 Groups to back up

Filter groups

---

▼ ☒ All groups

- ☒ Safety - safety@M365x378256.onmicrosoft.com
- ☒ Office 365 Adoption - office365adoption@M365x378256.onmicrosoft.com
- ☒ All Company - allcompany@M365x378256.onmicrosoft.com
- ☒ Sales and Marketing - SalesAndMarketing@M365x378256.onmicrosoft.com
- ☒ Digital Initiative Public Relations - DigitalInitiativePublicRelations@M365x378256.onmicrosoft...
- ☒ Operations - operations@M365x378256.onmicrosoft.com
- ☒ Leadership - leadership@M365x378256.onmicrosoft.com
- ☒ New Employee Onboarding - newemployeeonboarding@M365x378256.onmicrosoft.com
- ☒ Contoso Life - contosolife@M365x378256.onmicrosoft.com
- ☒ Contoso Team - contosoteam@M365x378256.onmicrosoft.com
- ☒ Contoso - Contoso@M365x378256.onmicrosoft.com
- ☒ Parents of Contoso - parentsofcontoso@M365x378256.onmicrosoft.com
- ☒ U.S. Sales - USSales@M365x378256.onmicrosoft.com
- ☒ Retail - Retail@M365x378256.onmicrosoft.com
- ☒ Mark 8 Project Team - Mark8ProjectTeam@M365x378256.onmicrosoft.com
- ☒ SOC Team - SOCTeam@M365x378256.onmicrosoft.com

Advanced

OK

Cancel

SharePoint Online Backup Settings

Here you can see all SharePoint sites that are included in your backup. You can customize your backup, but we recommend you include all sites so that all of your data is covered.

Select site collections to back up

Filter

- ☒ All sites
- ☒ <https://m365x378256.sharepoint.com/sites/droneproducttraining>
- ☒ <https://m365x378256.sharepoint.com/sites/askhr>
- ☒ <https://m365x378256.sharepoint.com/sites/SalesAndMarketing>
- ☒ <https://m365x378256.sharepoint.com/sites/safety>
- ☒ <https://m365x378256.sharepoint.com/sites/contosolife>
- ☒ <https://m365x378256.sharepoint.com/portals/Community>
- ☒ <https://m365x378256.sharepoint.com/sites/SOCTeam>
- ☒ <https://m365x378256.sharepoint.com/sites/USSales>
- ☒ <https://m365x378256.sharepoint.com/sites/ThePerspective>
- ☒ <https://m365x378256.sharepoint.com/sites/contentTypeHub>
- ☒ <https://m365x378256.sharepoint.com/sites/newemployeeonboarding>
- ☒ <https://m365x378256.sharepoint.com/sites/leadership>
- ☒ <https://m365x378256.sharepoint.com/sites/Contoso>
- ☒ <https://m365x378256.sharepoint.com/sites/benefits>
- ☒ <https://m365x378256.sharepoint.com/sites/ceoconnection>
- ☒ <https://m365x378256.sharepoint.com/sites/allcompany>
- ☒ <https://m365x378256.sharepoint.com/sites/ContosoNews>


Advanced

OK


Cancel

If a group is excluded from the backup in the Groups & Teams settings, but its team site is included in the backup in the SharePoint settings, the group will not have a folder in the Groups & Teams backup, but the team's site will be found in the SharePoint folder.

Groups & Teams Backup Settings



Here you can see all Microsoft 365 groups and data types that are included in your backup. You can customize your backup, but we recommend you include all groups and data types so that all your data is covered.



Select Microsoft 365 Groups to back up

▼ ☒ All groups


- ☒ Safety - safety@M365x378256.onmicrosoft.com
- ☒ Office 365 Adoption - office365adoption@M365x378256.onmicrosoft.com
- ☒ All Company - allcompany@M365x378256.onmicrosoft.com
- ☒ Sales and Marketing - SalesAndMarketing@M365x378256.onmicrosoft.com
- ☒ Digital Initiative Public Relations - DigitalInitiativePublicRelations@M365x378256.onmicrosoft...
- ☒ Operations - operations@M365x378256.onmicrosoft.com
- ☒ Leadership - leadership@M365x378256.onmicrosoft.com
- ☒ New Employee Onboarding - newemployeeonboarding@M365x378256.onmicrosoft.com
- ☒ Contoso Life - contosolife@M365x378256.onmicrosoft.com
- ☒ Contoso Team - contosoteam@M365x378256.onmicrosoft.com
- ☒ Contoso - Contoso@M365x378256.onmicrosoft.com
- ☒ Parents of Contoso - parentsofcontoso@M365x378256.onmicrosoft.com
- ☒ U.S. Sales - USSales@M365x378256.onmicrosoft.com
- ☒ Retail - Retail@M365x378256.onmicrosoft.com
- ☒ Mark 8 Project Team - Mark8ProjectTeam@M365x378256.onmicrosoft.com
- ☒ SOC Team - SOCTeam@M365x378256.onmicrosoft.com

Advanced


OK

Cancel

SharePoint Online Backup Settings



Here you can see all SharePoint sites that are included in your backup. You can customize your backup, but we recommend you include all sites so that all of your data is covered.



Select site collections to back up

Filter

---

- ☒ All sites
- ☒ <https://m365x378256.sharepoint.com/sites/droneproducttraining>
- ☒ <https://m365x378256.sharepoint.com/sites/askhr>
- ☒ <https://m365x378256.sharepoint.com/sites/SalesAndMarketing>
- ☒ <https://m365x378256.sharepoint.com/sites/safety>
- ☒ <https://m365x378256.sharepoint.com/sites/contosolife>
- ☒ <https://m365x378256.sharepoint.com/portals/Community>
- ☒ <https://m365x378256.sharepoint.com/sites/SOCTeam>
- ☒ <https://m365x378256.sharepoint.com/sites/USSales>
- ☒ <https://m365x378256.sharepoint.com/sites/ThePerspective>
- ☒ <https://m365x378256.sharepoint.com/sites/contentTypeHub>
- ☒ <https://m365x378256.sharepoint.com/sites/newemployeeonboarding>
- ☒ <https://m365x378256.sharepoint.com/sites/leadership>
- ☒ <https://m365x378256.sharepoint.com/sites/Contoso>
- ☒ <https://m365x378256.sharepoint.com/sites/benefits>
- ☒ <https://m365x378256.sharepoint.com/sites/ceoconnection>
- ☒ <https://m365x378256.sharepoint.com/sites/allcompany>
- ☒ <https://m365x378256.sharepoint.com/sites/ContosoNews>

Advanced

OK

Cancel

## SharePoint data type deselected

If the SharePoint data type is deselected, but the group's team site is selected in the SharePoint backup settings, the group's team site will be backed up, but there will be no link to the team site in the group's folder. The backed up site will be in the SharePoint folder.



### Groups & Teams Backup Settings

Here you can see all Microsoft 365 groups and data types that are included in your backup. You can customize your backup, but we recommend you include all groups and data types so that all your data is covered.

Select Microsoft 365 Groups to back up

0 items selected

▼ ☒ All groups

- ☒ Safety - safety@M365x378256.onmicrosoft.com
- ☒ Office 365 Adoption - office365adoption@M365x378256.onmicrosoft.com
- ☒ All Company - allcompany@M365x378256.onmicrosoft.com
- ☒ Sales and Marketing - SalesAndMarketing@M365x378256.onmicrosoft.com
- ☒ Digital Initiative Public Relations - DigitalInitiativePublicRelations@M365x378256.onmicrosoft.com
- ☒ Operations - operations@M365x378256.onmicrosoft.com
- ☒ Leadership - leadership@M365x378256.onmicrosoft.com
- ☒ New Employee Onboarding - newemployeeonboarding@M365x378256.onmicrosoft.com
- ☒ Contoso Life - contosolife@M365x378256.onmicrosoft.com
- ☒ Contoso Team - contosoteam@M365x378256.onmicrosoft.com

Groups & Teams data types

☒ Conversation

☒ Calendar

☒ SharePoint

☒ Files

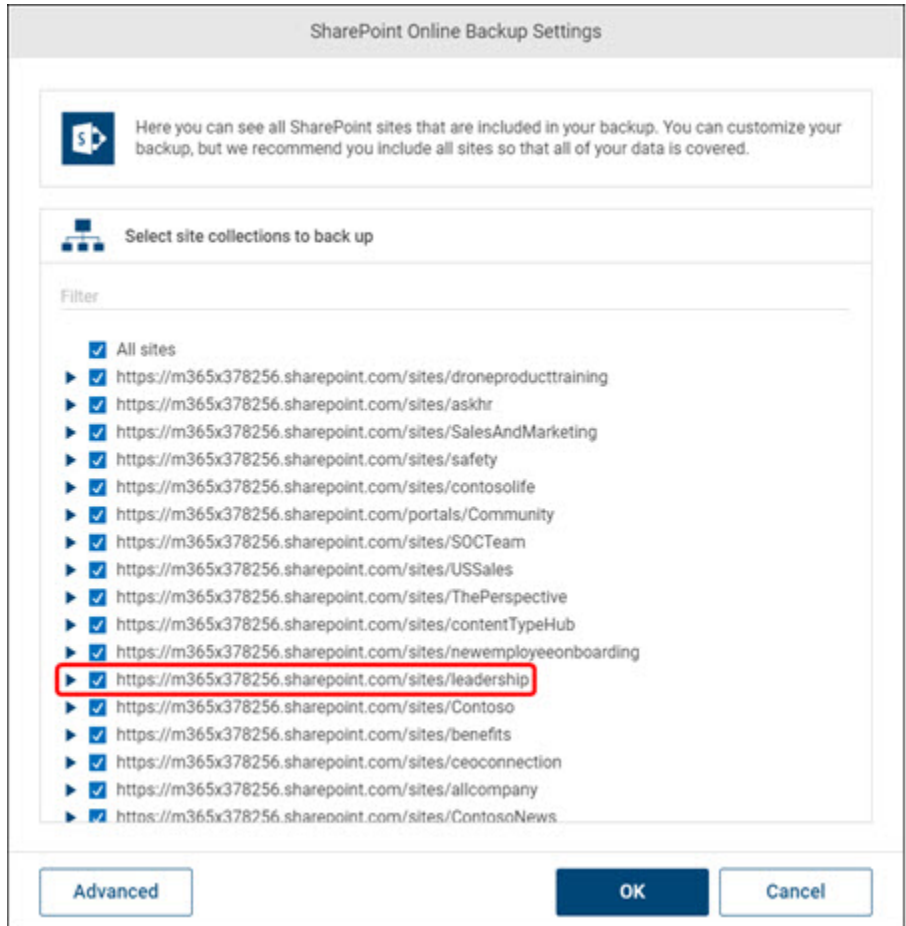
☒ Plans

☒ Channels

Advanced

OK

Cancel



## Restore Groups and Teams data using the Restore Wizard

You can use the Restore Wizard to restore entire groups along with their team data or to restore only parts of your group data.

You can restore individual channels or posts.

See [“Restoring Teams channels data”](#) on page 162.

You can restore individual groups or teams items.

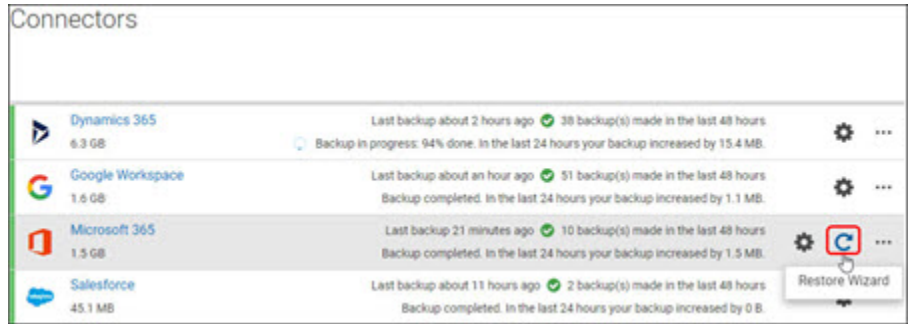
---

**Note:** Wiki pages are backed up, but they cannot be restored, only downloaded or shared.

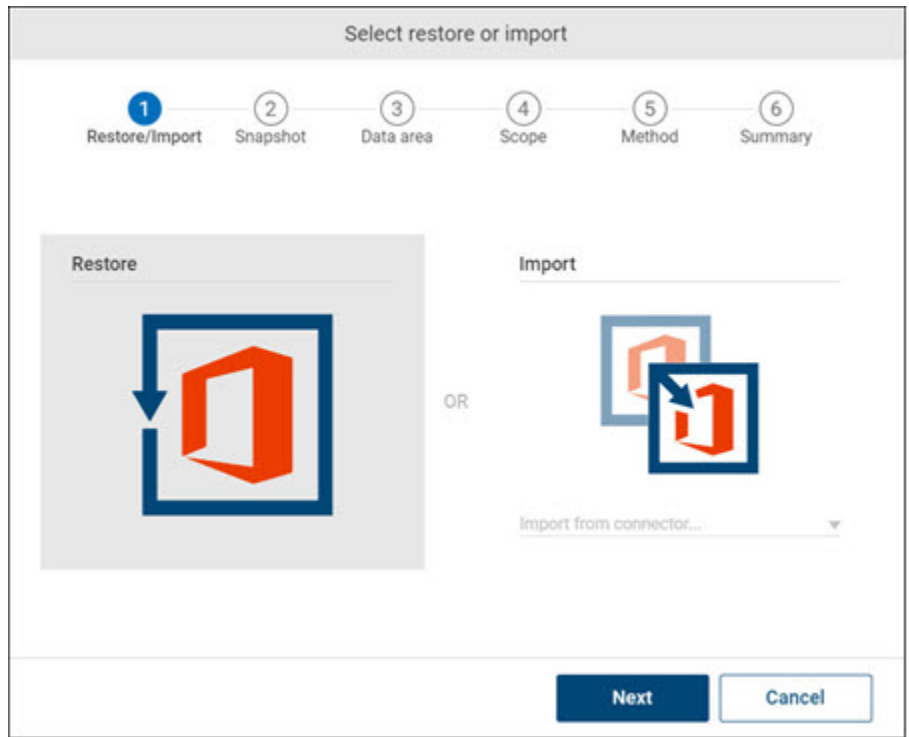
---

## To restore group and team data

- 1 To open the Restore Wizard, to the right of your connector select the **Restore** icon.



- 2 Select **Restore**, and then select **Next**.



- 3 Select a snapshot from the time you want to restore, and then select **Next**.

Select snapshot to restore

1

Restore/Import
 

2

Snapshot
 

3

Data area
 

4

Scope
 

5

Method
 

6

Summary

2/16/2021

6 Feb

9 Feb

12 Feb

15 Feb

Snapshots

February ▾	77 snapshots
16 - Tuesday ▾	3 snapshots
04:14:39 PM ●	1.5 GB
12:10:36 PM ●	1.5 GB
06:10:06 AM ●	1.5 GB
15 - Monday >	6 snapshots
14 - Sunday >	4 snapshots

Back





Next

Cancel

4 Select Groups & Teams, and then select **Next**.

Select data area to restore

1 Restore/Import 2 Snapshot 3 Data area 4 Scope 5 Method 6 Summary

	<b>Exchange</b> <ul style="list-style-type: none"><li>• Mail</li><li>• Calendar</li><li>• Tasks</li><li>• Contacts</li><li>• Public folders</li></ul>		<b>OneDrive</b> <ul style="list-style-type: none"><li>• Files</li></ul>
	<b>SharePoint</b> <ul style="list-style-type: none"><li>• Sites</li><li>• Subsites</li><li>• Team sites</li></ul>	 <b>Groups &amp; Teams</b> <ul style="list-style-type: none"><li>• Conversations</li><li>• Files &amp; Plans</li><li>• Calendar</li><li>• Sites &amp; Channels</li></ul>	

Back Next Cancel

- 5 Select the groups and data types you want to restore, and then select **Next**.

---

**Note:** To recover a whole group, select all data types.

---

Select how much data to restore

1 Restore/Import   
 2 Snapshot   
 3 Data area   
 4 Scope   
 5 Method   
 6 Summary

**Select groups to restore**

Filter groups

- ☐ Select all
- ☐ Ask HR
- ☐ CEO Connection
- ☐ Sales Best Practices
- ☐ Parents of Contoso
- ☒ Contoso Life
- ☐ Contoso Team
- ☒ Safety
- ☐ Office 365 Adoption
- ☐ All Company
- ☐ Operations
- ☐ Leadership

**Select what to restore**

- ☒ Conversations
- ☒ Calendar
- ☒ Plan
- ☒ Files
- ☒ Members
- ☒ Owners
- ☒ SharePoint
- ☒ Channels

Back
Next
Cancel

- 6 Select how to handle duplicate items, and then select **Next**.

You have two options:

- **Skip duplicate items**
  - Modified items (same item but with different timestamps) will be skipped.
  - Modified plan tasks (same item but with different timestamps) will overwrite the plan tasks in Groups.
- **Overwrite existing items**
  - Modified items (including plans) (same item but with different timestamps) will overwrite items in Groups & Teams.

Select how to restore the data

1

Restore/Import

2

Snapshot

3

Data area

4

Scope

5

Method

6

Summary

How should we restore your data?

To new folder

In-place

Clean existing data

How should we handle duplicates?

