



Veeam Backup for Microsoft 365

Version 7

User Guide

September, 2024

© 2024 Veeam Software.

All rights reserved. All trademarks are the property of their respective owners.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means, without written permission from Veeam Software (Veeam). The information contained in this document represents the current view of Veeam on the issue discussed as of the date of publication and is subject to change without notice. Veeam shall not be liable for technical or editorial errors or omissions contained herein. Veeam makes no warranties, express or implied, in this document. Veeam may have patents, patent applications, trademark, copyright, or other intellectual property rights covering the subject matter of this document. All other trademarks mentioned herein are the property of their respective owners. Except as expressly provided in any written license agreement from Veeam, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

NOTE

Read the End User Software License Agreement before using the accompanying software programs. Using any part of the software indicates that you accept the terms of the End User Software License Agreement.

Contents

CONTACTING VEEAM SOFTWARE	8
ABOUT VEEAM BACKUP FOR MICROSOFT 365	9
ABOUT THIS DOCUMENT	10
VEEAM BACKUP FOR MICROSOFT 365 ARCHITECTURE	11
GETTING STARTED WITH VEEAM BACKUP FOR MICROSOFT 365	14
PLANNING AND PREPARATION	16
System Requirements	17
Ports.....	23
Supported Amazon S3 Storage Classes.....	31
Supported Azure Storage Account Types.....	32
Permissions	33
Veeam Backup Account Permissions	35
Azure AD Application Permissions	40
Amazon S3 Storage Permissions	54
Azure Blob Storage Permissions	60
Permissions Changelog	61
Considerations and Limitations	63
LICENSING AND LICENSE TYPES.....	69
Subscription License	71
Rental License	72
Managing Monthly Usage Report	74
Not For Resale License	76
Evaluation License	77
INTEGRATION WITH VEEAM PRODUCTS.....	78
DEPLOYMENT	79
Downloading Installation Package	80
Installing Veeam Backup for Microsoft 365	81
Installing REST API	86
Installing Veeam Explorers	91
Installing in Unattended Mode	94
Deploying to Azure and AWS	97
Updating Veeam Backup for Microsoft 365	98
Automatic Update.....	99
Checking for Updates.....	100
Installing and Updating License	101
Uninstalling License.....	103
Upgrading Veeam Backup for Microsoft 365.....	104

Upgrading REST API on Separate Machine	109
Uninstalling Veeam Backup for Microsoft 365	112
LAUNCHING VEEAM BACKUP FOR MICROSOFT 365	113
User Interface.....	115
Current Session	119
Performing Search	120
CONFIGURATION.....	122
General Settings	123
Folder Exclusions	124
Session History	125
REST API Settings	126
Restore Portal Settings	128
Notification Settings	137
Security Settings.....	146
Authentication Settings.....	147
New Versions and Automatic Updates	149
Global Internet Proxy Server Settings	151
Configuring REST API and Restore Portal on Separate Machine	153
SSL Certificates Overview	156
SSL Certificate Usage Scenarios	157
Installing SSL Certificates	159
Backup Infrastructure	162
Backup Proxy Servers	163
Backup Repositories	177
Object Storage.....	202
Credentials.....	256
Managing Cloud Credentials	257
Managing Encryption Passwords.....	267
ORGANIZATION MANAGEMENT	269
Adding Microsoft 365 Organizations	270
Adding Microsoft 365 Organizations with Modern App-Only Authentication	271
Adding Microsoft 365 Organizations with Modern Authentication and Legacy Protocols	284
Adding Microsoft 365 Organizations with Basic Authentication	293
Adding On-Premises Microsoft Organizations	300
Step 1. Launch Add Organization Wizard	301
Step 2. Select Organization Deployment Type	302
Step 3. Specify Microsoft Exchange Connection Settings	303
Step 4. Specify Microsoft SharePoint Connection Settings	305
Step 5. Finish Working with Wizard	307
Adding Hybrid Organizations	308

Backup of Team Chats Using EWS	309
Backup of Team Chats Using Teams Export APIs	311
Backup Accounts	313
Adding Accounts.....	314
Changing Password and Removing Accounts	316
Backup Applications.....	317
Impact of Multiple Backup Applications on Performance	318
Adding Applications	319
Creating Applications	322
Updating Certificates and Removing Applications	325
Editing Organization Settings	326
Renaming Organizations	327
Removing Organizations	329
DATA BACKUP.....	330
Organization Object Types	331
Creating Backup Job	337
Step 1. Launch New Backup Job Wizard	338
Step 2. Specify Backup Job Name	339
Step 3. Select Objects to Back Up	340
Step 4. Select Objects to Exclude.....	349
Step 5. Specify Backup Proxy and Repository	351
Step 6. Specify Scheduling Options	352
Managing Backup Jobs.....	355
Starting Backup Job	356
Stopping Backup Job	357
Enabling or Disabling Backup Job	358
Editing Backup Job Settings	359
Removing Backup Job	360
Exploring Backup Job	361
BACKUP COPY.....	362
Getting Started with Backup Copy	364
Creating Backup Copy Job	366
Step 1. Launch New Backup Copy Job Wizard.....	367
Step 2. Select Target Backup Repository	368
Step 3. Specify Scheduling Options	369
Managing Backup Copy Jobs	371
Starting Backup Copy Job	372
Stopping Backup Copy Job	374
Enabling or Disabling Backup Copy Job	375
Editing Backup Copy Job Settings	376

Removing Backup Copy Job	377
Retrieving Backed-Up Data	378
Creating Retrieval Job	379
Editing Retrieval Job Settings	389
Extending Availability of Retrieved Data	390
DATA RESTORE	391
Exploring Backup Jobs	392
Exploring Single Organization	393
Exploring All Organizations	395
Exploring Point In Time	397
Exploring Retrieved Data	398
Exploring Backup Copies	399
BACKUP, BACKUP COPY, RETRIEVE AND RESTORE STATISTICS.....	401
Viewing Backup and Backup Copy Session Metrics	402
Viewing Retrieve Session Metrics	404
Viewing Restore Session Metrics	405
Performing Search	406
REPORTING	407
Creating Mailbox Protection Reports	408
Creating Storage Consumption Reports	410
Creating License Overview Reports	412
Creating User Protection Reports.....	414
MANAGING LOG FILES	416
Collecting Log Files	418
Enabling Extended Logging Mode	421
BACKUP AS SERVICE FOR MICROSOFT 365	423
For Service Providers	424
Configuring Veeam Backup for Microsoft 365	425
For Tenants	426
Exploring Backups in Veeam Explorers	427
DATA RESTORE USING RESTORE PORTAL.....	428
Restore Portal Usage Scenarios	429
How Restore Portal Works.....	430
Considerations and Limitations	431
Configuration	432
Adding Restore Operator Role	435
Editing Restore Operator Role Settings	445
Removing Restore Operator Role	446
Launching Restore Portal	447
User Interface	449

Managing Notifications	452
Changing Restore Operator Scope	453
Selecting Restore Point	455
Performing Restore.....	456
Using Restore List	457
Exchange Restore	459
SharePoint Restore	462
OneDrive Restore.....	465
Teams Restore	468
Exporting Teams Posts	471
DATA RESTORE USING VEEAM EXPLORERS.....	472

Contacting Veeam Software

At Veeam Software we value feedback from our customers. It is important not only to help you quickly with your technical issues, but it is our mission to listen to your input and build products that incorporate your suggestions.

Customer Support

Should you have a technical concern, suggestion or question, visit the [Veeam Customer Support Portal](#) to open a case, search our knowledge base, reference documentation, manage your license or obtain the latest product release.

Company Contacts

For the most up-to-date information about company contacts and office locations, visit the [Veeam Contacts Webpage](#).

Online Support

If you have any questions about Veeam products, you can use the following resources:

- Full documentation set: veeam.com/documentation-guides-datasheets.html
- Veeam R&D Forums: forums.veeam.com

About Veeam Backup for Microsoft 365

Veeam Backup for Microsoft 365 is a comprehensive solution that allows you to back up and restore data of your Microsoft 365 organizations, including Microsoft Exchange, Microsoft SharePoint, Microsoft OneDrive for Business and Microsoft Teams data, as well as data of on-premises Microsoft Exchange and on-premises Microsoft SharePoint organizations.

About This Document

This user guide provides information about main features, installation and use of Veeam Backup for Microsoft 365 to back up and restore data of your Microsoft 365 and on-premises Microsoft organizations.

The document applies to Veeam Backup for Microsoft 365 version 7 until it is replaced with a newer version of the product.

Intended Audience

This guide is intended for IT specialists who want to use Veeam Backup for Microsoft 365, protect Microsoft Exchange, Microsoft SharePoint, Microsoft OneDrive for Business and Microsoft Teams data, and provide availability of this data for users in Microsoft 365 and on-premises Microsoft organizations.

Veeam Backup for Microsoft 365 Architecture

Veeam Backup for Microsoft 365 architecture includes three core structural components – Veeam Backup for Microsoft 365 server, backup proxy server and backup repository, and additional components such as REST API along with Restore Portal and PowerShell.

Veeam Backup for Microsoft 365 Server

Veeam Backup for Microsoft 365 server is responsible for setting up and managing other backup infrastructure components, jobs scheduling and task coordination. As part of Veeam Backup for Microsoft 365 server, the following components are installed:

- Services:
 - *Veeam Backup for Microsoft 365 Service*

Coordinates all operations performed by the product, adds and manages other backup infrastructure components as well as controls global settings for the backup infrastructure.
 - *Veeam Backup Proxy for Microsoft 365 Service*

Manages backup proxy servers and backup repositories.
 - *Veeam Backup for Microsoft 365 REST API Service*

Processes REST API commands.

Restore Portal is deployed along with REST API on the same machine. Restore Portal is a web-based solution for self-service restore of backed-up data. Restore Portal uses REST API to communicate with the Veeam Backup for Microsoft 365 server. For more information, see [Data Restore Using Restore Portal](#).
- *Veeam Backup for Microsoft 365 Console*

Provides an interface that allows users to interact with the Veeam Backup for Microsoft 365 server and backup infrastructure components.
- Veeam Explorers

Set of instruments that comes as part of Veeam Backup for Microsoft 365 and allows you to restore or export your data from backups.

Backup Proxy Server

A backup proxy server is an architecture component that conducts all read and write activities during data backup and restore, routes backup traffic, handles data compression and encryption and sends email notifications about backup and backup copy job results.

For more information, see [Backup Proxy Servers](#).

Backup Repository

A backup repository is a storage system within the backup infrastructure where Veeam Backup for Microsoft 365 saves backup data.

You can extend a backup repository with object storage. Veeam Backup for Microsoft 365 supports cloud and on-premises storage systems as object storage.

For more information, see [Backup Repositories](#) and [Object Storage](#).

Deployment Scenarios

Veeam Backup for Microsoft 365 offers two deployment scenarios: simple and advanced. Before you install Veeam Backup for Microsoft 365, familiarize yourself with the deployment scenarios to carefully plan your backup infrastructure layout.

Simple Deployment

This deployment scenario is intended for small environments or for the purpose of the Veeam Backup for Microsoft 365 evaluation. In this scenario, Veeam Backup for Microsoft 365, Veeam Explorers, backup proxy server and backup repository are installed on a single machine.

This machine performs the following roles:

- [Veeam Backup for Microsoft 365 server](#)
- [Default backup proxy server](#)

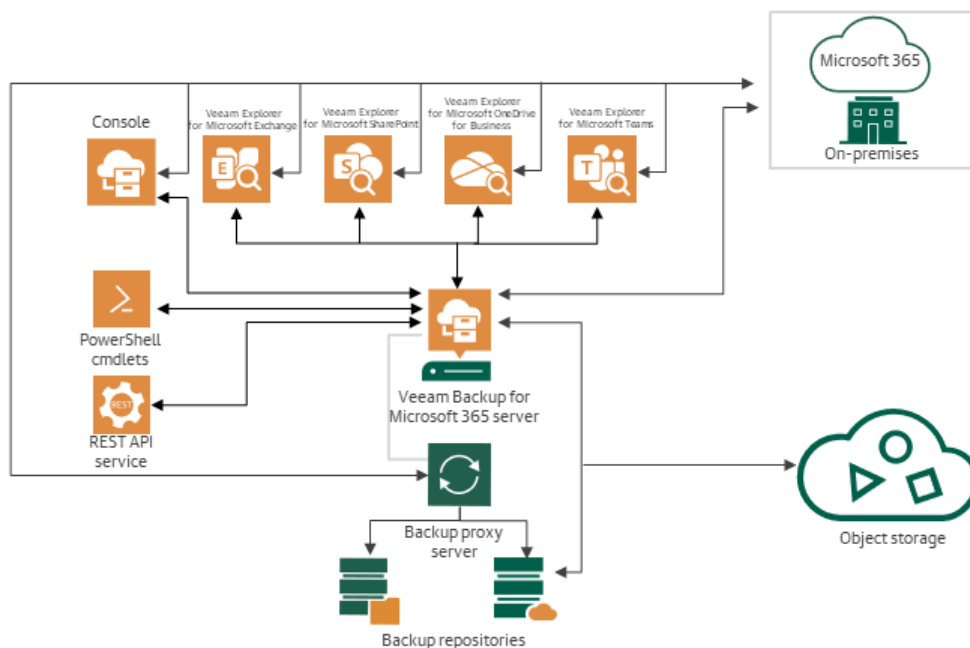
Veeam Backup for Microsoft 365 displays this backup proxy as *Local*.

- [Default backup repository](#)

Veeam Backup for Microsoft 365 creates the `C:\VeeamRepository` folder on the machine where the product is installed.

You can scale out a simple deployment by adding multiple backup repositories that are operated by the default backup proxy server.

The following diagram illustrates the interaction between Veeam Backup for Microsoft 365 components in a simple deployment scenario.



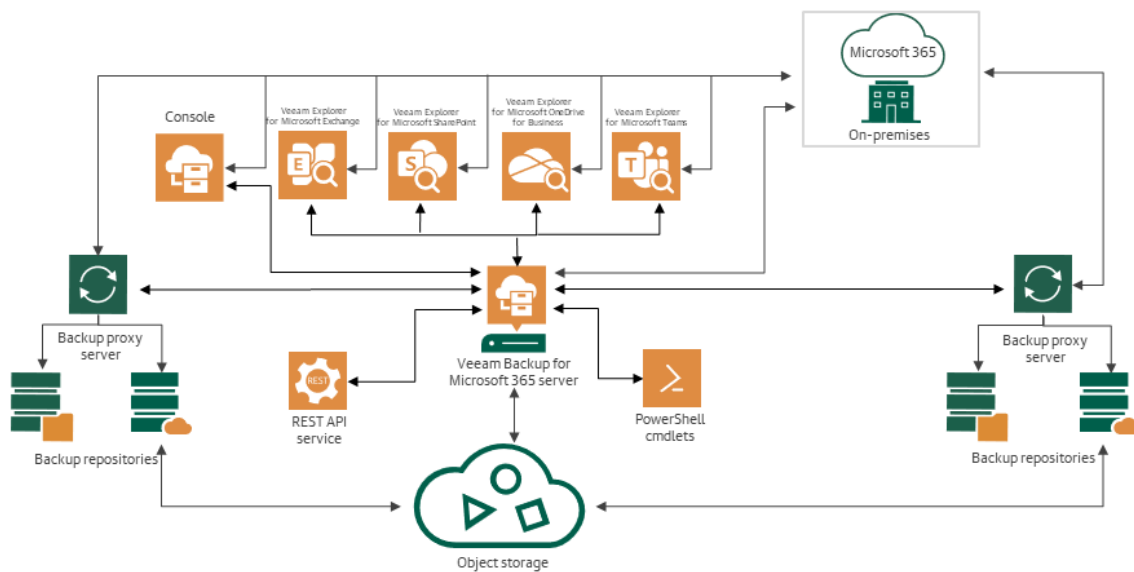
Advanced Deployment

This deployment scenario suits medium-sized or large-scale environments where the capacity of a single Veeam Backup for Microsoft 365 server is not enough. To scale out the backup infrastructure, you add additional backup proxy servers and backup repositories. These operations are handled by *Veeam Backup for Microsoft 365 Service* on the Veeam Backup for Microsoft 365 server and comprise the installation of necessary components on dedicated machines.

In environments with multiple backup proxy servers, you can distribute backup traffic among these proxies. This allows you to manage your data more efficiently.

For more information, see [Backup Proxy Server](#) and [Backup Repository](#).

The following diagram illustrates the interaction between Veeam Backup for Microsoft 365 components in an advanced deployment scenario.



Veeam Backup for Microsoft 365 REST API Server

The additional option in the advanced deployment scenario is to deploy the Veeam Backup for Microsoft 365 REST API component along with Restore Portal on a separate machine. This machine will perform the role of the Veeam Backup for Microsoft 365 REST API server. Deployment of the Veeam Backup for Microsoft 365 REST API component on a separate machine decreases the load on the backup infrastructure when exploring and restoring data from backups using Restore Portal.

Restore Portal is a web-based solution for self-service restore of backed-up data. For more information about Restore Portal, see [Data Restore Using Restore Portal](#).

Getting Started with Veeam Backup for Microsoft 365

Before you start using Veeam Backup for Microsoft 365, you can check the following prerequisites:

- Become familiar with the Veeam Backup for Microsoft 365 architecture and deployment scenarios to carefully plan your backup infrastructure layout. For more information, see [Veeam Backup for Microsoft 365 Architecture](#).
- Make sure that machines on which you plan to deploy the Veeam Backup for Microsoft 365 components meet hardware recommendations and system requirements. For more information, see [System Requirements](#).
- Become familiar with the authentication options that Veeam Backup for Microsoft 365 requires. For more information about permissions in Veeam Backup for Microsoft 365, see [Permissions](#).

To use Veeam Backup for Microsoft 365, perform the following steps:

1. Deploy Veeam Backup for Microsoft 365. For more information, see [Deployment](#).
2. Launch *Veeam Backup for Microsoft 365 Console*. For more information, see [Launching Veeam Backup for Microsoft 365](#).
3. Configure general settings of Veeam Backup for Microsoft 365. For more information, see [General Settings](#).

This step is optional. You can use Veeam Backup for Microsoft 365 with the default settings, or, for example, configure REST API and Restore Portal if you plan to use these product components.

4. Configure backup infrastructure. You can configure the following backup infrastructure components:
 - Backup proxy servers
By default, Veeam Backup for Microsoft 365 runs with the default backup proxy server hosted on the same machine where the product is installed. You can add additional backup proxy servers to distribute backup traffic among these proxies. For more information, see [Backup Proxy Servers](#).
 - Backup repositories
By default, Veeam Backup for Microsoft 365 uses the default backup repository located on the same machine where the product is installed. You can add additional backup repositories to store backups in different locations for enhanced protection. For more information, see [Backup Repositories](#).
 - Object storage
You can extend a backup repository with object storage. In this case, Veeam Backup for Microsoft 365 stores backups and backup copies in supported cloud or on-premises storage systems. For more information, see [Object Storage](#).
5. Add a Microsoft organization whose data you want to protect. For more information, see [Organization Management](#).
6. Create a backup job. You can create different backup jobs with different objects added to a backup job scope and map backup jobs to different backup repositories. For more information, see [Data Backup](#).

7. Create a backup copy job to transfer backups created by a source backup job to object storage for long-term storage.

This step is optional. You can create a backup copy job right after configuring a backup job or at any time later. For more information, see [Backup Copy](#).
8. Whenever you need, explore and restore backed-up data of your Microsoft organizations. For more information, see [Data Restore](#).

Planning and Preparation

Before you install Veeam Backup for Microsoft 365, make sure that your environment and machines that you plan to use as backup infrastructure components meet product hardware recommendations and system requirements.

System Requirements

Make sure that your Microsoft organizations and backup infrastructure components meet the listed requirements.

Supported Organizations

The following table lists supported Microsoft Exchange and Microsoft SharePoint organizations:

Organization	Requirement
Microsoft Exchange	<p>Veeam Backup for Microsoft 365 supports the following Microsoft Exchange versions:</p> <ul style="list-style-type: none">• Microsoft 365 Exchange Online <p>Microsoft 365 and Office 365 service families, standalone services and plans for Business, Education, and Government* hosted by Microsoft are supported. For more information about system requirements and limitations for Microsoft 365, see this Microsoft article.</p> <ul style="list-style-type: none">• Microsoft Exchange Server 2019 (on-premises)• Microsoft Exchange Server 2016 (on-premises)• Microsoft Exchange Server 2013 (on-premises) <p>For more information about limitations for backup and restore of mail items, see Considerations and Limitations.</p>

Organization	Requirement
Microsoft SharePoint	<p>Veeam Backup for Microsoft 365 supports the following Microsoft SharePoint versions:</p> <ul style="list-style-type: none"> • Microsoft 365 SharePoint Online <p>Microsoft 365 and Office 365 service families, standalone services and plans for Business, Education, and Government* hosted by Microsoft are supported. For more information about system requirements and limitations for Microsoft 365, see this Microsoft article.</p> • Microsoft SharePoint Server 2019 <p>For more information about hardware and software requirements, see this Microsoft article.</p> • Microsoft SharePoint Server 2016 <p>For more information about hardware and software requirements, see this Microsoft article.</p> • Microsoft SharePoint Server Subscription Edition <p>For more information about hardware and software requirements, see this Microsoft article and this Microsoft article.</p>

*Government support is experimental.

NOTE

Throttling policies for Exchange Online cannot be managed in the Microsoft 365 interface.

Veeam Backup for Microsoft 365 Server

The following table lists system requirements for the machine with Veeam Backup for Microsoft 365:

Specification	Requirement
Hardware	<p>The following hardware is required:</p> <ul style="list-style-type: none">• <i>CPU</i>: any modern multi-core x64 processor, 8 cores minimum.• <i>Memory</i>: 16 GB RAM minimum. Additional RAM and CPU resources improve backup, restore and search performance. <p>If you plan to deploy Veeam Backup for Microsoft 365 on VM with dynamic memory allocation, such VM must have 16 GB RAM minimum.</p> <ul style="list-style-type: none">• <i>Disk Space</i>: 1 GB for product installation and additional free space for configuration and local cache databases (depending on the number of organizations, jobs, and sessions) and product logs. Keep in mind that local cache databases are only created for Microsoft 365 organizations with modern app-only authentication.
OS	<p>Only 64-bit version of the following operating systems are supported:</p> <ul style="list-style-type: none">• Microsoft Windows Server 2022• Microsoft Windows Server 2019• Microsoft Windows Server 2016• Microsoft Windows Server 2012 R2• Microsoft Windows Server 2012• Microsoft Windows 10 22H2 and earlier• Microsoft Windows 11 22H2 and earlier <p>Veeam Backup for Microsoft 365 server can be deployed on the following core editions:</p> <ul style="list-style-type: none">• Microsoft Windows Server 2022• Microsoft Windows Server 2019 LTSC, 1809• Microsoft Windows Server 2016 LTSC, 1607• Microsoft Windows Server 2012 R2• Microsoft Windows Server 2012
Software	<p>The following components are required:</p> <ul style="list-style-type: none">• Microsoft .NET Framework 4.7.2 or later.• Windows C Runtime and Update (UCRT) in Windows. For more information, see this Microsoft article.• To use PowerShell cmdlets, Windows PowerShell 5.1 is required. <p>For more information about Microsoft 365 system requirements and limitations, see this Microsoft article.</p>

IMPORTANT

Consider the following:

- When you install Veeam Explorers and Veeam Backup for Microsoft 365 on different servers, the OS version on computers with Veeam Explorers must be the same or later than the OS version on a computer with Veeam Backup for Microsoft 365.
- Veeam Explorers can be installed on a machine hosting Veeam Backup for Microsoft 365 7 or the *Veeam Backup for Microsoft 365 Console* component. You can also use a machine with Veeam Backup & Replication 10 or later that is deployed either along with any of these components, or as an independent solution.
- The account you want to use for launching Veeam Backup for Microsoft 365 must be a member of the local *Administrators* group on a computer with Veeam Backup for Microsoft 365.

Machine with REST API

The following table lists system requirements for the machine with the Veeam Backup for Microsoft 365 REST API component:

Specification	Requirement
Hardware	<p>The following hardware is required:</p> <ul style="list-style-type: none">• <i>CPU</i>: any modern multi-core x64 processor, 8 cores minimum.• <i>Memory</i>: 16 GB RAM minimum. Additional RAM and CPU resources improve backup, restore and search performance. <p>If you plan to deploy the Veeam Backup for Microsoft 365 REST API server on VM with dynamic memory allocation, such VM must have 16 GB RAM minimum.</p> <ul style="list-style-type: none">• <i>Disk Space</i>: 500 MB for the Veeam Backup for Microsoft 365 REST API server installation and additional free space for product logs.

Specification	Requirement
OS	<p>Only 64-bit version of the following operating systems are supported:</p> <ul style="list-style-type: none"> • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows 10 22H2 and earlier • Microsoft Windows 11 22H2 and earlier <p>Veeam Backup for Microsoft 365 REST API server can be deployed on the following core editions:</p> <ul style="list-style-type: none"> • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 LTSC, 1809 • Microsoft Windows Server 2016 LTSC, 1607 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012
Software	<p>The following components are required:</p> <ul style="list-style-type: none"> • Microsoft .NET Framework 4.7.2 or later. • Windows C Runtime and Update (UCRT) in Windows. For more information, see this Microsoft article.

Backup Proxy Server

The following table lists system requirements for machines that you plan to use as [backup proxy servers](#):

Specification	Requirement
Hardware	<p>The following hardware is required:</p> <ul style="list-style-type: none"> • <i>CPU</i>: any modern multi-core x64 processor, 8 cores minimum. • <i>Memory</i>: 16 GB RAM minimum. Additional RAM and CPU resources improve backup, restore and search performance. <p>If you plan to deploy Veeam Backup for Microsoft 365 backup proxy server on VM with dynamic memory allocation, such VM must have 16 GB RAM minimum.</p> <ul style="list-style-type: none"> • <i>Disk space</i>: 1 GB for backup proxy installation and additional free space for configuration and local cache databases (depending on the number of organizations, jobs, and sessions) and backup proxy logs. Keep in mind that local cache databases are only created for Microsoft 365 organizations with modern app-only authentication.

Specification	Requirement
<p>OS</p>	<p>Only 64-bit version of the following operating systems are supported:</p> <ul style="list-style-type: none"> • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows 10 22H2 and earlier • Microsoft Windows 11 22H2 and earlier <p>Proxy servers can be deployed to the following core editions:</p> <ul style="list-style-type: none"> • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 LTSC, 1809 • Microsoft Windows Server 2016 LTSC, 1607 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012
<p>Other</p>	<p>The following components are required:</p> <ul style="list-style-type: none"> • Microsoft .NET Framework 4.7.2 or later. • Windows C Runtime and Update (UCRT) in Windows. For more information, see this Microsoft article. <p>For a machine used as a workgroup backup proxy, the following settings are required:</p> <ul style="list-style-type: none"> • The <i>Remote Registry</i> service must run on the target machine. The service startup type must be set to <i>Automatic</i>. • Backup proxy server ports must be opened in Windows Firewall.

Ports

The following table lists ports that must be opened for inbound/outbound requests in Veeam Backup for Microsoft 365.

Depending on Microsoft 365 subscription location, Veeam Backup for Microsoft 365 uses the following endpoints:

- Worldwide endpoints
The endpoints for worldwide Microsoft 365 subscriptions. For more information, see [this Microsoft article](#).
- Microsoft 365 operated by 21 Vianet endpoints
The endpoints for Microsoft 365 operated by 21 Vianet which is designed to meet the needs for Microsoft 365 in *China*. For more information, see [this Microsoft article](#).

NOTE

Data communication between Microsoft 365 organizations and Veeam Backup for Microsoft 365 is performed through an SSL connection.

From	To	Protocol	Port	Description
Veeam Backup for Microsoft 365 server	Microsoft Exchange Online	TCP	443	Required to connect to Microsoft Exchange Online organizations. The Worldwide endpoints are: <i>outlook.office365.com</i> and <i>autodiscover-s.outlook.com</i> . The Microsoft 365 operated by 21 Vianet endpoints are: <i>partner.outlook.cn</i> and <i>autodiscover-s.partner.outlook.cn</i> .
	Microsoft SharePoint Online	TCP	443	Required to connect to Microsoft SharePoint Online organizations. The Worldwide endpoints are: <i><tenant>.sharepoint.com</i> , <i><tenant>-my.sharepoint.com</i> and <i><tenant>-admin.sharepoint.com</i> . The Microsoft 365 operated by 21 Vianet endpoints are: <i><tenant>-admin.sharepoint.cn</i> , <i><mytenant>-my.sharepoint.cn</i> and <i><mytenant>sharepoint.cn</i> .

From	To	Protocol	Port	Description
	On-premises Microsoft SharePoint server	HTTP (HTTPS)	5985 (5986 – used by default)	Required to connect to on-premises Microsoft SharePoint organizations through the WinRM port.
	On-premises Microsoft Exchange server	TCP	80 or 443	Required to connect to on-premises Microsoft Exchange organizations.
	Backup proxy server	TCP	9193 (used by default)	Required to manage inbound/outbound traffic when interacting with the Veeam Backup for Microsoft 365 server. Make sure to open this port on a backup proxy server.
		TCP	445	This port is used to: <ul style="list-style-type: none"> • Install and manage the <i>Veeam.Archiver.Proxy</i> service on a target proxy machine. • Perform RPC requests.
	Veeam auto-update server	TCP	443	Required to access the auto-update server and licensing server. For more information, see Updating Veeam Backup for Microsoft 365 and Installing and Updating License . The endpoints are: <i>https://vbo.butler.veeam.com</i> and <i>download2.veeam.com</i> .

From	To	Protocol	Port	Description
		TCP	80	<p>Required for certificate validation when Veeam Backup for Microsoft 365 connects to licensing server to check if the new license is available to update the product license automatically.</p> <p>The endpoints are: <i>*.ss2.us</i> and <i>*.amazontrust.com</i>.</p> <p>Consider that certificate verification endpoints (CRL URLs and OCSP servers) are subject to change. The actual list of addresses can be found in the certificate itself.</p>
	S3 Compatible object storage / IBM Cloud / WasabiCloud object storage	TCP	443	<p>Required to work with object storage.</p> <p>The endpoint is <i><account>.blob.core.windows.net</i>.</p>
	Amazon S3 object storage			
	Azure Blob Storage			
	Microsoft 365	TCP	443	<p>Required to connect to Microsoft 365.</p> <p>The Worldwide endpoints are: <i>graph.microsoft.com</i>, <i>graph.windows.net</i> and <i>login.microsoftonline.com</i>.</p> <p>The Microsoft 365 operated by 21 Vianet endpoints are: <i>login.partner.microsoftonline.cn</i> and <i>microsoftgraph.chinacloudapi.cn</i>.</p>
	SMTP server	TCP	25 or 465 or 587	<p>Required to send email notifications using an SMTP server.</p> <p>The Worldwide endpoint is <i>smtp.office365.com</i>.</p> <p>The Microsoft 365 operated by 21 Vianet endpoint is <i>smtp-legacy.partner.outlook.cn</i>.</p>

From	To	Protocol	Port	Description
Veeam Backup for Microsoft 365 components	Veeam Backup for Microsoft 365 server	TCP	9191	<p>Required to manage inbound/outbound traffic when interacting with the following components:</p> <ul style="list-style-type: none"> • REST API • PowerShell • Veeam.Archiver.Shell (UI) • [Optionally] A remote management server (if any) <p>Make sure to open port on the Veeam Backup for Microsoft 365 server.</p>
Veeam Explorer for Microsoft Exchange	Veeam Backup for Microsoft 365 server	TCP	9194	<p>Required to manage inbound/outbound traffic when interacting with Veeam Explorer for Microsoft Exchange.</p> <p>Make sure to open this port on the Veeam Backup for Microsoft 365 server.</p>
	Microsoft Exchange Online	TCP	443	Required to restore Microsoft Exchange data.
	SMTP server	TCP	25 or 465 or 587	<p>Required to send email notifications using an SMTP server.</p> <p>The Worldwide endpoint is <i>smtp.office365.com</i>.</p> <p>The Microsoft 365 operated by 21 Vianet endpoint is <i>smtp-legacy.partner.outlook.cn</i>.</p>
Veeam Explorer for Microsoft SharePoint (including Veeam Explorer for Microsoft OneDrive for Business)	Veeam Backup for Microsoft 365 server	TCP	9194	<p>Required to manage inbound/outbound traffic when interacting with Veeam Explorer for Microsoft SharePoint.</p> <p>Make sure to open this port on the Veeam Backup for Microsoft 365 server.</p>
	Microsoft SharePoint Online	TCP	443	Required to restore Microsoft SharePoint data.

From	To	Protocol	Port	Description
	SMTP server	TCP	25 or 465 or 587	<p>Required to send email notifications using an SMTP server.</p> <p>The Worldwide endpoint is <i>smtp.office365.com</i>.</p> <p>The Microsoft 365 operated by 21 Vianet endpoint is <i>smtp-legacy.partner.outlook.cn</i>.</p>
Veeam Explorer for Microsoft Teams	Veeam Backup for Microsoft 365 server	TCP	9194	<p>Required to manage inbound/outbound traffic when interacting with Veeam Explorer for Microsoft Teams.</p> <p>Make sure to open this port on the Veeam Backup for Microsoft 365 server.</p>
	Microsoft Teams Online	TCP	443	<p>Required to restore Microsoft Teams data.</p> <p>The endpoint is <i>developer.microsoft.com</i>.</p>
	SMTP server	TCP	25 or 465 or 587	<p>Required to send email notifications using an SMTP server.</p> <p>The Worldwide endpoint is <i>smtp.office365.com</i>.</p> <p>The Microsoft 365 operated by 21 Vianet endpoint is <i>smtp-legacy.partner.outlook.cn</i>.</p>
Backup proxy server¹	Veeam Backup for Microsoft 365 server	TCP	9191	<p>Required to manage inbound/outbound traffic when interacting with backup proxy servers.</p> <p>Make sure to open this port on the Veeam Backup for Microsoft 365 server.</p> <p>You can also change this port. For more information, see Editing Backup Proxy Server Settings.</p>

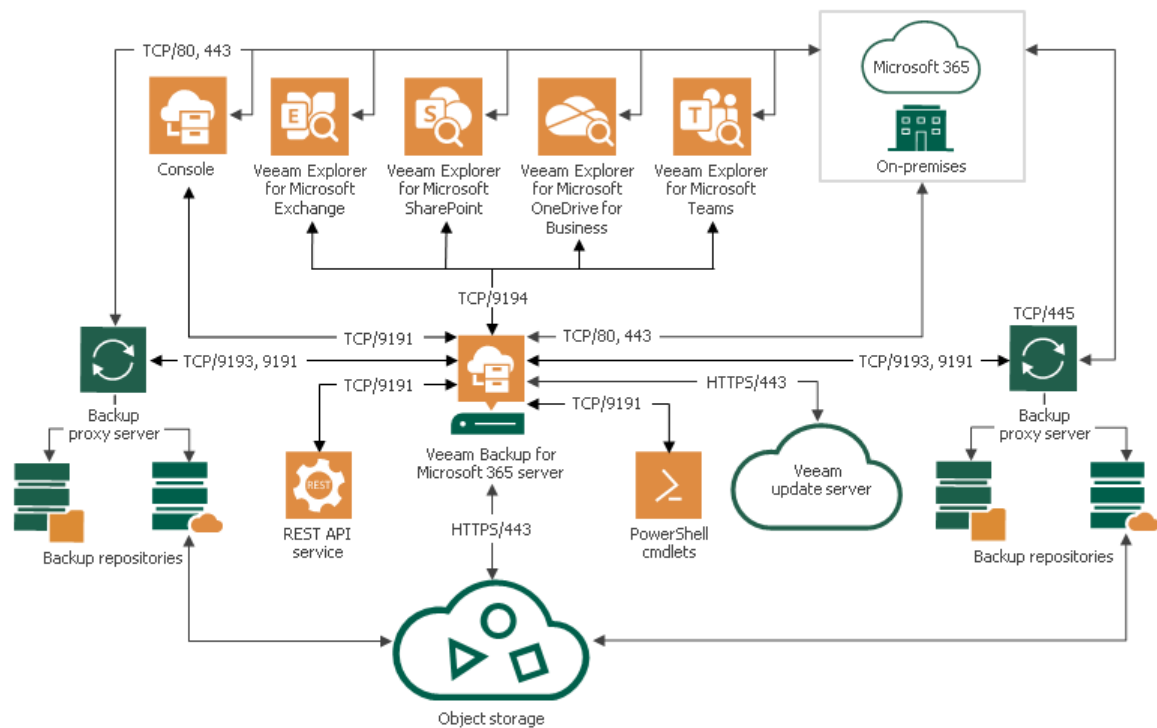
From	To	Protocol	Port	Description
	Backup proxy server	TCP	9193	Required to move an organization data between repositories. Make sure to open this port on each backup proxy server.
	Microsoft Exchange Online	TCP	443	Required to connect to Microsoft Exchange Online through EWS (Exchange Web Services). The Worldwide endpoints are: <i>outlook.office365.com</i> and <i>autodiscover-s.outlook.com</i> . The Microsoft 365 operated by 21 Vianet endpoints are: <i>partner.outlook.cn</i> and <i>autodiscover-s.partner.outlook.cn</i> .
	Microsoft SharePoint Online	TCP	443	Required to connect to Microsoft SharePoint Online organizations. The Worldwide endpoints are: <i><tenant>.sharepoint.com</i> , <i><tenant>-my.sharepoint.com</i> and <i><tenant>-admin.sharepoint.com</i> . The Microsoft 365 operated by 21 Vianet endpoints are: <i><tenant>-admin.sharepoint.cn</i> , <i><mytenant>-my.sharepoint.cn</i> and <i><mytenant>sharepoint.cn</i> .
	On-premises Microsoft SharePoint server	HTTP (HTTPS)	5985 (5986)	Required to connect to on-premises Microsoft SharePoint organizations through the WinRM port.
	On-premises Microsoft Exchange server	TCP	80 or 443	Required to connect to on-premises Microsoft Exchange organizations.
	S3 Compatible object storage / IBM Cloud / WasabiCloud object storage	TCP	443	Required to work with object storage. The endpoint is <i><account>.blob.core.windows.net</i> .
	Amazon S3 object storage			

From	To	Protocol	Port	Description
	Azure Blob Storage			
	Microsoft 365	TCP	443	<p>Required to connect to Microsoft 365.</p> <p>The Worldwide endpoints are: <i>graph.microsoft.com</i>, <i>graph.windows.net</i> and <i>login.microsoftonline.com</i>.</p> <p>The Microsoft 365 operated by 21 Vianet endpoints are: <i>login.partner.microsoftonline.cn</i> and <i>microsoftgraph.chinacloudapi.cn</i>.</p>
	SMTP server	TCP	25 or 465 or 587	<p>Required to send email notifications using an SMTP server.</p> <p>The Worldwide endpoint is <i>smtp.office365.com</i>.</p> <p>The Microsoft 365 operated by 21 Vianet endpoint is <i>smtp-legacy.partner.outlook.cn</i>.</p>
	Amazon archiver appliance ¹	TCP	443	Required to communicate with the Amazon archiver appliance.
		TCP	22	Required to install the Amazon archiver appliance.
	Azure archiver appliance ¹	TCP	443	Required to communicate with the Azure archiver appliance.
		TCP	22	Required to install the Azure archiver appliance.
Cloud gateway	Server that hosts Veeam Backup & Replication and Veeam Backup for Microsoft 365	TCP	9194	Required to maintain inbound/outbound traffic.
Web browser	Veeam Backup for Microsoft 365 REST API	HTTPS	4443 (used by default)	Required to connect to Restore Portal. You can also use a different port.

From	To	Protocol	Port	Description
Machine with REST API	Veeam Backup for Microsoft 365 server	TCP	9194	Required for data exchange between Restore Portal and Veeam Backup for Microsoft 365 server.
	Microsoft 365	TCP	443	Required for user login to Restore Portal. The endpoint is <i>login.microsoftonline.com</i> (depends on a Microsoft Azure region).

To manage outbound traffic, TCP outgoing ports must be opened for backup proxy servers, Amazon and Azure archiver appliances. For backup proxy servers, these ports are required to access Microsoft 365 organizations and communicate with object storage; for Amazon and Azure archiver appliances – to communicate with object storage.

The following diagram illustrates the interaction between Veeam Backup for Microsoft 365 components and used ports.



Supported Amazon S3 Storage Classes

Veeam Backup for Microsoft 365 supports the following [Amazon S3 Storage Classes](#):

- Amazon S3 Standard (S3 Standard)
Use this storage class for general-purpose storage of frequently accessed data. Veeam Backup for Microsoft 365 supports this storage class as a target for both backup and backup copy jobs.
- Amazon S3 Standard-Infrequent Access (S3 Standard-IA)
Use this storage class for long-lived, but less frequently accessed data. Veeam Backup for Microsoft 365 supports this storage class as a target for both backup and backup copy jobs.
- Amazon S3 Glacier Instant Retrieval (S3 Glacier Instant Retrieval)
Use this storage class for storing data that is regularly accessed and requires data retrieval in milliseconds. Veeam Backup for Microsoft 365 supports this storage class only as a target for backup copy jobs.
- Amazon S3 Glacier Flexible Retrieval (S3 Glacier Flexible Retrieval)
Use this storage class for storing data that is accessed 1–2 times per year and is retrieved asynchronously. Veeam Backup for Microsoft 365 supports this storage class only as a target for backup copy jobs.
- Amazon S3 Glacier Deep Archive (S3 Glacier Deep Archive)
Use this storage class for storing data that may be rarely accessed. Veeam Backup for Microsoft 365 supports this storage class only as a target for backup copy jobs.

Supported Azure Storage Account Types

Veeam Backup for Microsoft 365 supports different Azure [storage account types](#) for standard and premium performance tiers. Tables in this section list the supported storage account types.

Standard Performance Tier

The following table lists supported storage account types for *Standard Performance Tier*.

Supported Storage Account Type	Supported Services	Supported Access Tiers
General-purpose V2	Blob	Hot, Cool, Archive
General-purpose V1	Blob	N/A
Blob Storage	Blob (block blobs and append blobs only)	Hot, Cool, Archive

NOTE

Veeam Backup for Microsoft 365 uses Azure Blob Storage Archive access tier only as a target for backup copy jobs.

Premium Performance Tier

The following table lists supported storage account types for *Premium Performance Tier*.

Supported Storage Account Type	Supported Services	Supported Access Tiers
Block Blob Storage	Blob (block blobs and append blobs only)	N/A

Permissions

Microsoft Organizations

Veeam Backup for Microsoft 365 uses Veeam Backup account and Azure AD application to establish and maintain connection between Veeam Backup for Microsoft 365 and Microsoft 365 organizations or on-premises Microsoft organizations and perform backup and restore of the organization data.

NOTE

Microsoft has recently renamed Azure Active Directory to Microsoft Entra ID and Azure AD applications to Microsoft Entra applications. However, these entities are still referred to as Azure Active Directory and Azure AD applications both in this guide and the Veeam Backup for Microsoft 365 user interface, and are subject to change in a future release. For more information, see [this Microsoft article](#).

What the product requires depends on a Microsoft organization type and an authentication method used to add a Microsoft 365 organization. The following options are available:

- For on-premises Microsoft organizations, Veeam Backup for Microsoft 365 uses only Veeam Backup account.
- For Microsoft 365 organizations, it depends on an authentication method that you use when adding a particular Microsoft 365 organization.

Depending on configuration of Microsoft 365 organizations and the restrictions on using legacy authentication protocols, you can add organizations using either [modern app-only authentication](#), or [modern authentication method with legacy protocols allowed](#), or [basic authentication method](#).

Consider the following:

- When you add a Microsoft 365 organization using the modern app-only authentication method, Veeam Backup for Microsoft 365 uses only Azure AD application.
- When you add a Microsoft 365 organization using modern authentication method with legacy protocols allowed, Veeam Backup for Microsoft 365 uses both Veeam Backup account and Azure AD application. The product requires MFA-enabled Microsoft 365 user account as Veeam Backup account.
- When you add a Microsoft 365 organization using basic authentication, Veeam Backup for Microsoft 365 uses only Veeam Backup account.

Depending on authentication methods you use, you must grant permissions to Veeam Backup account or Azure AD application, or both entities. For more information, see [Veeam Backup Account Permissions](#) and [Azure AD Application Permissions](#).

Restore Portal

If you allow users to perform [self-service restore](#) using Restore Portal, you must grant permissions to an Azure AD application to ensure users authentication to the portal with their Microsoft 365 user account credentials. For more information, see [Permissions for Authentication to Restore Portal](#).

Azure Archiver Appliance

If you want to use the [Azure archiver appliance](#) when Veeam Backup for Microsoft 365 copies backed-up data between different instances of Azure Blob Storage or to Azure Blob Storage Archive, you must assign the required roles to a user account that you use to create an Azure AD application for the [Microsoft Azure service account](#). For more information, see [Permissions for Azure Archiver Appliance](#).

Amazon S3 Storage

If you want to store Microsoft 365 and on-premises Microsoft organization backups and backup copies in Amazon S3 object storage, you must grant permissions for each Amazon S3 object storage and allow a user account access to Amazon buckets and folders. For more information, see [Amazon S3 Storage Permissions](#).

Azure Blob Storage and Azure Blob Storage Archive

If you want to store Microsoft 365 and on-premises Microsoft organization backups and backup copies in Azure Blob Storage and Azure Blob Storage Archive, you must grant permissions to a user account that you use to access this object storage. For more information, see [Azure Blob Storage Permissions](#).

Veeam Backup Account Permissions

Veeam Backup for Microsoft 365 requires the Veeam Backup account credentials when you add the following Microsoft organizations:

- [Microsoft 365 organizations with modern authentication and legacy protocols](#)
- [Microsoft 365 organization with basic authentication](#)
- [On-premises Microsoft Exchange organizations](#)
- [On-premises Microsoft SharePoint organizations](#)

Veeam Backup account is required to establish and maintain connection between Veeam Backup for Microsoft 365 and Microsoft 365 organizations or on-premises Microsoft organizations and perform backup and restore of the organization data.

Depending on data that you want to protect, you must assign the following roles and permissions to the Veeam Backup account:

- [Microsoft Exchange Data](#)
Roles and permissions required to protect data in Microsoft Exchange organizations.
- [Microsoft SharePoint and OneDrive for Business Data](#)
Roles and permissions required to protect data in Microsoft SharePoint and OneDrive for Business organizations.
- [Microsoft Teams Data](#)
Roles and permissions required to protect Microsoft Teams data.

Microsoft Exchange

The following table lists roles and permissions that must be assigned to the Veeam Backup account to protect data in Microsoft Exchange organizations. Veeam Backup for Microsoft 365 requires these roles and permissions when you add Microsoft 365 organizations using [modern authentication method with legacy protocols allowed](#) or [basic authentication method](#), and on-premises Microsoft organizations.

Consider the following:

- The account you use to add an organization must be a member of this organization.
- The account you use to add an organization is not required to have a mailbox in this organization.
- If you plan to back up public folder mailboxes, the Veeam Backup account must have a valid Exchange Online license and an active mailbox within the Microsoft 365 organization.

NOTE

For more information about permissions required to restore Microsoft Exchange data from backups created by Veeam Backup for Microsoft 365, see [Permissions](#) for Veeam Explorer for Microsoft Exchange.

Role	Description
Role Management	Required to grant the <i>ApplicationImpersonation</i> role.

Role	Description
ApplicationImpersonation	Required to back up Exchange data.
Organization Configuration	Required to manage role assignments.
View-Only Configuration	Required to obtain necessary configuration parameters.
View-Only Recipients	Required to view mailbox recipients.
Mailbox Search or Mail Recipients	Required to back up groups.
Owner	Required to back up and restore public folders.

Granting ApplicationImpersonation Role in PowerShell

For On-Premises Microsoft Exchange Organizations

To grant the *ApplicationImpersonation* role for on-premises Microsoft Exchange organizations, do the following:

1. Connect to the Exchange server. For more information, see [this Microsoft article](#).
2. Run the following cmdlet to grant the role:

```
New-ManagementRoleAssignment -Role ApplicationImpersonation -User "Administrator"
```

For Microsoft 365 Exchange Organizations

To grant the *ApplicationImpersonation* role for Microsoft 365 Exchange organizations, do the following:

1. Connect to the Exchange server:
 - For *Basic Authentication*, see [this Microsoft article](#).
 - For *Modern Authentication*, see [this Microsoft article](#).
2. Run the following cmdlet to grant the role:

```
New-ManagementRoleAssignment -Role ApplicationImpersonation -User user.name@domain.com
```

Checking and Removing ApplicationImpersonation Role in PowerShell

To obtain the list of users whom the *ApplicationImpersonation* role has already been granted, use the following cmdlet (for both on-premises and Online organizations):

```
Get-ManagementRoleAssignment -Role "ApplicationImpersonation"
```

To remove the role, use the following cmdlet (for both on-premises and Online organizations):

```
Get-ManagementRoleAssignment -RoleAssignee "Administrator" -Role ApplicationImpersonation -RoleAssigneeType user | Remove-ManagementRoleAssignment
```

Creating and Configuring New Authentication Policy for Exchange Online Organizations

When you add a Microsoft 365 Exchange organization using either modern authentication method with legacy protocols allowed or basic authentication method, you need to create a new authentication policy to protect Exchange Online data. This policy must have the `AllowBasicAuthPowershell` and `AllowBasicAuthWebService` parameters enabled for the Veeam Backup account. To do this, use the following example:

```
New-AuthenticationPolicy -Name "Allow Basic Auth"  
Set-AuthenticationPolicy -Identity "Allow Basic Auth" -AllowBasicAuthPowershell  
Set-AuthenticationPolicy -Identity "Allow Basic Auth" -AllowBasicAuthWebService  
Set-User -Identity <VeeamBackupAccount> -AuthenticationPolicy "Allow Basic Auth"  
"
```

To back up public folder mailboxes correctly, enable the `AllowBasicAuthAutodiscover` parameter for the created authentication policy by using the following cmdlet:

```
Set-AuthenticationPolicy -Identity "Allow Basic Auth" -AllowBasicAuthAutodiscover
```

Microsoft SharePoint and OneDrive for Business

The following tables list roles and permissions that must be assigned to the Veeam Backup account to protect data in Microsoft SharePoint and OneDrive for Business organizations. Veeam Backup for Microsoft 365 requires these roles and permissions when you add Microsoft 365 organizations using [modern authentication method with legacy protocols allowed](#) or [basic authentication method](#), and on-premises Microsoft organizations.

Consider the following:

- To add Microsoft SharePoint Online organizations, make sure that the *LegacyAuthProtocolsEnabled* parameter is enabled.

To enable this parameter, use the following cmdlet:

```
Set-SPOTenant -LegacyAuthProtocolsEnabled $True
```

For more information about the *Set-SPOTenant* cmdlet, see [this Microsoft article](#).

- The account you use to add an organization must be a member of this organization.

NOTE

For more information about permissions required to restore Microsoft SharePoint data from backups created by Veeam Backup for Microsoft 365, see [Permissions](#) for Veeam Explorer for Microsoft SharePoint.

On-Premises Microsoft SharePoint Organizations

The following table lists roles that must be assigned to the account that you want to use to add on-premises Microsoft SharePoint organizations:

Role	Description
Site Collection Administrator	Required to back up Microsoft SharePoint sites. The account must be a member of the <i>Farm Administrator</i> group.

Microsoft SharePoint Online Organizations

The following table lists roles that must be assigned to the account that you want to use to add Microsoft SharePoint Online organizations:

Role	Description
SharePoint Admin	Required to back up Microsoft SharePoint sites.
View-only Configuration	Required to get a list of available groups and users.
View-Only Recipients	

TIP

You can assign the *Global Admin* role that overrides these roles.

Granting SharePoint Administrator Role in PowerShell

To grant the *SharePoint Administrator* role using PowerShell (for Microsoft SharePoint Online organizations), use the following example:

```
Connect-MsolService
$role=Get-MsolRole -RoleName "SharePoint Administrator"
$accountname="example@domain.com"
Add-MsolRoleMember -RoleMemberEmailAddress $accountname -RoleName $role.Name
```

The `$accountname` variable must be a user UPN (*example@domain.com*).

The MSOL module can be downloaded from [this Microsoft page](#).

Microsoft Teams

To back up Microsoft Teams data, Veeam Backup for Microsoft 365 requires access to the Exchange mailbox of the group associated with a team and to the SharePoint site of this group. Thus, the Veeam Backup account that you use to add an organization using [modern authentication method with legacy protocols allowed](#) or [basic authentication method](#) must have permissions required for backup of Exchange Online and SharePoint Online data. For more information, see [Microsoft Exchange](#) and [Microsoft SharePoint and OneDrive for Business](#).

In addition, the Veeam Backup account that you use to add an organization must meet the following requirements:

- The account must have a Microsoft 365 license that permits access to Microsoft Teams APIs. The minimum sufficient license is Microsoft Teams Exploratory experience. For more information about the Microsoft Teams Exploratory experience, see [this Microsoft article](#).
- The account must have the *Team Administrator* role assigned.

NOTE

Consider the following:

- In case you add an organization in Veeam Backup for Microsoft 365 using the modern authentication method with legacy protocols allowed and specify different accounts to connect to Microsoft Exchange and Microsoft SharePoint, the required license and role must be assigned to the account used to connect to Microsoft SharePoint.
- When you back up Microsoft Teams data in an organization added using the basic authentication method, Veeam Backup for Microsoft 365 adds a service account to every team and then removes it.
- For more information about permissions required to restore Microsoft Teams data from backups created by Veeam Backup for Microsoft 365, see [Permissions](#) for Veeam Explorer for Microsoft Teams.

Azure AD Application Permissions

Veeam Backup for Microsoft 365 requires that you grant permissions to Azure AD applications within the following usage scenarios:

- [Back up](#) and [restore](#) data of your [Microsoft 365 organizations](#).

Permissions of the Azure AD application depend on the authentication method that you plan to use when adding a Microsoft 365 organization. For more information, see the following sections:

- [Permissions for Modern App-Only Authentication](#)
- [Permissions for Modern Authentication and Legacy Protocols](#)

- [Self-service restore](#) using Restore Portal.

If you allow users to perform self-service restore using Restore Portal, they will authenticate to the portal with their Microsoft 365 user account credentials. To ensure such authentication, an Azure AD application must be configured. Veeam Backup for Microsoft 365 automatically grants the required permissions to this Azure AD application or you can grant permissions manually. For more information, see the following sections:

- [Permissions for Authentication to Restore Portal](#)
- [Creating or Configuring Azure AD Application](#)

- [Backup copy](#) to Microsoft Azure Blob Storage.

You can optionally use the [Azure archiver appliance](#) when Veeam Backup for Microsoft 365 copies backed-up data between different instances of Azure Blob Storage or to Azure Blob Storage Archive. To enable usage of the Azure archiver appliance, the Microsoft Azure service account is required. You must assign the required roles to a user account that you use to create an Azure AD application for the Microsoft Azure service account. Veeam Backup for Microsoft 365 automatically grants the required permissions to this Azure AD application or you can grant permissions manually. For more information, see the following sections:

- [Permissions for Azure Archiver Appliance](#)
- [Adding Microsoft Azure Service Account](#)

For more information about permissions in Azure, see [this Microsoft article](#).

Permissions for Modern App-Only Authentication

Tables in this section list permissions for Azure AD applications that are granted automatically by Veeam Backup for Microsoft 365 when you add organizations using the [modern app-only authentication method](#).

If you prefer to use a custom application of your own, make sure to grant all the permissions listed in these tables manually to perform the following operations:

- [Backup](#)
- [Restore Using Device Code Flow](#)
- [Restore Using Application Certificate](#)

NOTE

For a user account that the Azure AD application will use to log in to Microsoft 365, consider the following:

- You must assign the [required roles](#) to this user account.
- If you plan to back up public folder mailboxes, this user account must have a valid Exchange Online license and an active mailbox within the Microsoft 365 organization.

The following sections contain additional instructions that help you to check Office 365 Exchange Online API permissions and configure the Azure AD application settings:

- [Checking Permissions for Office 365 Exchange Online API](#)

Follow this instruction to check Office 365 Exchange Online API permissions in Microsoft Entra ID (formerly Azure Active Directory).

- [Configuring Azure AD Application Settings](#)

Follow this instruction to configure the Azure AD application settings in Microsoft Entra ID (formerly Azure Active Directory) for data restore.

Veeam Backup for Microsoft 365 also requires you to grant permissions to Azure AD applications that you add as backup applications. For more information, see [Backup Application Permissions](#).

Required User Account Roles for Azure AD Applications

Azure AD application uses a user account to log in to Microsoft 365. This user account must be assigned the following roles:

- *Global Administrator* – required for adding organizations with modern app-only authentication, creating backup applications, registering Azure AD application for Restore Portal and creating Azure AD application for the Microsoft Azure service account.
- *ApplicationImpersonation*, and *Global Administrator* or *Exchange Administrator* – required for data restore with Veeam Explorer for Microsoft Exchange.
- *Global Administrator* or *SharePoint Administrator* – required for data restore with Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft OneDrive for Business.
- *Global Administrator* or *Teams Administrator* – required for data restore with Veeam Explorer for Microsoft Teams.
- *Global Administrator* – required for establishing a connection to a service provider in the [Backup as Service for Microsoft 365](#) scenario.
- *Owner* – requires to back up public folder mailboxes in organizations with modern app-only authentication.

Granting Owner Role in PowerShell

To grant the *Owner* role to a user account that the Azure AD application uses to log in to Microsoft 365, do the following:

1. Connect to the Exchange server. For more information, see [this Microsoft article](#).

2. Use the following example to grant the role:

```
$folders = get-publicfolder "\" -recurse
foreach($folder in $folders)
{
Add-PublicFolderClientPermission -Identity $folder.identity -user <user_ac
count> -AccessRights Owner
}
```

Permissions for Backup

All listed permissions are of the *Application* type.

API	Permission name	Exchange Online	SharePoint Online and OneDrive for Business	Microsoft Teams	Description
Microsoft Graph	Directory.Read.All	✓	✓	✓	Querying Azure AD for organization properties, the list of users and groups and their properties.
	Group.Read.All	✓	✓	✓	Querying Azure AD for the list of groups and group sites.
	Sites.Read.All		✓	✓	Querying Azure AD for the list of sites and getting download URLs for files and their versions.
	TeamSettings.ReadWrite.All			✓	Accessing archived teams.

API	Permission name	Exchange Online	SharePoint Online and OneDrive for Business	Microsoft Teams	Description
	ChannelMessage.Read.All			✓	<p>Accessing all Teams public channel messages.</p> <p>Note: This permission is only required if you want to back up team chats using Teams Export APIs. For more information, see Organization Object Types.</p>
	full_access_as_app	✓		✓	Reading mailboxes content.

API	Permission name	Exchange Online	SharePoint Online and OneDrive for Business	Microsoft Teams	Description
Office 365 Exchange Online ¹	Exchange.ManageAsApp	✓			<p>Accessing Exchange Online PowerShell to do the following:</p> <ul style="list-style-type: none"> • Back up public folder and discovery search mailboxes. • Determine object type for shared mailboxes as <i>Shared Mailbox</i>. <p>Note: This permission is required only to back up public folder and discovery search mailboxes as well as determine correctly object type for shared mailboxes starting from Veeam Backup for Microsoft 365 version 7 CP4 (build 7.0.0.3968). This permission works along with the <i>Global Reader</i> role granted to the Azure AD application. For more information, see Granting Global Reader Role to Azure AD Application.</p>
Office 365 SharePoint Online	Sites.FullControl.All		✓	✓	Reading SharePoint sites and OneDrive accounts content.

API	Permission name	Exchange Online	SharePoint Online and OneDrive for Business	Microsoft Teams	Description
	User.Read.All		✓	✓	<p>Reading OneDrive accounts (getting site IDs).</p> <p>Note: This permission is not used to back up Microsoft Teams data, but you must grant it along with SharePoint Online and OneDrive for Business permission to add a Microsoft 365 organization successfully.</p>

You can check permissions for Office 365 Exchange Online API. For more information, see [Checking Permissions for Office 365 Exchange Online API](#).

Granting Global Reader Role to Azure AD Application

Starting from version 7 CP4 (build 7.0.0.3968), Veeam Backup for Microsoft 365 supports backup of public folder and discovery search mailboxes and determines correctly object type for shared mailboxes in Microsoft 365 organizations with modern app-only authentication. To back up these objects, Veeam Backup for Microsoft 365 needs access to Exchange Online PowerShell. To do this, an Azure AD application additionally needs the *Global Reader* role.

To grant the *Global Reader* role to the Azure AD application, do the following:

1. Sign in to the Azure portal.
2. Go to **Microsoft Entra ID > Roles and administrators**.
3. In the **Administrative roles** list, find the **Global Reader** role and click on it.
4. In the **Global Reader** window, click **Add assignments**.
The **Add assignments** wizard runs.
5. In the **Select member(s)** section, click the link.
6. In the **Select a member** window, select the Azure AD application in the list and click **Select**.
The selected application appears in the **Selected member(s)** list.
7. Click **Next** and then **Assign** to finish the wizard.

Permissions for Restore

NOTE

To restore data using Azure AD application, make sure that you configure the Azure AD application settings. For more information, see [Configuring Azure AD Application Settings](#).

Restore Using Device Code Flow

All listed permissions are of the *Delegated* type and required for data restore using Veeam Explorers.

API	Permission name	Exchange Online	SharePoint Online and OneDrive for Business	Microsoft Teams	Description
Microsoft Graph	Directory.Read.All	✓	✓	✓	Querying Azure AD for organization properties, the list of users and groups and their properties.
	Group.ReadWrite.All			✓	Recreating in Azure AD an associated group in case of teams restore.
	Sites.Read.All		✓	✓	Accessing sites of the applications that are installed from the SharePoint store.
	Directory.ReadWrite.All			✓	Setting the preferred data location when creating a new M365 group for a multi-geo tenant in case of teams restore.
	offline_access	✓	✓	✓	Obtaining a refresh token from Azure AD.
Office 365 Exchange Online ¹	EWS.AccessAsUser.All	✓			Accessing mailboxes as the signed-in user (impersonation) through EWS.

API	Permission name	Exchange Online	SharePoint Online and OneDrive for Business	Microsoft Teams	Description
	full_access_as_user	✓			<p>Reading the current state and restoring mailboxes content.</p> <p>This permission is only required when you add an organization in legacy Microsoft Azure <i>Germany</i> region.</p>
Office 365 SharePoint Online	AllSites.FullControl		✓	✓	Reading the current state and restoring SharePoint sites and OneDrive accounts content.
	User.Read.All		✓		<p>Resolving OneDrive accounts (getting site IDs).</p> <p>Note: This permission is not required to restore SharePoint Online data.</p>

You can check permissions for Office 365 Exchange Online API. For more information, see [Checking Permissions for Office 365 Exchange Online API](#).

Restore Using Application Certificate

All listed permissions are of the *Application* type and required for the following scenarios of data restore:

- Data restore by Veeam Explorer for Microsoft Exchange using modern authentication with Azure AD application certificate. For more information, see the [Restore to Microsoft 365 Organizations](#) section of the Veeam Explorers User Guide.
- Data restore using Restore Portal.

- Data restore through REST API and PowerShell.

API	Permission name	Exchange Online	SharePoint Online and OneDrive for Business	Microsoft Teams	Description
Microsoft Graph	Directory.Read.All	✓		✓	Querying Azure AD for organization properties, the list of users and groups and their properties.
	Group.ReadWrite.All		✓	✓	Recreating in Azure AD an associated group in case of a deleted team site restore. Note: This permission is only required for restore of SharePoint site data through REST API and PowerShell.
	Sites.Read.All		✓	✓	Accessing sites of the applications that are installed from the SharePoint store.
	Directory.ReadWrite.All			✓	Setting the preferred data location when creating a new M365 group for a multi-geo tenant in case of teams restore.
Office 365 Exchange Online ¹	full_access_as_app	✓			Reading the current state and restoring mailboxes content.
Office 365 SharePoint Online	Sites.FullControl.All		✓	✓	Reading the current state and restoring SharePoint sites and OneDrive accounts content.

API	Permission name	Exchange Online	SharePoint Online and OneDrive for Business	Microsoft Teams	Description
	User.Read.All		✓		Resolving OneDrive accounts (getting site IDs). Note: This permission is not required to restore SharePoint Online data.

¹You can check permissions for Office 365 Exchange Online API. For more information, see [Checking Permissions for Office 365 Exchange Online API](#).

Checking Permissions for Office 365 Exchange Online API

To check Office 365 Exchange Online API permissions, do the following:

1. Sign in to the Azure portal.
2. Go to **Microsoft Entra ID > App registrations**, and select an application.
3. Select **API permissions > Add a permission > APIs my organization uses**.
4. Select *Office 365 Exchange Online* API in the list, check its permissions and configure them if needed.

Configuring Azure AD Application Settings

For data restore using Azure AD application, do the following to configure the application settings in Microsoft Azure:

1. Sign in to the Azure portal.
2. Go to **Microsoft Entra ID > App registrations**, and select an application.
3. Select **Authentication > Advanced settings > Allow public client flows** and set the **Enable the following mobile and desktop flows** option to **Yes**. For more information on application settings, see [this Microsoft article](#).

Keep in mind that this option is unavailable in Microsoft Azure for legacy *Germany* region. In this region, you must register Azure AD applications used for backup and restore as applications of the *Public client/Native* type.

4. Select **Authentication > Platform configurations > Add a platform > Configure platforms > Mobile and desktop applications** and specify a redirect URI for the application. For more information, see [this Microsoft article](#).

When creating a new Azure AD application automatically, Veeam Backup for Microsoft 365 specifies *http://localhost* as a redirect URI.

Backup Application Permissions

The following table lists permissions for Azure AD applications that you [add as backup applications](#).

NOTE

Using multiple applications may impact the performance of your production SharePoint environment. This functionality will be deprecated in future versions of Veeam Backup for Microsoft 365.

All listed permissions are of the *Application* type and required for data backup.

API	Permission name	Exchange Online	SharePoint Online and OneDrive for Business	Microsoft Teams	Description
Microsoft Graph	Sites.Read.All		✓		Getting download URLs for files and their versions. Note: In the Microsoft Azure <i>China</i> region, the Sites.ReadWrite.All permission is used instead.
Office 365 SharePoint Online	Sites.FullControl.All		✓		Reading SharePoint sites and OneDrive accounts content.
	User.Read.All		✓		Reading OneDrive accounts (getting site IDs).

Permissions for Modern Authentication and Legacy Protocols

The following table lists permissions that must be granted to Azure AD applications to perform a backup for [Microsoft 365 organizations with modern authentication and legacy protocols](#).

All listed permissions are of the *Application* type and required for data backup.

API	Permission name	Exchange Online	SharePoint Online and OneDrive for Business	Microsoft Teams	Description
Microsoft Graph	Directory.Read.All	✓	✓	✓	Querying Azure AD for organization properties, the list of users and groups and their properties.

API	Permission name	Exchange Online	SharePoint Online and OneDrive for Business	Microsoft Teams	Description
	Group.Read.All	✓	✓	✓	Querying Azure AD for the list of groups and group sites.
	TeamSettings.ReadWrite.All			✓	Accessing archived teams.
	Sites.Read.All		✓		Accessing sites of the applications that are installed from the SharePoint store.
Office 365 Exchange Online	full_access_as_app	✓		✓	Reading mailboxes content.
Office 365 SharePoint Online	Sites.FullControl.All		✓	✓	Reading SharePoint sites and OneDrive accounts content.
	User.Read.All		✓	✓	Reading OneDrive accounts (getting site IDs).

Permissions for Authentication to Restore Portal

The following table lists permissions for Azure AD applications that are granted automatically by Veeam Backup for Microsoft 365 when you [configure the Restore Portal settings](#).

If you prefer to use a custom application of your own, make sure to grant all the permissions listed in this table manually.

All listed permissions are of the *Delegated* type.

API	Permission name	Description
Microsoft Graph	User.Read	Sign in and read user profile.

API	Permission name	Description
<Azure AD application>	access_as_user	<p>Obtain an access token on behalf of the user to implement On-Behalf-Of flow.</p> <p>For more information about On-Behalf-Of flow, see this Microsoft article.</p> <p>For more information on how to expose a web API, see this Microsoft article.</p>

Permissions for Azure Archiver Appliance

Veeam Backup for Microsoft 365 allows you to use the Azure archiver appliance when the product copies backed-up data between different instances of Azure Blob Storage or to Azure Blob Storage Archive. To enable usage of the Azure archiver appliance, the Microsoft Azure service account is required.

A user account that you use to create Azure AD application for the Microsoft Azure service account must be assigned the following roles:

- *Application Administrator*
- *Owner* of the Microsoft Azure subscription that you selected for the Microsoft Azure service account

Make sure that this user account is not a *Contributor* of the Microsoft Azure subscription that you selected for the Microsoft Azure service account.

If you prefer to use a custom application of your own for the Microsoft Azure service account, the following are minimal required permissions for this Azure AD application:

```
{
  "properties": {
    "roleName": "APPLICATION_MINIMAL_PERMISSIONS",
    "description": "APPLICATION_MINIMAL_PERMISSIONS",
    "assignableScopes": [
      "/subscriptions/*"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.ApiManagement/service/subscriptions/read",
          "Microsoft.Storage/storageAccounts/read",
          "Microsoft.Resources/subscriptions/resourceGroups/read",
          "Microsoft.Resources/subscriptions/resourceGroups/write",
          "Microsoft.Compute/virtualMachines/*",
          "Microsoft.Network/virtualNetworks/read",
          "Microsoft.Network/virtualNetworks/write",
          "Microsoft.Network/virtualNetworks/subnets/join/action",
          "Microsoft.Network/networkSecurityGroups/read",
          "Microsoft.Network/networkSecurityGroups/write",
          "Microsoft.Network/networkSecurityGroups/join/action",
          "Microsoft.Network/publicIPAddresses/read",
          "Microsoft.Network/publicIPAddresses/write",
          "Microsoft.Network/publicIPAddresses/delete",
          "Microsoft.Network/publicIPAddresses/join/action",
          "Microsoft.Network/networkInterfaces/*",
          "Microsoft.Compute/disks/delete"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```

Amazon S3 Storage Permissions

This section contains permissions required by Veeam Backup for Microsoft 365 for Amazon S3 object storage in the following usage scenarios:

- Data backup

Veeam Backup for Microsoft 365 supports Amazon S3 Standard and Amazon S3 Standard-Infrequent Access storage classes as a target for backup jobs.

- Backup copy

Veeam Backup for Microsoft 365 supports the following storage classes as a target for backup copy jobs:

- Amazon S3 Standard
- Amazon S3 Standard-Infrequent Access
- all Amazon S3 Glacier storage classes

For more information about supported Amazon S3 storage classes, see [Supported Amazon S3 Storage Classes](#).

NOTE

Make sure the account you are using has access to Amazon S3 buckets and folders.

For each Amazon S3 object storage that Veeam Backup for Microsoft 365 uses regardless of the usage scenario, the following permissions must be granted:

- For EC2 instance (Amazon archiver appliance)

```
[
  "ec2:CreateTags",
  "ec2:DescribeInstances",
  "ec2:StartInstances",
  "ec2:RunInstances",
  "ec2:StopInstances",
  "ec2:TerminateInstances",
  "ec2:CreateKeyPair",
  "ec2>DeleteKeyPair",
  "ec2:DescribeVpcs",
  "ec2:CreateVpc",
  "ec2>DeleteVpc",
  "ec2:DescribeSubnets",
  "ec2:CreateSubnet",
  "ec2>DeleteSubnet",
  "ec2:DescribeRouteTables",
  "ec2:CreateRouteTable",
  "ec2>DeleteRouteTable",
  "ec2:CreateRoute",
  "ec2>DeleteRoute",
  "ec2:DescribeInternetGateways",
  "ec2:CreateInternetGateway",
  "ec2:AttachInternetGateway",
  "ec2>DeleteInternetGateway",
  "ec2:DescribeSecurityGroups",
  "ec2:CreateSecurityGroup",
  "ec2>DeleteSecurityGroup",
  "ec2:DescribeConversionTasks",
  "ec2:DescribeInstanceTypes",
  "ec2:AuthorizeSecurityGroupIngress",
  "ssm:GetParameter"
]
```

- For Amazon S3 object storage

```
[
  "s3:ListAllMyBuckets",
  "s3:GetBucketLocation"
]
```

- For a bucket

```
[  
  "s3:ListBucket",  
  "s3:ListBucketMultipartUploads",  
  "s3:GetBucketObjectLockConfiguration",  
  "s3:GetBucketVersioning",  
  "s3:ListBucketVersions"  
]
```

- For an object

```
[  
  "s3:PutObject",  
  "s3:GetObject",  
  "s3:DeleteObject",  
  "s3:AbortMultipartUpload",  
  "s3:ListMultipartUploadParts",  
  "s3:RestoreObject",  
  "s3:GetObjectVersion",  
  "s3:GetObjectRetention",  
  "s3:PutObjectRetention",  
  "s3:DeleteObjectVersion"  
]
```


IAM Policy Example

The following is the example of an IAM policy:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3Repository",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketVersioning",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts",
        "s3:RestoreObject",
        "s3:GetObjectVersion",
        "s3:GetObjectRetention",
        "s3:PutObjectRetention",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Sid": "EC2ArchiverAppliance",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags",
        "ec2:DescribeInstances",
        "ec2:StartInstances",
        "ec2:RunInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:CreateKeyPair",
        "ec2:DeleteKeyPair",
        "ec2:DescribeVpcs",
        "ec2:CreateVpc",
        "ec2:DeleteVpc",
        "ec2:DescribeSubnets",
        "ec2:CreateSubnet",
        "ec2:DeleteSubnet",
        "ec2:DescribeRouteTables",
        "ec2:CreateRouteTable",
        "ec2:DeleteRouteTable",
        "ec2:CreateRoute",
        "ec2:DeleteRoute",
        "ec2:DescribeInternetGateways",
        "ec2:CreateInternetGateway",
        "ec2:AttachInternetGateway",
        "ec2:DeleteInternetGateway",

```

```
        "ec2:DescribeSecurityGroups",
        "ec2:CreateSecurityGroup",
        "ec2>DeleteSecurityGroup",
        "ec2:DescribeConversionTasks",
        "ec2:DescribeInstanceTypes",
        "ec2:AuthorizeSecurityGroupIngress",
        "ssm:GetParameter"
    ],
    "Resource": "arn:aws:ec2:::*"
}
]
```

For more information on how to create an IAM policy, see [this Veeam KB article](#). For more information on permissions, see [this Amazon article](#).

Azure Blob Storage Permissions

Veeam Backup for Microsoft 365 requires only a Microsoft Azure Blob storage account and shared key to use Azure Blob Storage and Azure Blob Storage Archive as a target for backup and backup copy jobs.

Permissions Changelog

This section contains information about changes in permissions required for Veeam Backup for Microsoft 365 7a comparing to version 6.0.

Azure AD Application Permissions

The following table lists changes in permissions for modern app-only authentication:

API	Permission name	Type	Usage	Description	Status
Microsoft Graph	Directory.ReadWrite.All	Application	Restore	Setting the preferred data location when creating a new M365 group for a multi-geo tenant in case of teams restore.	new
Office 365 Exchange Online	Exchange.ManageAsApp	Application	Backup	Accessing Exchange Online PowerShell. Note: This permission is required only to back up public folder and discovery search mailboxes as well as determine correctly object type for shared mailboxes starting from Veeam Backup for Microsoft 365 version 7 CP4 (build 7.0.0.3968). This permission works along with the <i>Global Reader</i> role granted to the Azure AD application. For more information, see Permissions for Backup and Granting Global Reader Role to Azure AD Application .	new

Azure Blob Storage and Azure Blob Storage Archive

If you want to use the Azure archiver appliance when Veeam Backup for Microsoft 365 copies backed-up data between different instances of Azure Blob Storage or to Azure Blob Storage Archive, you must assign the required roles to a user account that you use to create Azure AD application for the Microsoft Azure service account.

The changes are:

- A user account must have the *Application Administrator* role instead of *Global Administrator*.
- Minimal required permissions for a custom Azure AD application are added.

For more information, see [Permissions for Azure Archiver Appliance](#).

If you want to store Microsoft 365 and on-premises Microsoft organization backups and backup copies in Azure Blob Storage and Azure Blob Storage Archive, you must grant permissions to a user account that you use to access this object storage. For more information, see [Azure Blob Storage Permissions](#).

Amazon S3 Object Storage

If you want to store Microsoft 365 and on-premises Microsoft organization backups and backup copies in Amazon S3 object storage, you must grant permissions for each Amazon S3 object storage and allow a user account access to Amazon buckets and folders. For more information, see [Supported Amazon S3 Storage Classes](#) and [Amazon S3 Storage Permissions](#).

Considerations and Limitations

This section lists considerations and known limitations in Veeam Backup for Microsoft 365 7a.

NOTE

For the complete list of known issues and limitations in Veeam Backup for Microsoft 365 7a, see [Release Notes](#).

For limitations in Veeam Backup for Microsoft 365 functionality when protecting organizations with modern app-only authentication, see [this Veeam KB article](#).

Infrastructure

- *Veeam Backup for Microsoft 365 REST API Service*, *Veeam Backup for Microsoft 365 Service* and *Veeam Backup Proxy for Microsoft 365 Service* must be started using the *Local System* account.
- You cannot change the Veeam Backup for Microsoft 365 server name or the server domain without resetting the configuration.
- System date and time in the UTC format must be the same on all machines with the Veeam Backup for Microsoft 365 components installed.
- If the organization has multiple domains, they must be configured as a mesh to cross authenticate to download content from all domains with the service account. For more information, see [this Microsoft article](#).
- Veeam Backup for Microsoft 365 does not support encryption at-rest for the following JET-based backup repositories:
 - A local directory on a backup proxy server.
 - Direct Attached Storage (DAS) connected to the backup proxy server.
 - Storage Area Network (SAN).
 - Network Attached Storage (SMB shares version 3.0 or later).
- For Outlook for Microsoft 365, only the *Semi-Annual Enterprise Channel* is supported. For more information, see [this Microsoft article](#).
- If the Veeam Backup for Microsoft 365 console and the Veeam Backup for Microsoft 365 server are deployed on different machines, make sure that the server is trusted for delegation. For more information, see [this Microsoft article](#).
- If any of the machines with any of the Veeam Backup for Microsoft 365 components has been renamed (or its FQDN has been changed), or any machine has been added to a different domain, then all the components become unavailable to each other. If any of the listed has occurred on a server that acts as a backup proxy server, then such a server becomes *Offline* in the Veeam Backup for Microsoft 365 console. To make a server available, re-add it. For more information, see [Adding Backup Proxy Servers](#).
- IPv6 is not supported for Microsoft Azure *China* region.
- If you roll back a successful automatic update of the remote *Veeam Backup for Microsoft 365 Console* and *PowerShell* components, the Veeam Backup for Microsoft 365 server will not re-update these components.

- Installing *Veeam Backup for Microsoft 365 REST API Service* on a machine running *Veeam Backup Proxy for Microsoft 365 Service* is not supported.

Microsoft 365 organizations

- Adding Microsoft 365 organizations using modern authentication method with legacy protocols allowed is not supported for Microsoft Azure *China* region.
- Adding Microsoft 365 organizations using modern app-only authentication is not supported for legacy Microsoft Azure *Germany* region.
- Microsoft Teams service is not supported for organizations in Microsoft Azure *China* and legacy Microsoft Azure *Germany* regions. For more information about Azure *Germany*, see [this Microsoft article](#).
- Backup of team chats using Teams Export APIs is not supported for Microsoft organizations in Microsoft Azure *China*, legacy *Germany*, *US Government GCC* and *US Government GCC High* regions.
- Email notifications about backup and backup copy job results may not work properly in Microsoft Azure *China* and legacy Microsoft Azure *Germany* regions.

Backup Repositories

General

If you already backed up team chats using Teams Export APIs, you must not change a backup proxy server where backups are stored to another backup proxy server for which usage of Teams Export APIs for team chats backup is not enabled yet.

JET-Based Backup Repositories

To save data in JET-based backup repositories, Veeam Backup for Microsoft 365 uses Extensible Storage Engine (ESE) databases, also known as JET Blue.

For storage systems that you can add to the Veeam Backup for Microsoft 365 backup infrastructure, consider the following:

- **Block Storage Systems including Direct Attached Storage (DAS)**
 - Primary Storage Hardware Systems both with and without deduplication or compression are supported. If the storage system uses compression or deduplication, this storage system and its operating system must be listed on the Certified for Windows Server list. For more information, see [this Microsoft article](#).
 - Software Defined Storage Systems with deduplication or compression are not supported.
 - For Microsoft Windows operating system or other operating systems, built-in deduplication of the file system is not supported.
 - A symbolic link that is configured as a mapped drive is not supported.
 - Storage volumes that host backup repositories must be formatted with NTFS or ReFS.
 - A 3rd party encryption software is not supported for backups in backup repositories. This may lead to unpredictable system behavior and inevitable data loss.

- **Backup Target Deduplication Storage**
 - Based on the format of the used Microsoft JET database, deduplication backup storage appliances are not supported.
- **Network Attached Storage (SMB Shares)**
 - SMB shares version 3.0 are only supported when they are within the Microsoft Exchange Storage definition. For more information, see [this Microsoft article](#).
 - NFS shares are not supported.

Object Storage

- Veeam Backup for Microsoft 365 does not support the *\$root* container in Azure Blob storage.
- Veeam Backup for Microsoft 365 does not support Lifecycle policy in data management.
- S3 Compatible device that you add to Veeam Backup for Microsoft 365 must be fully compatible with the AWS S3 operations and support AWS S3 Signature Version 4 standard. For more information about authentication requests, see [this Amazon article](#).
- Veeam Backup for Microsoft 365 allows you to move data from a local backup repository to object storage, but not vice versa. For more information, see the [Move-VBOEntityData](#) section of the Veeam Backup for Microsoft 365 PowerShell Reference.
- Veeam Backup for Microsoft 365 does not support the *Versioning* feature for Amazon S3 buckets and S3 Compatible buckets unless *Object Lock* is enabled for buckets and immutability is enabled for object storage.
- Veeam Backup for Microsoft 365 does not support the *Versioning* feature for Azure storage accounts unless immutability is enabled for object storage.
- Veeam Backup for Microsoft 365 supports only object storage migrated using native Azure or AWS services. Migration of object storage using different applications may lead to the corruption of data blobs.
- Veeam Backup for Microsoft 365 cannot correctly process data in object storage whose structure was changed using a 3rd party application.

Backup

General

- Project Web Apps are not supported for backup.
- On-premises service accounts cannot be used for multi-factor authentication.
- Backup of a Microsoft 365 tenant organization is not supported if the initial domain of the organization was changed.
- Backup of dynamic distribution groups is not supported for Microsoft 365 organizations with modern app-only authentication. Members of dynamic distribution groups cannot be resolved.

Exchange Data

- Backup of *In-Place Hold Items* is not supported for on-premises Microsoft Exchange 2013.

- To back up public folder mailboxes, the Veeam Backup account must have a valid Exchange Online license and an active mailbox within the Microsoft 365 organization.
- Starting from version 7 CP4 (build 7.0.0.3968), Veeam Backup for Microsoft 365 supports backup of public folder and discovery search mailboxes and determines correctly object type for shared mailboxes in Microsoft 365 organizations with modern app-only authentication. To back up these objects, Veeam Backup for Microsoft 365 needs access to Exchange Online PowerShell. To do this, an Azure AD application additionally needs the *Exchange.ManageAsApp* permission and the *Global Reader* role. For more information, see [Permissions for Backup](#) and [Granting Global Reader Role to Azure AD Application](#).
- To back up user mailboxes, make sure that a mailbox has a valid Microsoft 365 license. Otherwise, such unlicensed mailbox will not be backed up.
- Veeam Backup for Microsoft 365 backs up public folders that are located under the *IPM_SUBTREE* folder only.
- You can select only the root public mailbox when backing up public mailboxes. The child folders of the selected public mailbox will be backed up as well.
- If you modify a retention policy tag for a folder, Veeam Backup for Microsoft 365 will perform full synchronization of that folder during the subsequent backup job session. For more information, see [this Microsoft article](#).
- When backing up Microsoft Exchange mailboxes, Veeam Backup for Microsoft 365 does not create a new version of an item if the *Read/Unread* property of such item was changed. That said, the *Read/Unread* property of each of the backed-up items always remains exactly the same as it was during the initial backup.
- Veeam Backup for Microsoft 365 does not back up permissions for sharing mailbox folders and Calendar.

SharePoint and OneDrive Data

- To back up SharePoint and OneDrive for Business objects, make sure that a user account has a valid Microsoft 365 license with SharePoint plan enabled. Otherwise, a backup job will fail with the following error: "*User %name% does not have a valid Microsoft 365 license with SharePoint plan enabled*".
- A SharePoint Site Collection hierarchy is not supported if the root site was not configured. Make sure to configure the root site in advance using a SharePoint site template of your choice. Otherwise, the following error occurs: "*Error: Failed to find web template ID for: STS#-1. This organization account might be missing a valid SharePoint license. Web configuration is not complete*".
- If a SharePoint item has several versions with identical *owshiddenversion* values, only the latest version of this item is backed up, all the rest versions are skipped from processing.
- Veeam Backup for Microsoft 365 may not backup OneNote notebooks if their size is greater 2 GB. For more information, see [this Microsoft article](#).
- When you perform backup of SharePoint data, Veeam Backup for Microsoft 365 does not back up the following objects:
 - External SharePoint lists.
For more information, see [this Microsoft article](#).
 - SharePoint folder attachments.
 - SharePoint site collection recycle bin.

Microsoft Teams Data

- As part of Microsoft Teams data backup, Veeam Backup for Microsoft 365 backs up only the following types of channel tabs: Website, Planner, Word, Excel, PowerPoint, Visio, PDF, Document Library, OneNote, SharePoint, Stream, Forms, Power BI, Power Automate (ex Flow) and Azure DevOps.
- Backup of team chats using Teams Export APIs is limited to backup of public channel posts and is only supported for Microsoft 365 organizations with modern app-only authentication. For more information, see [this Veeam KB article](#).
- When you perform backup of Microsoft Teams data, Veeam Backup for Microsoft 365 does not back up the following objects:

- Private and shared channels.
- One-on-one and group chats.

For more information about chats in Microsoft Teams, see [this Microsoft article](#).

You can use Veeam Explorer for Microsoft Exchange to explore data from user mailboxes and view chat messages as MSG files. Keep in mind that it works only for backups that have been created before January 31, 2023. For more information, see [this Microsoft article](#).

- Audio and video calls.
- Video recordings saved to Microsoft Stream.
- Contacts.
- Calendar: information about meetings and meeting chats.
- Code snippets in posts.
- Banner notifications in posts.
- Data of applications added as channel tabs (such as Website, Planner, Word, Excel, PowerPoint, Visio, PDF, Document Library, OneNote, SharePoint, Stream, Forms, Power BI, Power Automate and Azure DevOps) and other 3rd party applications if their data does not reside in the SharePoint document library of the team.

Restore

NOTE

For more information about limitations that apply when you restore data from backups using Veeam Explorers, see the following sections of the Veeam Explorers User Guide:

- [Veeam Explorer for Microsoft Exchange](#)
- [Veeam Explorer for Microsoft SharePoint](#)
- [Veeam Explorer for Microsoft Teams](#)
- SharePoint sites with a red X over the symbol mean that there is an empty sector of the template and supported content is available in the subsites.
- Microsoft Teams messages cannot be restored directly back to Teams.
- Veeam Backup for Microsoft 365 restores public folders that are located under the *IPM_SUBTREE* folder only.

- Bulk restore (restore of multiple objects) is not supported for public folder mailboxes. Use the regular per-object restore instead.
- Bulk restore of Exchange mailboxes can be performed to the original location only. Use a single mailbox, folder or item restore if you want to restore such objects to another location.
- To restore *In-Place Hold Items* or *Litigation Hold Items* to the original location, consider the following:
 - Restore of *In-Place Hold Items* is not supported for on-premises Microsoft Exchange Server 2013 due to EWS limitations.
 - To restore *In-Place Hold Items* of Exchange 2016/2019 mailboxes, these mailboxes must have *In-Place Hold* enabled and applied at least once with the *DiscoveryHolds* system folder creation. Otherwise, restore of *In-Place Hold Items* will fail with the following error: "*Failed to restore In-Place Hold Items. Restore of In-Place Hold Items into Exchange 2013 is not supported*".

For more information about enabling *In-Place Hold* and *Litigation Hold*, see [this Microsoft article](#).

- Restore of OneNote notebooks from backups of Microsoft SharePoint, Microsoft OneDrive for Business and Microsoft Teams data for organizations with modern app-only authentication is not supported.
- If the size of a OneNote notebook is greater 2 GB, Veeam Backup for Microsoft 365 saves this OneNote notebook as a folder with OneNote items.
- Restore of OneNote tabs from backups of Microsoft Teams data may fail with the "*Configuration size exceeded. Provided: '4117' bytes MaxAllowed: '4096' bytes*" error if the OneNote tab name includes non-Latin or special characters.
- If a SharePoint site includes a hidden list, such list is not displayed in Veeam Explorer for Microsoft SharePoint after a site backup and thus, cannot be restored.
- Before restoring team data using Veeam Explorer for Microsoft Teams or team sites using Veeam Explorer for Microsoft SharePoint for a tenant organization with modern app-only authentication, make sure that a user account used for authorization has access to the root SharePoint site of this tenant organization.
- Restore of an organization data from a backup repository extended with object storage is not supported if such organization is not added to the Veeam Backup for Microsoft 365 infrastructure.
- When restoring team sites, Veeam Backup for Microsoft 365 does not restore team site owners or Microsoft 365 group members.

Licensing and License Types

Licensing in Veeam Backup for Microsoft 365 is based on user accounts whose data you back up. Each protected user account consumes one Veeam license unit.

The Veeam license units are consumed by the following objects included to a user account:

- **Microsoft Exchange Online and on-premises Microsoft Exchange mailboxes**
Such a mailbox can be a personal mailbox, an Online Archive mailbox or both – you will only need one Veeam license unit per object.
- **Microsoft OneDrive for Business account**
Consider that OneDrive (without *for Business*) is an independent storage service and is not supported by Veeam Backup for Microsoft 365.
- **Microsoft SharePoint Online and on-premises Microsoft SharePoint personal sites**
A personal SharePoint site of a licensed user consumes one Veeam license unit.

The Veeam license units are consumed by mailboxes, OneDrive for Business accounts and SharePoint personal sites for which at least one restore point has been created within the last 31 days. If an object was not backed up for 31 days, its license unit is automatically revoked.

NOTE

When you plan a number of units in your Veeam license, consider the following:

- All users in your Microsoft 365 subscription or on-premises deployment that are members of a backed-up team or have access to a backed-up team, communication, collaboration and other non-personal SharePoint sites must be licensed. If you have a hybrid SharePoint deployment (on-premises Microsoft SharePoint and SharePoint Online), and the same user has access to both, then only one Veeam license is required.
- If you back up only Microsoft Teams objects or non-personal SharePoint sites, the Veeam license units are not consumed by Veeam Backup for Microsoft 365.

The following objects do not require the Veeam license and do not consume units from it:

- **Microsoft Teams objects**
These objects do not consume units from the Veeam license.
- **Group and non-personal SharePoint sites**
These sites do not consume units from the Veeam license.
- **Shared, resource, group and public folder mailboxes**
These mailboxes do not consume units from the Veeam license if such mailboxes do not have a Microsoft 365 license assigned.
- **External SharePoint users**
An external SharePoint user is a user from outside your Microsoft 365 subscription who has access to one or more sites, files or folders. External authenticated users are limited to basic collaboration tasks, and external anonymous users can edit or view specific documents if they have specific permissions.

- **Guest Microsoft Teams users**

A guest team user is a user from outside your Microsoft 365 subscription who has access to a backed-up team.

NOTE

For more information on Microsoft licenses required to back up user mailboxes, public folder mailboxes, SharePoint and OneDrive for Business objects, see [Considerations and Limitations](#).

License Types

Veeam Backup for Microsoft 365 supports the following types of licenses:

- [Subscription License](#)

Paid, fully-functional license that expires at the end of the subscription term. The subscription license term is normally 1-5 years from the contract start date (depending on the subscription length).

- [Rental License](#)

Paid, fully-functional license that expires at the end of the contract. The rental license term is normally 1 month from the contract start date. The license expiration date is the last day of the month. This license type is distributed only to service providers.

- [Not For Resale License](#)

Free, fully-functional license that can be used for product demonstration, training and education. This license is not for resale or other commercial use.

- [Evaluation License](#)

Free, fully-functional license that can be used for evaluation and testing purposes only.

NOTE

After you install Veeam Backup for Microsoft 365, you will be prompted to provide a license. You can dismiss this step and continue using the product without any [license installed](#). In this case, the product will operate in the *Community Edition* mode that allows you to process up to 10 user accounts, up to 1 TB of Microsoft SharePoint data and up to 10 teams in all organizations. *Community Edition* mode is not limited in time and does not have limitations in terms of application functionality.

Subscription License

Subscription License is a paid and fully-functional license that expires at the end of the subscription term. The subscription license term is normally 1-5 years from the contract start date (depending on the subscription length).

Subscription license is available in the *M365* and *M365Suite* license packages. Veeam ONE monitoring is available if the *M365Suite* license package is installed.

For more information on the compatibility of Veeam Backup for Microsoft 365 licenses with Veeam ONE licenses, see the [Compatibility with Veeam Backup for Microsoft 365 Licenses](#) section of the Veeam ONE Deployment Guide and [this Veeam KB article](#).

License Expired

For purpose of renewal, Veeam Backup for Microsoft 365 grants a grace period of 1 month after the license expiration. During this period, the product functionality is not limited. After this period, Veeam Backup for Microsoft 365 stops processing all user accounts in all organizations and terminates all scheduled jobs with failure. Veeam Backup for Microsoft 365 sends you a notification message to inform you that the license is either about to expire or has expired.

The restore abilities will continue to function regardless of whether your license has expired or not.

License Exceeded

Additional processing of no more than 10 user accounts or 10% of the license count (whichever is greater) is granted if you exceed the license limit.

Starting from version 7 CP4 (build 7.0.0.3968), Veeam Backup for Microsoft 365 doubles grace limit after the following conditions are met:

- You selected the **Update license automatically** check box in the **License Information** window. For more information, see [Installing and Updating License](#).
- At least one usage report has been successfully sent from the Veeam Backup for Microsoft 365 server to Veeam during the last month. Veeam Backup for Microsoft 365 sends this report automatically.

As a result, Veeam Backup for Microsoft 365 allows you to exceed the license limit by up to 20 user accounts or up to 20% of the license count (whichever is greater).

Extra user accounts that go beyond the exceeded license limit are not processed. Veeam Backup for Microsoft 365 displays a warning message to notify you that the license limit is exceeded.

Veeam Backup for Microsoft 365 allows you to process extra user accounts according to the FIFO queue logic (that is, "first in – first out"). Extra accounts are queued for processing. Once the unconsumed license unit appears, the first extra user account from the queue obtains this license unit and will be backed up.

The grace period is not limited and lasts during the whole term of the subscription.

Rental License

Rental License is a paid and fully-functional license that expires at the end of the contract. The rental license term is normally 1 month from the contract start date. The license expiration date is the last day of the month. This license type is distributed only to service providers.

In contrast to Subscription license, Rental license is available only in the *M365* license package. For Veeam Backup for Microsoft 365 with this type of license, Veeam ONE monitoring is available if Veeam ONE also has Rental license.

For more information on the compatibility of Veeam Backup for Microsoft 365 licenses with Veeam ONE licenses, see the [Compatibility with Veeam Backup for Microsoft 365 Licenses](#) section of the Veeam ONE Deployment Guide and [this Veeam KB article](#).

New User

When Veeam Backup for Microsoft 365 backs up a user account for the first time, such user account obtains the *new user* status until the first day of the following month. During this period, user accounts with the *new user* status do not consume the rental license units.

For example, you want to back up three user accounts A, B and C and the first session of a backup job is scheduled on January 13, 2022. After the backup session, these user accounts will be given the *new user* status until February 1, 2022. On February 1, 2022, the *new user* status for each of these accounts will be automatically reset. After the *new user* status is reset, upon the next backup job session these user accounts start consuming the rental license immediately.

You can avoid consuming the rental license by user accounts with the *new user* status that you no longer want to process. For example, you may not want to continue backing up the user account B. To do this, remove this account from the backup job processing list before Veeam Backup for Microsoft 365 resets automatically the *new user* status for this account. Starting from the following month, user accounts A and C will start consuming the rental license, but the user account B will not.

License Expired

For purpose of renewal, Veeam Backup for Microsoft 365 grants a grace period of 2 months after the license expiration. During this period, the product functionality is not limited. After this period, Veeam Backup for Microsoft 365 stops processing all user accounts in all organizations and terminates all scheduled jobs with failure. Veeam Backup for Microsoft 365 sends you a notification message to inform you that the license is either about to expire or has expired.

The restore abilities will continue to function regardless of whether your license has expired or not.

License Exceeded

Additional processing of no more than 20 user accounts or 20% of the license count (whichever is greater) is granted if you exceed the license limit.

Starting from version 7 CP4 (build 7.0.0.3968), Veeam Backup for Microsoft 365 doubles grace limit after the following conditions are met:

- You selected the **Update license automatically** check box in the **License Information** window. For more information, see [Installing and Updating License](#).
- At least one usage report has been successfully sent from the Veeam Backup for Microsoft 365 server to Veeam during the last month. Veeam Backup for Microsoft 365 sends this report automatically.

As a result, Veeam Backup for Microsoft 365 allows you to exceed the license limit by up to 40 user accounts or up to 40% of the license count (whichever is greater).

Extra user accounts that go beyond the exceeded license limit are not processed. Veeam Backup for Microsoft 365 displays a warning message to notify you that the license limit is exceeded.

Veeam Backup for Microsoft 365 allows you to process extra user accounts according to the FIFO queue logic (that is, "first in – first out"). Extra accounts are queued for processing. Once the unconsumed license unit appears, the first extra user account from the queue obtains this license unit and will be backed up.

The grace period is 2 months. After this period, Veeam Backup for Microsoft 365 stops processing extra user accounts (in FIFO queue); no more extra accounts will be queued for processing.

The restore abilities will continue to function regardless of exceeding the grace limit and the grace period state.

Managing Monthly Usage Report

When using a rental license, service providers can manually submit a monthly usage report. Such reports contain information on processed user accounts per each Microsoft organization added to the Veeam Backup for Microsoft 365 backup infrastructure.

Veeam Backup for Microsoft 365 displays the **Monthly Usage Report** notification message during the 5-day period starting from the first day of each month. During this period, the notification message appears every time you launch Veeam Backup for Microsoft 365 until you send your monthly usage report to Veeam. After you submit the report, Veeam Backup for Microsoft 365 stops displaying the notification message.

If you do not submit a monthly usage report to Veeam during the 5-day period, Veeam Backup for Microsoft 365 stops displaying the notification message and sends the report to Veeam automatically. Sending the monthly usage report to Veeam from the Veeam Backup for Microsoft 365 user interface becomes unavailable, but you can review the report – Veeam Backup for Microsoft 365 automatically saves it to the

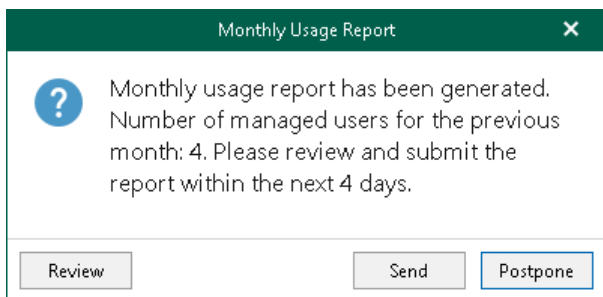
`%ProgramData%\Veeam\Backup365\Reports` folder in PDF and CSV formats.

NOTE

If Veeam Backup for Microsoft 365 is integrated with *Veeam Service Provider Console*, the product will not notify you about the necessity to submit a monthly usage report. For more information, see [Integration with Veeam Products](#).

When the **Monthly Usage Report** window appears, do one of the following:

- Click **Review** to open the **Monthly Usage Report** window and review details of a monthly usage report.
- Click **Send** to send the report immediately to Veeam.
- Click **Postpone** to postpone your actions to the next launch of the product.



Reviewing and Sending Reports

To review details of a monthly usage report, in the **Monthly Usage Report** window, click **Review**.

By default, Veeam Backup for Microsoft 365 lists all backed-up user accounts of all Microsoft organizations added to the product scope.

Before sending a monthly usage report, Veeam Backup for Microsoft 365 allows you to review a list of backed-up user accounts. You can do the following:

- Select a particular Microsoft organization from the drop-down list to view all backed-up user accounts of this organization.
- Use the search field to find user accounts of the selected organization.
- Exclude user accounts from the monthly usage report. To do this, select a user account in the list and click **Remove**. Veeam Backup for Microsoft 365 will prompt you to provide the removal reason.

TIP

To reset changes introduced in the report, click **Reset**.

You can save your monthly usage report as a PDF or CSV file. To do this, click **Save As** and specify a location.

To submit a monthly usage report to Veeam, click **Send**.

Account	Organization Name	Last Processed
AdeleV@qwbs.onmicrosoft.com	abc.onmicrosoft.com	2/27/2023 2:00...
administrator@qwbs.onmicrosoft.com	abc.onmicrosoft.com	2/27/2023 2:00...
DiegoS@qwbs.onmicrosoft.com	abc.onmicrosoft.com	2/27/2023 2:00...
IsaiahL@qwbs.onmicrosoft.com	abc.onmicrosoft.com	2/27/2023 2:00...
JohannaL@qwbs.onmicrosoft.com	abc.onmicrosoft.com	2/27/2023 2:00...

Not For Resale License

Not For Resale (NFR) license is a free and fully-functional license that can be used for product demonstration, training and education.

License Expired

Within a month before the expiration date, you will receive a notification message stating that your license is about to expire. During this period, the product functionality will not be limited by any means. After your license expires, Veeam Backup for Microsoft 365 stops processing of all user accounts.

The restore abilities will continue to function regardless of whether your license has expired or not.

License Exceeded

Processing of user accounts that exceed the allowed license count is not possible.

Evaluation License

Evaluation License is a free and fully-functional license that can be used for evaluation and testing purposes only.

License Expired

Within a month before the expiration date, you will receive a notification message stating that your license is about to expire. During this period, the product functionality will not be limited by any means. After your license expires, Veeam Backup for Microsoft 365 stops processing of all user accounts.

The restore abilities will continue to function regardless of whether your license has expired or not.

License Exceeded

Processing of user accounts that exceed the allowed license count is not possible.

Integration with Veeam Products

Integration with Veeam Service Provider Console

Veeam Backup for Microsoft 365 supports integration with *Veeam Service Provider Console* that monitors licenses consumed by Veeam Backup for Microsoft 365 servers and the state of the product services. Integration is available starting from Veeam Service Provider Console version 6.0. For more information, see the [Integration with Veeam Backup for Microsoft 365](#) section of the Veeam Service Provider Console Guide for Service Providers.

Integration with Veeam ONE

Starting from version 12.0, Veeam ONE Client offers advanced functionality for monitoring Veeam Backup for Microsoft 365 infrastructure and data protection operations in the managed virtual environment. For more information, see the [Veeam Backup for Microsoft 365 Monitoring](#) section of the Veeam ONE Monitoring Guide.

NOTE

Consider the following:

- Veeam ONE monitoring is available if Veeam Backup for Microsoft 365 has Subscription license with the *M365Suite* license package.
- Veeam ONE monitoring is not supported for on-premises and hybrid Microsoft organizations.
- For Veeam Backup for Microsoft 365 with Rental license, Veeam ONE monitoring is available if Veeam ONE also has Rental license.
- To support integration with Veeam ONE after upgrading Veeam Backup for Microsoft 365 to version 7, you can either wait 7 days for the automatic license package update or update the current license manually, or install a new license. For more information, see [Installing and Updating License](#).

For more information on the compatibility of Veeam Backup for Microsoft 365 licenses with Veeam ONE licenses, see the [Compatibility with Veeam Backup for Microsoft 365 Licenses](#) section of the Veeam ONE Deployment Guide and [this Veeam KB article](#).

Organization Cache Database

To ensure integration, Veeam Service Provider Console and Veeam ONE get information from an *organization cache database* created by Veeam Backup for Microsoft 365.

Veeam Backup for Microsoft 365 uses an organization cache database to store information about all restore points created for Microsoft 365 organizations. Data is saved to the `%ProgramData%\Veeam\Backup365\Controller.sqlite` database file.

To index all objects in Microsoft 365 organizations with modern app-only authentication, Veeam Backup for Microsoft 365 uses the `Controller.sqlite` database as well. For more information about synchronization of Microsoft organization objects with the organization cache database, see the [Synchronization of Organization Objects](#) section of REST API Reference.

NOTE

Veeam Backup for Microsoft 365 does not save information about restore points created for retrieval jobs in the `Controller.sqlite` database.

Deployment

To start working with Veeam Backup for Microsoft 365, you must deploy the solution to your environment. For more information about Veeam Backup for Microsoft 365 architecture and deployment scenarios, see [Veeam Backup for Microsoft 365 Architecture](#).

Consider the following:

- If you have been participating in the public beta testing of Veeam Backup for Microsoft 365, make sure to uninstall the pre-release (BETA) versions of Veeam Backup for Microsoft 365 and Veeam Explorers.
- To use the solution in hybrid Exchange deployment or on-premises organizations with SPN and Kerberos authentication, make sure to install Veeam Backup for Microsoft 365 on a server that is located within the domain with the source Microsoft Exchange server.
- The solution can be deployed to virtual or physical machines or directly to cloud platforms such as Microsoft Azure or Amazon Web Services (AWS).
- Veeam Backup for Microsoft 365 REST API component can be deployed either on the Veeam Backup for Microsoft 365 server or on a separate machine. Deployment of the Veeam Backup for Microsoft 365 REST API component on a separate machine decreases the load on the backup infrastructure when exploring and restoring data from backups using Restore Portal. For more information, see [Installing REST API](#), [Configuring REST API and Restore Portal on Separate Machine](#) and [Data Restore Using Restore Portal](#).

Downloading Installation Package

You can download the latest version of the `Veeam.Backup365.iso` file – the Veeam Backup for Microsoft 365 installation image – from the official [Veeam website](#).

The `Veeam.Backup365.iso` file includes the following folders and files:

- `Backup`. This folder includes the `Veeam.Backup365.msi` file.
- `Explorers`. This folder includes MSI files that install Veeam Explorers:
 - `VeeamExplorerForExchange.msi` – installs Veeam Explorer for Microsoft Exchange.
For more information, see [Veeam Explorer for Microsoft Exchange](#).
 - `VeeamExplorerForSharePoint.msi` – installs Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft OneDrive for Business.
For more information, see [Veeam Explorer for Microsoft SharePoint](#) and [Veeam Explorer for Microsoft OneDrive for Business](#).
 - `VeeamExplorerForTeams.msi` – installs Veeam Explorer for Microsoft Teams.
For more information, see [Veeam Explorer for Microsoft Teams](#).
- [Optional] `Patches`. If exists, this folder includes MSP files that Windows uses to install patches along with the Veeam Backup for Microsoft 365 and Veeam Explorers installation.
- `Redistr`. This folder includes Microsoft .NET Framework installation file.
- `Setup`. This folder includes the *End User Software License Agreement* and *3rd party software notices and information* documents, `Veeam.Archiver.Autorun.exe`, and other files required for the installation and operation of Veeam Backup for Microsoft 365.
- `autorun.inf` – includes the setup information.
- `Veeam.Setup.exe` – launches the Veeam Backup for Microsoft 365 installation wizard.

Installing Veeam Backup for Microsoft 365

This installation scenario allows you to install Veeam Backup for Microsoft 365 along with Veeam Explorers on a physical or virtual Windows-based machine. After completing the installation process, this machine will perform the role of the Veeam Backup for Microsoft 365 server.

The wizard deploys the following components of Veeam Backup for Microsoft 365:

- Services:
 - *Veeam Backup for Microsoft 365 Service*

Coordinates all operations performed by the product, adds and manages other backup infrastructure components as well as controls global settings for the backup infrastructure.
 - *Veeam Backup Proxy for Microsoft 365 Service*

Manages backup proxy servers and backup repositories.
 - *Veeam Backup for Microsoft 365 REST API Service*

Processes REST API commands. This service is disabled by default and can be enabled. For more information, see [REST API Settings](#).

Restore Portal is deployed along with REST API on the same machine. Restore Portal is a web-based solution for self-service restore of backed-up data. Restore Portal uses REST API to communicate with the Veeam Backup for Microsoft 365 server. For more information, see [Data Restore Using Restore Portal](#).
- *Veeam Backup for Microsoft 365 Console*

Provides an interface that allows users to interact with the Veeam Backup for Microsoft 365 server and backup infrastructure components.
- Veeam Explorers

Set of instruments that comes as part of Veeam Backup for Microsoft 365 and allows you to restore or export your data from backups.

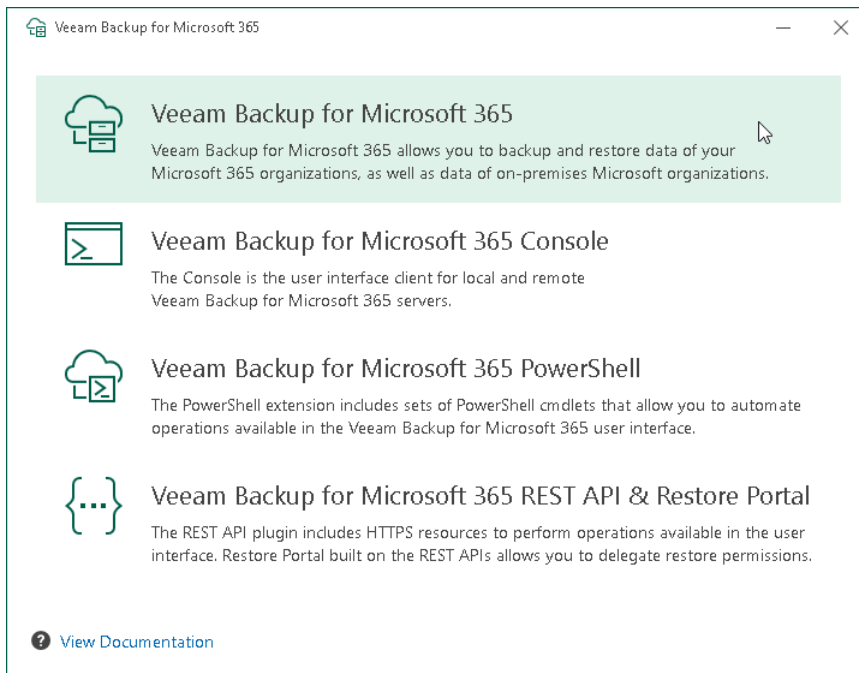
To install Veeam Backup for Microsoft 365 along with Veeam Explorers, do the following:

1. Download the Veeam Backup for Microsoft 365 installation package. For more information, see [Downloading Installation Package](#).
2. Open the `Veeam.Backup365.iso` file and run the `Veeam.Setup.exe` file.

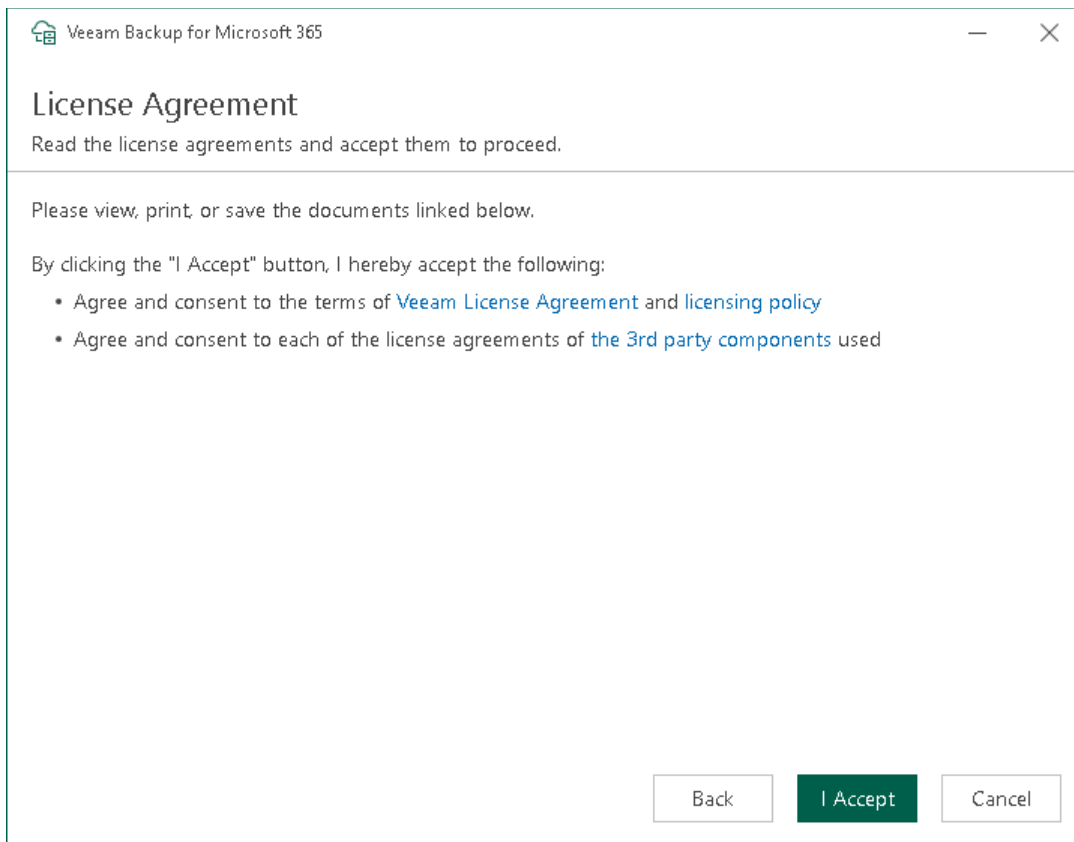
3. On the splash screen, click **Install**.



4. Click **Veeam Backup for Microsoft 365**.



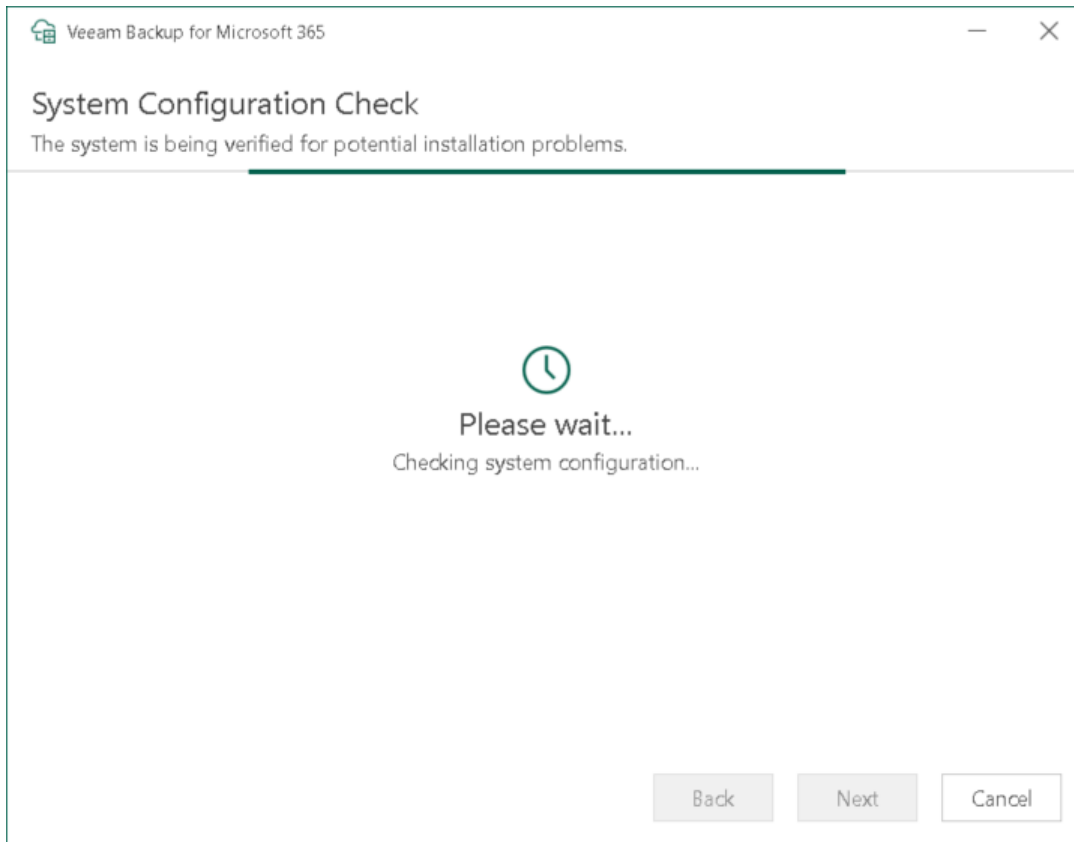
5. At the **License Agreement** step, click the links to read the following documents: *End User Software License Agreement*, *Licensing policy* and *3rd party software notices and information*. To accept the license agreements and continue installing Veeam Backup for Microsoft 365, click **I Accept**.



6. At the **System Configuration Check** step, wait until the wizard checks the system configuration to find the potential installation problems. If the wizard detects problems, you will be prompted to fix the issues to continue the installation.

NOTE

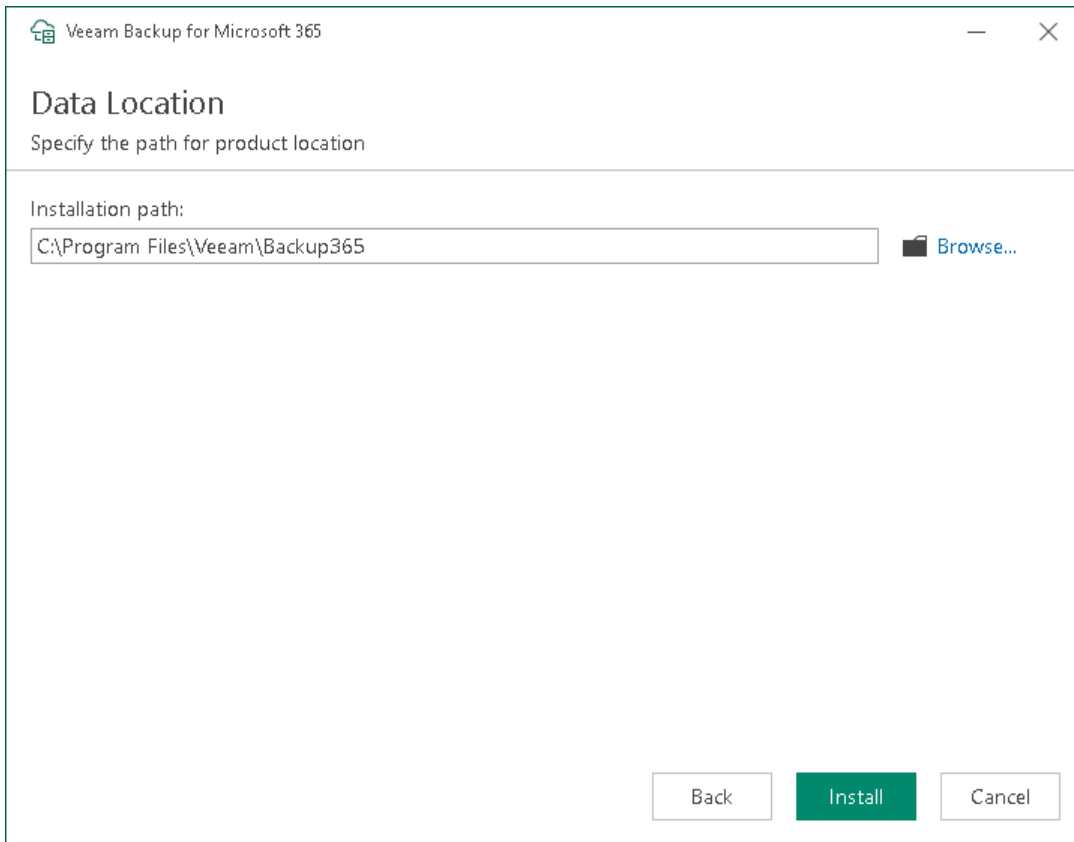
If problems are not detected, the **System Configuration Check** step will be skipped.



7. At the **Data Location** step, specify the installation folder.

By default, all Veeam Backup for Microsoft 365 components are installed to the `C:\Program Files\Veeam\Backup365` folder. To install to a different location, click **Browse** and specify a folder.

Veeam Explorers are installed to the C:\Program Files\Veeam\Backup and Replication\Explorers folder. Keep in mind that you cannot specify a different location for Veeam Explorers.



8. Click **Install**.
9. Wait for the installation process to complete and click **Finish** to exit the wizard.

Installing REST API

This installation scenario allows you to install the Veeam Backup for Microsoft 365 REST API component on a separate physical or virtual Windows-based machine. After completing the installation process, this machine will perform the role of the Veeam Backup for Microsoft 365 REST API server.

Restore Portal is deployed along with REST API on the same machine. Restore Portal is a web-based solution for self-service restore of backed-up data. Restore Portal uses REST API to communicate with the Veeam Backup for Microsoft 365 server. For more information, see [Data Restore Using Restore Portal](#).

Deployment of the Veeam Backup for Microsoft 365 REST API component on a separate machine decreases the load on the backup infrastructure when exploring and restoring data from backups using Restore Portal.

Consider the following:

- Before you begin to deploy the Veeam Backup for Microsoft 365 REST API server on a separate machine, check [system requirements](#).
- If you want to restore your backed-up data using Restore Portal in different regions, you must use a separate installation of the Veeam Backup for Microsoft 365 REST API component and a separate Azure AD application in each Microsoft Azure region.

NOTE

After you installed the Veeam Backup for Microsoft 365 REST API component on a separate machine, you must configure the REST API and Restore Portal settings. It is required to establish communication and data exchange between Veeam Backup for Microsoft 365, *Veeam Backup for Microsoft 365 REST API Service* and Restore Portal. For more information, see [Configuring REST API and Restore Portal on Separate Machine](#).

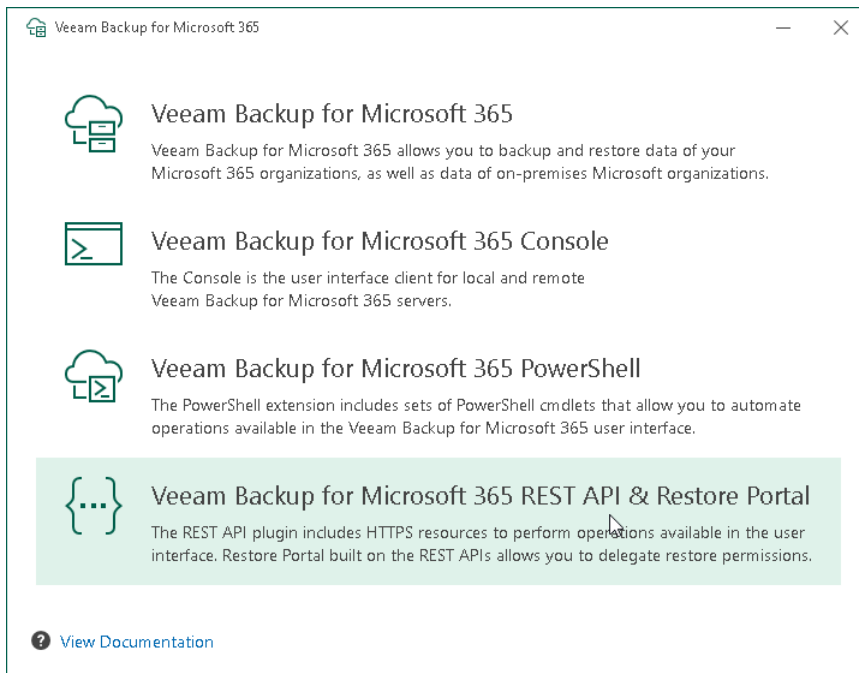
To install the Veeam Backup for Microsoft 365 REST API component on a separate machine, do the following:

1. Download the Veeam Backup for Microsoft 365 installation package. For more information, see [Downloading Installation Package](#).
2. Open the `Veeam.Backup365.iso` file and run the `Veeam.Setup.exe` file.

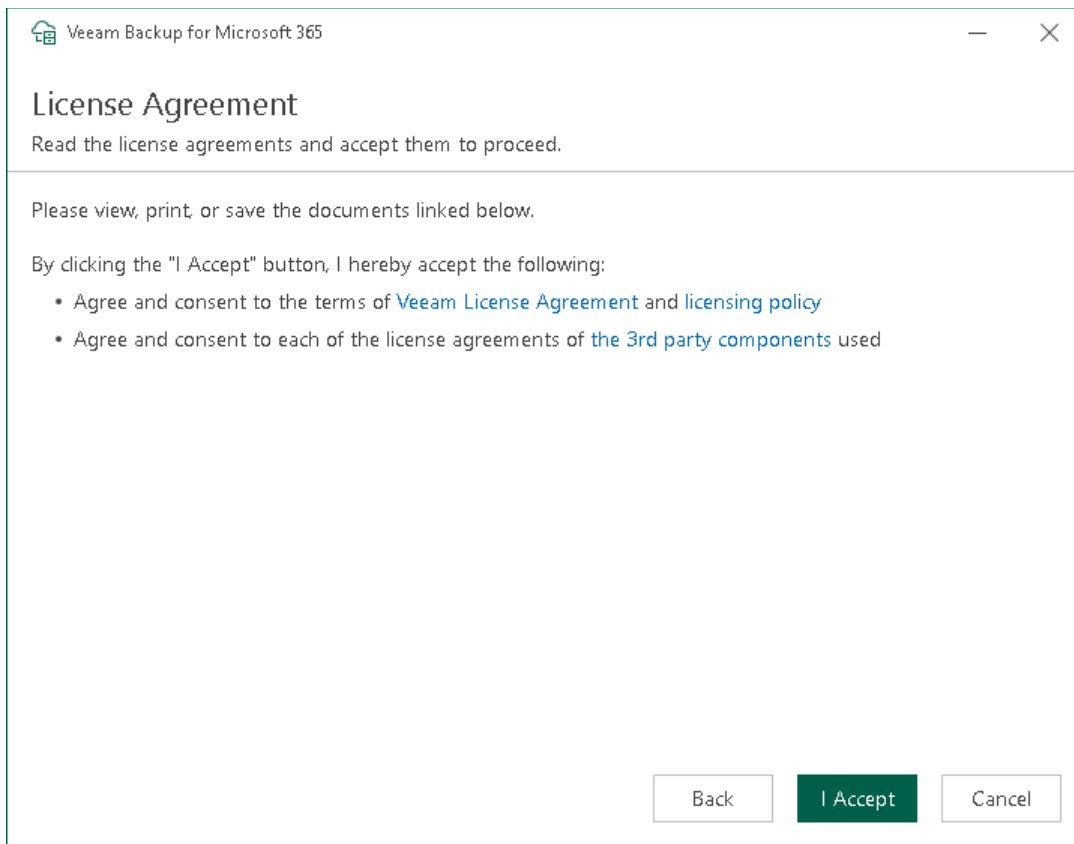
3. On the splash screen, click **Install**.



4. Click **Veeam Backup for Microsoft 365 REST API & Restore Portal**.



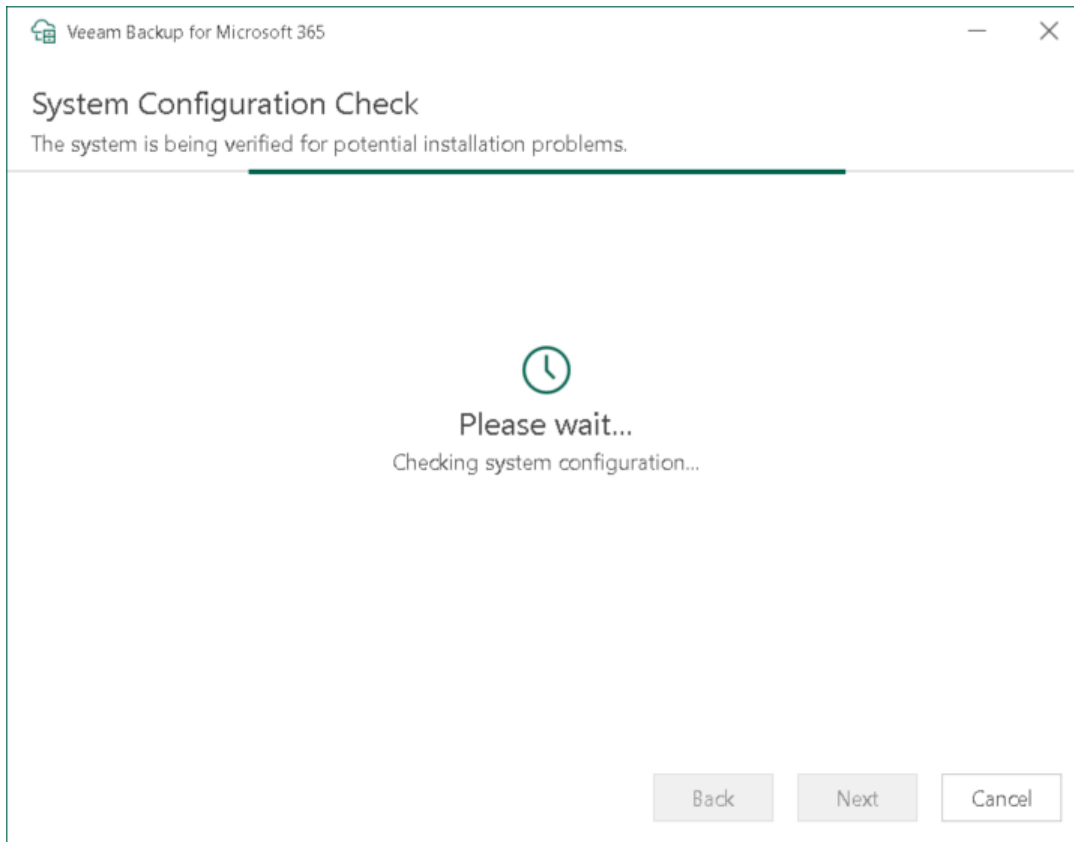
- At the **License Agreement** step, click the links to read the following documents: *End User Software License Agreement*, *Licensing policy* and *3rd party software notices and information*. To accept the license agreements and continue installing Veeam Backup for Microsoft 365, click **I Accept**.



- At the **System Configuration Check** step, wait until the wizard checks the system configuration to find the potential installation problems. If the wizard detects problems, you will be prompted to fix the issues to continue the installation.

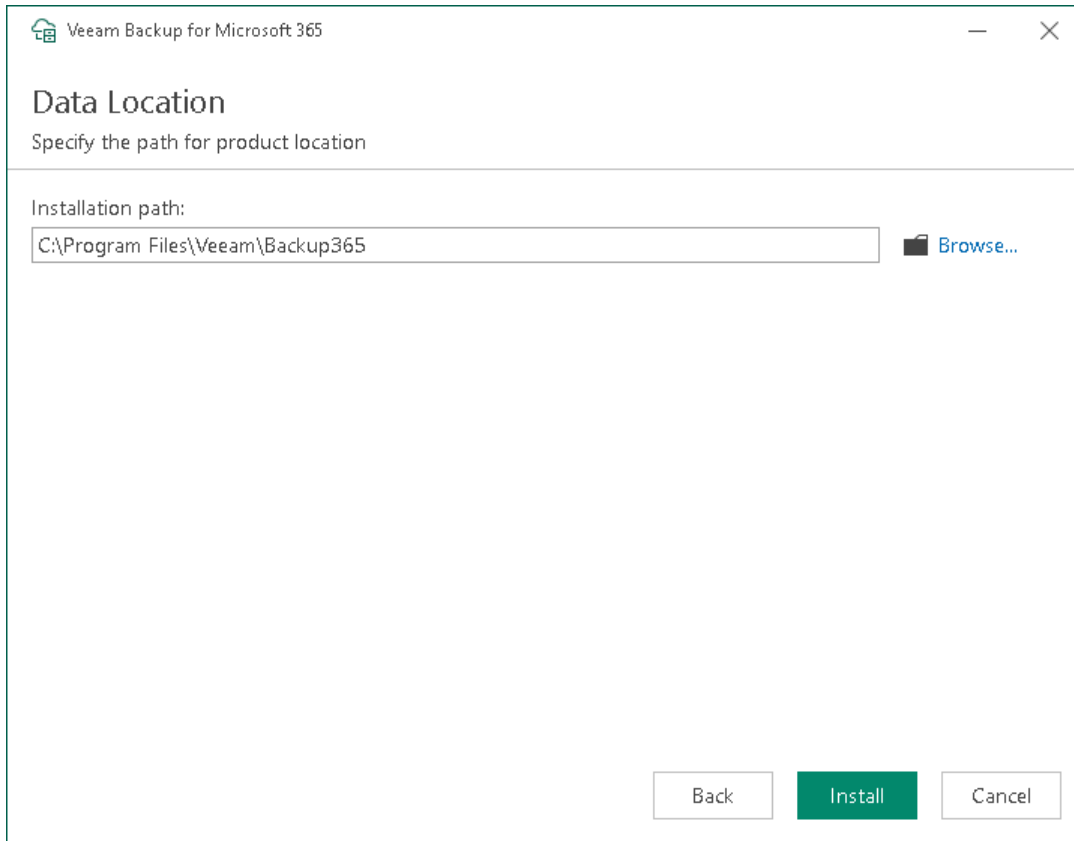
NOTE

If problems are not detected, the **System Configuration Check** step will be skipped.



7. At the **Data Location** step, specify the installation folder.

By default, Veeam Backup for Microsoft 365 REST API component is installed to the `C:\Program Files\Veeam\Backup365` folder. To install to a different location, click **Browse** and specify a folder.



8. Click **Install**.
9. Wait for the installation process to complete and click **Finish** to exit the wizard.

Installing Veeam Explorers

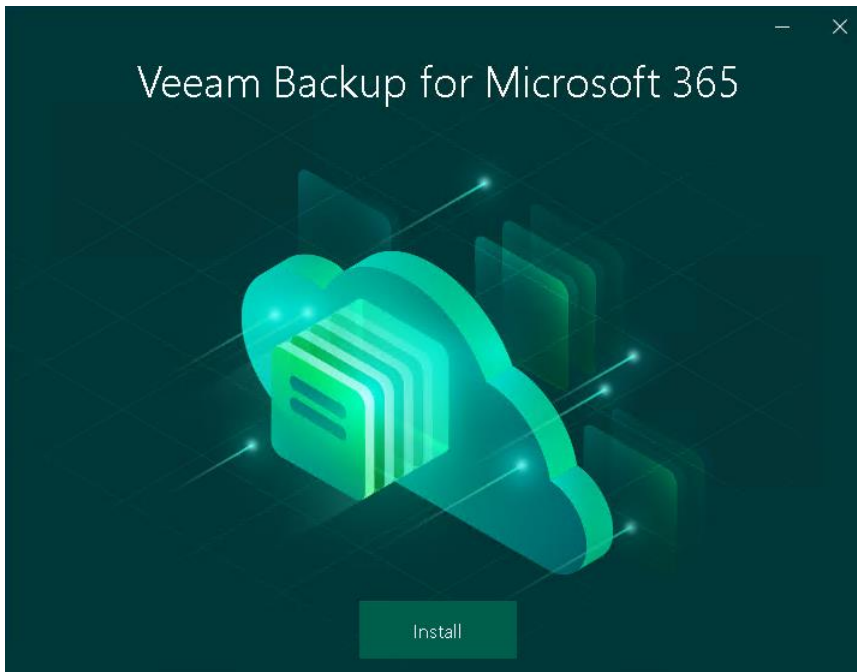
This installation scenario allows you to install Veeam Explorers when configuring *Backup as a Service for Microsoft 365* for tenants. For more information, see [For Tenants](#).

NOTE

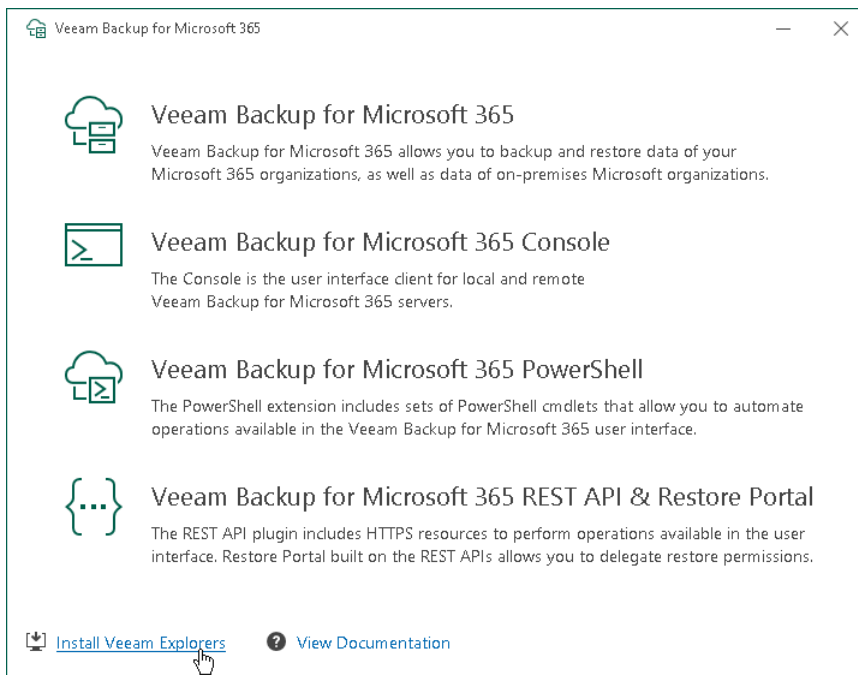
You can install Veeam Explorers individually only on a server running Veeam Backup & Replication.

To install Veeam Explorers on a server with Veeam Backup & Replication, do the following:

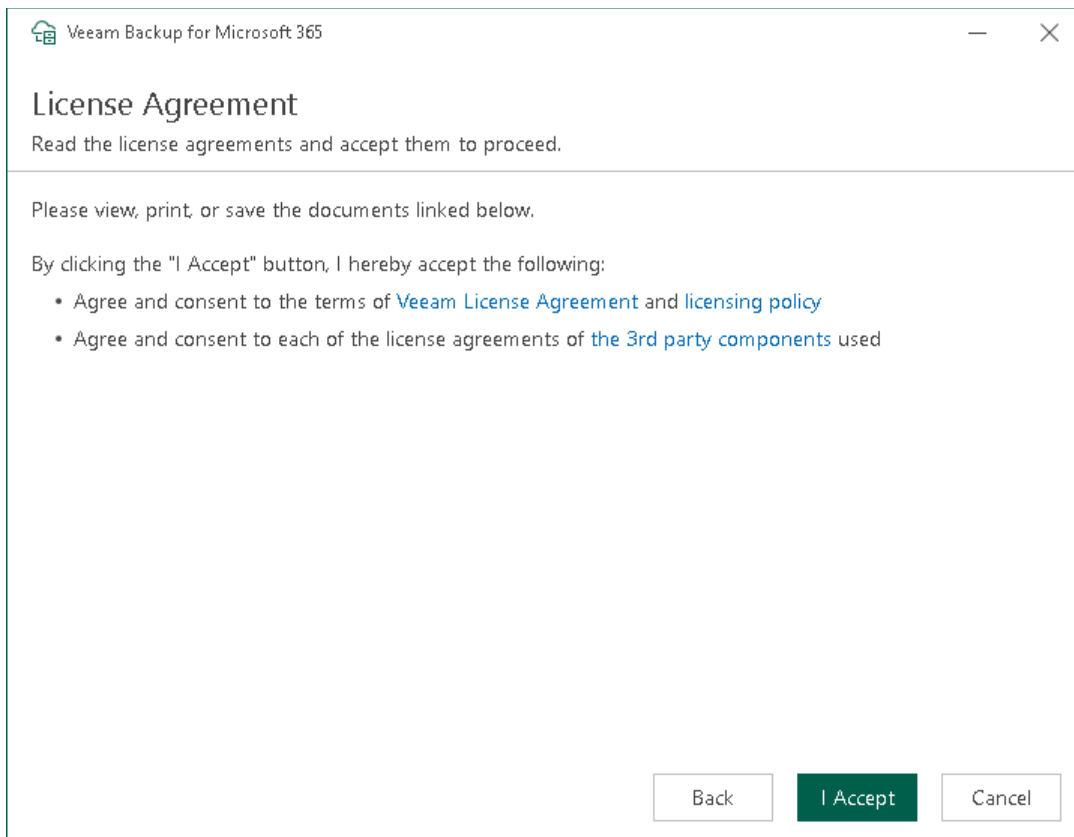
1. Download the Veeam Backup for Microsoft 365 installation package. For more information, see [Downloading Installation Package](#).
2. Open the `Veeam.Backup365.iso` file and run the `Veeam.Setup.exe` file.
3. On the splash screen, click **Install**.



4. Click the **Install Veeam Explorers** link. This link is available only if you run the installation wizard on a server with Veeam Backup & Replication.



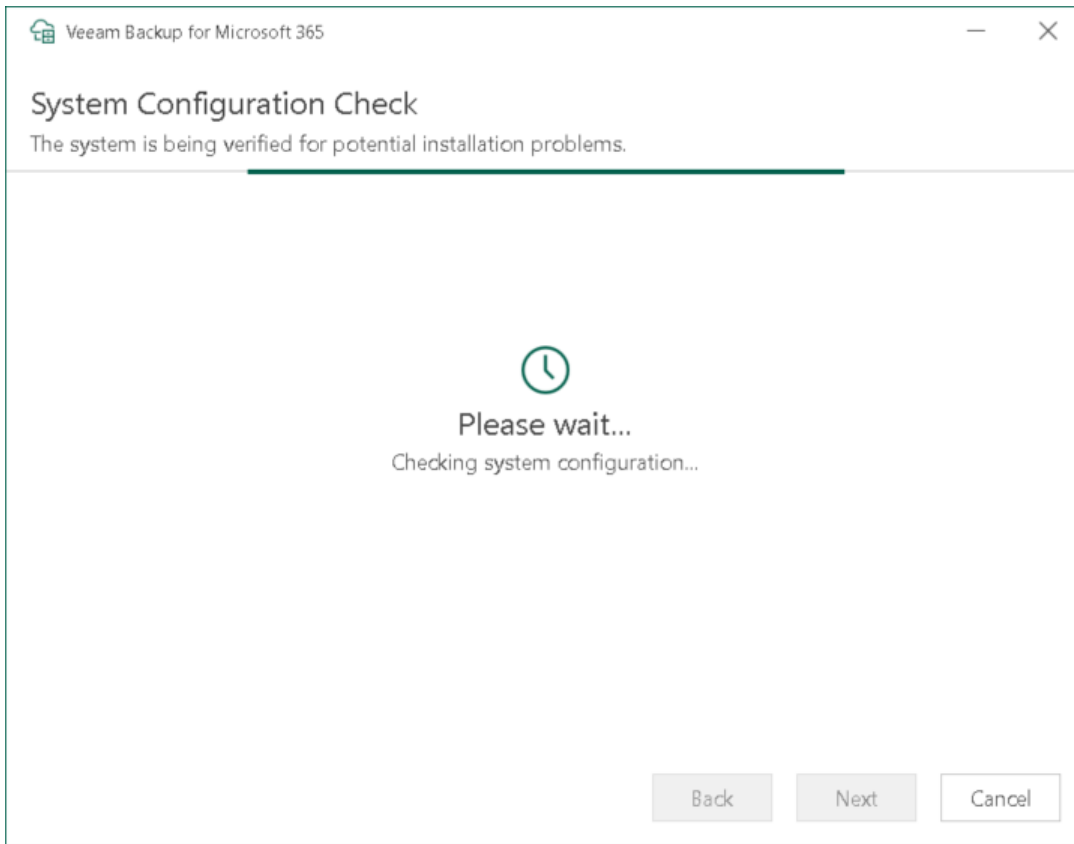
5. At the **License Agreement** step, click the links to read the following documents: *End User Software License Agreement*, *Licensing policy* and *3rd party software notices and information*. To accept the license agreements and continue installing Veeam Backup for Microsoft 365, click **I Accept**.



6. At the **System Configuration Check** step, wait until the wizard checks the system configuration to find the potential installation problems. If the wizard detects problems, you will be prompted to fix the issues to continue the installation.

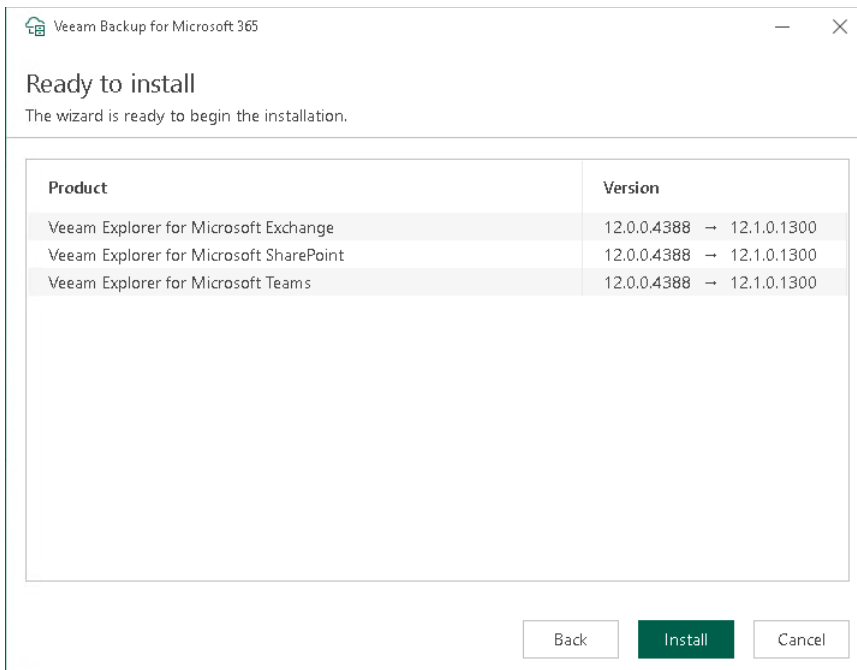
NOTE

If problems are not detected, the **System Configuration Check** step will be skipped.



- At the **Ready to install** step, review versions of Veeam Explorers that are ready to install and click **Install**.

Veeam Explorers are installed to the `C:\Program Files\Veeam\Backup and Replication\Explorers` folder. Keep in mind that you cannot specify a different location for Veeam Explorers.



- Wait for the installation process to complete and click **Finish** to exit the wizard.

Installing in Unattended Mode

You can install Veeam Backup for Microsoft 365, Veeam Explorer for Microsoft Exchange, Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft Teams in unattended mode.

Use the following syntax to run an MSI file:

```
msiexec /i <path_to_msi> /qn ADDLOCAL=<feature1,feature2,feature3> ACCEPT_THIRD  
PARTY_LICENSES=1 ACCEPT_EULA=1
```

The following table lists components and feature names for *Veeam Backup for Microsoft 365*:

Component	Feature name
EXO V3 PowerShell Module ¹	PS_MODULES
Server	BR_OFFICE365
Console	CONSOLE_OFFICE365
PowerShell	PS_OFFICE365
REST API	REST_OFFICE365

¹Starting from Veeam Backup for Microsoft 365 version 7 CP5 (build 7.0.0.4385), the EXO V3 PowerShell Module component must be installed along with any other component.

The following table lists components and feature names for *Veeam Explorer for Microsoft Exchange*:

Component	Feature name
UI	BR_EXCHANGEEXPLORER
PowerShell	PS_EXCHANGEEXPLORER

The following table lists components and feature names for *Veeam Explorer for Microsoft SharePoint*:

NOTE

Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft OneDrive for Business are distributed in a single package.

Component	Feature name
UI	BR_SHAREPOINTEXPLOLER
PowerShell	PS_SHAREPOINTEXPLOLER

The following table lists components and feature names for *Veeam Explorer for Microsoft Teams*:

Component	Feature name
UI	BR_TEAMSEXPLORER
PowerShell	PS_TEAMSEXPLORER

Examples

To install *Veeam Backup for Microsoft 365*, and the *EXO V3 PowerShell Module*, *Console*, *PowerShell* and *REST API* components:

```
msiexec /i Veeam.Backup365.msi /qn ADDLOCAL=BR_OFFICE365,CONSOLE_OFFICE365,PS_OFFICE365,REST_OFFICE365,PS_MODULES ACCEPT_THIRDPARTY_LICENSES=1 ACCEPT_EULA=1
```

To install the *EXO V3 PowerShell Module* and *REST API* components:

```
msiexec /i Veeam.Backup365.msi /qn ADDLOCAL=REST_OFFICE365,PS_MODULES ACCEPT_THIRDPARTY_LICENSES=1 ACCEPT_EULA=1
```

To install the *Veeam Explorer for Microsoft Exchange*, *UI* and *PowerShell* components:

```
msiexec /i VeeamExplorerForExchange.msi /qn ADDLOCAL=BR_EXCHANGEEXPLORER,PS_EXCHANGEEXPLORER ACCEPT_THIRDPARTY_LICENSES=1 ACCEPT_EULA=1
```

To install the *Veeam Explorer for Microsoft SharePoint*, *UI* and *PowerShell* components:

```
msiexec /i VeeamExplorerForSharePoint.msi /qn ADDLOCAL=BR_SHAREPOINTEXPLOLER,PS_SHAREPOINTEXPLOLER ACCEPT_THIRDPARTY_LICENSES=1 ACCEPT_EULA=1
```

NOTE

Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft OneDrive for Business are distributed in a single package.

To install the *Veeam Explorer for Microsoft Teams, UI* and *PowerShell* components:

```
msiexec /i VeeamExplorerForTeams.msi /qn ADDLOCAL=BR_TEAMSEXPLORER,PS_TEAMSEXPLORER ACCEPT_THIRDPARTY_LICENSES=1 ACCEPT_EULA=1
```


Deploying to Azure and AWS

To deploy Veeam Backup for Microsoft 365 to Microsoft Azure or Amazon Web Services (AWS) cloud platforms, do the following:

1. Install Veeam Backup for Microsoft 365 on an Azure or AWS virtual machine. For more information, see [Installing Veeam Backup for Microsoft 365](#).

Alternatively, you can deploy Veeam Backup for Microsoft 365 from [Azure Marketplace](#) and [AWS Marketplace](#).

When deploying to Azure, you can use [F-Series VM Sizes](#) for better performance. You can use only VM Sizes that meet [system requirements](#).

NOTE

For more information on how to deploy and use Veeam Backup for Microsoft 365 in the AWS environment, see the [Veeam Backup for Microsoft 365 in AWS Deployment Guide](#).

2. Configure additional backup proxy servers. For more information, see [Backup Proxy Servers](#).
For more information on how to deploy a backup proxy server to AWS, see [this Veeam KB article](#).
3. Configure backup repositories. For more information, see [Backup Repositories](#).

After deployment is complete, you can:

- Add Microsoft 365 and on-premises Microsoft organizations to the Veeam Backup for Microsoft 365 scope. For more information, see [Organization Management](#).
- Create backups. For more information, see [Data Backup](#).
- View and restore your data. For more information, see [Data Restore](#).

Updating Veeam Backup for Microsoft 365

Apart from major version releases of Veeam Backup for Microsoft 365, Veeam Software provides cumulative patches. Cumulative patches contain bug fixes and performance enhancements and introduce new product features. You need to install a cumulative patch to update Veeam Backup for Microsoft 365.

You can update Veeam Backup for Microsoft 365 in one of the following ways:

- **Automatically.** Veeam Backup for Microsoft 365 regularly checks Veeam servers for critical updates. If a new critical update is available, Veeam Backup for Microsoft 365 downloads this update in the background and installs it to the backup infrastructure components.
- **Manually.** You can manually check updates for Veeam Backup for Microsoft 365 and Veeam Explorers at any time.

NOTE

Starting from Veeam Backup for Microsoft 365 version 7 CP4 (build 7.0.0.3968), Veeam Backup for Microsoft 365 supports backup of public folder and discovery search mailboxes and determines correctly object type for shared mailboxes in Microsoft 365 organizations with modern app-only authentication.

If you want to back up these objects after installing Veeam Backup for Microsoft 365 version 7 CP4, do the following:

1. Edit your Microsoft 365 organization with modern app-only authentication. For more information, see [Editing Organization Settings](#).
2. Select the **Use an existing Azure AD application** option.
3. Clear and then select again the **Grant this application required permissions and register its certificate in Azure AD** check box to automatically update permissions of the existing Azure AD application.

Alternatively, you can sign in to the Azure portal and manually grant this Azure AD application the *Exchange.ManageAsApp* permission and the *Global Reader* role. For more information, see [Permissions for Backup](#) and [Granting Global Reader Role to Azure AD Application](#).

Automatic Update

By default, Veeam Backup for Microsoft 365 automatically checks Veeam servers for critical updates once a day. If a new critical update is available, Veeam Backup for Microsoft 365 downloads this update in the background and installs it to the following backup infrastructure components:

- Veeam Backup for Microsoft 365 server

This target is used to update Veeam Backup for Microsoft 365, Veeam Explorers, PowerShell, and REST API.

- Remote backup proxy servers

IMPORTANT

Automatic update is not supported for the Veeam Backup for Microsoft 365 REST API component installed on a separate machine and Veeam Explorers installed on a server with Veeam Backup & Replication for tenants.

Veeam Backup for Microsoft 365 updates the backup infrastructure components in the following order:

1. Veeam Backup for Microsoft 365 server (including the local backup proxy).

Update is performed within the *update window* that is a period of the Veeam Backup for Microsoft 365 server idleness. The following conditions must be met:

- Restore sessions are not running on the Veeam Backup for Microsoft 365 server.
- The Veeam Backup for Microsoft 365 console and PowerShell console are closed. Otherwise, you will be prompted to close these consoles.
- Backup, backup copy and retrieval jobs as well as data management jobs are not running on the local backup proxy.

2. Veeam Explorer, remote *Veeam Backup for Microsoft 365 Console* and *PowerShell* components.

Veeam Backup for Microsoft 365 will update these components only after the Veeam Backup for Microsoft 365 server update finishes.

3. Remote backup proxy servers.

Update is performed within the different *update window*. Veeam Backup for Microsoft 365 determines a time period when backup, backup copy and retrieval jobs as well as data management jobs are not running on a backup proxy server.

Thus, automatic update of Veeam Backup for Microsoft 365 can only be performed when the load on the backup infrastructure components is minimal. If Veeam Backup for Microsoft 365 cannot determine the proper update window during the 3-day period, you will be prompted to install updates manually. For more information, see [Checking for Updates](#).

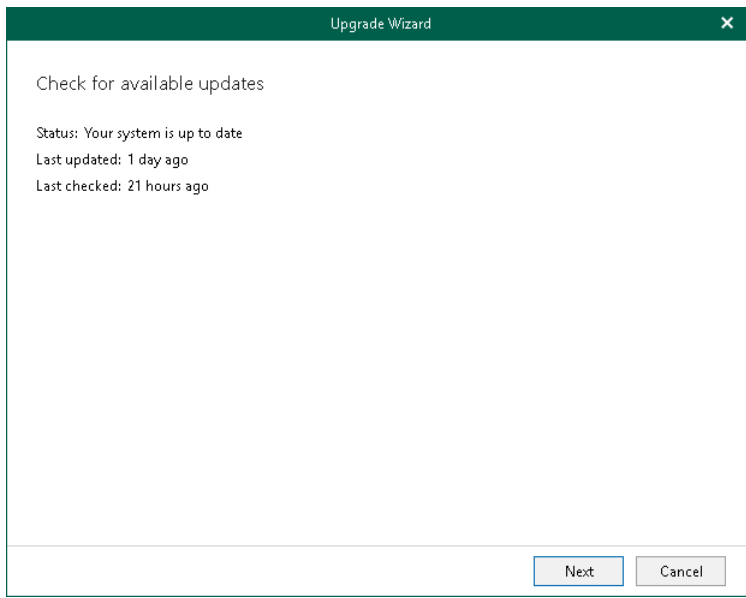
You can disable automatic update in the Veeam Backup for Microsoft 365 settings. To do this, clear the **Allow for automatic updates** check box on the **Updates** tab. For more information, see [New Versions and Automatic Updates](#).

Checking for Updates

To update Veeam Backup for Microsoft 365 and Veeam Explorers manually, do the following:

1. In the main menu, click **Upgrade**.
2. In the **Check for available updates** step, click **Next**.

Make sure to open the port that is required to access the Veeam auto-update server. For more information, see [Ports](#).



3. Wait until Veeam Backup for Microsoft 365 checks whether a newer version is available. To abort the request, click **Cancel**.
4. If available, click the **What's new** links to review details about new features and enhancements of Veeam Backup for Microsoft 365 and Veeam Explorers and click **Install**.
During update, the Veeam Backup for Microsoft 365 console will be closed, and you will be offered to go through the setup steps. For more information, see [Installing Veeam Backup for Microsoft 365](#).
5. Once installation is complete, launch Veeam Backup for Microsoft 365. For more information, see [Launching Veeam Backup for Microsoft 365](#).

NOTE

You can configure whether Veeam Backup for Microsoft 365 will notify you when new versions appear on Veeam servers and allow Veeam Backup for Microsoft 365 to download available updates automatically. For more information, see [New Versions and Automatic Updates](#).

Installing and Updating License

After you install Veeam Backup for Microsoft 365, you will be prompted to provide a license. You can dismiss this step and continue using the product without any license installed. In this case, the product will operate in the *Community Edition* mode that allows you to process up to 10 user accounts, up to 1 TB of Microsoft SharePoint data and up to 10 teams in all organizations. *Community Edition* mode is not limited in time and does not have limitations in terms of application functionality.

Installing Fully-Functional License

You can purchase and install a fully-functional license if you plan to back up more than 10 user accounts, more than 1 TB of Microsoft SharePoint data or more than 10 teams. For more information about available license types in Veeam Backup for Microsoft 365, see [Licensing and License Types](#).

The number of user accounts that you will be able to back up depends on the purchase agreement with Veeam sales representatives. You can find how many accounts Veeam Backup for Microsoft 365 can protect in the **Users** row of the [License Information](#) window.

To install a license, do the following:

1. In the main menu, click **License**.
2. In the **License Information** window, click **Install** and specify the path to the `.lic` file.
3. If you install Rental or Subscription license, Veeam Backup for Microsoft 365 prompts you whether the product can update your license automatically when you renew or expand your contract. If you agree, in the displayed window, click **Yes**.

The **Update license automatically** check box in the **License Information** window will be selected automatically.

NOTE

If you allow Veeam Backup for Microsoft 365 to update your license automatically, the following data will be periodically sent to the Veeam servers:

- License ID
- Installation ID
- License usage counters

Updating License

You can update an existing license, for example, if you want to extend the number of protected user accounts that you need to back up.

To update an existing license, click **Update Now** and wait until Veeam Backup for Microsoft 365 downloads and installs the license.

To enable automatic updates of your current license, select the **Update license automatically** check box.

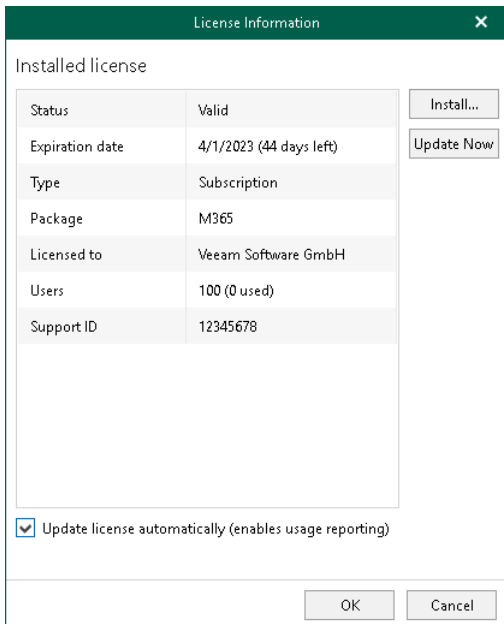
NOTE

To use the **Update license automatically** option, make sure to open the required port to access the Veeam auto-update server. For more information, see [Ports](#).

Updating License Package for Veeam ONE Monitoring

For Veeam Backup for Microsoft 365 with Subscription license, Veeam ONE monitoring is available if the *M365Suite* license package is installed. If you selected the **Update license automatically** check box before the product upgrade to version 7a, Veeam Backup for Microsoft 365 license package will be updated automatically from *M365* to *M365Suite* during the next 7 days after the product upgrade.

To update the license manually, click **Update Now**.



The image shows a 'License Information' dialog box with a dark green header and a close button. The main content area is titled 'Installed license' and contains a table with the following data:

Status	Valid
Expiration date	4/1/2023 (44 days left)
Type	Subscription
Package	M365
Licensed to	Veeam Software GmbH
Users	100 (0 used)
Support ID	12345678

Below the table, there is a checked checkbox labeled 'Update license automatically (enables usage reporting)'. To the right of the table, there are two buttons: 'Install...' and 'Update Now'. At the bottom of the dialog, there are 'OK' and 'Cancel' buttons.

Uninstalling License

You can remove the currently installed license from Veeam Backup for Microsoft 365. To do this, run the [Uninstall-VBOLicense](#) cmdlet.

Upgrading Veeam Backup for Microsoft 365

You can upgrade Veeam Backup for Microsoft 365 by installing a major version of the product.

Veeam Backup for Microsoft 365 supports upgrade to version 7a from the following versions of the product:

- 5.0 (builds 5.0.0.1061, 5.0.0.1063)
- 5a (build 5.0.0.1070)
- 5b (builds 5.0.1.179, 5.0.1.207, 5.0.1.225, 5.0.1.252)
- 5c (builds 5.0.2.22, 5.0.2.42)
- 5d (builds 5.0.3.1033, 5.0.3.1035, 5.0.3.1051, 5.0.3.1060, 5.0.3.1063)
- 6.0 (builds 6.0.0.367, 6.0.0.379, 6.0.0.385, 6.0.0.400)
- 6a (builds 6.1.0.222, 6.1.0.254, 6.1.0.423, 6.1.0.438, 6.1.0.1015)
- 7.0 (builds 7.0.0.2911, 7.0.0.2914, 7.0.0.3007, 7.0.0.3604, 7.0.0.3968, 7.0.0.4385, 7.0.0.4388, 7.0.0.4551)

NOTE

All modifications made to the `Config.xml` file manually will be lost.