Skip duplicate items

Rename duplicate items

Overwrite existing items

Back

Next

Cancel



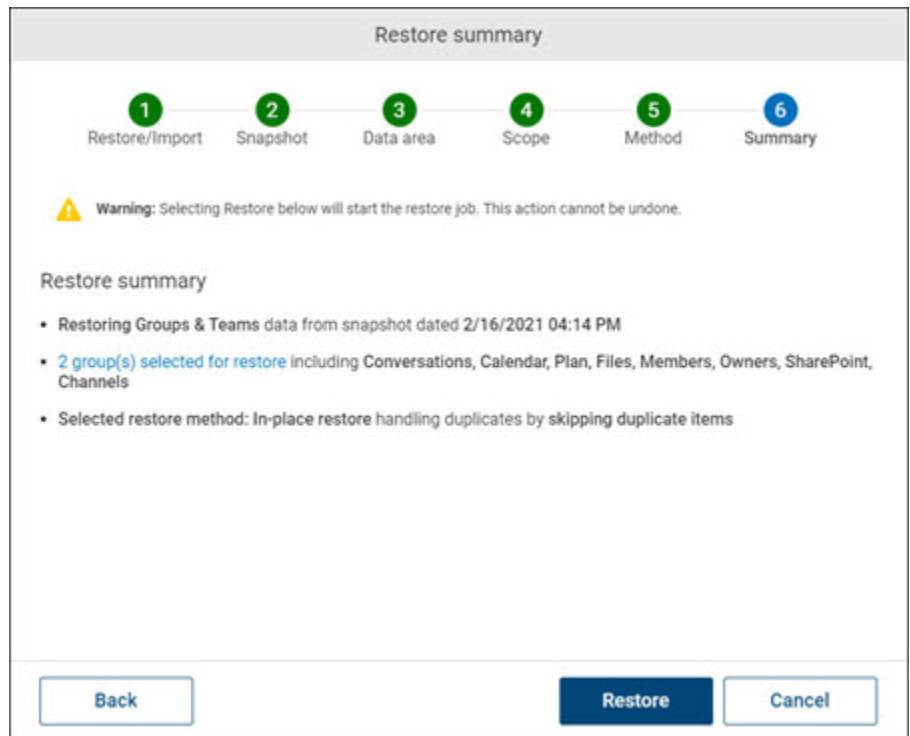
**7** Review the summary, and then select **Restore**.

---

**Note:** Group conversations, calendar events, plan tasks, and files present in Groups & Teams but not in the snapshot will be deleted.

---

Team channel posts and replies present in Groups & Teams but not in the snapshot will not be deleted.



## Adding global administrator to the Teams channel

SaaS Backup cannot automatically add the Global Administrator to Teams channel to access its data. Therefore, Private channels in Teams are not backed up by default. The Global admin is the Microsoft service account used for the backup, that is the service account used to authenticate a connector.

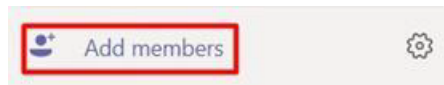
To back up the data of a private channel, the channel owner needs to add Global Administrator as a member of channel.

### To add global administrator to the Teams channel

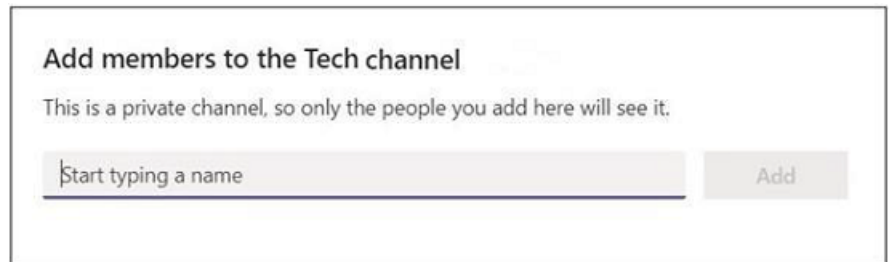
- 1 In Teams, open the private team channel. Private channels are marked with a lock icon.



- 2 In the upper-right corner of the **Posts** page, click **People**.



- 3 At the bottom of the People window, select **Add members**.



- 4 Enter the email address of the Global admin and select **Add**.  
 The application backs up the private channel.

## Restoring Teams channels data

Team channels data can be restored at various levels: all of a team's channels, an individual channel, or an individual post.

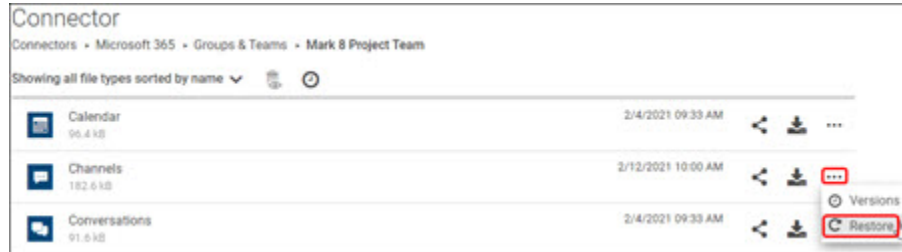
Restoring a channel brings back all conversations, but not Wiki pages. Wiki pages cannot be restored, only shared and downloaded.

If a channel has been **deleted within the last 30 days**, the channel cannot be restored, and thus the item restore job will be marked as failed. Only once the channel has been completely removed from Teams (after 30 days) will it be possible to restore it from SAAS BACKUP. If fewer than 21 days have passed since the channel was deleted, it is possible to restore the channel from Teams.

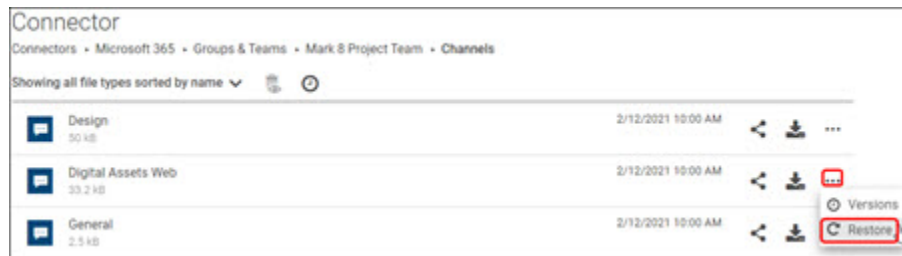
## To restore channel data

- 1 Find the group in your connector and then navigate to the data you want to restore.

- To restore all of a team's channels, locate the **Channels** folder.



- To restore an individual channel, open the **Channels** folder and then locate the channel.



- To restore an individual post, navigate **Channels > channel name > Conversation**, then locate the chat message.



- 2 Select **... > Restore**.

What happens to channel data when it is restored?

## Restored channel data

- Restoring the Channels folder brings back all channels of a team, including all posts and replies.
- If the channel still exists in Teams, deleted and edited messages will be added to the bottom of the posts feed.

All existing messages that have not been edited will be skipped.

- If the channel has been deleted from Teams, the channel with all posts will be restored.
- Restoring an individual channel brings back all deleted and edited posts of a channel, including all replies.  
Existing posts that have not been edited will be skipped.
- Restoring an individual post brings back all replies. The message will be restored as a new one at the end of the channel's posts.

## Replies

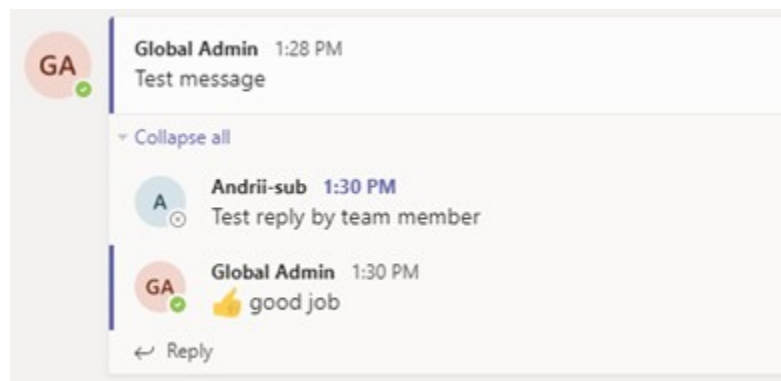
If a reply was deleted or edited, then it can be restored by restoring the main message, even if the main message was not deleted. The reply is restored at the end of all the replies.

## Message sender and timestamp

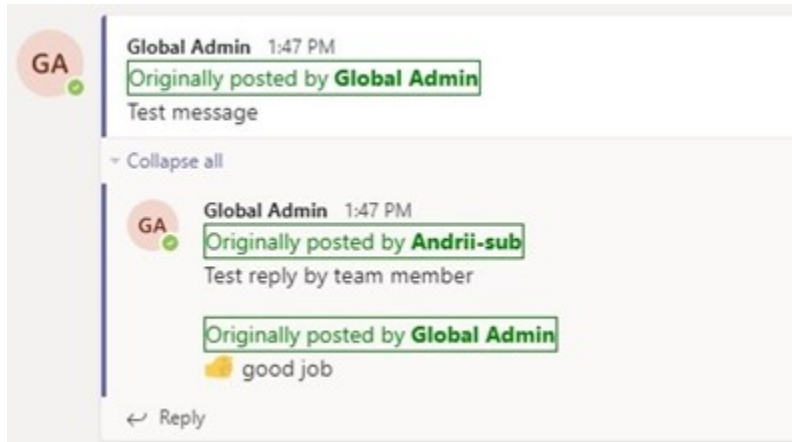
All restored messages and replies will be posted by the Global admin account. The name of the original sender will be found in the body of the message as a header inside a green box.

The timestamp will reflect the data that the message was restored, not the date that it was sent.

Original messages



Restored messages

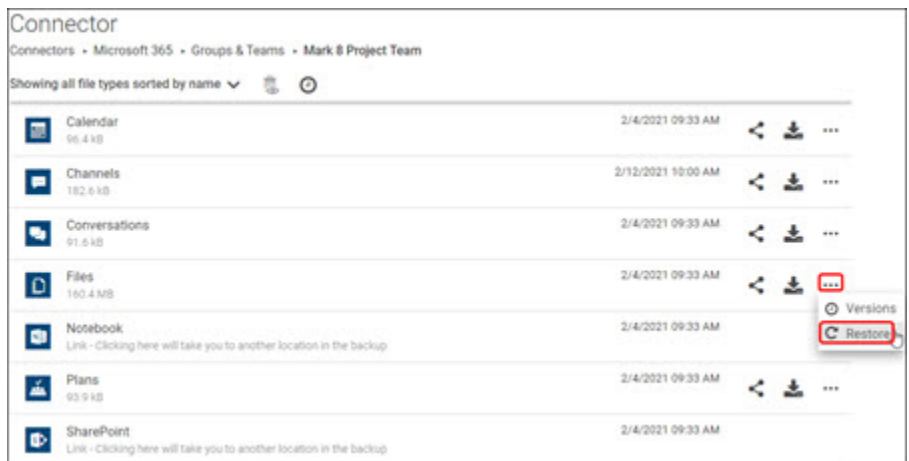


## Message Attachments

Attachments – files such as images, Word documents, etc., – are not restored together with messages or replies as attachments.

All files that are attached to messages are saved in the channel in the Files tab and in the team's SharePoint site.

This means that it is possible to return these files to Teams by restoring the group's Files folder.



## Other Elements of Messages

Embedded text and other items such as code snippets, gifs, stickers, and emojis are restored. Reactions to messages are not restored.

# Managing single sign-on (SSO) authentication in Office 365

This chapter includes the following topics:

- [About single sign-on authentication](#)
- [Creating a single sign-on administrator profile](#)
- [Configuring single sign-on using Azure Active Directory](#)
- [Assigning users to single sign-on application in Azure Active Directory](#)
- [Configuring single sign-on using ADFS](#)
- [Configuring single sign-on in SaaS Backup](#)

## About single sign-on authentication

Single sign-on authentication allows you to log in to the application using a single set of credentials. If you use single sign-on to sign in to SaaS Backup, SaaS Backup uses the credentials of your Microsoft account you are already signed in to. To log in with the credentials of a different user, it is recommended to use an incognito window.

When you enter your email address for log in, SaaS Backup checks if the user with that email address has single sign-on configured. If it is configured, SaaS Backup creates an authentication request and sends it to the identity provider's (Microsoft) login page. At this stage, SaaS Backup requests Microsoft to perform authentication on its behalf.

If you are not already logged in to Microsoft, you can log in with the same user credentials (the email address mentioned above and the user password), and Microsoft redirects you to SaaS Backup.

If the you are already logged in to Microsoft and the Single sign-on authentication is configured, Microsoft automatically uses those credentials to log you in to SaaS Backup.

To avoid this situation where SaaS Backup automatically uses the credentials of the user logged in to Microsoft, it is recommended to use an incognito window.

## Creating a single sign-on administrator profile

Before you configure single sign-on authentication in SaaS Backup and your identity provider Azure AD, it is recommended that the master administrator must create a single sign-on admin user role in SaaS Backup. The single sign-on administrator is a dedicated user with the permission to access the single sign-on configuration. Single sign-on is never enabled for this administrator. They can always sign in to the account with their SaaS Backup credentials.

This ensures that the master administrator and the other users do not get locked out of their account if the single sign-on is configured incorrectly or if the single sign-on certificate expires.

## Configuring single sign-on using Azure Active Directory

If you are using Azure AD as your identity provider, you need a Microsoft Azure account with the active Azure AD Premium subscription so that you can add non-gallery applications.

Before you configure single sign-on in SaaS Backup, you need to configure single sign-on with Azure AD. During this configuration, you will obtain the IDP URL and the certificate that are required to configure single sign-on in SaaS Backup.

### To configure single sign-on using Azure Active Directory

- 1 Sign in to the Azure portal.
- 2 Navigate to **Azure Active Directory > Enterprise applications**.
- 3 Select **+New application > Non-gallery application**.
- 4 Under **Add your own application**, enter a name for the application, and click **Add**.
- 5 In the application's left-hand navigation menu, select **Single sign-on**.

- 6 Under **Select a single sign-on method**, select **SAML**.
- 7 In the **Basic SAML Configuration** dialog box, click the Edit icon to open the configuration window

**Basic SAML Configuration**

[Save](#)

Values for the fields below are provided by [redacted]. You may either enter those values manually, or upload a pre-configured SAML metadata file if provided by [redacted] [Upload metadata file.](#)

\* Identifier (Entity ID)  Enter an identifier  
 Please enter an identifier which is unique within your organization.  
 This field is required

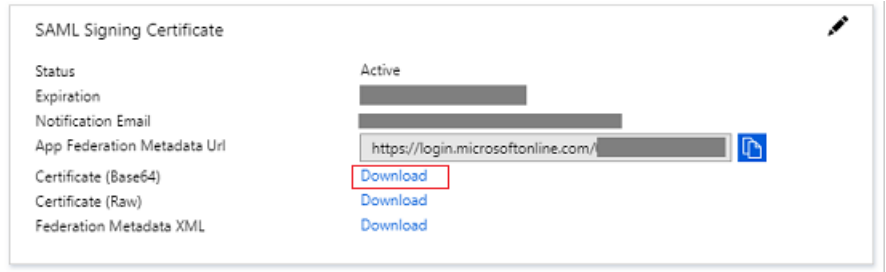
\* Reply URL (Assertion Consumer Service URL)  Enter a reply URL  
 Please enter a valid URL.  
 This field is required

[Set additional URLs](#)

- 8 In the Identifier field, enter the URL depending on datacenter location:
  - Europe, Middle East, Africa: <https://eu.saasbackup.veritas.com/sso/metadata>
  - Americas: <https://us.saasbackup.veritas.com/sso/metadata>
  - Asia, Pacific, Japan: <https://ap.saasbackup.veritas.com/sso/metadata>
- 9 In the Reply URL field enter the URL depending on datacenter location:
  - Europe, Middle East, Africa: <https://eu.saasbackup.veritas.com/sso/login>
  - Americas: <https://us.saasbackup.veritas.com/sso/login>
  - Asia, Pacific, Japan: <https://ap.saasbackup.veritas.com/sso/login>
- 10 Click **Save**.



- 11 To download the certificate with a \*.cer extension, in the **SAML Signing Certificate** dialog box, click **Download** to the right of **Certificate (Base64)**.



- 12 In the **Set up SSO Demo** dialog box, locate the Login URL.
  - This is the IDP URL that you need to configure SSO in VSB.

#### Set up SSO Demo

You'll need to configure the application to link with Azure AD.

Login URL

https://login.microsoftonline.com/6bc17c1c-6785-4b1e-90d4-11a724cc3f/saml2

Azure AD Identifier

https://sts.windows.net/6bc17c1c-6785-4b1e-90d4-11a724cc3f/

Logout URL

https://login.microsoftonline.com/common

[View step-by-step instructions](#)

- Alternatively, you can click **View step-by-step instructions** to open the Configure sign-on guide on how to configure SSO in VSB with Azure AD.
- The IDP URL is named **SAML Single Sign-On Service URL**

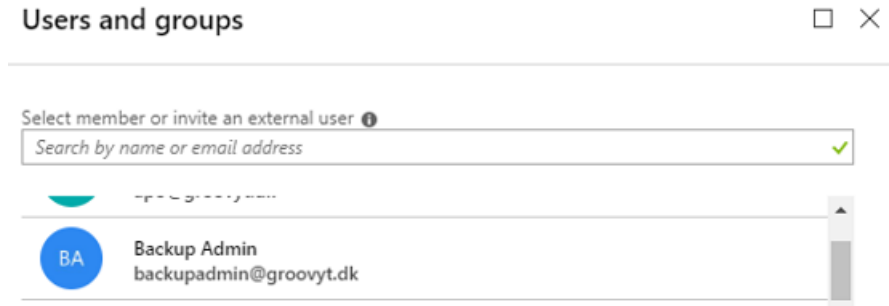
During this process, you will be prompted to provide files and URLs that correspond to Azure Active Directory. When prompted, use the files and URLs shown below:

- **SAML Single Sign-On Service URL:**

https://login.microsoftonline.com/6bc17c1c-6785-4b1e-90d4-11a724cc3f/saml2

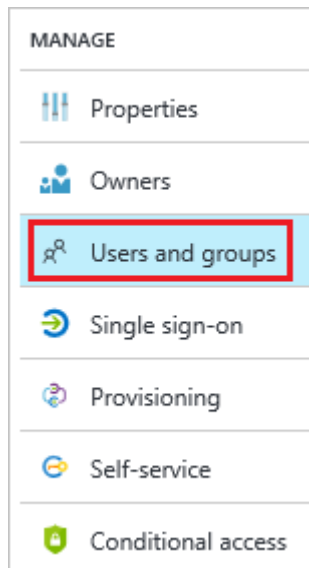
# Assigning users to single sign-on application in Azure Active Directory

To enable SSO for individual users, you need to assign these users to your SSO application in Azure AD. Ensure that these users exist in SaaS Backup.