Upgrading Veeam Backup for Microsoft 365 and Veeam Explorers

To upgrade Veeam Backup for Microsoft 365 and Veeam Explorers, do the following:

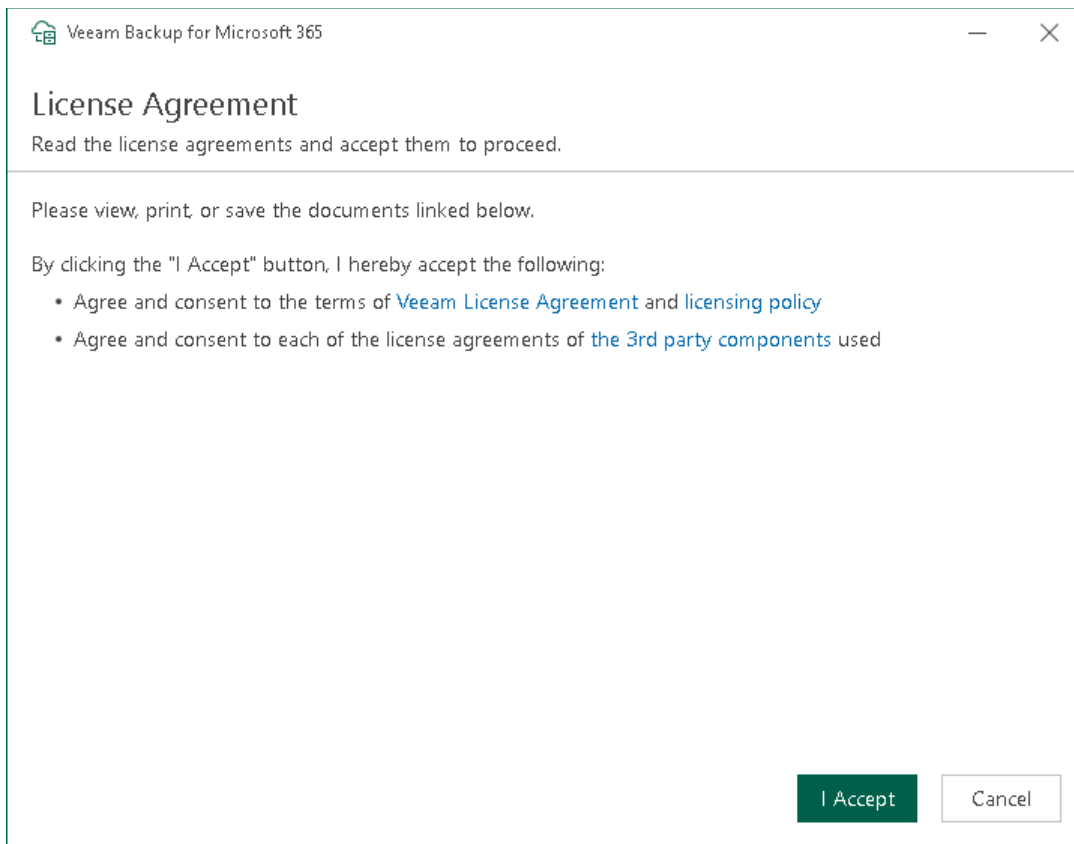
1. Download the Veeam Backup for Microsoft 365 installation package. For more information, see [Downloading Installation Package](#).
2. Open the `Veeam.Backup365.iso` file and run the `Veeam.Setup.exe` file.

3. On the splash screen, click **Update**.



4. In the displayed dialog box, read the information about operating systems that Veeam Backup for Microsoft 365 version 7 does not support. If your operating system meets [system requirements](#), click **OK**.

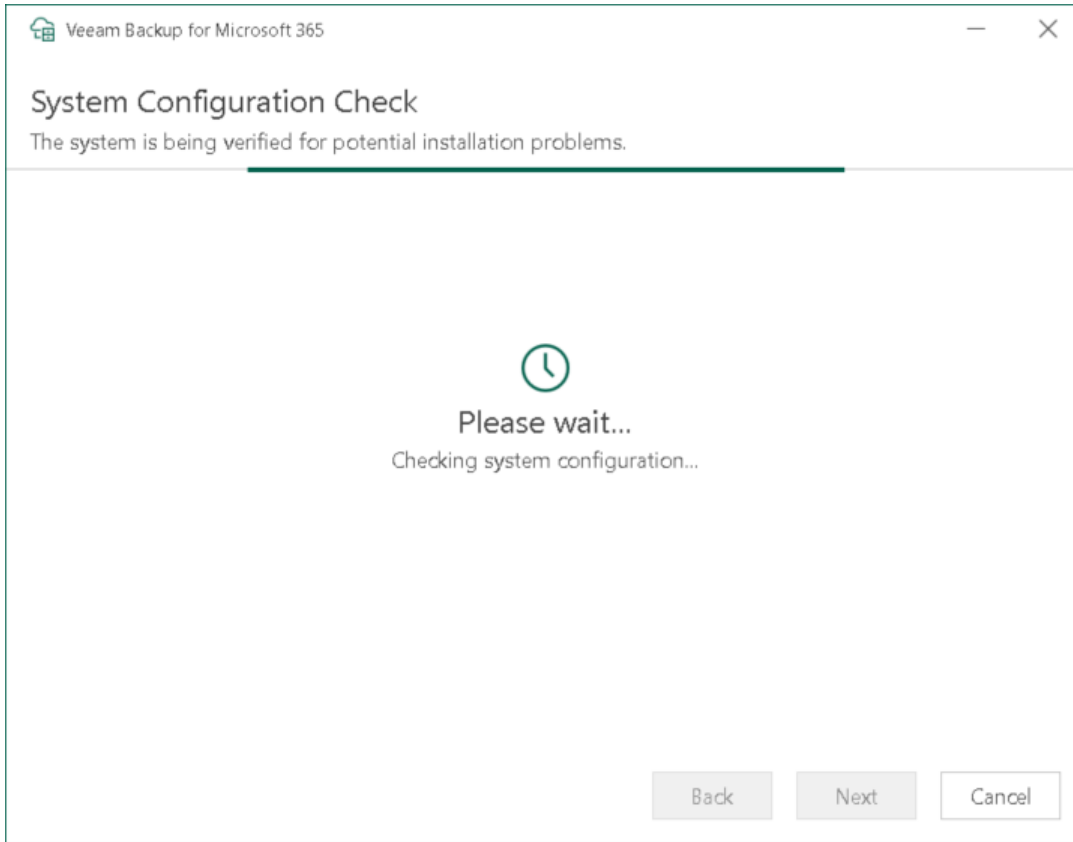
5. At the **License Agreement** step, click the links to read the following documents: *End User Software License Agreement*, *Licensing policy* and *3rd party software notices and information*. To accept the license agreements and continue installing Veeam Backup for Microsoft 365, click **I Accept**.



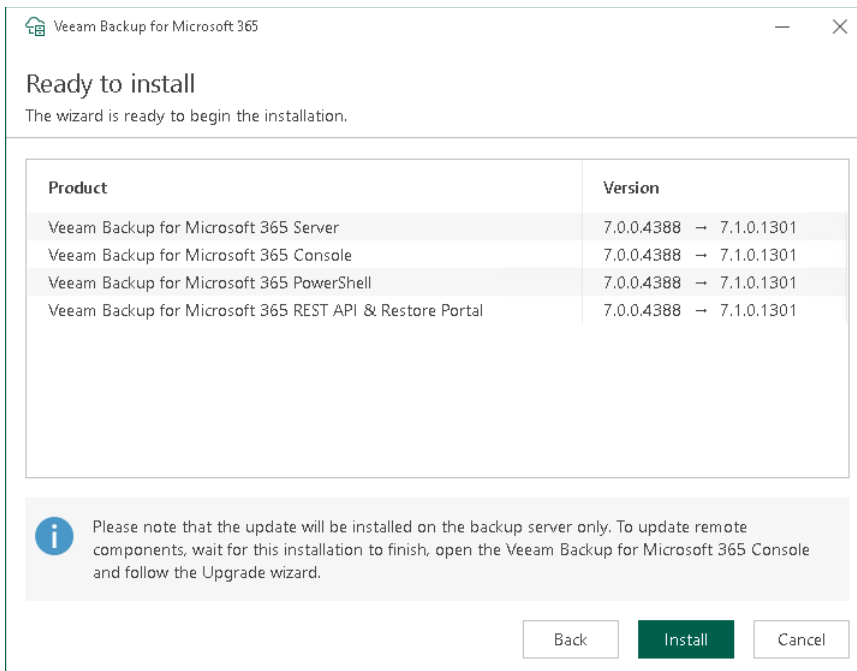
6. At the **System Configuration Check** step, wait until the wizard checks the system configuration to find the potential installation problems. If the wizard detects problems, you will be prompted to fix the issues to continue the installation.

NOTE

If problems are not detected, the **System Configuration Check** step will be skipped.



7. At the **Ready to install** step, review versions of Veeam Backup for Microsoft 365 components that are ready to upgrade and click **Install**.



8. Wait for the installation process to complete and click **Finish** to exit the wizard.

What You Do After Upgrade

After you upgraded Veeam Backup for Microsoft 365, you must upgrade the Veeam Backup for Microsoft 365 REST API component on a separate machine, update Subscription license and upgrade other backup entities.

Upgrading REST API on Separate Machine

If you use a separate machine with REST API for communicating with Restore Portal, you must manually upgrade the Veeam Backup for Microsoft 365 REST API component on this machine. For more information, see [Upgrading REST API on Separate Machine](#).

Updating Veeam Backup for Microsoft 365 License

To support integration with Veeam ONE, Veeam Backup for Microsoft 365 with Subscription license requires the *M365Suite* license package. For more information on how to update the current license or install a new license, see [Installing and Updating License](#).

Upgrading Backup Infrastructure Components

Once Veeam Backup for Microsoft 365 is upgraded, the following entities will be marked as *Out of Date*:

- *Backup repositories*

For information on how to upgrade backup repositories, see [Upgrading Backup Repositories](#).

- *Backup proxy servers*

For information on how to upgrade backup proxy servers, see [Upgrading Backup Proxy Servers](#)

Consider that a default backup proxy server will be upgraded automatically.

Upgrading REST API on Separate Machine

NOTE

Consider the following:

- All modifications made to the `Config.xml` file manually will be lost.
- *Veeam Backup for Microsoft 365 REST API Service* must be enabled manually after the upgrade. To do this, use the `services.msc` console.

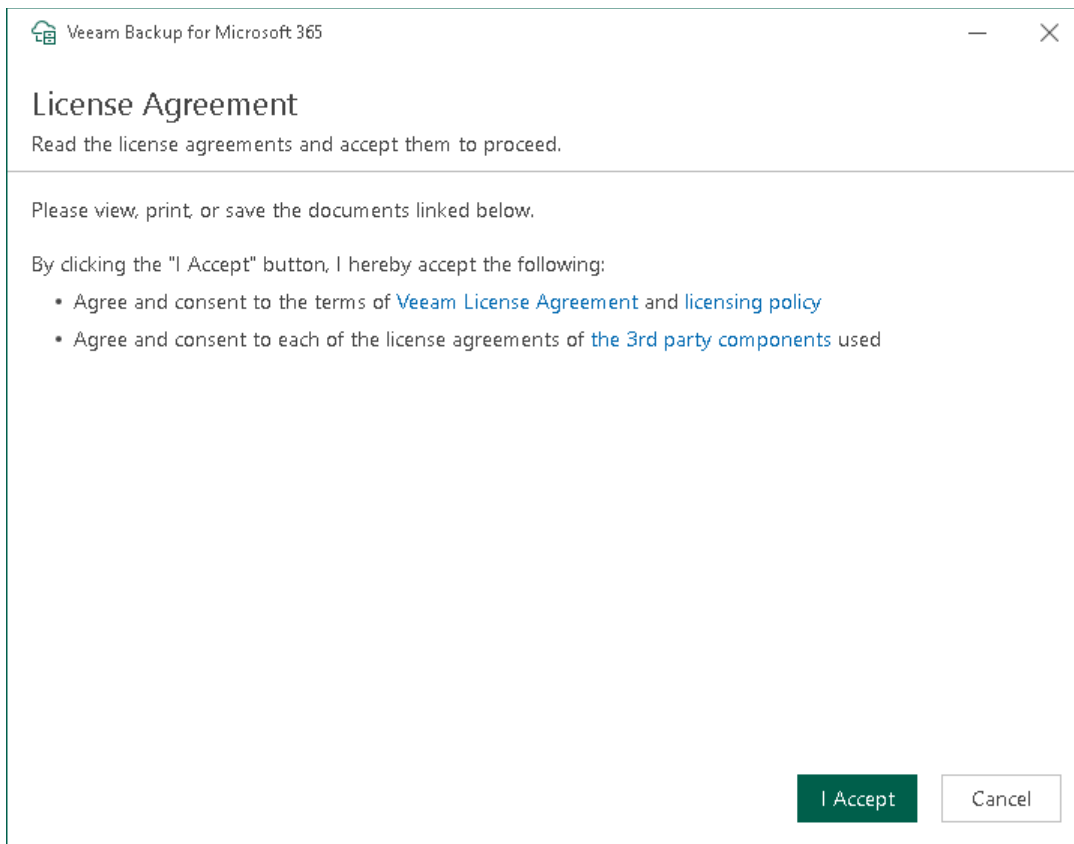
To upgrade the Veeam Backup for Microsoft 365 REST API component on a separate machine, do the following:

1. Download the Veeam Backup for Microsoft 365 installation package. For more information, see [Downloading Installation Package](#).
2. Open the `Veeam.Backup365.iso` file and run the `Veeam.Setup.exe` file.
3. On the splash screen, click **Update**.



4. In the displayed dialog box, read the information about operating systems that Veeam Backup for Microsoft 365 version 7 does not support. If your operating system meets [system requirements](#), click **OK**.

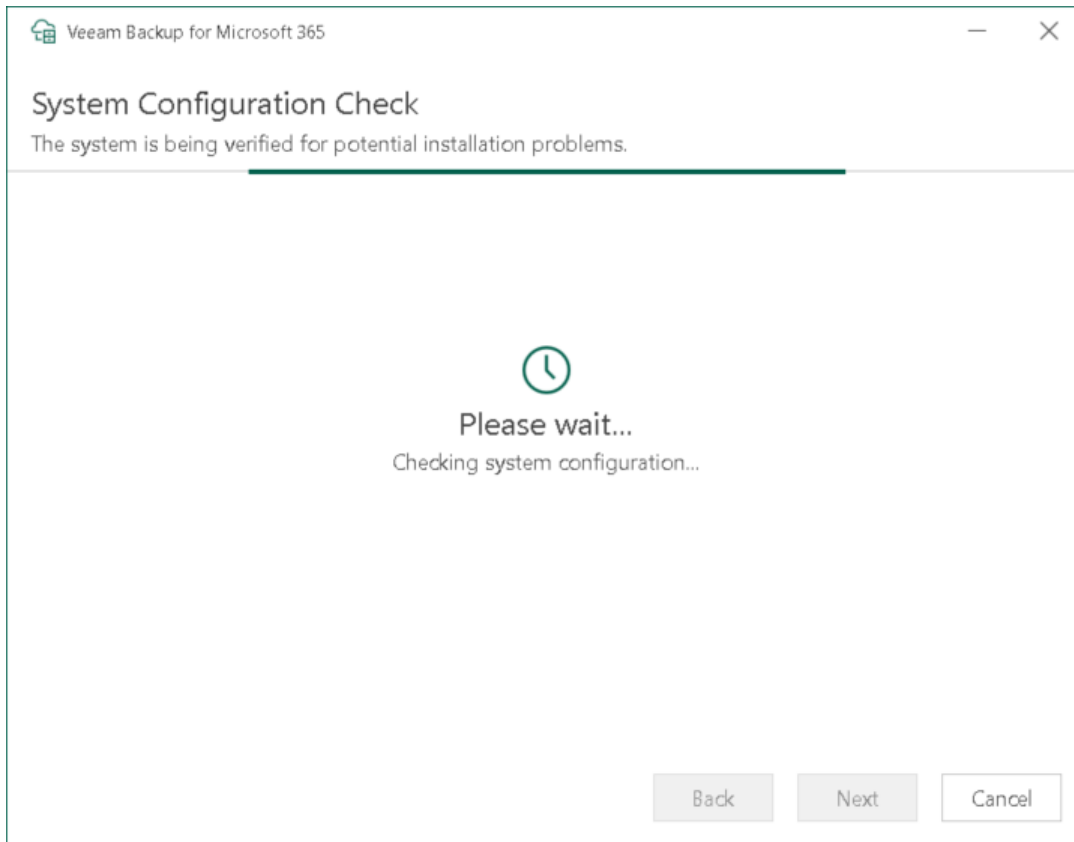
- At the **License Agreement** step, click the links to read the following documents: *End User Software License Agreement*, *Licensing policy* and *3rd party software notices and information*. To accept the license agreements and continue installing Veeam Backup for Microsoft 365, click **I Accept**.



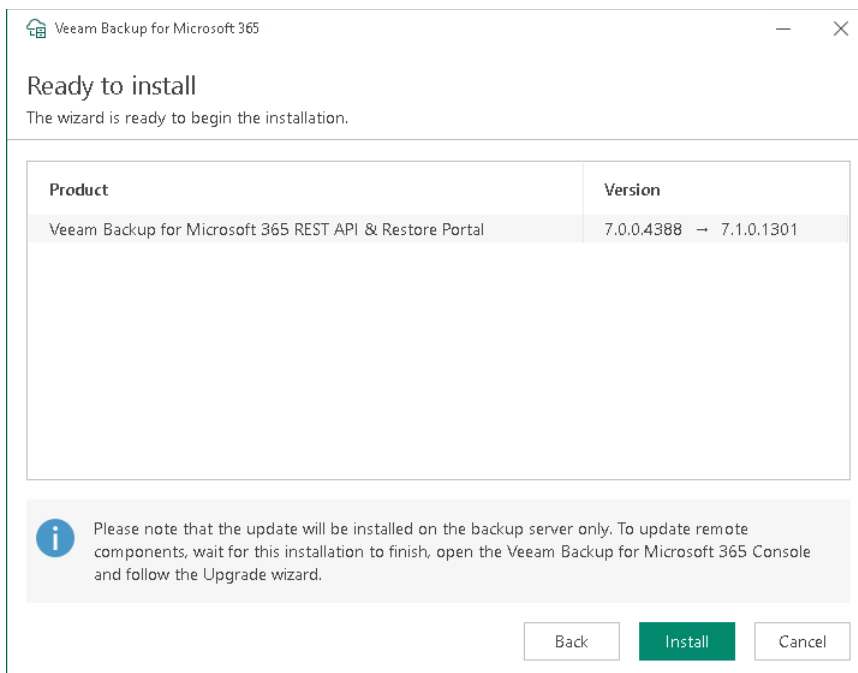
- At the **System Configuration Check** step, wait until the wizard checks the system configuration to find the potential installation problems. If the wizard detects problems, you will be prompted to fix the issues to continue the installation.

NOTE

If problems are not detected, the **System Configuration Check** step will be skipped.



7. At the **Ready to install** step, review versions of Veeam Backup for Microsoft 365 components that are ready to upgrade and click **Install**.



8. Wait for the installation process to complete and click **Finish** to exit the wizard.

Uninstalling Veeam Backup for Microsoft 365

To uninstall Veeam Backup for Microsoft 365, do the following:

1. Stop all restore sessions (if any) in Veeam Explorer for Microsoft Exchange, Veeam Explorer for Microsoft SharePoint, Veeam Explorer for Microsoft OneDrive for Business and Veeam Explorer for Microsoft Teams.
2. Open the Veeam Backup for Microsoft 365 console, go to **Backup Infrastructure > Backup Proxies** and remove all configured backup proxy servers. For more information, see [Removing Backup Proxy Server](#).
3. From the **Start** menu, select **Control Panel > Programs and Features**.
4. In the programs list, right-click **Veeam Backup for Microsoft 365** and select **Uninstall**.

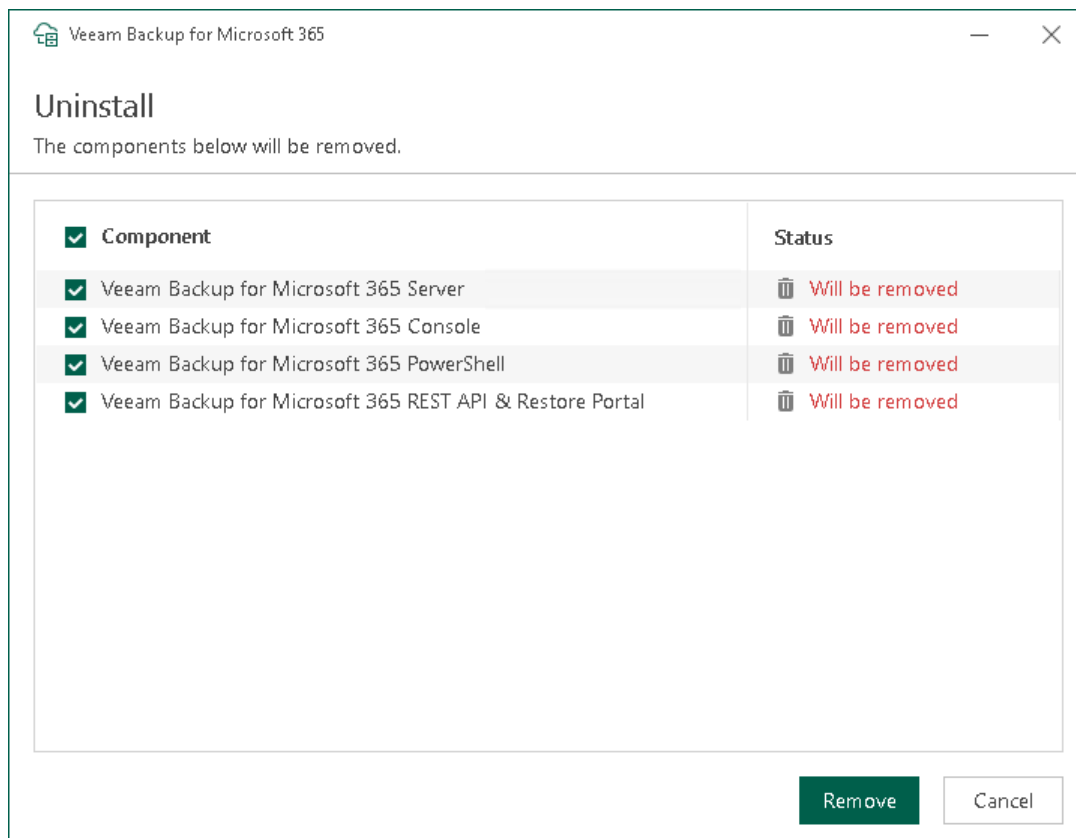
The Veeam Backup for Microsoft 365 uninstallation wizard runs.

5. At the **Uninstall** step, select check boxes next to the items that you want to uninstall and click **Remove**. Keep in mind that the Veeam Backup for Microsoft 365 uninstallation wizard uninstalls Veeam Explorers that are included in the Veeam Backup for Microsoft 365 installation package if you have only Veeam Backup for Microsoft 365 on your machine.

IMPORTANT

If you have both Veeam Backup for Microsoft 365 and Veeam Backup & Replication installed, uninstall Veeam Explorers using the procedure in [this section](#) of the Veeam Backup & Replication Best Practices Guide.

6. Wait for the uninstallation process to complete and click **Finish** to exit the wizard.



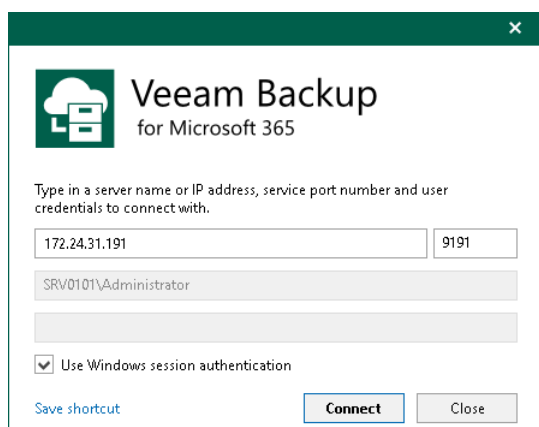
Launching Veeam Backup for Microsoft 365

To launch *Veeam Backup for Microsoft 365 Console*, do the following:

1. From the **Start** menu, select **Veeam Backup for Microsoft 365**.
2. In the displayed window, specify the following:
 - A name or IP address of the Veeam Backup for Microsoft 365 server.
 - A port number which is used to connect to the specified Veeam Backup for Microsoft 365 server.
 - Authentication credentials that you want to use to connect to the specified Veeam Backup for Microsoft 365 server.

Keep in mind that the account you are using must be a member of the local *Administrators* group on the specified Veeam Backup for Microsoft 365 server. To use your current account, select **Use Windows session authentication**.

3. If you want to save a connection shortcut to the desktop, click **Save shortcut** in the lower-left corner.
4. Click **Connect**.



Launching with Command Line

To launch Veeam Backup for Microsoft 365 using the command-line tool, run the `C:\Program Files\Veeam\Backup365\Veeam.Archiver.Shell.exe` file with the following parameters:

- `/local=true`

To connect to Veeam Backup for Microsoft 365 that is installed on a local machine using the *Local System* account.

For example:

```
C:\Program Files\Veeam\Backup365\Veeam.Archiver.Shell.exe /local=true
```

- */host=<hostname> /port=<port> /usewincredentials=true*

To connect to Veeam Backup for Microsoft 365 that is installed on a remote machine using the */host* and */port* parameters.

For example:

```
C:\Program Files\Veeam\Backup365\Veeam.Archiver.Shell.exe /host=192.168.0.12 /port=9895 /usewincredentials=true
```

- */host=<host> /port=<port> /account=<domain\accountName>*

To connect to Veeam Backup for Microsoft 365 that is installed on a remote machine using the */host* and */port* parameters.

You can also provide an account that you want to use to launch Veeam Backup for Microsoft 365 using the */account=<domain\accountName>* format.

For example:

```
C:\Program Files\Veeam\Backup365\Veeam.Archiver.Shell.exe /host=192.168.0.12 /port=9895 /account=tech.local\Administrator
```

User Interface

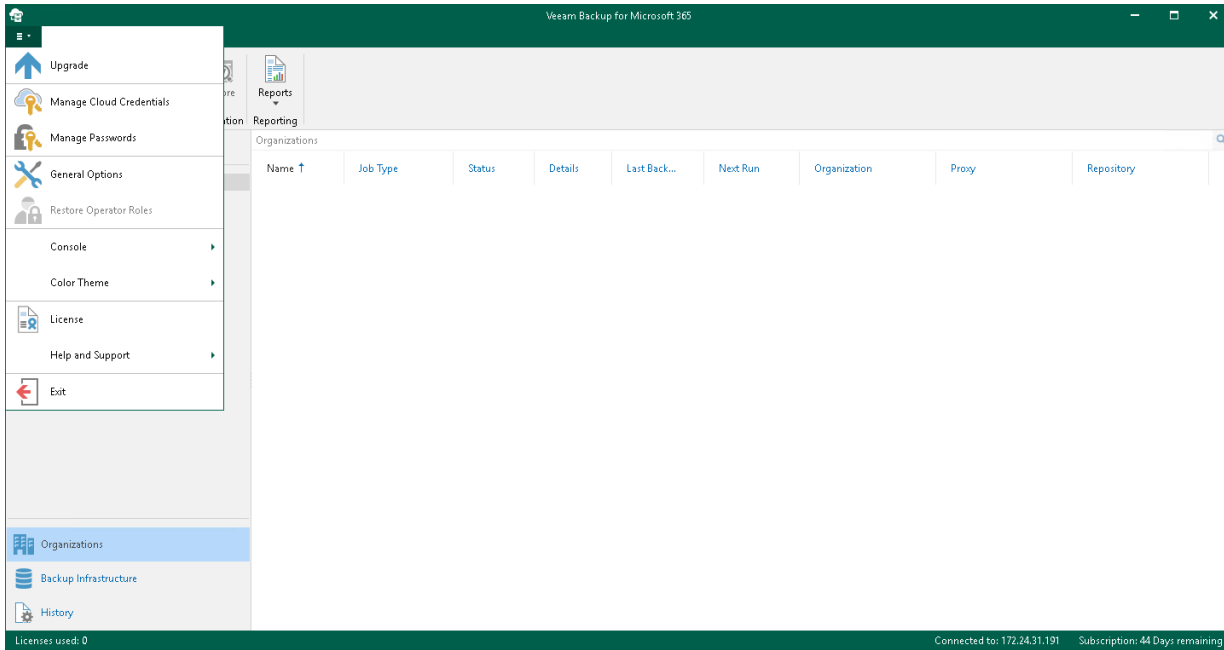
The user interface of Veeam Backup for Microsoft 365 is designed to let you quickly find commands that you need to protect data of Microsoft organizations against disasters and configure backup infrastructure.

Main Menu

The main menu comprises the following:

- **Upgrade.** Allows you to update Veeam Backup for Microsoft 365 manually.
For more information, see [Checking for Updates](#).
- **Manage Cloud Credentials.** Allows you to manage cloud credentials that you use to access object storage.
For more information, see [Managing Cloud Credentials](#).
- **Manage Passwords.** Allows you to manage encryption passwords.
For more information, see [Managing Encryption Passwords](#).
- **General Options.** Allows you to configure general application settings.
For more information, see [General Settings](#).
- **Restore Operator Roles.** Allows you to manage restore operator roles that you add in the operator restore scenario for data restore using Restore Portal.
For more information, see [Adding Restore Operator Role](#).
- **Console.**
 - **PowerShell.** Opens the PowerShell toolkit.
 - **Swagger.** Opens swagger website. Unavailable until you enable the REST service. For more information, see [REST API Settings](#).
- **Color Theme.** Contains four different color schemes that you can select for the Veeam Backup for Microsoft 365 console.
- **License.** Shows license information.
For more information, see [Installing and Updating License](#).
- **Help and Support.**
 - **Online help.** Opens the online help page.
 - **Support information.** Launches the support information collection wizard.
For more information, see [Collecting Log Files](#).
 - **About.** Shows the additional information including build number.

- **Exit.** Closes the Veeam Backup for Microsoft 365 console window.



Main Application Window

The main application window can be divided into five categories:

- The views switch that allows you to switch among the following infrastructure views:
 - The **Organizations** view is intended to work with Microsoft organizations, as well as backup, backup copy and retrieval jobs. It provides search capabilities and statistics for recently performed backup, backup copy and restore sessions.
 - The **Backup Infrastructure** view displays a list of backup infrastructure components: backup proxies, backup repositories and object storage. You can use this view for backup infrastructure setup – here you can configure backup infrastructure components that will be used for data backup, backup copy and restore of backed-up data.
 - The **History** view displays statistics on backup, backup copy, retrieve and restore sessions performed with Veeam Backup for Microsoft 365. Also, it allows you to search for backup, backup copy, retrieve and restore sessions using keywords.
- The inventory pane that displays a hierarchy or list of items relevant for a specific view. Lists are displayed in the preview pane.

Items displayed in the inventory pane differ depending on the active view. For example, in the **Organizations** view, the inventory pane displays the following nodes:

- The **Organizations** node that includes Microsoft organizations added to the scope and a list of backup and backup copy jobs configured for these organizations. Also, it allows you to search for backup and backup copy jobs using keywords.
- The **Data retrieval** node with a list of retrieval jobs and their statuses. Keep in mind that this node is displayed only if you have created a retrieval job.

- The **Last 24 hours** node with the list of backup, backup copy, retrieve and restore sessions performed within the last 24 hours and their statuses. Also, it allows you to search for backup, backup copy, retrieve and restore sessions using keywords.

In the **Backup Infrastructure** view, the inventory pane displays nodes for backup infrastructure components – backup proxies, backup repositories and object storage. The **Backup Repositories** node includes the following nodes for different backup repositories added to Veeam Backup for Microsoft 365:

- **Object storage**. Contains backup repositories extended with S3 Compatible object storage, Azure Blob Storage Hot/Cool access tiers, Amazon S3 Standard and Amazon S3 Standard-Infrequent Access storage classes.
- **Local disk**. Contains *Default Backup Repository* and other JET-based backup repositories.
- **Archive**. Contains backup repositories extended with Azure Blob Storage Archive access tier and all Amazon S3 Glacier storage classes.

For more information, see [Supported Azure Storage Account Types](#) and [Supported Amazon S3 Storage Classes](#).

Keep in mind that the **Archive** and **Object storage** nodes are displayed only if you have added a backup repository extended with a particular object storage.

- The ribbon that contains operation commands organized into logical groups represented as tabs. The ribbon is displayed at the top of the main application window.

On the ribbon, the following tabs are displayed:

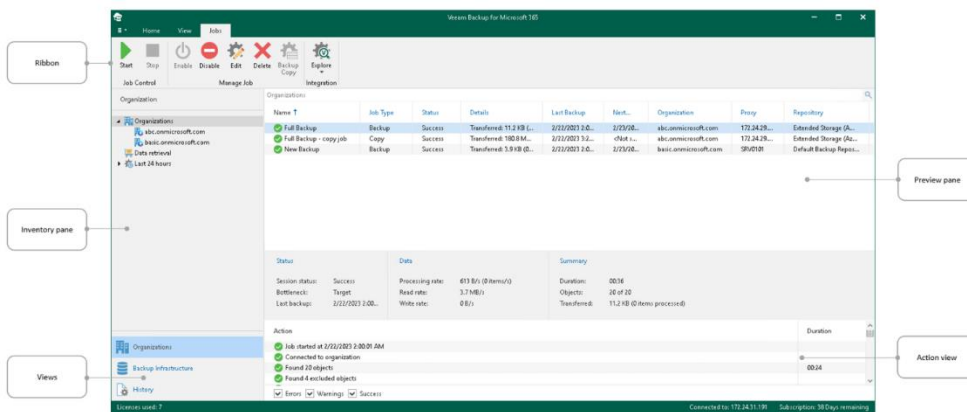
- The **Home** tab provides quick access to the most common operations. It lets you manage organizations, create backup jobs, explore backed-up data, retrieve data from backup copies and configure reports. This tab is always available, no matter which view is currently active.
- Other tabs contain commands specific for certain items and appear when these items are selected in the inventory or preview pane.
 - The **View** tab allows you to switch between the compact and full view modes.
 - The **Jobs** tab contains commands specific for backup jobs.
 - The **Backup Proxy** tab contains commands specific for backup proxies.
 - The **Backup Repository** tab contains commands specific for backup repositories.
 - The **Object Storage** tab contains commands specific for object storage.
 - The **Retrievals** tab contains commands specific for retrieval jobs.
 - The **Last 24 Hours** tab allows you to stop backup, backup copy and restore sessions.

TIP

Commands for operations with items in Veeam Backup for Microsoft 365 are also available from the shortcut menu.

- The preview pane that provides search capabilities and shows you, for example, a list of backup and backup copy jobs configured for the selected organization.

- The action view that allows you to view details about backup and backup copy jobs progress and results.



TIP

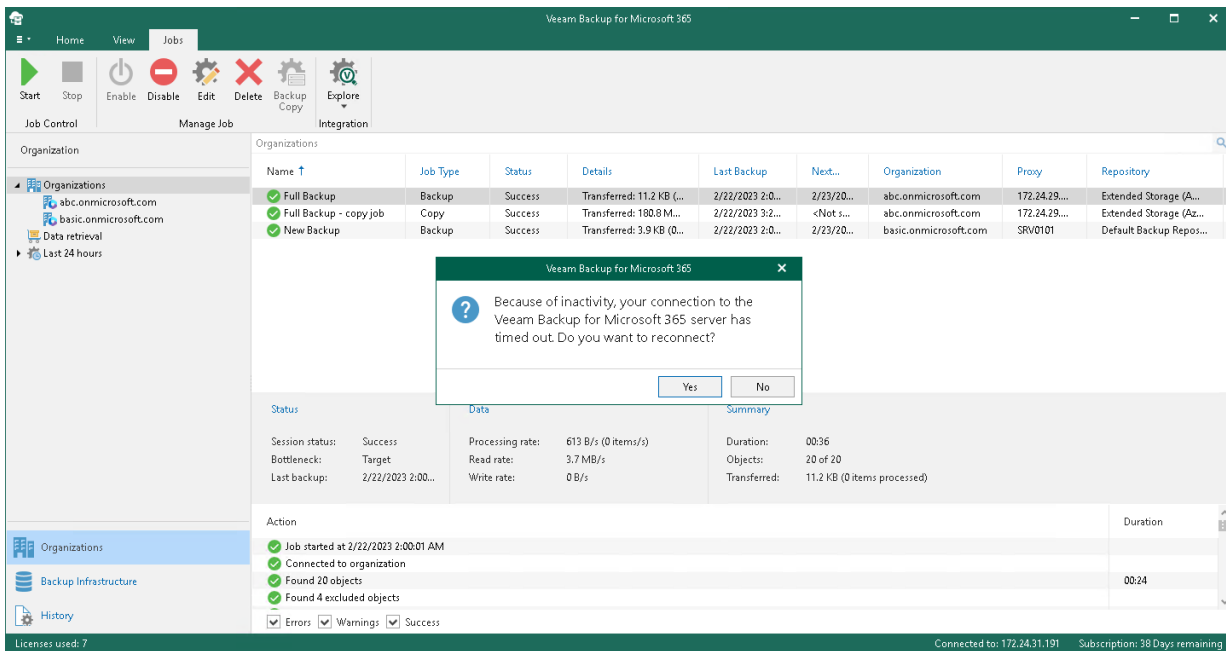
To open online help, press **[F1]** in any Veeam Backup for Microsoft 365 wizard or window.

Current Session

Every time you open the Veeam Backup for Microsoft 365 console, a new connection is established to the [specified backup server](#). After 30 minutes of idleness, such a connection is timed out. Veeam Backup for Microsoft 365 prompts you whether to re-establish a connection and continue using the product or exit the console.

Consider the following:

- When closing the Veeam Backup for Microsoft 365 console, all running backup and backup copy sessions will continue to be executed in the background.
- Restore sessions (if any) will not be affected.



Performing Search

In the **Organizations** view of the Veeam Backup for Microsoft 365 console, you can search for the following entities using keywords:

- Backup and backup copy jobs configured for Microsoft organizations.
- Backup, backup copy, retrieve and restore sessions performed by Veeam Backup for Microsoft 365 within the last 24 hours.

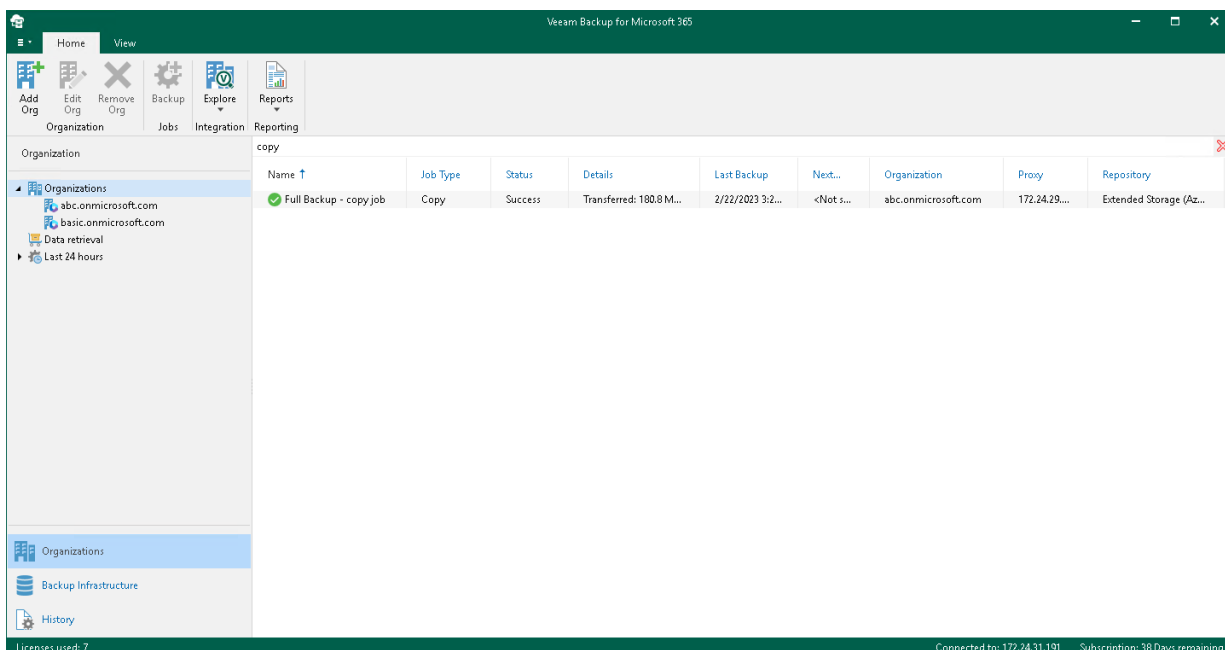
Searching for Jobs

To search for backup and backup copy jobs, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, do one of the following:
 - If you want to search for backup and backup copy jobs configured for all organizations added to Veeam Backup for Microsoft 365, select the root **Organizations** node.
 - If you want to search for backup and backup copy jobs configured for a specific organization, select an organization node.
3. Enter a search query in the search field at the top of the preview pane.

Veeam Backup for Microsoft 365 will display only backup and backup copy jobs whose names include keywords that you are searching for.

To remove a keyword, click the cross mark.



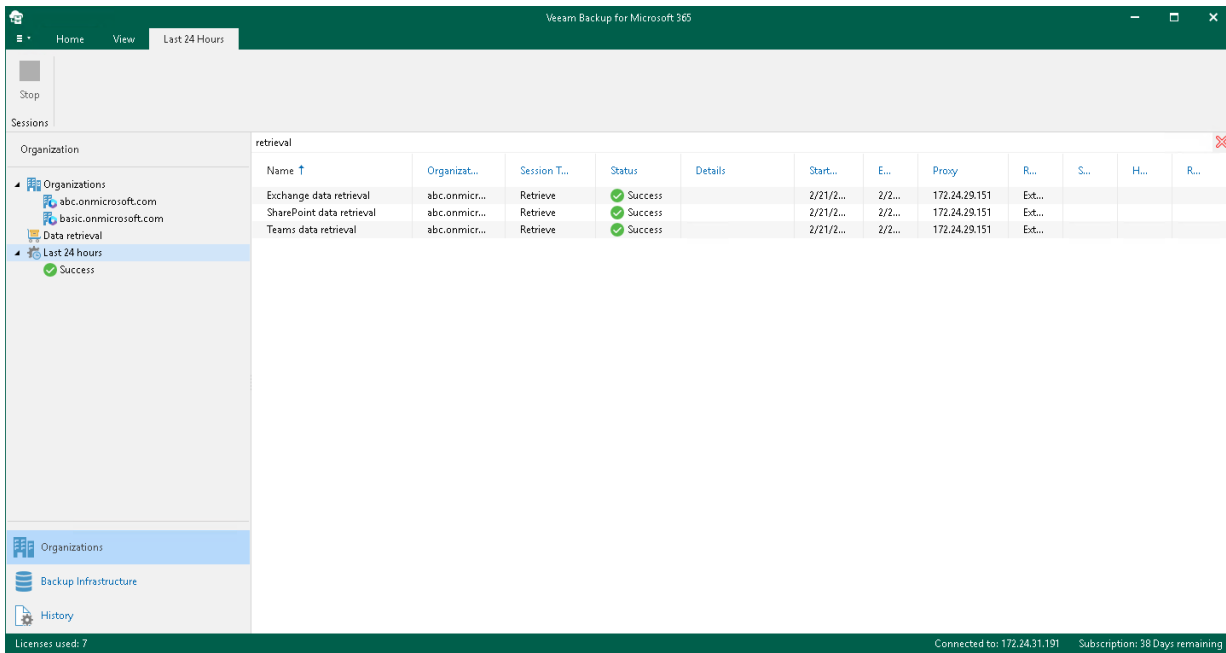
Searching for Sessions

To search for backup, backup copy, retrieve and restore sessions performed by Veeam Backup for Microsoft 365 within the last 24 hours, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select either the **Last 24 hours** node or one of its subnodes to search for sessions with a particular status.
3. Enter a search query in the search field at the top of the preview pane.

Veeam Backup for Microsoft 365 will display only sessions whose names include keywords that you are searching for.

To remove a keyword, click the cross mark.



Configuration

Before you start using Veeam Backup for Microsoft 365 for data protection and disaster recovery, make sure to configure general application settings and backup infrastructure.

General Settings

You configure general settings for Veeam Backup for Microsoft 365. General settings are applied to all [backup](#) and [backup copy](#) jobs, [backup infrastructure](#) components and [data restore using Restore Portal](#).

Folder Exclusions

You can configure folder exclusions if you do not want certain folders to be backed up by a [backup job](#) or removed by a [retention policy](#).

To configure exclusions, do the following:

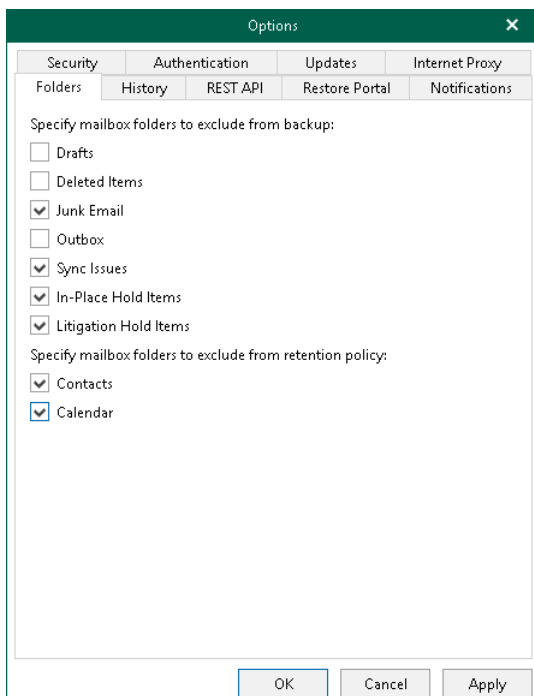
1. In the main menu, click **General Options**.
2. Open the **Folders** tab.
3. In the **Specify mailbox folders to exclude from backup** section, select check boxes next to folders that you want to exclude from a backup.
4. Click **OK**.

NOTE

When you select **Deleted Items**, both *deleted* and *permanently deleted* items will be excluded.

To prevent mailbox folders to be removed by a retention policy, do the following:

1. In the main menu, click **General Options**.
2. Open the **Folders** tab.
3. In the **Specify mailbox folders to exclude from retention policy** section, select folders that you want to preserve during a retention session.
4. Click **OK**.



Session History

Veeam Backup for Microsoft 365 saves information about backup, backup copy and restore sessions to the configuration database. You can review this information. For more information, see [Backup, Backup Copy and Restore Statistics](#).

To specify a period during which Veeam Backup for Microsoft 365 keeps information about backup, backup copy and restore sessions, do the following:

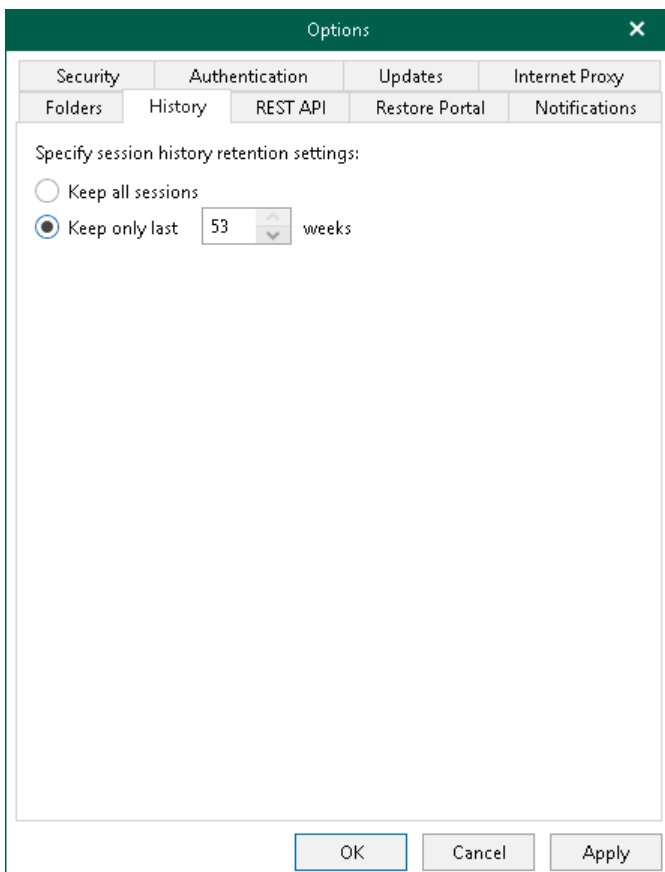
1. In the main menu, click **General Options**.
2. Open the **History** tab.
3. Specify for how long Veeam Backup for Microsoft 365 will keep history for backup, backup copy and restore sessions.

You can select one of the following options:

- **Keep all sessions**
- **Keep only last <N> weeks**

If you select this option, you can specify a number of weeks during which Veeam Backup for Microsoft 365 will keep history for backup, backup copy and restore sessions.

4. Click **OK**.



REST API Settings

You can use the REST API to communicate with Veeam Backup for Microsoft 365. For more information, see [REST API Reference](#).

Also, REST API is used by Restore Portal to communicate with the Veeam Backup for Microsoft 365 server. Restore Portal allows users to perform self-service restore. For more information about Restore Portal, see [Data Restore Using Restore Portal](#).

To configure Veeam Backup for Microsoft 365 REST API settings, do the following:

1. In the main menu, click **General Options**.
2. Open the **REST API** tab.
3. Select the **Enable REST service** check box.
4. In the **Authentication token lifetime** field, specify the lifetime value for an authentication token (in minutes).

REST API authorization is based on the [OAuth 2.0 Authorization Framework](#).

5. In the **HTTPS port** field, specify a port number which you use to access *Veeam Backup for Microsoft 365 REST API Service*.

Also, Restore Portal uses this port to communicate with *Veeam Backup for Microsoft 365 REST API Service*. For more information, see [Ports](#).

NOTE

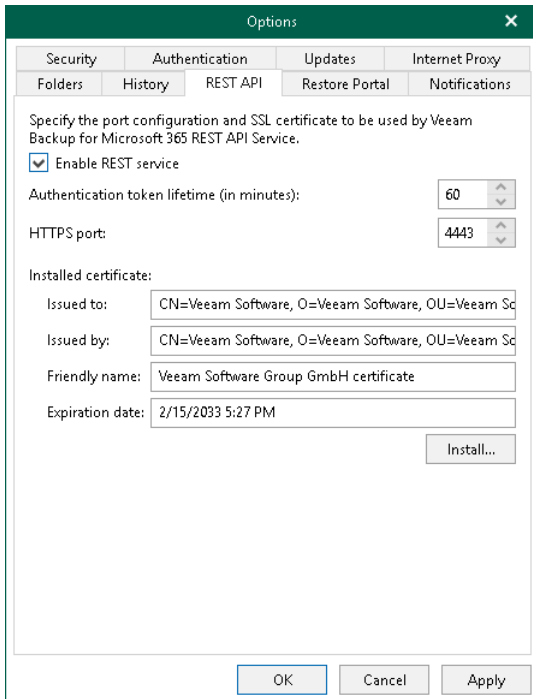
The default value is *4443*. If you use a different port, make sure that you configure the same value for the Restore Portal web address. Otherwise, Restore Portal will be unavailable. For more information, see [Register or Configure Azure AD Application](#).

6. Click **Install** to specify an SSL certificate.

You can generate a new certificate or select an existing certificate using the **Select Certificate** wizard. For more information, see [Installing SSL Certificates](#).

Keep in mind that Restore Portal also uses this SSL certificate to communicate with the Veeam Backup for Microsoft 365 server and perform restore operations through REST API.

7. Click **OK**.



Restore Portal Settings

Veeam Backup for Microsoft 365 provides users with the ability to explore and restore data from backups by themselves or delegate this task to restore operators. In these scenarios, Veeam Explorers are not needed to explore and restore backed-up data. Users use Restore Portal – a web-based solution instead and perform all operations in a web browser window. You configure the Restore Portal settings if you want to allow users to perform self-service restore. For more information about Restore Portal, see [Data Restore Using Restore Portal](#).

NOTE

If you want to restore your backed-up data using Restore Portal in different regions, you must use a separate installation of the Veeam Backup for Microsoft 365 REST API component and a separate Azure AD application in each Microsoft Azure region.

To configure the Restore Portal settings, do the following:

1. In the main menu, click **General Options**.
2. Open the **Restore Portal** tab.
3. Select the **Enable Restore Portal** check box.
4. Do one of the following:

- Register a new Azure AD application automatically

To do this, click **Configure** and follow the steps of the **Configure Application** wizard. For more information, see [Creating or Configuring Azure AD Application](#).

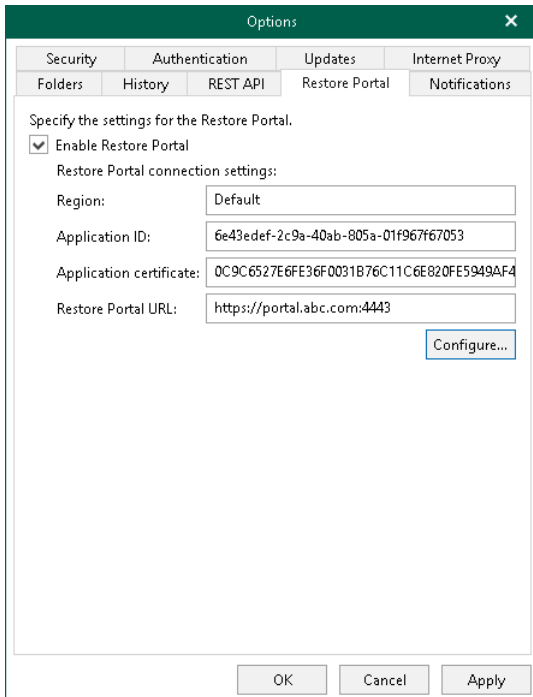
Veeam Backup for Microsoft 365 automatically grants the [required permissions](#) to the Azure AD application that you create and generates an SSL certificate. For more information, see [Registering New Azure AD Application](#).

- Configure an existing Azure AD application

To do this, click **Configure** and follow the steps of the **Configure Application** wizard. For more information, see [Creating or Configuring Azure AD Application](#).

Veeam Backup for Microsoft 365 checks the Azure AD application permissions, grants the missing [permissions](#) if needed and updates an SSL certificate. For more information, see [Configuring Existing Azure AD Application](#).

5. Click **OK**.



Creating or Configuring Azure AD Application

To create a new Azure AD application for Restore Portal or configure an existing Azure AD application, do the following:

1. [Launch the Configure Application wizard.](#)
2. [Configure connection to Restore Portal.](#)
3. [Register or configure Azure AD application.](#)
4. [Log in to Microsoft 365.](#)

Step 1. Launch Configure Application Wizard

To launch the **Configure Application** wizard, do the following:

1. In the main menu, click **General Options**.
2. Open the **Restore Portal** tab.
3. Select the **Enable Restore Portal** check box.
4. Click **Configure**.

Step 2. Configure Connection to Restore Portal

At this step of the wizard, choose whether you want to register a new [Azure AD application](#) to connect to Restore Portal or configure an existing Azure AD application.

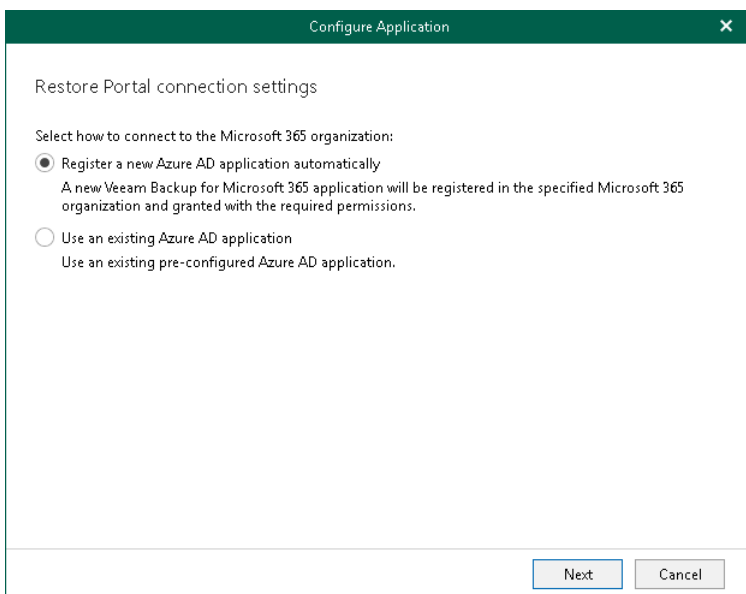
You can select one of the following options:

- **Register a new Azure AD application automatically**

With this option selected, Veeam Backup for Microsoft 365 requires to provide an application name, a certificate to register a new Azure AD application in Microsoft Entra ID (formerly Azure Active Directory) and specify web address of a machine with the Veeam Backup for Microsoft 365 REST API component installed. For more information, see [Registering New Azure AD Application](#).

- **Use an existing Azure AD application**

With this option selected, Veeam Backup for Microsoft 365 requires to modify connection parameters of the existing Azure AD application. For more information, see [Configuring Existing Azure AD Application](#).



Step 3. Register or Configure Azure AD Application

At this step of the wizard, you can create a new application in Microsoft Entra ID (formerly Azure Active Directory) or configure an existing one.

- [Registering a new application](#)
Use this method if you have selected the **Register a new Azure AD application automatically** option at the previous step of the wizard.
- [Configure an existing application](#)
Use this method if you have selected the **Use an existing Azure AD application** option at the previous step of the wizard.

NOTE

Restore operators and end users will be able to use the only URI that you specify in the **Restore Portal web address** field. If you want to specify multiple redirect URIs that will be used as the Restore Portal web address or set the application as enterprise to allow multi-tenant access, you must configure these settings manually in your Microsoft Entra ID (formerly Azure Active Directory).

Registering New Azure AD Application

You can register a new Azure AD application in Microsoft Entra ID (formerly Azure Active Directory). Veeam Backup for Microsoft 365 will use this application to connect to Restore Portal. When registering a new Azure AD application, Veeam Backup for Microsoft 365 automatically grants the [required permissions](#) to this application.

To register a new Azure AD application, do the following:

1. From the **Region** drop-down list, select a Microsoft Azure region.
2. In the **Name** field, enter a name that you want to use to register a new Azure AD application in your Microsoft Entra ID (formerly Azure Active Directory).
3. Click **Install** to specify an SSL certificate that you want to use for data exchange between Restore Portal and the created Azure AD application.
4. In the **Select Certificate** wizard, select a certificate. For more information, see [Installing SSL Certificates](#).

You can generate a new self-signed certificate or use an existing one. Before using an existing certificate, make sure to register this certificate in Microsoft Entra ID (formerly Azure Active Directory). For more information, see [this Microsoft article](#). When generating a new self-signed certificate, Veeam Backup for Microsoft 365 will register it automatically.

NOTE

Veeam Backup for Microsoft 365 uses this SSL certificate only for the Azure AD application that you are registering. To communicate with the Veeam Backup for Microsoft 365 server and perform restore operations, Restore Portal uses the REST API SSL certificate. For more information, see [REST API Settings](#).

5. In the **Restore Portal web address** field, specify web address of a machine with the Veeam Backup for Microsoft 365 REST API component installed. Restore operators and end users will use this web address to open Restore Portal in a web browser window.

Consider the following:

- The website is available over HTTPS protocol only.
- By default, port *4443* must be opened on the Veeam Backup for Microsoft 365 server or a machine with the Veeam Backup for Microsoft 365 REST API component installed. For more information, see [Ports](#).
- If you configured a different port in the REST API settings, you must specify the same value for the Restore Portal web address. Otherwise, Restore Portal will be unavailable. For more information, see [REST API Settings](#).
- The web address must be specified in one of the following formats:
 - `https://<IPv4 address>:<port number>`, where `<IPv4 address>` is a public IPv4 address of a machine with the Veeam Backup for Microsoft 365 REST API component installed. For example, `https://135.169.170.192:4443`.
 - `https://<DNS hostname>:<port number>`, where `<DNS hostname>` is DNS hostname of a machine with the Veeam Backup for Microsoft 365 REST API component installed. For example, `https://portal.abc.com:4443`.

The screenshot shows a 'Configure Application' dialog box with the following fields and values:

- Region: Default
- Name: Azure AD application for Restore Portal
- Certificate to authenticate with Azure AD: OC9C6527E6FE36F0031B76C11C6E820FE5949AF4
- Restore Portal web address: https://portal.abc.com:4443

Buttons: Back, Next, Cancel

Configuring Existing Azure AD Application

You can configure an existing Azure AD application to connect to Restore Portal. Veeam Backup for Microsoft 365 checks the Azure AD application permissions, grants the missing [permissions](#) if needed and updates an SSL certificate.

To configure an existing application, do the following:

1. From the **Region** drop-down list, select a Microsoft Azure region.

Keep in mind that if you change your Microsoft Azure region, you must also specify another Azure AD application.

2. In the **Application ID** field, specify an identification number of Azure AD application that you want to use to connect to Restore Portal.

You can find this number in the application settings of your Microsoft Entra ID (formerly Azure Active Directory). For more information, see [this Microsoft article](#).

3. Click **Install** to specify an SSL certificate that you want to use for data exchange between Restore Portal and the created Azure AD application.

4. In the **Select Certificate** wizard, select a certificate. For more information, see [Installing SSL Certificates](#).

You can generate a new self-signed certificate or use an existing one. Before using an existing certificate, make sure to register this certificate in Microsoft Entra ID (formerly Azure Active Directory). For more information, see [this Microsoft article](#). When generating a new self-signed certificate, Veeam Backup for Microsoft 365 will register it automatically.

NOTE

Veeam Backup for Microsoft 365 uses this SSL certificate only for the Azure AD application that you are configuring. To communicate with the Veeam Backup for Microsoft 365 server and perform restore operations, Restore Portal uses the REST API SSL certificate. For more information, see [REST API Settings](#).

5. In the **Restore Portal web address** field, specify web address of a machine with the Veeam Backup for Microsoft 365 REST API component installed. Restore operators and end users will use this web address to open Restore Portal in a web browser window.

Consider the following:

- The website is available over HTTPS protocol only.
- By default, port *4443* must be opened on the Veeam Backup for Microsoft 365 server or a machine with the Veeam Backup for Microsoft 365 REST API component installed. For more information, see [Ports](#).
- If you configured a different port in the REST API settings, you must specify the same value for the Restore Portal web address. Otherwise, Restore Portal will be unavailable. For more information, see [REST API Settings](#).
- The web address must be specified in one of the following formats:
 - `https://<IPv4 address>:<port number>`, where `<IPv4 address>` is a public IPv4 address of a machine with the Veeam Backup for Microsoft 365 REST API component installed. For example, `https://135.169.170.192:4443`.

- `https://<DNS hostname>:<port number>`, where `<DNS hostname>` is DNS hostname of a machine with the Veeam Backup for Microsoft 365 REST API component installed. For example, `https://portal.abc.com:4443`.

The screenshot shows a 'Configure Application' dialog box with a dark green title bar. The main content area is white and contains the following fields and controls:

- Region:** A dropdown menu with 'Default' selected.
- Application ID:** A text input field containing '6e43edef-2c9a-40ab-805a-01f967f67053'.
- Certificate to authenticate with Azure AD:** A text input field containing '09892852067104BD8BFC11E6A59A7B33EAC700A' and an 'Install...' button to its right.
- Restore Portal web address:** A text input field containing 'https://portal.org.com:4443'.

At the bottom of the dialog, there are three buttons: 'Back', 'Next', and 'Cancel'. The 'Next' button is highlighted with a blue border.

Step 4. Log In to Microsoft 365

At this step of the wizard, log in to your Microsoft 365 organization.

To log in to the Microsoft 365 organization, do the following:

1. Click **Copy code** to copy an authentication code.

Keep in mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.

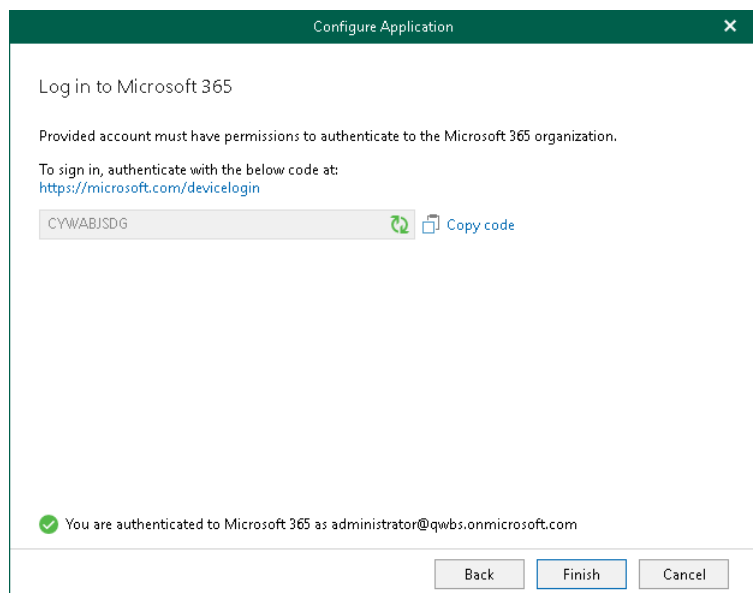
2. Click the Microsoft authentication portal link.

A web browser window opens.

3. On the **Sign in to your account** webpage, paste the code that you have copied and sign in to Microsoft Azure.

Make sure to sign in with the user account that has the *Global Administrator* role. For more information about this role, see [this Microsoft article](#).

4. Return to the **Configure Application** wizard and click **Finish**.



Notification Settings

You can configure notification settings if you want Veeam Backup for Microsoft 365 to send email notifications about backup and backup copy job results.

You can allow Veeam Backup for Microsoft 365 to send email notifications on behalf of your Google or Microsoft 365 account using [OAuth 2.0 Authorization Framework](#), or you can specify connection settings of your SMTP server that uses basic authentication.

For more information, see the following sections:

- [SMTP Server with Basic Authentication](#)
- [Google Account](#)
- [Microsoft 365 Account](#)

NOTE

Notifications about the backup and backup copy job results are sent by a backup proxy server specified in the properties of the backup job. For more information, see [Specify Backup Proxy and Repository](#).

SMTP Server with Basic Authentication

To configure sending email notifications using a custom SMTP server with basic authentication, do the following:

1. In the main menu, click **General Options**.
2. Open the **Notifications** tab.
3. Select the **Enable email notifications** check box.
4. From the **Mail server** drop-down list, select *SMTP server (basic authentication)*.
5. Click **Advanced** to configure advanced settings. You can do the following:
 - Specify a port number of an SMTP server that you want to use.
By default, Veeam Backup for Microsoft 365 uses the port number *587*. For more information, see [this Microsoft article](#).
 - Select the **Connect using SSL** check box to establish a secure connection.
 - If an SMTP server requires an authentication for outgoing mail, select the **The SMTP server requires authentication** check box and provide authentication credentials.
6. In the **SMTP server** field, specify the address of a server that you want to use as an SMTP server.
By default, Veeam Backup for Microsoft 365 establishes a connection to the *smtp.office365.com* server through the port *587*. For more information, see [this Microsoft article](#).
7. In the **From** field, specify the email address to be shown as a sender.
8. In the **To** field, specify the email address of the notification recipient.
To specify multiple email addresses, use semicolon.

9. In the **Subject** field, edit a notification subject if needed.

By default, a notification subject is "*[%JobResult%] %OrgName% - %JobName% (%ObjectCount% objects), %Issues% issues*",

where:

- *%JobResult%*. A job result (*Success, Warning, Failed*).
- *%OrgName%*. A Microsoft 365 organization for which the job was configured.
- *%JobName%*. A job name.
- *%ObjectCount%*. Total number of processed objects.
- *%Issues%*. Number of objects with *Failed* or *Warning* statuses.
- *%Time%*. Date and time of a job completion.

10. Select the **Include detailed report as an attachment** check box if you want to include a detailed report as an email attachment.

If you select this option, Veeam Backup for Microsoft 365 will provide a summary about the job results in the notification body and a detailed report for each object processed by the job in the email attachment. Keep in mind that for jobs that process up to 1000 objects, Veeam Backup for Microsoft 365 always provides both a summary and a detailed report in the notification body.

11. By default, system notifications are sent every time a job session is completed with any of the following statuses: *Success, Warning* and *Failure*. To turn off unwanted notifications, clear check boxes next to the events for which you do not want to receive notifications:

- **Notify on success**

Veeam Backup for Microsoft 365 will send email notifications if a backup or backup copy job completes successfully without any warnings or errors.

- **Notify on warning**

Veeam Backup for Microsoft 365 will send email notifications if a backup or backup copy job completes with warnings.

- **Notify on failure**

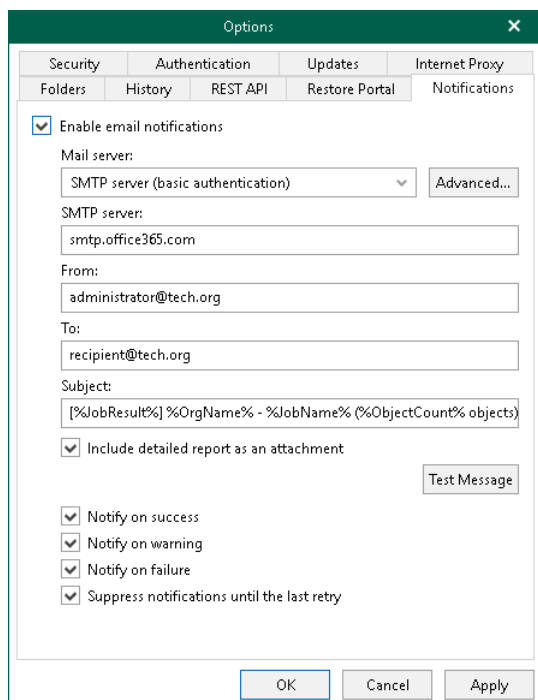
Veeam Backup for Microsoft 365 will send email notifications if a backup or backup copy completes with errors.

12. If a backup or backup copy job is configured to perform retry attempts, select the **Suppress notifications until the last retry** check box to send email notifications according to the job schedule settings. The following email notification scenarios are possible:

- If the job fails, Veeam Backup for Microsoft 365 will send a notification message on the last job retry.
- If the job completes with *Success* or *Warning*, Veeam Backup for Microsoft 365 will send a notification message on the last completion status.
- If the job is scheduled to *Terminate job if it exceeds allowed backup window*, Veeam Backup for Microsoft 365 will send a notification message on the last attempt within the configured interval.

13. Click **Test Message** to send a test message.

14. Click **OK**.



Google Account

You can authorize Veeam Backup for Microsoft 365 to send email notifications on behalf of your Google account. To send notifications, Veeam Backup for Microsoft 365 communicates with the Gmail API. For authentication, Veeam Backup for Microsoft 365 uses an access token issued by Google Authorization Server. To acquire an access token, you can either use an application preinstalled by Veeam or specify OAuth 2.0 client credentials of the custom application registered in the Google Cloud console. For more information on obtaining client credentials, see [Registering Application in Google Cloud Console](#).

To configure sending email notifications on behalf of your Google account, do the following:

1. In the main menu, click **General Options**.
2. Open the **Notifications** tab.
3. Select the **Enable email notifications** check box.
4. From the **Mail server** drop-down list, select *Google Gmail (modern authentication)*.
5. Do one of the following:
 - To use an application preinstalled by Veeam, click **Sign in with Google** and enter credentials of your Google account to complete authentication.
 - To use the custom application, click **Advanced** to specify [the advanced settings](#), then click **Sign in with Google** and enter credentials of your Google account to complete authentication.
6. In the **From** field, specify the email address to be shown as a sender.
7. In the **To** field, specify the email address of the notification recipient.
To specify multiple email addresses, use semicolon.

8. In the **Subject** field, edit a notification subject if needed.

By default, a notification subject is "[%JobResult%] %OrgName% - %JobName% (%ObjectCount% objects), %Issues% issues",

where:

- *%JobResult%*. A job result (*Success*, *Warning*, *Failed*).
- *%OrgName%*. A Microsoft 365 organization for which the job was configured.
- *%JobName%*. A job name.
- *%ObjectCount%*. Total number of processed objects.
- *%Issues%*. Number of objects with *Failed* or *Warning* statuses.
- *%Time%*. Date and time of a job completion.

9. Select the **Include detailed report as an attachment** check box if you want to include a detailed report as an email attachment.

If you select this option, Veeam Backup for Microsoft 365 will provide a summary about the job results in the notification body and a detailed report for each object processed by the job in the email attachment. Keep in mind that for jobs that process up to 1000 objects, Veeam Backup for Microsoft 365 always provides both a summary and a detailed report in the notification body.

10. By default, system notifications are sent every time a job session is completed with any of the following statuses: *Success*, *Warning* and *Failure*. To turn off unwanted notifications, clear check boxes next to the events for which you do not want to receive notifications:

- **Notify on success**

Veeam Backup for Microsoft 365 will send email notifications if a backup or backup copy job completes successfully without any warnings or errors.

- **Notify on warning**

Veeam Backup for Microsoft 365 will send email notifications if a backup or backup copy job completes with warnings.

- **Notify on failure**

Veeam Backup for Microsoft 365 will send email notifications if a backup or backup copy completes with errors.

11. If a backup or backup copy job is configured to perform retry attempts, select the **Suppress notifications until the last retry** check box to send email notifications according to the job schedule settings. The following email notification scenarios are possible:

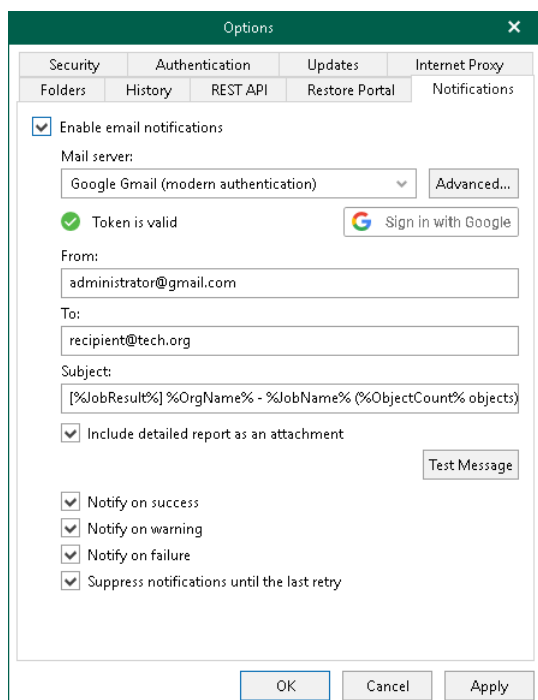
- If the job fails, Veeam Backup for Microsoft 365 will send a notification message on the last job retry.
- If the job completes with *Success* or *Warning*, Veeam Backup for Microsoft 365 will send a notification message on the last completion status.
- If the job is scheduled to *Terminate job if it exceeds allowed backup window*, Veeam Backup for Microsoft 365 will send a notification message on the last attempt within the configured interval.

12. Click **Test Message** to send a test message.

13. Click **OK**.

NOTE

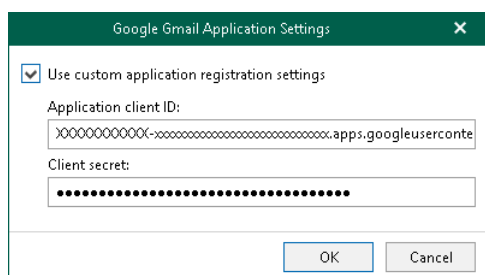
You can change the sender email address. To send email notifications on behalf of another Google account, specify a new email address in the **From** field and click **Sign in with Google**.



Configuring Advanced Settings

In the **Google Gmail Application Settings** window, select the **Use custom application registration settings** check box and specify the following:

1. In the **Application client ID** field, specify the obtained client ID.
2. In the **Client secret** field, specify the client secret.



Registering Application in Google Cloud Console

To register an application in the Google Cloud console, do the following:

1. Sign in to the Google Cloud console under a Google account that you want to use for sending emails.
2. Create a new project and enable *Gmail API* for the project.
You can do this with [the Google setup tool](#).
3. Configure *OAuth consent screen* for your project.

4. Create the *OAuth 2.0 client ID* credentials – a client ID and client secret for the custom application.
5. Record the following data required for acquiring an access token:
 - Client ID
 - Client secret

Microsoft 365 Account

You can authorize Veeam Backup for Microsoft 365 to send email notifications on behalf of your Microsoft 365 account. To send notifications, Veeam Backup for Microsoft 365 communicates with the Microsoft Graph API. For authentication, Veeam Backup for Microsoft 365 uses an access token issued by the Microsoft identity platform. To acquire an access token, you can either use an application preinstalled by Veeam or specify details of the custom Azure AD application registered in the Azure portal. For more information on obtaining client credentials, see [Registering Application in Azure Portal](#).

To configure sending email notifications on behalf of your Microsoft 365 account, do the following:

1. In the main menu, click **General Options**.
2. Open the **Notifications** tab.
3. Select the **Enable email notifications** check box.
4. From the **Mail server** drop-down list, select *Microsoft 365 (modern authentication)*.
5. Do one of the following:
 - To use an application preinstalled by Veeam, click **Authorize now** and enter credentials of your Microsoft 365 account to complete authentication.
 - To use the custom application, click **Advanced** to specify [the advanced settings](#), then click **Authorize now** and enter credentials of your Microsoft 365 account to complete authentication.
6. In the **From** field, specify the email address to be shown as a sender.
7. In the **To** field, specify the email address of the notification recipient.
To specify multiple email addresses, use semicolon.
8. In the **Subject** field, edit a notification subject if needed.

By default, a notification subject is "*[%JobResult%] %OrgName% - %JobName% (%ObjectCount% objects), %Issues% issues*",

where:

- *%JobResult%*. A job result (*Success, Warning, Failed*).
- *%OrgName%*. A Microsoft 365 organization for which the job was configured.
- *%JobName%*. A job name.
- *%ObjectCount%*. Total number of processed objects.
- *%Issues%*. Number of objects with *Failed* or *Warning* statuses.
- *%Time%*. Date and time of a job completion.

9. Select the **Include detailed report as an attachment** check box if you want to include a detailed report as an email attachment.

If you select this option, Veeam Backup for Microsoft 365 will provide a summary about the job results in the notification body and a detailed report for each object processed by the job in the email attachment. Keep in mind that for jobs that process up to 1000 objects, Veeam Backup for Microsoft 365 always provides both a summary and a detailed report in the notification body.

10. By default, system notifications are sent every time a job session is completed with any of the following statuses: *Success*, *Warning* and *Failure*. To turn off unwanted notifications, clear check boxes next to the events for which you do not want to receive notifications:

- **Notify on success**

Veeam Backup for Microsoft 365 will send email notifications if a backup or backup copy job completes successfully without any warnings or errors.

- **Notify on warning**

Veeam Backup for Microsoft 365 will send email notifications if a backup or backup copy job completes with warnings.

- **Notify on failure**

Veeam Backup for Microsoft 365 will send email notifications if a backup or backup copy completes with errors.

11. If a backup or backup copy job is configured to perform retry attempts, select the **Suppress notifications until the last retry** check box to send email notifications according to the job schedule settings. The following email notification scenarios are possible:

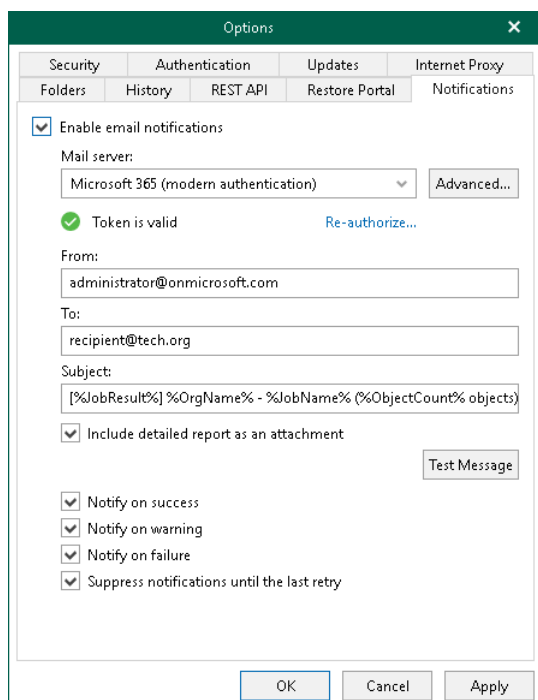
- If the job fails, Veeam Backup for Microsoft 365 will send a notification message on the last job retry.
- If the job completes with *Success* or *Warning*, Veeam Backup for Microsoft 365 will send a notification message on the last completion status.
- If the job is scheduled to *Terminate job if it exceeds allowed backup window*, Veeam Backup for Microsoft 365 will send a notification message on the last attempt within the configured interval.

12. Click **Test Message** to send a test message.

13. Click **OK**.

NOTE

You can change the sender email address. To send email notifications on behalf of another Microsoft 365 account, specify a new email address in the **From** field and click **Re-authorize**.

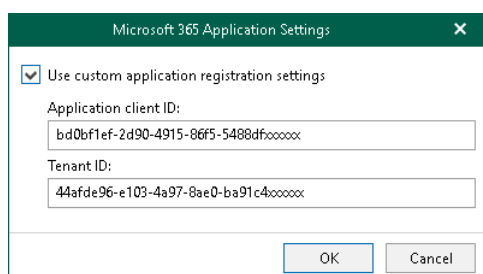


The screenshot shows the 'Options' dialog box with the 'Notifications' tab selected. The 'Enable email notifications' checkbox is checked. The 'Mail server' dropdown is set to 'Microsoft 365 (modern authentication)'. The 'Token is valid' status is shown with a green checkmark and a 'Re-authorize...' link. The 'From' field contains 'administrator@onmicrosoft.com', the 'To' field contains 'recipient@tech.org', and the 'Subject' field contains a placeholder: '[%JobResult%] %OrgName% - %JobName% (%ObjectCount% objects)'. There are checkboxes for 'Include detailed report as an attachment', 'Notify on success', 'Notify on warning', 'Notify on failure', and 'Suppress notifications until the last retry'. A 'Test Message' button is also present.

Configuring Advanced Settings

In the **Microsoft 365 Application Settings** window, select the **Use custom application registration settings** check box and specify:

6. In the **Application client ID** field, specify an identification number of your Microsoft Entra application.
You can find this number in an application settings in your Microsoft Entra ID. For more information, see [this Microsoft article](#).
7. In the **Tenant ID** field, specify the Microsoft Entra tenant ID.



The screenshot shows the 'Microsoft 365 Application Settings' dialog box. The 'Use custom application registration settings' checkbox is checked. The 'Application client ID' field contains 'bd0bf1ef-2d90-4915-86f5-5488dfxxxxx' and the 'Tenant ID' field contains '44afde96-e103-4a97-8ae0-ba91c4xxxxx'.

Registering Application in Azure Portal

To register an application in Microsoft Identity platform, do the following:

1. Sign in to Microsoft Identity platform using an account that you want to use for sending emails. The account must have an active subscription.
2. Register an application. For more information on registering applications, see [this Microsoft article](#).

3. Select **API permissions** and grant the application the *Mail.Send* permission of the *Application* type for the Microsoft Graph API.
4. Select **Authentication > Platform configurations > Add a platform > Configure platforms > Mobile and desktop applications** and specify *http://localhost* as a redirect URI. For more information, see [this Microsoft article](#).
5. Record the following data required for acquiring an access token:
 - Directory (tenant) ID
 - Application (client) ID

Security Settings

Veeam Backup for Microsoft 365 uses an SSL certificate to communicate with a backup proxy server deployed in a workgroup. By default, Veeam Backup for Microsoft 365 uses a certificate automatically generated by the product during the installation process. You can view this certificate or install a custom certificate, if necessary.