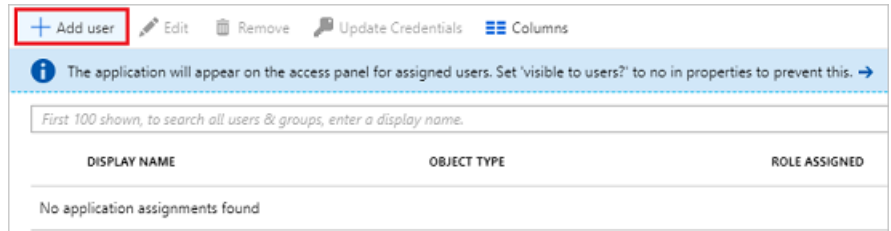


## To assign users to single sign-on application in Azure Active Directory

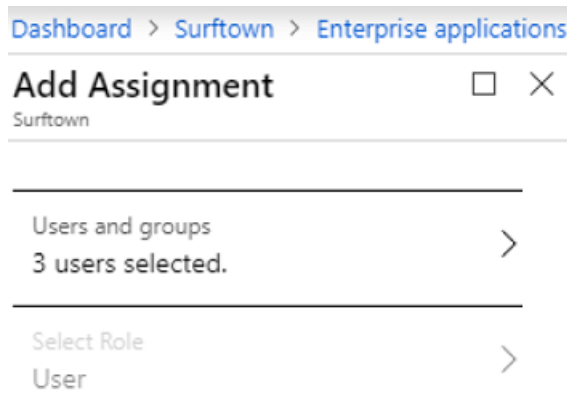
- 1 Sign in to your Azure account, and select **Enterprise applications**.
- 2 Search for and select the application you have created for SSO.
- 3 Under **Manage**, select **Users and groups**.



- 4 Click **+ Add user** to open the **Add Assignment** window.

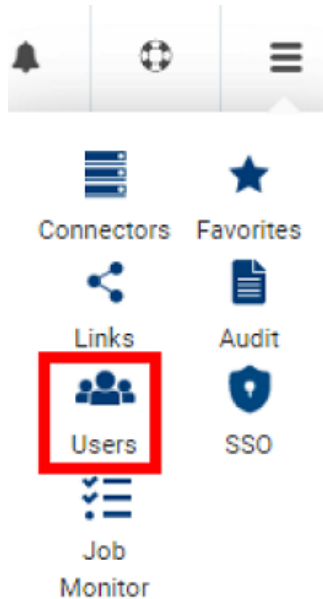


- 5 Select **Users** and groups **None Selected**.
- 6 Search for the users you want to be able to use SSO in the field provided, and then select them from the list below. Here you must also include the **Backup Administrator** (the Global Admin who is setting up SSO) as well as all other users for whom you want to enable SSO.
- 7 When all desired users appear under **Selected members**, click **Select**.
- 8 The number of users you selected will appear under **Users and groups**.



- 9 Click **Assign**.







- 10 Navigate to your SaaS Backup User Admin account. Expand the menu and select **Users**.



---

**Note:** In the list of users, make sure that all the users that were assigned to the Azure SSO application exist in SaaS Backup. If there is no such user, then create a user with the same name and email address as the user in Office 365.

SaaS Backup follows case sensitivity rule, thus, while creating a new user in SaaS Backup, ensure that the email address is in the same case as the email address in the Active Directory.

User List		
	Role: User Administrator admin1 admin1@vsbtest.com Created at: 2019-07-06 17:02:21 Expire time: 2020-06-06 17:02:21	 
	Role: SSO Admin admin sso_admin@vsbtest.com Created at: 2019-06-06 19:37:49 Expire time: Never	 

### How the users can sign in with SSO?

#### To use SSO for signing in to SaaS Backup

- 1 Log in to the SaaS Backup console. Add the region identifier to the URL in the following format:
  - Europe, Middle East, Africa: <https://eu.saasbackup.veritas.com/v-signin.html>
  - Americas: <https://us.saasbackup.veritas.com/v-signin.html>
  - Asia, Pacific, Japan: <https://ap.saasbackup.veritas.com/v-signin.html>
- 2 At the time of signing in to user's Veritas SaaS Backup account, enter only user email address.

---

**Note:** Users do not require to provide their password.

---

- 3 Click Sign in to redirect to the Microsoft page, and sign in using the Microsoft login credentials.

---

**Note:** After successful signing in, the users are redirected to their Veritas SaaS Backup account. The Veritas SaaS Backup user account case sensitivity must match the SSO configuration. If the format is incorrect, an error from SSO will be displayed noting that the user was not found.

---

# Configuring single sign-on using ADFS

This section explains how to configure Active Directory Federation Service (ADFS) to work together with Office 365. It involves the following procedures:

- Configuring the identity provider

---

**Note:** If you are using Azure AD skip this section.

---

- Configuring SaaS Backup

## Configuring the identity provider

Administrators must configure the identity provider to prepare for SSO access. During this configuration, the administrator registers Veritas as a trusted party. Use Open ADFS 2.0 to configure the identity provider.

### To configure the identity provider

- 1 Open ADFS 2.0 management console, and click **Add new** relying party trust to start configuration wizard.





- 2 In **Select Data Source**, select **Enter data** about the relying party manually, and click **Next**.

The screenshot shows the 'Add Relying Party Trust Wizard' window, specifically the 'Select Data Source' step. On the left, a 'Steps' pane lists the wizard's progression: Welcome, Select Data Source (current), Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains three radio button options for selecting data source information. The first option, 'Import data about the relying party published online or on a local network', includes a text field for 'Federation metadata address (host name or URL)' with an example 'fs.contoso.com or https://www.contoso.com/app'. The second option, 'Import data about the relying party from a file', includes a text field for 'Federation metadata file location' and a 'Browse...' button. The third option, 'Enter data about the relying party manually', is selected and underlined in red. Below the options are navigation buttons: '< Previous', 'Next >', 'Cancel', and 'Help'.

**Add Relying Party Trust Wizard**

**Select Data Source**

**Steps**

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this relying party:

☐ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

☐ Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

Browse...

☒ Enter data about the relying party manually

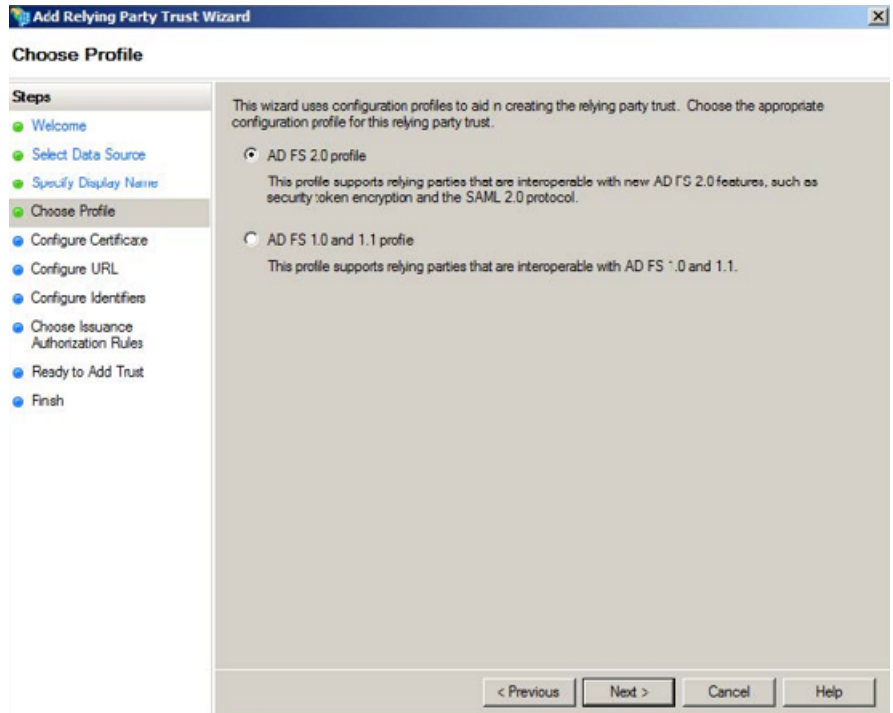
Use this option to manually input the necessary data about this relying party organization.

< Previous Next > Cancel Help

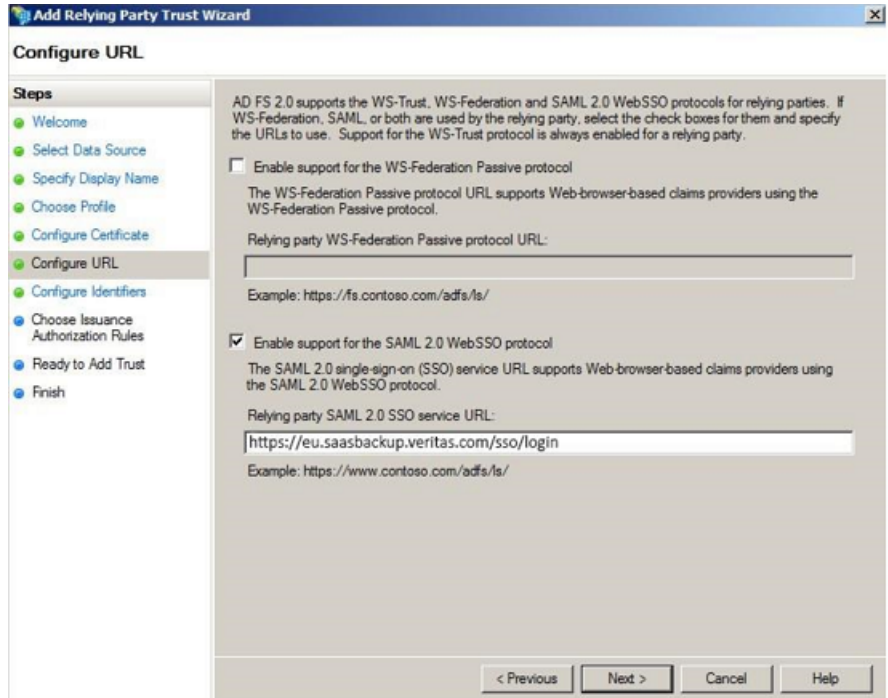
- 3 In **Specify Display Name**, type **Veritas** as display name of the relying party, and click **Next**.

The screenshot shows the 'Add Relying Party Trust Wizard' window. The title bar reads 'Add Relying Party Trust Wizard'. The main heading is 'Specify Display Name'. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source, Specify Display Name (highlighted with a green dot), Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains the instruction 'Type the display name and any optional notes for this relying party.' Below this, there is a 'Display name:' label followed by a text box containing the word 'Veritas'. Below the text box is a 'Notes:' label followed by a large, empty text area. At the bottom right, there are four buttons: '< Previous', 'Next >', 'Cancel', and 'Help'.

- 4 In **Choose Profile**, select ADFS 2.0 profile, but do not specify certificate. Click **Next**.



- 5 In **Configure URL**, select the **Enable support for the SAML 2.0 Web SSO protocol** check-box.

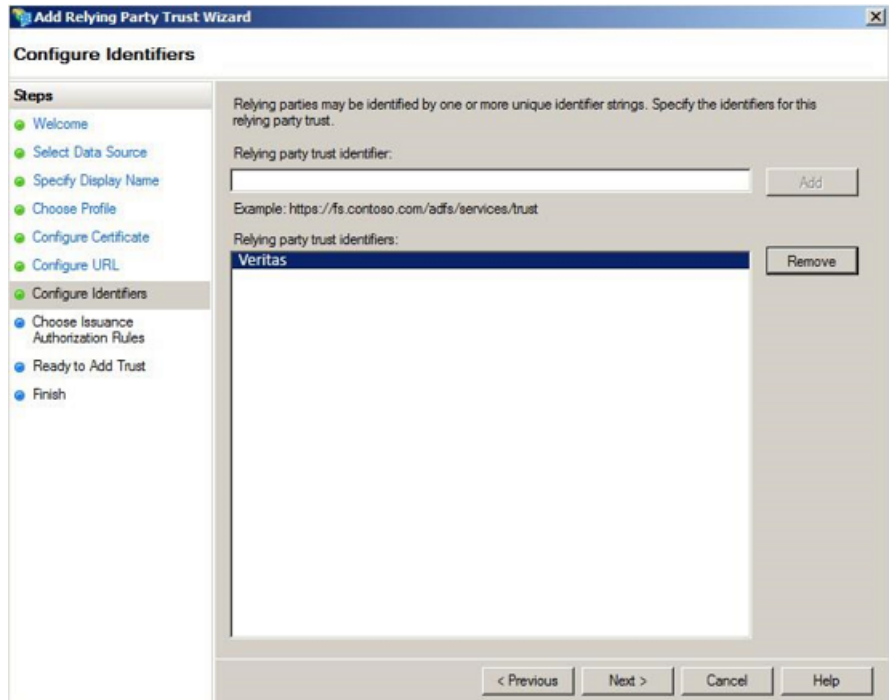


Add the following URL for relying party SAML 2.0 SSO service URL:

- Veritas users in Europe, Middle East, Africa: <https://eu.saasbackup.veritas.com/sso/login>
- Veritas users in Americas: <https://us.saasbackup.veritas.com/sso/login>
- Veritas users in Asia, Pacific, Japan: <https://ap.saasbackup.veritas.com/sso/login>

Click **Next**.

- 6** In **Configure Identifiers**, add **Veritas** as trust identifier.

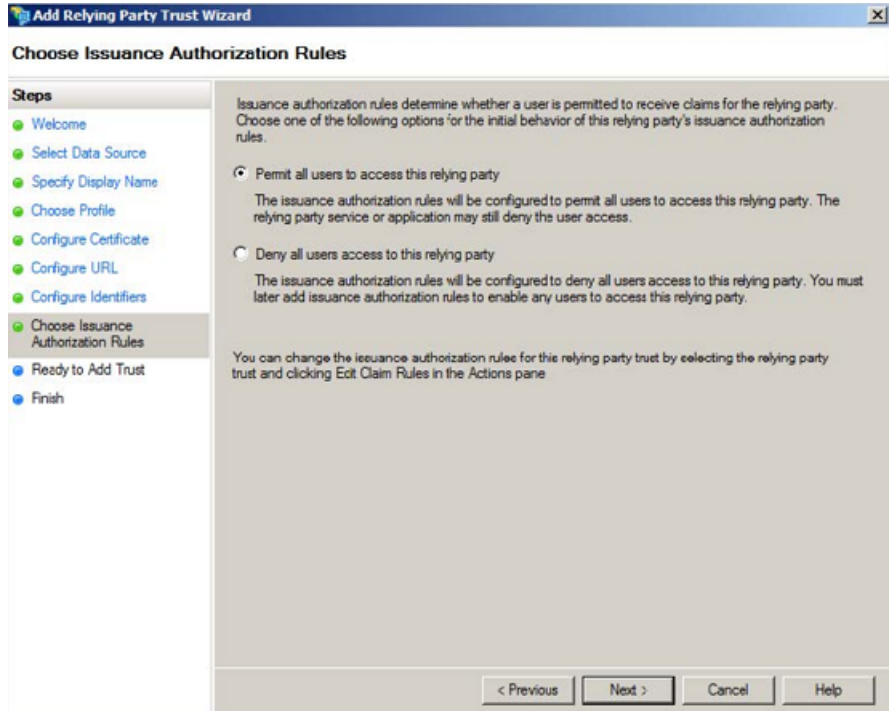


Add the following URL for relying party identifiers:

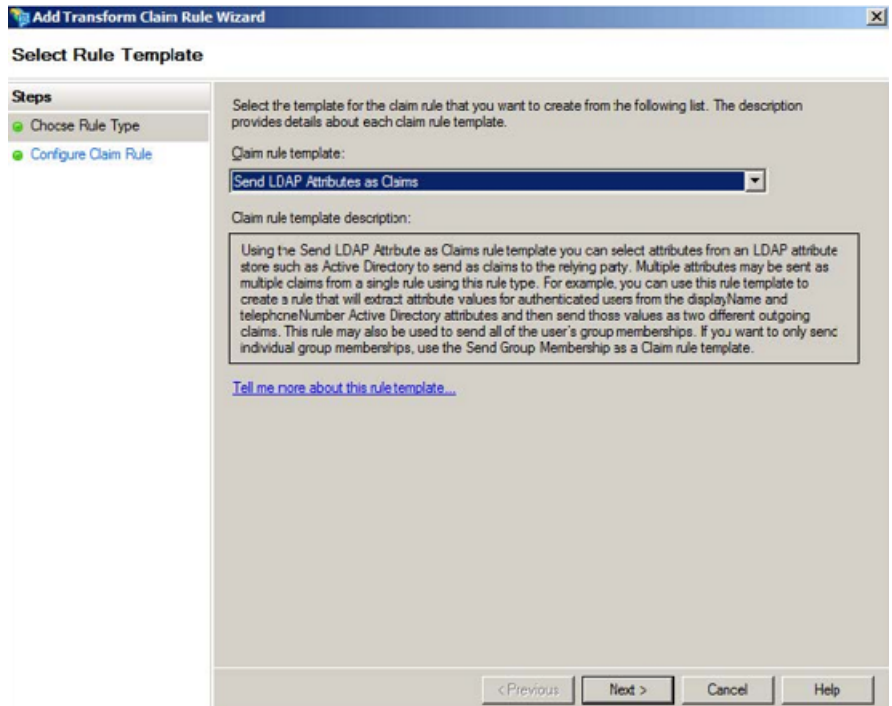
- Veritas users in Europe, Middle East, Africa:  
<https://eu.saasbackup.veritas.com/sso/metadata>
- Veritas users in Americas: <https://us.saasbackup.veritas.com/sso/metadata>
- Veritas users in Asia, Pacific, Japan:  
<https://ap.saasbackup.veritas.com/sso/metadata>

Click **Next**.