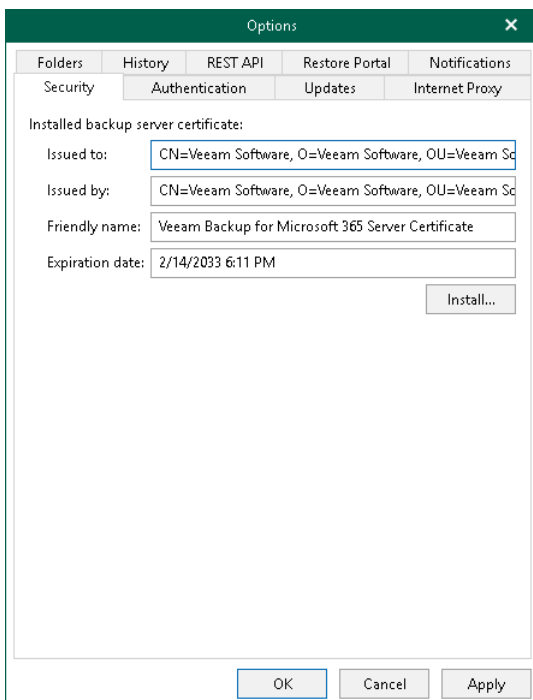
To configure security settings, do the following:

1. In the main menu, click **General Options**.
2. Open the **Security** tab.
3. In the **Installed backup server certificate** section, review information about the certificate that is used to establish a connection with a backup proxy server deployed in a workgroup.

If you want to use another certificate, click **Install** to specify an SSL certificate. You can generate a new certificate or select an existing certificate using the **Select Certificate** wizard. For more information, see [Installing SSL Certificates](#).

4. Click **OK**.

Veeam Backup for Microsoft 365 will install a new certificate. If a previously installed certificate is already used by one or more workgroup backup proxy servers, Veeam Backup for Microsoft 365 will connect to these backup proxy servers and update certificate settings. After that, the Veeam Backup for Microsoft 365 server and backup proxy servers will communicate using the new certificate.



Authentication Settings

You can configure authentication settings to the Veeam Backup for Microsoft 365 server for tenants and restore operators.

Authentication to the Veeam Backup for Microsoft 365 server is required for them to connect to Veeam Backup for Microsoft 365 and perform restore operations within the following usage scenarios:

- *Backup as a Service for Microsoft 365.* In this scenario, tenants authenticate to Veeam Backup for Microsoft 365 server with Microsoft organization credentials.

Enabling tenant authentication is required for users from tenant organizations to view and restore backups that are located on the service provider side. For more information, see [Enabling tenant authentication](#).

- *Operator restore.* In this scenario, restore operators authenticate to Veeam Backup for Microsoft 365 with their Microsoft 365 credentials. Restore operators use Restore Portal to view and restore data from backups created by Veeam Backup for Microsoft 365 for other users, groups, sites, teams or the entire Microsoft 365 organization.

Enabling restore operator authentication is required if you want to configure Restore Portal. For more information, see [Enabling restore operator authentication](#).

NOTE

To configure access to Veeam Backup for Microsoft 365 for users and restore operators from multiple tenant organizations, you must enable both options.

Enabling Tenant Authentication

To enable tenant authentication, do the following:

1. In the main menu, click **General Options**.
2. Open the **Authentication** tab.
3. Select the **Enable tenants authentication with organization credentials** check box.
4. Click **Install** to specify an SSL certificate.

You can generate a new certificate or select an existing certificate using the **Select Certificate** wizard. For more information, see [Installing SSL Certificates](#).

5. Click **OK**.

TIP

You can use the same certificate for both Veeam Backup for Microsoft 365 and Veeam Backup & Replication.

Enabling Restore Operator Authentication

To enable restore operator authentication, do the following:

1. In the main menu, click **General Options**.
2. Open the **Authentication** tab.

3. Select the **Enable restore operator authentication with Microsoft credentials** check box.
4. Click **Install** to specify an SSL certificate.

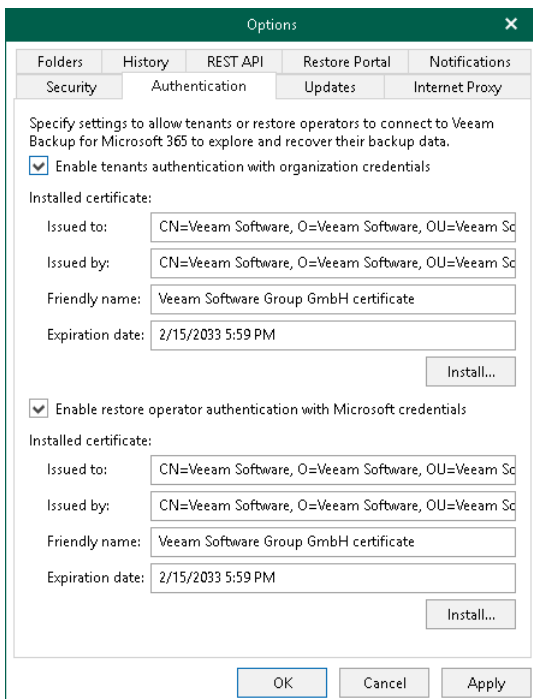
You can generate a new certificate or select an existing certificate using the **Select Certificate** wizard. For more information, see [Installing SSL Certificates](#).

Veeam Backup for Microsoft 365 will use this certificate to encrypt network traffic between *Veeam Backup for Microsoft 365 Service* and *Veeam Backup for Microsoft 365 REST API Service*.

NOTE

If you have installed the Veeam Backup for Microsoft 365 REST API component on a separate machine and generated a new self-signed certificate for restore operators, you must import this certificate to the Trusted Root Certification Authorities certificate store on the separate machine with REST API installed.

5. Click **OK**.



New Versions and Automatic Updates

You can configure whether Veeam Backup for Microsoft 365 will notify you when new versions appear on Veeam servers and allow Veeam Backup for Microsoft 365 to download available updates automatically.

To configure notifications on new versions and automatic updates, do the following:

1. In the main menu, click **General Options**.
2. Open the **Updates** tab.
3. Select the **Automatically check and notify me on available updates** check box.

If you select this check box, Veeam Backup for Microsoft 365 will notify you about available updates with a dialog message in the user interface.

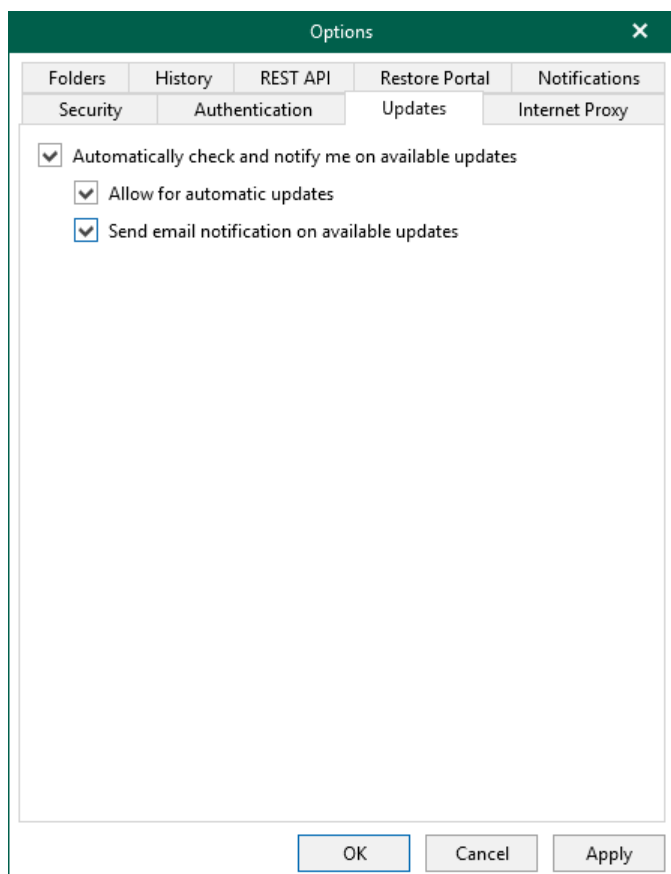
4. Select the following check boxes:
 - **Allow for automatic updates.** If you select this check box, Veeam Backup for Microsoft 365 will regularly check Veeam servers for critical updates. If a new critical update is available, Veeam Backup for Microsoft 365 will notify you about available update with an email message, download this update in the background and install it to the backup infrastructure components.
 - **Send email notification on available updates.** If you select this check box, Veeam Backup for Microsoft 365 will notify you about available updates with an email message.

For sending email notifications, Veeam Backup for Microsoft 365 uses the email notification settings. For more information, see [Notification Settings](#).

5. Click **OK**.

TIP

For information on how to update Veeam Backup for Microsoft 365, see [Updating Veeam Backup for Microsoft 365](#).



Global Internet Proxy Server Settings

If a server on which Veeam Backup for Microsoft 365 is deployed does not have a direct access to the internet, you can assign an internet proxy server to be used as a gateway.

NOTE

When you allow Veeam Backup for Microsoft 365 to use internet proxy and you configure new connection settings to an internet proxy server, the product overwrites the system proxy settings for Microsoft Windows HTTP Services (WinHTTP).

To enable usage of an internet proxy server, do the following:

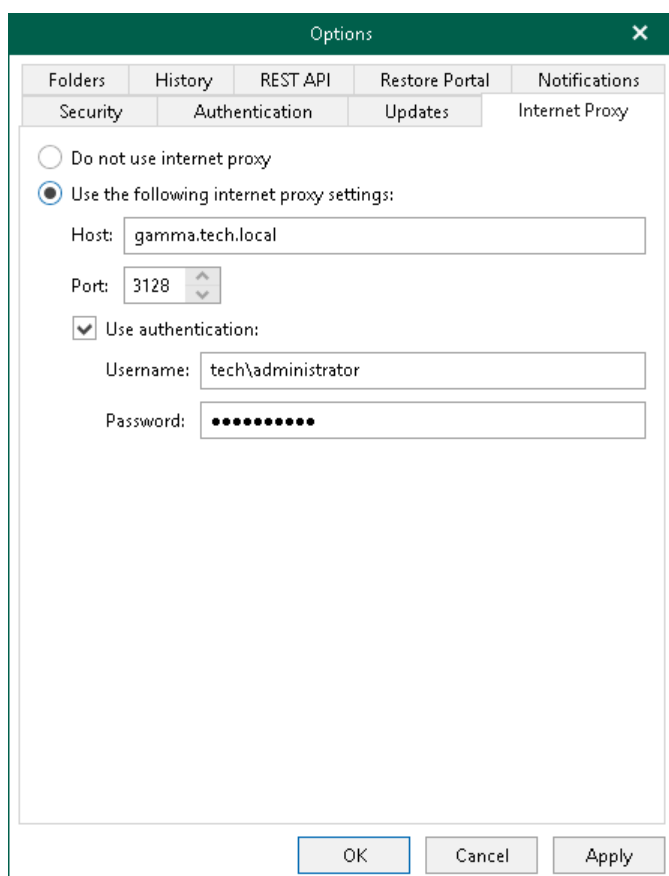
1. In the main menu, click **General Options**.
2. Open the **Internet Proxy** tab.
3. Select the **Use the following internet proxy settings** option.
4. In the **Host** field, specify a server that has access to the internet and which you want to use as your internet proxy.

You can provide a DNS or IP address of a server.

5. In the **Port** field, provide a port number over which to connect to the specified server.
6. Select the **Use authentication** check box to provide authentication credentials to access the internet proxy server.
7. Click **OK**.

TIP

Also, you can configure an internet proxy server for each of your backup proxies. For more information, see [Configuring Internet Proxy Server for Backup Proxies](#).



To disable usage of the internet proxy server, do the following:

1. In the main menu, click **General Options**.
2. Open the **Internet Proxy** tab.
3. Select the **Do not use internet proxy** option.

NOTE

After you disable usage of the internet proxy, you must reset the WinHTTP settings. To do this, open the Command Prompt and run the `netsh winhttp reset proxy` command.

Configuring REST API and Restore Portal on Separate Machine

To configure REST API and Restore Portal on a separate machine, do the following:

1. Open the Veeam Backup for Microsoft 365 REST API component installation folder.
By default, Veeam Backup for Microsoft 365 REST API component is installed to the `C:\Program Files\Veeam\Backup365` folder.
2. Run the `Veeam.Archiver.REST.Configurator.exe` file.
The **Veeam Backup for Microsoft 365** window opens.
3. Configure REST API settings. For more information, see [Configuring REST API Settings](#).
4. Configure Restore Portal settings. For more information, see [Configuring Restore Portal Settings](#).
5. Click **Apply**.
6. Click **OK** to close the **Veeam Backup for Microsoft 365** window.

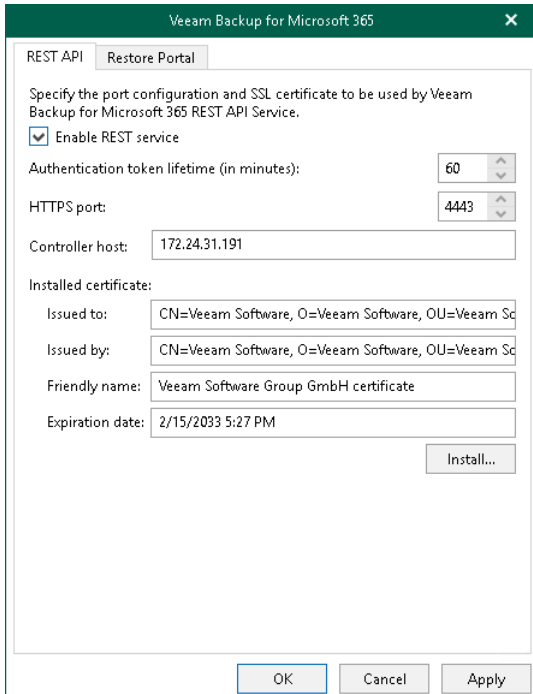
Configuring REST API Settings

On the **RESTAPI** tab, do the following:

1. Select the **Enable REST service** check box.
2. In the **Authentication token lifetime** field, specify the lifetime value for an authentication token (in minutes).
REST API authorization is based on the [OAuth 2.0 Authorization Framework](#).
3. In the **HTTPS port** field, specify a port number which Veeam Backup for Microsoft 365 use to access *Veeam Backup for Microsoft 365 REST API Service*.
4. In the **Controller host** field, specify a DNS name or IP address of the Veeam Backup for Microsoft 365 server.
5. Click **Install** to specify an SSL certificate.
You can generate a new certificate or select an existing certificate using the **Select Certificate** wizard. For more information, see [Installing SSL Certificates](#).

NOTE

If you have generated a new [self-signed certificate for restore operators](#), you must import the certificate for restore operators to the Trusted Root Certification Authorities certificate store on the separate machine with REST API installed.



The screenshot shows the 'Veeam Backup for Microsoft 365' dialog box with the 'Restore Portal' tab selected. The dialog contains the following fields and controls:

- Enable REST service:** A checked checkbox.
- Authentication token lifetime (in minutes):** A spinner box set to 60.
- HTTPS port:** A spinner box set to 4443.
- Controller host:** A text box containing '172.24.31.191'.
- Installed certificate:** A section with several text boxes:
 - Issued to:** 'CN=Veeam Software, O=Veeam Software, OU=Veeam Sc'
 - Issued by:** 'CN=Veeam Software, O=Veeam Software, OU=Veeam Sc'
 - Friendly name:** 'Veeam Software Group GmbH certificate'
 - Expiration date:** '2/15/2033 5:27 PM'
- Buttons:** 'OK', 'Cancel', 'Apply', and 'Install...'.

Configuring Restore Portal Settings

On the **Restore Portal** tab, do the following:

1. Select the **Enable Restore Portal** check box.
2. From the **Region** drop-down list, select a Microsoft Azure region.
Keep in mind that if you change your Microsoft Azure region, you must also specify another Azure AD application.
3. In the **Application ID** field, specify an identification number of Azure AD application that you want to use to access Restore Portal.
You can find this identification number in the application settings of your Microsoft Entra ID (formerly Azure Active Directory). For more information, see [this Microsoft article](#). Make sure to manually grant the [required permissions](#) to your Azure AD application.
4. In the **Restore Portal URL** field, specify web address of a machine with the Veeam Backup for Microsoft 365 REST API component installed. Restore operators and end users will use this web address to open Restore Portal in a web browser window.

Consider the following:

- The website is available over HTTPS protocol only.
- By default, port **4443** must be opened on the Veeam Backup for Microsoft 365 server or a machine with the Veeam Backup for Microsoft 365 REST API component installed. For more information, see [Ports](#).

- The web address must be specified in one of the following formats:
 - `https://<IPv4 address>:<port number>`, where <IPv4 address> is a public IPv4 address of a machine with the Veeam Backup for Microsoft 365 REST API component installed. For example, `https://135.169.170.192:4443`.
 - `https://<DNS hostname>:<port number>`, where <DNS hostname> is DNS hostname of a machine with the Veeam Backup for Microsoft 365 REST API component installed. For example, `https://portal.abc.com:4443`.
5. In the **Application certificate** section, click **Install** to specify an SSL certificate that you want to use for data exchange between Restore Portal and the specified Azure AD application.

You can generate a new certificate or select an existing certificate using the **Select Certificate** wizard. For more information, see [Installing SSL Certificates](#).

NOTE

If you generated a new self-signed certificate for the specified Azure AD application, you must add this certificate in the application settings of your Microsoft Entra ID (formerly Azure Active Directory).

SSL Certificates Overview

When you manage Microsoft 365 organizations and configure general application settings and backup infrastructure, Veeam Backup for Microsoft 365 requires to install an SSL certificate.

SSL Certificate Usage Scenarios

The following table lists usage scenarios when Veeam Backup for Microsoft 365 requires to install an SSL certificate.

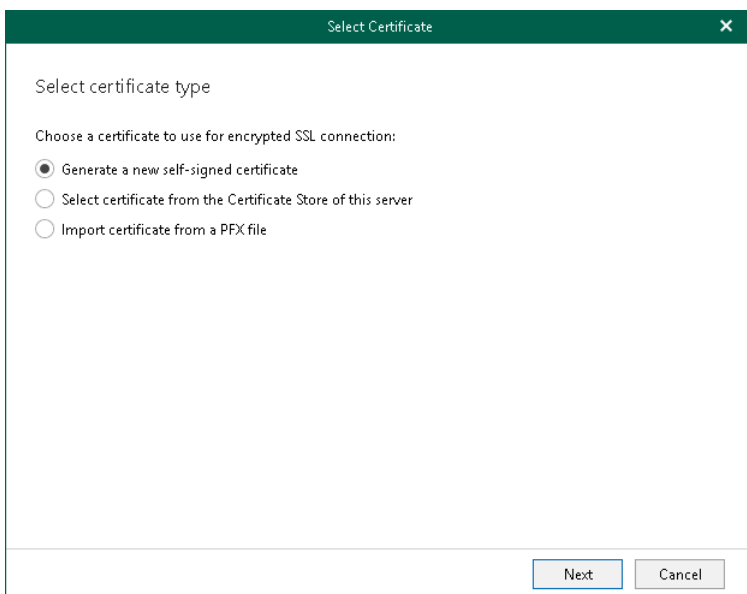
Usage Scenario	Description	Reference
Managing Microsoft 365 Organization	Required to establish communication and data exchange between Veeam Backup for Microsoft 365 and Azure AD application when adding Microsoft 365 organizations.	For more information, see Adding Microsoft 365 Organizations .
	Required to establish communication and data exchange between Veeam Backup for Microsoft 365 and Azure AD application when configuring backup applications.	For more information, see Backup Applications .
Communicating with Backup Proxy Server	Required to establish communication and data exchange between the Veeam Backup for Microsoft 365 server and a backup proxy server deployed in a workgroup.	For more information, see Security Settings .
Communicating with REST API on Veeam Backup for Microsoft 365 server	Required to establish communication and data exchange between the following: <ul style="list-style-type: none"> • <i>Veeam Backup for Microsoft 365 REST API Service</i> and the Veeam Backup for Microsoft 365 server • Restore Portal and Veeam Backup for Microsoft 365 	For more information, see REST API Settings .
Communicating with REST API on Separate Machine	Required to establish communication and data exchange between the following: <ul style="list-style-type: none"> • <i>Veeam Backup for Microsoft 365 REST API Service</i> and the Veeam Backup for Microsoft 365 server • Restore Portal and Veeam Backup for Microsoft 365 	For more information, see Configuring REST API and Restore Portal on Separate Machine .
Communicating with Restore Portal	Required to establish communication and data exchange between the Veeam Backup for Microsoft 365 server, Microsoft 365 organization, Azure AD application, <i>Veeam Backup for Microsoft 365 REST API Service</i> and Restore Portal.	For more information, see Restore Portal Settings , Configuring REST API and Restore Portal on Separate Machine , How Restore Portal Works .

Usage Scenario	Description	Reference
Authenticating Restore Operators to Veeam Backup for Microsoft 365 server	Required to authenticate restore operators to Veeam Backup for Microsoft 365 with Microsoft 365 credentials and encrypt network traffic between <i>Veeam Backup for Microsoft 365 Service</i> and <i>Veeam Backup for Microsoft 365 REST API Service</i> .	For more information, see Authentication Settings .
Authenticating Tenants to Veeam Backup for Microsoft 365 in Service Provider Infrastructure	Required to authenticate tenants to Veeam Backup for Microsoft 365 with Microsoft organization credentials.	For more information, see Authentication Settings and Backup as Service for Microsoft 365 .

Installing SSL Certificates

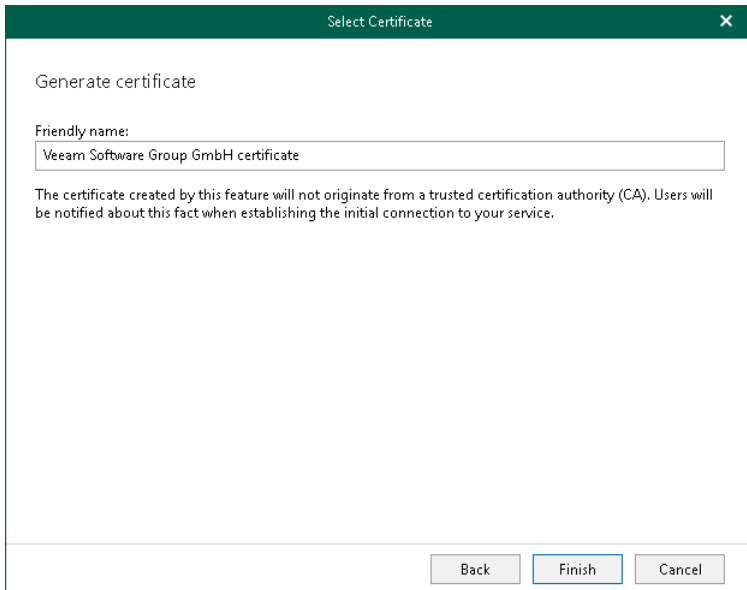
To install an SSL certificate from the Veeam Backup for Microsoft 365 console main menu, do the following:

1. In the main menu, click **General Options**.
2. Open either the **REST API**, or **Restore Portal**, or **Security**, or **Authentication** tab.
3. Click **Install** to run the **Select Certificate** wizard.
4. Proceed to any of the following options:
 - [Generate new self-signed certificate](#)
 - [Select certificate from the Certificate Store of this server](#)
 - [Import certificate from PFX file](#)



Generating New Certificate

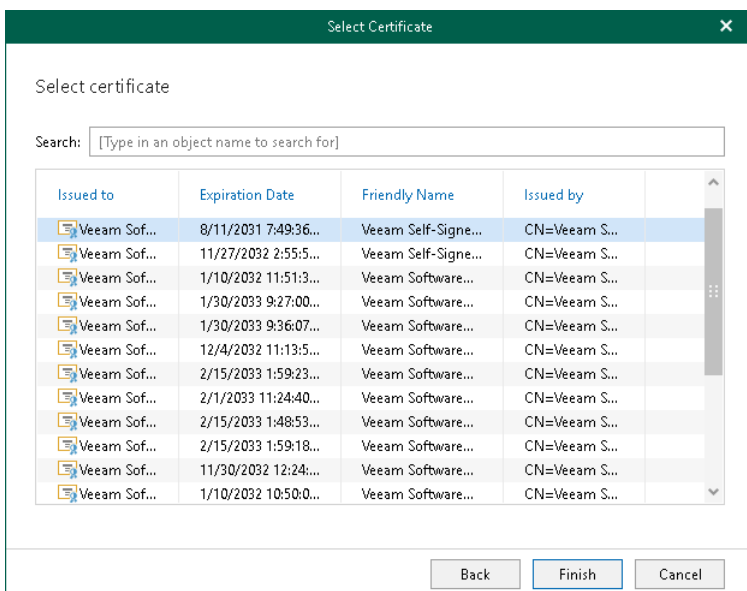
To generate a new certificate, specify a certificate name and click **Finish**.



Selecting Certificate

To select an existing certificate from the certificate store, select a certificate that you want to use and click **Finish**.

For communicating with backup proxy server, Veeam Backup for Microsoft 365 requires a certificate from the Trusted Root Certification Authorities certificate store. In other usage scenarios, use a certificate from the Personal\Certificates directory. The certificate key must be exportable. For more information about an SSL certificate usage scenarios, see [SSL Certificate Usage Scenarios](#).



Importing Certificate

To import a certificate, do the following:

1. Click **Browse** and select a PFX file to use.
2. In the **Password** field, specify the certificate password.
3. Click **Finish**.

Select Certificate

Import certificate

Certificate:
C:\Certificate.pfx

Password:
●●●●●●●●●●

A password is only required if this certificate was exported with password protection enabled.

Backup Infrastructure

The backup infrastructure of Veeam Backup for Microsoft 365 consists of the following:

- [Backup proxy servers](#)

Backup proxy servers are auxiliary machines that you configure to conduct all read and write activities, route backup traffic, handle data compression and encryption and send email notifications.

- [Backup repositories](#)

Backup repositories are storage systems within the backup infrastructure where Veeam Backup for Microsoft 365 saves backups and backup copies.

- [Object storage](#)

Object storage is cloud-based or on-premises storage system that you employ to store your backups and backup copies as part of the extended backup repository storage system. Keep in mind that you can use Azure Blob Storage Archive access tier, Amazon S3 Glacier Instant Retrieval, Amazon S3 Glacier Flexible Retrieval and Amazon S3 Glacier Deep Archive storage classes only as a target for backup copy jobs.

Backup Proxy Servers

A backup proxy server is an architecture component that conducts all read and write activities during [data backup](#) and [restore](#), routes backup traffic, handles data compression and encryption and sends email notifications about backup and backup copy job results.

Consider the following:

- By default, the role of the backup proxy server is assigned to the machine where Veeam Backup for Microsoft 365 is installed. The default backup proxy server is displayed as *Local* backup proxy in Veeam Backup for Microsoft 365.

After you install Veeam Backup for Microsoft 365, you should configure an additional set of backup proxy servers to manage your data in a more efficient manner.

- A backup proxy server can be a physical or virtual machine.
- Veeam Backup for Microsoft 365 automatically installs the *Veeam Backup Proxy for Microsoft 365 Service* on a computer that you want to use as a backup proxy server when you add a backup proxy server to the Veeam Backup for Microsoft 365 backup infrastructure. For more information, see [Adding Backup Proxy Servers](#).
- Veeam Backup for Microsoft 365 allows you to deploy the following types of backup proxy servers:
 - Domain backup proxy
 - Workgroup backup proxy

For more information, see [Backup Proxy Deployment Scenarios](#).

- Each backup proxy server can process one or several organizations.
- An organization can be processed by one or several backup proxies.
- A backup proxy server is responsible for sending email notifications about backup and backup copy job results.

For more information on how to configure email notification settings, see [Notification Settings](#).

- For each backup proxy server, Veeam Backup for Microsoft 365 saves information about restore points to the `Proxy.sqlite` database file. Veeam Backup for Microsoft 365 collects this information from all backup repositories located on this backup proxy server.

Backup Proxy Deployment Scenarios

Veeam Backup for Microsoft 365 offers the following deployment scenarios for a backup proxy server:

- *Domain backup proxy*

In this scenario, a machine used as a backup proxy server resides in the same domain as the Veeam Backup for Microsoft 365 server or in a trusted domain. To establish a connection with a domain backup proxy, Veeam Backup for Microsoft 365 uses credentials that you provide when you add a backup proxy server to the Veeam Backup for Microsoft 365 infrastructure.

- *Workgroup backup proxy*

In this scenario, a machine used as a backup proxy server resides in a workgroup. To establish a connection with a workgroup backup proxy, Veeam Backup for Microsoft 365 uses an SSL certificate. For more information, see [Security Settings](#).

You can deploy the Veeam Backup for Microsoft 365 server and backup proxy servers in different workgroup-domain combinations.

The following table lists possible variants of interactions between the Veeam Backup for Microsoft 365 server and backup proxy servers in the backup infrastructure.

Veeam Backup for Microsoft 365 server resides in	Backup proxy servers reside in
Domain	Workgroup
Workgroup	Workgroup
Workgroup	Domain
Domain	Domain
Domain	Domain and Workgroup
Workgroup	Domain and Workgroup

Adding Backup Proxy Servers

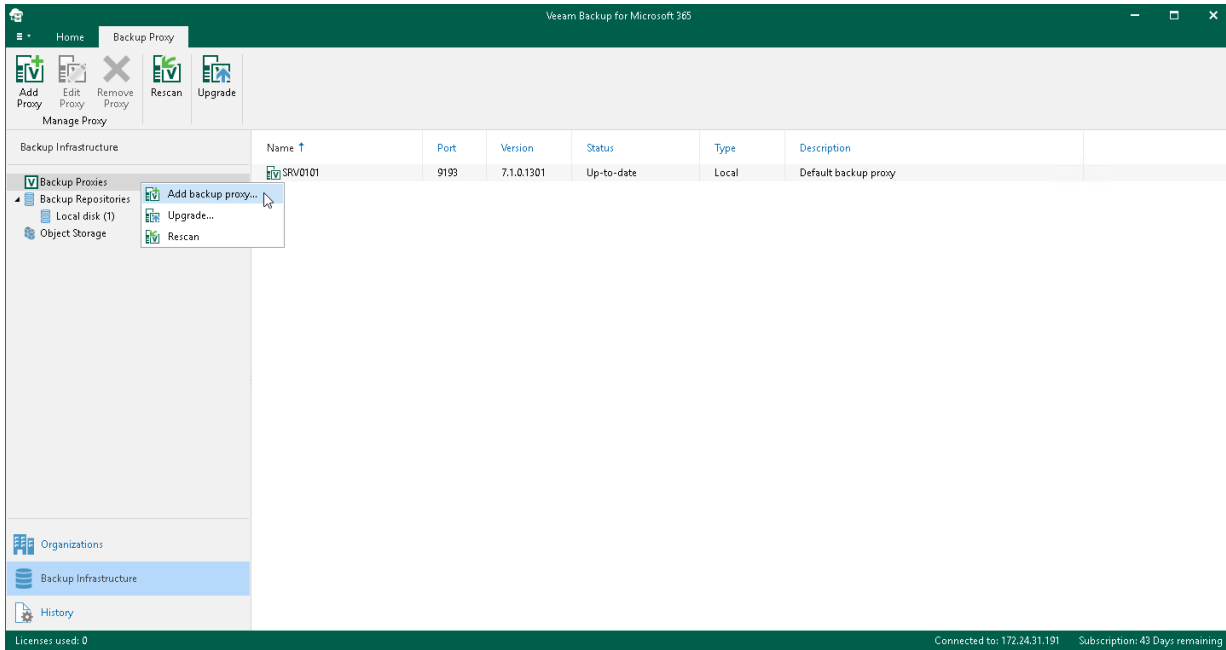
To add a new backup proxy server to the Veeam Backup for Microsoft 365 backup infrastructure, do the following:

1. [Launch the New Backup Proxy wizard.](#)
2. [Specify a backup proxy server address.](#)
3. [Specify credentials.](#)

Step 1. Launch New Backup Proxy Wizard

To launch the **New Backup Proxy** wizard, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Backup Proxies** node.
3. Do one of the following:
 - On the **Backup Proxy** tab, click **Add Proxy** on the ribbon.
 - Right-click the **Backup Proxies** node and select **Add backup proxy**.



Step 2. Specify Backup Proxy Server Address

At this step of the wizard, specify a computer that you want to use as a backup proxy server, its port number and optional description.

1. In the **Host** field, enter a DNS name or IP address of a computer that you want to use as a backup proxy server.

If the specified computer does not have a direct access to the internet, you can [configure an internet proxy server](#) for such a computer.

Make sure that the default admin share ADMIN\$ (C:\Windows) is enabled on the specified computer.

2. In the **Port** field, enter a port number to access the specified computer.
3. If you want to add a domain backup proxy server, select the **Use domain network** check box. Otherwise, Veeam Backup for Microsoft 365 will add a workgroup backup proxy server. For more information, see [Backup Proxy Deployment Scenarios](#).

NOTE

Once the backup proxy server is deployed, you will not be able to change its type from the domain backup proxy to the workgroup backup proxy and vice versa.

4. In the **Description** field, enter optional description.

The screenshot shows a dialog box titled "New Backup Proxy" with a close button (X) in the top right corner. The main heading inside the dialog is "Specify DNS name or IP address of the proxy server". Below this heading, there are two input fields: "Host" and "Port". The "Host" field contains the text "srv05.tech.local". The "Port" field is a spinner box showing the number "9193". Below these fields is a checkbox labeled "Use domain network" which is checked. Underneath the checkbox is a "Description:" label followed by a text area containing the text "Created by SRV0101\Administrator at 1:47:34 PM". At the bottom of the dialog, there are two buttons: "Next" and "Cancel".

Step 3. Specify Credentials

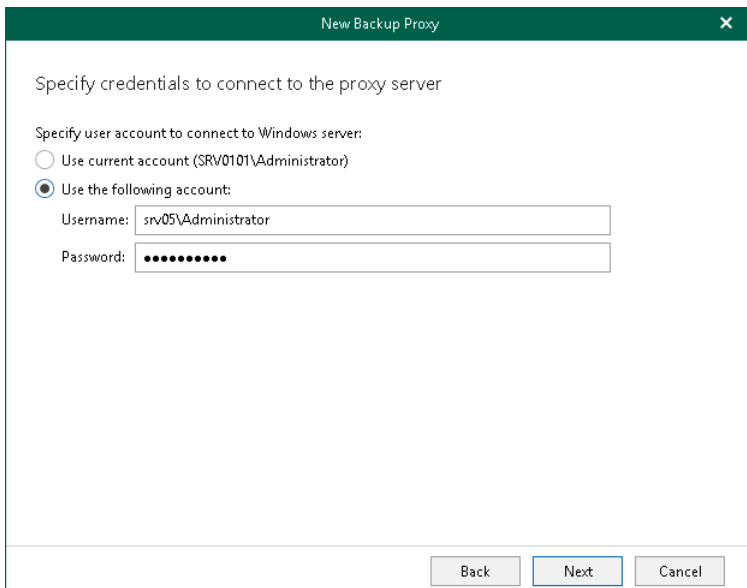
At this step of the wizard, enter user credentials to connect to the [specified computer](#).

The account must be a member of the local *Administrators* group.

Veeam Backup for Microsoft 365 uses the specified credentials for different purposes depending on the type of the backup proxy:

- For a domain backup proxy, Veeam Backup for Microsoft 365 uses credentials for entire communication with the backup proxy server.
- For a workgroup backup proxy, Veeam Backup for Microsoft 365 uses credentials only to connect to a computer in a workgroup and upload backup proxy components to this machine. After the backup proxy is deployed, Veeam Backup for Microsoft 365 uses an SSL certificate to communicate with the backup proxy server.

Once a new proxy is added, you will be prompted to create a new backup repository on this proxy. You can dismiss this step and create a backup repository later. For more information, see [Adding Backup Repository](#).



The screenshot shows a dialog box titled "New Backup Proxy" with a close button (X) in the top right corner. The main text reads "Specify credentials to connect to the proxy server". Below this, there is a section "Specify user account to connect to Windows server:" with two radio button options. The first option is "Use current account (SRV0101\Administrator)" and is unselected. The second option is "Use the following account:" and is selected. Under the second option, there are two text input fields: "Username:" containing "srv05\Administrator" and "Password:" containing a series of dots. At the bottom of the dialog box, there are three buttons: "Back", "Next" (highlighted with a blue border), and "Cancel".

Editing Backup Proxy Server Settings

Veeam Backup for Microsoft 365 allows you to edit settings of your backup proxy server. Actually, when you edit backup proxy server settings, you add the backup proxy anew to the Veeam Backup for Microsoft 365 backup infrastructure with modified settings.

To edit backup proxy server settings, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Backup Proxies** node.
3. In the preview pane, do one of the following:
 - Select a backup proxy server and click **Edit Proxy** on the ribbon.
 - Right-click a backup proxy server and select **Edit**.

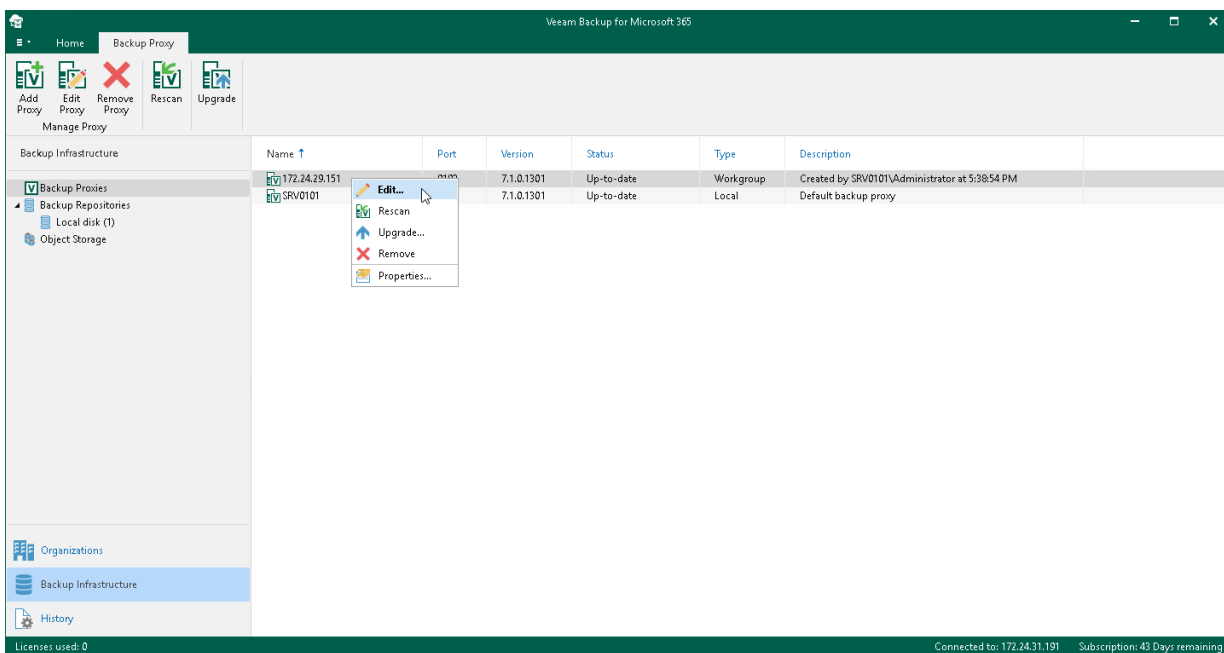
4. Modify the required settings.

You can change the following parameters:

- The port number to access the backup proxy server computer.
- Description.
- User credentials to connect this backup proxy.

Consider the following:

- Editing a proxy server name is prohibited once it is set.
- The **Edit** command is unavailable if a backup proxy server needs to be upgraded. For more information, see [Upgrading Backup Proxy Servers](#).
- You cannot change the type of a backup proxy server from the domain backup proxy to the workgroup backup proxy and vice versa.



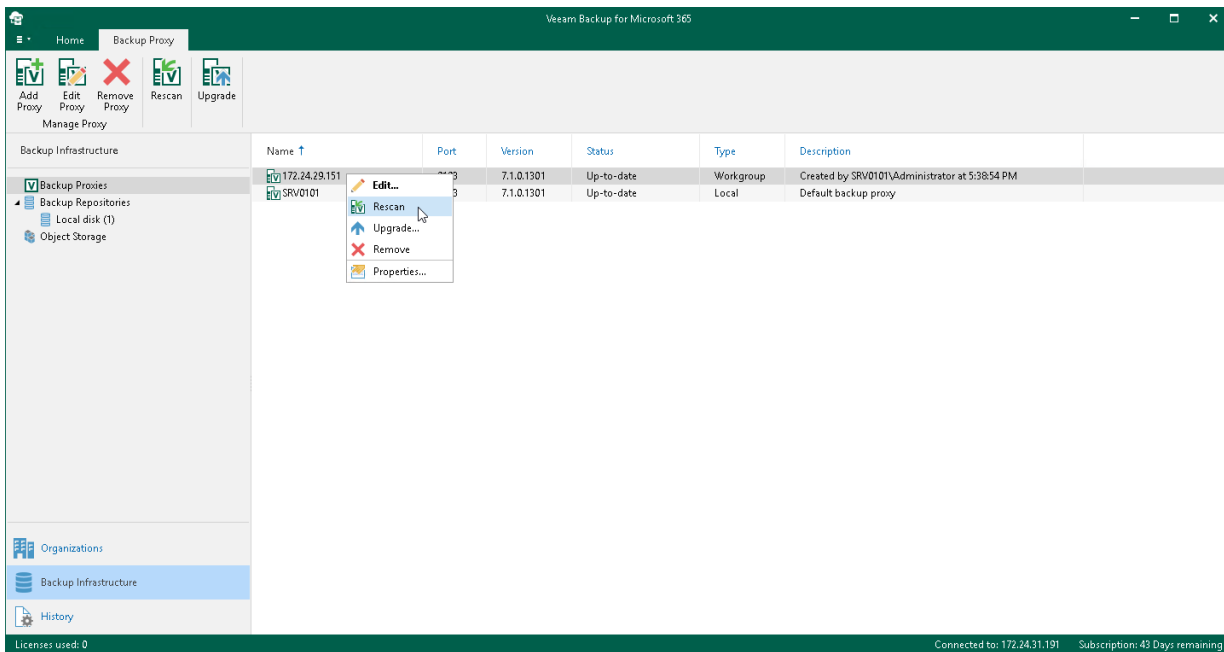
Rescanning Backup Proxy Servers

Rescan is required if some of your backup proxy servers are unavailable.

To rescan a backup proxy server, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Backup Proxies** node.
3. In the preview pane, do one of the following:
 - Select a backup proxy server and click **Rescan** on the ribbon.
 - Right-click a backup proxy server and select **Rescan**.

If you want to rescan all backup proxy servers in your environment, right-click the **Backup Proxies** node and select **Rescan**.



Upgrading Backup Proxy Servers

To communicate with backup proxy servers, Veeam Backup for Microsoft 365 uses the proprietary service – *Veeam Backup Proxy for Microsoft 365 Service* that is installed on the target proxy machine. When you upgrade Veeam Backup for Microsoft 365 to a newer version, this service becomes outdated and all backup proxies configured in your environment are marked as *Out of Date* and must be upgraded manually.

To upgrade backup proxy servers, do the following:

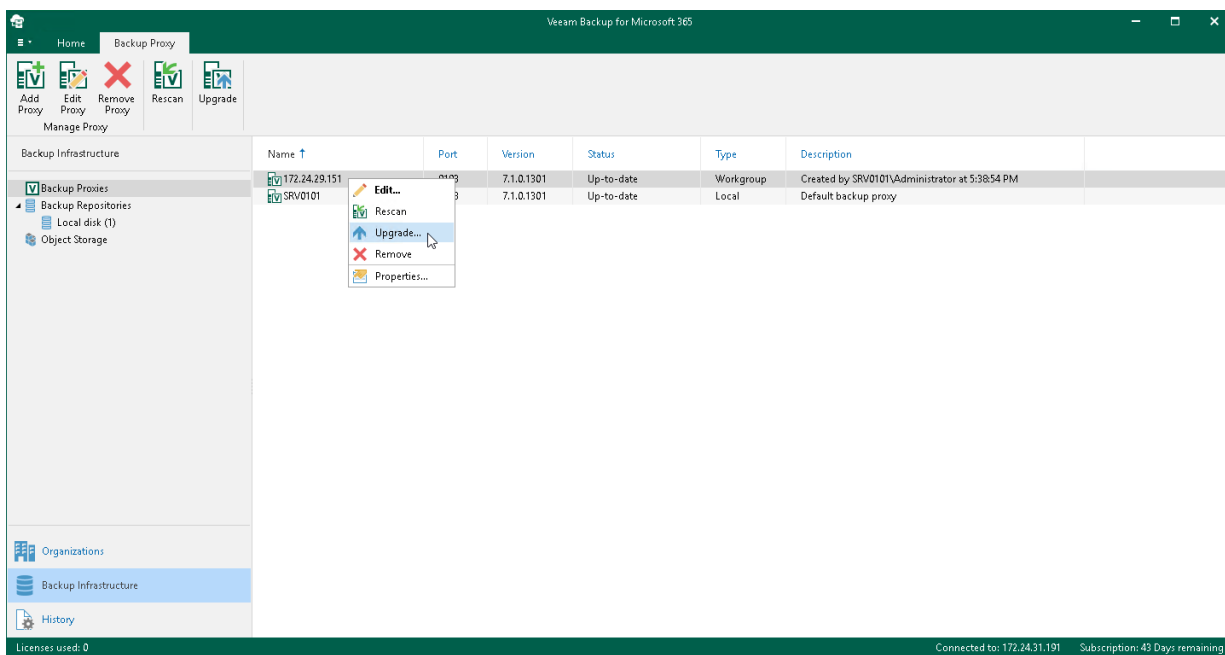
1. [Launch the Proxy Upgrade wizard.](#)
2. [Select a backup proxy server to upgrade.](#)
3. [Specify credentials.](#)

Step 1. Launch Proxy Upgrade Wizard

To launch the **Proxy Upgrade** wizard, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Backup Proxies** node.
3. In the preview pane, do one of the following:
 - Select a backup proxy server and click **Upgrade** on the ribbon.
 - Right-click a backup proxy server and select **Upgrade**.

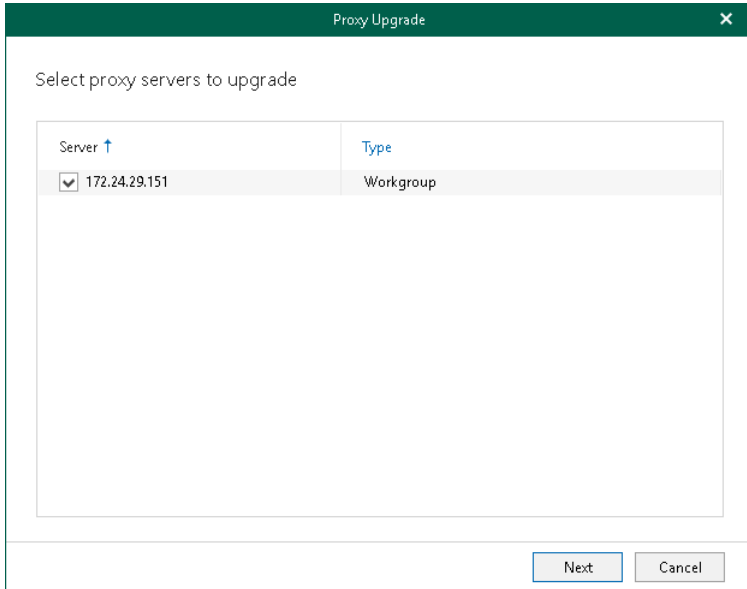
If you want to upgrade all backup proxy servers at the same time, right-click the **Backup Proxies** node and click **Upgrade**.



Step 2. Select Backup Proxy Server to Upgrade

At this step of the wizard, select a backup proxy server to upgrade. You can select multiple proxies at the same time.

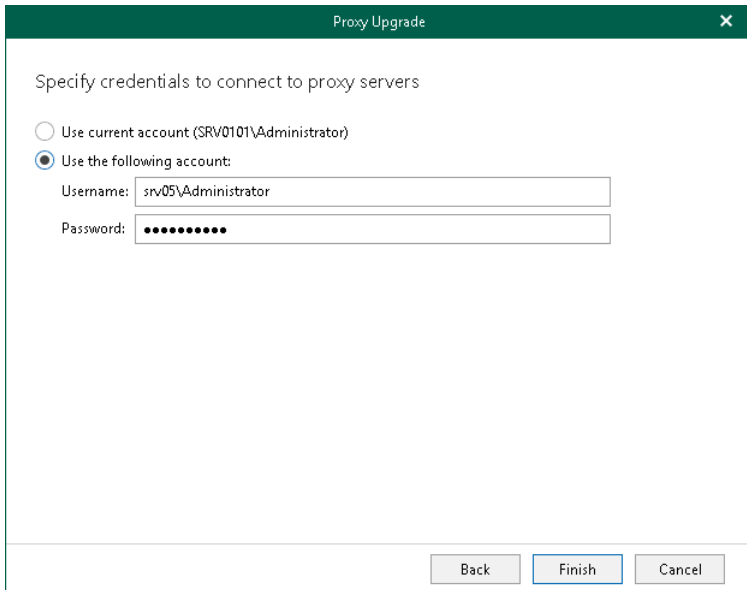
The local backup proxy server (that is, the default backup proxy server) will be upgraded automatically.



Step 3. Specify Credentials

At this step of the wizard, enter user credentials to connect to the backup proxy server.

The account must be a member of the local *Administrators* group.



The screenshot shows a dialog box titled "Proxy Upgrade" with a close button (X) in the top right corner. The main text reads "Specify credentials to connect to proxy servers". There are two radio button options: "Use current account (SRV0101\Administrator)" which is unselected, and "Use the following account:" which is selected. Below the selected option, there are two text input fields: "Username:" containing "srv05\Administrator" and "Password:" containing a series of dots. At the bottom of the dialog, there are three buttons: "Back", "Finish", and "Cancel".

Removing Backup Proxy Servers

You can remove a backup proxy server from the Veeam Backup for Microsoft 365 backup infrastructure if you no longer need it.

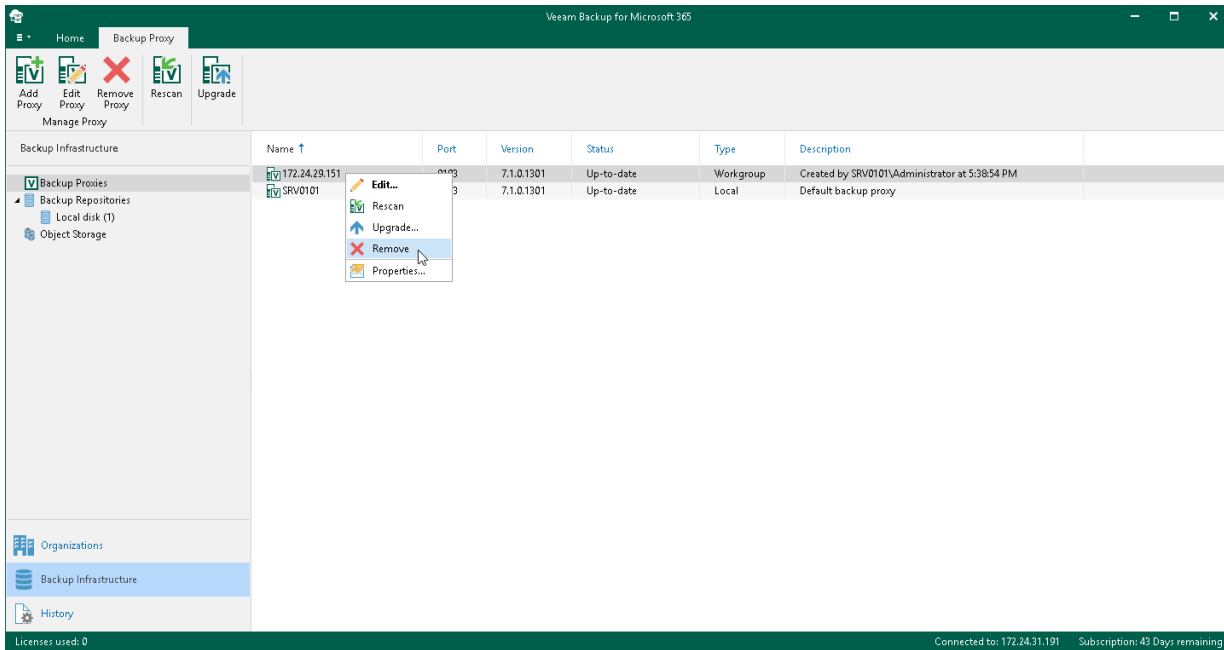
Consider the following:

- A default backup proxy server cannot be removed.
- The *Veeam Backup Proxy for Microsoft 365 Service* will be uninstalled from the target server.
- Backup data and log files will be preserved.

To remove a backup proxy server from the backup infrastructure, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Backup Proxies** node.
3. In the preview pane, do one of the following:
 - Select a backup proxy server and click **Remove Proxy** on the ribbon.

- Right-click a backup proxy server and select **Remove**.



Modifying Backup Proxy Server Properties

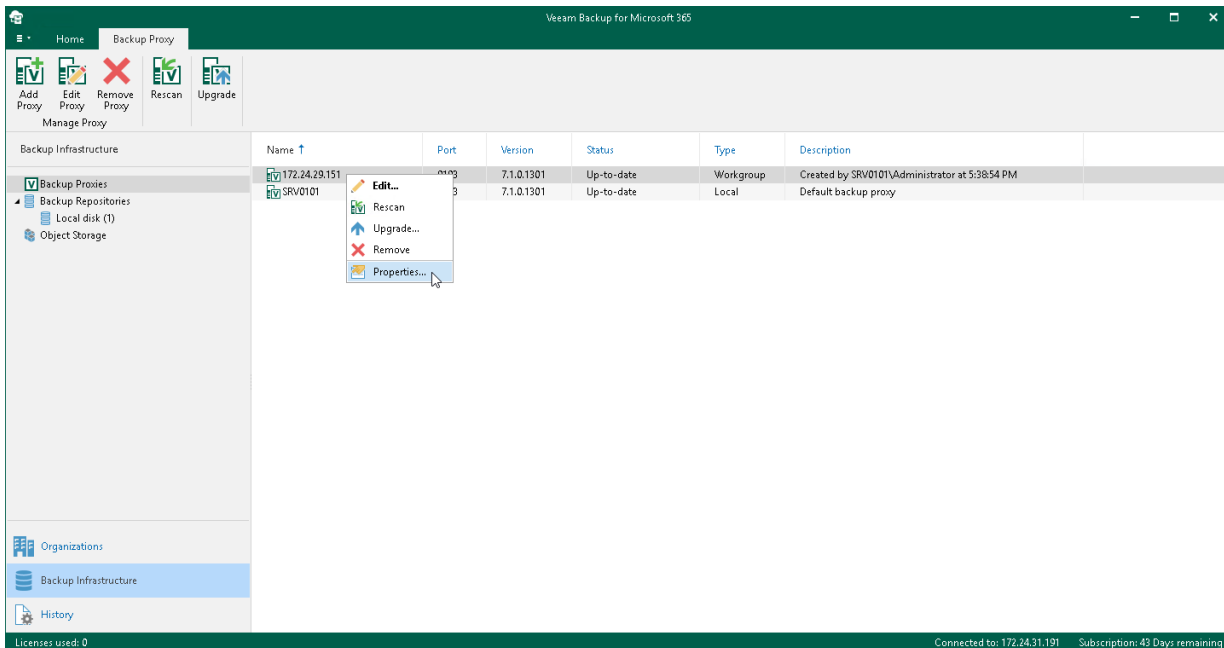
Veeam Backup for Microsoft 365 allows you to configure backup proxy server properties. In contrast with the editing of backup proxy server settings, modifying backup proxy server properties does not lead to adding backup proxy anew to the Veeam Backup for Microsoft 365 backup infrastructure. You just apply new values for the modified parameters.

To configure backup proxy server properties, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Backup Proxies** node.
3. In the preview pane, right-click a backup proxy server, select **Properties** and proceed to:
 - [Configuring Threads and Network Bandwidth](#)
 - [Configuring Internet Proxy Server for Backup Proxies](#)

NOTE

The **Properties** option is unavailable if a backup proxy server needs to be upgraded. For more information about upgrading backup proxy servers, see [Upgrading Backup Proxy Servers](#).



Configuring Threads and Network Bandwidth

Veeam Backup for Microsoft 365 allows you to configure threads and limit download speed.

To specify the number of threads and limit download speed, do the following:

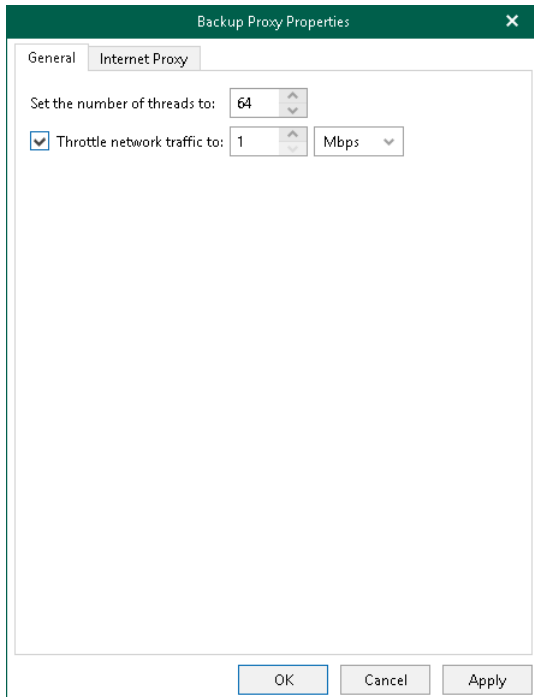
1. On the **General** tab, do the following:
 - In the **Set the number of threads to** field, specify the allowed number of threads.

A thread defines the total number of proxy server threads that are responsible for handling data transfer to/from backup repositories. By default, 64 threads are used. Depending on your environment configuration and capacities (low CPU or RAM deficiency), running too many threads may significantly reduce the efficiency due to possible throttling errors or connection failures. As every production environment operates under different equipment capacity, Veeam Backup for Microsoft 365 allows you to explicitly define the number of threads that your infrastructure is potentially able to handle without losing performance.

- Select the **Throttle network traffic to** check box and specify the average download speed.

For example, if you have set this value to 10 Mbps and have downloaded 100 Mb in 8 seconds, Veeam Backup for Microsoft 365 will stop retrieving new data for approximately 2 minutes after which download will be resumed automatically. The exact time for which Veeam Backup for Microsoft 365 stops getting data is calculated by predefined algorithms and depends upon the value that you specify as traffic throttling, the amount of downloaded data and the amount of time it took to get this data.

2. Click **OK**.



Configuring Internet Proxy Server for Backup Proxies

Veeam Backup for Microsoft 365 allows you to assign an internet proxy server to backup proxy that does not have direct access to the internet.

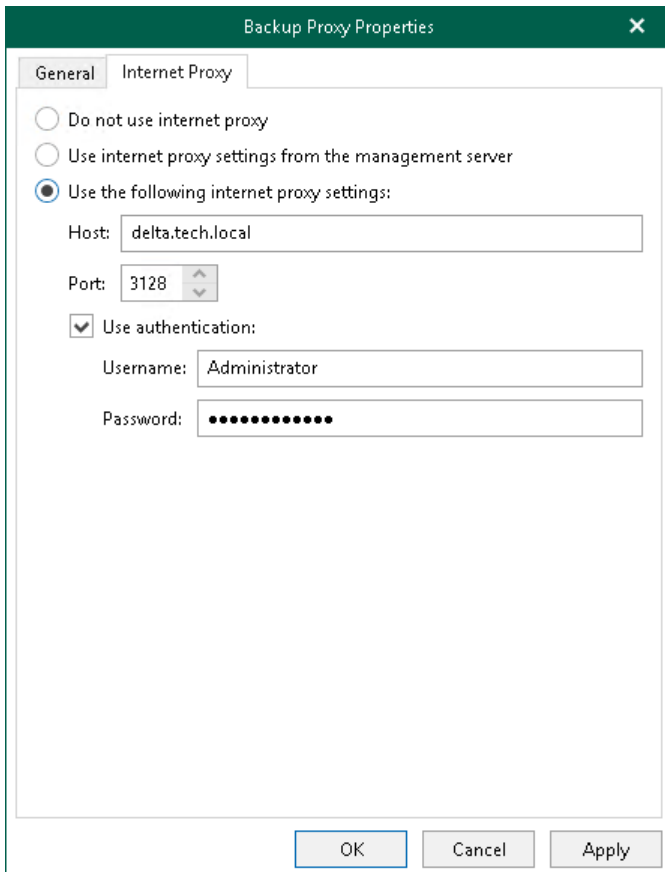
To configure an internet proxy server for a backup proxy server, do the following:

1. On the **Internet Proxy** tab, select one of the following options:
 - **Do not use internet proxy.** Select this option if your backup proxy server has direct access to the internet and you do not want to use any other internet proxy servers.
 - **Use internet proxy settings from the management server.** Select this option to use an internet proxy that is configured for your management server.
For more information, see [Global Internet Proxy Server Settings](#).
 - **Use the following internet proxy settings.** Select this option to configure a dedicated internet proxy server and provide the following:
 - In the **Host** field, enter a DNS name or IP address of a server that has access to the internet and which you want to use as an internet proxy.
 - In the **Port** field, specify a port number which you use to connect to the specified server.
 - Select the **Use authentication** check box to authenticate yourself on a server and provide authentication credentials.

2. Click **OK**.

NOTE

The local backup proxy server (that is, the default backup proxy server) always uses an internet proxy that is configured for your management server. For more information, see [Global Internet Proxy Server Settings](#).



The screenshot shows the 'Backup Proxy Properties' dialog box with the 'Internet Proxy' tab selected. The dialog has two tabs: 'General' and 'Internet Proxy'. Under the 'Internet Proxy' tab, there are three radio button options: 'Do not use internet proxy', 'Use internet proxy settings from the management server', and 'Use the following internet proxy settings:'. The third option is selected. Below this, there are fields for 'Host' (delta.tech.local), 'Port' (3128), and a checked checkbox for 'Use authentication:'. The 'Username' field contains 'Administrator' and the 'Password' field is masked with dots. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

Backup Proxy Properties

General Internet Proxy

Do not use internet proxy

Use internet proxy settings from the management server

Use the following internet proxy settings:

Host: delta.tech.local

Port: 3128

Use authentication:

Username: Administrator

Password: ●●●●●●●●

OK Cancel Apply

Backup Repositories

Veeam Backup for Microsoft 365 uses backup repositories as storage systems for [backups](#) and [backup copies](#) created for Microsoft 365 and on-premises Microsoft organizations. You can add to Veeam Backup for Microsoft 365 storage systems of the following types:

- [JET-based backup repository](#)
- [Backup repository extended with object storage](#)

The following table lists supported backup repositories depending on their type and purpose of usage.

	JET-based backup repository	Backup repository extended with object storage		
		Azure Blob Storage	Amazon S3 object storage	S3 Compatible object storage
Data backup	✓	✓	✓	✓
Backup copy		✓	✓	✓

For more information about backup repository structure, see [Backup Repository Structure](#).

For more information about Azure Blob Storage and Amazon S3 object storage supported by Veeam Backup for Microsoft 365, see [Supported Azure Storage Account Types](#) and [Supported Amazon S3 Storage Classes](#).

JET-Based Backup Repositories

Veeam Backup for Microsoft 365 uses JET-based backup repositories only to store backups created by backup jobs. To save data in storage systems of this type, Veeam Backup for Microsoft 365 uses Extensible Storage Engine (ESE) databases, also known as JET Blue.

You can add the following JET-based backup repositories to the Veeam Backup for Microsoft 365 backup infrastructure:

- A local directory on a backup proxy server.
A default backup repository is the `C:\VeeamRepository` directory on a computer with Veeam Backup for Microsoft 365.
- Direct Attached Storage (DAS) connected to the backup proxy server.
- Storage Area Network (SAN).
A backup proxy server must be connected to the SAN fabric using hardware, virtual HBA or software iSCSI initiator.
- Network Attached Storage (SMB shares version 3.0 or later).
Experimental support.

NOTE

Consider the following:

- Veeam Backup for Microsoft 365 does not support encryption at-rest for JET-based backup repositories.
- You can store your backups on volumes encrypted using the BitLocker technology if it applies to your system. After encryption, the I/O rate of the volume may change.

Extended Backup Repositories

You can extend a local JET-based backup repository with object storage. For more information on how to extend a backup repository with object storage, see [Specify Object Storage](#).

The following table lists supported object storage that you can use to extend a local JET-based backup repository for data backup and backup copy.

	Data backup	Backup copy
Azure Blob Storage Hot access tier	✓	✓
Azure Blob Storage Cool access tier	✓	✓
Azure Blob Storage Archive access tier		✓
Amazon S3 Standard storage class	✓	✓
Amazon S3 Standard-Infrequent Access storage class	✓	✓
Amazon S3 Glacier Instant Retrieval storage class		✓
Amazon S3 Glacier Flexible Retrieval storage class		✓
Amazon S3 Glacier Deep Archive storage class		✓
S3 Compatible object storage (if applicable)	✓	✓

For more information about object storage, see [Object Storage](#).

If you extended a local JET-based backup repository with object storage, you can do the following:

- Back up your data directly to the supported cloud or on-premises storage system. This is not applicable to backup repositories extended with Azure Blob Storage Archive access tier and all Amazon S3 Glacier storage classes.

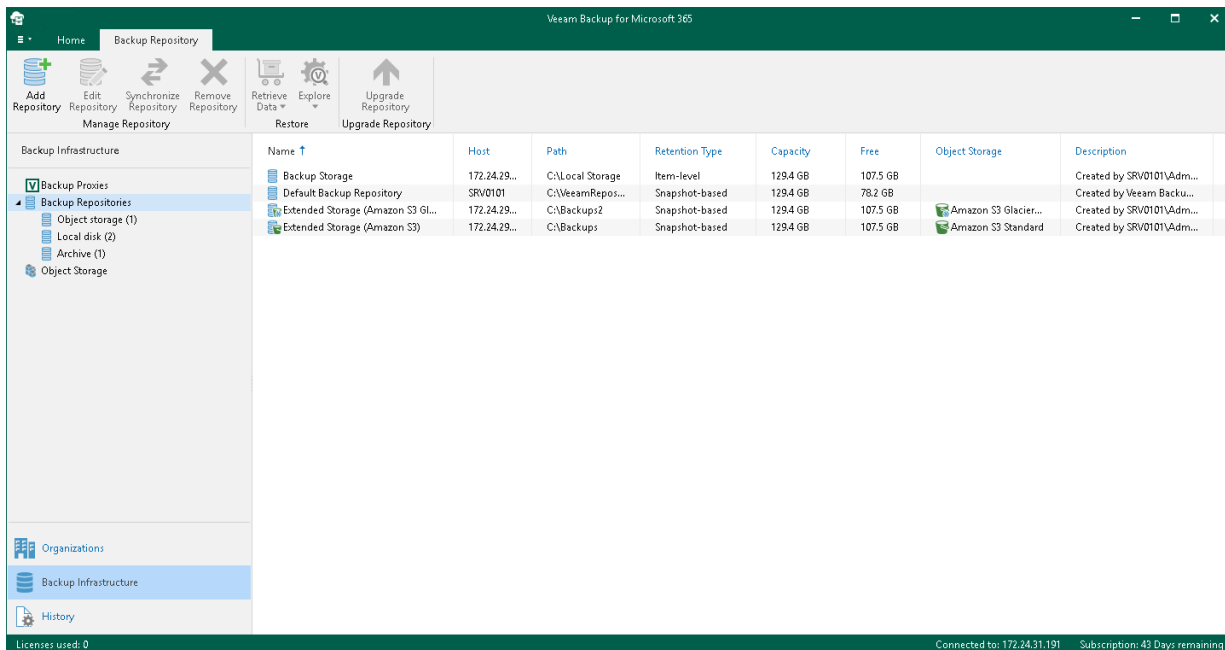
- Transfer your backed-up data as backup copies to such repositories. Keep in mind that if you extend a backup repository with Azure Blob Storage Archive access tier or any of Amazon S3 Glacier storage classes, you can use this backup repository only to store backup copies and select it as a target for backup copy jobs.

What Is Under Backup Repositories Node

In the **Backup Infrastructure** view, the **Backup Repositories** node includes the following nodes for different backup repositories added to Veeam Backup for Microsoft 365:

- **Object storage.** Contains backup repositories extended with S3 Compatible object storage, Azure Blob Storage Hot/Cool access tiers, Amazon S3 Standard and Amazon S3 Standard-Infrequent Access storage classes. Veeam Backup for Microsoft 365 uses such repositories to store both backups and backup copies.
- **Local disk.** Contains *Default Backup Repository* and other JET-based backup repositories. Veeam Backup for Microsoft 365 uses such repositories only to store backups.
- **Archive.** Contains backup repositories extended with Azure Blob Storage Archive access tier and all Amazon S3 Glacier storage classes. Veeam Backup for Microsoft 365 uses such repositories only to store backup copies.

Keep in mind that the **Archive** and **Object storage** nodes are displayed only if you have added a backup repository extended with a particular object storage.



Backup Repository Structure

In a backup repository, all backed-up items are stored in a way that each item belongs to a separate folder named after the year when the item has been modified.

Each folder contains `repository.adb` – a backup file with the Microsoft 365 organization data – along with a number of auxiliary files required to retain information about restore points and repository configuration settings. To determine the period during which backup data must be stored in a backup repository, Veeam Backup for Microsoft 365 applies retention policy settings specified while adding the repository.

NOTE

Consider the following:

- If a backup repository is **extended with object storage**, only **cache** will be saved to such an extended backup repository.
- For each backup repository, Veeam Backup for Microsoft 365 saves information about restore points to the `Repository.sqlite` database file. Veeam Backup for Microsoft 365 collects this information for all backups and backup copies that are stored in this backup repository.

The following example represents a Microsoft organization with a mailbox that contains 3 email items; each item has been modified on a different date (10:00 AM on 9/1/2016, 10:20 AM on 11/11/2017 and 3:20 PM on 12/21/2018). To protect these items, you configure a backup job that stores backed-up files in a specific backup repository. When running backup job sessions, Veeam Backup for Microsoft 365 adds items to the backup repository in the following way:

- During the initial backup job session, Veeam Backup for Microsoft 365 collects all data from the Microsoft organization and saves the data to folders in the backup repository.

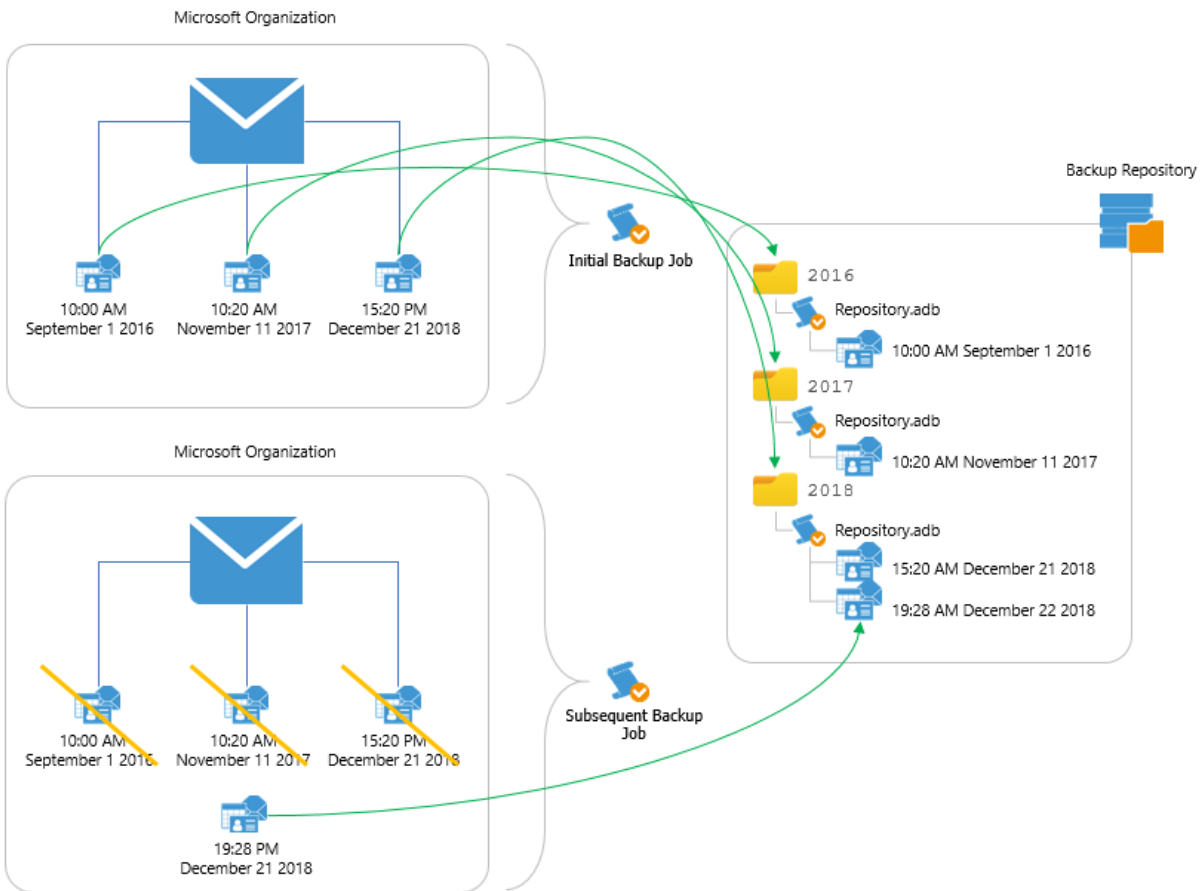
As each email item has been modified on a different date, Veeam Backup for Microsoft 365 creates 3 different folders in the backup repository: 2016, 2017 and 2018. Each folder contains its own backup file `repository.adb`.

- During subsequent backup job sessions, Veeam Backup for Microsoft 365 backs up only those email items that were changed since the last backup job session.

This means that if the organization receives a new email item at 7:28 PM on 12/21/2018, and no other items change since the initial backup job session, Veeam Backup for Microsoft 365 will back up only the new item – and save the data to the `repository.adb` file in the 2018 repository folder.

NOTE

Although the example describes only Microsoft Exchange items, the same approach applies to Microsoft SharePoint items, Microsoft OneDrive for Business items and Microsoft Teams items.



Retention Policy

A retention policy defines how long and under which retention type your backup data should be stored in a backup repository.

Veeam Backup for Microsoft 365 provides the following types of retention:

- [Snapshot-Based Retention](#)

Select this type if you want to keep an item state until the restore point of an item state is within the retention coverage.

- [Item-Level Retention](#)

Select this type if you want to keep an item until its creation time or last modification time is within the retention coverage.

Snapshot-Based Retention

In Microsoft 365, any modification of an item in the production environment leads to the creation of a new item version. A modification means that the user has changed any attribute of an item in the production environment. For example, a new category has been assigned to an email in the mailbox or a document has been renamed in a SharePoint site.

In Veeam Backup for Microsoft 365, each item in a backup repository has its own *item state*. The item state comprises a cumulative set of item versions created for an item in Microsoft 365. The item state belongs to a specific restore point.

During the initial backup of an item, Veeam Backup for Microsoft 365 creates its initial item state in the first restore point. This item state contains all versions of this item that exist in Microsoft 365 at the moment. After a user has modified the item again, Microsoft 365 creates its new version. During the subsequent incremental backup, Veeam Backup for Microsoft 365 creates a new restore point with a new item state. This new item state cumulatively includes all versions of an item created by Microsoft 365.

When a retention policy is applied to a backup repository with the snapshot-based retention type, Veeam Backup for Microsoft 365 removes the item states. Data removal from a backup repository occurs every time the restore point goes beyond the retention coverage. The items that were never changed stay in a backup repository with the snapshot-based retention type until their restore point is within the retention coverage.

The following example represents two backup files consisting of three items each, where each item has its own backup date. Consider the *Item 1* of the *Backup 1* storage to be an email message, the attributes of which have been modified three times in the production environment; each modification was made on different days (Monday, Tuesday, and Wednesday) and each modification was successfully backed up.

There are the following states of the *Item 1* in the backup repository:

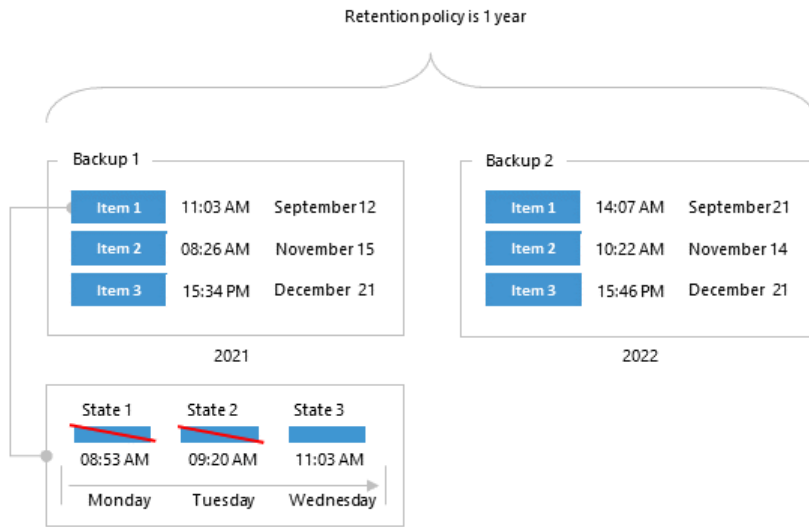
- *State 1* includes the initial version of the *Item 1* and the modification made on Monday.
- *State 2* includes the initial version of the *Item 1* and modifications made on Monday and Tuesday.
- *State 3* includes the initial version of the *Item 1* and modifications made on Monday, Tuesday and Wednesday.

If the retention policy is 1 year and will be applied at 10:00 AM on September 12, 2022, then all states of the *Item 1* that exceed the specified retention threshold will be removed from the backup repository. These item states are the *State 1* and *State 2*.

The *State 3* is the latest and if no more states will be created for the *Item 1*, it will be kept in the *Backup 1* storage along with the initial states of *Item 2* and *Item 3*.

NOTE

Backup jobs process all available items regardless of their creation time or last modification time.



Item-Level Retention

Data removal from backup repositories with the item-level retention type occurs every time the creation time or last modification time of an item in a backup file goes beyond the retention coverage.

The following example represents three backup files; each file contains Microsoft 365 items per year where each item has its own last modification time.

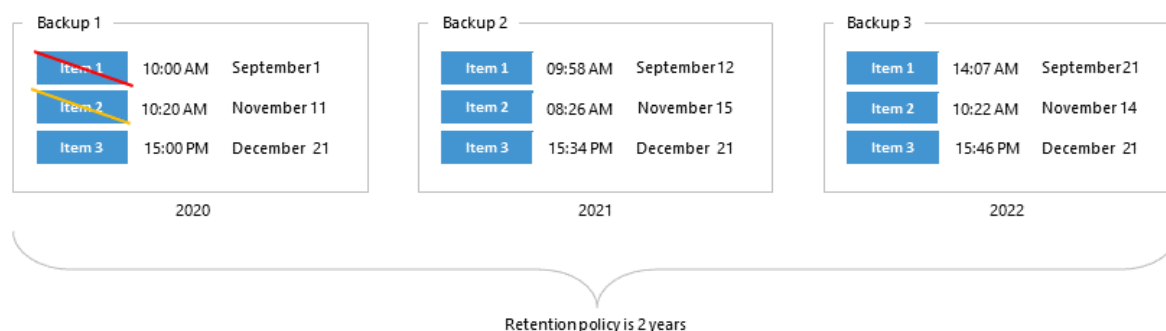
For example, your retention policy is said to be applied at 10:20 AM on September 1, 2022. In such a scenario, Veeam Backup for Microsoft 365 will remove the *Item 1* from the *Backup 1* repository because the *Item 1* exceeds the retention period (2 years in our example) by 20 minutes.

The next item to be removed is the *Item 2* because its last modifications were made at 10:20 AM on November 11, 2020. When a retention policy is being applied, for example, at 10:30 AM on November 11, 2022, Veeam Backup for Microsoft 365 removes the *Item 2* because its age equals 2 years and 10 minutes which exceeds the specified threshold.

The same is repeated until no items left in a repository. After that, Veeam Backup for Microsoft 365 completely removes such a repository from the hard drive.

NOTE

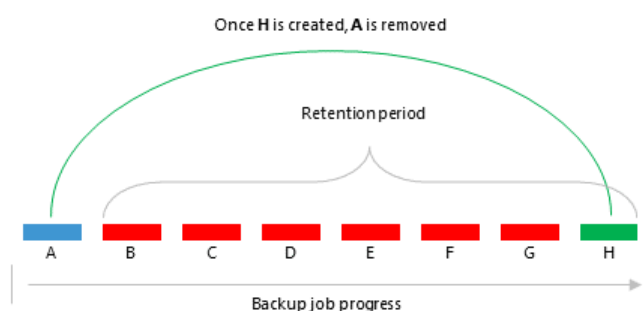
Backup jobs do not process items the last modification time of which exceeds the specified retention period.



Removing Items After Unsuccessful Backup Attempts

If during the subsequent backup job sessions Veeam Backup for Microsoft 365 fails to back up organization mailboxes, Microsoft SharePoint items, Microsoft OneDrive for Business items, or Microsoft Teams items, the product preserves the latest backup state of such items until the next successful backup is created.

The following example represents a backup of the mailbox *A* which is followed by 6 consecutive unsuccessful attempts (*B* through *G*) of backing up that same mailbox during the subsequent backup job sessions. The mailbox *A* will not be removed until this mailbox is successfully backed up during the attempt *H*.