- 7 In **Choose Insurance Authorization Rules**, select the **Permit all users to access this (Veritas) relying party** check-box, and click **Next**.



- 8 In **Select Rule Template**, select the **Send LDAP Attributes as Claims**, and click **Next**.



- 9 In **Configure Rule**, specify the following, and Click **Finish**, and click **Finish**.

**Add Transform Claim Rule Wizard**

**Configure Rule**

**Steps**

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

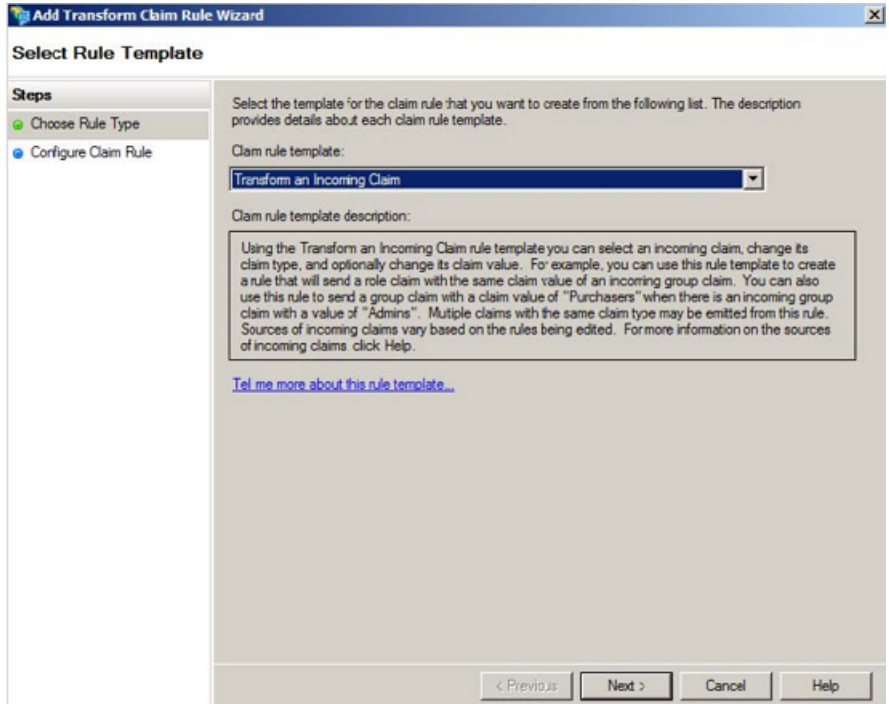
	LDAP Attribute	Outgoing Claim Type
▶	E-Mail-Addresses	E-Mail Address
*		

< Previous   Finish   Cancel   Help

- Specify the claim rule name as **Send email**.
- Specify the attribute store as **Active Directory**.
- Map E-Mail-Addresses LDAP attribute to E-Mail Address outgoing claim type.



- 10 In **Select Rule Template**, select **Transform an Incoming Claim**, and click **Next**.



- 11 In **Configure Rule**, specify the following, and click **Finish**.

**Add Transform Claim Rule Wizard**

**Configure Rule**

**Steps**

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Rule template: Transform an Incoming Claim

Incoming claim type:

Incoming name ID format:

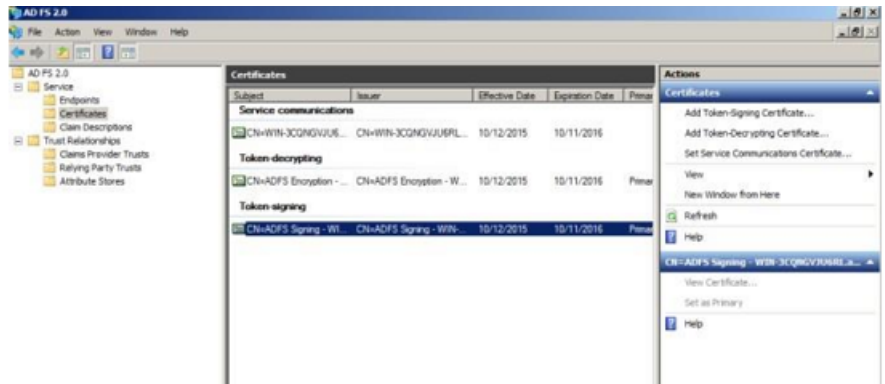
Outgoing claim type:

Outgoing name ID format:

☒ Pass through all claim values  
☐ Replace an incoming claim value with a different outgoing claim value  
 Incoming claim value:   
 Outgoing claim value:    
☐ Replace incoming email suffix claims with a new email suffix  
 New e-mail suffix:   
 Example: fabrikam.com

- Specify the rule name as **Transform email to NameID**.
- Specify the incoming claim type as **E-Mail Address**.
- Specify the outgoing claim type as **Name ID**.
- Specify the outgoing Name ID format as **Email**.

- 12 Save ADFS token-signing certificate into file in .pem format.



- 13 Use the content of this file as a certificate of your identity provider in Veritas SSO configuration.

```

1  -----BEGIN CERTIFICATE-----
2  MIIC9DCCAdygAwIBAgIQTCgV2xQQLicFVztaSucaujANBgkqhkiG9w0BAQsFADA2
3  MTQwMgYDVQQDEyBtBREZTIFNpZ25pbmcgLSBXSU4tM0NRTkdWSlU2UkwuYwR0ZXN0
4  LmxvY2FzMB4XDTE1MTAxMjA4NDYzM1cXDTE2MTAxMTA4NDYzM1owNjE0MDIGA1UE
5  AxMrQURGUyBtWduaw5nIC0gV010LNDUU5HVkpVNlJMLmFkdGVzZC5sb2NhbDCC
6  ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBBAKvKFoHpmXsHvZ0GnmZoBBtg
7  W8NDZR7+06CsQ0UyFcX89X4QsX0pcstNAopFwgl700LW9d6Im3egplvdNX0w+IAG
8  kztqtAnyF7SA0IM3Bm6GcJo5xepJS/h7NG0/7ysnIP20R8bVIpBcAl+LhPj5rAvJ
9  2flzqDy+I66Gh6upMZtvmFstQHsPovTQpdyYqyGU6qCRzxd4J5sUwvm5BOCCakc4
10 KQn9b5Um8WCBBiZ2R0wvi6f1cD5zciWgUNMNBxonac6tgTX8m9jBRMHQN9Ydu9mq
11 wpNpkiQMGH1qYs9Cha60Z2lpWQpdzze0+EIPtjdqtWiwj4RF0TWZV9J2nIL0vMLC
12 AwEAATANBgkqhkiG9w0BAQsFAAOCAQEAN2aIhHQ/Z6wvQ2Z3j0YWFAMzN6H0loZA
13 Z09H60DIUmdvyRynZVb5/EiLRtFcoG31JmXdagAvWbNqrvZdtFicPfn6lygq7Q5Q
14 jo+catlRfFoyWvVjV2oH1znv1bof/FMMU+fwgP7jYn2xwR0bVF3v/tAmj1zEzEAlt
15 TzGYh1yKlvUrHiIZDUJre1+BjIRjKA7jh9nVBGFQC6CK3M/MLUeDOHKHBpc1kUQF
16 m82JT1aOM73bFiugpT89smsn0aV0w+1gPJdLk0TKvbw0tIkTEPwLwK7V3Cy3vFrE
17 1k9VKfgLKjE4inE7B6n+8pmiAgchtYN723vEfMqQ99LFRcaZAB5cSA==
18  -----END CERTIFICATE-----
19

```

---

**Note:** Copy the certificate excluding the begin/end markers in the certificate.

---

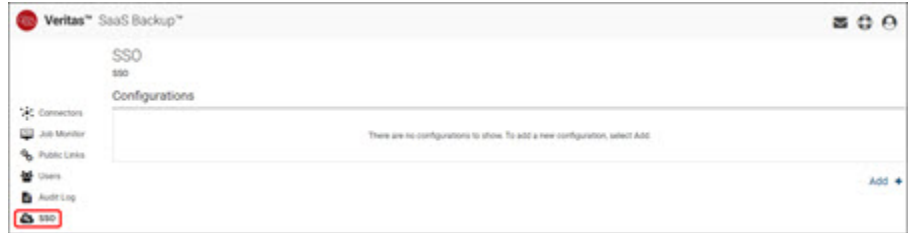
## Configuring Veritas SaaS Backup

Note: Sign-in URL of AD FS 2.0 server is <https://<adfs-server-name>/adfs/ls>

# Configuring single sign-on in SaaS Backup

To create a single sign-on administrator profile

- 1 Sign in to SaaS Backup as a master administrator.
- 2 Click the **SSO** icon on the left Menu bar.



- 3 On the **Configurations** page, click **Add** in the lower-right corner.


---

**Note:** If you set up your single sign-on inappropriately, it may result in locking yourself and everyone else out of the account. Before completing the single sign-on setup, ensure that a single sign-on Admin user is created, who can prevent you from locking out.

---

## SSO

SSO > New configuration



Misconfiguring your SSO setup may result in locking yourself and everyone else out of the account. Please make sure an SSO Admin user has been created before you finish the SSO setup.

### SSO Configuration

Name

IDP URL

Certificate

☒ Enabled

☒ Optional

Save

Cancel

#### 4 On the **SSO Configuration Strings** page, provide the following information:

Fields	Description
Name	<p>Provide a name and select <b>Apply</b>.</p> <p>To undo the unsaved changes in this field, click <b>Reset</b>.</p>
IDP URL	<p>Provide the Identity Provider URL and select <b>Apply</b>.</p> <p>IDP URL validates the credentials. You can obtain this IDP URL from Azure AD. In Azure AD, IDP URL is known as Login URL or SAML single sign-on service URL.</p> <p>During this process, you will be prompted to provide files and URLs that correspond to Azure Active Directory. When prompted, use the files and URLs shown below:</p> <ul style="list-style-type: none"> <li><b>SAML Single Sign-On Service URL:</b>  <a href="https://login.microsoftonline.com/6bc17c1c-6785-4b1e-90d4-11a724ccc3f/saml2">https://login.microsoftonline.com/6bc17c1c-6785-4b1e-90d4-11a724ccc3f/saml2</a></li> </ul> <p>To undo the unsaved changes in this field, click <b>Reset</b>.</p>
Certificate	<p>The Certificate (Base 64) is the certificate you downloaded when you configured SSO with Azure AD Premium.</p>

```

1 -----BEGIN CERTIFICATE-----
2 MIICDCCAdigAwIBAgIQNAP13FJ/maNMIQm11va6TANBgkqhkiG9w0BAQsFADAO
3 KzlNaNRYb3NvZnQxcmUgRmVxZXJhdGVkIENNTTYyBDZXJ0aWZpY2FOZTAE
4 MjdaFw0yMTEyMTIwOTE1MjdaMDQxOTQxMjYyMTEyMTIwOTE1MjdaMDQxOTQx
5 MjdaFw0yMTEyMTIwOTE1MjdaMDQxOTQxMjYyMTEyMTIwOTE1MjdaMDQxOTQx
6 MjdaFw0yMTEyMTIwOTE1MjdaMDQxOTQxMjYyMTEyMTIwOTE1MjdaMDQxOTQx
7 MjdaFw0yMTEyMTIwOTE1MjdaMDQxOTQxMjYyMTEyMTIwOTE1MjdaMDQxOTQx
8 MjdaFw0yMTEyMTIwOTE1MjdaMDQxOTQxMjYyMTEyMTIwOTE1MjdaMDQxOTQx
9 MjdaFw0yMTEyMTIwOTE1MjdaMDQxOTQxMjYyMTEyMTIwOTE1MjdaMDQxOTQx
10 MjdaFw0yMTEyMTIwOTE1MjdaMDQxOTQxMjYyMTEyMTIwOTE1MjdaMDQxOTQx
11 MjdaFw0yMTEyMTIwOTE1MjdaMDQxOTQxMjYyMTEyMTIwOTE1MjdaMDQxOTQx
12 MjdaFw0yMTEyMTIwOTE1MjdaMDQxOTQxMjYyMTEyMTIwOTE1MjdaMDQxOTQx
13 MjdaFw0yMTEyMTIwOTE1MjdaMDQxOTQxMjYyMTEyMTIwOTE1MjdaMDQxOTQx
14 MjdaFw0yMTEyMTIwOTE1MjdaMDQxOTQxMjYyMTEyMTIwOTE1MjdaMDQxOTQx
15 MjdaFw0yMTEyMTIwOTE1MjdaMDQxOTQxMjYyMTEyMTIwOTE1MjdaMDQxOTQx
16 MjdaFw0yMTEyMTIwOTE1MjdaMDQxOTQxMjYyMTEyMTIwOTE1MjdaMDQxOTQx
17 -----END CERTIFICATE-----

```

Copy the text, excluding the BEGIN and END markers, as shown below. Paste it in the Certificate field.

Enabled	Select the <b>Enabled</b> check box to make single sign-on active for the master administrator and all other sub-users created by the master administrator.
Optional	Select the <b>Optional</b> check box if you want the master administrator and sub-users to have the option to sign in with either single sign-on or with the SaaS Backup credentials.

**5** Click **Save**.



# Managing cloud services for Dynamics 365

This chapter includes the following topics:

- [Dynamics 365 cloud connectors overview](#)
- [Protected Dynamics 365 data types](#)
- [Adding Dynamics 365 cloud connectors](#)
- [Deleting Office 365 connectors](#)
- [Restoring files and folders from Dynamics 365 cloud connectors](#)
- [Monitoring jobs of Dynamics 365 cloud connectors](#)
- [Sharing files and folders of Dynamics 365 cloud connectors](#)
- [Downloading files and folders on Dynamics 365 cloud connector](#)

## Dynamics 365 cloud connectors overview

Dynamics 365 is an enterprise resource planning (ERP) and customer relationship management (CRM) applications developed by Microsoft. Enterprises that use Dynamics 365 ERP and CRM for their business keep their crucial business data on this platform.

SaaS Backup provides a complete, flexible data protection solution for the Dynamics 365 platform. SaaS Backup lets you back up, restore backup, download data, share data, and monitor your Dynamics 365 -specific jobs.

To use SaaS Backup with Dynamics 365, need to have an Office 365 Global administrator account with a proper Dynamics license.

You must use the incognito (private) mode of supported browser to avoid cached credentials.

## Protected Dynamics 365 data types

SaaS Backup backs up the Dynamics 365 entities and the corresponding metadata. You can protect metadata of the following Dynamic 365 applications:

- Dynamics 365 for Customer Service
- Dynamics 365 for Field Service
- Dynamics 365 for Marketing
- Dynamics 365 for Project Service Automation
- Dynamics 365 for Sales

---

**Note:** SaaS Backup does not currently support Dynamics 365 for Talent.

---

Data of these applications is structured as follows:

- Dynamics 365 Connector
  - Instances
    - Data
      - Entities
        - Records
    - Meta
      - Entity meta
      - Entity attribute meta
      - Entity relationship 1:N meta
      - Entity relationship N:1 meta
      - Entity relationship N:N meta

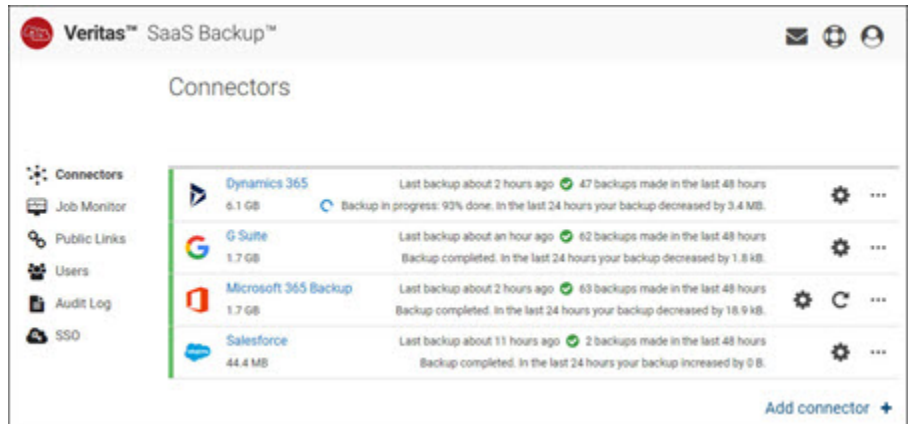
## Adding Dynamics 365 cloud connectors

A Dynamics 365 cloud connector represents the backup of a Dynamics 365 cloud service. You need to create a Dynamics 365 cloud connector to back up a Dynamics 365 cloud service. To manage the Dynamics 365 cloud services, you need to have an Office 365 Global administrator account with a proper Dynamics license.

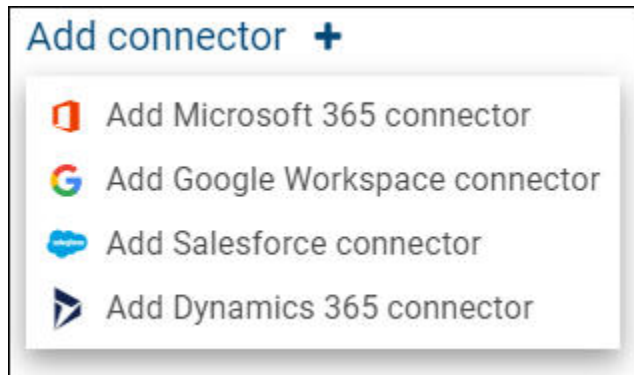
## To add a Dynamics 365 cloud connector

- 1 Sign in to SaaS Backup.

**Note:** The **Connector** page appears by default. If you are on working on any other page (Links, Job Monitor, Audit, and so on), you can click **Connectors** from the menu icon. This page lets you view a list of connectors, the last updated date, side of data on connector, and the action icons.

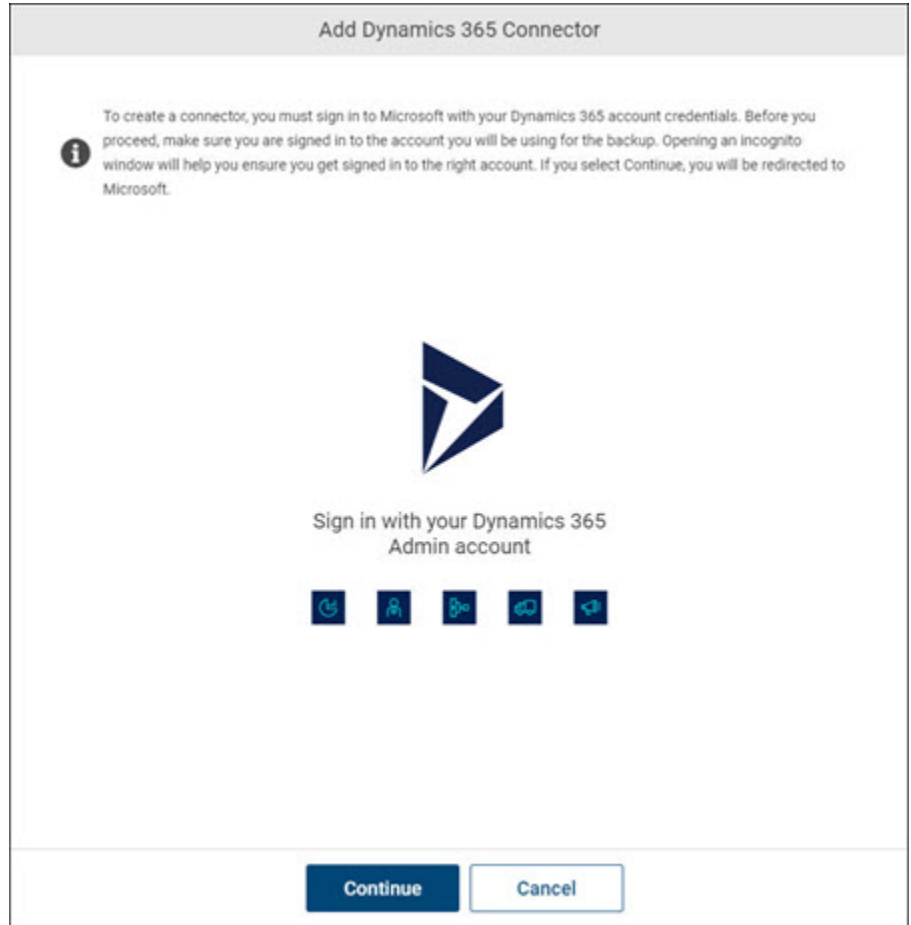


- 2 On the **Connectors** page, click **Add**.



**3** Click **Dynamics 365**.

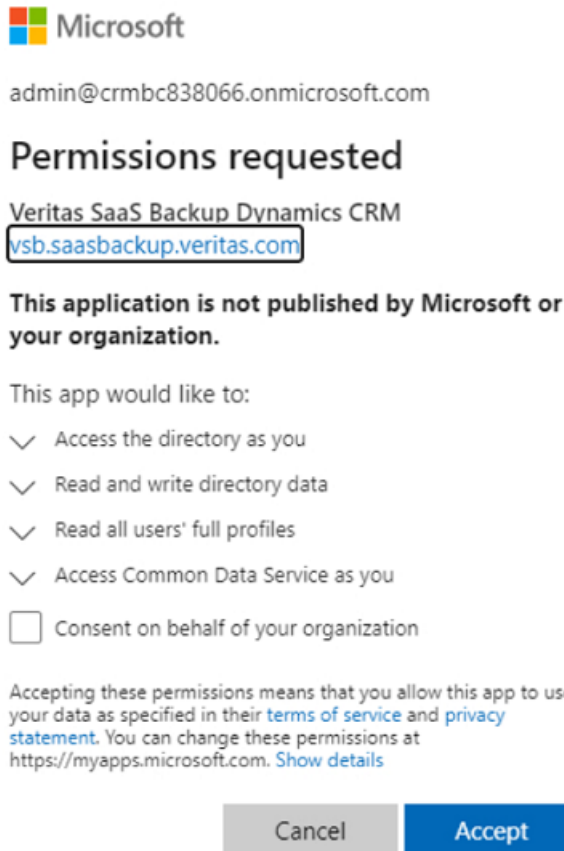
The **Dynamics 365** setup dialog box appears.



**4** Enter Dynamics 365 connector name, and click **Sign in with Dynamics 365 account**.

the application redirects you to the **Microsoft sign in** page

- 5 Enter your credentials for your Dynamics 365 account (the Office 365 Global administrator account you use to sign into Dynamics), and click **Sign In**.



- 6 When you are prompted for permission to access files, review the list of permissions, and click **Accept**.

---

**Note:** The application redirects you to SaaS Backup **Connectors** page. SaaS Backup schedules the first backup. You can follow the progress of your backup by hovering over **Synchronizing** under **Last Update**.

---

# Deleting Office 365 connectors

You can delete an expired or outdated Office 365 cloud connector. Ensure that you have permissions to delete a cloud connector.

## To delete an Office 365 cloud connector

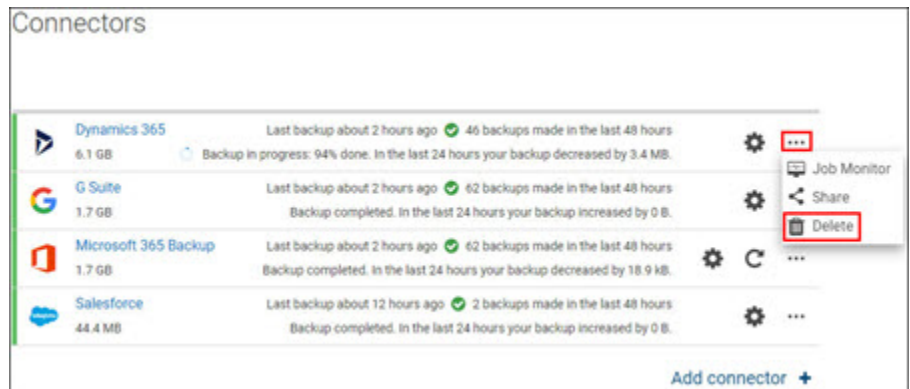
- 1 Sign in to SaaS Backup.

---

### Note:

The **Connector** page appears by default. If you are on working on any other page (Job Monitor, Public Links, Users, Audit Log, SSO), you can click **Connectors** from the menu icon. This page lets you view a list of connectors, the last updated date, side of data on connector, and the action icons.

---



- 2 Search for and select the Office 365 cloud connector you want to delete and click the **More Options** click the **Delete** icon.

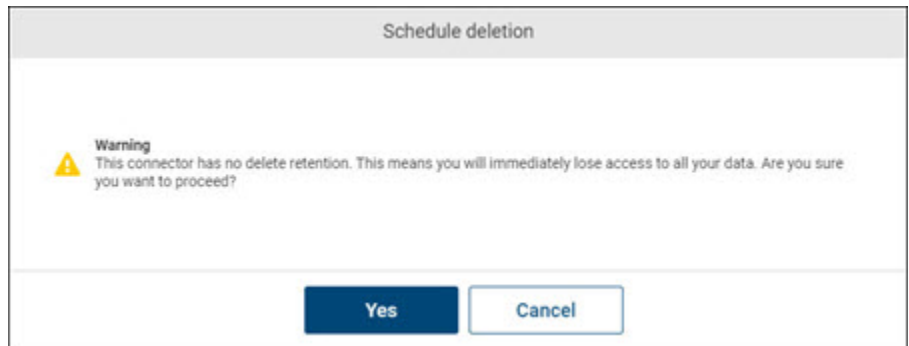
- 3 The application prompts you to confirm that you want to perform the operation.

---

**Note:** SaaS Backup schedules the deletion of the selected connector. The connector is deleted after the retention period is over. If you remove a Microsoft 365 connector, entire data that is associated with the connector is deleted. You cannot revert the changes.

---

- 4 Click **Yes** to complete the operation or click **Cancel** to cancel it.



## Restoring files and folders from Dynamics 365 cloud connectors

SaaS Backup incrementally captures snapshots of cloud connectors. You can restore the indexed or the complete history snapshots of the cloud connector. If required, you can restore an individual file or a folder. When you restore files and folders, it is restored to its original location. If the file or folder with the same name already exists in the location, the application overwrites it.

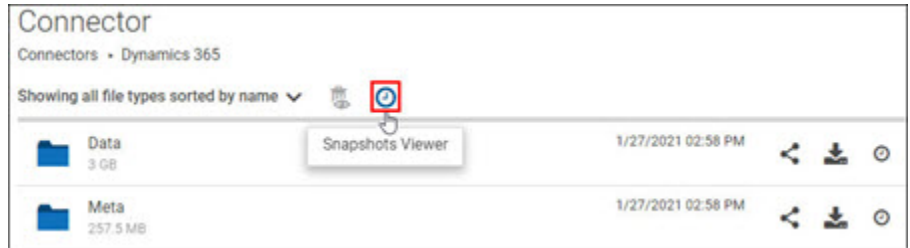
---

**Note:** If you restore the files and folders while browsing, application restores the file that you are viewing in the interface. Before restoring the data, ensure that you have selected the correct snapshot. If you have not selected any snapshot, the application restores the latest version of files and folders.

---

### To restore the indexed or the complete history snapshot of a connector

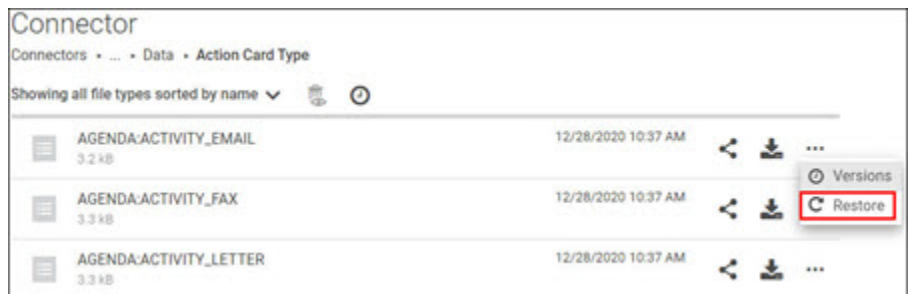
- 1 Open the connector to view files and folders of which you want to restore a snapshot.



- 2 Click the **Snapshots Viewer** icon, and select a point in time.
- 3 Select the point in time from which you want to restore the data. use one of the following options:
  - To restore the indexed snapshot, click the **Indexed Snapshot** icon.
  - To restore the complete snapshot, click the **Complete Snapshot** icon.

### To restore an individual file or a folder

- 1 Open the connector to view files and folders of which you want to restore a snapshot.
- 2 Navigate to the file or a folder you want to restore.



- 3 Click the **More Options** icon, and select **Restore**.



- 4 The application prompts you to select the restore method and afterwards click **Next**.

Restore

1 Restore 2 Summary

**i** Restoring only this record will restore the selected record and no related records.

To restore a record we need to process metafiles. This will result in a number of files being restored. Are you sure you want to restore **AGENDA:ACTIVITY\_EMAIL?**

Select method:

☒ Restore only this record

☐ Also restore related records

Next Cancel

5 Review the summary and confirm the restore.

Restore

1

Restore

2

Summary

i

Restoring only this record will restore the selected record and no related records.

Restore summary

- Selected method: Restore only this record
- Record to be restored: AGENDA:ACTIVITY\_EMAIL
- Restore location: /Dynamics 365/Keepit A/S/Data/Action Card Type

Back

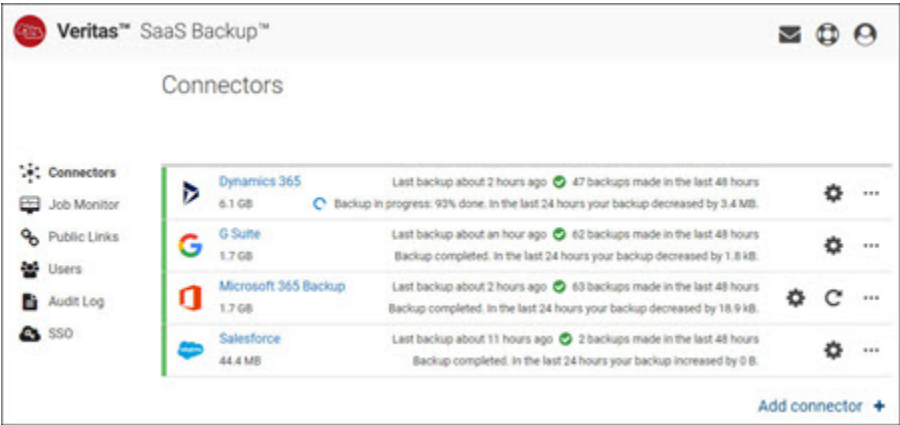
Confirm

Cancel

# Monitoring jobs of Dynamics 365 cloud connectors

To monitor backup and restoring jobs of Dynamics 365 cloud connectors

- 1
- Select the Dynamics 365 connector for which you want to monitor jobs.



- 2
- Click **Job Monitor**.
- 3
- On the **Job Monitor** page, specify the following information.

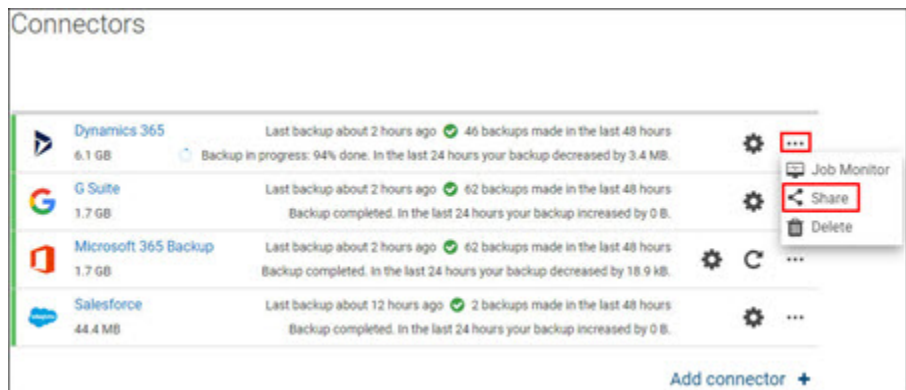
Field	Description
Connector	Displays the connector name for which you want to generate a job monitoring report.
Status	Select the job status from the drop-down list for which you want to generate a report.
Type	Select the job type from the drop-down list for which you want to generate a report.
Time span	Specify the time span of the report you want to generate a job monitoring report. Predefined options are available. However, you can customize duration of report as per your requirement.
Start date	If the time span value is selected as <b>Custom period</b> , specify the date from which you want to generate a job monitoring report.
End date	If the time span value is selected as <b>Custom period</b> , specify the date up to which you want to generate a job monitoring report.

- 4 To view the result, click **Refresh**.
- 5 To sort a column details, click the respective column header.
- 6 To further narrow down the result, type a keyword in the **Filter** field, and click the search icon.
- 7 To view the statistic of a specific item, click its **Show more** link in the **Description** column.

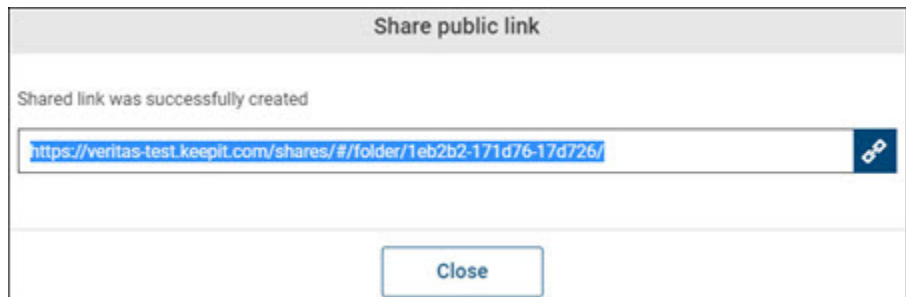
## Sharing files and folders of Dynamics 365 cloud connectors

To share files and folders of Dynamics 365 cloud connectors

- 1 Select the Dynamics 365 connector for which you want to share the data.