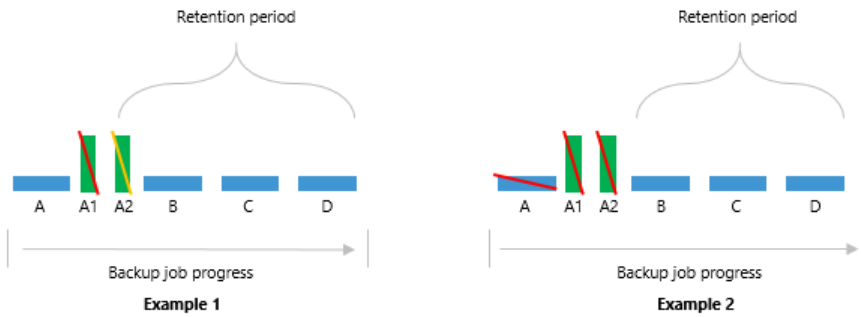


Removing Restore Points

The restore points of items are removed as soon as they are out of the retention coverage. Once the latest available restore point is removed, the parent item of such a restore point will be removed as well.

The following example represents four items (*A* through *D*) and two restore points (*A1* and *A2*) both of which belong to the item *A*. The *A1* restore point has already been removed since it was out of the retention coverage, whereas the *A2* restore point will only be removed after it goes out of the retention coverage (*Example 1*).

Once the latest restore point is out of the retention coverage and, therefore, can safely be removed, the item *A* – the parent item of the latest restore point *A2* – will be removed as well (*Example 2*).

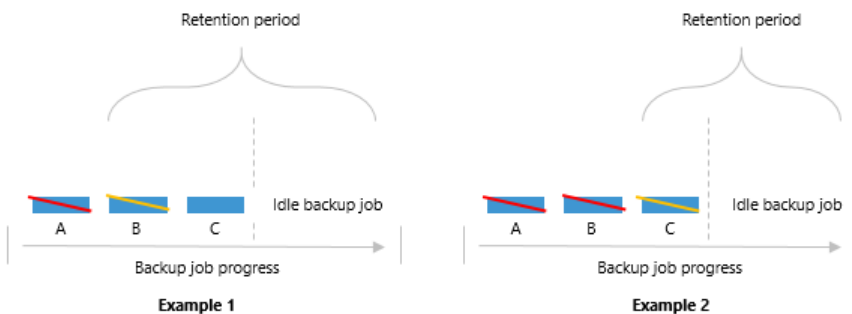


Backup Job Idleness

If a backup job has created a successful backup and then went idle for an indefinite period of time (for example, it become disabled), then all the data created by such a job will be removed once it is out of the retention coverage.

The following example represents the mailbox *A* that has been removed because it was already out of the retention coverage (*Example 1*). The next mailbox that will be removed is the mailbox *B*, the removal of which will happen once it goes beyond the retention coverage (*Example 2*).

The same is applicable to Microsoft SharePoint, Microsoft OneDrive for Business and Microsoft Teams.



Direct Attached Storage (DAS)

In Veeam Backup for Microsoft 365, you can use the following Microsoft Windows and Linux-based storage types as backup repositories:

- A Windows-based server with local or directly attached storage.
Such storage can be a local disk, directly attached disk-based storage (such as a USB hard drive), or iSCSI/FC SAN LUN in case the server is connected into the SAN fabric.
- Linux-based storage connected to the Veeam Backup for Microsoft 365 server.
Such storage can be a local disk, directly attached disk-based storage (such as a USB hard drive), NFS share, or iSCSI/FC SAN LUN in case the server is connected into the SAN fabric. The storage must then be provisioned to the Windows-based host as a volume in the guest OS.

Network Attached Storage (SMB Shares)

Veeam Backup for Microsoft 365 allows you to use network attached storage (NAS) as backup repositories. Such NAS can be a shared folder on your computer, or any other physical device that can be accessed using the *Server Message Block* (SMB) protocol.

Consider the following:

- Network share browsing is not supported; make sure to prove the path to the shared folder manually.
- A shared folder must be on a computer or device located within the same or a trusted domain.
- To use SMB 3.0 or later, make sure you are using Microsoft Windows 8 or later or Microsoft Windows Server 2012 or later. Keep in mind that Network Attached Storage repository is on experimental support.
- SMB shares version 3.0 are only supported when they are within the Microsoft Exchange Storage definition. For more information, see [this Microsoft article](#).

To access and use a shared folder, do the following:

- Configure NTFS permissions.
- Configure share permissions.

For more information, see [this Veeam article](#).

After you share a folder, you can access it using the SMB 3.0 protocol to read/write data to/from this folder.

To add a shared folder as a backup repository, in the [Specify Backup Proxy Server](#) step, in the **Path** field, specify the path to the shared folder using the following syntax: `\\<FQDN_name>` or `<ip_address>\<shared_folder_name>`.

The screenshot shows a dialog box titled "New Backup Repository". The main instruction is "Specify location for backup repository". It features three input fields: "Backup proxy:" with a dropdown menu set to "SERV001 (Default backup proxy)"; "Path:" with a text box containing "\\serv001\share" and a "Browse..." button; and a status bar indicating "98.4 GB free of 119.7 GB". At the bottom, there are "Back", "Next", and "Cancel" buttons.

Adding Backup Repositories

To add a new backup repository, do the following:

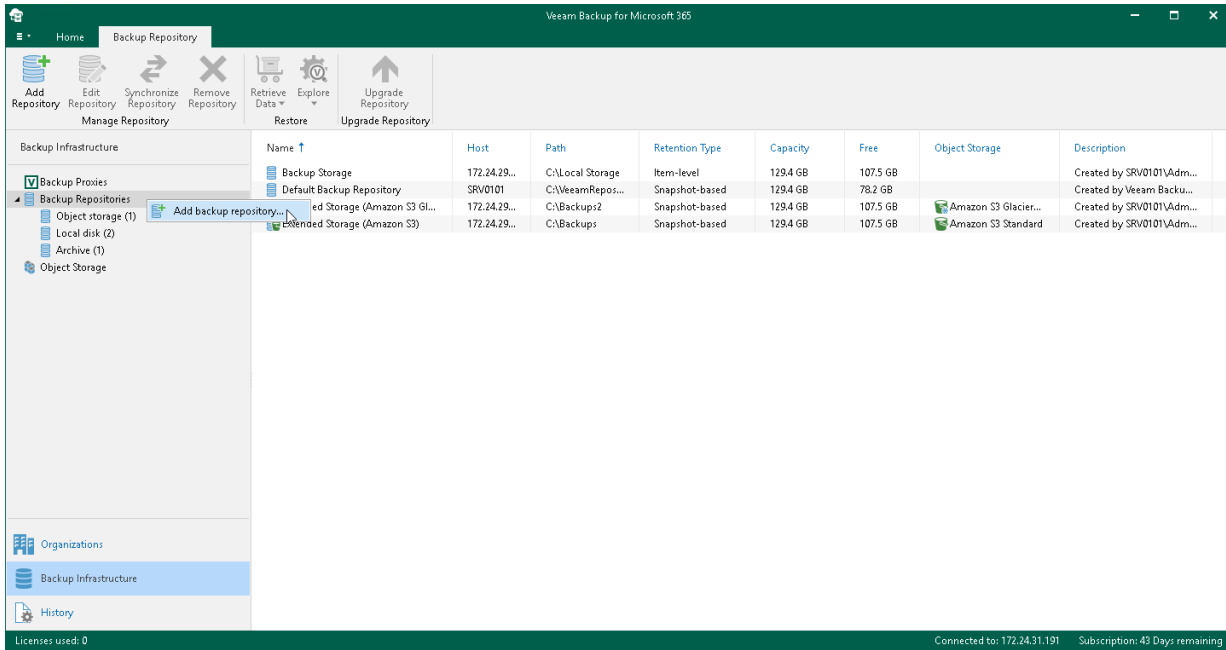
1. [Launch the New Backup Repository wizard](#).
2. [Specify a backup repository name](#).

3. [Select target location for backups.](#)
4. [Specify a backup proxy server.](#)
5. [Specify object storage.](#)
6. [Specify retention policy settings.](#)

Step 1. Launch New Backup Repository Wizard

To launch the **New Backup Repository** wizard, do the following:

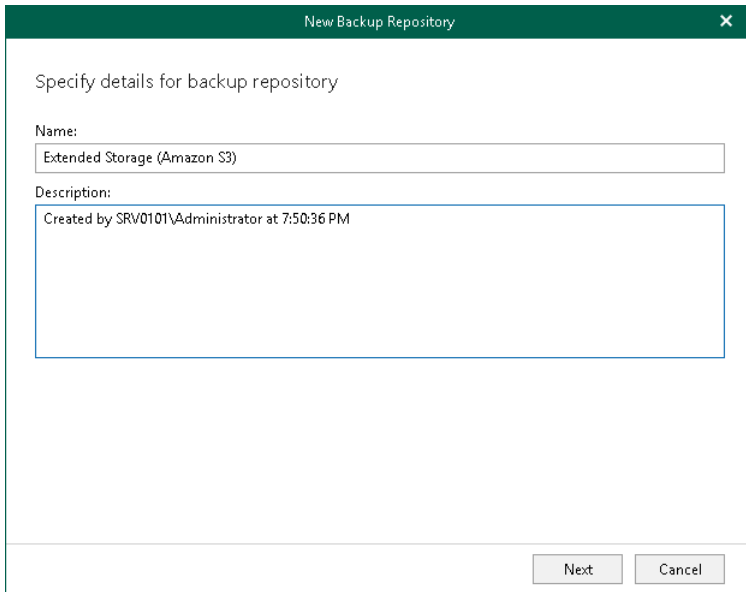
1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Backup Repositories** node.
3. Do one of the following:
 - On the **Backup Repository** tab, click **Add Repository** on the ribbon.
 - Right-click the **Backup Repositories** node and select **Add backup repository**.



Step 2. Specify Backup Repository Name

At this step of the wizard, enter a name for the backup repository and provide optional description:

1. In the **Name** field, enter a name for the backup repository.
2. In the **Description** field, enter optional description.



New Backup Repository

Specify details for backup repository

Name:
Extended Storage (Amazon S3)

Description:
Created by SRV0101\Administrator at 7:50:36 PM

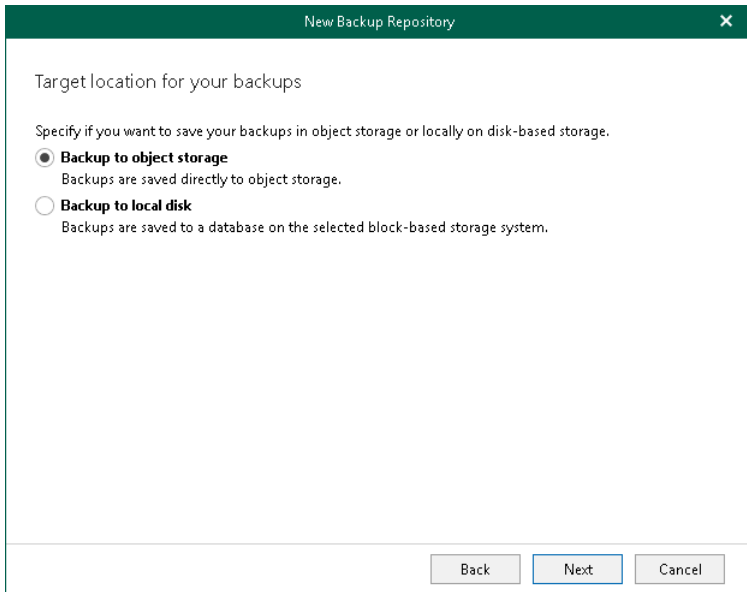
Next Cancel

Step 3. Select Target Location for Backups

At this step of the wizard, select whether you want to back up your data directly to the supported cloud or on-premises storage system or save your backups locally in a JET-based storage system.

Select one of the following options:

- **Backup to object storage.** Select this option if you want to extend your backup repository with object storage and back up data directly to the supported cloud or on-premises storage system.
- **Backup to local disk.** Select this option if you want to store backups locally in the repository database.



Step 4. Specify Backup Proxy Server

At this step of the wizard, select a backup proxy server and specify a directory where you want to store backups.

NOTE

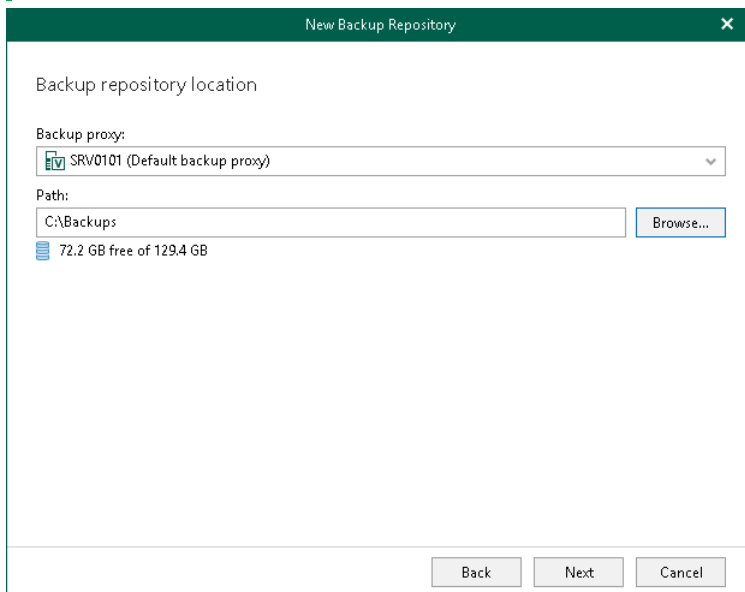
Directory where you want to store backups must not be the Veeam Backup for Microsoft 365 installation folder.

To specify a backup proxy server and directory for storing backups, do the following:

1. From the **Backup proxy** drop-down list, select a backup proxy server. For more information, see [Backup Proxy Servers](#).
2. Do one of the following:
 - If you have selected the **Backup to local disk** option at the [previous](#) step, in the **Path** field, specify a directory to store your backups. Click **Browse** to select a directory.

NOTE

To use a shared folder, provide the path manually. For more information about shared folders, see [Network Attached Storage \(SMB Shares\)](#).



The screenshot shows a dialog box titled "New Backup Repository". It has a dark green header bar with a close button (X). The main content area is white and contains the following elements:

- Backup repository location**: A section header.
- Backup proxy:**: A dropdown menu with "SRV0101 (Default backup proxy)" selected.
- Path:**: A text input field containing "C:\Backups" and a "Browse..." button to its right.
- Below the path field, there is a storage icon and the text "72.2 GB free of 129.4 GB".
- At the bottom of the dialog, there are three buttons: "Back", "Next", and "Cancel".

- If you have selected the **Backup to object storage** option at the [previous](#) step, in the **Local cache path** field, specify a directory to keep **cache** that contains backup metadata. The actual data will be compressed and backed up directly to object storage that you specify at the [next step](#).

When specifying a directory that already contains cache, at the next step, make sure to select the same exact object storage for which this cache was created.

New Backup Repository

Backup proxy and cache location

Backup proxy:
172.24.29.151 (Created by SRV0101\Administrator at 5:38:54 PM)

Local cache path:
C:\Backups

107.6 GB free of 129.4 GB

3. Click **Get free space** if you want to know the available space on the selected backup proxy server.

Step 5. Specify Object Storage

This step is only available if you have selected the **Backup to object storage** option at the [Select Target Location for Backups](#) step of the wizard.

At this step of the wizard, you can extend a backup repository with object storage to back up data directly to the cloud or on-premises storage system. For more information about object storage, see [Object Storage](#).

Consider the following:

- You cannot extend a backup repository with object storage that is already an extension to another backup repository.
- Extending an existing backup repository is not possible.
- If object storage that you select contains offloaded backup data, you will be offered to synchronize required metadata (cache) of such offloaded backups with the backup repository that is being added.
If you skip synchronization, the backup repository will be added with the *Out of Sync* state. To use such a repository, make sure to synchronize it manually. For more information, see [Synchronizing Repositories](#).
- If object storage that you select contains encrypted data, make sure to provide the same exact password with which this data was encrypted. Otherwise, the addition of object storage will not be possible.
- Removing object storage from the backup repository configuration is not possible after the backup repository was extended with object storage.

To extend a backup repository with object storage, do the following:

1. From the drop-down list, select object storage to which you want to offload your data.

Make sure that object storage has been added to your environment in advance. Otherwise, click **Add** and follow the steps of the wizard. For more information on how to add object storage, see [Adding Object Storage](#).

3. Select the **Encrypt data uploaded to object storage** check box to encrypt the offloaded data.
4. From the **Password** drop-down list, select an encryption password.

If you already have a password record that was configured beforehand, select such a record from the drop-down list. Otherwise, click **Add** and add an encryption password. For more information, see [Managing Encryption Passwords](#). You can also click **Manage passwords** to [manage existing password records](#).

A password can be changed at any time. A password change does not impose any restrictions on accessing existing backup data in object storage.

IMPORTANT

Make sure to remember your password because, if lost, it cannot be restored.

New Backup Repository

Object storage backup repository

Specify object storage to store your backups to:

Amazon S3 Standard Add...

Encrypt data uploaded to object storage:

Password:

Created by SRV0101/Administrator at 8:09 PM. (last edited: less than a day ago) Add...

[Manage passwords](#)

Back Next Cancel

Step 6. Specify Retention Policy Settings

At this step of the wizard, specify [retention policy](#) settings.

To specify retention settings, do the following:

1. From the **Retention policy** drop-down list, choose how long your data should be stored in the backup repository.

NOTE

If you have extended your backup repository with object storage for which immutability was enabled, you cannot configure Veeam Backup for Microsoft 365 to store data in the backup repository forever. The *Keep forever* option becomes unavailable. Keep in mind that once configured, this setting cannot be changed for such backup repositories.

2. Select a retention type:
 - **Snapshot-based retention.**
Select this type if you want to keep an item until the restore point of an item's version is within the retention coverage.
 - **Item-level retention.**
Select this type if you want to keep an item until its creation time or last modification time is within the retention coverage.
3. Click **Advanced** if you want to specify when to apply a retention policy. You can select the following options:
 - **Daily at**
Select this option if you want a retention policy to be applied on a daily basis and choose the time and day.
 - **Monthly at**
Select this option if you want a retention policy to be applied on a monthly basis and choose the time and day which can be the first, second, third, fourth or even the last one in the month.

Consider the following:

- The retention type of a backup repository cannot be changed once set.
- The retention type of a backup repository cannot be modified when [extending](#) a repository with object storage that contains offloaded backup data.

In such a scenario, the retention type will be inherited from that of object storage that you have selected at the [previous step](#) of the wizard.

- A retention policy configured in this step removes outdated restore points located in object storage.

The screenshot shows a dialog box titled "New Backup Repository" with a close button (X) in the top right corner. The main heading is "Specify retention policy settings". Below this, there is a "Retention policy:" label followed by a dropdown menu currently set to "3 years". There are two radio button options: "Snapshot-based retention" (which is selected) and "Item-level retention". Under "Snapshot-based retention", the text reads: "Each restore point represents the snapshot (actual state) of each mailbox, library or folder at the time of backup. Items will be deleted from backup once the last restore point they are contained within leaves the retention period. This is similar to how image-level backup works." Under "Item-level retention", the text reads: "Individual items will be deleted from backup once their creation or last modification date exceeds the data retention period. This is similar to how classic documents archive works, and is useful if you need to ensure that items are not stored in backup longer than required. Using this option increases egress charges when using object storage." Below the radio buttons, there is a text prompt: "Click Advanced to customize how often the retention policy should be applied" and an "Advanced" button. At the bottom of the dialog, there are three buttons: "Back", "Finish", and "Cancel".

Editing Backup Repository Settings

Veeam Backup for Microsoft 365 allows you to edit backup repository settings.

Consider the following:

- Editing the **Backup proxy** and **Path** values is not possible after the repository was created.
- Extending a backup repository with object storage is not possible after the backup repository was added to the Veeam Backup for Microsoft 365 backup infrastructure.

For more information on how to extend a backup repository with object storage, see [Specify Object Storage](#).

- Removing object storage from the backup repository configuration is not possible after the backup repository was extended with object storage.
- The retention type of a backup repository cannot be changed once set.
- The **Edit** command is unavailable if a backup repository is out of date.

For information on how to upgrade a backup repository, see [Upgrading Backup Repositories](#).

To edit backup repository settings, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select one of the following nodes:
 - **Backup Repositories**. Contains all backup repositories added to the Veeam Backup for Microsoft 365 backup infrastructure.
 - **Object storage**. Contains backup repositories extended with S3 Compatible object storage, Azure Blob Storage Hot/Cool access tiers, Amazon S3 Standard and Amazon S3 Standard-Infrequent Access storage classes.
 - **Local disk**. Contains *Default Backup Repository* and other JET-based backup repositories.

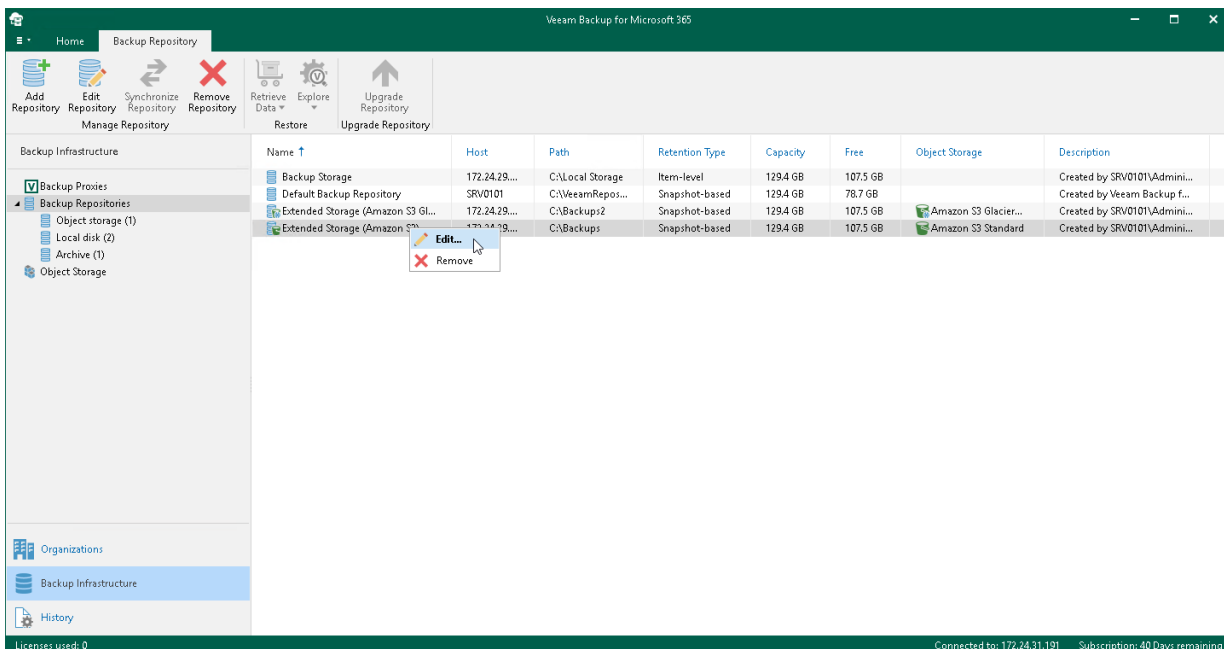
- **Archive.** Contains backup repositories extended with Azure Blob Storage Archive access tier and all Amazon S3 Glacier storage classes.
3. In the preview pane, do one of the following:
 - Select a backup repository and click **Edit Repository** on the ribbon.
 - Right-click a backup repository and select **Edit**.
 4. Modify the required settings.

You can change the following parameters:

- The backup repository name and description.
- The retention period.

NOTE

If you have extended your backup repository with object storage for which immutability was enabled, you cannot change the retention period.



Removing Backup Repositories

Veeam Backup for Microsoft 365 allows you to remove backup repositories from the backup infrastructure if you no longer need them.

Consider the following:

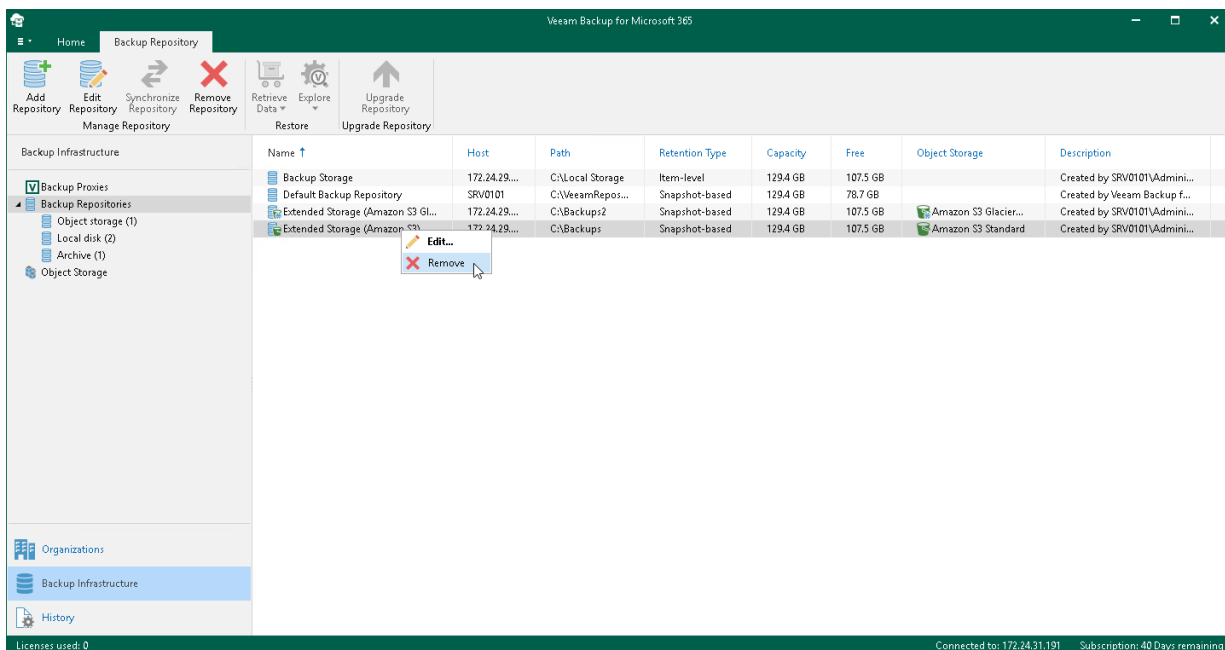
- When removing a backup repository, backup files that reside in such a repository will not be removed.
- The last remaining backup repository cannot be removed.
- When removing an extended backup repository that was synchronized, the backup data located in associated object storage becomes unavailable. For more information about repositories synchronization, see [Synchronizing Repositories](#).

- You cannot remove a backup repository that is in use by backup jobs.

To remove such a repository, remove (or re-map) all backup jobs that are mapped to this repository and then remove a repository. For more information on how to remove a backup job, see [Removing Backup Job](#).

To remove a backup repository, do the following:

- Open the **Backup Infrastructure** view.
- In the inventory pane, select one of the following nodes:
 - Backup Repositories.** Contains all backup repositories added to the Veeam Backup for Microsoft 365 backup infrastructure.
 - Object storage.** Contains backup repositories extended with S3 Compatible object storage, Azure Blob Storage Hot/Cool access tiers, Amazon S3 Standard and Amazon S3 Standard-Infrequent Access storage classes.
 - Local disk.** Contains *Default Backup Repository* and other JET-based backup repositories.
 - Archive.** Contains backup repositories extended with Azure Blob Storage Archive access tier and all Amazon S3 Glacier storage classes.
- In the preview pane, do one of the following:
 - Select a backup repository and click **Remove Repository** on the ribbon.
 - Right-click a backup repository and select **Remove**.



Upgrading Backup Repositories

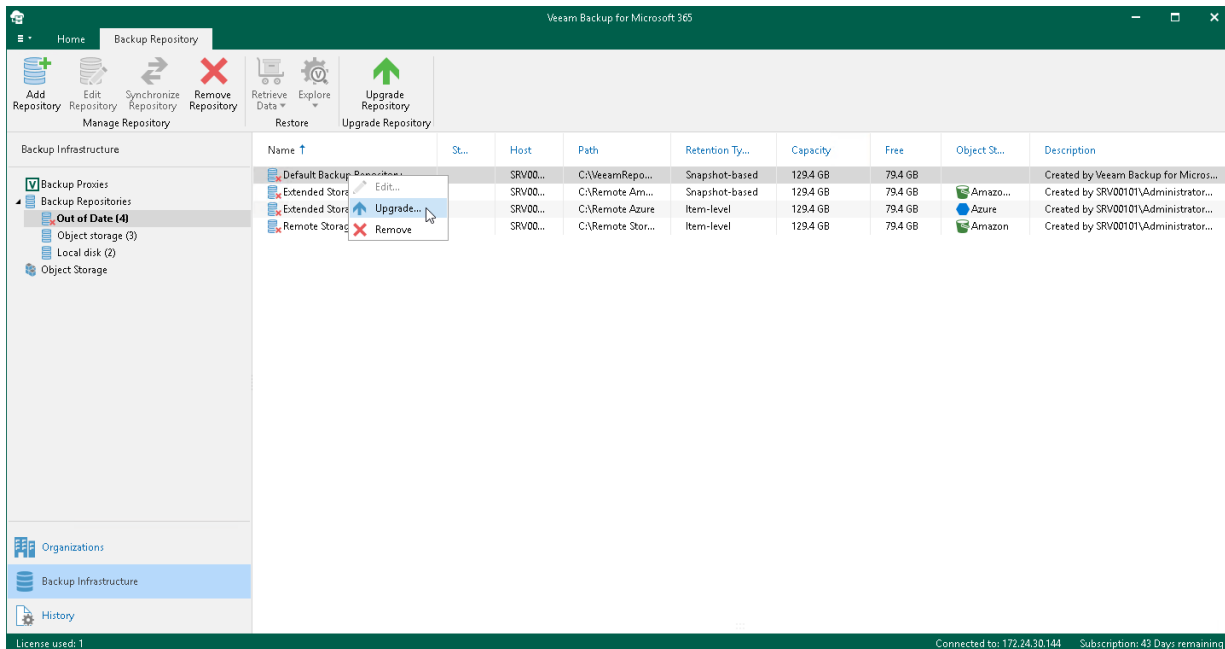
When you upgrade Veeam Backup for Microsoft 365 to a newer version, all backup repositories configured in your environment are marked as *Out of Date* and must be upgraded manually.

To upgrade backup repositories, do the following:

- Open the **Backup Infrastructure** view.

2. In the inventory pane, select the **Backup Repositories > Out of Date** node.
3. In the preview pane, do one of the following:
 - Select a backup repository and click **Upgrade Repository** on the ribbon.
 - Right-click a backup repository and select **Upgrade**.

If you want to stop upgrade, click **Stop Upgrade** on the ribbon.



Synchronizing Repositories

The **Synchronize Repository** option allows you to synchronize cache between object storage and extended backup repositories.

Such synchronization is required when an extended backup repository has the *Out of Sync* state. This state is assigned if you skip synchronization during [extension](#) of a backup repository with object storage.

Once cache is synchronized, you can do the following:

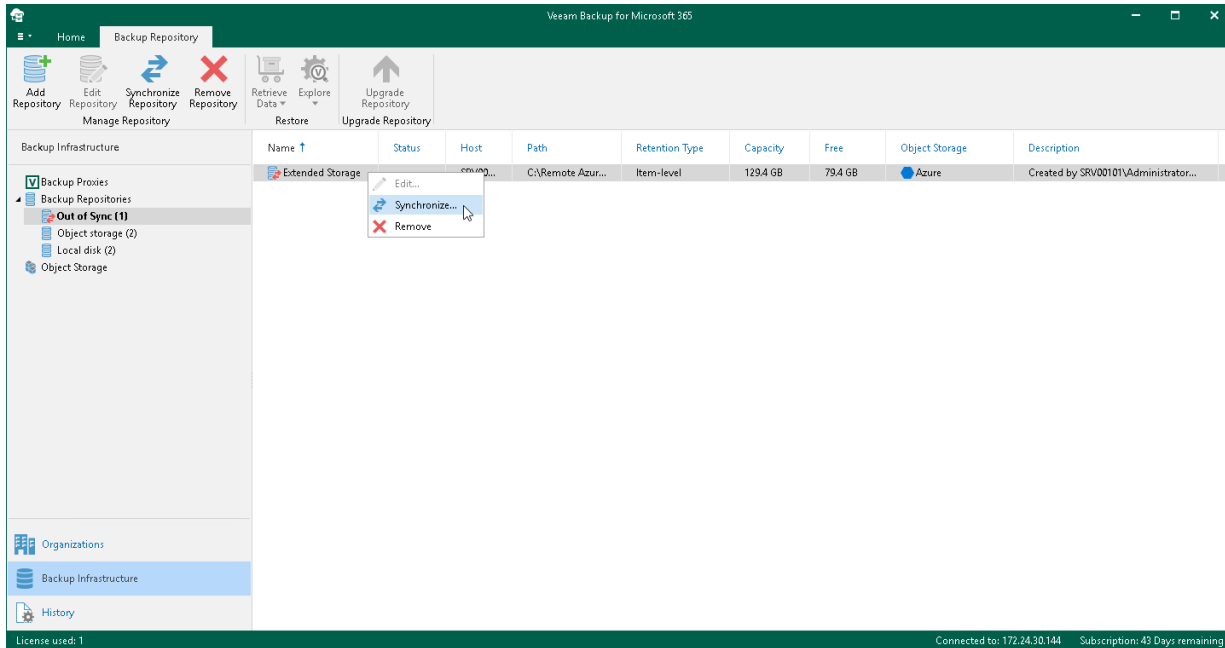
- Open and restore data from backups located in object storage.
Backups located in object storage become available for browsing and restore. For more information, see [Exploring Single Organization](#) and [Exploring All Organizations](#).
- Create new backups and offload these backups to object storage. For more information, see [Data Backup](#).

To synchronize cache between object storage and extended backup repositories, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Backup Repositories > Out of Sync** node.
3. In the preview pane, do one of the following:
 - Select a backup repository and click **Synchronize Repository** on the ribbon.
 - Right-click a backup repository and select **Synchronize**.

During synchronization, Veeam Backup for Microsoft 365 downloads metadata (cache) from object storage to the selected backup repository. For more information about cache, see [Cache](#).

If you want to stop synchronization, click **Stop Sync** on the ribbon.



Invalid State

In Veeam Backup for Microsoft 365, a backup repository can be put into the *Invalid* state in any of the following cases:

- Local cache on an extended backup repository is different from that in object storage.
A cache state is verified by comparing timestamps and an identification number of the associated backup and proxy repositories; these values must be identical to each other.
- A repository lock in object storage is missing.
A repository lock is imposed by the backup proxy server and prevents such locked object storage from being added as an extension to any other backup repository configuration. A lock file is saved to the *RepositoryLock* directory. For more information, see [Object Storage Structure](#).
- A trusted certificate for S3 Compatible object storage has been changed.
- If any of the following is true for extended backup repositories:
 - A connection to object storage is missing.
 - A container/bucket is missing or has been renamed.
 - A repository folder is missing or has been renamed.
- A connection to DAS or NAS is missing.
Such an invalid backup repository becomes available after your DAS or NAS is online.

Once a repository is put into the *Invalid* state, restore or backup from/to such a repository is impossible.

Invalid backup repositories can be found in the **Backup Infrastructure** view under the **Backup Repositories > Invalid** node.

NOTE

For more information on how to troubleshoot the *Invalid* state, see [this Veeam KB article](#).

The screenshot displays the Veeam Backup for Microsoft 365 console. The left-hand navigation pane shows a tree view under 'Backup Infrastructure' with 'Backup Repositories' expanded to show 'Invalid (1)'. The main pane features a table of repository details.

Name	Status	Host	Path	Retention...	Capacity	Free	Object Sto...	Description
Extended Storage (Amazo...	Invalid	SRV00...	C:\Remote A...	Snapshot-ba...	129.4 GB	79.4 GB	Amazon S3	Created by SRV00101VAdministrator...

At the bottom of the interface, the status bar indicates 'License used: 1', 'Connected to: 172.24.30.144', and 'Subscription: 43 Days remaining'.

Object Storage

Veeam Backup for Microsoft 365 uses object storage as part of the [extended backup repository storage system](#) to store backups and backup copies created for Microsoft 365 and on-premises Microsoft organizations. Veeam Backup for Microsoft 365 supports the following cloud and on-premises storage systems:

- S3 Compatible object storage
Any S3 Compatible object storage device fully compatible with the AWS S3 operations and AWS S3 Signature Version 4 standard.
- Amazon S3 object storage
For more information about Amazon S3 object storage, see [this Amazon article](#). For more information about Amazon S3 storage classes that Veeam Backup for Microsoft 365 supports, see [Supported Amazon S3 Storage Classes](#). For more information about required permissions, see [Amazon S3 Storage Permissions](#).
- Microsoft Azure Blob storage
For more information about Microsoft Azure Blob storage, see [this Microsoft article](#). For more information about Azure storage account types that Veeam Backup for Microsoft 365 supports, see [Supported Azure Storage Account Types](#). For more information about Azure Blob storage permissions, see [Azure Blob Storage Permissions](#).
- IBM Cloud Object Storage
For more information about IBM Cloud Object Storage, see [this IBM article](#).
- Wasabi Cloud Object Storage
For more information about Wasabi Cloud Object Storage, see [this Wasabi article](#).

Object Storage Usage Scenarios

Veeam Backup for Microsoft 365 offers the following usage scenarios for object storage:

- *Data backup.* In this scenario, you extend a backup repository with object storage supported for data backup and target a backup job at such an extended repository. During a backup job, data will be compressed and backed up directly to object storage. For more information, see [Extended Backup Repositories](#) and [Specify Backup Proxy and Repository](#).
- *Backup copy.* In this scenario, you extend a backup repository with object storage supported for backup copy and select such an extended repository as a target for a backup copy job. For more information, see [Extended Backup Repositories](#) and [Getting Started with Backup Copy](#).

Veeam Backup for Microsoft 365 allows you to protect data in backup copies from loss as a result of attacks, malware activity or other injurious actions that may be performed by 3rd party applications. To do this, you need to enable immutability when adding object storage to Veeam Backup for Microsoft 365. Keep in mind that object storage with enabled immutability can be used only to store backup copies. For more information about protecting data in backup copies, see [Immutability](#).

NOTE

Veeam Backup for Microsoft 365 supports Azure Blob Storage Archive access tier, Amazon S3 Glacier Instant Retrieval, Amazon S3 Glacier Flexible Retrieval and Amazon S3 Glacier Deep Archive storage classes only as a target for backup copy jobs.

Data Validation

Veeam Backup for Microsoft 365 provides a self-check mechanism that allows the product to validate if backed-up data appears in object storage uncorrupted after compression and transfer.

The process of data validation involves the following steps:

1. Before sending data to object storage, Veeam Backup for Microsoft 365 calculates hash: for Amazon S3 object storage and S3 Compatible object storage both the MD5 and SHA256 checksums are calculated, for Microsoft Azure Blob storage – the MD5 checksum only.
2. When the backed-up data appears in object storage, checksums are calculated again and are compared with values obtained before data was sent to object storage.

NOTE

Different checksums mean that data was corrupted during transfer to object storage. Such data will not be saved to object storage. Veeam Backup for Microsoft 365 will try to resend data to object storage.

Object Storage Structure

Object storage is cloud-based or on-premises storage system that you can employ to store your backups and backup copies as part of the extended backup repository storage system.

Veeam Backup for Microsoft 365 creates and maintains the following different structures for object storage depending on their usage scenario:

- [Storage for Backups](#)
- [Storage for Backup Copies](#)

Storage for Backups

The following table lists the structure that is created and maintained by Veeam Backup for Microsoft 365 in object storage where you store your backups. You can use S3 Compatible object storage, Azure Blob Storage Hot/Cool access tiers, Amazon S3 Standard and Amazon S3 Standard-Infrequent Access storage classes for this purpose.

NOTE

Veeam Backup for Microsoft 365 does not support this structure for Azure Blob Storage Archive access tier and all Amazon S3 Glacier storage classes. You cannot target a backup job at a backup repository extended with such object storage.

Directory	Description
<bucket_name/container_name>	A bucket or container name. Buckets and containers must be created in advance using the cloud provider tools. Veeam Backup for Microsoft 365 does not support creating new buckets or containers.

Directory	Description
<bucket_name/container_name>/Veeam/Backup365/	A set of mandatory folders created by Veeam Backup for Microsoft 365.
<repository_folder_name>	<p>A repository folder that you create when adding a new object storage.</p> <p>For more information on how to add a new object storage, see Adding Object Storage.</p>
<repository_folder_name>/CommonInfo	<p>Contains the following directories and blob files:</p> <ul style="list-style-type: none"> • <i>[Directory] RestorePoints</i>. Contains information about available restore points for Microsoft Exchange. • <i>[Directory] WebRestorePoints</i>. Contains information about available restore points for Microsoft SharePoint and OneDrive for Business. <p>Both directories keep a blob file that contains a list of available restore points. Each blob may store up to 100,000 records after which another blob file is created.</p> <ul style="list-style-type: none"> • <i>[Blob file] Organizations</i>. Contains a list of backed-up organizations. • <i>[Blob file] RepositoryConfig</i>. Contains extended backup repository configuration such as the retention type and other auxiliary information.
<repository_folder_name>/CriticalDataBackup	<p>Contains identical copies of the following blob files:</p> <ul style="list-style-type: none"> • <i>[Blob file] Organizations</i>. Contains a list of backed-up organizations. • <i>[Blob file] RepositoryConfig</i>. Contains extended backup repository configuration such as the retention type and other auxiliary information. • <i>[Blob file] BackupKeys</i>. Contains information about the encryption keys that you set during extension of a backup repository with object storage.

Directory	Description
<repository_folder_name>/Encryption	<p>Contains the <i>BackupKeys</i> blob file that holds information about the encryption keys that you set during extension of a backup repository with object storage.</p> <p>For more information on how to extend a backup repository with object storage, see Specify Object Storage.</p>
<repository_folder_name>/Organizations	<p>The root folder that contains backed-up Microsoft organizations. Each organization is kept in its own folder with a unique identification number.</p>
Organizations/<organization_Id>	<p>The <i><organization_Id></i> directory contains the following blob files:</p> <ul style="list-style-type: none"> • <i>AccountMailbox</i>. Contains information required to load the backup contents into the Veeam Explorer for Microsoft Exchange scope. • <i>AccountWeb</i>. Contains information required to load the backup contents into the Veeam Explorer for Microsoft SharePoint scope.

Directory	Description
<p><organization_Id>/Mailboxes/<mailbox_Id></p>	<p>The <i>Mailboxes</i> directory contains backed-up Exchange mailboxes. Each mailbox is saved under a unique identification number to the < <i>mailbox_Id</i> > directory.</p> <p>The < <i>mailbox_Id</i> > directory contains the following directories:</p> <ul style="list-style-type: none"> • <i>Folders</i>. Contains backed-up Exchange folders such as <i>Inbox</i>, <i>Drafts</i>, <i>Sent Items</i>, and other. • <i>FoldersHistory</i>. Contains folder changes. <p>For example, you may have renamed a folder. In such a scenario, after the subsequent backup session, Veeam Backup for Microsoft 365 will update information about the renamed folders and save each new folder version to the <i>FoldersHistory</i> directory.</p> <ul style="list-style-type: none"> • <i>ItemsChanges</i>. Contains incremental backup data. • <i>ItemsData</i>. Contains blob data of the backed-up Exchange messages. <p>For example, attachments are saved to this folder.</p> <ul style="list-style-type: none"> • <i>ItemsPreview</i>. Contains required data to load the backup contents into the Veeam Explorer for Microsoft Exchange scope. • <i>PostsPreview</i>. Contains required data to load the backup contents into the Veeam Explorer for Microsoft Teams scope.
<p><organization_Id>/RestorePointObjects</p>	<p>Contains blob files with a list of objects (mailboxes, sites, and other) that were backed up by Veeam Backup for Microsoft 365 per a particular restore point at the specified point in time.</p>
<p><organization_Id>/Sites</p>	<p>Contains a blob file with a list of backed-up SharePoint sites.</p>

Directory	Description
<organization_id>/Teams	<p>Contains the following directories:</p> <ul style="list-style-type: none"> • <i>Accounts</i>. Contains names and descriptions of all users included in all teams at the moment of the latest backup. • <i><team_id></i>. Contains backed-up Microsoft Teams data such as <i>Channels</i>, <i>Tabs</i> and <i>Users</i>. • <i>TeamHistorySnapshots</i>. Contains blob files with team changes and information about team <i>Applications</i> at the specified point in time. • <i>TeamInfos</i>. Contains blob files with unchanged information about teams.
<organization_id>/WebData	Contains data that is required to restore SharePoint or OneDrive items.
<organization_id>/WebBackups	Contains a list of SharePoint sites to be loaded into the Veeam Explorer for Microsoft SharePoint scope.
<organization_id>/WebPreview	<p>Contains backup dates of SharePoint sites.</p> <p>Required for a snapshot-based retention policy.</p>
<organization_id>/Webs/<web_id>	<p>A set of folders that contain backed-up SharePoint sites and OneDrive Items.</p> <p>The <i><web_id></i> directory contains the following directories:</p> <ul style="list-style-type: none"> • <i>Files</i>. Contains files of the SharePoint site. • <i>Items</i>. Contains items such as those located under the <i>Subsites</i> and <i>Content</i> folders for SharePoint, and users folders for OneDrive. • <i>Lists</i>. Contains SharePoint lists. • <i>ListsData</i>. Contains properties of SharePoint lists. • <i>ListViews</i>. Contains SharePoint list views.
<repository_folder_name>/RepositoryLock	<p>Contains a lock file that tells that this storage is already an extension to a backup repository.</p> <p>Object storage can only be owned by one owner (a backup repository) at a time.</p> <p>For more information on how to extend a backup repository with object storage, see Specify Object Storage.</p>



Storage for Backup Copies

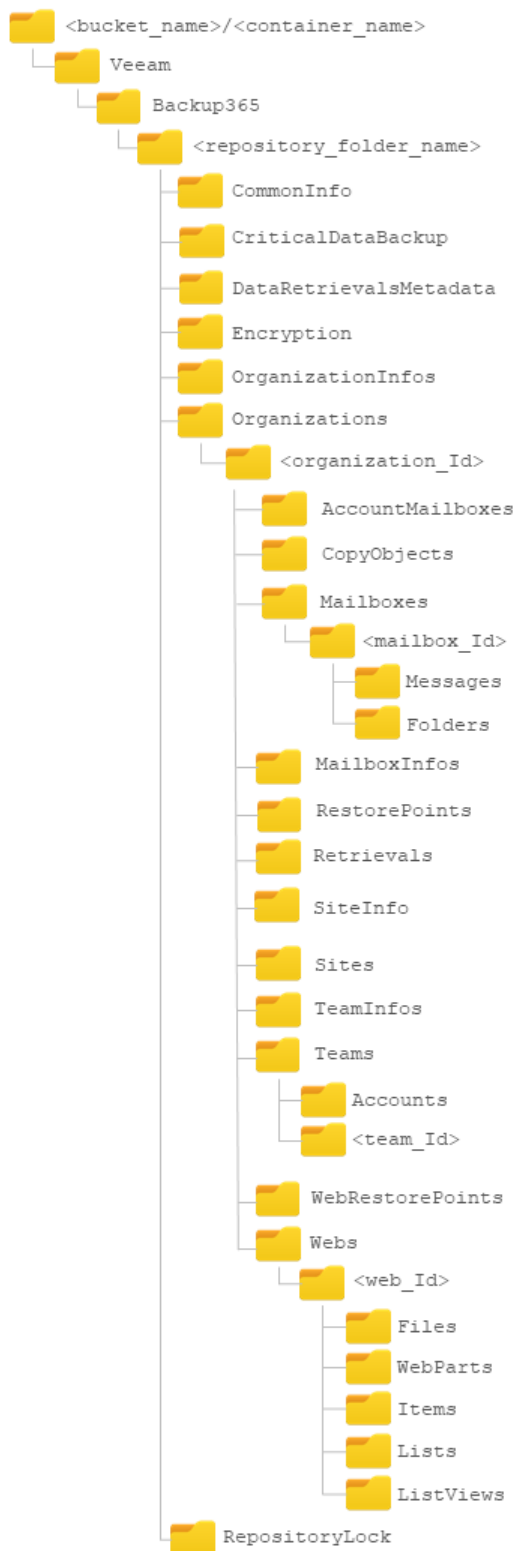
The following table lists the structure that is created and maintained by Veeam Backup for Microsoft 365 in object storage where you create an instance of your backups using backup copy. You can use any supported object storage for this purpose. For more information, see [Object Storage](#).

Directory	Description
<bucket_name/container_name>	<p>A bucket or container name.</p> <p>Buckets and containers must be created in advance using the cloud provider tools. Veeam Backup for Microsoft 365 does not support creating new buckets or containers.</p>

Directory	Description
<bucket_name/container_name>/Veeam/Backup365/	A set of mandatory folders created by Veeam Backup for Microsoft 365.
<repository_folder_name>	<p>A repository folder that you create when adding a new object storage.</p> <p>For more information on how to add a new object storage, see Adding Object Storage.</p>
<repository_folder_name>/CommonInfo	<p>Contains the following blob files:</p> <ul style="list-style-type: none"> • <i>[Blob file] StorageStatistics</i>. Contains information on used space in object storage per organization. • <i>[Blob file] RepositoryConfig</i>. Contains extended backup repository configuration such as the retention type and other auxiliary information, as well as version of the blob file.
<repository_folder_name>/CriticalDataBackup	<p>Contains identical copies of the following blob files:</p> <ul style="list-style-type: none"> • <i>[Blob file] RepositoryConfig</i>. Contains extended backup repository configuration such as the retention type and other auxiliary information, as well as version of the blob file. • <i>[Blob file] BackupKeys</i>. Contains information about the encryption keys that you set during extension of a backup repository with object storage, as well as version of the blob file.
<repository_folder_name>/DataRetrievalsMetadata	Contains information about backed-up data retrievals.
<repository_folder_name>/Encryption	<p>Contains the <i>BackupKeys</i> blob file that holds information about the encryption keys that you set during extension of a backup repository with object storage, as well as version of the blob file.</p> <p>For more information on how to extend a backup repository with object storage, see Specify Object Storage.</p>
<repository_folder_name>/OrganizationInfos	Contains blob files with the information about archived Microsoft organizations.

Directory	Description
<repository_folder_name>/Organizations	The root folder that contains archived Microsoft organizations. Each organization is kept in its own folder with a unique identification number.
<organization_id>/AccountMailboxes	Contains blob files with the information about account mailboxes.
<organization_id>/CopyObjects	Contains dates of the latest attempt of saving backed-up data of objects per object.
<organization_id>/Mailboxes/<mailbox_id>	<p>The <i>Mailboxes</i> directory contains archived Exchange mailboxes. Each mailbox is saved under a unique identification number to the <mailbox_id> directory.</p> <p>The <mailbox_id> directory contains the following directories:</p> <ul style="list-style-type: none"> • <i>Messages</i>. Contains archived Exchange data. • <i>Folders</i>. Contains a snapshot of Exchange folders at the specified point in time.
<organization_id>/MailboxInfos	Contains blob files with the information about archived Exchange mailboxes.
<organization_id>/RestorePoints	Contains blob files with the information about restore points created by Veeam Backup for Microsoft 365 and a list of restore point objects per restore point.
<organization_id>/Retrievals	Contains blob files with the information about backed-up data that was retrieved.
<organization_id>/SiteInfo	Contains blob files with the information about archived SharePoint sites.
<organization_id>/Sites	Contains a blob file with a list of archived SharePoint sites.
<organization_id>/TeamInfos	Contains blob files with the unchanged information about teams.

Directory	Description
<organization_id>/Teams	<p>Contains the following directories:</p> <ul style="list-style-type: none"> • <i>Accounts</i>. Contains names and descriptions of all users included in all teams. • <i><team_id></i>. Contains archived Microsoft Teams data such as <i>Channels</i>, <i>Tabs</i>, <i>Applications</i> and <i>UsersMembership</i>.
<organization_id>/WebRestorePoints	<p>Contains information on how web objects were backed up per restore point.</p>
<organization_id>/Webs/<web_id>	<p>A set of folders that contain archived SharePoint sites and OneDrive Items.</p> <p>The <i><web_id></i> directory contains the following directories:</p> <ul style="list-style-type: none"> • <i>Files</i>. Contains archived files of the SharePoint site. • <i>WebParts</i>. Contains Web Parts of SharePoint sites. • <i>Items</i>. Contains archived items such as those located under the <i>Subsites</i> and <i>Content</i> folders for SharePoint, and users folders for OneDrive. • <i>Lists</i>. Contains archived SharePoint lists. • <i>ListViews</i>. Contains archived SharePoint list views.
<repository_folder_name>/RepositoryLock	<p>Contains a lock file that tells that this storage is already an extension to a backup repository.</p> <p>Object storage can only be owned by one owner (a backup repository) at a time.</p> <p>For more information on how to extend a backup repository with object storage, see Specify Object Storage.</p>



Cache

Cache helps you reduce costs incurred by your cloud storage provider when reading or writing data to/from object storage.

For example, when you use Veeam Explorers to open backups located in object storage, Veeam Backup for Microsoft 365 uses cache from which it retrieves the structure of the backed-up objects of your organizations. Such a structure is then loaded into the inventory pane of each of the Veeam Explorers so that you can navigate through it without actually downloading any data from object storage.

Consider the following about cache:

- Cache is metadata that holds information about backed-up objects.
- Cache is created (or updated) during each backup session.
- Cache is saved to the *PersistentCache* directory in an extended backup repository as a JET-based database and also replicated to object storage.

Replication gives Veeam Backup for Microsoft 365 the ability to synchronize cache between object storage and the backup repository when:

- Creating a new backup repository and extending it with object storage that contains offloaded backup data.

For more information on how to extend a backup repository, see [Specify Object Storage](#).

- Recovering lost cache.

For example, you may have accidentally removed a directory with cache from the extended backup repository. In such a scenario, manual synchronization is required. For more information on how to synchronize data, see [Synchronizing Repositories](#).

The location of the *PersistentCache* directory is specified at the [Specify Backup Proxy Server](#) step.

Compression

Compression in Veeam Backup for Microsoft 365 helps you save storage space and reduce costs incurred by your cloud storage provider for maintaining backup data.

Compression works in the following way:

- All chunks of data that are larger than 512 bytes are subject to compression; each blob file that is created is compressed first and then saved to object storage.

To compress data, Veeam Backup for Microsoft 365 uses the *ZSTD* algorithm. For more information about this algorithm, see [this Zstandard article](#).

- Compression is done by the backup proxy server that you specify at the [Specify Backup Proxy Server](#) step.
- Certain types of data such as images or other media files cannot be compressed properly. Thereby an output compressed blob file becomes larger than it could be if it was not compressed at all. In such a scenario, the uncompressed version of the file will be saved.

Data Encryption

Data security is an important part of the backup strategy. You can use data encryption to protect your backups from unauthorized access in object storage.

Before transferring your backed-up data to object storage, *Veeam Backup Proxy for Microsoft 365 Service* encrypts data with the help of a cryptographic algorithm and a secret key. If encrypted data is intercepted, it cannot be unlocked and read by the eavesdropper. Only intended recipients who know the secret key can reverse encrypted information back to a readable format.

Veeam Backup for Microsoft 365 generates a secret key based on an encryption password that you create by yourself. For more information on how to configure encryption passwords, see [Managing Encryption Passwords](#).

For data encryption, Veeam Backup for Microsoft 365 uses the 256-bit Advanced Encryption Standard (AES). For more information about AES, see [this article](#).

Encryption Algorithm

To encrypt backed-up data, Veeam Backup for Microsoft 365 employs a *symmetric-key* encryption algorithm.

The symmetric, or single-key encryption algorithm, uses a single, common secret key to encrypt and decrypt data. Before data is sent to object storage, it is encoded with a secret key. To restore encrypted data, you must have the same secret key. Users who do not have the secret key cannot decrypt data and get access to it.

Object Storage Retention

Obsolete restore points are removed from object storage automatically by Veeam Backup for Microsoft 365. Data removal is based on the [retention policy settings](#) that you configure when extending a backup repository with object storage.

Depending on how frequently your retention policy is configured to be executed, Veeam Backup for Microsoft 365 initiates a service task that calculates the age of offloaded restore points and if the age exceeds the specified retention period, this task purges obsolete restore points from object storage.

IMPORTANT

Do not remove anything from object storage manually, as this will irreversibly damage your backup structure to the point where you will be completely unable to read data from such corrupted backups.

Object Storage Retention for Backup Copies

Consider the following:

- The retention type of an extended backup repository selected as a target for a backup copy job must match that of an extended backup repository where you store your backups. The retention period can be different. For more information, see [Specify Retention Policy Settings](#).
- If you increase the retention policy value for an extended backup repository selected as a target for a backup copy job that has the item-level retention type and start a backup copy job without source backup job started prior to that, Veeam Backup for Microsoft 365 will not copy backed-up data of items whose last modification time fits the updated retention coverage of backup copy.

Immutability

Veeam Backup for Microsoft 365 allows you to prohibit deletion of backup copies from object storage by making that data temporarily immutable. It is done for increased security: immutability protects your data from loss as a result of attacks, malware activity or other injurious actions that may be performed by 3rd party applications.

You can enable immutability when adding object storage to Veeam Backup for Microsoft 365. Keep in mind that object storage with enabled immutability can be used only to store backup copies. The immutability period matches the retention period configured for the backup repository which is extended with such object storage. Data will be blocked for deletion or modification for the same period as the retention period. For more information, see [Specify Retention Policy Settings](#).

Veeam Backup for Microsoft 365 extends the immutability period in the following ways:

- If the extended backup repository has the *snapshot-based* retention type, the duration of the immutability period for backup copies stored in object storage will be prolonged only for those parts of a snapshot for which retention policy still can be applied.
- If the extended backup repository has the *item-level* retention type, the duration of the immutability period for backup copies stored in object storage will be prolonged only for those objects for which retention policy still can be applied.

Before You Begin to Use Immutability

Amazon S3 and S3 Compatible Object Storage

To use immutability for backed-up data that you want to store in Amazon S3, Amazon S3 Glacier and S3 Compatible object storage, you must enable the *Object Lock* and *Versioning* features on your Amazon S3 bucket and S3 Compatible bucket at the time you create the bucket. Keep in mind that most vendors allow enabling *Object Lock* only at the moment of creating the bucket. Once imposed, the *Object Lock* prohibits deletion of data from object storage until the immutability period ends.

For more information, see these Amazon articles: [Creating a bucket](#), [Using S3 Object Lock](#), [Using versioning in S3 buckets](#).

Azure Blob Storage

If you want to use immutability for backed-up data that you want to store in Microsoft Azure Blob Storage, you must enable the immutability settings for the object storage.

Do the following:

- Enable either [version-level immutability support](#) or [blob versioning](#) for the Microsoft Azure Blob storage account.
- Make sure that the [default time-based retention policy](#) is not configured for the Microsoft Azure Blob storage account.
- Enable [version-level immutability support](#) for the Azure container.

For more information about immutable Microsoft Azure Blob Storage, see [this Microsoft article](#).

Adding Object Storage

You can add the following types of object storage to the Veeam Backup for Microsoft 365 backup infrastructure:

- [S3 Compatible Object Storage](#)
- [Amazon S3 Object Storage](#)
- [Microsoft Azure Blob Storage](#)
- [IBM Cloud Object Storage](#)

- [Wasabi Cloud Object Storage](#)

Adding S3 Compatible Object Storage

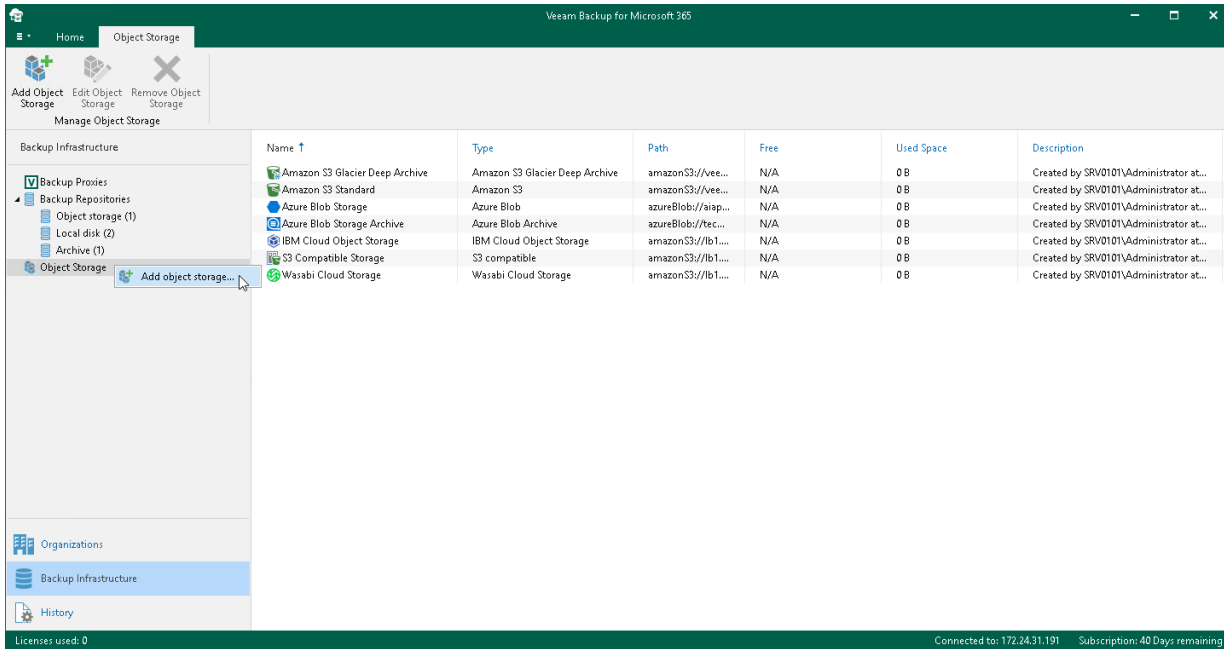
To add a new S3 Compatible object storage to the Veeam Backup for Microsoft 365 backup infrastructure, do the following:

1. [Launch the Add Object Storage wizard.](#)
2. [Specify object storage name.](#)
3. [Select object storage type.](#)
4. [Specify object storage service point and account.](#)
5. [Specify object storage bucket.](#)

Step 1. Launch Add Object Storage Wizard

To launch the **Add Object Storage** wizard, do the following:

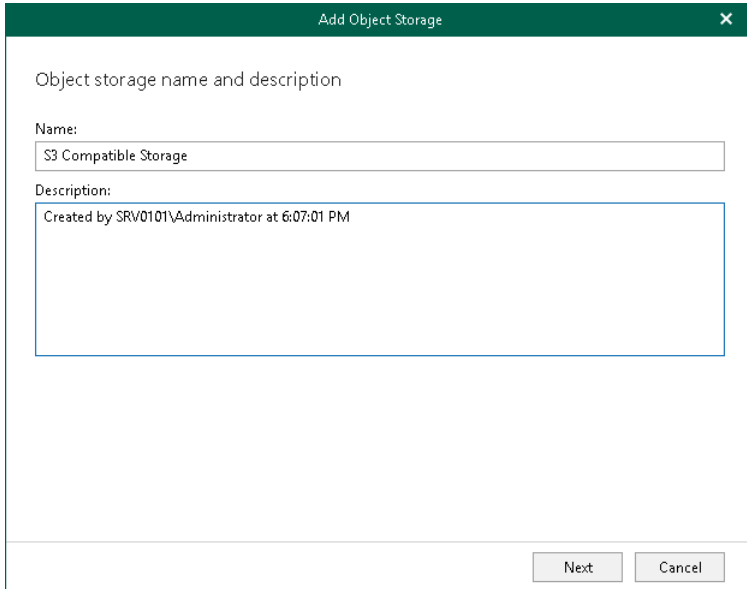
1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Object Storage** node.
3. Do one of the following:
 - On the **Object Storage** tab, click **Add Object Storage** on the ribbon.
 - Right-click the **Object Storage** node and select **Add object storage**.



Step 2. Specify Object Storage Name

At this step of the wizard, enter a name for object storage and provide optional description:

1. In the **Name** field, enter a name for object storage.
2. In the **Description** field, enter optional description.



Object storage name and description

Name:
S3 Compatible Storage

Description:
Created by SRV0101\Administrator at 6:07:01 PM

Next Cancel

Step 3. Select Object Storage Type

At this step of the wizard, select **S3 Compatible**.

Object storage type

- S3 Compatible**
Adds a cloud object storage provider, or an on-premises object storage system.
- Amazon S3**
Adds Amazon S3 storage. Standard, Infrequent Access (IA), S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval and S3 Glacier Deep Archive are supported.
- Microsoft Azure Blob Storage**
Adds Microsoft Azure cloud object storage. Microsoft Azure Blob Storage and Microsoft Azure Archive Storage are supported.
- IBM Cloud Object Storage**
Adds IBM Cloud object storage. S3 compatible versions of both on-premises and IBM Cloud storage offerings are supported.
- Wasabi Cloud Storage**
Adds Wasabi cloud object storage.

Back Next Cancel

Step 4. Specify Object Storage Service Point and Account

At this step of the wizard, specify a service point of your S3 Compatible device, select a datacenter region and specify account credentials.

1. In the **Service point** field, specify an endpoint address of your S3 Compatible device.
2. In the **Data center region** field, specify a region.
3. From the **Specify account credentials to connect to S3 compatible storage bucket** drop-down list, select user credentials to access your S3 Compatible object storage.

If you already have a credentials record that was configured beforehand, select such a record from the drop-down list. Otherwise, click **Add** and provide your access and secret keys. For more information, see [Adding S3 Compatible, IBM Cloud and Wasabi Cloud Storage Access Key](#). You can also click **Manage cloud accounts** to [manage existing credentials records](#).

S3 compatible storage system

Service point:
172.17.186.13:9000

Data center region:
us-east-1

Specify account credentials to connect to S3 compatible storage bucket:
XXXXXXXXXXXXXXXXXXXXXXXXX (Created by SRV0101/Administrator at 6:11 PM., last ed) Add...

[Manage cloud accounts](#)

Back Next Cancel

Step 5. Specify Object Storage Bucket

At this step of the wizard, specify object storage bucket and folder where you want to save your data.

1. From the **Bucket** drop-down list, select a bucket.

Make sure that the bucket you want to use to store your data was created in advance; Veeam Backup for Microsoft 365 does not support creating new buckets.

2. In the **Folder** field, select a folder to which you want to map your object storage, and which will be used to store offloaded data.

To select a folder, click **Browse** and either select an existing folder or create a new one by clicking **New Folder**.

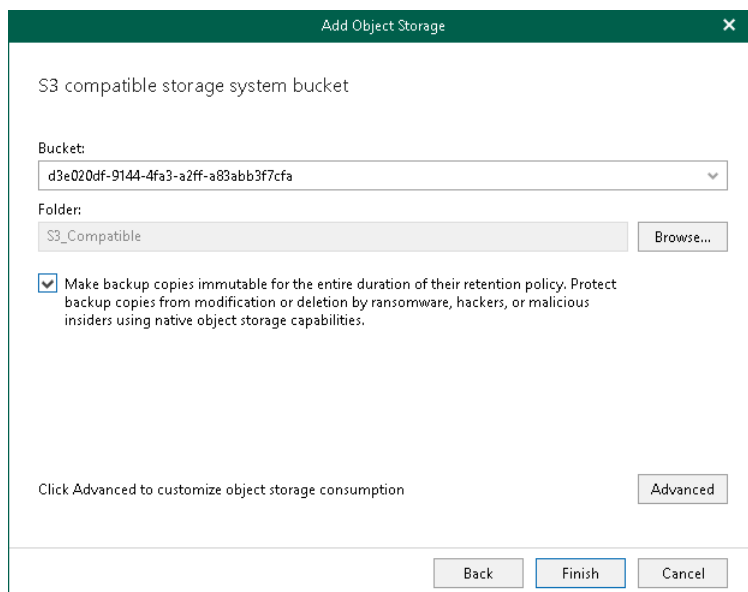
For more information on how data is stored, see [Object Storage Structure](#).

3. Select the **Make backup copies immutable for the entire duration of their retention policy** check box to enable protection of backup copies against accidental data deletions, malware activity and modifications that may be performed by 3rd party applications. For more information about immutability, see [Immutability](#).

NOTE

If you do not want to use immutability, make sure that *Versioning* is not enabled for the S3 Compatible bucket in which you want to save your data.

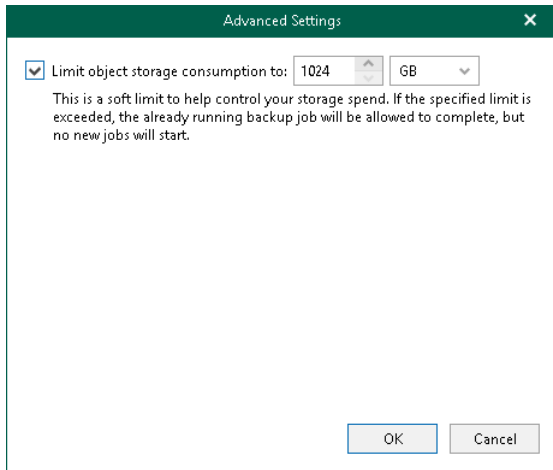
4. Click **Advanced** if you want to configure storage consumption limitations.



4. In the **Advanced Settings** window, do the following:
 - a. Select the **Limit object storage consumption** to check box and specify the limit value in GB, TB or PB.

If you select this check box, Veeam Backup for Microsoft 365 limits object storage capacity and prohibits running new jobs when the specified value is exceeded.

b. Click **OK**.



Adding Amazon S3 Object Storage

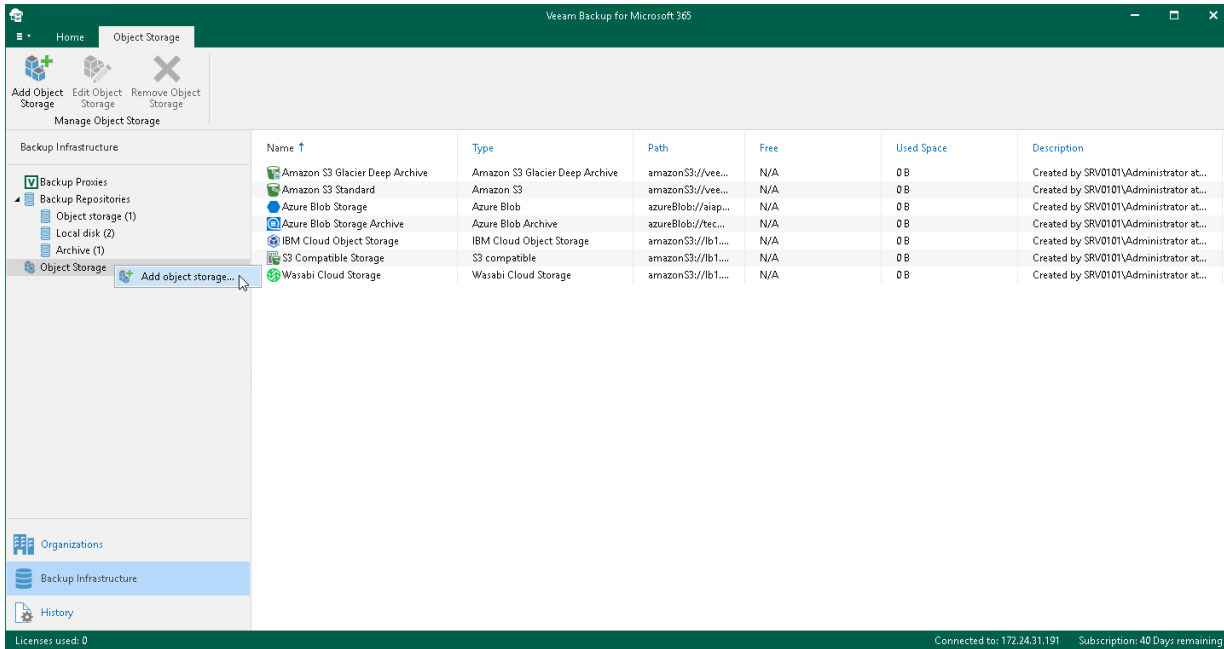
To add a new Amazon S3 object storage to the Veeam Backup for Microsoft 365 backup infrastructure, do the following:

1. [Launch the Add Object Storage wizard.](#)
2. [Specify object storage name.](#)
3. [Select object storage type.](#)
4. [Select Amazon S3 storage type.](#)
5. [Specify object storage account.](#)
6. [Specify object storage settings.](#)
7. [Select Amazon S3 Glacier storage class.](#)
8. [Configure the Amazon archiver appliance.](#)

Step 1. Launch Add Object Storage Wizard

To launch the **Add Object Storage** wizard, do the following:

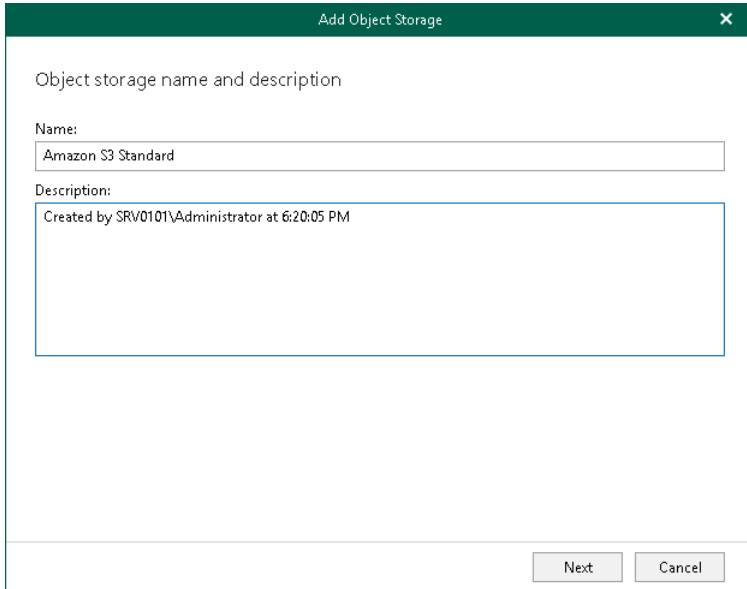
1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Object Storage** node.
3. Do one of the following:
 - On the **Object Storage** tab, click **Add Object Storage** on the ribbon.
 - Right-click the **Object Storage** node and select **Add object storage**.



Step 2. Specify Object Storage Name

At this step of the wizard, enter a name for object storage and provide optional description:

1. In the **Name** field, enter a name for object storage.
2. In the **Description** field, enter optional description.



Object storage name and description

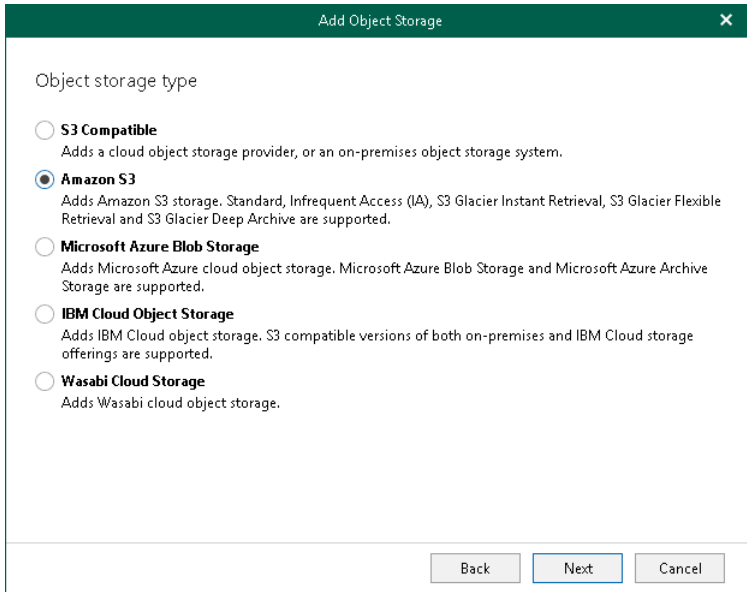
Name:
Amazon S3 Standard

Description:
Created by SRV0101\Administrator at 6:20:05 PM

Next Cancel

Step 3. Select Object Storage Type

At this step of the wizard, select **Amazon S3**.



The screenshot shows a dialog box titled "Add Object Storage" with a close button (X) in the top right corner. The main content area is titled "Object storage type" and contains five radio button options, each with a brief description:

- S3 Compatible**
Adds a cloud object storage provider, or an on-premises object storage system.
- Amazon S3**
Adds Amazon S3 storage. Standard, Infrequent Access (IA), S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval and S3 Glacier Deep Archive are supported.
- Microsoft Azure Blob Storage**
Adds Microsoft Azure cloud object storage. Microsoft Azure Blob Storage and Microsoft Azure Archive Storage are supported.
- IBM Cloud Object Storage**
Adds IBM Cloud object storage. S3 compatible versions of both on-premises and IBM Cloud storage offerings are supported.
- Wasabi Cloud Storage**
Adds Wasabi cloud object storage.

At the bottom of the dialog box, there are three buttons: "Back", "Next" (which is highlighted with a blue border), and "Cancel".

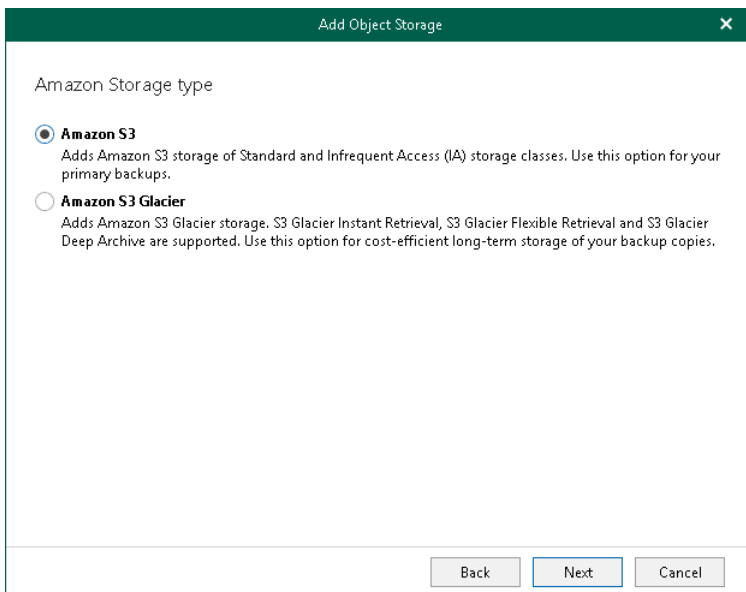
For more information about supported Amazon S3 storage classes, see [Supported Amazon S3 Storage Classes](#).

Step 4. Select Amazon Storage Type

At this step of the wizard, select one of the following options:

- **Amazon S3.** Select this option if you want to add Amazon S3 Standard and Amazon S3 Standard-Infrequent Access storage classes. You can use these storage classes as a target for both backup and backup copy jobs.
- **Amazon S3 Glacier.** Select this option if you want to use this object storage only to store backup copies and select it as a target for backup copy jobs. Veeam Backup for Microsoft 365 supports Amazon S3 Glacier Instant Retrieval, Amazon S3 Glacier Flexible Retrieval and Amazon S3 Glacier Deep Archive storage classes for this purpose.

For more information about supported Amazon S3 storage classes, see [Supported Amazon S3 Storage Classes](#).



Step 5. Specify Object Storage Account

At this step of the wizard, specify an Amazon account and select a datacenter region.

1. From the **Specify account credentials to connect to Amazon S3 storage bucket** drop-down list, select user credentials to access your Amazon S3 object storage.

If you already have a credentials record that was configured beforehand, select such a record from the drop-down list. Otherwise, click **Add** and provide your access and secret keys. For more information, see [Adding Amazon AWS Access Key](#). You can also click **Manage cloud accounts** to [manage existing credentials records](#).

2. From the **Region** drop-down list, select a datacenter region.

Amazon AWS account

Specify account credentials to connect to Amazon S3 storage bucket:

XXXXXXXXXXXXXXXXXXXX (Created by SRV0101/Administrator at 6:27 PM., last ed Add...

[Manage cloud accounts](#)

Region:

Global

Back Next Cancel

Step 6. Specify Object Storage Settings

At this step of the wizard, select a location of your Amazon bucket, a bucket and folder where you want to save your data.

1. From the **Data center location** drop-down list, select a region that contains available buckets.
2. From the **Bucket** drop-down list, select a bucket.

Make sure that the bucket you want to use to store your data was created in advance; Veeam Backup for Microsoft 365 does not support creating new buckets.

3. In the **Folder** field, select a cloud folder to which you want to map your object storage, and which will be used to store offloaded data.

To select a folder, click **Browse** and either select an existing folder or create a new one by clicking **New Folder**.

For more information on how data is stored, see [Object Storage Structure](#).

4. Select the **Make backup copies immutable for the entire duration of their retention policy** check box to enable protection of backup copies against accidental data deletions, malware activity and modifications that may be performed by 3rd party applications. For more information about immutability, see [Immutability](#).

NOTE

If you do not want to use immutability, make sure that *Versioning* is not enabled for the Amazon S3 bucket in which you want to save your data.

5. Click **Advanced** if you want to configure storage consumption limitations and select Amazon S3 storage classes. For more information, see [Configuring Advanced Settings](#).