- 2 To share entire connector data, click **Share folder** on the **Connectors** page. The application opens the **Share public link** page.



- 3 In the **Share public link** dialog box, specify the following information:

Field	Description
Time limit public link	Select this check-box to view the <b>Set expiration time</b> field.
Set expiration time	Set the expiration time of a public share link.
Password protect public link	Select this check-box to specify the password for user to access the shared content. You need to share this password with the user via email.

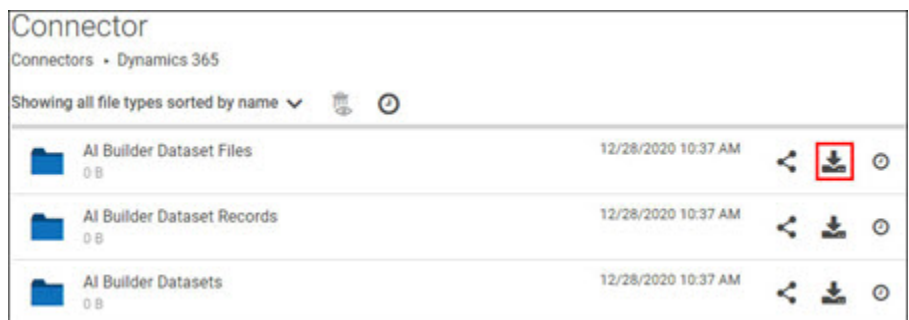
- 4 Click **Share**.  
The application opens the **Share public link** page.
- 5 Copy the link to share with the user, and click **Close** to exit this page.

## Downloading files and folders on Dynamics 365 cloud connector

You can download the entire folder with the latest data or the specific version of files and folders within it.

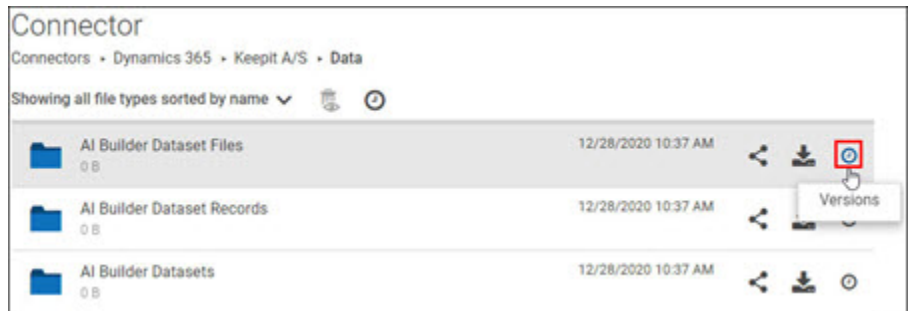
### To download the entire folder with the latest data

- 1 Select the Dynamics 365 connector, and navigate to the file or folder.
- 2 To download the entire folder with the latest data, click **Download**.

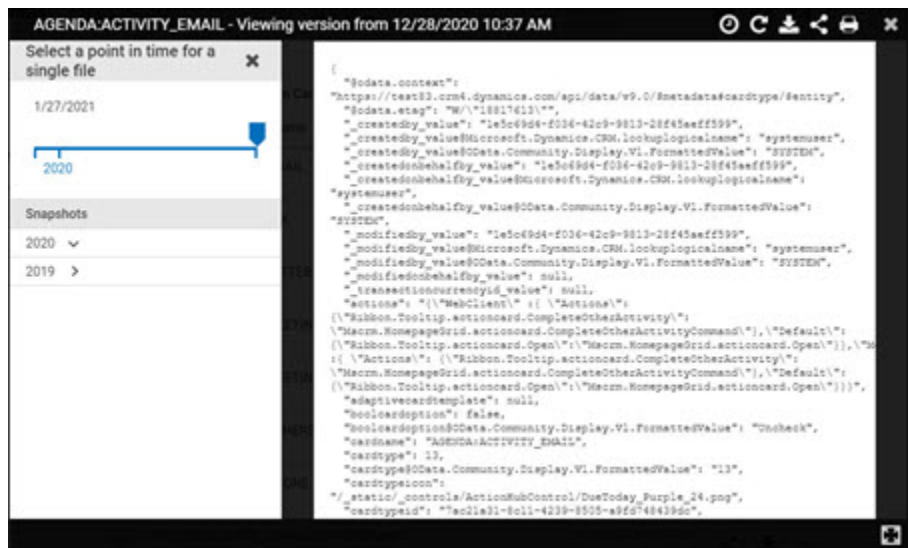


The application downloads one single file or multiple files into a .zip file on your local drive.

- 3 To download a specific snapshot (version), click **Version**.



- 4 To download the specific version of the file, click the **More options** icon and **Version**.



The application displays all the captured snapshots.

- 5 Select the required snapshot or provide a start date to search a particular point in time snapshot, and click **Restore / Download / Share / Print**.
- 6 Click the **X** icon to **Close**.

# Managing cloud services for Google Workspace

This chapter includes the following topics:

- [Google Workspace cloud connectors overview](#)
- [Protected Google Workspace components](#)
- [Preparing a Google Workspace service account for SaaS Backup](#)
- [Adding Google Workspace cloud connectors](#)
- [Deleting Google Workspace cloud connectors](#)
- [Restoring files and folders on Google Workspace cloud connectors](#)
- [Monitoring jobs of Google Workspace cloud connectors](#)
- [Sharing files and folders of Google Workspace cloud connectors](#)
- [Downloading files and folders from Google Workspace cloud connector](#)

## Google Workspace cloud connectors overview

Google Workspace is a suite of cloud computing, productivity and collaboration tools, software and products developed by Google Cloud. Enterprises that use Google Workspace for their business keep their crucial business data on this platform.

SaaS Backup provides a complete, flexible data protection solution for the Google Workspace platform. SaaS Backup lets you back up, restore backup, download data, share data, and monitor your Google Workspace-specific jobs.

To use SaaS Backup with Google Workspace, SaaS Backup needs access to Google Workspace APIs. To enable APIs, see <https://support.google.com/a/answer/60757?hl=en>

SaaS Backup supports the following Google Workspace editions:

- Basic Edition
- Business Edition
- Enterprise Edition
- Not supported: Google Workspace Legacy Free Edition

You must use the incognito (private) mode of supported browser to avoid cached credentials.

## Protected Google Workspace components

SaaS Backup backs up the following Google Workspace (G Suite) data:

- All Google shared drives and Google Sites (only classic sites, not modern ones) across the entire G Suite tenant
- Gmail, Google Drive, Calendar, and Tasks for account(s) selected for backup
- Items in the trash bin (but not in the secondary trash)

SaaS Backup does not back up:

- Contacts
- Google Workspace Notes
- Shared folders
- Email lists (groups)

For Google Drive and Gmail usage, only users that are selected in the configuration window are counted as seats.

For Google Sites, all users in the Google Workspace tenant are counted as seats.

## Preparing a Google Workspace service account for SaaS Backup

Before you back up data of a Google Workspace connector, you need to prepare a Google Workspace service account. You need to add the Veritas SaaS Backup app from the Google Workspace Marketplace.



## To prepare a Google Workspace service account for SaaS Backup

- 1 Log in to your Google Admin account.



### Apps

Manage apps and their settings

- 2 On the home page, select **Apps**.

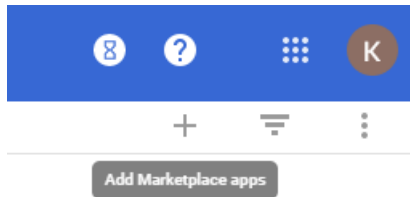


7

### Marketplace apps

Add and manage third-party apps

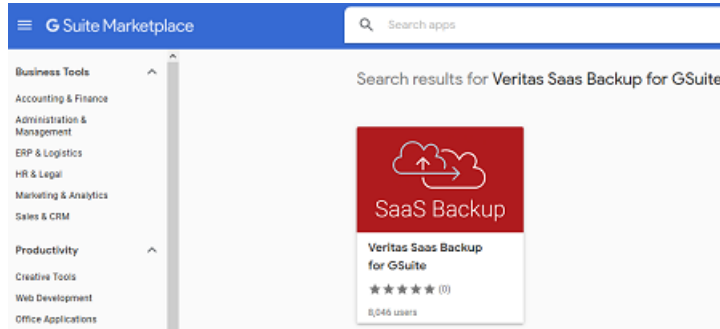
- 3 Select **Marketplace apps**.



- 4 To add a new app, select the **Add** icon.



- 5 Enter **Veritas SaaS Backup for GSuite** in the search box to find the app.
- 6 Click **Install**, and follow the on-screen instructions.




---

**Note:** To configure backup, it is necessary to use an administrator account that has access to all data across all accounts.

---

## Adding Google Workspace cloud connectors

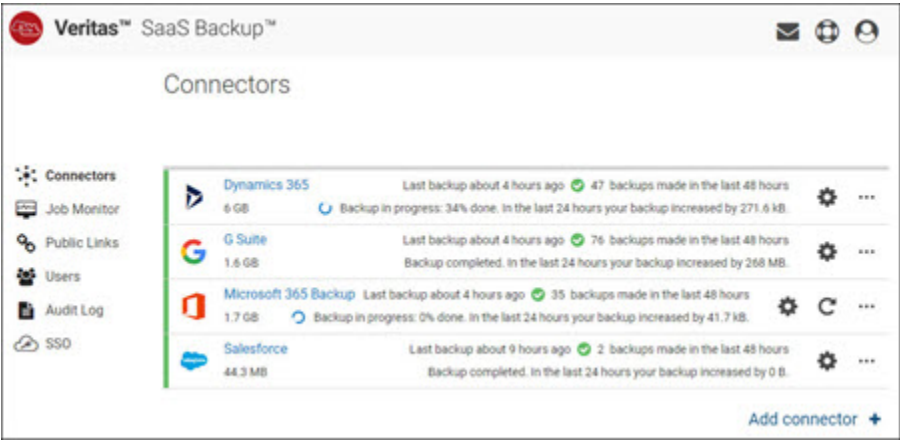
A Google Workspace cloud connector represents the backup of a Google Workspace cloud service. You need to create a Google Workspace cloud connector to back up a Google Workspace cloud service. To manage the Google Workspace cloud services, you need valid credentials.

Ensure that you have access to the Google Workspace APIs and a user account with permissions to access all the data on your Google Workspace agent.

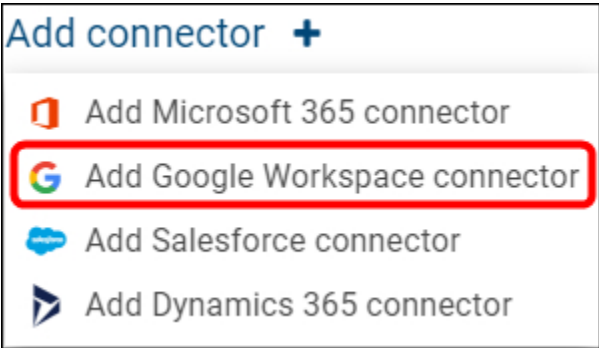
To add a Google Workspace cloud connector

- 1 Sign in to SaaS Backup.

**Note:** The **Connector** page appears by default. If you are on working on any other page (Links, Job Monitor, Audit, and so on), you can click **Connectors** from the menu icon. This page lets you view a list of connectors, the last updated date, side of data on connector, and the action icons.

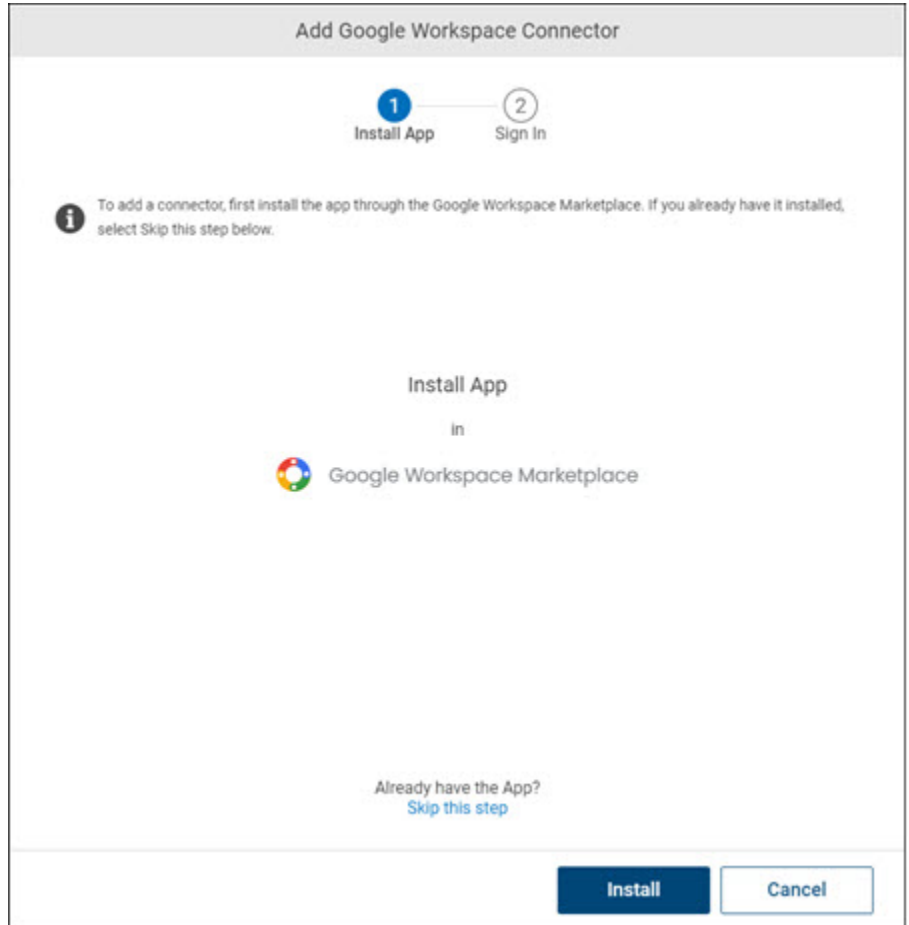


- 2 On the **Connectors** page, click **Add**.



3 Click **Google Workspace**.

The **Create new Google Workspace connector** dialog box appears.



- 4 If you have not already installed the Veritas SaaS Backup app from the Google Workspace Marketplace, click **Google Workspace Marketplace** to download the app.
- 5 In the **Identify your Google Workspace backup** field, type a name of a Google Workspace cloud connector.
- 6 Click **Sign in with Google account**.
- 7 Sign into your Google account, and follow the steps on the screen.
- 8 On the **Edit Device** dialog box, do one of the following:

- To select individual users to back up, select the check-box next to the names of the users.
- To enable new users to be added to backups automatically, select **Auto add new users to Google Workspace** backup.

9 Click **Save**.

## Deleting Google Workspace cloud connectors

You can delete an expired or outdated Google Workspace cloud connector. Ensure that you have permissions to delete a cloud connector.

### To delete a Google Workspace cloud connector

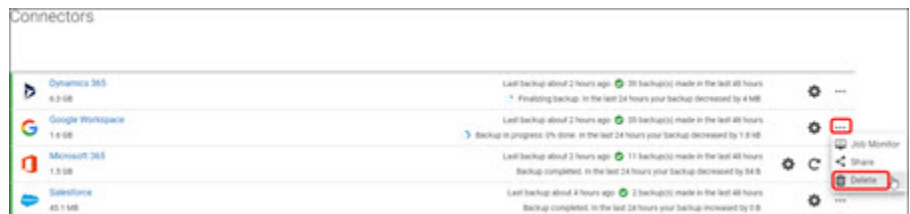
1 Sign in to SaaS Backup.

---

#### Note:

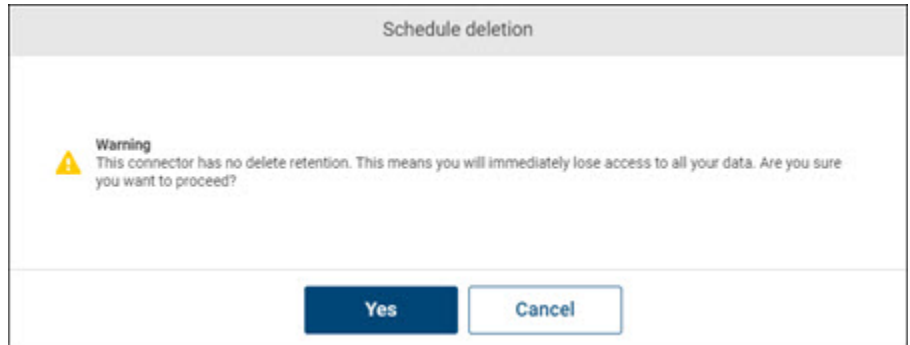
The **Connector** page appears by default. If you are on working on any other page (Links, Job Monitor, Audit, and so on), you can click **Connectors** from the menu icon. This page lets you view a list of connectors, the last updated date, side of data on connector, and the action icons.

---



2 Search for and select the Google Workspace cloud connector you want to delete.

- 3 Click the **More Options** icon and click the **Delete** icon.



The application prompts you to confirm that you want to perform the operation.

---

**Note:** SaaS Backup schedules the deletion of the selected connector. The connector is deleted after the retention period is over. If you remove a Google Workspace connector, entire data that is associated with the connector is deleted. You cannot revert the changes.

---

- 4 Click **Yes** to complete the operation or click **Cancel** to cancel it.

## Restoring files and folders on Google Workspace cloud connectors

You can easily restore single files and folders. The file or folder that you select is restored to its original location. If a file or folder with the same name already exists in the location, it will be overwritten.

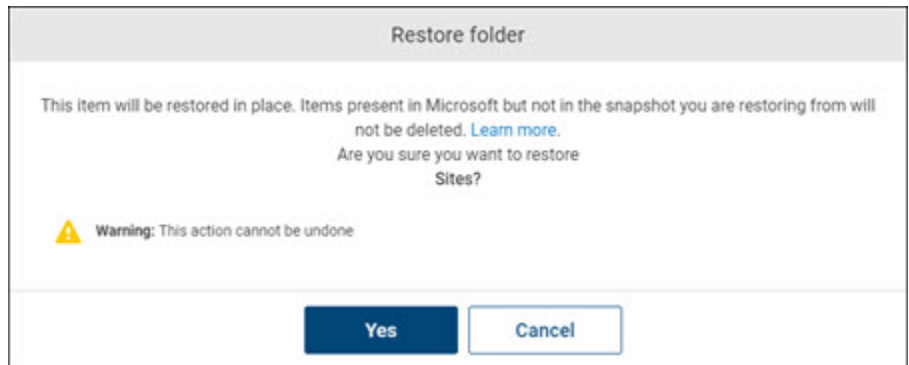
### To restore the indexed or the complete history snapshot of a connector

- 1 Browse your folders or use the search to find the folder or file you want to restore.
- 2 (Optional) If you want to restore a record from an earlier point in time, select the **Snapshots Viewer**, and then select the appropriate snapshot.

- 3 To the left of the item, select **⋮ > Restore**.



- 4 Select **Yes** to confirm the restore.




---

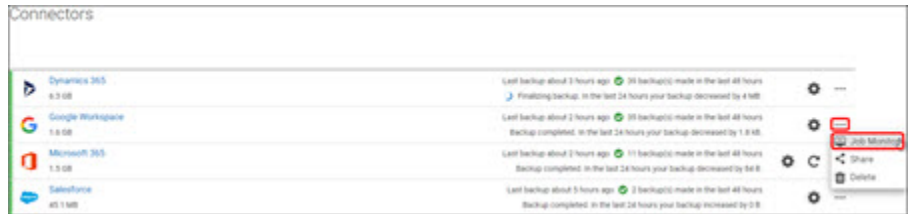
**Note:** Due to API limitations, Google Calendar tasks with an assigned time are restored to the due date without the time. This means that in the Calendar, the tasks will be applied to the whole day, rather than to a particular time.

---

# Monitoring jobs of Google Workspace cloud connectors

To monitor backup and restoring jobs of Google Workspace cloud connectors

- 1 Select the connector for which you want to monitor jobs.



- 2 Click the **More Options** icon and then click the **Job Monitor** icon.
- 3 On the **Job Monitor** page, specify the following information.

Field	Description
Connector	Displays the connector name for which you want to generate a job monitoring report.
Status	Select the job status from the drop-down list for which you want to generate a report.
Type	Select the job type from the drop-down list for which you want to generate a report.
Time span	Specify the time span of the report you want to generate a job monitoring report. Predefined options are available. However, you can customize duration of report as per your requirement.
Start date	If the time span value is selected as <b>Custom period</b> , specify the date from which you want to generate a job monitoring report.
End date	If the time span value is selected as <b>Custom period</b> , specify the date up to which you want to generate a job monitoring report.

- 4 To view the result, click **Refresh**.
- 5 To sort a column details, click the respective column header.

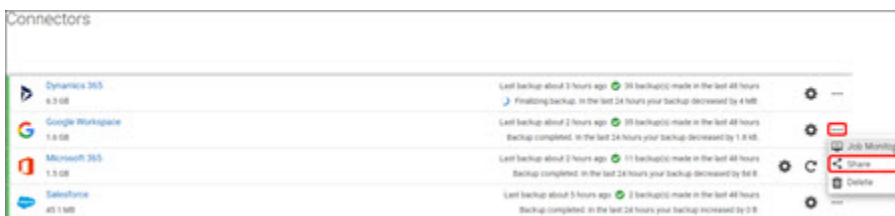


- 6 To further narrow down the result, type a keyword in the **Filter** field, and click the search icon.
- 7 To view the statistic of a specific item, click its **Show more** link in the **Description** column.

## Sharing files and folders of Google Workspace cloud connectors

To share files and folders of Google Workspace cloud connectors

- 1 Select the Google Workspace connector for which you want to share the data.



- 2 Click the **More Options** icon and then click the **Share folder** icon.  
The application opens the **Share public link** page.

The screenshot shows the 'Share public link' dialog box. It contains a message: 'Shared link was successfully created and copied to the clipboard'. Below this is a text field with the link: 'https://veritas-test.com/shares/#/folder/1e0ae3-11d963-1e25d1/'. There are two checkboxes: 'Set time limit for public link' (checked) and 'Add password to public link' (checked). Below the second checkbox is a 'Password' field. At the bottom are 'Cancel' and 'Save' buttons.

- 3 In the **Share public link** dialog box, specify the following information:

Field	Description
Time limit public link	Select this check-box to view the <b>Set expiration time</b> field.
Set expiration time	Set the expiration time of a public share link.
Password protect public link	Select this check-box to specify the password for user to access the shared content. You need to share this password with the user via email.

- 4 Click **Share**.
- The application opens the **Share public link** page.
- 5 Copy the link to share with the user, and click **Close** to exit this page.

# Downloading files and folders from Google Workspace cloud connector

To download files and folders from your Google Workspace connector

- 1 Select the connector from which you want to download a file or folder.
- 2 Find the item you want to download.
- 3 (Optional) If you want to download an older version of the item, select the **Snapshots Viewer** icon and then select an earlier snapshot.
- You will now be viewing data from that particular time.
- 4 To the right of the file or folder name, select the **Download** icon.
- The file or folder will be download to your browser’s default download location.



# Managing cloud services for Salesforce

This chapter includes the following topics:

- [Salesforce cloud connectors overview](#)
- [Protected Salesforce data types](#)
- [About campaigns and campaign members backup](#)
- [Salesforce throttling and API request usage](#)
- [Adding Salesforce cloud connectors](#)
- [Deleting Salesforce cloud connectors](#)
- [Restoring records, files, and attachments on the Salesforce cloud connector](#)
- [Monitoring backup and restoring jobs of Salesforce cloud connectors](#)
- [Sharing files and folders of Salesforce cloud connectors](#)
- [Downloading files and folders from Salesforce cloud connector](#)

## Salesforce cloud connectors overview

Salesforce is the cloud-based software-as-a-service (SaaS) platform that specializes in the customer relationship management (CRM) domain. Enterprises that use Salesforce CRM for their business keep their crucial business data on this platform.

SaaS Backup provides a complete, flexible data protection solution for the Salesforce platform. SaaS Backup lets you back up, restore backup, download data, share data, and monitor your Salesforce-specific jobs.

To use SaaS Backup with Salesforce, SaaS Backup needs access to Salesforce APIs. SaaS Backup supports the following Salesforce editions:

- Enterprise Edition
- Unlimited Edition
- Developer Edition
- Performance Edition

You must use the incognito (private) mode of supported browser to avoid cached credentials.

## Protected Salesforce data types

### Protected data types

Salesforce supports the following data types:

- **Standard and custom objects**
  - All the standard and custom objects
  - Main standard objects
    - Account
    - Campaign
    - CampaignMember
    - Case
    - Contact
    - Event
    - Lead
    - Note
    - Opportunity
    - Task
  - Other standard objects that the Salesforce API allows us to access. (The exact types of objects that are supported may vary for each organization.)
- **Files and Attachments**
  - Attachments (files attached to record from Salesforce Classic)
  - Files
  - Files attached to record from Lightning Experience

- Files uploaded to Files on Salesforce organization

---

**Note:** Files and attachments are automatically restored together with records. These data types cannot be restored on their own. You need to download and share it. To back up all your organization files and attachments, enable the **Query All Files** permission in Salesforce.

---

- **Object Metadata**

- Parent-child relationship
- Field configurations
- General information

---

**Note:** Metadata is backed up to help administrator to process records during backup and restore. Metadata is not visible to the user and cannot be restored separately.

---

## **Unprotected data types**

Salesforce do not protect the following data types:

- **Objects disabled from backup**

The following standard objects are not supported due to API limitations and have been disabled from the backup.

- AppTabMember
- CaseStatus
- ColorDefinition
- ContentDocumentLink
- ContentFolderItem
- ContentFolderMember
- ContractStatus
- DataStatistics
- DatacloudAddress
- DatacloudDandBCompany
- EntityDefinition
- EntityParticle

- FieldDefinition
- FieldSecurityClassification
- FlexQueueItem
- FlowDefinitionView
- FlowVariableView
- FlowVersionView
- IconDefinition
- IdeaComment
- ListViewChartInstance
- ObjectPermissions
- OrderStatus
- OutgoingEmail
- OutgoingEmailRelation
- OwnerChangeOptionInfo
- PartnerRole
- PicklistValueInfo
- PlatformAction
- RelationshipDomain
- RelationshipInfo
- SearchLayout
- SiteDetail
- SolutionStatus
- TaskPriority
- TaskStatus
- UserEntityAccess
- UserFieldAccess
- UserRecordAccess
- Vote
- AppDefinition
- DataType

- FormulaFunction
- FormulaFunctionAllowedType
- FormulaFunctionCategory
- OAuthToken
- Publisher
- TabDefinition
- UserAppMenuItem
- LoginHistory
- LoginGeo
- AuthSession
- DatacloudContact
- DatacloudCompany
- **Objects with API limitations**  
Standard objects that we cannot access due to unforeseen API limitations. The exact types of objects may vary for each organization.
- **Objects not queryable**  
Standard objects that are not queryable (the object's configuration gives us this information). The exact types of objects may vary for each organization.
- **Other Unsupported Items**
  - Approval processes
  - Flows
  - Workflows
  - Chatter and feeds
  - Documents
  - Reports
  - Dashboards
  - Page layouts

## About campaigns and campaign members backup

SaaS Backup backs up details of campaigns and campaign members in two different folders.

**Campaign folder**

When you open a backed-up Campaign in SaaS Backup, a .json file shows campaign details only. Though Campaign Hierarchy, Open Activities, Active History, Opportunities, and Campaign Members – except for Attachments data is backed up as a Campaign, it is found in other Objects folders.

For example, tasks under Open Activities are backed up in the Task folder, items under Opportunities are backed up in the Opportunity folder, and so on. When you restore an entire campaign, all of this are restored under your Campaign in Salesforce.

**CampaignMember folder**

In Salesforce, you can add a contact or a lead as a campaign member. It means, the contacts and the leads are duplicated. These are backed up in two objects folders - the Contacts or Leads folder and the CampaignMember folder. When you restore a campaign member from the CampaignMember folder, the item is restored to the campaign folder, and not to the Contacts or Leads folder.

The SaaS Backup application backs up members from all the campaigns in the CampaignMember folder. To restore an individual campaign member, open the CampaignMember folder, select the member you want to restore, and click Restore. To restore all members of a campaign, open the Campaign folder, select the campaign that these members are a part of.

## Salesforce throttling and API request usage

Throttling is a security mechanism that keeps a server healthy and responsive. It is called "throttling" because it limits the workload coming through the server by regulating network traffic and minimizing bandwidth congestion.

Salesforce uses throttling to manage uninterrupted operation of salesforce.com and ensure that all customers receive a quality service. If you use other applications that require API requests with salesforce, the performance of SaaS Backup may be affected. Salesforce limits the number of API requests that can be sent every day. If you reach the request limit, Salesforce stops responding for the remainder of the day. Administrator can set the percentage of APIs during configuring Salesforce connectors.



Setup Veritas for the Salesforce

Here you can set a different API limit if the default does not match your needs. For the initial backup we recommend using a higher percentage than 50%. A higher usage such as 90% or 100% will ensure that your Salesforce data will be quickly secured.

**Configure Connector**

Salesforce connector  
Salesforce

**Change number of API requests**

Your usage is set to 90%. This means the backup will stop when 10% of your total 15000 Salesforce API daily requests remain.

10% 90% 100%

? [Learn more about API requests](#)

Save Close

Using other applications that require several API requests to run with Salesforce affects the backup performance. Salesforce limits the number of API requests per day. If the configured API limit is reached, Salesforce stops responding for the remainder of that day.

## Adding Salesforce cloud connectors

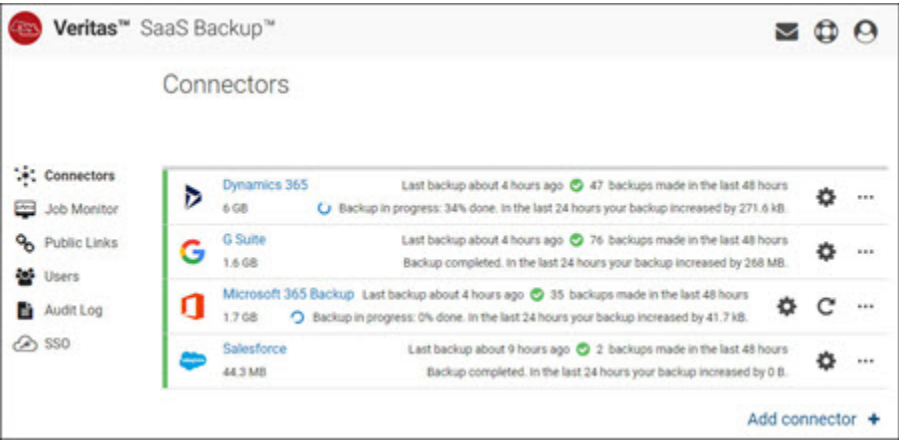
A Salesforce cloud connector represents the backup of a Salesforce cloud service. You need to create a Salesforce cloud connector to back up a Salesforce cloud service. To manage the Salesforce cloud services, you need valid credentials.

Ensure that you have access to the Salesforce APIs and a user account with permissions to access all the data on your Salesforce agent.

To add a Salesforce cloud connector


- 1
- Sign in to SaaS Backup.


**Note:** The **Connector** page appears by default. If you are on working on any other page (Links, Job Monitor, Audit, and so on), you can click **Connectors** from the menu icon. This page lets you view a list of connectors, the last updated date, side of data on connector, and the action icons.



2 On the **Connectors** page, click **Add**.

Connector Snapshot Retention

 Here you can change the retention period for your connector. Remember that decreasing the retention period may result in a loss of data.

 Change Snapshot Retention

Current connector retention period - 1 month

☐ Limit retention period

Set new retention period: 

Value

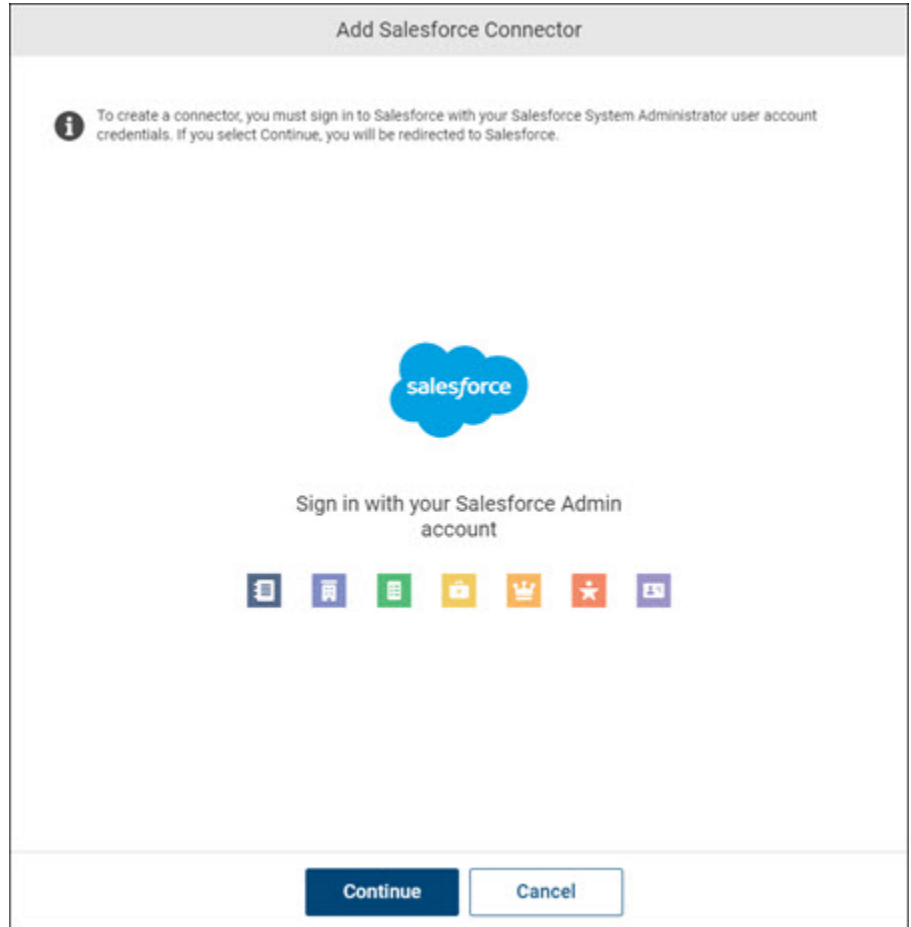
Period

Update

Cancel

**3 Click Salesforce.**

The Salesforce setup dialog box appears.