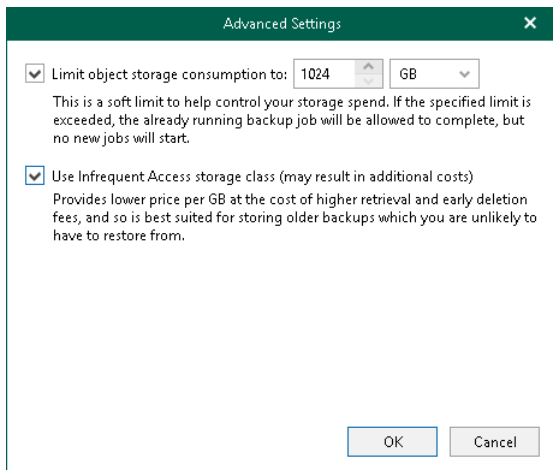
The screenshot shows a dialog box titled "Add Object Storage" with a close button (X) in the top right corner. The dialog is for configuring an Amazon S3 bucket. It contains the following fields and options:

- Amazon S3 bucket** (header)
- Data center location:** A dropdown menu with "US East (Ohio)" selected.
- Bucket:** A dropdown menu with "veeam-bw" selected.
- Folder:** A text input field containing "Amazon Storage" and a "Browse..." button to its right.
- A checked checkbox with the text: "Make backup copies immutable for the entire duration of their retention policy. Protect backup copies from modification or deletion by ransomware, hackers, or malicious insiders using native object storage capabilities."
- A text label: "Click Advanced to customize object storage consumption" and an "Advanced" button to its right.
- At the bottom, there are three buttons: "Back", "Next", and "Cancel".

Configuring Advanced Settings

In the **Advanced Settings** window, do the following:

1. Select the **Limit object storage consumption to** check box and specify the limit value in GB, TB or PB.
If you select this check box, Veeam Backup for Microsoft 365 limits object storage capacity and prohibits running new jobs when the specified value is exceeded.
2. If you have selected the **Amazon S3** option on the [Select Amazon Storage Type](#) step, select the **Use Infrequent Access storage class** check box if you plan to access your backup data in an infrequent manner and to mark each block as Amazon S3 Standard-Infrequent Access. For more information about infrequent access, see [this Amazon article](#).



3. Click **OK**.

Step 7. Select Amazon Storage Class

This step is only available if you have selected the **Amazon S3 Glacier** option at the [Select Amazon Storage Type](#) step of the wizard.

At this step of the wizard, select one of the following options:

- **Deep Archive.** Select this option if you plan to access your data in backup copies rarely. Veeam Backup for Microsoft 365 will mark each block as Amazon S3 Glacier Deep Archive.
- **Flexible Retrieval.** Select this option if you plan to access your data in backup copies 1-2 times per year and retrieve it asynchronously. Veeam Backup for Microsoft 365 will mark each block as Amazon S3 Glacier Flexible Retrieval.
- **Instant Retrieval.** Select this option if you plan to access your data in backup copies regularly and retrieve data in milliseconds. Veeam Backup for Microsoft 365 will mark each block as Amazon S3 Glacier Instant Retrieval.

Amazon Storage class

Specify a storage class based on your restore time and cost requirements.

- Deep Archive (lowest storage costs)**
This storage class has the lowest price per GB balanced by the longest early deletion period, the highest data retrieval costs, and the slowest data retrieval process. This makes this storage class ideal for "Write Once Read Never" use cases such as long-term storage for compliance purposes.
- Flexible Retrieval**
This storage class has a higher price per GB balanced by a shorter early deletion fee, lower data retrieval costs, and a faster data retrieval process. Choose this storage class if you foresee a need to restore a few times per year.
- Instant Retrieval (fastest restore)**
This storage class has the highest price per GB balanced by a shorter early deletion period, the lowest data retrieval costs, and the fastest (instant) data access. Choose this storage class if you foresee a need to restore regularly.

Back Next Cancel

Step 8. Configure Amazon Archiver Appliance

At this step of the wizard, you can optionally enable usage of the Amazon archiver appliance when Veeam Backup for Microsoft 365 creates a backup copy. Backed-up data is transferred between different instances of the general purpose object storage (Amazon S3 Standard and Amazon S3 Standard-Infrequent Access storage classes) or to any of Amazon S3 Glacier object storage (Amazon S3 Glacier Instant Retrieval, Amazon S3 Glacier Flexible Retrieval and Amazon S3 Glacier Deep Archive storage classes). For more information about supported Amazon S3 storage classes, see [Supported Amazon S3 Storage Classes](#).

If you use the archiver appliance, it usually speeds up the backup copy process and helps you reduce costs incurred by your cloud storage provider. Also, using the archiver appliance, you protect your backups because all operations with backed-up data are performed within the Amazon cloud.

The Amazon archiver appliance is an auxiliary EC2 instance that is deployed and configured automatically by Veeam Backup for Microsoft 365 in Amazon EC2 only for the duration of a backup copy job. Veeam Backup for Microsoft 365 removes or reuses it after a backup copy job completes. By default, Veeam Backup for Microsoft 365 always keeps one archiver appliance for reuse.

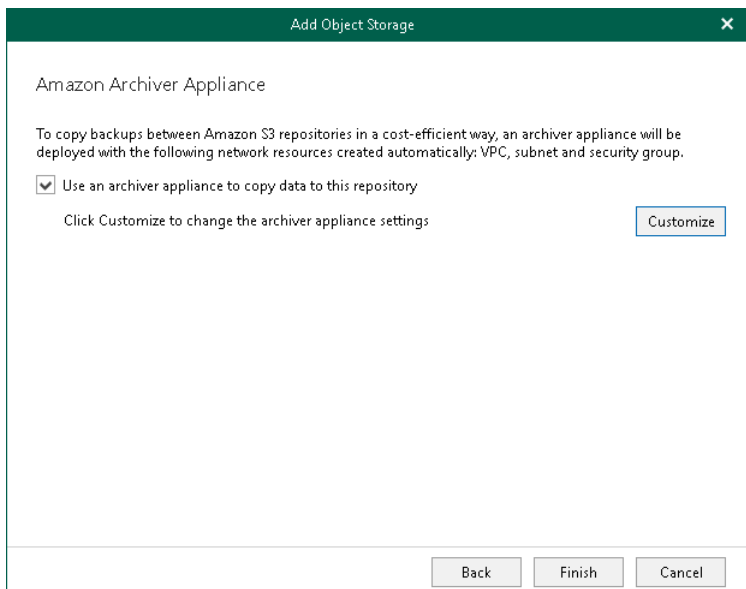
If you do not want to use the Amazon archiver appliance, skip this step and click **Finish**.

NOTE

Even if you have enabled usage of the archiver appliance for object storage, Veeam Backup for Microsoft 365 will not create it when transferring backed-up data between object storage of different vendors.

To enable usage of the Amazon archiver appliance, do the following:

1. Select the **Use an archiver appliance to copy data to this repository** check box.
2. Click **Customize** if you want to change the default settings of the archiver appliance.



3. In the **Cloud Archiver Appliance Settings** window, do the following:
 - a. From the **EC2 instance type** drop-down list, select the instance type for the archiver appliance. For more information on instance types, see [this Amazon article](#).
 - b. From the **Amazon Virtual Private Cloud (VPC)** drop-down list, select the Amazon VPC where Veeam Backup for Microsoft 365 will launch the target instance. For more information on the Amazon VPC, see [this Amazon article](#).

- c. From the **Subnet** drop-down list, select the subnet for the archiver appliance.

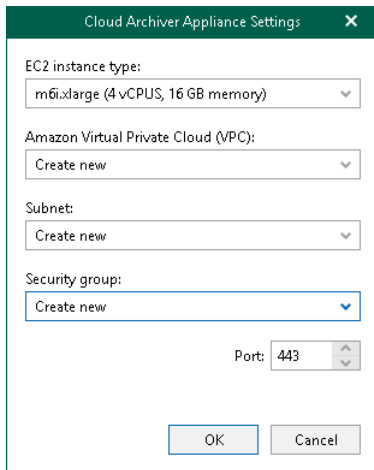
Keep in mind that auto-assignment of public IPv4 addresses must be enabled in the subnet. For more information, see [this Amazon article](#).

- d. From the **Security group** drop-down list, select a security group that will be associated with the archiver appliance.

Keep in mind that the security group must allow inbound and outbound traffic through the listed [ports](#). For more information on security groups for Amazon VPC, see [this Amazon article](#).

- e. Specify the port that Veeam Backup for Microsoft 365 will use to route requests between the archiver appliance and backup infrastructure components.

- f. Click **OK**.



The screenshot shows a dialog box titled "Cloud Archiver Appliance Settings" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- EC2 instance type:** A dropdown menu with "m6i.xlarge (4 vCPUS, 16 GB memory)" selected.
- Amazon Virtual Private Cloud (VPC):** A dropdown menu with "Create new" selected.
- Subnet:** A dropdown menu with "Create new" selected.
- Security group:** A dropdown menu with "Create new" selected.
- Port:** A numeric input field with "443" entered and up/down arrow buttons.
- Buttons:** "OK" and "Cancel" buttons at the bottom.

Adding Microsoft Azure Blob Storage

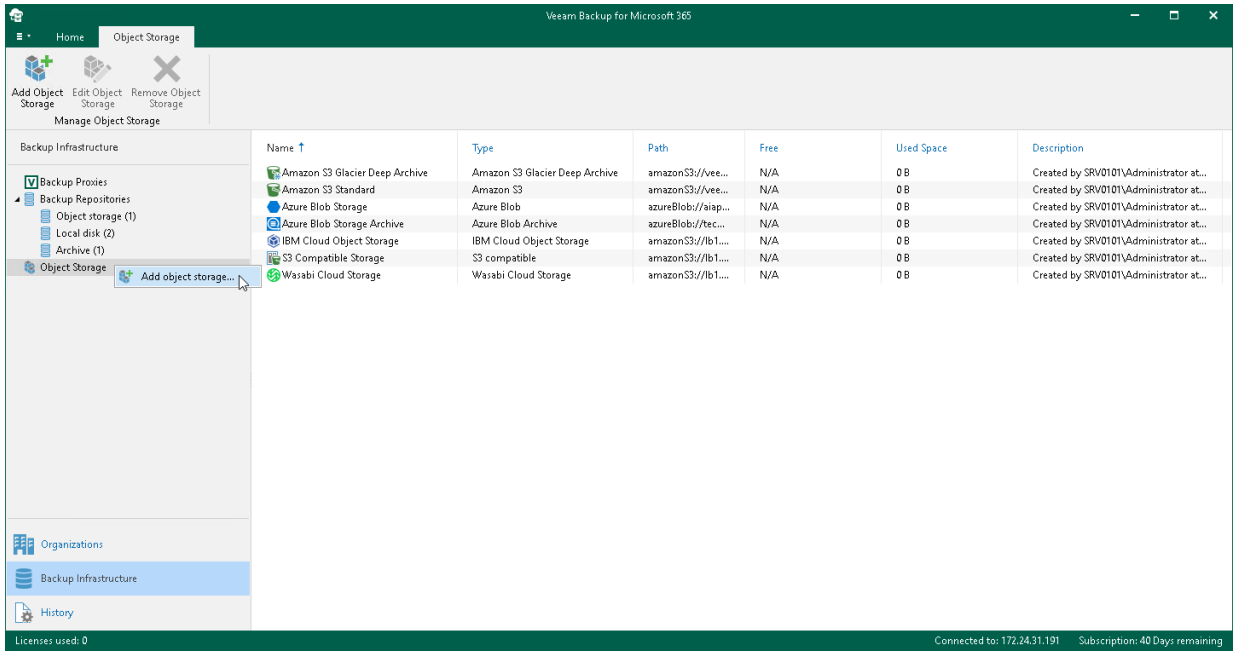
To add a new Microsoft Azure Blob Storage to the Veeam Backup for Microsoft 365 backup infrastructure, do the following:

1. [Launch the Add Object Storage wizard](#).
2. [Specify object storage name](#).
3. [Select object storage type](#).
4. [Select Microsoft Azure Blob Storage type](#).
5. [Specify object storage account](#).
6. [Specify object storage container](#).
7. [Configure the Azure archiver appliance](#).

Step 1. Launch Add Object Storage Wizard

To launch the **Add Object Storage** wizard, do the following:

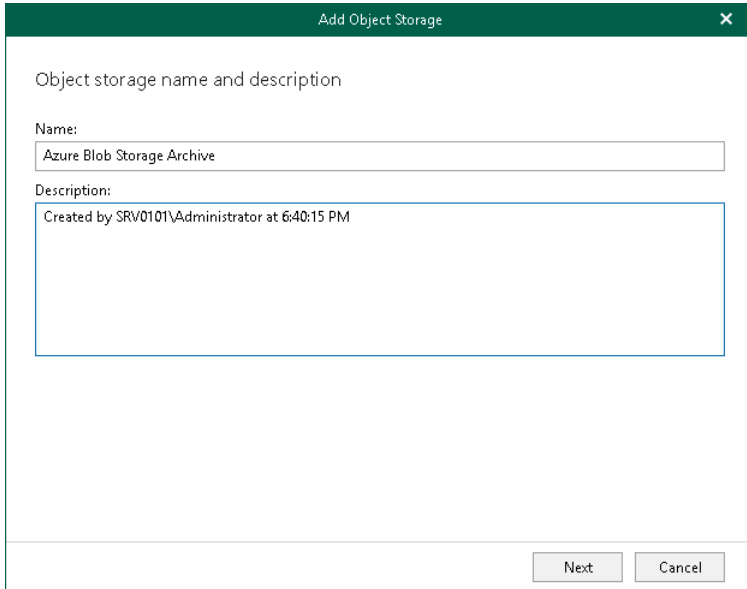
1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Object Storage** node.
3. Do one of the following:
 - On the **Object Storage** tab, click **Add Object Storage** on the ribbon.
 - Right-click the **Object Storage** node and select **Add object storage**.



Step 2. Specify Object Storage Name

At this step of the wizard, enter a name for object storage and provide optional description:

1. In the **Name** field, enter a name for object storage.
2. In the **Description** field, enter optional description.



Object storage name and description

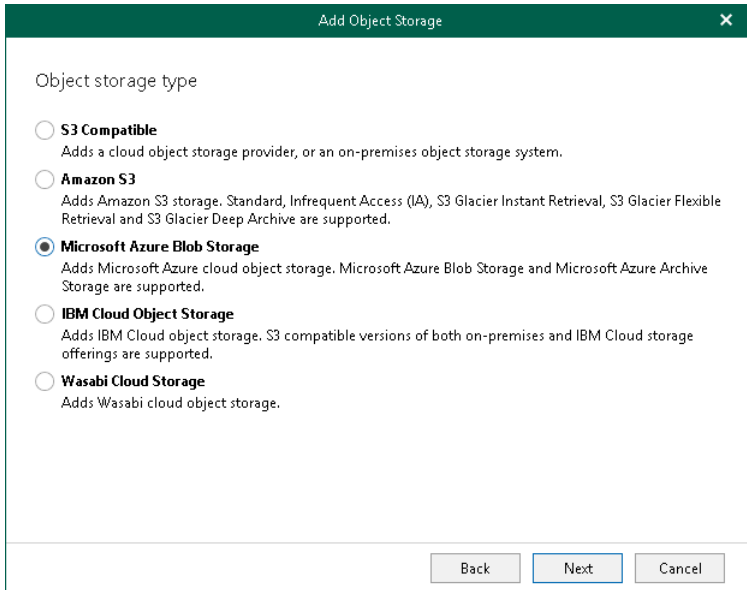
Name:
Azure Blob Storage Archive

Description:
Created by SRV0101\Administrator at 6:40:15 PM

Next Cancel

Step 3. Select Object Storage Type

At this step of the wizard, select **Microsoft Azure Blob Storage**.



The screenshot shows a dialog box titled "Add Object Storage" with a close button (X) in the top right corner. The main area is titled "Object storage type" and contains five radio button options, each with a description:

- S3 Compatible**
Adds a cloud object storage provider, or an on-premises object storage system.
- Amazon S3**
Adds Amazon S3 storage. Standard, Infrequent Access (IA), S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval and S3 Glacier Deep Archive are supported.
- Microsoft Azure Blob Storage**
Adds Microsoft Azure cloud object storage. Microsoft Azure Blob Storage and Microsoft Azure Archive Storage are supported.
- IBM Cloud Object Storage**
Adds IBM Cloud object storage. S3 compatible versions of both on-premises and IBM Cloud storage offerings are supported.
- Wasabi Cloud Storage**
Adds Wasabi cloud object storage.

At the bottom of the dialog box, there are three buttons: "Back", "Next", and "Cancel". The "Next" button is highlighted with a blue border.

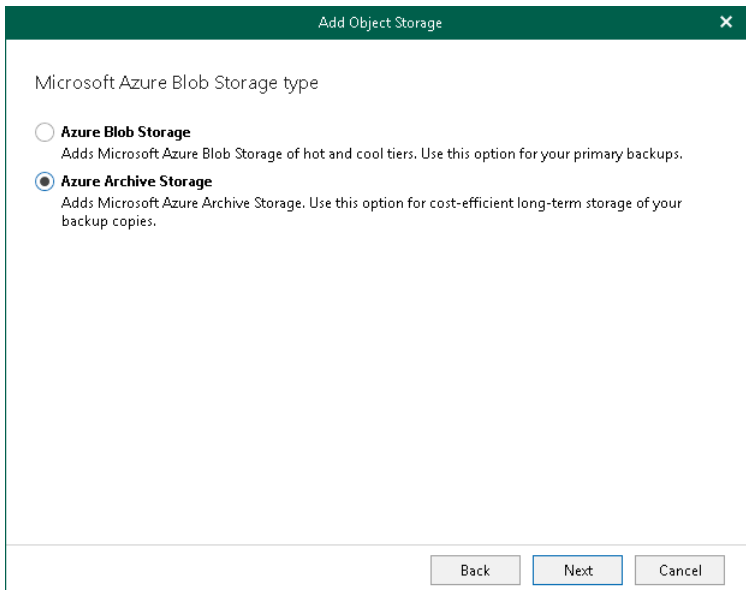
For more information about supported Azure storage account types and supported access tiers for Azure Blob Storage, see [Supported Azure Storage Account Types](#).

Step 4. Select Microsoft Azure Blob Storage Type

At this step of the wizard, select one of the following options:

- **Azure Blob Storage.** Select this option if you want to use this object storage as a target for both backup and backup copy jobs.
- **Azure Archive Storage.** Select this option if you want to use this object storage only to store backup copies and select it as a target for backup copy jobs. Veeam Backup for Microsoft 365 supports Azure Blob Storage Archive access tier for this purpose.

For more information about supported Azure storage account types and supported access tiers for Azure Blob Storage, see [Supported Azure Storage Account Types](#).



The screenshot shows a dialog box titled "Add Object Storage" with a close button (X) in the top right corner. The main content area is titled "Microsoft Azure Blob Storage type" and contains two radio button options:

- Azure Blob Storage**
Adds Microsoft Azure Blob Storage of hot and cool tiers. Use this option for your primary backups.
- Azure Archive Storage**
Adds Microsoft Azure Archive Storage. Use this option for cost-efficient long-term storage of your backup copies.

At the bottom of the dialog box, there are three buttons: "Back", "Next", and "Cancel". The "Next" button is highlighted with a blue border, indicating it is the active or default action.

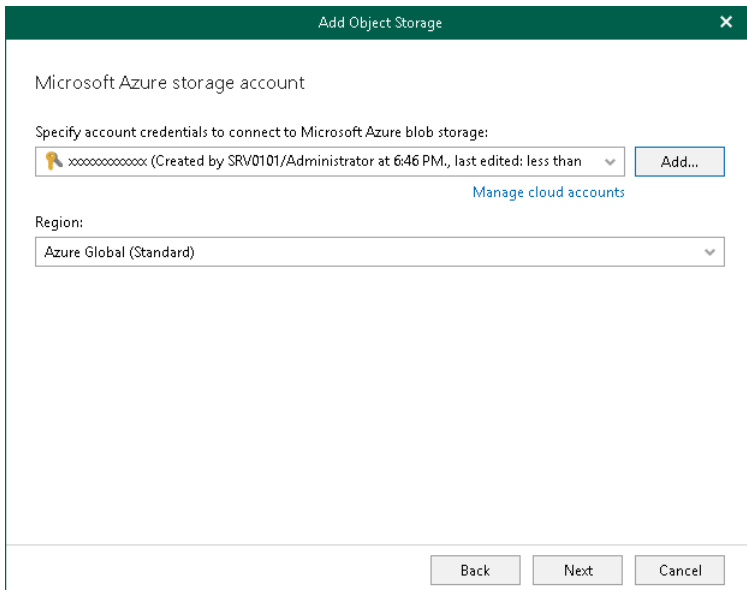
Step 5. Specify Object Storage Account

At this step of the wizard, specify a Microsoft Azure storage account and select a region.

1. From the **Specify account credentials to connect to Microsoft Azure blob storage** drop-down list, select user credentials to access your Azure Blob storage.

If you already have a credentials record that was configured beforehand, select such a record from the drop-down list. Otherwise, click **Add** and provide your account and a shared key. For more information, see [Adding Microsoft Azure Blob Storage Account](#). You can also click **Manage cloud accounts** to [manage existing credentials records](#).

2. From the **Region** drop-down list, select a Microsoft Azure region.



Microsoft Azure storage account

Specify account credentials to connect to Microsoft Azure blob storage:

xxxxxxxxxxxx (Created by SRV0101/Administrator at 6:46 PM., last edited: less than) Add...

[Manage cloud accounts](#)

Region:

Azure Global (Standard)

Back Next Cancel

Step 6. Specify Object Storage Container

At this step of the wizard, specify object storage container and folder where you want to save your data.

1. From the **Container** drop-down list, select an Azure container.

Make sure that the container you want to use to store your data was created in advance; Veeam Backup for Microsoft 365 does not support creating new containers.

2. In the **Folder** field, select a cloud folder to which you want to map your object storage, and which will be used to store offloaded data.

To select a folder, click **Browse** and either select an existing folder or create a new one by clicking **New Folder**.

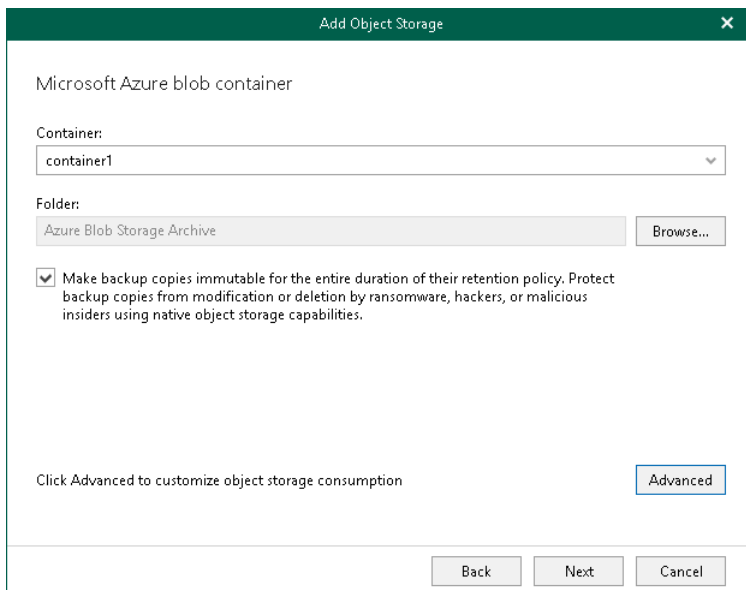
For more information on how data is stored, see [Object Storage Structure](#).

3. Select the **Make backup copies immutable for the entire duration of their retention policy** check box to enable protection of backup copies against accidental data deletions, malware activity and modifications that may be performed by 3rd party applications. For more information about immutability, see [Immutability](#).

NOTE

If you do not want to use immutability, make sure that *Versioning* is not enabled for the Microsoft Azure Blob storage account that you want to use.

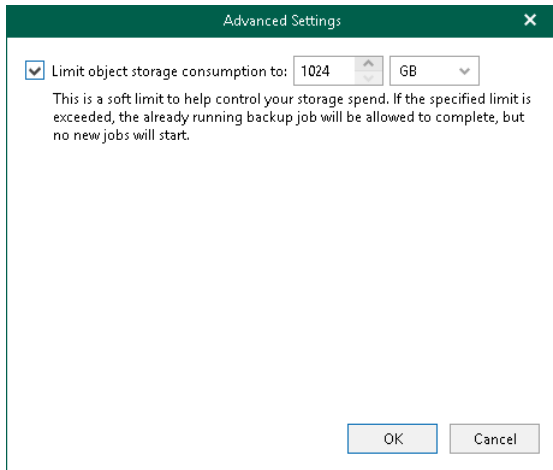
4. Click **Advanced** if you want to configure storage consumption limitations.



4. In the **Advanced Settings** window, do the following:
 - a. Select the **Limit object storage consumption to** check box and specify the limit value in GB, TB or PB.

If you select this check box, Veeam Backup for Microsoft 365 limits object storage capacity and prohibits running new jobs when the specified value is exceeded.

b. Click **OK**.



Step 7. Configure Azure Archiver Appliance

At this step of the wizard, you can optionally enable usage of the Azure archiver appliance when Veeam Backup for Microsoft 365 transfers backed-up data between different instances of Azure Blob Storage or to Azure Blob Storage Archive. If you use the Azure archiver appliance, it usually speeds up the backup copy process and helps you reduce costs incurred by your cloud storage provider.

The Azure archiver appliance is a small auxiliary machine in Microsoft Azure that is deployed and configured automatically by Veeam Backup for Microsoft 365. Veeam services that Veeam Backup for Microsoft 365 installs on the Azure archiver appliance compress data passed through. This helps reduce network traffic and increase the speed of backup copy.

The process of the Azure archiver appliance deployment takes a couple of minutes. If you enable usage of the Azure archiver appliance, Veeam Backup for Microsoft 365 will create the archiver appliance at the beginning of a backup copy job and remove or reuse it after a backup copy job completes. By default, Veeam Backup for Microsoft 365 always keeps one archiver appliance for reuse.

If you do not want to use the Azure archiver appliance, skip this step and click **Finish**.

NOTE

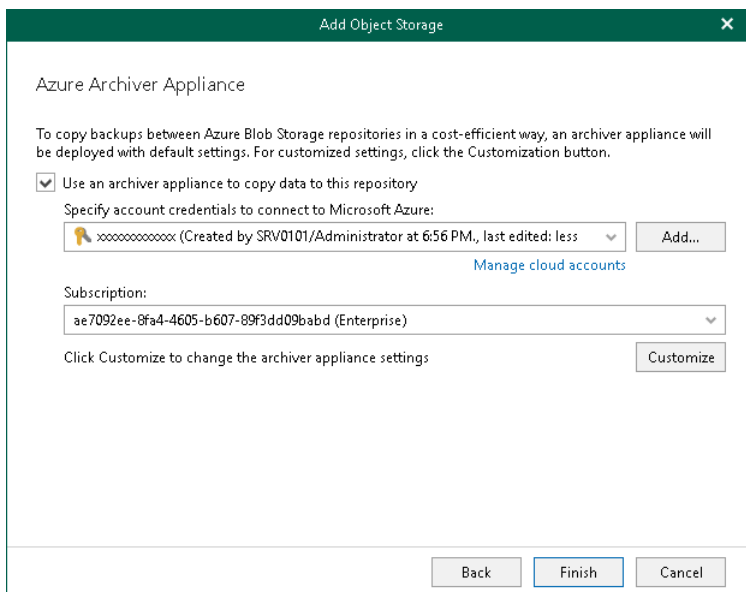
Even if you have enabled usage of the archiver appliance for object storage, Veeam Backup for Microsoft 365 will not create it when transferring backed-up data between object storage of different vendors.

To enable usage of the Azure archiver appliance, do the following:

1. Select the **Use an archiver appliance to copy data to this repository** check box.
2. From the **Specify account credentials to connect to Microsoft Azure** drop-down list, select a service account credentials to access Microsoft Azure.

If you already have a credentials record that was configured beforehand, select such a record from the drop-down list. Otherwise, click **Add** and configure a new Azure service account using the **Add Azure Service Account** wizard. For more information, see [Adding Microsoft Azure Service Account](#). You can also click **Manage cloud accounts** to [manage existing credentials records](#).

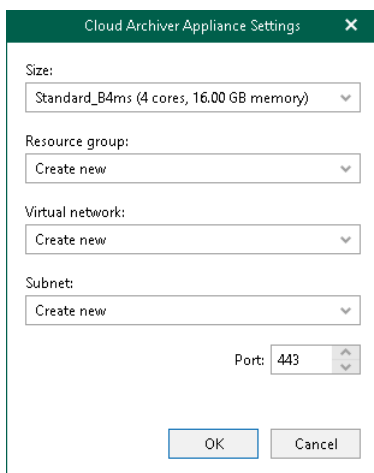
3. From the **Subscription** drop-down list, select Microsoft Azure subscription.
4. Click **Customize** if you want to change the default settings of the archiver appliance.



The screenshot shows a window titled "Add Object Storage" with a close button (X) in the top right corner. The main heading is "Azure Archiver Appliance". Below the heading, there is a paragraph: "To copy backups between Azure Blob Storage repositories in a cost-efficient way, an archiver appliance will be deployed with default settings. For customized settings, click the Customization button." Below this paragraph, there is a checked checkbox labeled "Use an archiver appliance to copy data to this repository". Underneath the checkbox, there is a label "Specify account credentials to connect to Microsoft Azure:" followed by a dropdown menu showing a service account name and an "Add..." button. Below the dropdown menu, there is a link "Manage cloud accounts". Below the link, there is a label "Subscription:" followed by a dropdown menu showing a subscription ID and name. Below the dropdown menu, there is a label "Click Customize to change the archiver appliance settings" followed by a "Customize" button. At the bottom of the window, there are three buttons: "Back", "Finish", and "Cancel".

5. In the **Cloud Archiver Appliance Settings** window, do the following:
 - a. From the **Size** drop-down list, select the size of the appliance.
 - b. From the **Resource group** drop-down list, select a resource group that will be associated with the archiver appliance.

Keep in mind that the resource group must allow inbound and outbound traffic through the listed [ports](#).
 - c. From the **Virtual network** drop-down list, select a network to which the archiver appliance must be connected.
 - d. From the **Subnet** drop-down list, select the subnet for the archiver appliance.
 - e. Specify the port that Veeam Backup for Microsoft 365 will use to route requests between the archiver appliance and backup infrastructure components.
 - f. Click **OK**.



The screenshot shows a dialog box titled "Cloud Archiver Appliance Settings". It contains the following fields and controls:

- Size:** A dropdown menu with the selected option "Standard_B4ms (4 cores, 16.00 GB memory)".
- Resource group:** A dropdown menu with the selected option "Create new".
- Virtual network:** A dropdown menu with the selected option "Create new".
- Subnet:** A dropdown menu with the selected option "Create new".
- Port:** A spinner control set to the value "443".
- Buttons:** "OK" and "Cancel" buttons at the bottom.

Adding IBM Cloud Object Storage

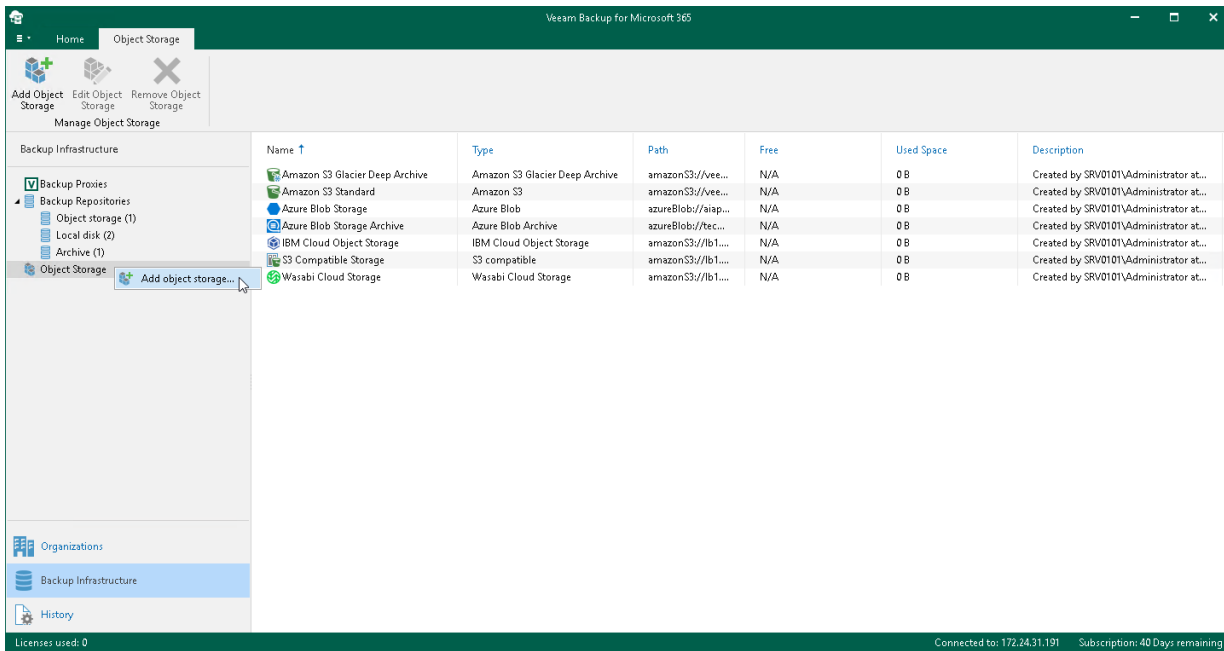
To add a new IBM Cloud object storage to the Veeam Backup for Microsoft 365 backup infrastructure, do the following:

1. [Launch the Add Object Storage wizard.](#)
2. [Specify object storage name.](#)
3. [Select object storage type.](#)
4. [Specify object storage service point and account.](#)
5. [Specify object storage bucket.](#)

Step 1. Launch Add Object Storage Wizard

To launch the **Add Object Storage** wizard, do the following:

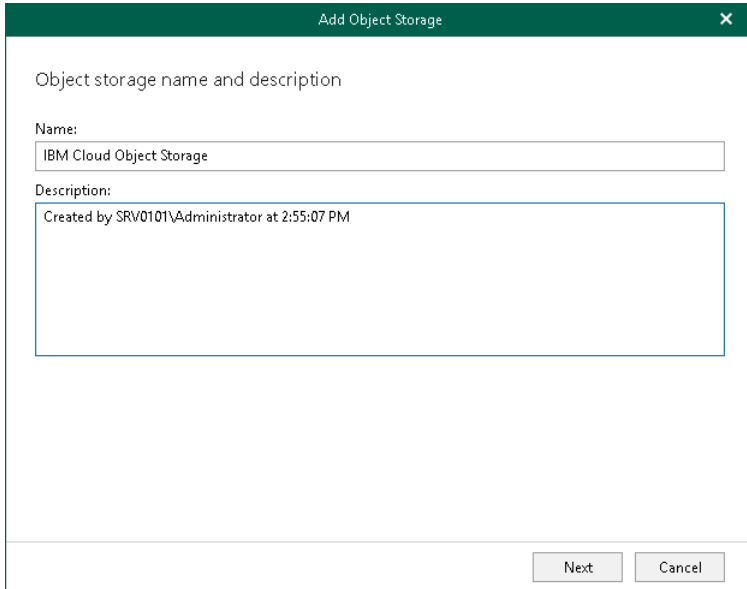
1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Object Storage** node.
3. Do one of the following:
 - On the **Object Storage** tab, click **Add Object Storage** on the ribbon.
 - Right-click the **Object Storage** node and select **Add object storage**.



Step 2. Specify Object Storage Name

At this step of the wizard, enter a name for object storage and provide optional description:

1. In the **Name** field, enter a name for object storage.
2. In the **Description** field, enter optional description.



Object storage name and description

Name:
IBM Cloud Object Storage

Description:
Created by SRV0101\Administrator at 2:55:07 PM

Next Cancel

Step 3. Select Object Storage Type

At this step of the wizard, select **IBM Cloud Object Storage**.

Object storage type

- S3 Compatible**
Adds a cloud object storage provider, or an on-premises object storage system.
- Amazon S3**
Adds Amazon S3 storage. Standard, Infrequent Access (IA), S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval and S3 Glacier Deep Archive are supported.
- Microsoft Azure Blob Storage**
Adds Microsoft Azure cloud object storage. Microsoft Azure Blob Storage and Microsoft Azure Archive Storage are supported.
- IBM Cloud Object Storage**
Adds IBM Cloud object storage. S3 compatible versions of both on-premises and IBM Cloud storage offerings are supported.
- Wasabi Cloud Storage**
Adds Wasabi cloud object storage.

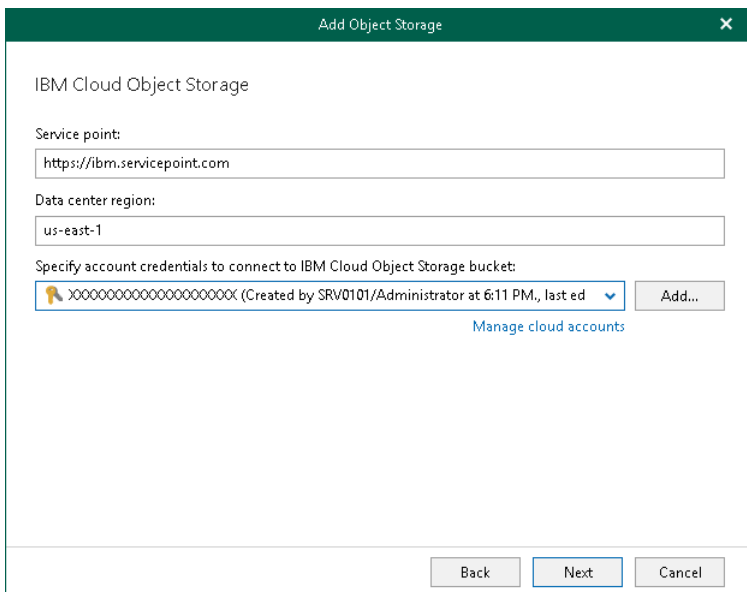
Back Next Cancel

Step 4. Specify Object Storage Service Point and Account

At this step of the wizard, specify a service point of your IBM Cloud object storage, select a datacenter region and specify account credentials.

1. In the **Service point** field, specify an endpoint address of your IBM Cloud object storage.
2. In the **Data center region** field, specify a region.
3. From the **Specify account credentials to connect to IBM Cloud Object Storage bucket** drop-down list, select user credentials to access your IBM Cloud object storage.

If you already have a credentials record that was configured beforehand, select such a record from the drop-down list. Otherwise, click **Add** and provide your access and secret keys. For more information, see [Adding S3 Compatible, IBM Cloud and Wasabi Cloud Storage Access Key](#). You can also click **Manage cloud accounts** to [manage existing credentials records](#).



The screenshot shows a window titled "Add Object Storage" with a close button (X) in the top right corner. The window content is as follows:

- IBM Cloud Object Storage**
- Service point:** A text input field containing "https://ibm.servicepoint.com".
- Data center region:** A text input field containing "us-east-1".
- Specify account credentials to connect to IBM Cloud Object Storage bucket:** A dropdown menu showing a red key icon, a masked string "XXXXXXXXXXXXXXXXXXXX", and the text "(Created by SRV0101/Administrator at 6:11 PM., last ed)". To the right of the dropdown is an "Add..." button.
- Below the dropdown is a blue link: [Manage cloud accounts](#).
- At the bottom of the window are three buttons: "Back", "Next", and "Cancel".

Step 5. Specify Object Storage Bucket

At this step of the wizard, specify object storage bucket and folder where you want to save your data.

1. From the **Bucket** drop-down list, select a bucket.

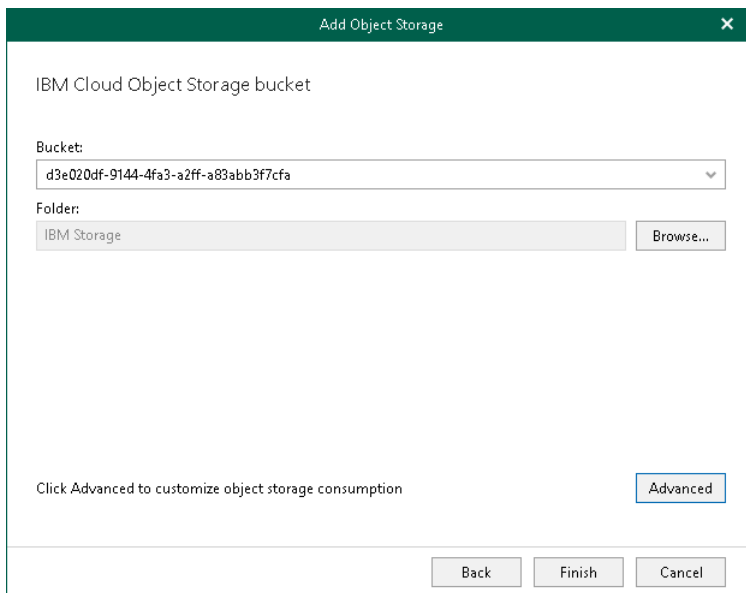
Make sure that the bucket you want to use to store your data was created in advance; Veeam Backup for Microsoft 365 does not support creating new buckets.

2. In the **Folder** field, select a folder to which you want to map your object storage, and which will be used to store offloaded data.

To select a folder, click **Browse** and either select an existing folder or create a new one by clicking **New Folder**.

For more information on how data is stored, see [Object Storage Structure](#).

3. Click **Advanced** if you want to configure storage consumption limitations.

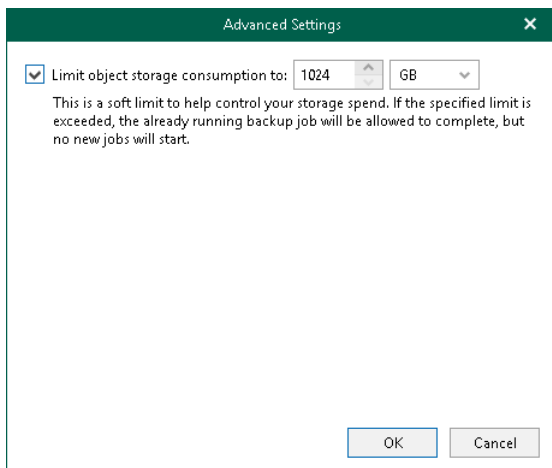


4. In the **Advanced Settings** window, do the following:

- a. Select the **Limit object storage consumption to** check box and specify the limit value in GB, TB or PB.

If you select this check box, Veeam Backup for Microsoft 365 limits object storage capacity and prohibits running new jobs when the specified value is exceeded.

- b. Click **OK**.



Adding Wasabi Cloud Object Storage

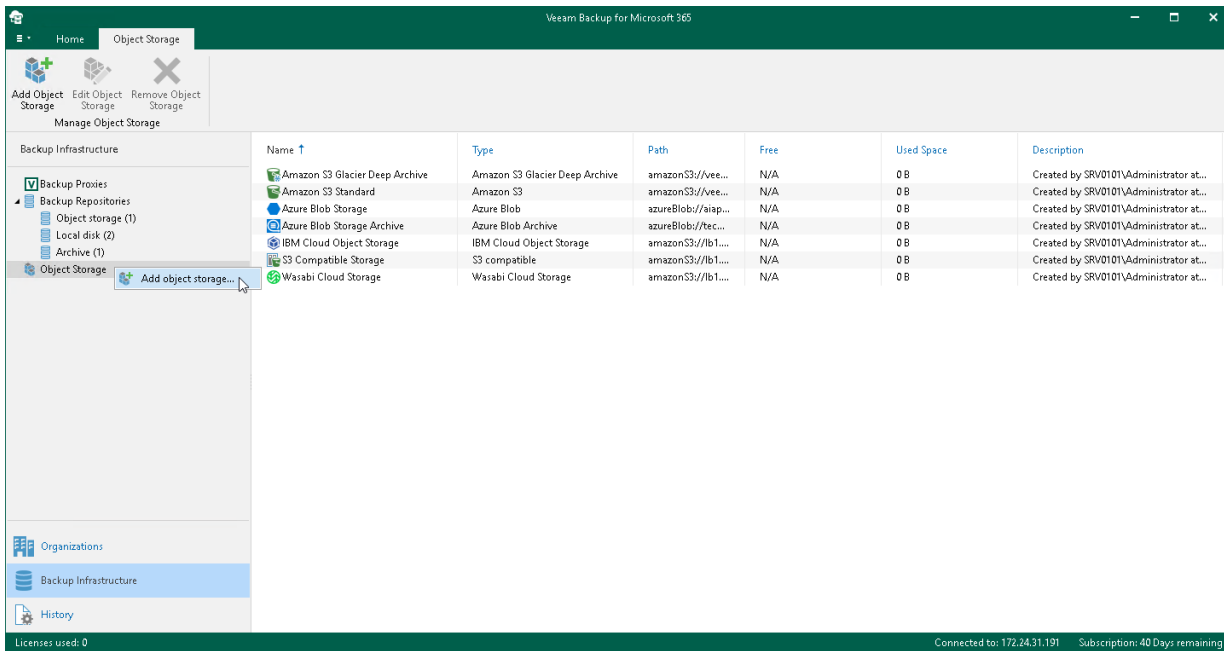
To add a new Wasabi Cloud object storage to the Veeam Backup for Microsoft 365 backup infrastructure, do the following:

1. [Launch the Add Object Storage wizard.](#)
2. [Specify object storage name.](#)
3. [Select object storage type.](#)
4. [Specify object storage service point and account.](#)
5. [Specify object storage bucket.](#)

Step 1. Launch Add Object Storage Wizard

To launch the **Add Object Storage** wizard, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Object Storage** node.
3. Do one of the following:
 - On the **Object Storage** tab, click **Add Object Storage** on the ribbon.
 - Right-click the **Object Storage** node and select **Add object storage**.



Step 2. Specify Object Storage Name

At this step of the wizard, enter a name for object storage and provide optional description:

1. In the **Name** field, enter a name for object storage.
2. In the **Description** field, enter optional description.

The screenshot shows a dialog box titled "Add Object Storage" with a close button (X) in the top right corner. The main content area is titled "Object storage name and description". It contains two input fields: "Name:" with the text "Wasabi Cloud Storage" and "Description:" with the text "Created by SRV0101\Administrator at 3:05:44 PM". At the bottom right, there are "Next" and "Cancel" buttons.

Step 3. Select Object Storage Type

At this step of the wizard, select **Wasabi Cloud storage**.

Object storage type

- S3 Compatible**
Adds a cloud object storage provider, or an on-premises object storage system.
- Amazon S3**
Adds Amazon S3 storage. Standard, Infrequent Access (IA), S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval and S3 Glacier Deep Archive are supported.
- Microsoft Azure Blob Storage**
Adds Microsoft Azure cloud object storage. Microsoft Azure Blob Storage and Microsoft Azure Archive Storage are supported.
- IBM Cloud Object Storage**
Adds IBM Cloud object storage. S3 compatible versions of both on-premises and IBM Cloud storage offerings are supported.
- Wasabi Cloud Storage**
Adds Wasabi cloud object storage.

Back Next Cancel

Step 4. Specify Object Storage Service Point and Account

At this step of the wizard, specify a service point of your Wasabi Cloud object storage, select a datacenter region and specify account credentials.

1. In the **Service point** field, specify an endpoint address of your Wasabi Cloud object storage.
2. In the **Data center region** field, specify a region.
3. From the **Specify account credentials to connect to Wasabi Cloud Object Storage bucket** drop-down list, select user credentials to access your Wasabi Cloud object storage.

If you already have a credentials record that was configured beforehand, select such a record from the drop-down list. Otherwise, click **Add** and provide your access and secret keys. For more information, see [Adding S3 Compatible, IBM Cloud and Wasabi Cloud Storage Access Key](#). You can also click **Manage cloud accounts** to [manage existing credentials records](#).

Wasabi Cloud Object Storage

Service point:

Data center region:

Specify account credentials to connect to Wasabi Cloud Object Storage bucket:

[Manage cloud accounts](#)

Step 5. Specify Object Storage Bucket

At this step of the wizard, specify object storage bucket and folder where you want to save your data.

1. From the **Bucket** drop-down list, select a bucket.

Make sure that the bucket you want to use to store your data was created in advance; Veeam Backup for Microsoft 365 does not support creating new buckets.

2. In the **Folder** field, select a folder to which you want to map your object storage, and which will be used to store offloaded data.

To select a folder, click **Browse** and either select an existing folder or create a new one by clicking **New Folder**.

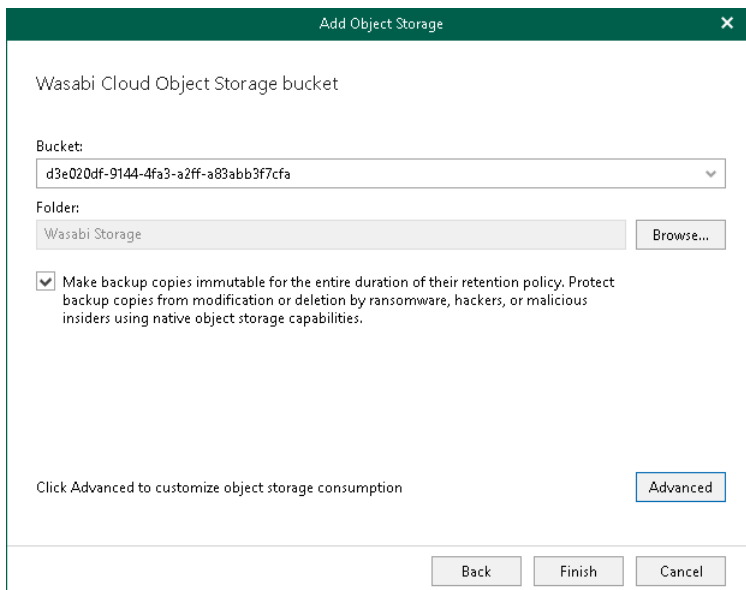
For more information on how data is stored, see [Object Storage Structure](#).

3. Select the **Make backup copies immutable for the entire duration of their retention policy** check box to enable protection of backup copies against accidental data deletions, malware activity and modifications that may be performed by 3rd party applications. For more information about immutability, see [Immutability](#).

NOTE

If you do not want to use immutability, make sure that *Versioning* is not enabled for the bucket in which you want to save your data.

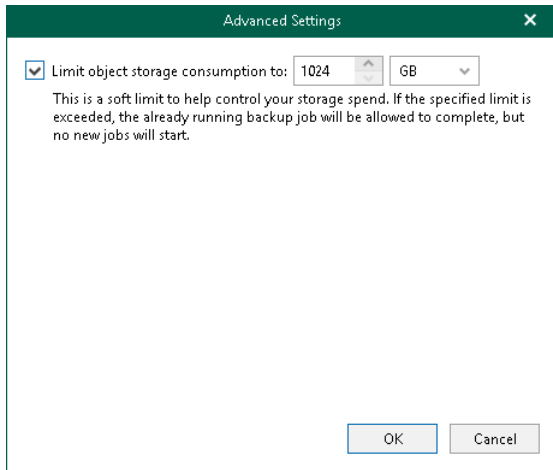
4. Click **Advanced** if you want to configure storage consumption limitations.



4. In the **Advanced Settings** window, do the following:
 - a. Select the **Limit object storage consumption to** check box and specify the limit value in GB, TB or PB.

If you select this check box, Veeam Backup for Microsoft 365 limits object storage capacity and prohibits running new jobs when the specified value is exceeded.

b. Click **OK**.



Editing Object Storage Settings

Veeam Backup for Microsoft 365 allows you to edit object storage settings.

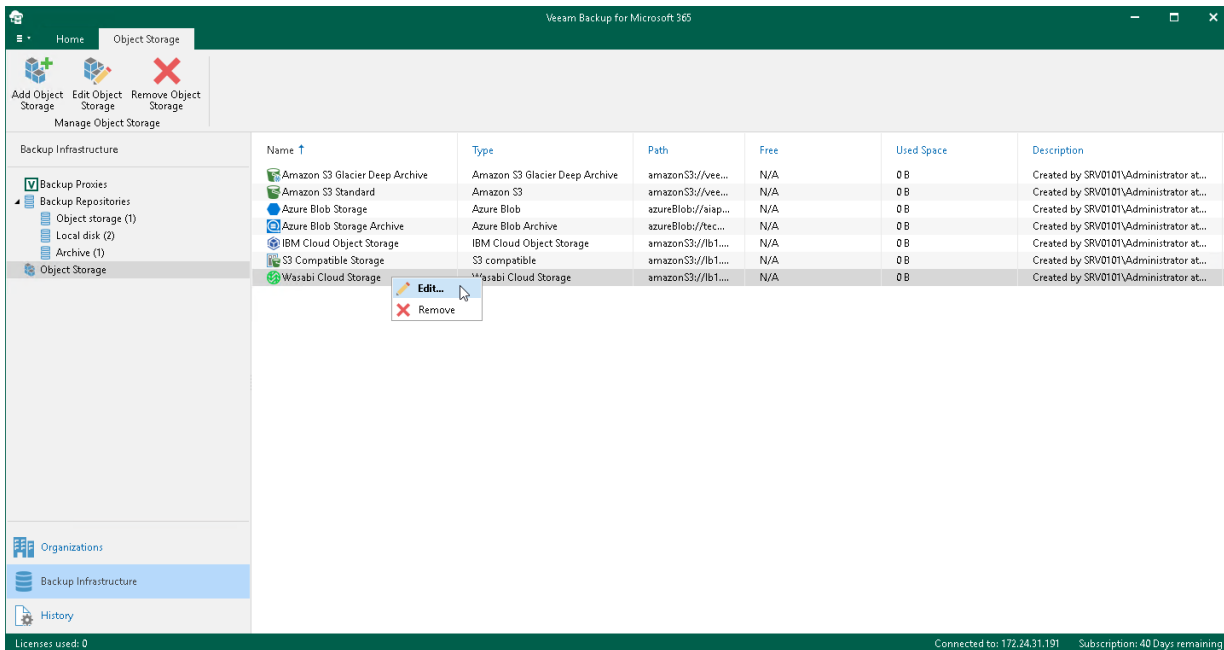
To edit object storage settings, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Object Storage** node.
3. In the preview pane, do one of the following:
 - Select object storage and click **Edit Object Storage** on the ribbon.
 - Right-click object storage and select **Edit**.
4. Modify the required settings.

You can change the following parameters:

- The name and description of object storage.
- Its capacity to prohibit running new jobs when the specified value is exceeded.

- For Microsoft Azure Blob and Amazon S3 object storage, you can enable or disable usage of the archiver appliance.



Removing Object Storage

Veeam Backup for Microsoft 365 allows you to remove object storage from the backup infrastructure if you no longer need them.

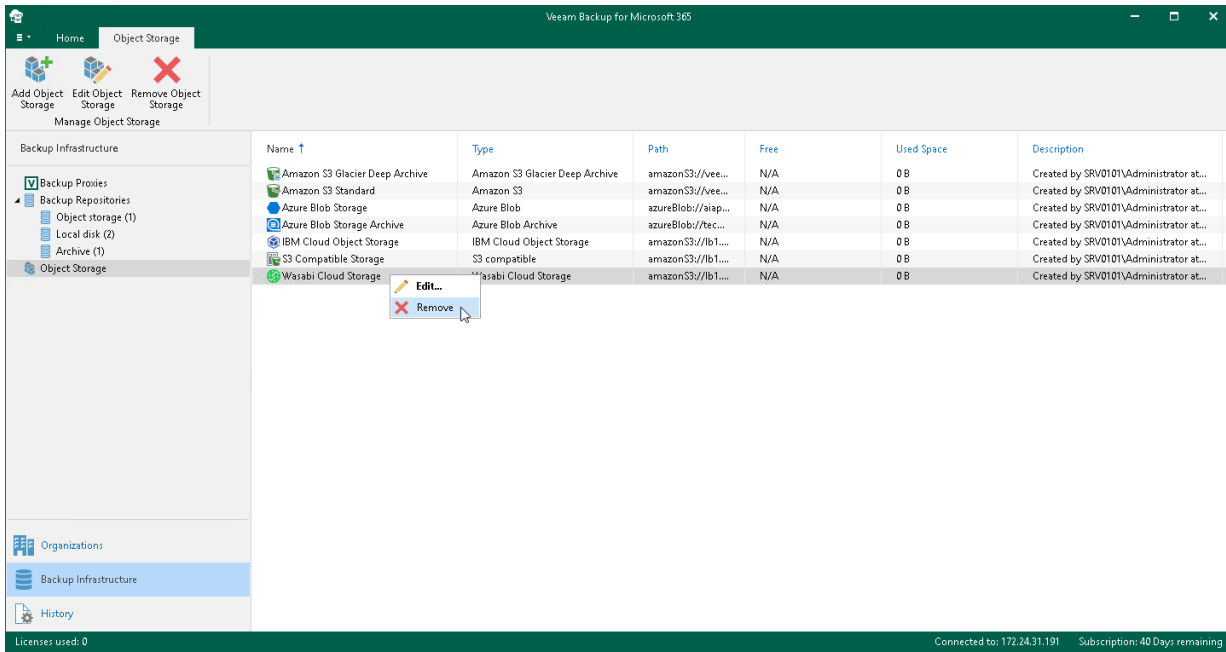
Consider the following:

- You cannot remove object storage that is in use by an extended backup repository. To remove such object storage, remove an **extended** backup repository and then remove object storage. For more information on how to remove a backup repository, see [Removing Backup Repositories](#).
- When removing object storage from the Veeam Backup for Microsoft 365 infrastructure, the backup data will not be removed from this storage.

To remove object storage from the Veeam Backup for Microsoft 365 backup infrastructure, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Object Storage** node.
3. In the preview pane, do one of the following:
 - Select object storage and click **Remove Object Storage** on the ribbon.

- Right-click object storage and select **Remove**.



Credentials

In Veeam Backup for Microsoft 365, you can use the following types of credentials:

- [Cloud credentials](#)

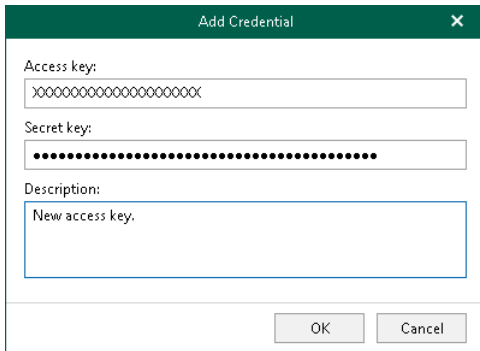
You can use this type of credentials to work with [object storage](#).

- [Encryption passwords](#)

You can use this type of credentials to [encrypt data](#) in object storage.

Both cloud credentials and encryption passwords are stored in Veeam Backup for Microsoft 365 and encrypted using the Data Protection API (DPAPI) mechanisms. For more information, see [this Microsoft article](#).

4. In the **Secret key** field, enter your secret key.
5. In the **Description** field, enter optional description.
6. Click **OK**.

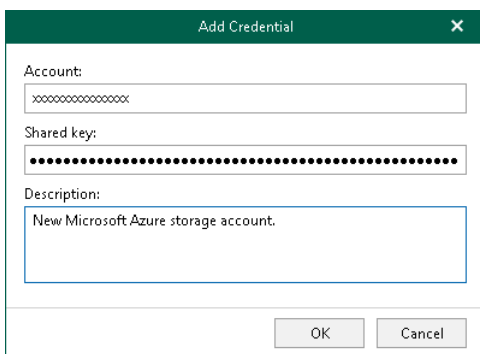


Adding Microsoft Azure Blob Storage Account

You can add new credentials for [Microsoft Azure Blob storage](#).

To add credentials, do the following:

1. In the main menu, click **Manage Cloud Credentials**.
2. In the **Cloud Credential Manager** window, click **Add > Microsoft Azure storage account**.
3. In the **Account** field, enter your storage account name.
4. In the **Shared key** field, enter your shared key.
5. In the **Description** field, enter optional description.
6. Click **OK**.



Adding Microsoft Azure Service Account

You can add new credentials to use the [Azure archiver appliance](#).

To add a new Microsoft Azure service account, do the following:

1. [Launch the Add Azure Service Account wizard](#).
2. [Configure connection to Microsoft Azure](#).
3. [Register or select Azure AD Application](#).

4. [Log in to Microsoft 365.](#)
5. [Select Microsoft Azure subscription.](#)

Step 1. Launch Add Azure Service Account Wizard

To launch the **Add Azure Service Account** wizard, do the following:

1. In the main menu, click **Manage Cloud Credentials**.
2. In the **Cloud Credential Manager** window, click **Add > Microsoft Azure service account**.

Step 2. Configure Connection to Microsoft Azure

At this step of the wizard, select a Microsoft Azure region and choose whether you want to register a new [Azure AD application](#) to connect to Microsoft Azure or use an existing Azure AD application.

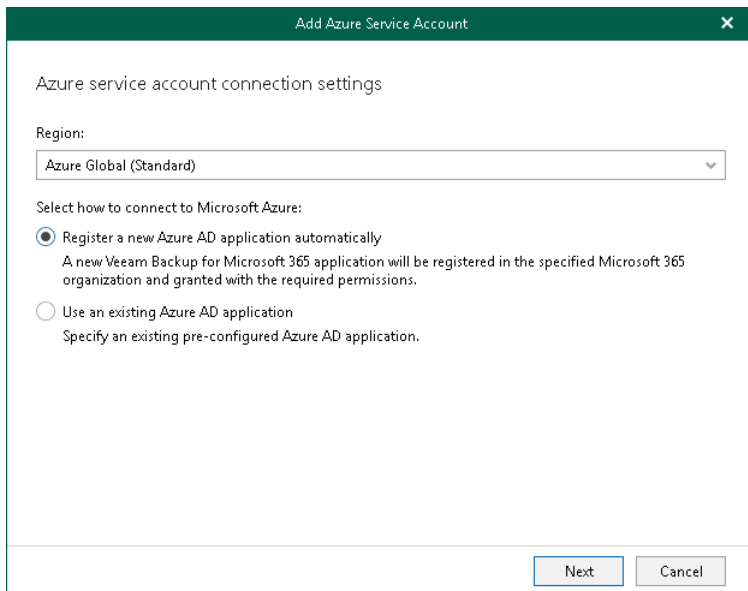
To select a region and connection method, do the following:

1. From the **Region** drop-down list, select a Microsoft Azure region.
2. Select one of the following options:
 - **Register a new Azure AD application automatically**

With this option selected, Veeam Backup for Microsoft 365 requires to provide an application name and certificate to register a new Azure AD application in Microsoft Entra ID (formerly Azure Active Directory). For more information, see [Registering New Azure AD Application](#).

- **Use an existing Azure AD application**

With this option selected, Veeam Backup for Microsoft 365 requires to provide connection parameters to the existing Azure AD application. For more information, see [Using Existing Azure AD Application](#).



The screenshot shows a dialog box titled "Add Azure Service Account" with a close button (X) in the top right corner. The main content area is titled "Azure service account connection settings". Below this title, there is a "Region:" label followed by a dropdown menu currently displaying "Azure Global (Standard)". Underneath, the text "Select how to connect to Microsoft Azure:" is followed by two radio button options. The first option, "Register a new Azure AD application automatically", is selected and includes the subtext: "A new Veeam Backup for Microsoft 365 application will be registered in the specified Microsoft 365 organization and granted with the required permissions." The second option, "Use an existing Azure AD application", is unselected and includes the subtext: "Specify an existing pre-configured Azure AD application." At the bottom right of the dialog, there are two buttons: "Next" and "Cancel".

Step 3. Register or Select Azure AD Application

At this step of the wizard, you can create a new application in Microsoft Entra ID (formerly Azure Active Directory) or select an existing one.

- [Registering a new application](#)

Use this method if you have selected the **Register a new Azure AD application automatically** option at the previous step of the wizard.

- [Using an existing application](#)

Use this method if you have selected the **Use an existing Azure AD application** option at the previous step of the wizard.

Registering New Azure AD Application

You can register a new Azure AD application in Microsoft Entra ID (formerly Azure Active Directory). Veeam Backup for Microsoft 365 will use this application for data exchange when transferring backed-up data between different instances of Azure Blob Storage or to Azure Blob Storage Archive during backup copy jobs.

When registering a new Azure AD application, Veeam Backup for Microsoft 365 automatically grants the [required permissions](#) to this application.

To register a new Azure AD application, do the following:

1. In the **Name** field, enter a name that you want to use to register a new Azure AD application in your Microsoft Entra ID (formerly Azure Active Directory).
2. Click **Install** to specify an SSL certificate that you want to use for data exchange between Veeam Backup for Microsoft 365 and an Azure AD application.
3. In the **Select Certificate** wizard, select a certificate. For more information, see [Installing SSL Certificates](#).

You can generate a new self-signed certificate or use an existing one. Before using an existing certificate, make sure to register this certificate in Microsoft Entra ID (formerly Azure Active Directory). For more information, see [this Microsoft article](#). When generating a new self-signed certificate, Veeam Backup for Microsoft 365 will register it automatically.

4. In the **Specify Azure service account description** field, enter optional description.

The screenshot shows a dialog box titled "Add Azure Service Account" with a close button (X) in the top right corner. The dialog is titled "Azure AD application registration". It contains the following fields and controls:

- Name:** A text input field containing "Azure Service Account".
- Certificate to authenticate with Azure AD:** A text input field containing the certificate ID "54E969ABACD550DE2E5F3804AC2F0E61C9B003CE". To the right of this field is an "Install..." button.
- Specify Azure service account description:** A text input field containing the text "Created by SRV0101/Administrator at 6:56 PM.".

At the bottom of the dialog, there are three buttons: "Back", "Next", and "Cancel".

Using Existing Azure AD Application

You can specify an existing Azure AD application in your Microsoft Entra ID (formerly Azure Active Directory). Veeam Backup for Microsoft 365 will use this application for data exchange when transferring backed-up data between different instances of Azure Blob Storage or to Azure Blob Storage Archive during backup copy jobs.

To use an existing application, do the following:

1. In the **Tenant ID** field, specify Microsoft Entra ID (formerly Azure Active Directory) tenant ID.
2. In the **Application ID** field, specify an identification number of your Azure AD application.

You can find this number in an application settings in your Microsoft Entra ID (formerly Azure Active Directory). For more information, see [this Microsoft article](#).

3. Select an Azure AD application authentication type. You can select either **Application secret** or **Application certificate**:

- a. To use a certificate, select the **Application certificate** option and click **Install**. For more information, see [Installing SSL Certificates](#).

Keep in mind that you must upload a certificate file to the Azure portal beforehand. For more information, see [this Microsoft article](#).

- b. To use a secret key, select the **Application secret** option and enter a secret key in the field nearby to access your custom application.

To obtain a secret key, you will need to generate it first. For more information on how to generate a secret key, see [this Microsoft article](#).

Keep in mind that a key will become hidden once you leave or refresh the page in the Azure portal. Consider saving the key to a secure location.

4. Select the **Grant this application required permissions and register its certificate in Azure AD** check box to automatically grant [required permissions](#) to Azure AD application.

Veeam Backup for Microsoft 365 will also register the specified certificate in your Microsoft Entra ID (formerly Azure Active Directory).

Keep in mind that you do not need to select this check box if you have granted the required permissions to the specified Azure AD application beforehand and already registered its certificate in Microsoft Entra ID (formerly Azure Active Directory). If the **Grant this application required permissions and register its certificate in Azure AD** check box is not selected, Veeam Backup for Microsoft 365 skips the [Log in to Microsoft 365](#) and [Select Microsoft Azure Subscription](#) steps and finishes the wizard.

5. In the **Specify Azure service account description** field, enter optional description.

4468fde5-48b8-4f24-b3f0-ce8a40xxxx

e7268d27-0165-4778-9db6-5cfcb80a7636

54E969ABACD550DE2E5F3804AC2F0E61C9B003CE

Application secret:

Grant this application required permissions and register its certificate in Azure AD.

Specify Azure service account description:
Created by SRV0101/Administrator at 6:56 PM.

Back Next Cancel

Step 4. Log In to Microsoft 365

At this step of the wizard, log in to your Microsoft 365 organization.

To log in to the Microsoft 365 organization, do the following:

1. Click **Copy code** to copy an authentication code.

Keep in mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.

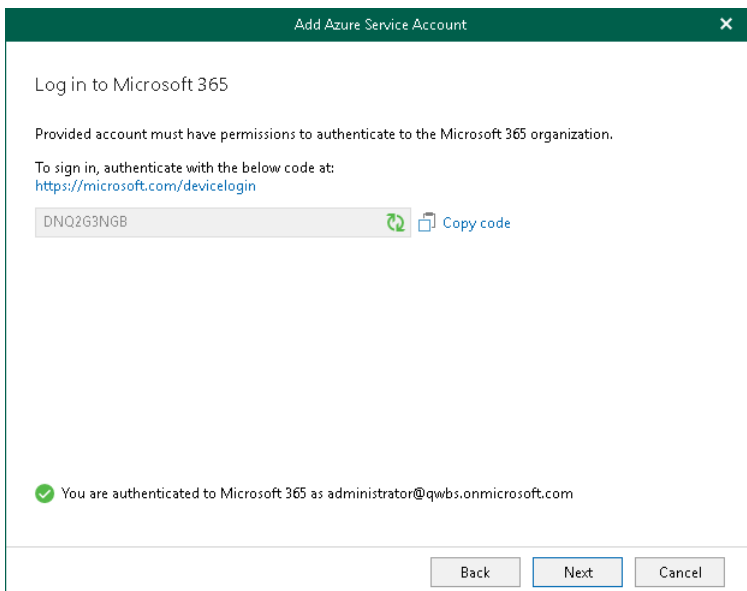
2. Click the Microsoft authentication portal link.

A web browser window opens.

3. On the **Sign in to your account** webpage, paste the code that you have copied and sign in to Microsoft Azure.

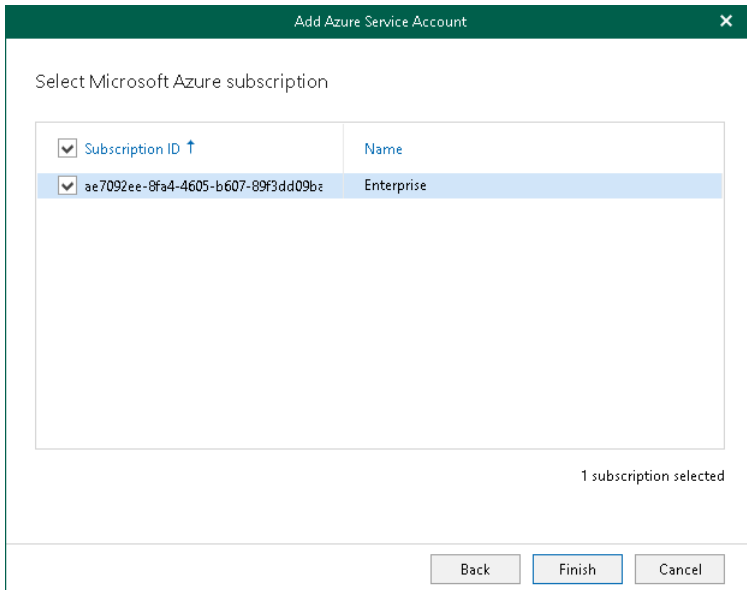
Make sure to sign in with the user account that has the *Global Administrator* role. For more information about this role, see [this Microsoft article](#).

4. Return to the **Add Azure Service Account** wizard and click **Next**.



Step 5. Select Microsoft Azure Subscription

At this step of the wizard, select check boxes next to Microsoft Azure subscriptions in the list. The subscription list contains all subscriptions associated with the user account that you have used to sign in to Microsoft Azure.



The screenshot shows a dialog box titled "Add Azure Service Account" with a close button (X) in the top right corner. The main heading is "Select Microsoft Azure subscription". Below this is a table with two columns: "Subscription ID ↑" and "Name". The first row is selected and highlighted in blue, showing a checkmark in the "Subscription ID" column, the ID "ae7092ee-8fa4-4605-b607-89f3dd09b2", and the name "Enterprise". Below the table, it says "1 subscription selected". At the bottom of the dialog are three buttons: "Back", "Finish" (which is highlighted with a blue border), and "Cancel".

Editing and Removing Cloud Credentials

Veeam Backup for Microsoft 365 allows you to edit and remove cloud credentials that you use to access object storage.

Editing Credentials

To edit credentials, do the following:

1. In the main menu, click **Manage Cloud Credentials**.
2. In the **Cloud Credential Manager** window, select an account and click **Edit**.
3. Modify the selected credentials if needed.

NOTE

When editing Microsoft Azure storage accounts, you can change the shared key only.

Removing Credentials

To remove credentials, do the following:

1. In the main menu, click **Manage Cloud Credentials**.
2. In the **Cloud Credential Manager** window, select an account and click **Remove**.

NOTE

You cannot remove cloud credentials that are in use.

Managing Encryption Passwords

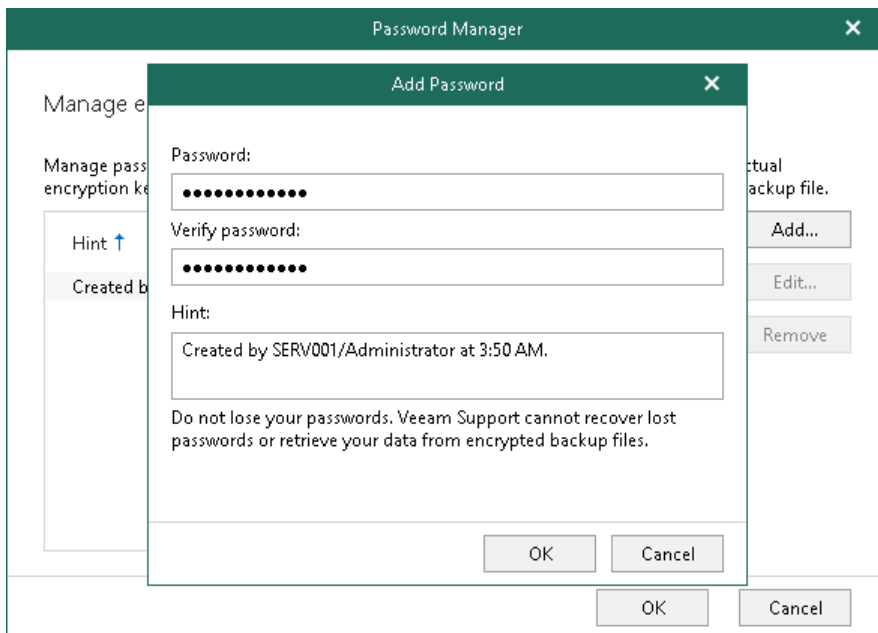
Veeam Backup for Microsoft 365 allows you to configure passwords that you can use to encrypt data in object storage using the 256-bit Advanced Encryption Standard (AES).

To add an encryption password, do the following:

1. In the main menu, click **Manage Passwords**.
2. In the **Password Manager** window, click **Add**.
3. In the **Password** field, enter a new password.
4. In the **Verify password** field, re-enter the password.
5. In the **Hint** field, enter a hint that will help you to remember the password.

IMPORTANT

Make sure to remember your encryption password because, if lost, it cannot be restored.



Editing and Removing Encryption Passwords

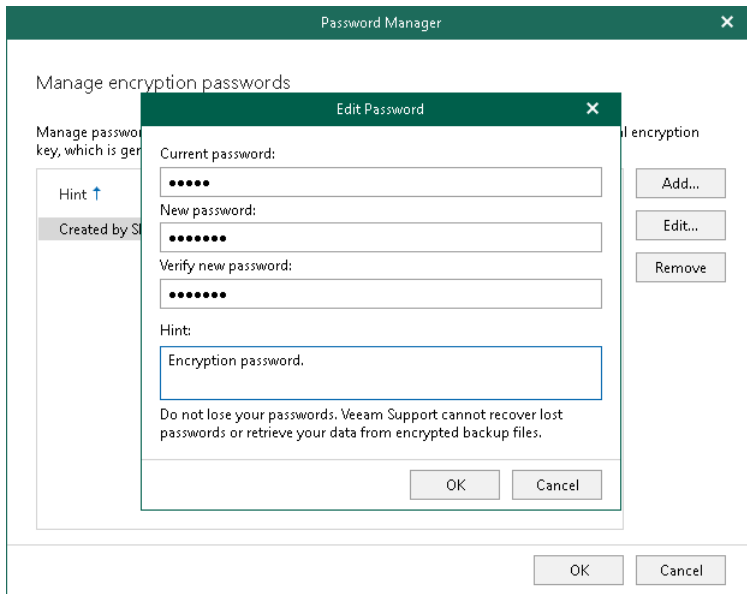
Veeam Backup for Microsoft 365 allows you to edit and remove encryption passwords.

Editing Encryption Passwords

To edit an encryption password, do the following:

1. In the main menu, click **Manage Passwords**.
2. In the **Password Manager** window, select a password and click **Edit**.
3. In the **Current password** field, enter your current password.
4. In the **New password** field, enter a new password.

5. In the **Verify new password** field, re-enter the password.
6. In the **Hint** field, enter a hint that will help you to remember the password.



Removing Encryption Passwords

To remove an encryption password, do the following:

1. In the main menu, click **Manage Passwords**.
2. In the **Password Manager** window, select a password and click **Remove**.

NOTE

You cannot remove passwords that are in use.

Organization Management

You can add the following types of Microsoft organizations to the Veeam Backup for Microsoft 365 environment:

- [Microsoft 365 organizations](#)
- [On-Premises Microsoft organizations](#)
- [Hybrid organizations](#)

To connect to Microsoft 365 and on-premises Microsoft organizations, Veeam Backup for Microsoft 365 uses the following components:

- *Exchange Web Services (EWS)* and *PowerShell* to connect to Microsoft 365 and on-premises Microsoft Exchange organizations.
- *SharePoint Client Object Model (CSOM)* and *Windows Remote Management* to connect to on-premises Microsoft SharePoint organizations.

For more information about Windows Remote Management, see [this Microsoft article](#).

- *Microsoft Graph API* to connect to Microsoft 365 organizations.

Adding Microsoft 365 Organizations

You can add Microsoft 365 organizations to the Veeam Backup for Microsoft 365 infrastructure to back up data of these organizations and quickly restore it back to production servers in case of an unexpected disaster.

When you add Microsoft 365 organizations, you can use the following authentication methods:

- [Modern app-only authentication](#)

When you use this method, Veeam Backup for Microsoft 365 uses only Azure AD application to authenticate to your Microsoft 365 organizations. You cannot use Veeam Backup account with the modern app-only authentication method.

- [Modern authentication with legacy protocols allowed](#)

When you use this method, you can use both Veeam Backup account and Azure AD application to authenticate to your Microsoft 365 organizations. You use MFA-enabled Microsoft 365 user account as Veeam Backup account.

- [Basic authentication](#)

When you use this method, you are required to provide a user account as Veeam Backup account to authenticate to your Microsoft 365 organization.

NOTE

Consider that backup and restore functionality of Veeam Backup for Microsoft 365 differs depending on authentication method that you use. For limitations in Veeam Backup for Microsoft 365 functionality when protecting organizations with modern app-only authentication, see [this Veeam KB article](#).

Adding Microsoft 365 Organizations with Modern App-Only Authentication

When you add an organization using the [modern app-only authentication method](#), you are required to provide [Azure AD application](#) settings. Veeam Backup for Microsoft 365 uses such an application to establish a connection to your Microsoft 365 organizations and maintain data transfer during [backup](#) and [restore](#) sessions.

With modern app-only authentication, you cannot use Veeam Backup account; only communications through Azure AD application is possible.

NOTE

Adding Microsoft 365 organizations using modern app-only authentication is not supported for legacy Microsoft Azure *Germany* region. For limitations in Veeam Backup for Microsoft 365 functionality when protecting organizations with modern app-only authentication, see [this Veeam KB article](#).

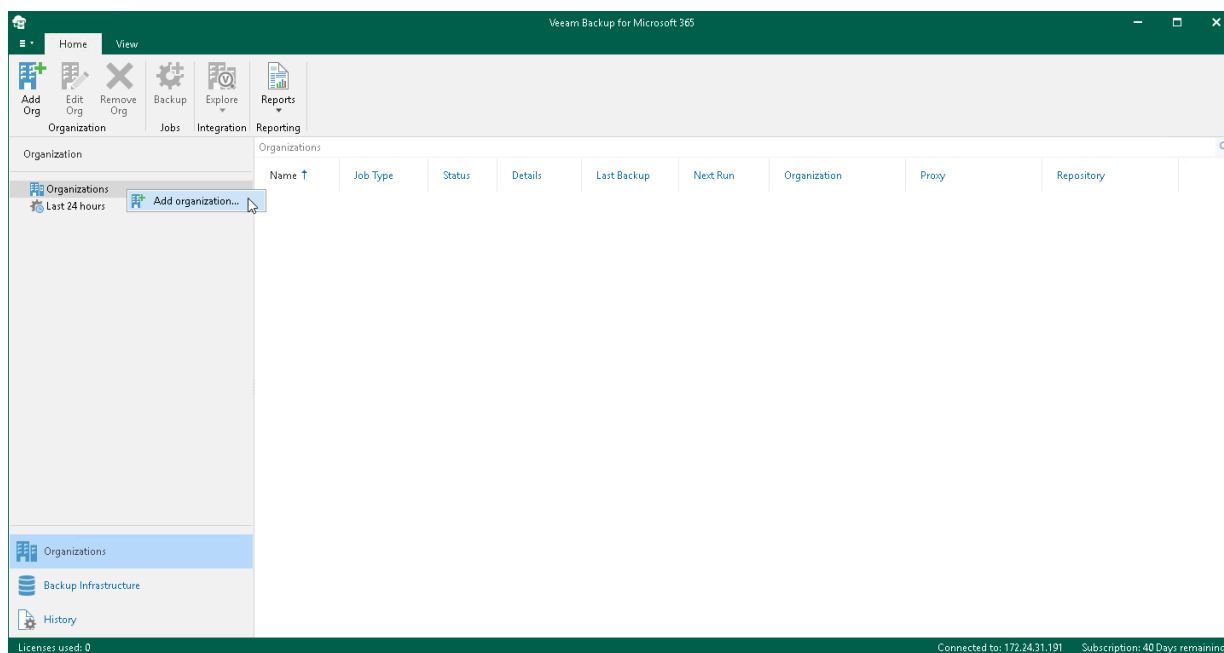
To add a new Microsoft 365 organization to Veeam Backup for Microsoft 365, do the following:

1. [Launch the Add Organization wizard](#).
2. [Select an organization deployment type](#).
3. [Select Azure region and authentication method](#).
4. [Configure connection to Microsoft 365](#).
5. [Register or select Azure AD Application](#).
6. [Log in to Microsoft 365](#).
7. [Finish the wizard](#).

Step 1. Launch Add Organization Wizard

To launch the **Add Organization** wizard, do the following:

1. Open the **Organizations** view.
2. Do one of the following:
 - On the **Home** tab, click **Add Org** on the ribbon.
 - In the inventory pane, right-click the **Organizations** node and select **Add organization**.



Step 2. Select Organization Deployment Type

At this step of the wizard, select a deployment type and Microsoft Online services whose data you want to protect.

NOTE

Veeam Backup for Microsoft 365 can back up Microsoft Teams messages using Microsoft Graph Teams Export APIs. This method substitutes backup of team chats using EWS APIs that will be deprecated by Microsoft. Keep in mind that backup of team chats using Teams Export APIs is limited to backup of public channel posts.

For more information on how to set up Veeam Backup for Microsoft 365 to use Teams Export APIs for team chats backup, see [Getting Started with Teams Export APIs](#).

Depending on whether you enabled usage of Teams Export APIs for team chats backup, Veeam Backup for Microsoft 365 displays different settings at this step of the wizard. You can proceed to one of the following scenarios:

- [Backup of team chats using EWS](#)
Veeam Backup for Microsoft 365 displays these settings if you did not enable usage of Teams Export APIs for team chats backup.
- [Backup of team chats using Teams Export APIs](#)
Veeam Backup for Microsoft 365 displays these settings if you enabled usage of Teams Export APIs for team chats backup.

Backup of Team Chats Using EWS

Veeam Backup for Microsoft 365 displays these settings if you did not enable usage of Teams Export APIs for team chats backup.

NOTE

For more information about team chats backup in Veeam Backup for Microsoft 365, see [Backup of Team Chats Using Teams Export APIs](#).

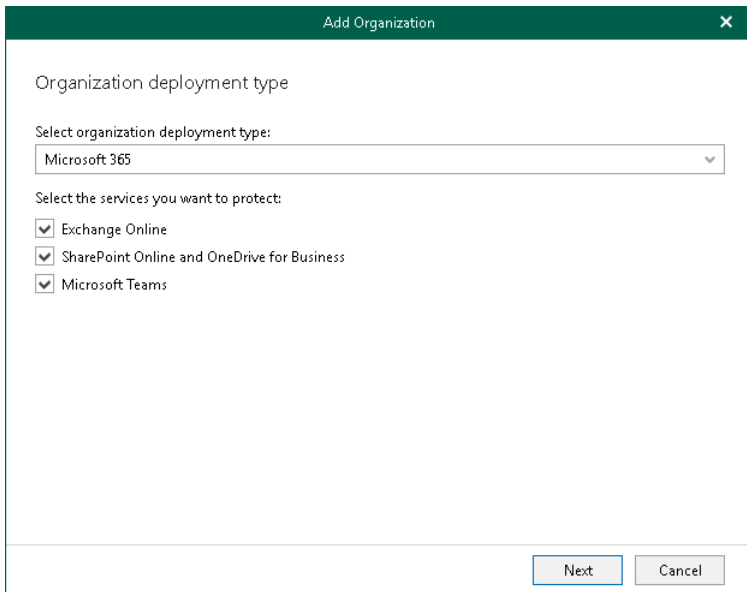
To select an organization deployment type and Microsoft Online services whose data you want to protect, do the following:

1. From the **Select organization deployment type** drop-down list, select *Microsoft 365*.
2. If you want to back up Exchange Online data, select the **Exchange Online** check box.
3. If you want to back up SharePoint Online and OneDrive for Business data, select the **SharePoint Online and OneDrive for Business** check box.
4. If you want to back up Microsoft Teams data, select the **Microsoft Teams** check box.

You can select this check box only if both **Exchange Online** and **SharePoint Online and OneDrive for Business** check boxes are selected.

NOTE

Microsoft Teams service is not supported for organizations in Microsoft Azure *China* and legacy Microsoft Azure *Germany* regions. For more information about Azure Germany, see [this Microsoft article](#).



Organization deployment type

Select organization deployment type:

Microsoft 365

Select the services you want to protect:

- Exchange Online
- SharePoint Online and OneDrive for Business
- Microsoft Teams

Next Cancel

Backup of Team Chats Using Teams Export APIs

Veeam Backup for Microsoft 365 displays these settings if you enabled usage of Teams Export APIs for team chats backup.

To select an organization deployment type and Microsoft Online services whose data you want to protect, do the following:

1. From the **Select organization deployment type** drop-down list, select *Microsoft 365*.
2. If you want to back up Exchange Online data, select the **Exchange Online** check box.
3. If you want to back up SharePoint Online and OneDrive for Business data, select the **SharePoint Online and OneDrive for Business** check box.
4. If you want to back up Microsoft Teams data, select the **Microsoft Teams** check box.

You can select this check box only if both **Exchange Online** and **SharePoint Online and OneDrive for Business** check boxes are selected.

5. If you want to back up team chats using Teams Export APIs, select the **Teams chats** check box.

This check box is available only if the **Microsoft Teams** check box is selected. For more information on how to back up team chats, see [Organization Object Types](#).

NOTE

Consider the following:

- Backup of team chats using Teams Export APIs is limited to backup of public channel posts.
- Microsoft Teams service is not supported for organizations in Microsoft Azure *China* and legacy Microsoft Azure *Germany* regions. For more information about Azure Germany, see [this Microsoft article](#).
- Backup of team chats using Teams Export APIs is not supported for Microsoft organizations in Microsoft Azure *China*, legacy *Germany*, *US Government GCC* and *US Government GCC High* regions.

Add Organization

Organization deployment type

Select organization deployment type:

Microsoft 365

Select the services you want to protect:

- Exchange Online
- SharePoint Online and OneDrive for Business
- Microsoft Teams
 - Teams chats
Teams chats backup requires using protected APIs and additional billing charges from Microsoft. For more information on pricing, see [this Microsoft article](#).

Next Cancel

Step 3. Select Azure Region and Authentication Method

At this step of the wizard, select a region and authentication method.

To select a region and authentication method, do the following:

1. From the **Region** drop-down list, select a Microsoft Azure region your Microsoft 365 organization belongs to.

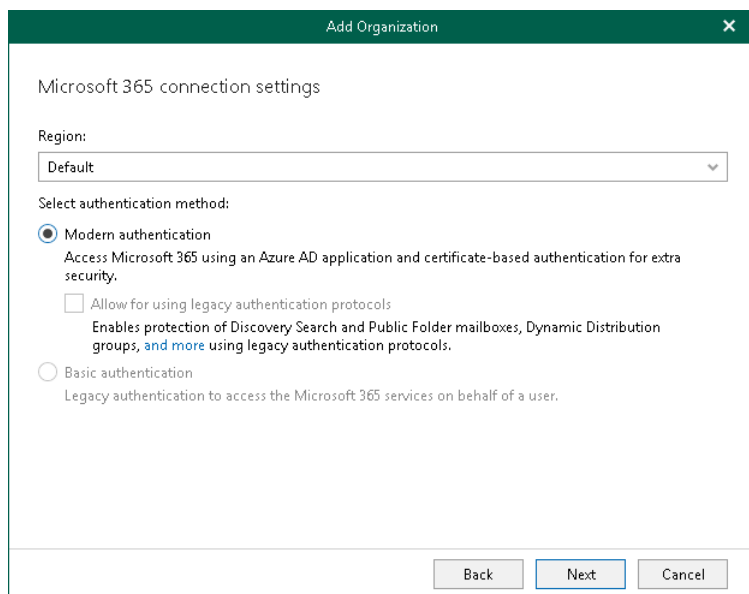
Keep in mind that you cannot select legacy Microsoft Azure *Germany* region for modern app-only authentication.

2. Select the **Modern authentication** option to use Azure AD application to connect to your Microsoft 365 organization.

Make sure to leave the **Allow for using legacy authentication protocols** check box cleared. This check box allows you to add a Microsoft 365 organization using legacy authentication protocols. For more information, see [Adding Microsoft 365 Organizations with Modern Authentication and Legacy Protocols](#).

NOTE

If you selected the **Teams chats** check box at the previous step of the wizard, the **Modern authentication** option is only available.



The screenshot shows a dialog box titled "Add Organization" with a close button (X) in the top right corner. The main content area is titled "Microsoft 365 connection settings". It features a "Region:" label above a dropdown menu currently set to "Default". Below this is the "Select authentication method:" section, which contains three radio button options: "Modern authentication" (selected), "Allow for using legacy authentication protocols" (unchecked), and "Basic authentication" (unchecked). The "Modern authentication" option includes a sub-description: "Access Microsoft 365 using an Azure AD application and certificate-based authentication for extra security." The "Allow for using legacy authentication protocols" option includes a sub-description: "Enables protection of Discovery Search and Public Folder mailboxes, Dynamic Distribution groups, and more using legacy authentication protocols." The "Basic authentication" option includes a sub-description: "Legacy authentication to access the Microsoft 365 services on behalf of a user." At the bottom of the dialog, there are three buttons: "Back", "Next", and "Cancel".

Step 4. Configure Connection to Microsoft 365

At this step of the wizard, choose whether you want to register a new [Azure AD application](#) to connect to your Microsoft 365 organization or use an existing Azure AD application.

Backup of Team Chats Using EWS

You can select one of the following options:

- **Register a new Azure AD application automatically**

With this option selected, Veeam Backup for Microsoft 365 requires to provide an application name and certificate to register a new Azure AD application in Microsoft Entra ID (formerly Azure Active Directory). For more information, see [Registering New Azure AD Application](#).

- **Use an existing Azure AD application**

With this option selected, Veeam Backup for Microsoft 365 requires to provide connection parameters to the existing Azure AD application. For more information, see [Using Existing Azure AD Application](#).

Add Organization

Microsoft 365 connection settings

Select how to connect to the Microsoft 365 organization:

- Register a new Azure AD application automatically
A new Veeam Backup for Microsoft 365 application will be registered in the specified Microsoft 365 organization and granted with the required permissions.
- Use an existing Azure AD application
Use an existing pre-configured Azure AD application.

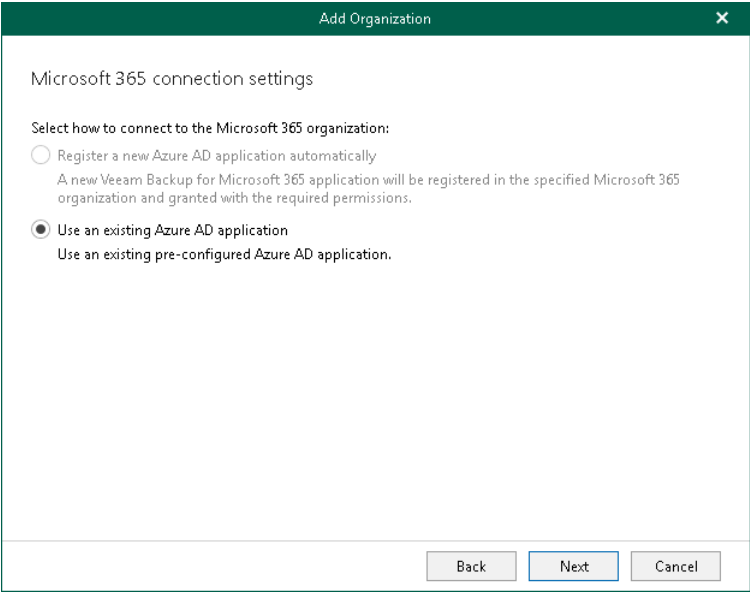
Back Next Cancel

Backup of Team Chats Using Teams Export APIs

NOTE

If you selected the **Teams chats** check box at the [Select Organization Deployment Type](#) step of the wizard, registering a new Azure AD application is unavailable.

You can only select the **Use an existing Azure AD application** option. Veeam Backup for Microsoft 365 requires to provide connection parameters to the existing Azure AD application. For more information, see [Using Existing Azure AD Application](#).



Step 5. Register or Select Azure AD Application

At this step of the wizard, you can create a new application in Microsoft Entra ID (formerly Azure Active Directory) or select an existing one.

- [Registering a new application](#)

Use this method if you have selected the **Register a new Azure AD application automatically** option at the previous step of the wizard.

- [Using an existing application](#)

Use this method if you have selected the **Use an existing Azure AD application** option at the previous step of the wizard.

Registering New Azure AD Application

NOTE

If you selected the **Teams chats** check box at the [Select Organization Deployment Type](#) step of the wizard, registering a new Azure AD application is unavailable.

You can register a new Azure AD application in Microsoft Entra ID (formerly Azure Active Directory). Veeam Backup for Microsoft 365 will use this application for data exchange with your Microsoft 365 organizations during backup and restore sessions.

When registering a new Azure AD application, Veeam Backup for Microsoft 365 automatically grants the [required permissions](#) to this application.

To register a new Azure AD application, do the following:

1. In the **Name** field, enter a name that you want to use to register a new Azure AD application in your Microsoft Entra ID (formerly Azure Active Directory).
2. Click **Install** to specify an SSL certificate that you want to use for data exchange between Veeam Backup for Microsoft 365 and an Azure AD application.
3. In the **Select Certificate** wizard, select a certificate. For more information, see [Installing SSL Certificates](#).

You can generate a new self-signed certificate or use an existing one. Before using an existing certificate, make sure to register this certificate in Microsoft Entra ID (formerly Azure Active Directory). For more information, see [this Microsoft article](#). When generating a new self-signed certificate, Veeam Backup for Microsoft 365 will register it automatically.

4. Select the **Allow this application to enable export mode for SharePoint Web Parts** check box to allow Veeam Backup for Microsoft 365 to back up web parts of your Microsoft SharePoint websites. For more information about web parts, see [this Microsoft article](#).

By default, web parts of Microsoft SharePoint sites that belong to a Microsoft 365 organization with modern app-only authentication have the *allowexport* property set to *false* which prevents Veeam Backup for Microsoft 365 from having a direct access to such web parts.

If this check box is selected, Veeam Backup for Microsoft 365 automatically alters the *allowexport* property of each web part and sets this property to *true*. After the *allowexport* property is set to *true*, a web part can be backed up without any limitations.

Azure AD application registration

Name:

New Azure AD Application

Certificate to authenticate with Azure AD:

1B336E22E231397C8B1CA0F4E0819E070861F1D0

Install...

Specify additional application permissions to process SharePoint Online data:

Allow this application to enable export mode for SharePoint Web Parts. Enabling export mode is required to back up customized content of SharePoint Online sites.

Back Next Cancel

Using Existing Azure AD Application

You can specify an existing Azure AD application in your Microsoft Entra ID (formerly Azure Active Directory). Veeam Backup for Microsoft 365 will use this application for data exchange with your Microsoft 365 organizations during backup and restore sessions.

To use an existing application, do the following:

1. In the **Username** field, enter a user account that you want to use for impersonation. For more information about impersonation, see [this Microsoft article](#).

You can enter any account that belongs to your Microsoft 365 organization using the following format: *name@<domain_name>.<domain>*. For example, *user@abc.com*.

NOTE

If you plan to back up public folder mailboxes, this user account must be granted the *Owner* role and have a valid Exchange Online license and an active mailbox within the Microsoft 365 organization.

Keep in mind that if you select only SharePoint Online and OneDrive for Business services to protect at the [Select Organization Deployment Type](#) step, Veeam Backup for Microsoft 365 displays the **Specify organization name** field instead. In this field, specify a domain name of your Microsoft 365 organization without the user name. For example, *abc.com*.

2. In the **Application ID** field, specify an identification number of Azure AD application that you want to use to access your Microsoft 365 organization.

You can find this number in the application settings of your Microsoft Entra ID (formerly Azure Active Directory). For more information, see [this Microsoft article](#).

3. Click **Install** to specify an SSL certificate that you want to use for data exchange between Veeam Backup for Microsoft 365 and the specified Azure AD application.

4. In the **Select Certificate** wizard, select a certificate. For more information, see [Installing SSL Certificates](#).

You can generate a new self-signed certificate or use an existing one. Before using an existing certificate, make sure to register this certificate in Microsoft Entra ID (formerly Azure Active Directory). For more information, see [this Microsoft article](#). When generating a new self-signed certificate, Veeam Backup for Microsoft 365 will register it automatically.

5. Select the **Grant this application required permissions and register its certificate in Azure AD** check box to automatically grant [required permissions](#) to Azure AD application.

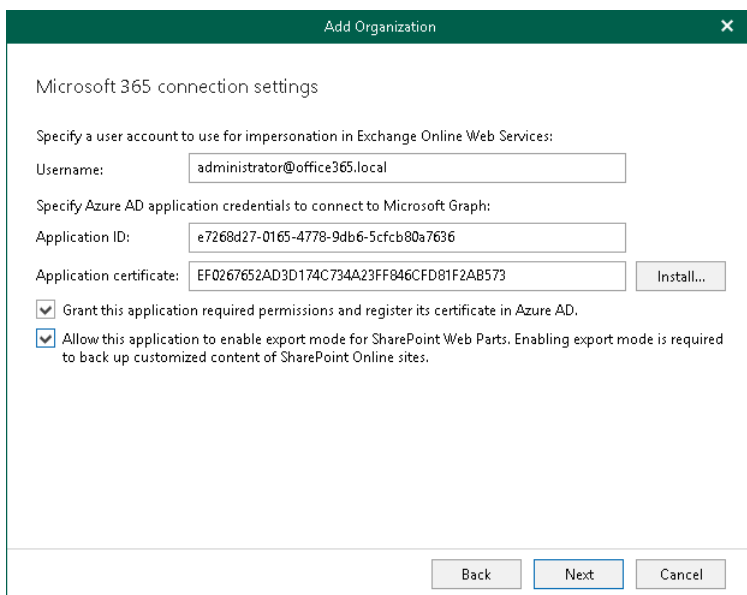
Veeam Backup for Microsoft 365 will also register the specified certificate in your Microsoft Entra ID (formerly Azure Active Directory).

Keep in mind that you do not need to select this check box if you have granted the required permissions to the specified Azure AD application beforehand and already registered its certificate in Microsoft Entra ID (formerly Azure Active Directory). If the **Grant this application required permissions and register its certificate in Azure AD** check box is not selected, Veeam Backup for Microsoft 365 skips the [Log in to Microsoft 365](#) step and proceeds to [Finish Working With Wizard](#).

6. Select the **Allow this application to enable export mode for SharePoint Web Parts** check box to allow Veeam Backup for Microsoft 365 to back up web parts of your Microsoft SharePoint websites. For more information about web parts, see [this Microsoft article](#).

By default, web parts of Microsoft SharePoint sites that belong to a Microsoft 365 organization with modern app-only authentication have the *allowexport* property set to *false* which prevents Veeam Backup for Microsoft 365 from having a direct access to such web parts.

If this check box is selected, Veeam Backup for Microsoft 365 automatically alters the *allowexport* property of each web part and sets this property to *true*. After the *allowexport* property is set to *true*, a web part can be backed up without any limitations.



The screenshot shows a dialog box titled "Add Organization" with a close button (X) in the top right corner. The main heading is "Microsoft 365 connection settings". Below this, there are three sections for configuration:

- Specify a user account to use for impersonation in Exchange Online Web Services:** A text box labeled "Username:" contains the value "administrator@office365.local".
- Specify Azure AD application credentials to connect to Microsoft Graph:** A text box labeled "Application ID:" contains the value "e7268d27-0165-4778-9db6-5cfc80a7636".
- Application certificate:** A text box contains the value "EF0267652AD3D174C734A23FF846CFD81F2AB573". To the right of this text box is an "Install..." button.

At the bottom of the dialog, there are two checked checkboxes:

- Grant this application required permissions and register its certificate in Azure AD.
- Allow this application to enable export mode for SharePoint Web Parts. Enabling export mode is required to back up customized content of SharePoint Online sites.

At the very bottom of the dialog, there are three buttons: "Back", "Next", and "Cancel".

Step 6. Log In to Microsoft 365

At this step of the wizard, log in to your Microsoft 365 organization.

To log in to the Microsoft 365 organization, do the following:

1. Click **Copy code** to copy an authentication code.

Keep in mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.

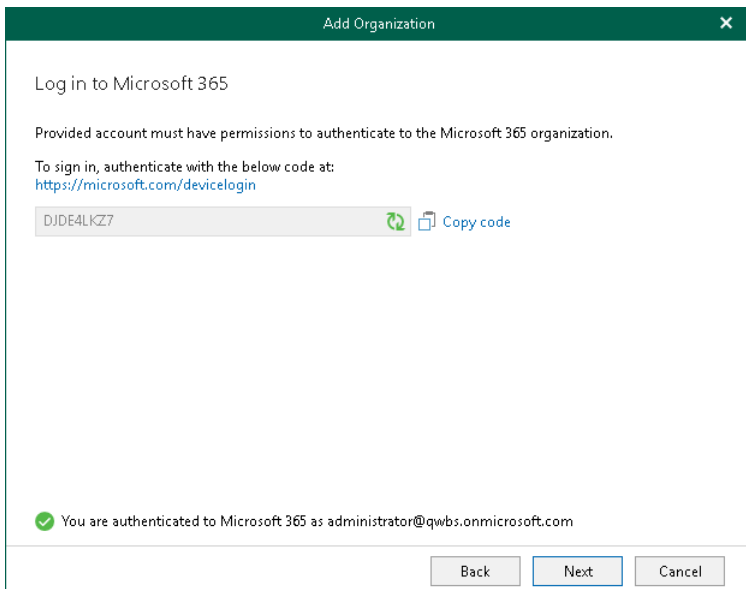
2. Click the Microsoft authentication portal link.

A web browser window opens.

3. On the **Sign in to your account** webpage, paste the code that you have copied and sign in to Microsoft Azure.

Make sure to sign in with the user account that has the *Global Administrator* role. For more information about this role, see [this Microsoft article](#).

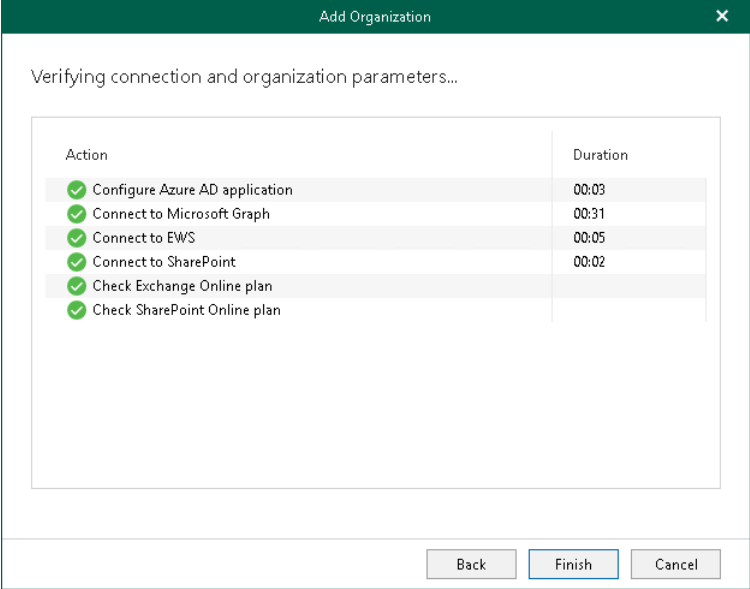
4. Return to the **Add Organization** wizard and click **Next**.



Step 7. Finish Working with Wizard

At this step of the wizard, wait for a connection to be established and click **Finish**.

The Microsoft 365 organization appears under the **Organizations** node in the inventory pane.



Adding Microsoft 365 Organizations with Modern Authentication and Legacy Protocols

When you add an organization using the [modern authentication method](#) with legacy protocols allowed, you use both Veeam Backup account and [Azure AD application](#) for authentication. Veeam Backup for Microsoft 365 uses Veeam Backup account and an application to establish a connection to your Microsoft 365 organizations and maintain data transfer during [backup](#) and [restore](#) sessions.

NOTE

Adding Microsoft 365 organizations using modern authentication method with legacy protocols allowed is not supported for Microsoft Azure *China* region.

To add a new Microsoft 365 organization to Veeam Backup for Microsoft 365, [check prerequisites](#) and do the following:

1. [Launch the Add Organization wizard](#).
2. [Select an organization deployment type](#).
3. [Select Azure region and authentication method](#).
4. [Specify Azure AD application credentials](#).
5. [Specify SharePoint Online, OneDrive for Business and Microsoft Teams credentials](#).
6. [Finish the wizard](#).

Before You Begin

Before you start adding a new Microsoft 365 organization using [multi-factor authentication](#) (MFA) and legacy authentication protocols, you must register a new [Azure AD application](#) in your Microsoft Entra ID (formerly Azure Active Directory).

You will be required to provide connection settings to this application at the [Specify Azure AD Application Credentials](#) step. Such an application is used for establishing and maintaining a connection to your Microsoft 365 organizations and to perform a [backup](#) and [restore](#) from/to such organizations.

Make sure to grant your Azure AD application [required permissions](#).

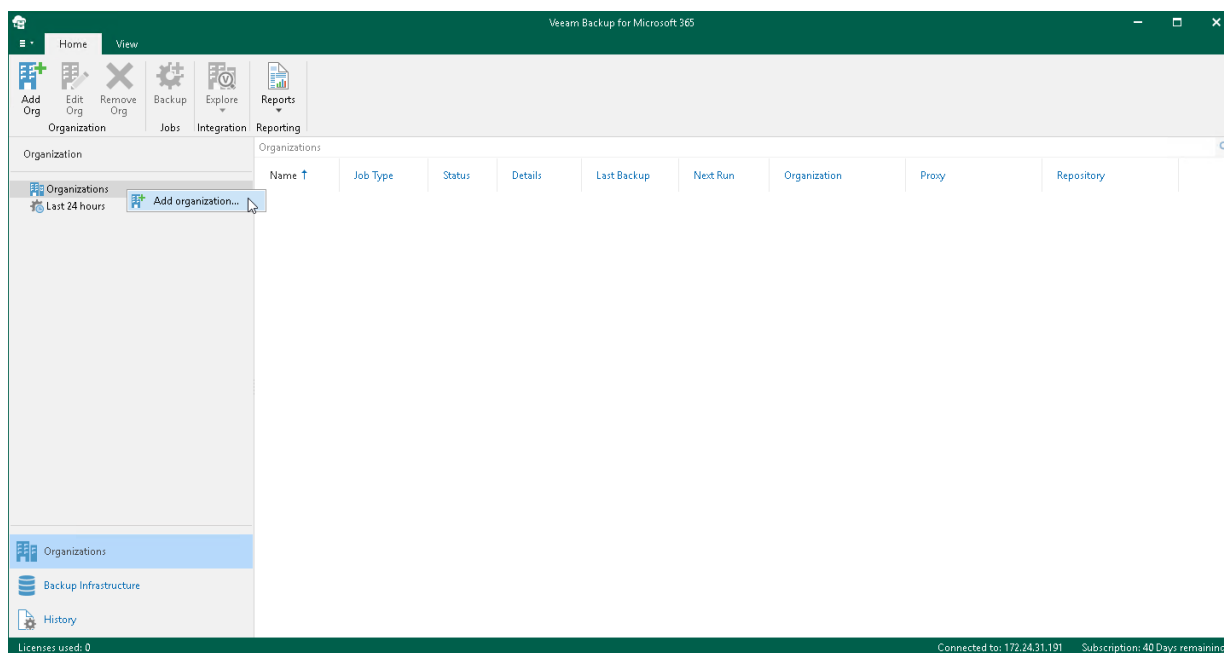
Check the following:

- [Security defaults](#) are disabled in your Microsoft 365 organization.
- [Conditional Access policies are not blocking legacy authentication protocols](#) for Veeam Backup account.

Step 1. Launch Add Organization Wizard

To launch the **Add Organization** wizard, do the following:

1. Open the **Organizations** view.
2. Do one of the following:
 - On the **Home** tab, click **Add Org** on the ribbon.
 - In the inventory pane, right-click the **Organizations** node and select **Add organization**.



Step 2. Select Organization Deployment Type

At this step of the wizard, select a deployment type and Microsoft Online services whose data you want to protect.

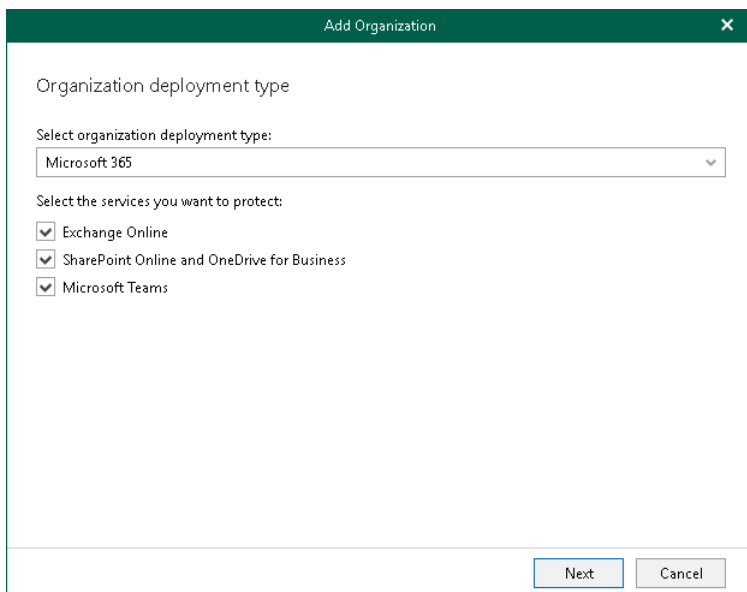
To select an organization deployment type and Microsoft Online services whose data you want to protect, do the following:

1. From the **Select organization deployment type** drop-down list, select *Microsoft 365*.
2. If you want to back up Exchange Online data, select the **Exchange Online** check box.
3. If you want to back up SharePoint Online and OneDrive for Business data, select the **SharePoint Online and OneDrive for Business** check box.
4. If you want to back up Microsoft Teams data, select the **Microsoft Teams** check box.

You can select this check box only if both **Exchange Online** and **SharePoint Online and OneDrive for Business** check boxes are selected.

NOTE

Microsoft Teams service is not supported for organizations in Microsoft Azure *China* and legacy Microsoft Azure *Germany* regions. For more information about Azure Germany, see [this Microsoft article](#).



The screenshot shows a dialog box titled "Add Organization" with a close button (X) in the top right corner. The main content area is titled "Organization deployment type". Below this title, there is a section "Select organization deployment type:" followed by a dropdown menu currently showing "Microsoft 365". Underneath, there is a section "Select the services you want to protect:" with three checked checkboxes: "Exchange Online", "SharePoint Online and OneDrive for Business", and "Microsoft Teams". At the bottom of the dialog, there are two buttons: "Next" (highlighted in blue) and "Cancel".

Step 3. Select Azure Region and Authentication Method

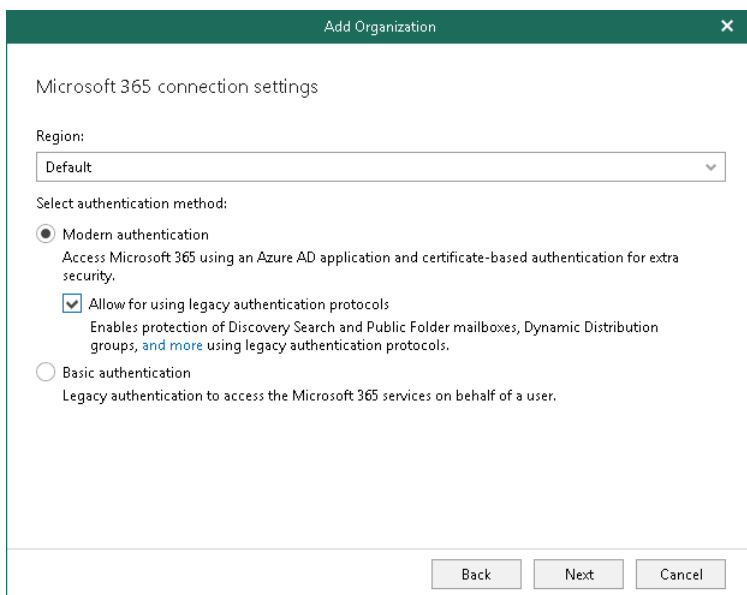
At this step of the wizard, select a region and authentication method.

To select a region and authentication method, do the following:

1. From the **Region** drop-down list, select a Microsoft Azure region your Microsoft 365 organization belongs to.

Keep in mind that you cannot select the *China* region for modern authentication with legacy protocols allowed.

2. Select the **Modern authentication** option and the **Allow for using legacy authentication protocols** check box to connect to your Microsoft 365 organization.



The screenshot shows a dialog box titled "Add Organization" with a close button (X) in the top right corner. The main content area is titled "Microsoft 365 connection settings".

Under "Region:", there is a dropdown menu currently showing "Default".

Under "Select authentication method:", there are two radio button options:

- Modern authentication**
Access Microsoft 365 using an Azure AD application and certificate-based authentication for extra security.
- Basic authentication**
Legacy authentication to access the Microsoft 365 services on behalf of a user.

Under the "Modern authentication" option, there is a checked checkbox for "Allow for using legacy authentication protocols" with the following text: "Enables protection of Discovery Search and Public Folder mailboxes, Dynamic Distribution groups, and more using legacy authentication protocols."

At the bottom of the dialog, there are three buttons: "Back", "Next", and "Cancel".

Step 4. Specify Azure AD Application Credentials

At this step of the wizard, specify credentials for Azure AD application that you want to use to access your Microsoft 365 resources.

To specify Azure AD application credentials, do the following:

1. In the **Application ID** field, specify an identification number of your Azure AD application.

You can find this number in an application settings in your Microsoft Entra ID (formerly Azure Active Directory). For more information, see [this Microsoft article](#).
2. Select an Azure AD application authentication type. You can select either **Application secret** or **Application certificate**:
 - To use a secret key, select the **Application secret** option and enter a secret key in the field nearby to access your custom application.

To obtain a secret key, you will need to generate it first. For more information on how to generate a secret key, see [this Microsoft article](#).

Keep in mind that a key will become hidden once you leave or refresh the page in the Azure portal. Consider saving the key to a secure location.
 - To use a certificate, select the **Application certificate** option and click **Install**. For more information, see [Installing SSL Certificates](#).

Keep in mind that you must upload a certificate file to the Azure portal beforehand. For more information, see [this Microsoft article](#).
3. In the **Username** and **App password** fields, specify Exchange Online credentials of your Microsoft 365 organization.

You must provide a user account in one of the following formats: *user@domain.com* or *user@domain.onmicrosoft.com*. If you are using an ADFS account, you can only use a non-MFA enabled ADFS account.
4. Select the **Grant this account required roles and permissions** check box to automatically assign the *ApplicationImpersonation* role. This role is required to back up Microsoft 365 Exchange mailboxes.

To assign the *ApplicationImpersonation* role, make sure the account that you use is a member of the *Organization Management* group and has been granted the *Role Management* role in advance.

5. Select the **Use the same credentials for SharePoint Online, OneDrive for Business and Microsoft Teams** check box if you want to use the same credentials to access your SharePoint Online, OneDrive for Business and Microsoft Teams organizations. This check box is only available if these organization types have been selected at the [Select Organization Deployment Type](#) step.

If the **Use the same credentials for SharePoint Online, OneDrive for Business and Microsoft Teams** check box is not selected, you will be offered to provide required credentials for the SharePoint Online, OneDrive for Business and Microsoft Teams organizations at the [Specify SharePoint Online, OneDrive for Business and Microsoft Teams Credentials](#) step.

The screenshot shows a dialog box titled "Add Organization" with a close button (X) in the top right corner. The main heading is "Exchange Online credentials". Below this, there are several input fields and checkboxes:

- Application ID:** A text box containing the value "e7268d27-0165-4778-9db6-5cfcb80a7636".
- Application secret:** A text box filled with black dots, with a radio button selected next to it.
- Application certificate:** A text box with a radio button next to it. To its right is a button labeled "Install...".
- Username:** A text box containing the value "administrator@abc.onmicrosoft.com".
- App password:** A text box filled with black dots.
- Checkboxes:**
 - Grant this account required roles and permissions
 - Use the same credentials for SharePoint Online, OneDrive for Business and Microsoft Teams

At the bottom of the dialog box, there are three buttons: "Back", "Next", and "Cancel". The "Next" button is highlighted with a blue border.

Step 5. Specify SharePoint Online, OneDrive for Business and Microsoft Teams Credentials

This step is only available if you did not select the **Use the same credentials for SharePoint Online, OneDrive for Business and Microsoft Teams** check box at the [Specify Azure AD Application Credentials](#) step of the wizard.

At this step of the wizard, enter credentials to connect to the SharePoint Online organization. Keep in mind that if you plan to back up Microsoft Teams data, Veeam Backup for Microsoft 365 will also use these credentials to connect to Microsoft Teams.

To enter credentials, do the following:

1. In the **Application ID** field, specify an identification number of your Azure AD application.

You can find this number in an application settings in your Microsoft Entra ID (formerly Azure Active Directory). For more information, see [this Microsoft article](#).
2. Select an Azure AD application authentication type. You can select either **Application secret** or **Application certificate**:
 - To use a secret key, select the **Application secret** option and enter a secret key in the field nearby to access your custom application.

To obtain a secret key, you will need to generate it first. For more information on how to generate a secret key, see [this Microsoft article](#).

Keep in mind that a key will become hidden once you leave or refresh the page in the Azure portal. Consider saving the key to a secure location.
 - To use a certificate, select the **Application certificate** option and click **Install**. For more information, see [Installing SSL Certificates](#).

Keep in mind that you must upload a certificate file to the Azure portal beforehand. For more information, see [this Microsoft article](#).
3. In the **Username** and **App password** fields, specify a user account credentials to connect to your Microsoft 365 organization.

You must provide a user account in one of the following formats: *user@domain.com* or *user@domain.onmicrosoft.com*. If you are using an ADFS account, you can only use a non-MFA enabled ADFS account.

4. Select the **Grant this account required roles and permissions** check box to automatically assign the *Site Collection Administrator* role that is required to back up Microsoft SharePoint Sites.

The screenshot shows a dialog box titled "Add Organization" with a close button (X) in the top right corner. The main heading is "SharePoint Online, OneDrive for Business and Microsoft Teams credentials".

The form contains the following fields and options:

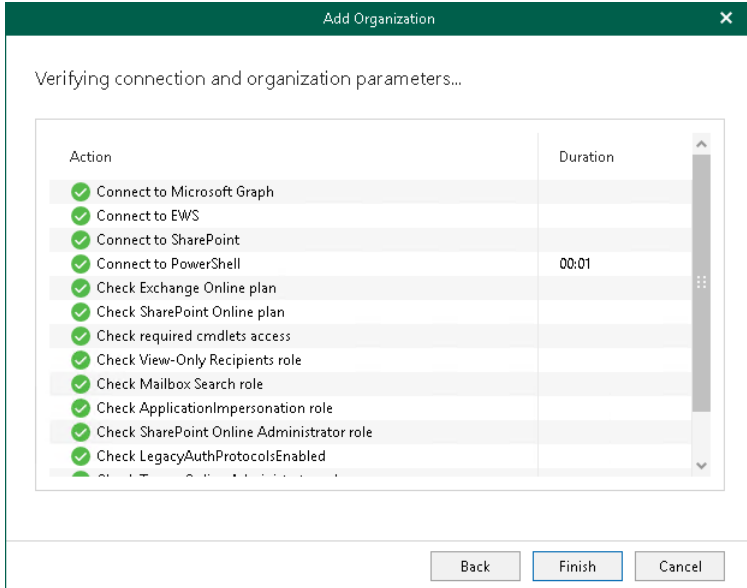
- Application ID:** A text box containing the value "e7268d27-0165-4778-9db6-5cfcb80a7636".
- Application secret:** A radio button is selected, followed by a text box filled with 20 black dots.
- Application certificate:** A radio button is unselected, followed by a text box and an "Install..." button.
- Username:** A text box containing the value "administrator@abc.onmicrosoft.com".
- App password:** A text box filled with 10 black dots.
- Grant this account required roles and permissions:** A checked checkbox.

At the bottom of the dialog, there are three buttons: "Back", "Next", and "Cancel". The "Next" button is highlighted with a blue border.

Step 6. Finish Working with Wizard

At this step of the wizard, wait for a connection to be established and click **Finish**.

The Microsoft 365 organization appears under the **Organizations** node in the inventory pane.



Adding Microsoft 365 Organizations with Basic Authentication

When you add an organization using the basic authentication method, you are required to provide a user name and password to authenticate to your Microsoft 365 organization.

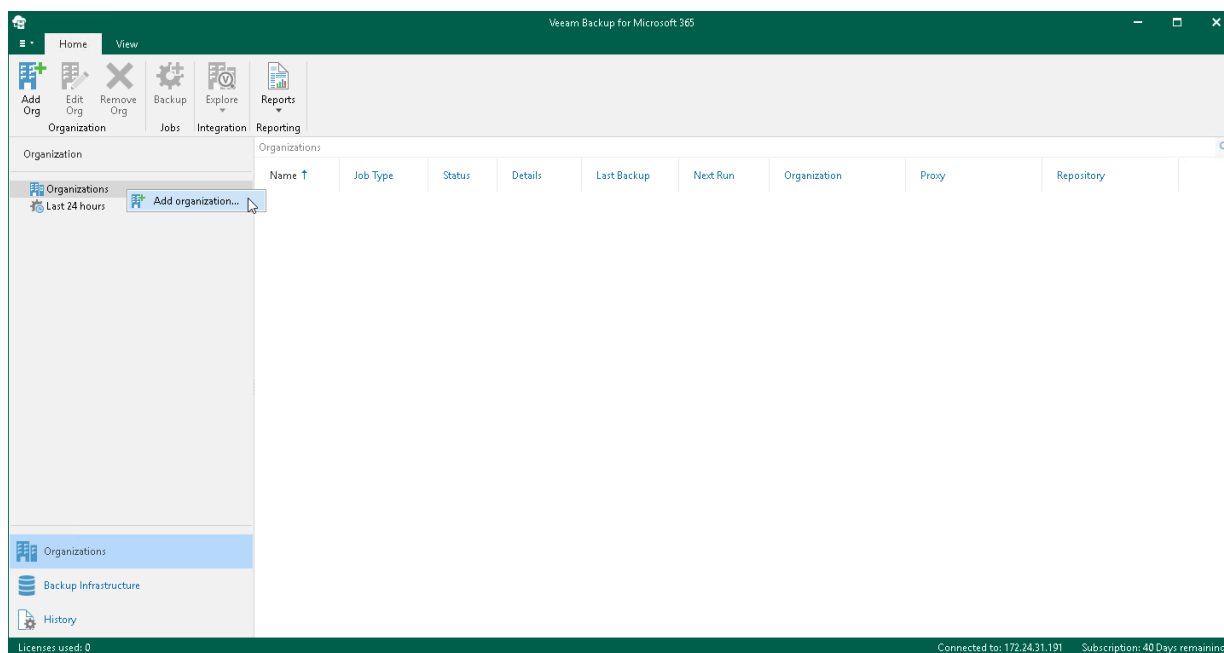
To add a new Microsoft 365 organization to Veeam Backup for Microsoft 365, do the following:

1. [Launch the Add Organization wizard.](#)
2. [Select an organization deployment type.](#)
3. [Select Azure region and authentication method.](#)
4. [Specify Exchange Online credentials.](#)
5. [Specify SharePoint Online, OneDrive for Business and Microsoft Teams credentials.](#)
6. [Finish the wizard.](#)

Step 1. Launch Add Organization Wizard

To launch the **Add Organization** wizard, do the following:

1. Open the **Organizations** view.
2. Do one of the following:
 - On the **Home** tab, click **Add Org** on the ribbon.
 - In the inventory pane, right-click the **Organizations** node and select **Add organization**.



Step 2. Select Organization Deployment Type

At this step of the wizard, select a deployment type and Microsoft Online services whose data you want to protect.

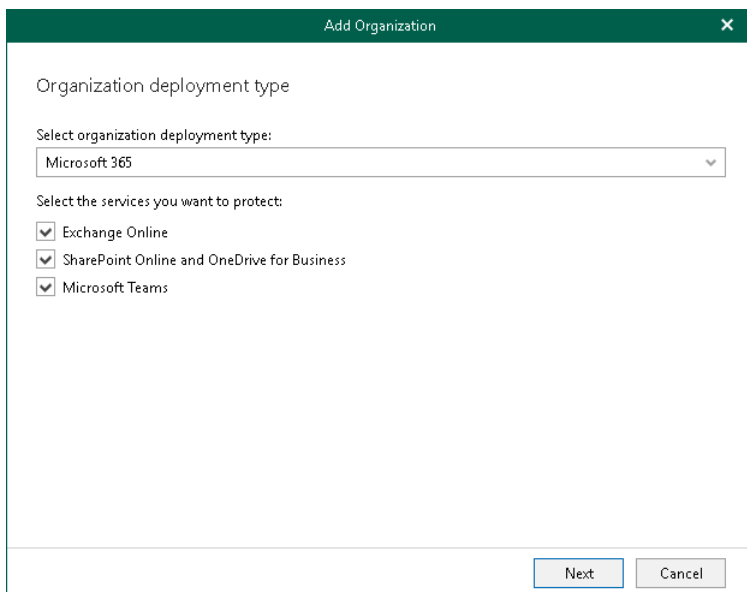
To select an organization deployment type and Microsoft Online services whose data you want to protect, do the following:

1. From the **Select organization deployment type** drop-down list, select *Microsoft 365*.
2. If you want to back up Exchange Online data, select the **Exchange Online** check box.
3. If you want to back up SharePoint Online and OneDrive for Business data, select the **SharePoint Online and OneDrive for Business** check box.
4. If you want to back up Microsoft Teams data, select the **Microsoft Teams** check box.

You can select this check box only if both **Exchange Online** and **SharePoint Online and OneDrive for Business** check boxes are selected.

NOTE

Microsoft Teams service is not supported for organizations in Microsoft Azure *China* and legacy Microsoft Azure *Germany* regions. For more information about Azure Germany, see [this Microsoft article](#).



The screenshot shows a dialog box titled "Add Organization" with a close button (X) in the top right corner. The main content area is titled "Organization deployment type". Below this title, there is a section "Select organization deployment type:" followed by a dropdown menu currently showing "Microsoft 365". Underneath, there is a section "Select the services you want to protect:" with three checked checkboxes: "Exchange Online", "SharePoint Online and OneDrive for Business", and "Microsoft Teams". At the bottom of the dialog, there are two buttons: "Next" (highlighted in blue) and "Cancel".

Step 3. Select Azure Region and Authentication Method

At this step of the wizard, select a region and authentication method.

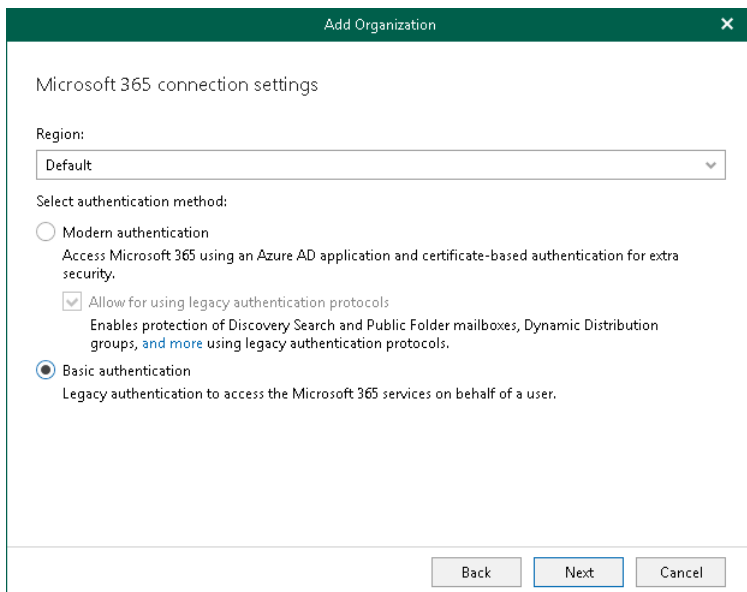
To select a region and authentication method, do the following:

1. From the **Region** drop-down list, select a Microsoft Azure region your Microsoft 365 organization belongs to.
2. Select the **Basic authentication** option to connect to your Microsoft 365 organization using the basic authentication method.

NOTE

To connect to Microsoft 365 organizations that belong to Microsoft Azure *China* and legacy Microsoft Azure *Germany* regions, Veeam Backup for Microsoft 365 requires an Azure AD application that is automatically deployed to your Microsoft Entra ID (formerly Azure Active Directory). To be able to deploy this application, Veeam Backup for Microsoft 365 requires the following roles to be granted to your Microsoft 365 account:

- *Application Administrator*
- *Cloud Application Administrator*



The screenshot shows a dialog box titled "Add Organization" with a close button (X) in the top right corner. The main content area is titled "Microsoft 365 connection settings". Below this title, there is a "Region:" label followed by a dropdown menu currently showing "Default". Underneath, the text "Select authentication method:" is followed by three radio button options. The first is "Modern authentication" with a description: "Access Microsoft 365 using an Azure AD application and certificate-based authentication for extra security." The second is "Allow for using legacy authentication protocols" (checked) with a description: "Enables protection of Discovery Search and Public Folder mailboxes, Dynamic Distribution groups, and more using legacy authentication protocols." The third is "Basic authentication" (selected) with a description: "Legacy authentication to access the Microsoft 365 services on behalf of a user." At the bottom of the dialog, there are three buttons: "Back", "Next", and "Cancel".

Step 4. Specify Exchange Online Credentials

At this step of the wizard, specify credentials to connect to your Exchange Online organization.

To specify credentials, do the following:

1. In the **Username** and **Password** fields, specify authentication credentials to connect to the Microsoft 365 organization.

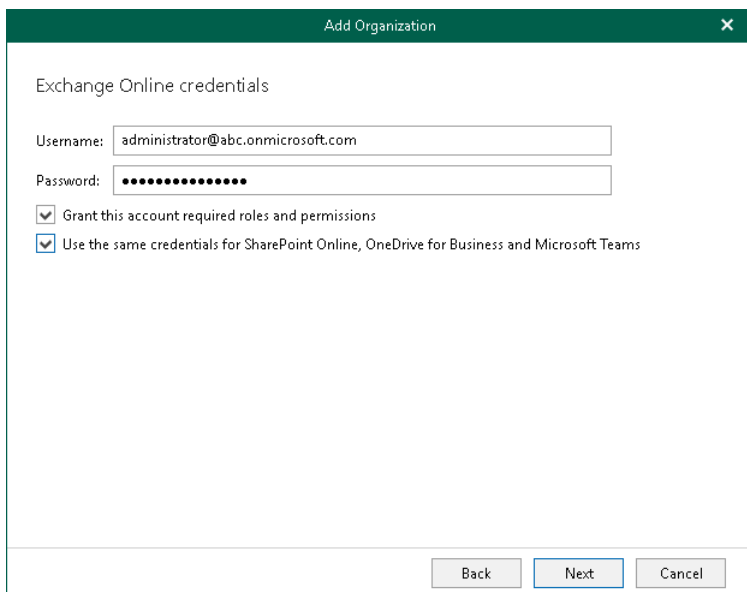
You must provide a user account in one of the following formats: *user@domain.com* or *user@domain.onmicrosoft.com*. If you are using an ADFS account, you can only use a non-MFA enabled ADFS account.

2. Select the **Grant this account required roles and permissions** check box to automatically assign the *ApplicationImpersonation* role. This role is required to back up Microsoft 365 Exchange mailboxes.

To assign the *ApplicationImpersonation* role, make sure the account that you use is a member of the *Organization Management* group and has been granted the *Role Management* role in advance.

3. Select the **Use the same credentials for SharePoint Online, OneDrive for Business and Microsoft Teams** check box if you want to use the same credentials to access your SharePoint Online, OneDrive for Business and Microsoft Teams organizations. This check box is only available if these organization types have been selected at the [Select Organization Deployment Type](#) step.

If the **Use the same credentials for SharePoint Online, OneDrive for Business and Microsoft Teams** check box is not selected, you will be offered to provide required credentials for the SharePoint Online, OneDrive for Business and Microsoft Teams organizations at the [Specify SharePoint Online, OneDrive for Business and Microsoft Teams Credentials](#) step.



The screenshot shows a dialog box titled "Add Organization" with a close button (X) in the top right corner. The main content area is titled "Exchange Online credentials" and contains the following elements:

- A "Username:" label followed by a text input field containing "administrator@abc.onmicrosoft.com".
- A "Password:" label followed by a password input field with 12 dots.
- Two checked checkboxes:
 - Grant this account required roles and permissions
 - Use the same credentials for SharePoint Online, OneDrive for Business and Microsoft Teams

At the bottom of the dialog box, there are three buttons: "Back", "Next", and "Cancel". The "Next" button is highlighted with a blue border.

Step 5. Specify SharePoint Online, OneDrive for Business and Microsoft Teams Credentials

This step is only available if you did not select the **Use the same credentials for SharePoint Online, OneDrive for Business and Microsoft Teams** check box at the [Specify Exchange Online Credentials](#) step of the wizard.

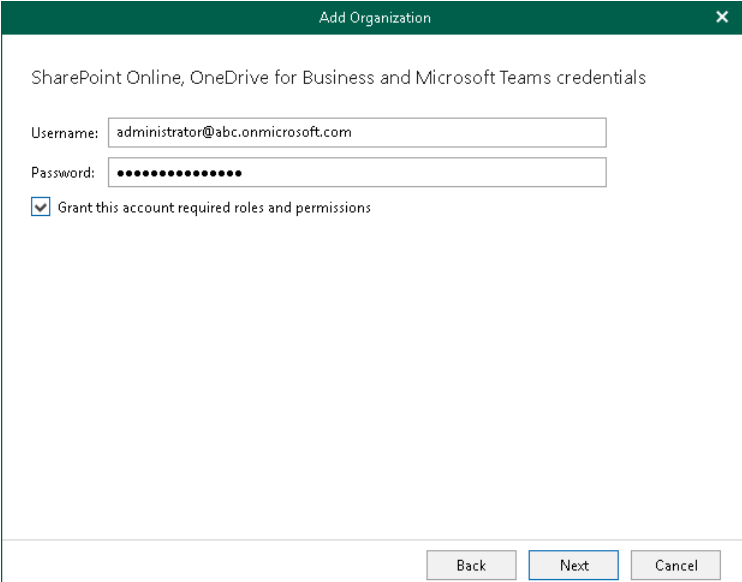
At this step of the wizard, enter credentials to connect to the SharePoint Online organization. Keep in mind that if you plan to back up Microsoft Teams data, Veeam Backup for Microsoft 365 will also use these credentials to connect to Microsoft Teams.

To enter credentials, do the following:

1. In the **Username** and **Password** fields, specify a user account credentials to connect to your Microsoft 365 organization.

You must provide a user account in one of the following formats: *user@domain.com* or *user@domain.onmicrosoft.com*. If you are using an ADFS account, you can only use a non-MFA enabled ADFS account.

2. Select the **Grant this account required roles and permissions** check box to automatically assign the *Site Collection Administrator* role that is required to back up Microsoft SharePoint Sites.

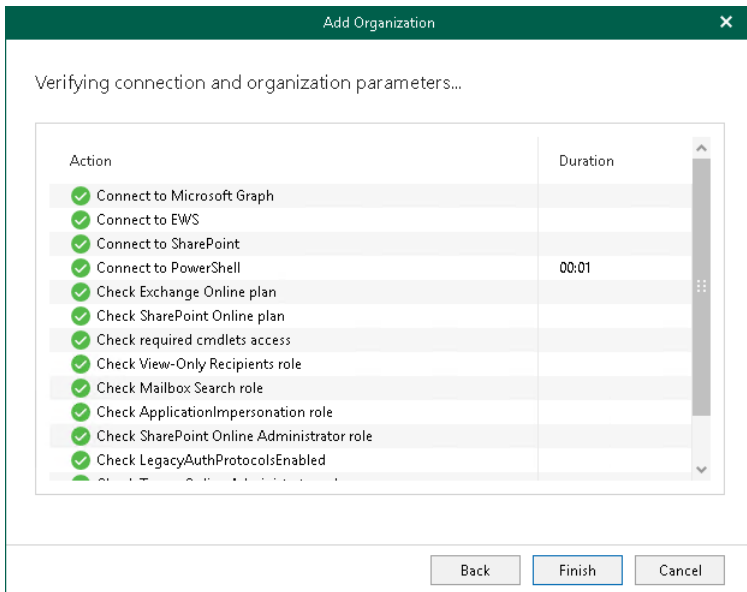


The screenshot shows a dialog box titled "Add Organization" with a close button (X) in the top right corner. The main content area is titled "SharePoint Online, OneDrive for Business and Microsoft Teams credentials". It contains three input fields: "Username:" with the text "administrator@abc.onmicrosoft.com", "Password:" with masked characters, and a checked checkbox labeled "Grant this account required roles and permissions". At the bottom of the dialog, there are three buttons: "Back", "Next", and "Cancel".

Step 6. Finish Working with Wizard

At this step of the wizard, wait for a connection to be established and click **Finish**.

The Microsoft 365 organization appears under the **Organizations** node in the inventory pane.



Adding On-Premises Microsoft Organizations

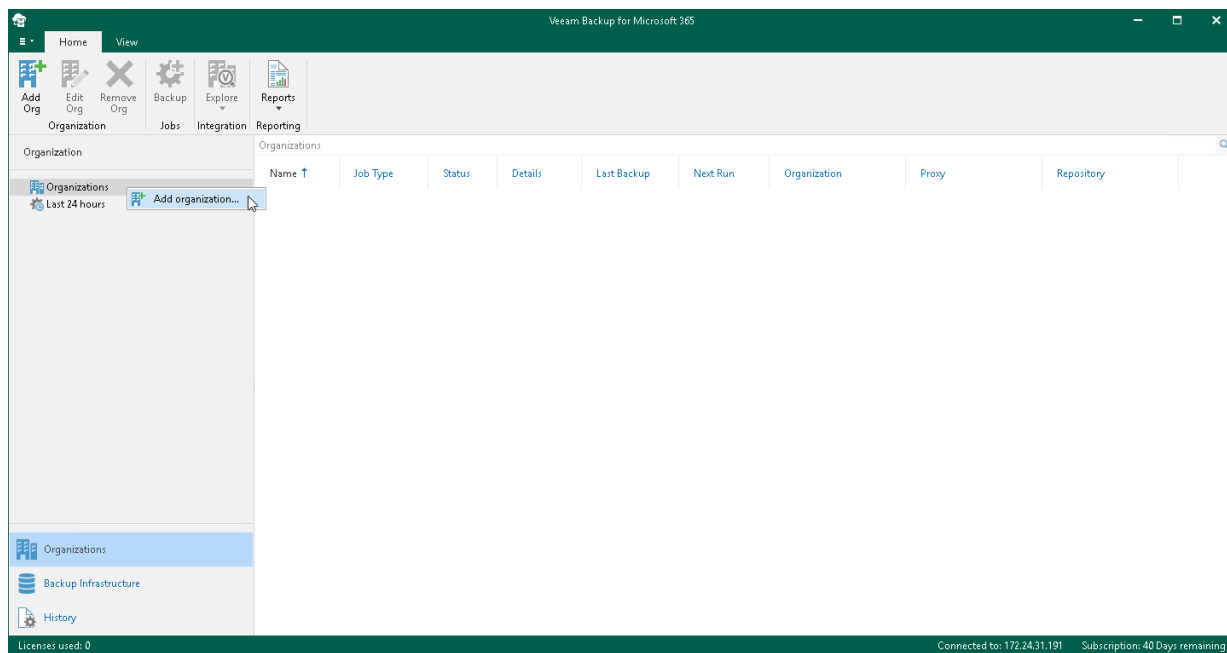
To add on-premises Microsoft Exchange and on-premises Microsoft SharePoint organizations, do the following:

1. [Launch the Add Organization wizard.](#)
2. [Select an organization deployment type.](#)
3. [Specify Microsoft Exchange connection settings.](#)
4. [Specify Microsoft SharePoint connection settings.](#)
5. [Finish the wizard.](#)

Step 1. Launch Add Organization Wizard

To launch the **Add Organization** wizard, do the following:

1. Open the **Organizations** view.
2. Do one of the following:
 - On the **Home** tab, click **Add Org** on the ribbon.
 - In the inventory pane, right-click the **Organizations** node and select **Add organization**.

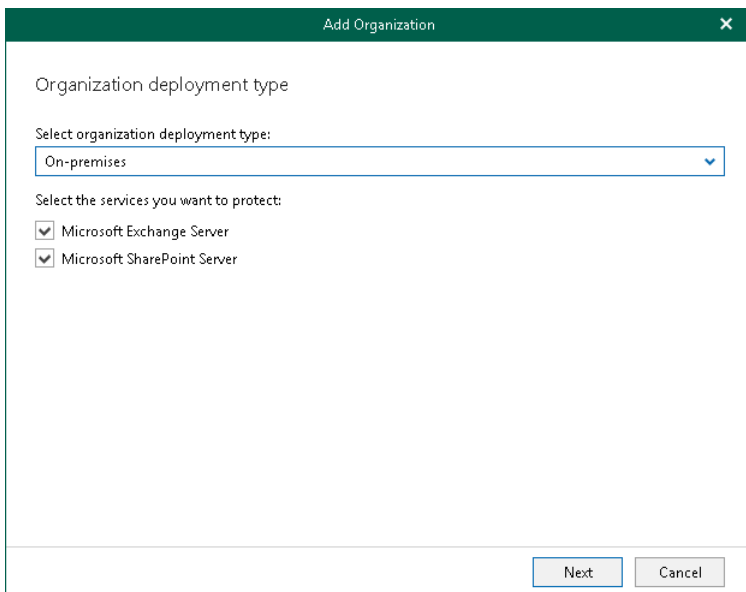


Step 2. Select Organization Deployment Type

At this step of the wizard, select a deployment type and on-premises services that you want to protect.

To select a deployment type and services, do the following:

1. From the **Select organization deployment type** drop-down list, select *On-premises*.
2. Select services that you want to protect:
 - **Microsoft Exchange Server**
Select this check box if you want to back up Microsoft Exchange data.
 - **Microsoft SharePoint Server**
Select this check box if you want to back up Microsoft SharePoint data.



The screenshot shows a dialog box titled "Add Organization" with a close button (X) in the top right corner. The dialog is divided into two main sections. The first section, "Organization deployment type", contains a label "Select organization deployment type:" followed by a dropdown menu currently displaying "On-premises". The second section, "Select the services you want to protect:", contains two checked checkboxes: "Microsoft Exchange Server" and "Microsoft SharePoint Server". At the bottom right of the dialog, there are two buttons: "Next" and "Cancel".

Step 3. Specify Microsoft Exchange Connection Settings

At this step of the wizard, specify a Microsoft Exchange server to which you want to connect, provide authentication credentials, assign permissions and configure advanced settings.

To specify connection settings to the on-premises Microsoft Exchange server, do the following:

1. In the **Server name** field, specify a Microsoft Exchange server to which you want to connect.

You can use a DNS name of a server, NetBIOS name or its IP address. Make sure that the server has the *Mailbox Server* role.

2. In the **Username** and **Password** fields, specify authentication credentials to connect to the Microsoft Exchange server.

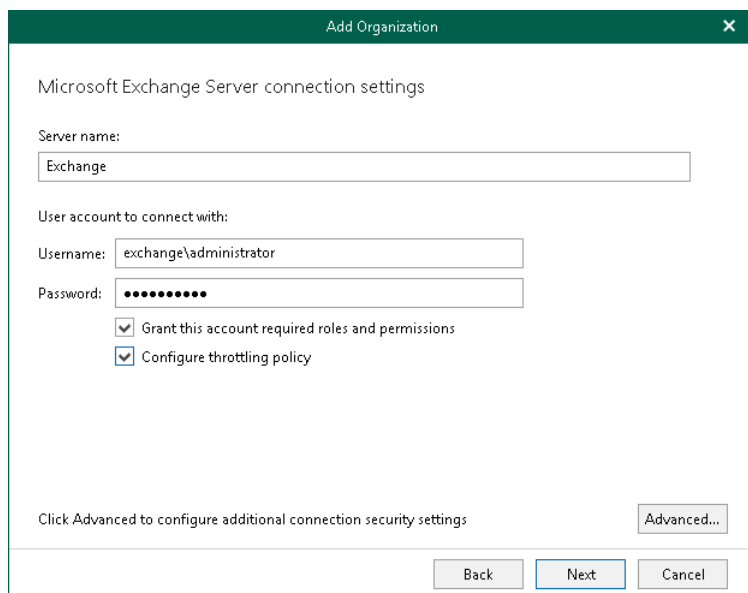
You must provide a user account in one of the following formats: *domain\account* or *account@domain*. Consider that using ADFS accounts to add on-premises Microsoft organizations is not possible. Only Microsoft 365 organizations can be added with non-MFA enabled ADFS accounts.

3. Select the **Grant this account required roles and permissions** check box to automatically assign the *ApplicationImpersonation* role.

Make sure the account that you use is a member of the *Organization Management* group and has been granted the *Role Management* role in advance. Otherwise, the automatic assignment of the *ApplicationImpersonation* role will fail; an organization will not be added.

For more information about the required roles and permissions, see [Veeam Backup Account Permissions](#).

4. Select the **Configure throttling policy** check box to set the throttling policy for the account being used to *Unlimited*.



The screenshot shows a dialog box titled "Add Organization" with a close button (X) in the top right corner. The main heading is "Microsoft Exchange Server connection settings". Below this, there are several input fields and checkboxes:

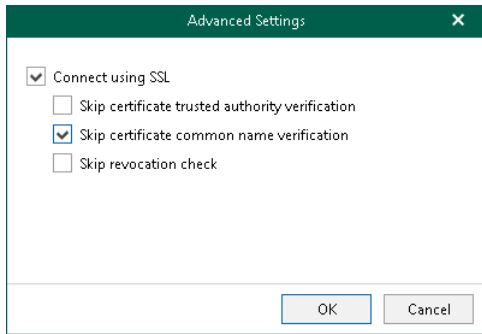
- Server name:** A text box containing the word "Exchange".
- User account to connect with:** A sub-heading for the following fields.
- Username:** A text box containing "exchange\administrator".
- Password:** A text box filled with ten black dots.
- Grant this account required roles and permissions**
- Configure throttling policy**

At the bottom left, there is a link: "Click Advanced to configure additional connection security settings". To its right is a button labeled "Advanced...". At the very bottom of the dialog are three buttons: "Back", "Next", and "Cancel".

5. Click **Advanced** if you want to configure whether to connect to the Microsoft Exchange server using SSL and to skip one or more SSL verifications. To do this, select or clear any of the following check boxes:

- **Connect using SSL**
 - **Skip certificate trusted authority verification**
 - **Skip certificate common name verification**

- Skip revocation check



Step 4. Specify Microsoft SharePoint Connection Settings

At this step of the wizard, specify a Microsoft SharePoint server to which you want to connect, provide authentication credentials, assign permissions and configure advanced settings.

To specify connection settings to the on-premises Microsoft SharePoint server, do the following:

1. In the **Server name and port** field, specify a Microsoft SharePoint server name and the WinRM port number.

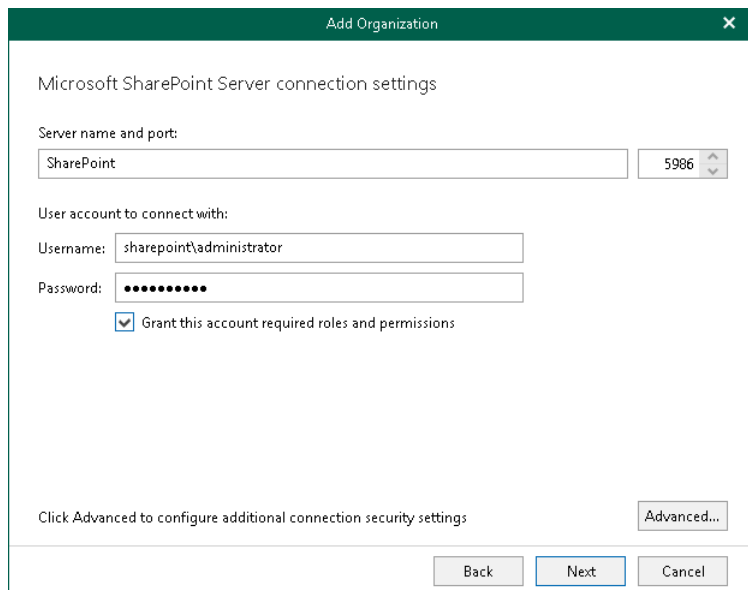
You can use a DNS name of a server, NetBIOS name or its IP address.

2. In the **Username** and **Password** fields, specify authentication credentials to connect to the Microsoft SharePoint server.

You must provide a user account in one of the following formats: *domain\account* or *account@domain*. Consider that using ADFS accounts to add on-premises Microsoft organizations is not possible. Only Microsoft 365 organizations can be added with non-MFA enabled ADFS accounts.

3. Select the **Grant this account required roles and permissions** check box to automatically add a user account to the SharePoint *Site Collection Administrators* group and grant this user administrative privileges to access Microsoft SharePoint sites. This option also grants access to the *User Profile* service to work with OneDrive data.

For more information about the required roles and permissions, see [Veeam Backup Account Permissions](#).



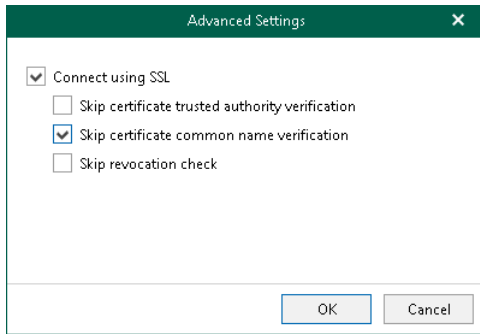
The screenshot shows a dialog box titled "Add Organization" with a close button (X) in the top right corner. The main heading is "Microsoft SharePoint Server connection settings". Below this, there are several input fields and a checkbox:

- Server name and port:** A text box containing "SharePoint" and a dropdown menu showing "5986".
- User account to connect with:** A section containing:
 - Username:** A text box containing "sharepoint\Administrator".
 - Password:** A text box filled with 10 black dots.
- Grant this account required roles and permissions:** A checked checkbox.
- Advanced settings:** A text box with the label "Click Advanced to configure additional connection security settings:" and a button labeled "Advanced...".

At the bottom of the dialog box, there are three buttons: "Back", "Next", and "Cancel".

4. Click **Advanced** if you want to configure whether to connect to the Microsoft SharePoint server using SSL and to skip one or more SSL verifications. To do this, select or clear any of the following check boxes:
 - **Connect using SSL**
 - **Skip certificate trusted authority verification**
 - **Skip certificate common name verification**

▪ Skip revocation check



Step 5. Finish Working with Wizard

At this step of the wizard, wait for a connection to be established and click **Finish**.

An on-premises Microsoft organization appears under the **Organizations** node in the inventory pane.

Adding Hybrid Organizations

Veeam Backup for Microsoft 365 allows you to create hybrid configurations consisting of Microsoft 365 organizations and on-premises Microsoft Exchange/SharePoint organizations.

You can add hybrid organizations as per the following scenarios:

- Microsoft Exchange Online + on-premises Microsoft Exchange.
- Microsoft Exchange Online + on-premises Microsoft Exchange + Microsoft SharePoint Online and OneDrive for Business.
- Microsoft Exchange Online + on-premises Microsoft Exchange + Microsoft SharePoint Online and OneDrive for Business + Microsoft Teams.
- Microsoft Exchange Online + on-premises Microsoft Exchange + Microsoft SharePoint Online and OneDrive for Business + on-premises Microsoft SharePoint.
- Microsoft Exchange Online + on-premises Microsoft Exchange + Microsoft SharePoint Online and OneDrive for Business + on-premises Microsoft SharePoint + Microsoft Teams.
- Microsoft SharePoint Online and OneDrive for Business + on-premises Microsoft SharePoint.
- Microsoft Exchange Online + Microsoft SharePoint Online and OneDrive for Business + on-premises Microsoft SharePoint.
- Microsoft Exchange Online + Microsoft SharePoint Online and OneDrive for Business + on-premises Microsoft SharePoint + Microsoft Teams.

NOTE

Veeam Backup for Microsoft 365 can back up Microsoft Teams messages using Microsoft Graph Teams Export APIs. This method substitutes backup of team chats using EWS APIs that will be deprecated by Microsoft. Keep in mind that backup of team chats using Teams Export APIs is limited to backup of public channel posts.

For more information on how to set up Veeam Backup for Microsoft 365 to use Teams Export APIs for team chats backup, see [Getting Started with Teams Export APIs](#).

Depending on whether you enabled usage of Teams Export APIs for team chats backup, Veeam Backup for Microsoft 365 displays different settings at the **Select Organization Deployment Type** step of the wizard. You can proceed to one of the following scenarios:

- [Backup of the Team Chats Using EWS](#)
Veeam Backup for Microsoft 365 displays these settings if you did not enable usage of Teams Export APIs for team chats backup.
- [Backup of team chats using Teams Export APIs](#)
Veeam Backup for Microsoft 365 displays these settings if you enabled usage of Teams Export APIs for team chats backup.

Backup of Team Chats Using EWS

Veeam Backup for Microsoft 365 displays these settings if you did not enable usage of Teams Export APIs for team chats backup.

NOTE

For more information about team chats backup in Veeam Backup for Microsoft 365, see [Backup of Team Chats Using Teams Export APIs](#).

To specify Microsoft services that you want to protect in your hybrid organization, select the following check boxes based on the listed scenarios:

- **Exchange Online**
To back up Exchange Online data.
- **Microsoft Exchange Server**
To back up on-premises Microsoft Exchange data.
- **SharePoint Online and OneDrive for Business**
To back up SharePoint Online and OneDrive for Business data.
- **Microsoft SharePoint Server**
To back up on-premises Microsoft SharePoint data.
- **Microsoft Teams**
Select this check box if you want to back up Microsoft Teams data.

You can select this check box only if both **Exchange Online** and **SharePoint Online and OneDrive for Business** check boxes are selected.

Depending on the types of services that you have selected, do the following:

- Select Microsoft Azure region and authentication method for the Microsoft 365 organization. For more information, see [Adding Microsoft 365 Organizations](#).
- Specify connection settings to the on-premises Microsoft Exchange and Microsoft SharePoint servers. For more information, see [Adding On-Premises Microsoft Organizations](#).

NOTE

Consider the following:

- To create a hybrid organization, services that you select must belong to the same Microsoft 365 organization.
- You can use a non-MFA enabled ADFS account to add a Microsoft 365 organization. Using ADFS accounts to add on-premises Microsoft organizations is not possible.

Organization deployment type

Select organization deployment type:

Hybrid

Select the services you want to protect:

- Exchange Online
- Microsoft Exchange Server
- SharePoint Online and OneDrive for Business
- Microsoft SharePoint Server
- Microsoft Teams

Next Cancel

Backup of Team Chats Using Teams Export APIs

Veeam Backup for Microsoft 365 displays these settings if you enabled usage of Teams Export APIs for team chats backup. Keep in mind that backup of team chats using Teams Export APIs is limited to backup of public channel posts.

To specify Microsoft services that you want to protect in your hybrid organization, select the following check boxes based on the listed scenarios:

- **Exchange Online**
To back up Exchange Online data.
- **Microsoft Exchange Server**
To back up on-premises Microsoft Exchange data.
- **SharePoint Online and OneDrive for Business**
To back up SharePoint Online and OneDrive for Business data.
- **Microsoft SharePoint Server**
To back up on-premises Microsoft SharePoint data.
- **Microsoft Teams**
Select this check box if you want to back up Microsoft Teams data.
You can select this check box only if both **Exchange Online** and **SharePoint Online and OneDrive for Business** check boxes are selected.
- **Teams chats**
Select this check box if you want to back up team chats using Teams Export APIs. For more information, see [Organization Object Types](#).
This check box is available only if the **Microsoft Teams** check box is selected.

Depending on the types of services that you have selected, do the following:

- Select Microsoft Azure region and authentication method for the Microsoft 365 organization. For more information, see [Adding Microsoft 365 Organizations](#).
- Specify connection settings to the on-premises Microsoft Exchange and Microsoft SharePoint servers. For more information, see [Adding On-Premises Microsoft Organizations](#).

NOTE

Consider the following:

- To create a hybrid organization, services that you select must belong to the same Microsoft 365 organization.
- You can use a non-MFA enabled ADFS account to add a Microsoft 365 organization. Using ADFS accounts to add on-premises Microsoft organizations is not possible.
- Backup of team chats using Teams Export APIs is only supported for Microsoft 365 organizations with modern app-only authentication.

The screenshot shows a dialog box titled "Add Organization" with a close button (X) in the top right corner. The main heading is "Organization deployment type". Below this, there is a section "Select organization deployment type:" with a dropdown menu currently showing "Hybrid". Underneath, there is a section "Select the services you want to protect:" followed by a list of services, each with a checked checkbox:

- Exchange Online
- Microsoft Exchange Server
- SharePoint Online and OneDrive for Business
- Microsoft SharePoint Server
- Microsoft Teams
- Teams chats

Below the "Teams chats" checkbox, there is a note: "Teams chats backup requires using protected APIs and additional billing charges from Microsoft. For more information on pricing, see this [Microsoft article](#)."

At the bottom of the dialog, there are two buttons: "Next" (highlighted with a blue border) and "Cancel".

Backup Accounts

When you add a Microsoft 365 organization using either basic authentication or modern authentication method with legacy protocols allowed, you can configure auxiliary backup accounts to minimize throttling when backing up Microsoft SharePoint and OneDrive for Business data.

To configure backup accounts, you use Microsoft 365 user accounts. You do not need to grant them any permissions or assign roles to them. Veeam Backup for Microsoft 365 automatically assigns the required roles to configured backup accounts.

NOTE

For Microsoft 365 organizations added using modern app-only authentication, you use backup applications instead. For more information, see [Backup Applications](#).

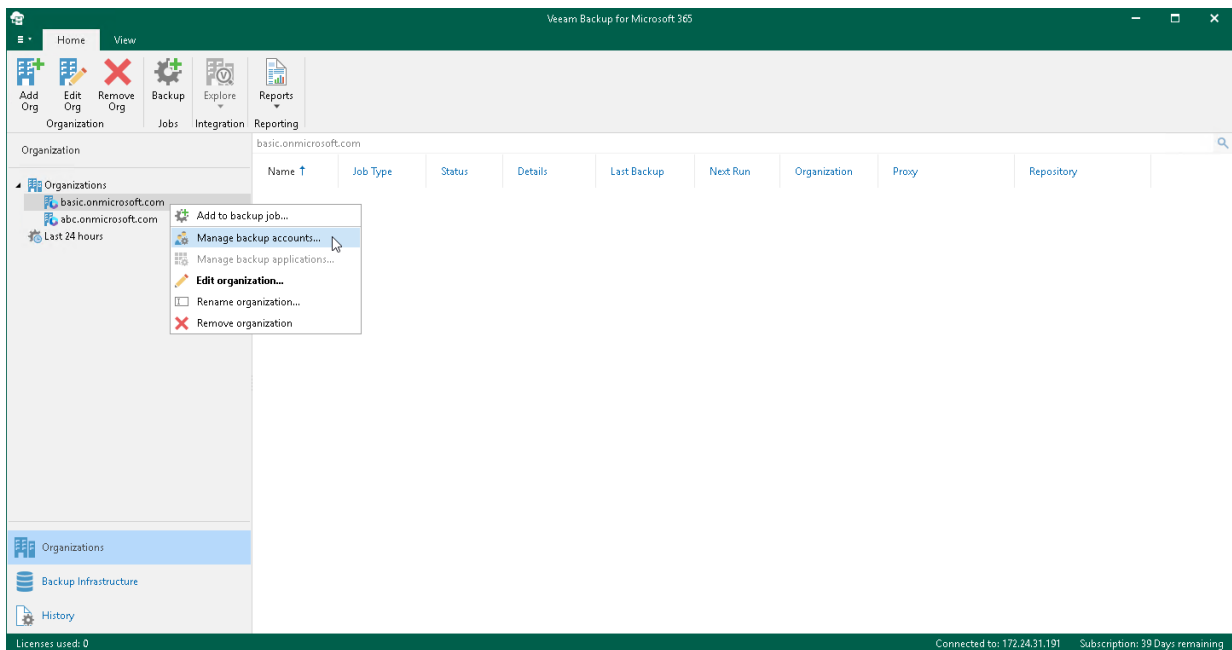
Adding Accounts

For Microsoft 365 organizations added using either basic authentication or modern authentication method with legacy protocols allowed, you can configure auxiliary backup accounts.

To add auxiliary backup accounts to the backup configuration, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, right-click an organization and select **Manage backup accounts**.

Keep in mind that the **Manage backup accounts** option is unavailable for organizations with modern app-only authentication. For organizations added using modern app-only authentication, you use the **Manage backup applications** option. For more information, see [Adding Applications](#).

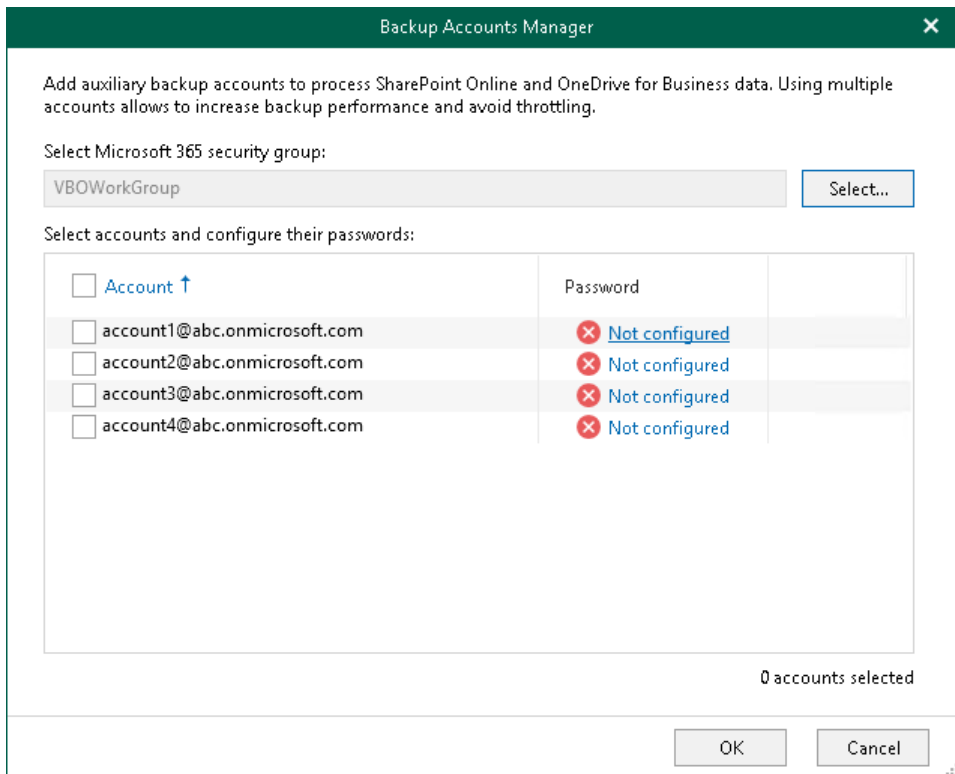


3. In the **Backup Accounts Manager** window, click **Select**.
4. In the **Select Security Group** window, select a security group with accounts that you want to use as auxiliary backup accounts and click **Add**.