**4 Enter Salesforce connector name, and click Sign in with Salesforce account.**

The application redirects you to <https://login.salesforce.com/>

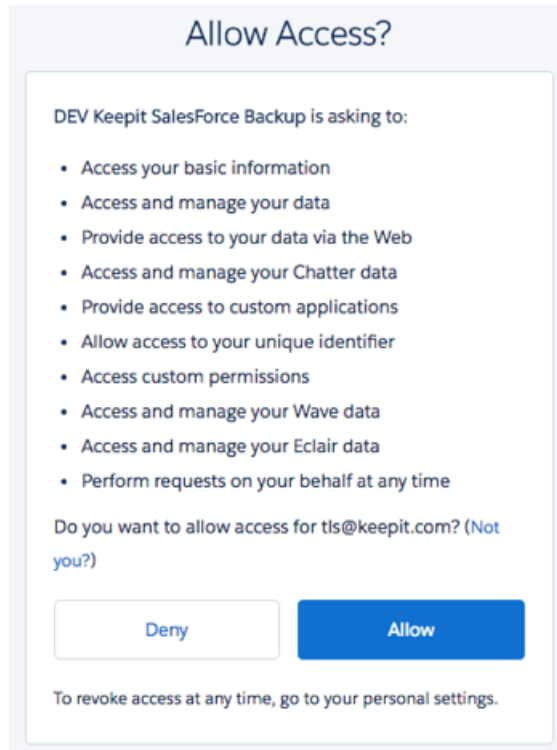
---

**Note:** The application cannot redirect you to <https://test.salesforce.com/>, and cannot back up files found in Salesforce Sandboxes.

---

**5 Enter your Salesforce credentials to sign in.**


- 6 When you are prompted for permission to access files, review the list of permissions.




- 7 Click **Allow** to add connector to SaaS Backup.

- 8 Select the connector, and click the **Configure** icon to open the configuration dialog box.

Setup Veritas for the Salesforce



Here you can set a different API limit if the default does not match your needs. For the initial backup we recommend using a higher percentage than 50%. A higher usage such as 90% or 100% will ensure that your Salesforce data will be quickly secured.


**Configure Connector**

Salesforce connector

Salesforce


**Change number of API requests**

Your usage is set to 90%. This means the backup will stop when 10% of your total 15000 Salesforce API daily requests remain.

10%



90%

100%


[Learn more about API requests](#)


Save

Close





- 9 Click the **Manage access** icon (lock icon) to view the **Access to Salesforce demopage**.
  - To provide access, select the check-boxes adjacent to users.
  - To revoke access, clear the check-boxes adjacent to users.
  - Click **Save** to confirm access.

Access to Salesforce Connector



Here you can see a list of users that have access to your connector. It is not possible to change the access for Master Administrators, SSO Admins, or Audit users.


**Users**

Users whose access can be changed

☐ Test - LimitedSupport - test@veritas.com

Users whose access cannot be changed

☒ Primary user login token - MasterAdmin - demo\_theme\_s@veritas.com

Save selection
Cancel

**10** Click **Save**.

## Deleting Salesforce cloud connectors

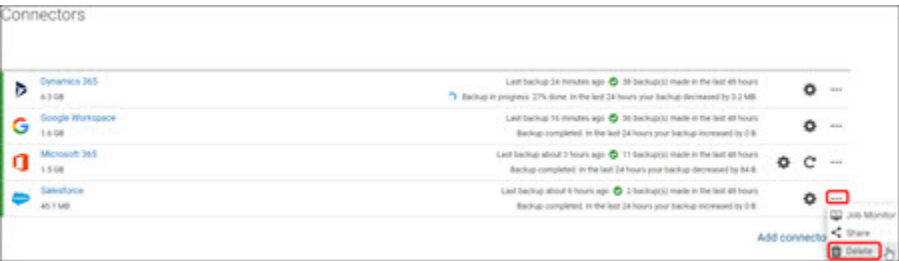
You can delete an expired or outdated Salesforce cloud connector. Ensure that you have permissions to delete a cloud connector.

To delete a Salesforce cloud connector

- 1 Sign in to SaaS Backup.

Note:

The **Connector** page appears by default. If you are on working on any other page (Links, Job Monitor, Audit, and so on), you can click **Connectors** from the menu icon. This page lets you view a list of connectors, the last updated date, side of data on connector, and the action icons.



- 2 Search for and select the Salesforce cloud connector you want to delete.
- 3 Click the **More Options** icon and select then the Delete icon.
- 4 Click the **Delete** icon

The application prompts you to confirm that you want to perform the operation.

**Note:** SaaS Backup schedules the deletion of the selected connector. The connector is deleted after the retention period is over. If you remove a Salesforce connector, entire data that is associated with the connector is deleted. You cannot revert the changes.

- 5 Click **Yes** to complete the operation or click **Cancel** to cancel it.

# Restoring records, files, and attachments on the Salesforce cloud connector

SaaS Backup supports in-place restore for individual Salesforce records. Records can be restored either by themselves or together with related records (all records lower in the hierarchy).



You can restore the records of the standard and custom objects, and can download and share the records of certain types of standard objects. These types of records are found in object folders, which are marked with a special icon as shown below:

Object Type	Icon	Restore
Account, Campaign, Campaign member, Case, Contact, Event, Lead, Note, Opportunity, Task	 and others	Yes
Custom objects		Yes
Standard objects: Type 1		Yes
Standard objects: Type 2		No

Restoring a record brings back all attached files and attachments. The content of files and attachments cannot be restored on their own.

#### To restore a Salesforce record

- 1 In the Salesforce connector, in the **Objects** folder, search for and select the record you want to restore.

---

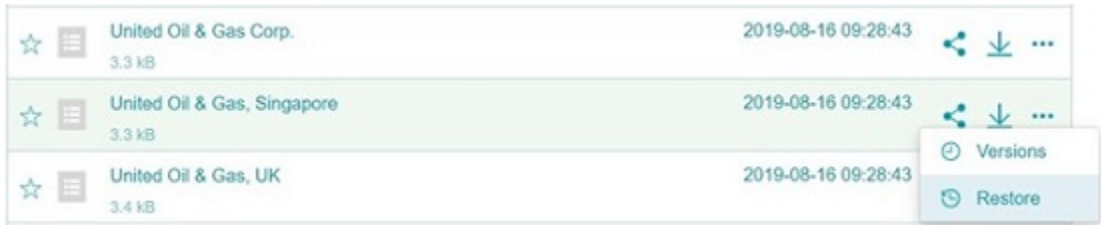
**Note:** For easy navigation, each type of object has its own icon. Alternately, use the search function to find your record.

---

- 2 To restore a record from an earlier point in time, in the upper-left corner, select the **Monitor** icon, select **History Snapshots**, and select the appropriate snapshot.

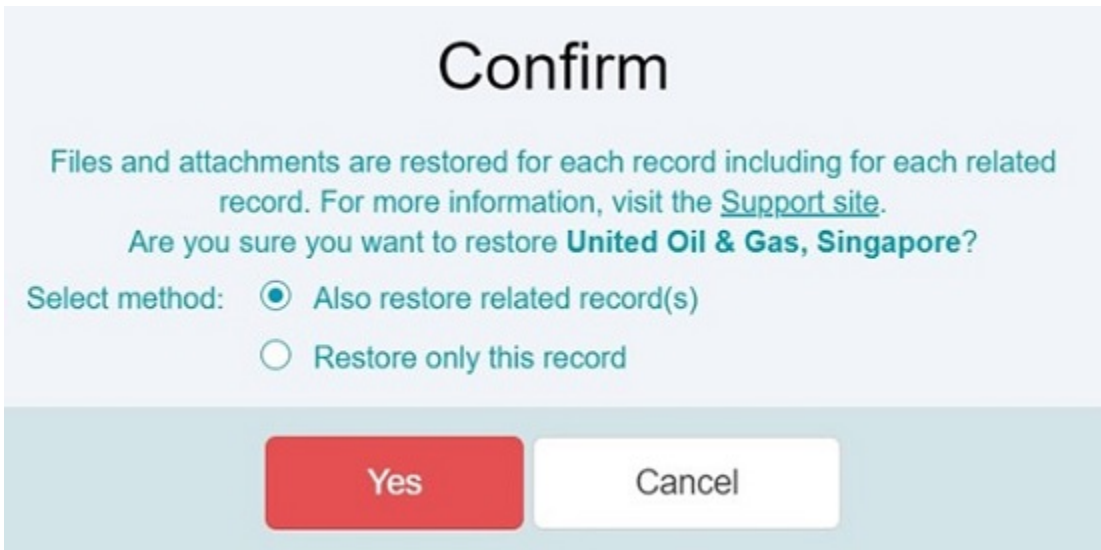
This is an optional step.

- 3 Select the **More options** icon to the right of the record, and select **Restore**.



- 4 Click the **More Options** icon, and select **Restore**.

The application prompts you to confirm that you want to perform the operation. Refer to the sample confirmation message.



- 5 Select any of the following restoration method:
  - To restore the selected record, select **Restore only this record**.
  - To restore all the related records along with the selected record, select **Also restore related record(s)**.

---

**Note:** If you select this option, some Microsoft system files may fail to restore. However, it does not affect restoration of your records.

---

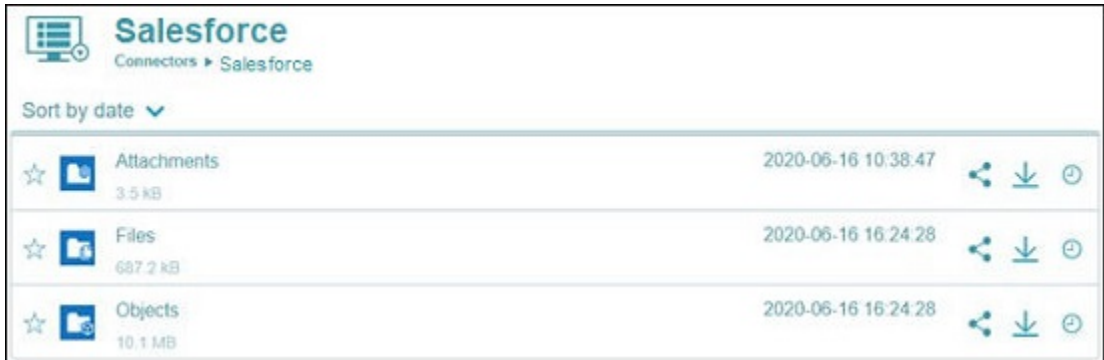
**6** Click **Yes** to complete the operation or click **Cancel** to cancel it.

After you restore your Salesforce data:

- All records receive new IDs.
- If the record exists in Salesforce and has the same ID, SaaS Backup checks the modification time:
  - If it has a different modification time, SaaS Backup overwrites the old record with the new record.
  - If it has the same modification time, SaaS Backup skip restoring the new file.
- If you want to restore records with mandatory links:
  - A child record with a mandatory link to a deleted parent record cannot be restored. The restore job fails. To restore this child record, you must first restore the parent record, and then restore the child record.
  - If SaaS Backup encounters a loop, in which two records are child and parent to one another and have mandatory links, restoring data becomes difficult. In this case, some of the items cannot be restored and the job is marked as failed.
- Custom picklist status fields are backed up and restored, but the Standard picklist status fields cannot be restored. To recover these statuses, it is recommended to open the backed-up records using the SaaS Backup previewer and enter the statuses in Salesforce manually.
- If custom records types and custom page layouts are restored:
  - If a record created via a custom record type is deleted from Salesforce and later restored from SaaS Backup, it is restored as the master (default) record type. The field values that do not belong to the master record type are not restored. The record is restored with the default page layout settings.
  - The set of users who have access to the restored record may change as only those who have access to the master record type can view the record.
  - To recover a record with a custom record type, copy the fields from the backed-up record in SaaS Backup and create a new record via a custom record type in Salesforce with these field values.

### To restore files and attachments

- 1 In the Salesforce connector, in the **Attachments** or the **Files** folder, search for and select the record you want to restore




---

**Note:** The **Attachments** folder contains files that were attached to records in Salesforce Classic. The **Files** folder contains files that were attached to record in Lightning Experience and file that were uploaded to Files in a Salesforce organization. You cannot restore the items in these folders individually.

---

- 2 To recover files and attachments, use any of the following options:
  - Download the file or attachment, and then manually upload it back to Salesforce.
  - If the file or attachment is attached to a record, restore the record to automatically bring back the file or attachment.

**Note:** Inside the **Objects** folder, there is also an **Attachments** folder. The items are the same as those in the **Attachments** root folder. However, these items only contain the metadata of the attachments. You can restore these items, but cannot recover the content.

☆	 Assignment Rules 1.3 kB	2020-07-16 12:25:42	  
☆	 Attachments 8.3 kB	2020-07-16 12:25:42	  
☆	 Audiences 1.6 kB	2020-07-16 12:25:42	  

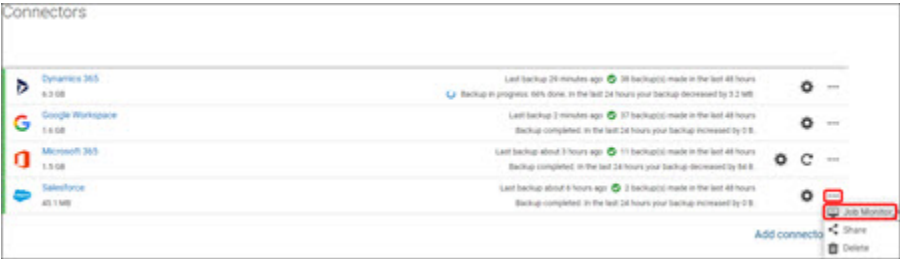
After you restore your Salesforce data:

- Restored files retain the same owners, but the creator becomes the administrator.
- All files are restored to the Files tab of the owner of that file.
- Only the latest version of a file is backed up and restored.
- All the files permissions are restored.
- Restored files receive a new modification time - the time of restore.
- If the restored file has a different modification time and differs from the latest version in Salesforce, SaaS Backup creates a new version of the file.
- If the restored file has a different modification time, SaaS Backup overwrites the latest version in Salesforce.
- If the restored file has the same modification time, then SaaS Backup skips restoring of that file.
- If you want to recover a file or attachment, you have the following options:
  - Download the file, and then upload again to Salesforce
  - Restore the record, which automatically brings back the file and attachments.

# Monitoring backup and restoring jobs of Salesforce cloud connectors

To monitor backup and restoring jobs of Salesforce cloud connectors

- 1    Select the connector for which you want to monitor jobs.



- 2    Click **Job Monitor**.
- 3    On the **Job Monitor** page, specify the following information.

Field	Description
Connector	Displays the connector name for which you want to generate a job monitoring report.
Status	Select the job status from the drop-down list for which you want to generate a report.
Type	Select the job type from the drop-down list for which you want to generate a report.
Time span	Specify the time span of the report you want to generate a job monitoring report. Predefined options are available. However, you can customize duration of report as per your requirement.
Start date	If the time span value is selected as <b>Custom period</b> , specify the date from which you want to generate a job monitoring report.
End date	If the time span value is selected as <b>Custom period</b> , specify the date up to which you want to generate a job monitoring report.

- 4    To view the result, click **Refresh**.
- 5    To sort a column details, click the respective column header.

- 6 To further narrow down the result, type a keyword in the **Filter** field, and click the search icon.
- 7 To view the statistic of a specific item, click its **Show more** link in the **Description** column.

## Sharing files and folders of Salesforce cloud connectors

### To share files and folders of Salesforce cloud connectors

- 1 Select the Salesforce connector for which you want to share the data.



- 2 To share entire connector data, click **Share folder** on the **Connectors** page. The application opens the **Share public link** page.

The screenshot shows the 'Share public link' page. It displays a message: 'Shared link was successfully created and copied to the clipboard'. Below this, there is a text box containing the URL: 'https://veritas-test.com/shares/#/folder/1b28c5-1ee5a2-1ba08f/'. Underneath the URL, there are two checkboxes: 'Set time limit for public link' (checked) and 'Add password to public link' (checked). Below the checkboxes, there is a 'Password' input field. At the bottom of the page, there are two buttons: 'Cancel' and 'Save'.

- 3 In the **Share public link** dialog box, specify the following information:

Field	Description
Time limit public link	Select this check-box to view the <b>Set expiration time</b> field.
Set expiration time	Set the expiration time of a public share link.
Password protect public link	Select this check-box to specify the password for user to access the shared content. You need to share this password with the user via email.

- 4 Click **Share**.  
The application opens the **Share public link** page.
- 5 Copy the link to share with the user, and click **Close** to exit this page.

## Downloading files and folders from Salesforce cloud connector

You can download the entire folder with the latest data or the specific version of files and folders within it.

### To download the entire folder with the latest data

- 1 Select the Salesforce connector, and navigate to the file or folder.
- 2 To download the entire folder with the latest data, click **Download**.





- 3 To download a specific snapshot (version), click **Version**.



Select the required snapshot, and click **Download**.

- 4 To download the specific version of the file, click the **More options** icon.



Select the point in time from which you want to download.

SaaS Backup downloads the files or folders to the **Downloads** folder of your computer.