Consider the following:

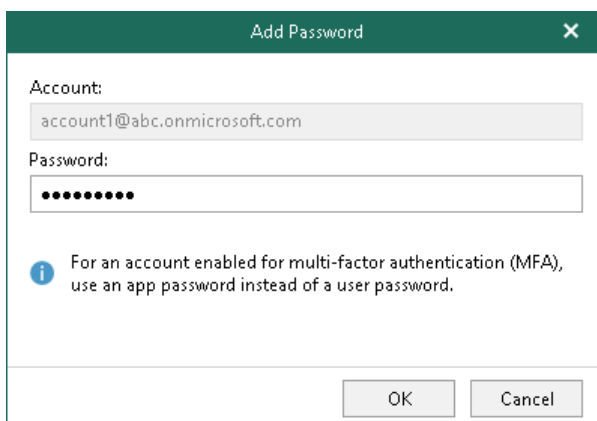
- The entire security group will be granted the *Site Collection Administrator* role. If a user ceases to be a member of the selected group, the role is automatically revoked for this user.
 - You should not select the **All Users** security group. Instead, you can create a new security group and populate this group with user accounts that you want to use during a backup session of Microsoft SharePoint data. For more information on how to create a new security group, see [this Microsoft article](#).
 - Mail-enabled security groups are not supported.
 - Veeam Backup for Microsoft 365 does not use an account under which you add your Microsoft 365 organization.
5. In the **Select accounts and configure their passwords** list, select check boxes next to accounts that you want to add as backup accounts.

6. In the **Password** column, click **Not configured**.



7. In the **Add Password** window, enter the password for the account and click **OK**.

Make sure to specify an **Azure AD application** password instead of a user account password when adding MFA-enabled accounts.



Changing Password and Removing Accounts

You can change the password of each [configured backup account](#) or you can remove an account from the backup configuration if you no longer want to use it.

Changing Password

To change the password of a backup account, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, right-click an organization and select **Manage backup accounts**.
3. In the **Backup Accounts Manager** window, in the **Password** column, click **Configured** next to the backup account whose password you want to change.
4. In the **Edit Password** window, modify the password.
5. Click **OK**.

Removing Account

To remove backup accounts from the backup configuration, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, right-click an organization and select **Manage backup accounts**.
3. In the **Backup Accounts Manager** window, in the **Account** column, clear check boxes next to accounts that you no longer want to use.
4. Click **OK**.

Backup Applications

You can configure [Azure AD applications](#) for Microsoft 365 organizations added using modern app-only authentication to minimize throttling when backing up Microsoft SharePoint Online and Microsoft OneDrive for Business data. You can add existing applications to the backup configuration or create new applications in your Microsoft Entra ID (formerly Azure Active Directory) using Veeam Backup for Microsoft 365 capabilities.

Consider the following:

- Using multiple applications may impact the performance of your production SharePoint environment. For more information, see [Impact of Multiple Backup Applications on Performance](#).

NOTE

This functionality will be deprecated in future versions of Veeam Backup for Microsoft 365.

- For security purposes, data exchange between applications in Azure and Veeam Backup for Microsoft 365 is maintained using SSL certificates only; you cannot use an [Azure AD application secret](#).
- For Microsoft 365 organizations added using either basic authentication or modern authentication method with legacy protocols allowed, you use backup accounts instead. For more information, see [Backup Accounts](#).

Impact of Multiple Backup Applications on Performance

Previously Veeam Backup for Microsoft 365 recommended you to add auxiliary Azure AD applications to the product configuration for Microsoft 365 organizations added using modern app-only authentication. Such backup applications were intended to improve performance and minimize throttling from Microsoft 365 when backing up Microsoft SharePoint Online and Microsoft OneDrive for Business data.

Due to recent restrictions that were applied by Microsoft, Veeam Backup for Microsoft 365 invokes you to use a single Azure AD application when backing up data in your production SharePoint environment.

In large-scale environments, you can use multiple backup applications to perform the initial backup under the supervision of Veeam Customer Support specialists. For all subsequent incremental backups, a single Azure AD application should be used.

Consider that this recommendation was designed in collaboration of Veeam together with Microsoft.

Those users who already use multiple backup applications to back up Microsoft SharePoint Online and Microsoft OneDrive for Business data and do not experience performance degradation in their Microsoft 365 environments can continue further without any changes in the Veeam Backup for Microsoft 365 configuration.

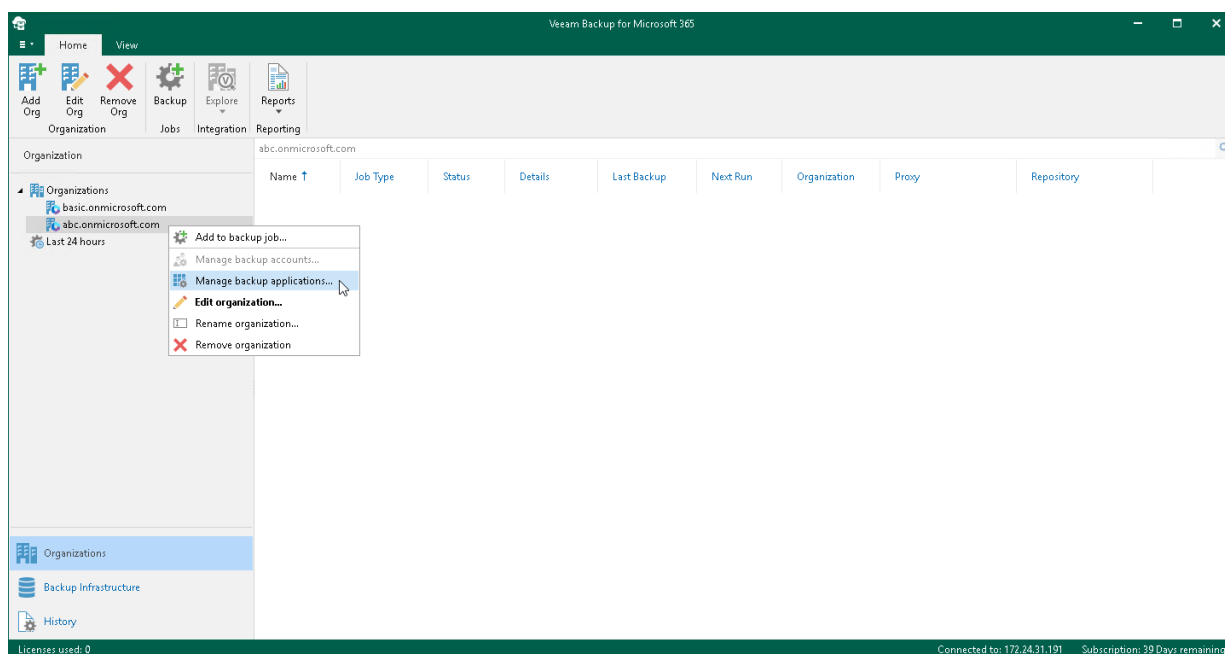
Adding Applications

When you add Azure AD applications to the backup configuration, Veeam Backup for Microsoft 365 retrieves a list of existing applications from your Microsoft Entra ID (formerly Azure Active Directory). From this list, you can select as many applications as you need. For more information about Azure AD applications, see [this Microsoft article](#).

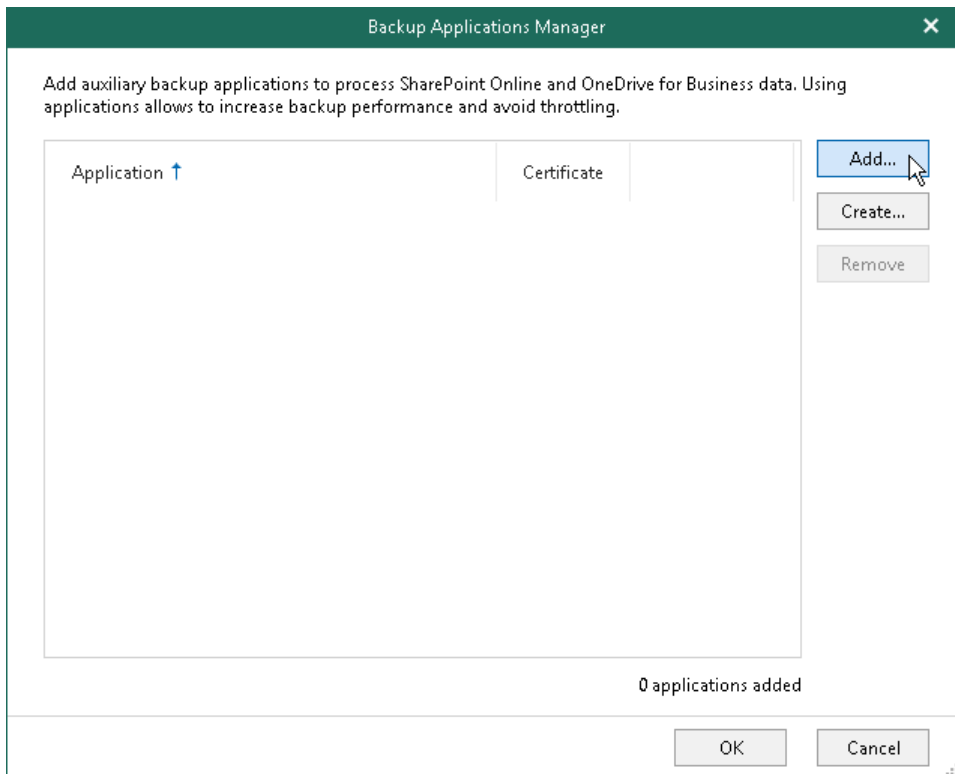
To add Azure AD applications to the backup configuration, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, right-click a Microsoft 365 organization with modern app-only authentication and select **Manage backup applications**.

Keep in mind that the **Manage backup applications** option is available only for organizations added using modern app-only authentication. For organizations added using either basic authentication or modern authentication method with legacy protocols allowed, you use the **Manage backup accounts** option. For more information, see [Adding Accounts](#).

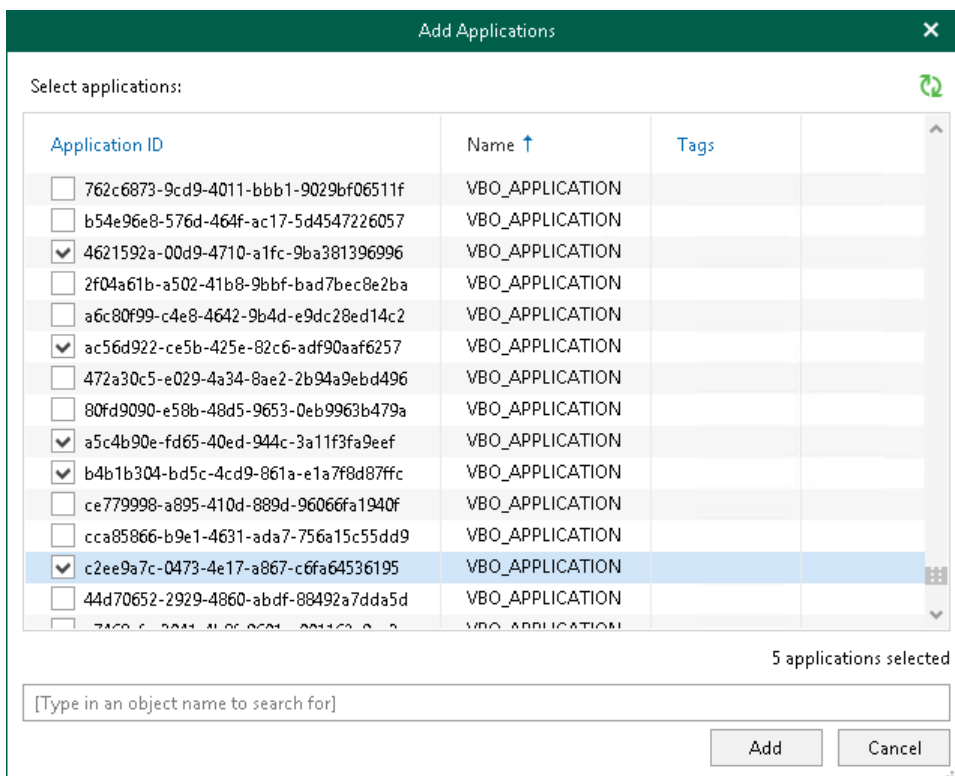


- In the **Backup Applications Manager** window, click **Add**.

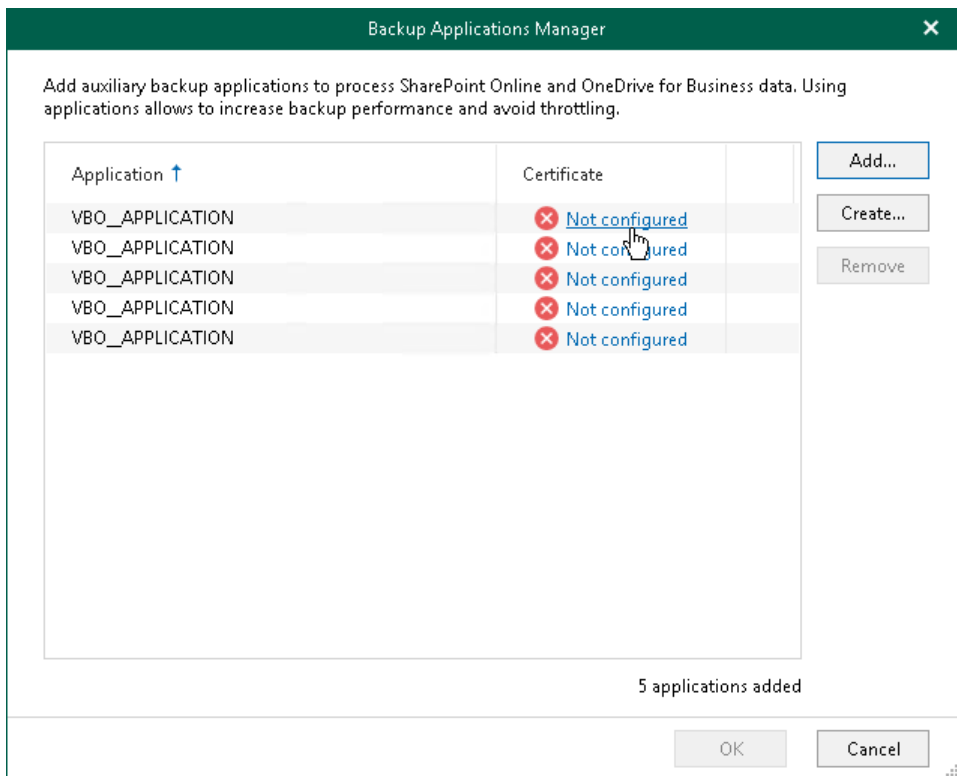


- In the **Add Applications** window, select Azure AD applications that you want to add and click **Add**.
Make sure to manually grant the [required permissions](#) to Azure AD applications in advance.

Also, keep in mind that Veeam Backup for Microsoft 365 ignores an Azure AD application that you use when [adding](#) your Microsoft 365 organization.



5. Click **Not configured** next to each added application to configure an SSL certificate that you want to use for secure communications between Veeam Backup for Microsoft 365 and your Azure AD application.



6. In the **Select Certificate** wizard, select an SSL certificate. For more information, see [Installing SSL Certificates](#).

Before selecting a certificate in Veeam Backup for Microsoft 365, you must upload a certificate file to the Microsoft Azure portal. For more information, see [this Microsoft article](#).

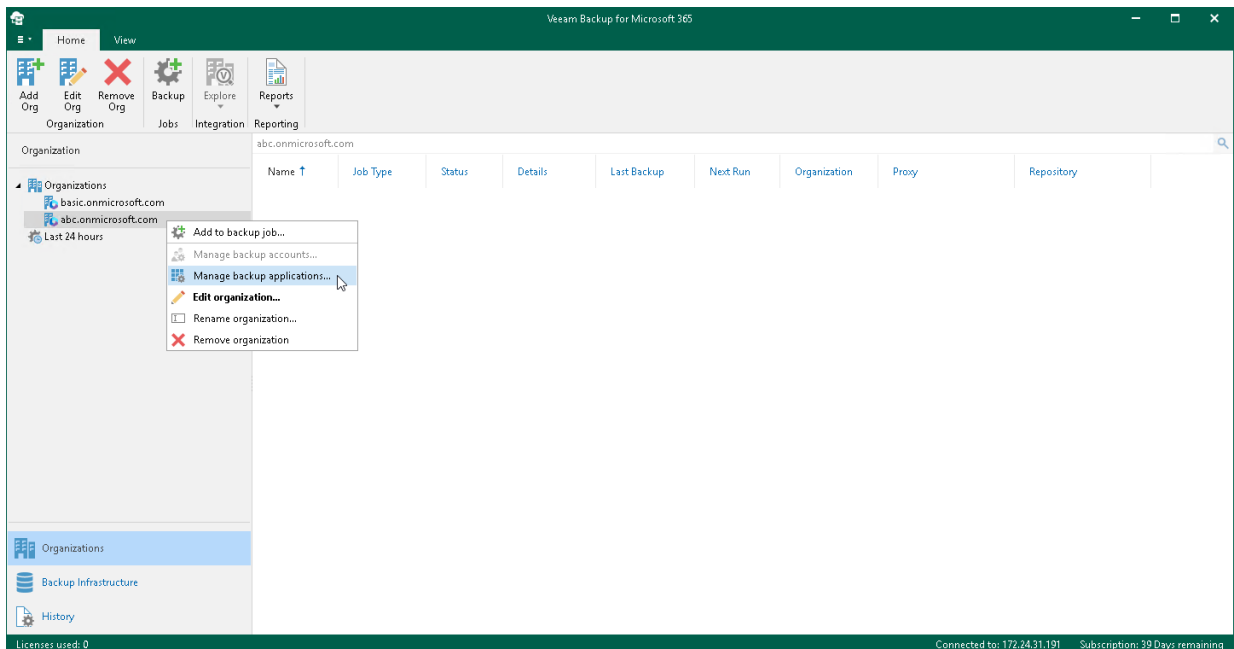
Creating Applications

When you create a new Azure AD application, Veeam Backup for Microsoft 365 automatically registers this application in Microsoft Entra ID (formerly Azure Active Directory) of your Microsoft 365 organization. After you create an application, Veeam Backup for Microsoft 365 automatically adds this application to the backup configuration. For more information about Azure AD applications, see [this Microsoft article](#).

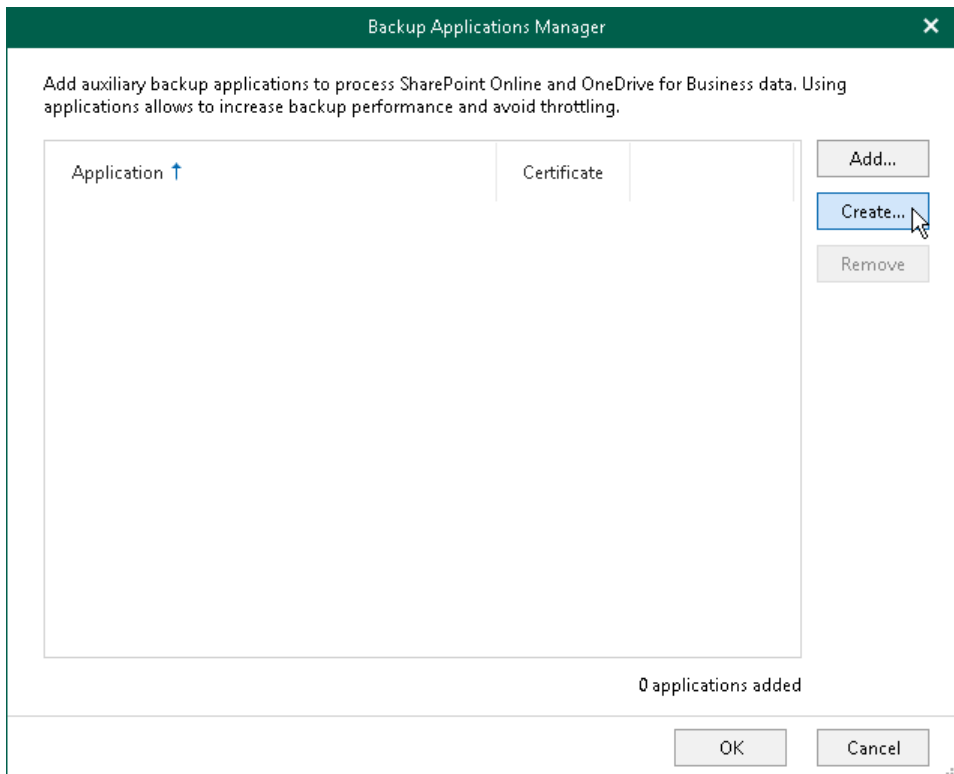
To create Azure AD applications and add them to the backup configuration, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, right-click a Microsoft 365 organization with modern app-only authentication and select **Manage backup applications**.

Keep in mind that the **Manage backup applications** option is available only for organizations added using modern app-only authentication. For organizations added using either basic authentication or modern authentication method with legacy protocols allowed, you use the **Manage backup accounts** option. For more information, see [Adding Accounts](#).



3. In the **Backup Applications Manager** window, click **Create**.

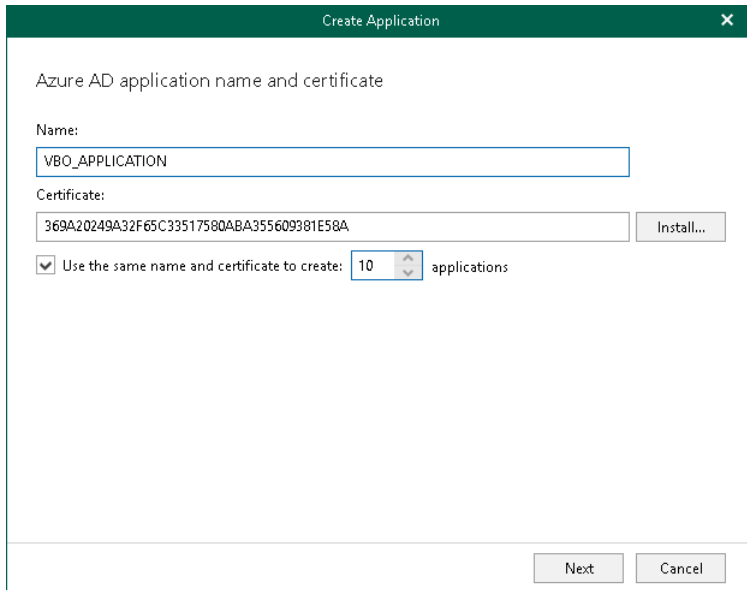


The **Create Application** wizard runs.

4. Enter a name that you want to use for the Azure AD application and specify an SSL certificate for secure communications between Veeam Backup for Microsoft 365 and your application. For more information on how to install a certificate, see [Installing SSL Certificates](#).

Veeam Backup for Microsoft 365 will automatically register the specified certificate in your Microsoft Entra ID (formerly Azure Active Directory) and assign this certificate to the Azure AD application. In addition, Veeam Backup for Microsoft 365 automatically grants the *Sites.FullControl.All* permission to the application.

If you want to create more than one Azure AD application, select the **Use the same name and certificate to create *N* applications** check box and specify how many applications Veeam Backup for Microsoft 365 must create. Applications may have the same name, however, each application always has a unique identification number. You can create maximum 100 applications per wizard session. If you need to create more than 100 applications, you can click **Create** and repeat the steps.



5. Click **Copy code** to copy an authentication code.

Keep in mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.

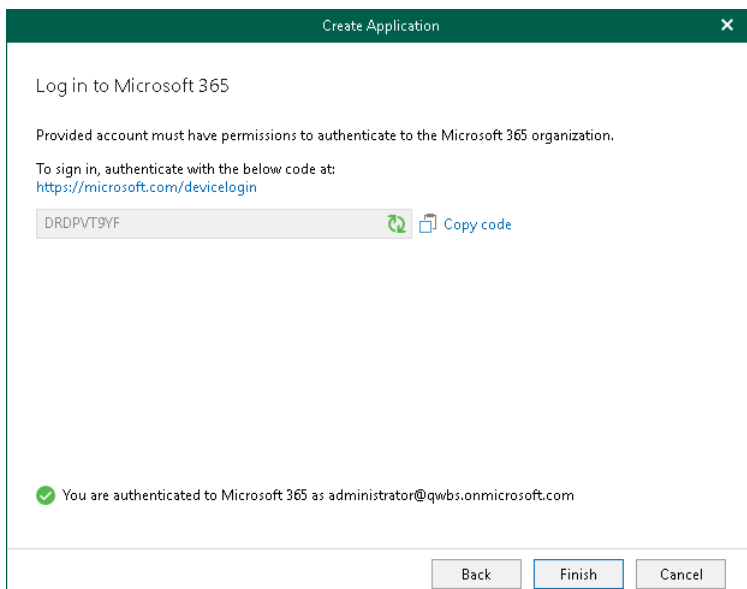
6. Click the Microsoft authentication portal link.

A web browser window opens.

7. On the **Sign in to your account** webpage, paste the code that you have copied and sign in to Microsoft Azure.

Make sure to sign in with the user account that has the *Global Administrator* role. For more information about this role, see [this Microsoft article](#).

8. Return to the **Create Application** wizard and click **Finish**.



Updating Certificates and Removing Applications

You can update an SSL certificate of each configured Azure AD application or you can remove an application from the backup configuration if you no longer want to use it. For more information on how to configure backup applications, see [Adding Applications](#) and [Creating Applications](#).

Updating Certificate

To update a certificate, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, right-click an organization and select **Manage backup applications**.
3. In the **Backup Applications Manager** window, in the **Certificate** column, click **Configured** next to the Azure AD application whose certificate you want to update.
4. Update the certificate using the **Select Certificate** wizard. For more information about this wizard, see [Installing SSL Certificates](#).

Removing Application

To remove an application, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, right-click an organization and select **Manage backup applications**.
3. In the **Backup Applications Manager** window, select Azure AD application that you want to remove in the list and click **Remove**.

You can select multiple applications using the **[CTRL]** key.

Editing Organization Settings

Veeam Backup for Microsoft 365 allows you to edit a Microsoft organization settings.

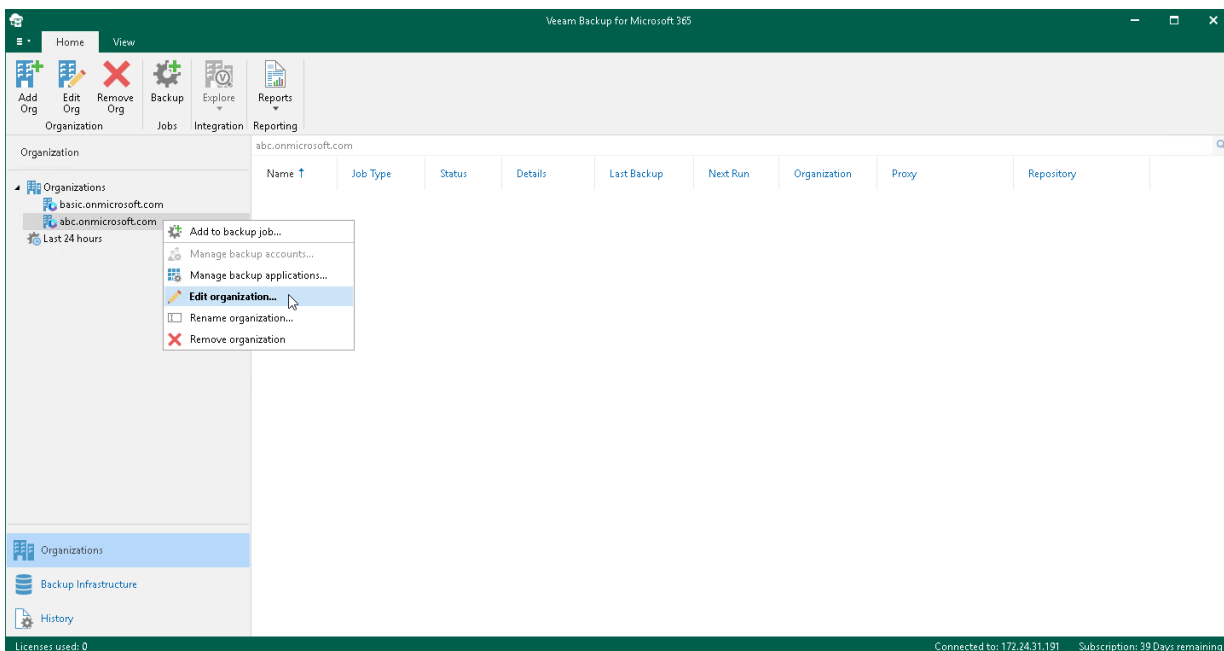
To edit a Microsoft organization settings, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select an organization.
3. Do one of the following:
 - On the **Home** tab, click **Edit Org** on the ribbon.
 - Right-click an organization and select **Edit organization**.
4. Modify the required settings.

You can edit the following organization settings:

- Organization deployment type.

Consider that you cannot change the *Microsoft 365* organization deployment type to the *On-premises* type.
- Services that you want to protect.
- Microsoft Azure region and authentication method.
- User name and password.

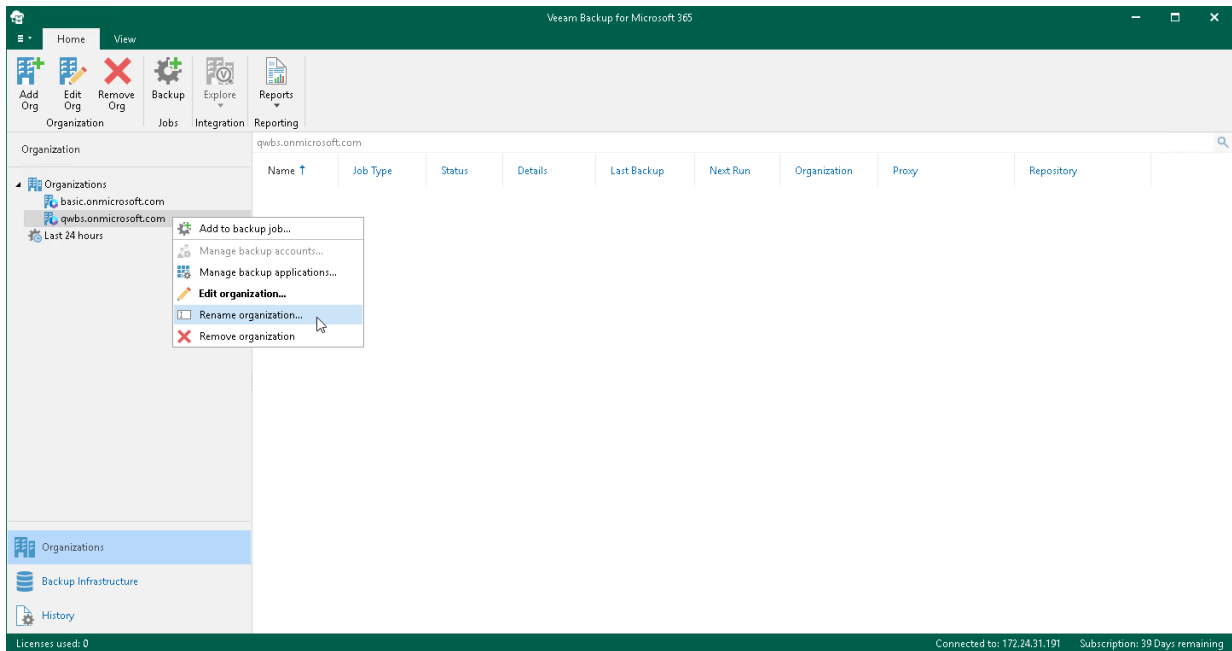


Renaming Organizations

You can rename your Microsoft 365 and on-premises Microsoft organizations. Keep in mind that you change the organization name that is displayed only in the Veeam Backup for Microsoft 365 console.

To rename an organization, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, right-click an organization and select **Rename organization**.



3. In the **Rename Organization** wizard, do the following:
 - a. Select one of the following options:
 - **Use the default name.** To continue using the default organization name.
 - **Use the following name.** To use a custom name.
When selecting this option, provide a new name.
Consider that when creating a [Mailbox Protection Reports](#) and [User Protection Reports](#), organizations will be shown with their default names.
 - b. In the **Description** field, enter optional description.

c. Click **Rename**.

Rename Organization

Specify organization name

Specify organization name to use in Veeam Backup for Microsoft 365:

Use the default name (qwbs.onmicrosoft.com)

Use the following name:

abc.onmicrosoft.com

Description:

ABC Organization

Rename Cancel

Removing Organizations

You can remove an organization from the Veeam Backup for Microsoft 365 console if you no longer need it.

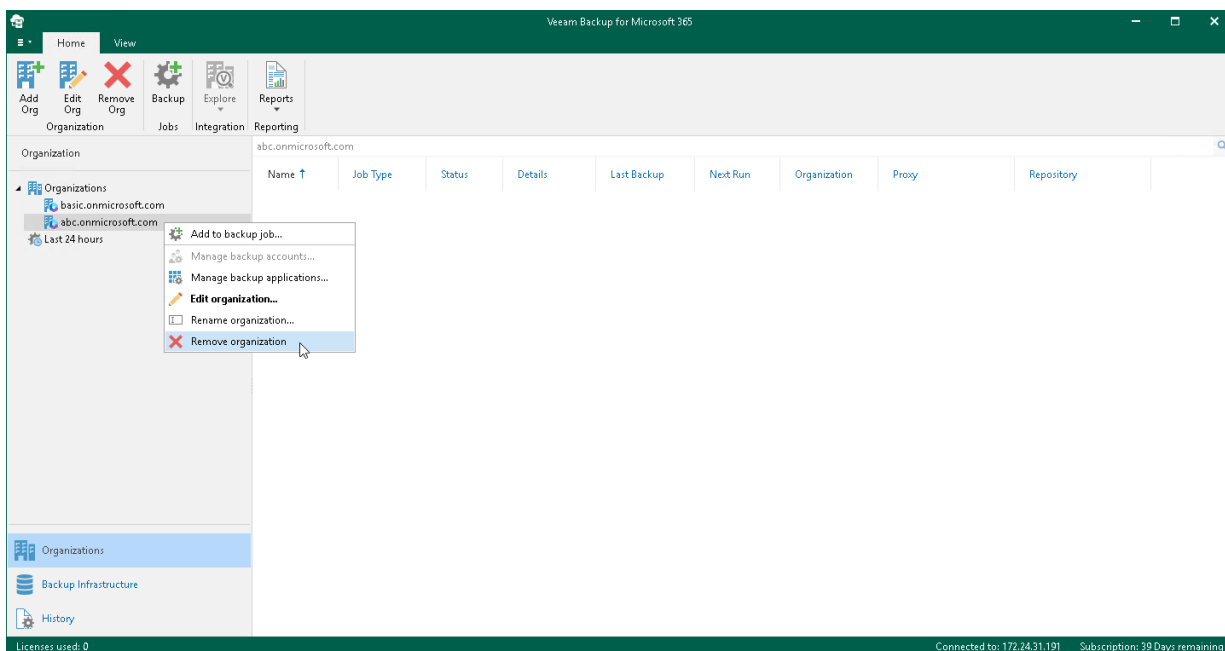
Consider the following:

- Backup jobs configured for the organization that you are removing will be permanently deleted.
- When removing an organization, its backups will not be removed. For local backup repositories, you can open the backed-up data as a separated database in Veeam Explorers. For more information, see the following sections:
 - [Veeam Explorer for Microsoft Exchange](#)
 - [Veeam Explorer for Microsoft SharePoint](#)
 - [Veeam Explorer for Microsoft OneDrive for Business](#)
 - [Veeam Explorer for Microsoft Teams](#)

If backups are stored in object storage, you must re-add an organization to Veeam Backup for Microsoft 365 to access the backed-up data and get restore points for object storage. For example, you can get restore points for object storage by running the [Get-VBORestorePoint](#) cmdlet.

To remove an organization, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select an organization.
3. Do one of the following:
 - On the **Home** tab, click **Remove Org** on the ribbon.
 - Right-click an organization and select **Remove organization**.



Data Backup

To back up data of your [Microsoft 365 and on-premises Microsoft organizations](#), you use backup jobs.

A backup job is a configuration unit of the backup activity. A backup job defines a list of users, groups, sites, teams, and organizations to back up, a location where to store backups, a schedule according to which new backups must be created. The first backup job session always produces a full backup of all objects added to a backup job scope. Subsequent backup job sessions are incremental – Veeam Backup for Microsoft 365 processes only those objects that have changed since the last backup job session.

Organization Object Types

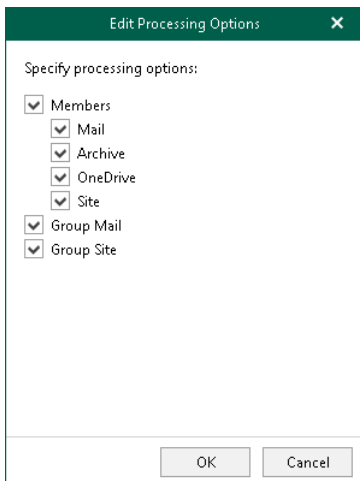
Veeam Backup for Microsoft 365 allows you to specify object types and their processing and exclusion options when creating and configuring backup jobs.

The following object types are available for [backup](#) and [restore](#):

- [Organizations](#)
Consists of organization objects and their processing options.
- [Groups](#)
Consists of Microsoft 365 groups (available only in Microsoft 365 organizations), security groups, distribution groups and dynamic distribution groups.
- [Users](#)
Consists of shared mailboxes, public mailboxes and users.
- [Sites](#)
Consists of Microsoft SharePoint sites and subsites.
- [Teams](#)
Consists of Microsoft Teams teams.

Each of these object types (except for the *Sites* and *Teams* types) consists of a set of processing/exclusion options such as **Mail**, **Archive**, **OneDrive**, **Site**, **Group Mail** and **Group Site** which you can select/clear to make data retrieval even more precise.

Processing and exclusion options can be selected at the [Select Objects to Back Up](#) and [Select Objects to Exclude](#) steps of the **New Backup Job** wizard.



†If you did not enable usage of Teams Export APIs for team chats backup.

Organizations

The following table lists processing/exclusion options available for *Organization* type:

Options for Microsoft 365 Organizations	Options for On-premises Microsoft Exchange Organizations	Options for On-premises Microsoft SharePoint Organizations
<i>Mail, Archive, OneDrive, Sites, Teams and Teams chats¹</i>	<i>Mail and Archive</i>	<i>OneDrive and Sites</i>

¹If you enabled usage of Teams Export APIs for team chats backup.

Groups

The following table lists available *Group* types and their processing/exclusion options:

Group Type	Options for Microsoft 365 Organizations	Options for On-premises Microsoft Exchange Organizations
M365 group (available only in Microsoft 365 organizations)	When configuring Microsoft 365 organizations, the following set of processing/exclusion options is available: <ul style="list-style-type: none"> • <i>Members with Mail, Archive, OneDrive and Site</i> • <i>Group Mail</i> • <i>Group Site</i> 	N/A
Security Group	<i>Members with Mail, Archive, OneDrive and Site options</i>	<i>Members with Mail and Archive options</i>
Distribution Group		
Dynamic Distribution Group		

NOTE

Groups are not available in on-premises Microsoft SharePoint organizations.

Users

The following table lists available *User* types and their processing/exclusion options:

User Type	Options for Microsoft 365 Organizations	Options for On-premises Microsoft Exchange Organizations	Options for On-premises Microsoft SharePoint Organizations
User	<i>Mail, Archive, OneDrive and Site</i>	<i>Mail and Archive</i>	<i>OneDrive and Site</i>
Shared Mailbox (available only in Microsoft 365 and Exchange organizations) ¹	Note: Veeam Backup for Microsoft 365 backs up SharePoint sites and OneDrive accounts content that belongs to a user account added to a backup job.		N/A
Public Mailbox (available only in Microsoft 365 and Exchange organizations) ¹			
Discovery Search Mailbox (available only in Microsoft 365 and Exchange organizations) ¹			
Note: Displayed with the <i>User</i> type.			

¹Starting from version 7 CP4 (build 7.0.0.3968), to back up public folder and discovery search mailboxes as well as determine correctly object type for shared mailboxes in Microsoft 365 organizations with modern app-only authentication, Veeam Backup for Microsoft 365 needs additional permission and role granted to an Azure AD application. For more information, see [Permissions for Backup](#) and [Granting Global Reader Role to Azure AD Application](#).

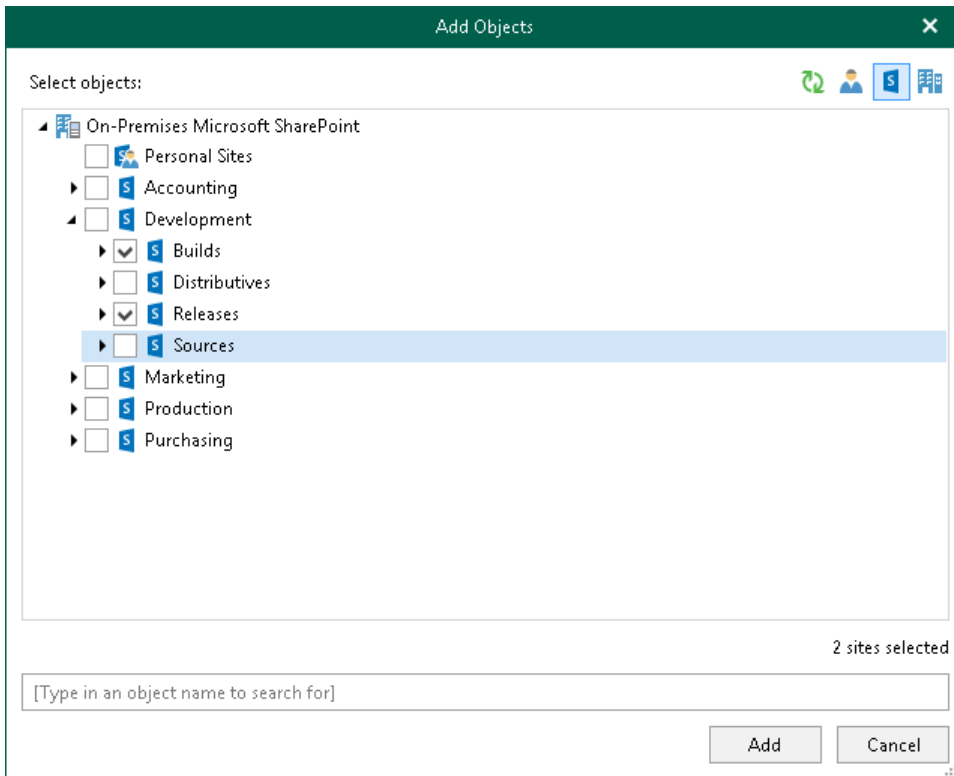
Sites

Consider the following:

- Objects of the *Site* type do not have any processing/exclusion options.

- You can select either the *root* site, or any of its *subsites*.

In the following example, you can select either the root *Development* site which automatically selects all of its subsites, or you can select, for example, *Builds* and *Releases*. In the latter case, the root *Development* site will not be selected.



Teams

Consider the following:

- Objects of this type are available in Microsoft 365 organizations only.
- When you add an object of this type to a backup job, Veeam Backup for Microsoft 365 backs up the following objects:

- o Team chats.

To backup team chats, Veeam Backup for Microsoft 365 does one of the following:

- Backs up the *TeamChat* and *TeamsMessagesData* folders of the group mailbox that belongs to the Microsoft 365 group associated with the backed-up team. This is the default scenario for team chats backup in Veeam Backup for Microsoft 365.
- Uses [Teams Export APIs](#). You can use Teams Export APIs for team chats backup only for Microsoft 365 organizations with modern app-only authentication. To proceed to this scenario, you must set up Veeam Backup for Microsoft 365 to use Teams Export APIs for team chats backup. For more information, see [Backup of Team Chats Using Teams Export APIs](#).

- o Document library of the SharePoint team site.

- o Team metadata, for example, settings of the team, information about team members, channels, tabs, applications.

-

- You can edit processing options for the *Team* type objects only if you enable usage of Teams Export APIs for team chats backup. For more information, see [Getting Started with Teams Export APIs](#).

The following table lists processing options available for objects of the *Team* type:

Options for Microsoft 365 Organizations with Modern App-Only Authentication	Options for Microsoft 365 Organizations with Modern Authentication and Legacy Protocols	Options for Microsoft 365 Organizations with Basic Authentication
<i>Chats and Channels, tabs, files, membership</i>	<i>Channels, tabs, files, membership</i>	<i>Channels, tabs, files, membership</i>
Note: Channels, tabs, files, membership of a team are always processed.		

If you enabled usage of Teams Export APIs for team chats backup.

Backup of Team Chats Using Teams Export APIs

Veeam Backup for Microsoft 365 can back up Microsoft Teams messages using Microsoft Graph Teams Export APIs. This method substitutes backup of team chats using EWS APIs that will be deprecated by Microsoft.

Teams Export APIs allow Veeam Backup for Microsoft 365 to access sensitive data of team chats, including channel messages. As a result, Veeam Backup for Microsoft 365 can back up such objects.

Because Teams Export APIs provide access to sensitive data, they are considered protected APIs. This is a reason that before starting to use Teams Export APIs in Veeam Backup for Microsoft 365, you must request access to Teams Export APIs and grant permissions. For more information, see [Getting Started with Teams Export APIs](#).

Consider the following:

- Microsoft applies an additional cost for using Microsoft Graph Teams Export APIs. Veeam Backup for Microsoft 365 API requests will be qualified as [Model B](#).
- Backup of team chats using the Teams Export APIs is only supported for Microsoft 365 organizations with modern app-only authentication.
- Backup of team chats using Teams Export APIs is not supported for Microsoft organizations in Microsoft Azure *China*, legacy *Germany*, *US Government GCC* and *US Government GCC High* regions.

For more information about Teams Export APIs, see [this Microsoft article](#).

Getting Started with Teams Export APIs

To set up Veeam Backup for Microsoft 365 to use Teams Export APIs for team chats backup, do the following:

- Make sure that your Microsoft 365 organization has access to the Teams Export APIs. For more information on how to request access to Teams Export APIs, see [this Veeam KB article](#).
- Enable usage of Teams Export APIs for team chats backup. Do the following:
 - Run the [Set-VBOServer](#) cmdlet with the `EnableTeamsGraphAPIBackup` parameter.
 - Run the [Set-VBOProxy](#) cmdlet with the `EnableTeamsGraphAPIBackup` parameter.

NOTE

If you enabled usage of Teams Export APIs for team chats backup in PowerShell, you cannot revert this action.

For more information, see [this Veeam KB article](#).

3. In the **Add Organization** or **Edit Organization** wizard, select the **Teams chats** check box when adding a new Microsoft 365 organization with modern app-only authentication or editing an existing one. If you do not select this check box, Veeam Backup for Microsoft 365 will not back up team chats.
4. Do one of the following to enable access for an existing Azure AD application to all Teams public channel messages:
 - In the **Add Organization** or **Edit Organization** wizard, allow Veeam Backup for Microsoft 365 to grant automatically the *ChannelMessage.Read.All* Microsoft Graph API permission to an existing Azure AD application when adding a new Microsoft 365 organization with modern app-only authentication or editing an existing one. For more information, see [Adding Microsoft 365 Organizations with Modern App-Only Authentication](#).
 - In the Microsoft Azure portal, grant manually the *ChannelMessage.Read.All* Microsoft Graph API permission to this Azure AD application. For more information, see [Permissions for Modern App-Only Authentication](#).

For more information on how to set up Veeam Backup for Microsoft 365 to use Teams Export APIs, see [this Veeam KB article](#).

Creating Backup Job

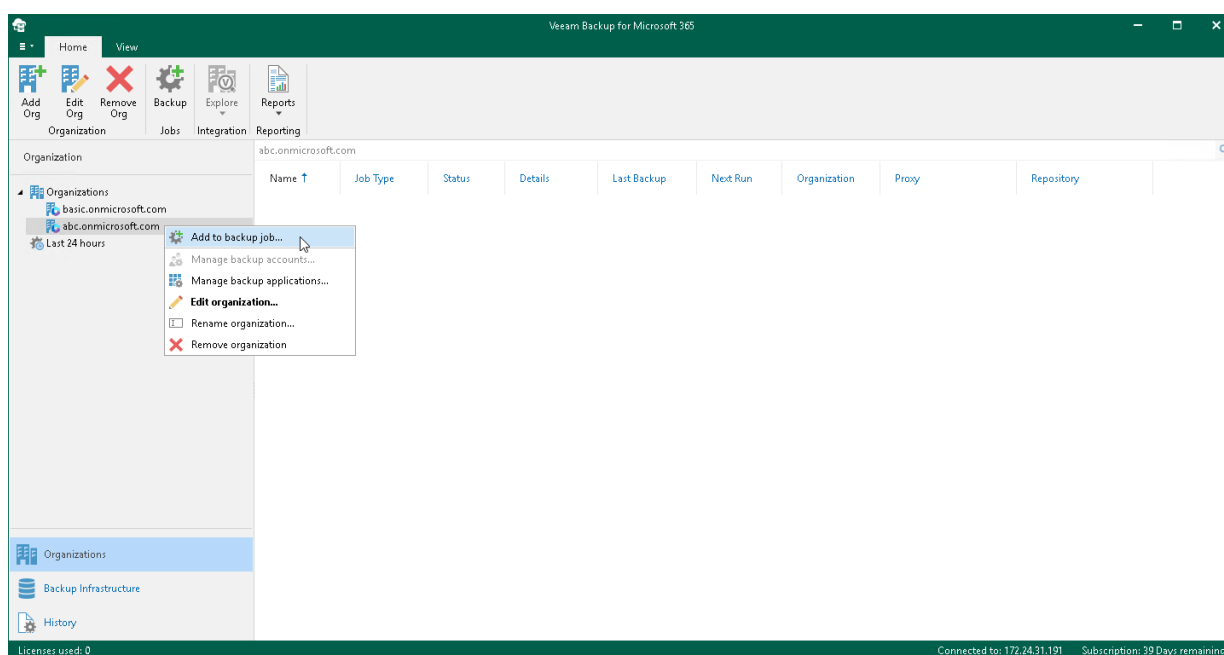
To create a backup job, do the following:

1. [Launch the New Backup Job wizard.](#)
2. [Specify a backup job name.](#)
3. [Select objects to back up.](#)
4. [Select objects to exclude.](#)
5. [Specify a backup proxy and repository.](#)
6. [Specify scheduling options.](#)

Step 1. Launch New Backup Job Wizard

To launch the **New Backup Job** wizard, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select an organization for which you want to create a backup job.
3. Do one of the following:
 - On the **Home** tab, click **Backup** on the ribbon.
 - Right-click an organization and select **Add to backup job**.



Step 2. Specify Backup Job Name

At this step of the wizard, enter a name for the backup job and provide optional description:

- 1. In the **Name** field, enter a name for the backup job.
- 2. In the **Description** field, enter optional description.

New Backup Job

Specify job name and description

Name:
Full Backup

Description:
Initial Backup

Next Cancel

Step 3. Select Objects to Back Up

At this step of the wizard, select objects that you want to back up.

In Veeam Backup for Microsoft 365, you can select to back up the entire organization or choose specific users, groups, sites, teams, and organizations.

Consider the following:

- You can create only one entire organization backup job per organization.
- Objects that are already added to the scope of any of your backup jobs will be skipped from the entire organization processing list.
- Due to possible access limitations some *Site* type objects may be unavailable.
- Starting from Veeam Backup for Microsoft 365 version 7 CP4 (build 7.0.0.3968), you can add the following objects for [Microsoft 365 organizations](#) with modern app-only authentication: *Public Folder Mailboxes* and *Discovery Search Mailboxes*. Backup of these objects in earlier versions of Veeam Backup for Microsoft 365 was not supported. For more information about additional permission and role that an Azure AD application needs to back up these objects, see [Permissions for Backup](#) and [Granting Global Reader Role to Azure AD Application](#).
- When you add an *Organization* object, [processing options](#) are applied to all users, groups and sites in the selected organization.

Back Up Entire Organization

To back up all objects within the selected Microsoft organization, select **Back up entire organization**. Veeam Backup for Microsoft 365 turns off team chats backup using Teams Export APIs to avoid unexpected costs incurred by Microsoft. Processing options for the entire organization cannot be configured.

Back Up Specific Objects

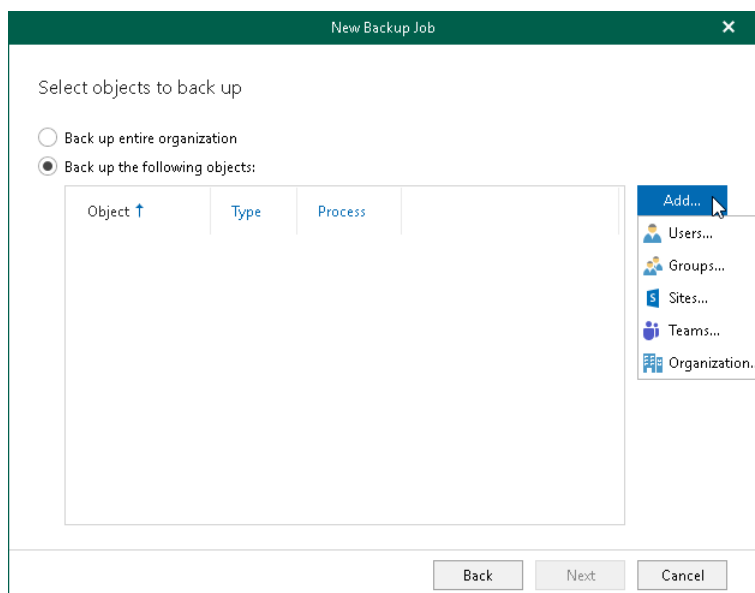
To back up specific users, groups, sites, teams, and organizations, do the following:

1. Select **Back up the following objects**.
2. Click **Add** and select one of the following options: [Users](#), [Groups](#), [Sites](#), [Teams](#), or [Organization](#).

If you set up Veeam Backup for Microsoft 365 to use Teams Export APIs for Microsoft 365 organizations, you can enable team chats backup using Teams Export APIs in processing options for [Teams](#) and [Organization](#).

NOTE

If you select a group, site or team as an individual object for backup (and not as a part of a user account, group or organization), this object does not consume a unit from the Veeam license.



Configuring Users Backup

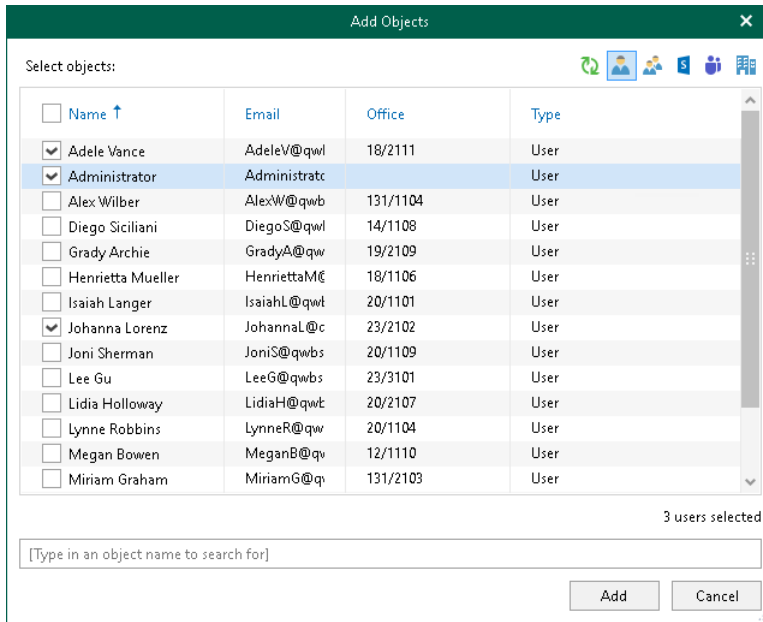
TIP

Consider the following:

- To switch between objects of different types, you can click the buttons in the upper-right corner.
- To refresh the objects list, you can click **Refresh**.
- To quickly find necessary objects, you can use the search field at the bottom.

To configure *Users* backup, do the following:

1. In the **Add Objects** window, select check boxes next to the users that you want to back up.

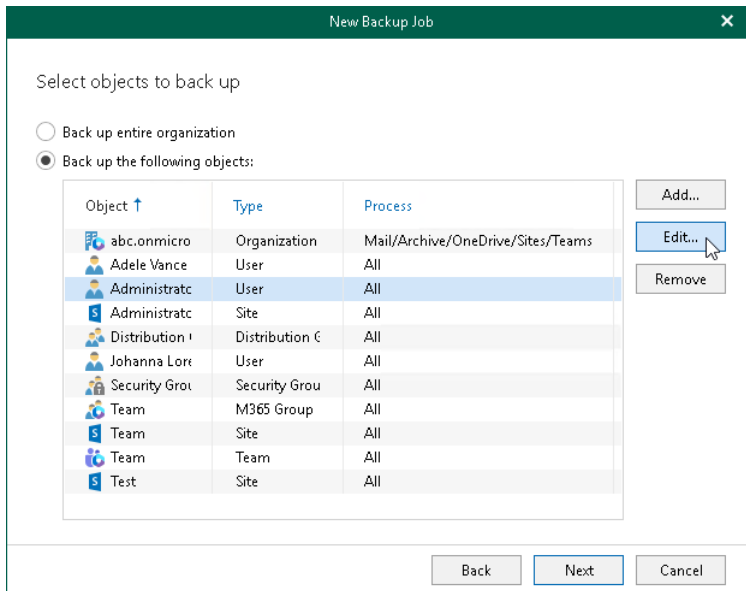


2. Click **Add**.

The selected objects appear in the list of objects to back up.

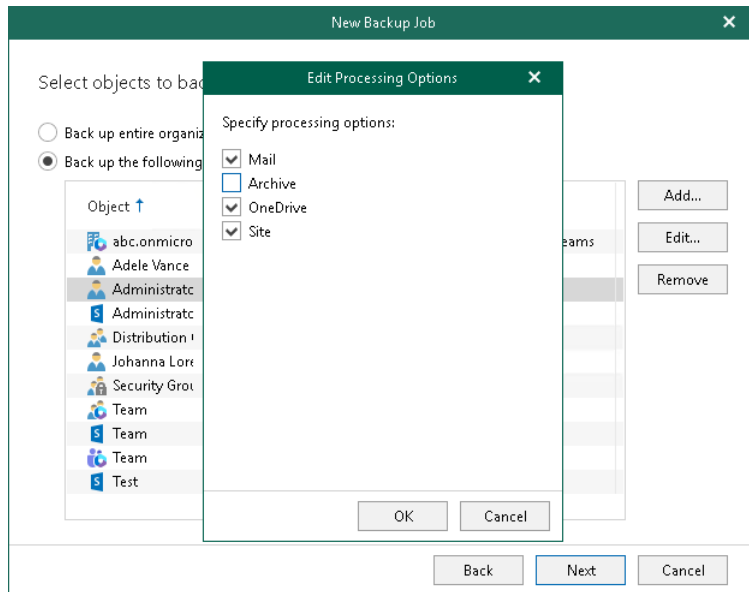
3. If you want to specify processing options, select the necessary *User* type object and click **Edit**.

Keep in mind that you cannot edit processing options for the *Public Mailbox* objects.



- In the **Edit Processing Options** window, select check boxes next to the processing options that you want to apply, and click **OK**.

For more information about available *User*types and their processing options, see [Organization Object Types](#).



Configuring Groups Backup

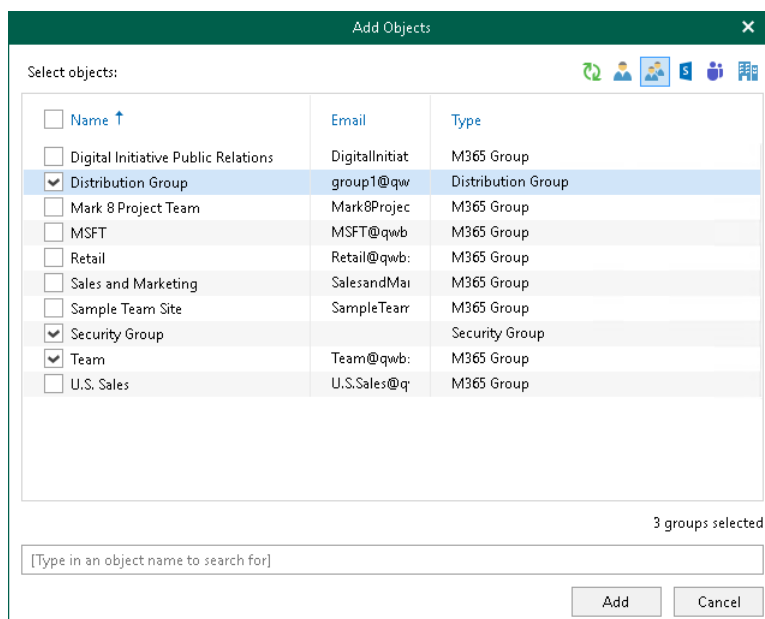
TIP

Consider the following:

- To switch between objects of different types, you can click the buttons in the upper-right corner.
- To refresh the objects list, you can click **Refresh**.
- To quickly find necessary objects, you can use the search field at the bottom.

To configure *Groups* backup, do the following:

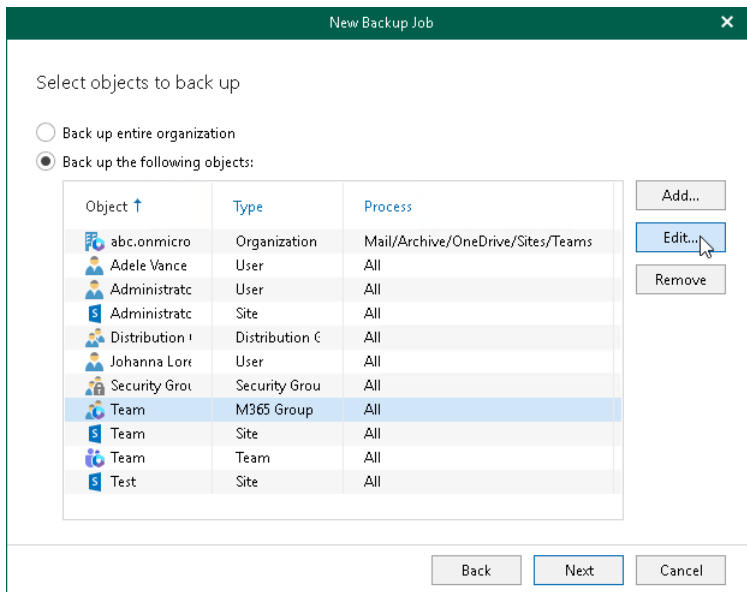
- In the **Add Objects** window, select check boxes next to the groups that you want to back up.



2. Click **Add**.

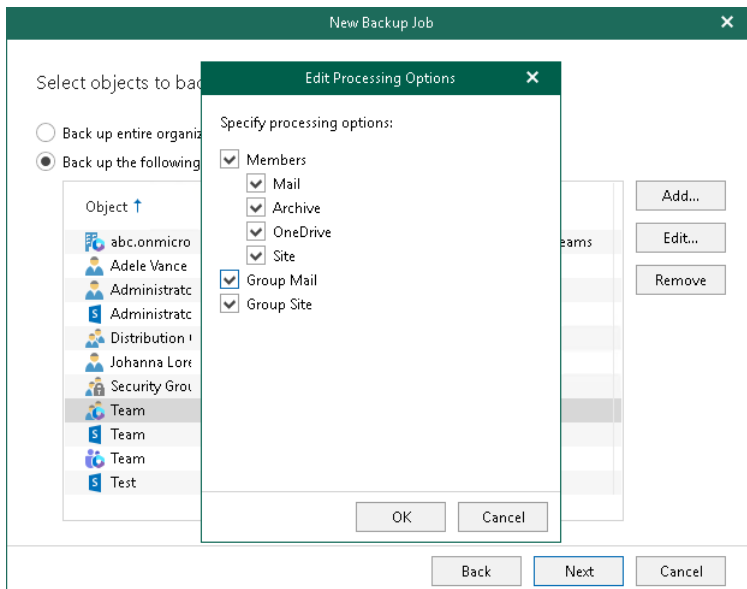
The selected objects appear in the list of objects to back up.

3. If you want to specify processing options, select the necessary *Group* type object and click **Edit**.



4. In the **Edit Processing Options** window, select check boxes next to the processing options that you want to apply, and click **OK**.

For more information about available *Group* types and their processing options, see [Organization Object Types](#).



Configuring Sites Backup

TIP

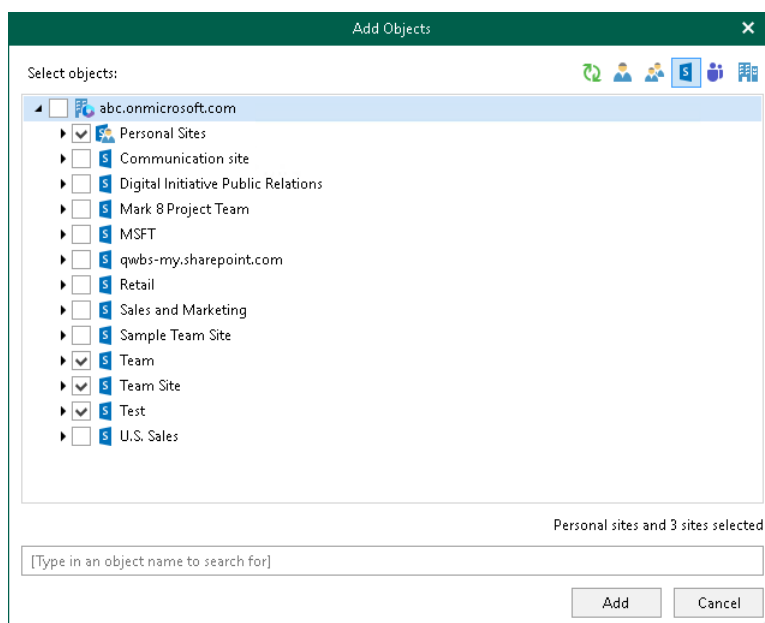
Consider the following:

- To switch between objects of different types, you can click the buttons in the upper-right corner.
- To refresh the objects list, you can click **Refresh**.
- To quickly find necessary objects, you can use the search field at the bottom. Search is available only for personal sites and subsites displayed in the objects tree.

To configure *Sites* backup, do the following:

1. In the **Add Objects** window, select check boxes next to the sites or subsites that you want to back up.

Keep in mind that you need to expand the **Personal Sites** node or a node of a parent site to view all personal sites or subsites.



2. Click **Add**.

The selected objects appear in the list of objects to back up.

Keep in mind that you cannot edit processing options for the *Site* type objects. For more information about the *Site* type, see [Organization Object Types](#).

Configuring Teams Backup

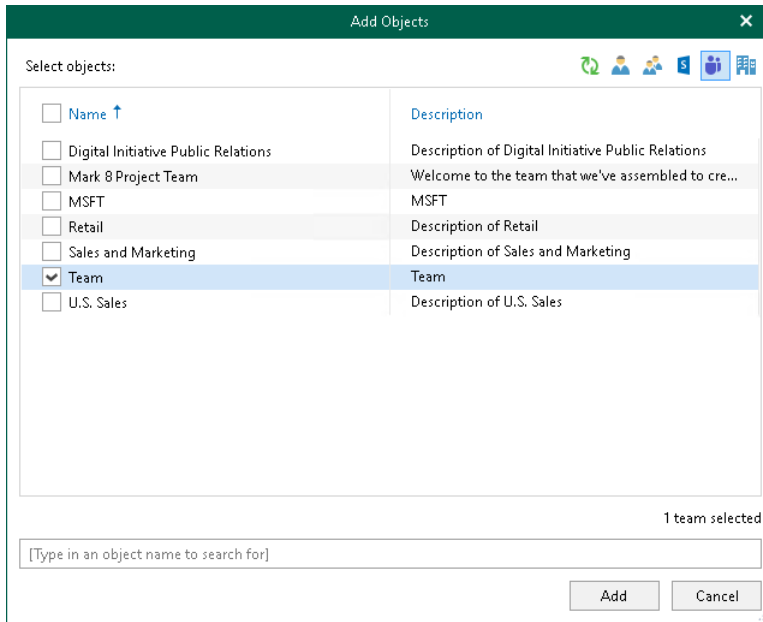
TIP

Consider the following:

- To switch between objects of different types, you can click the buttons in the upper-right corner.
- To refresh the objects list, you can click **Refresh**.
- To quickly find necessary objects, you can use the search field at the bottom.

To configure *Teams* backup, do the following:

1. In the **Add Objects** window, select check boxes next to the teams that you want to back up.



2. Click **Add**.

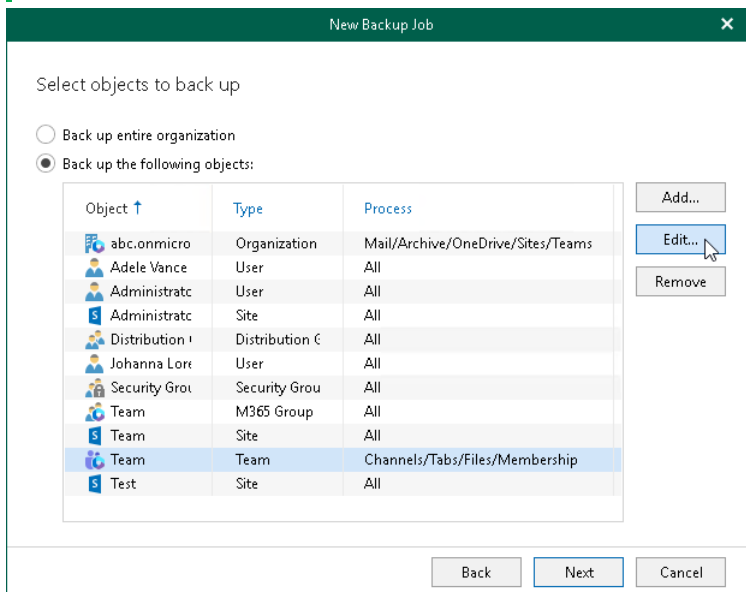
The selected objects appear in the list of objects to back up.

3. If you want to specify processing options, select the necessary *Team* type object and click **Edit**.

NOTE

You can edit processing options for the *Team* type objects only if you set up Veeam Backup for Microsoft 365 to use Teams Export APIs for team chats backup.

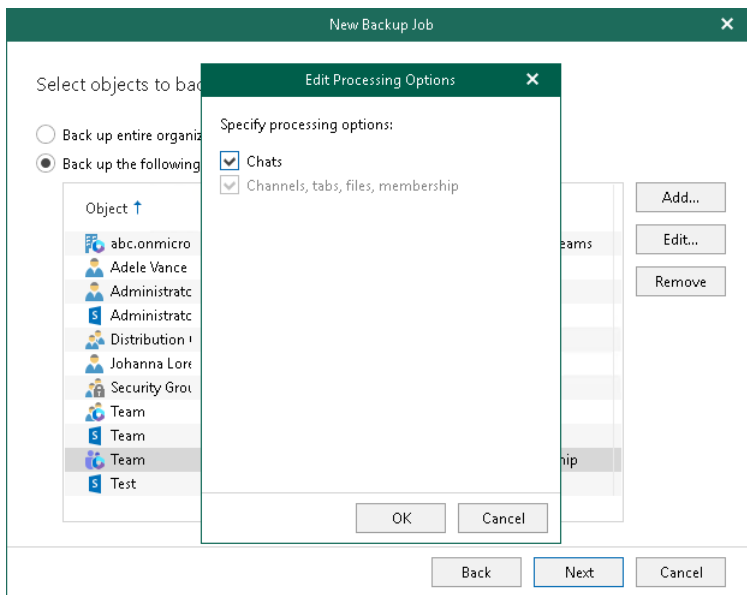
For more information, see [Getting Started with Teams Export APIs](#).



4. In the **Edit Processing Options** window, select check boxes next to the processing options that you want to apply, and click **OK**.

For more information about the *Team* type and its processing options, see [Organization Object Types](#).

Keep in mind that the **Chats** check box is available for editing only if you selected the **Teams chats** check box when adding a Microsoft 365 organization with modern app-only authentication.



Configuring Organization Backup

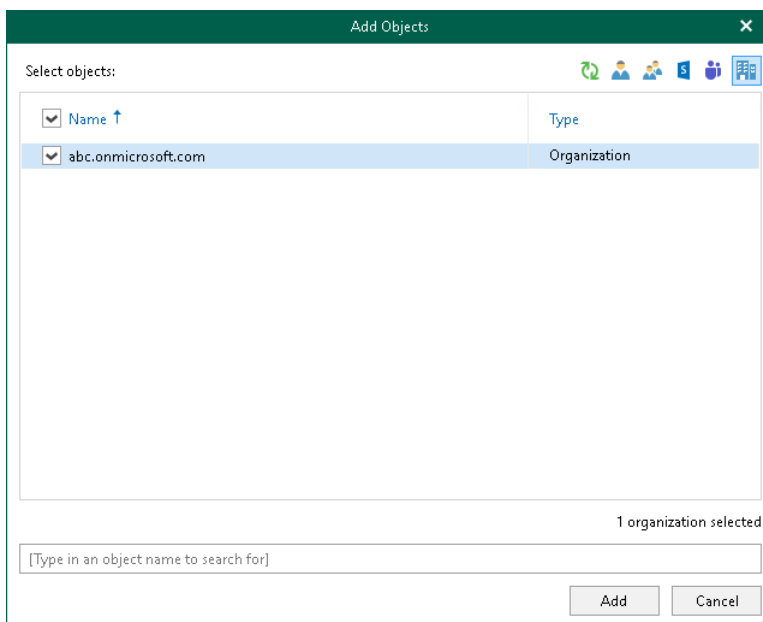
TIP

Consider the following:

- To switch between objects of different types, you can click the buttons in the upper-right corner.
- To refresh the objects list, you can click **Refresh**.
- To quickly find necessary objects, you can use the search field at the bottom.

To configure *Organization* backup, do the following:

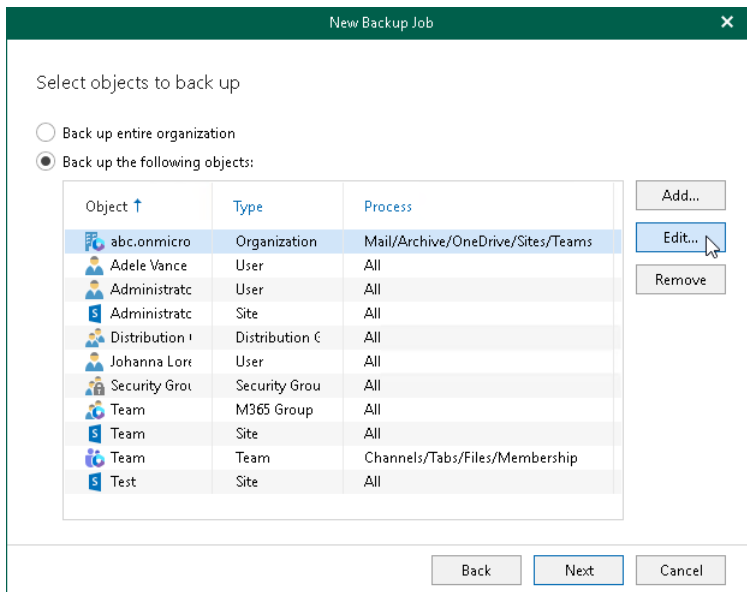
1. In the **Add Objects** window, select check boxes next to the organizations that you want to back up.



2. Click **Add**.

The selected objects appear in the list of objects to back up.

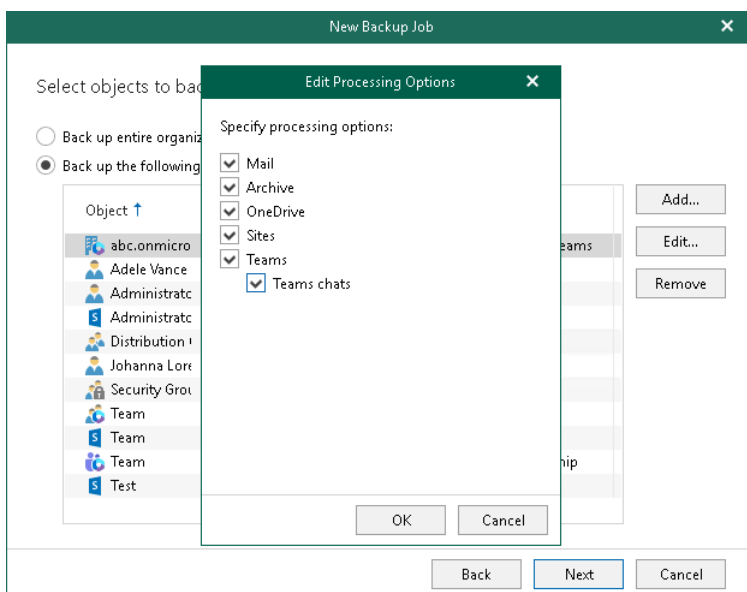
3. If you want to specify processing options, select the necessary *Organization* type object and click **Edit**.



4. In the **Edit Processing Options** window, select check boxes next to the processing options that you want to apply, and click **OK**.

For more information about the *Organization* type and its processing options, see [Organization Object Types](#).

Keep in mind that the **Teams chats** check box is displayed only if you set up Veeam Backup for Microsoft 365 to use Teams Export APIs for team chats backup. This check box is available for editing only if you selected the **Teams chats** check box when adding a Microsoft 365 organization with modern app-only authentication.



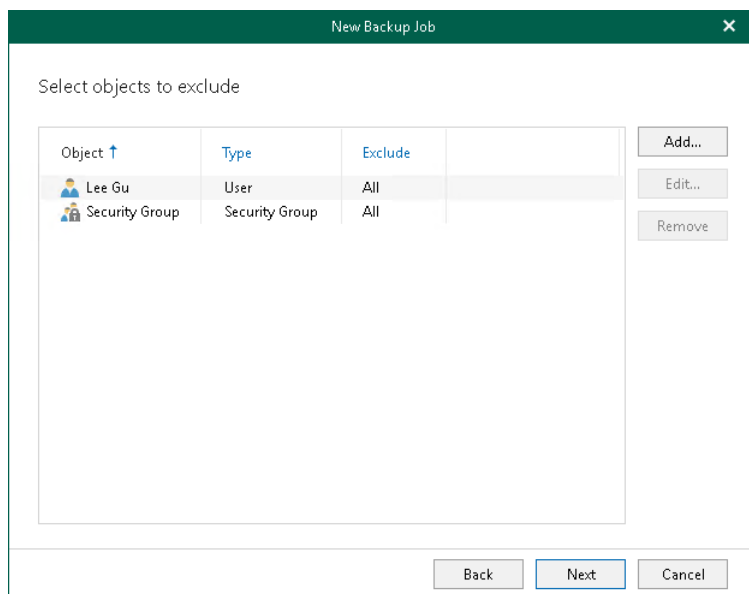
Step 4. Select Objects to Exclude

At this step of the wizard, select objects that you do not want to back up.

To exclude an object, click **Add** and select users, groups, sites, and teams that you do not want to back up.

NOTE

Starting from Veeam Backup for Microsoft 365 version 7 CP4 (build 7.0.0.3968), you can add the following objects for [Microsoft 365 organizations](#) with modern app-only authentication: *Public Folder Mailboxes* and *Discovery Search Mailboxes*. Backup of these objects in earlier versions of Veeam Backup for Microsoft 365 was not supported. For more information about additional permission and role that an Azure AD application needs to back up these objects, see [Permissions for Backup](#) and [Granting Global Reader Role to Azure AD Application](#).



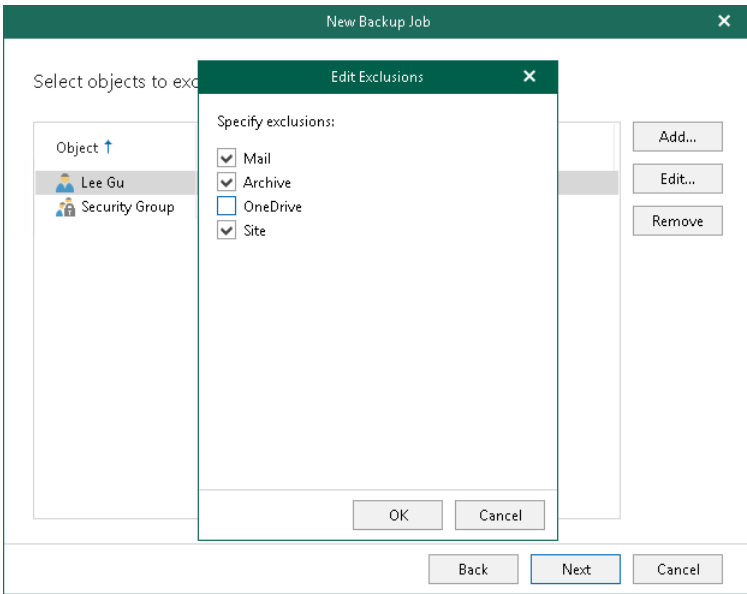
If you want to specify exclusion options, select an object in the list, click **Edit** and in the **Edit Exclusions** window, select exclusion options that you want to apply.

For more information about available object types and their exclusion options, see [Organization Object Types](#).

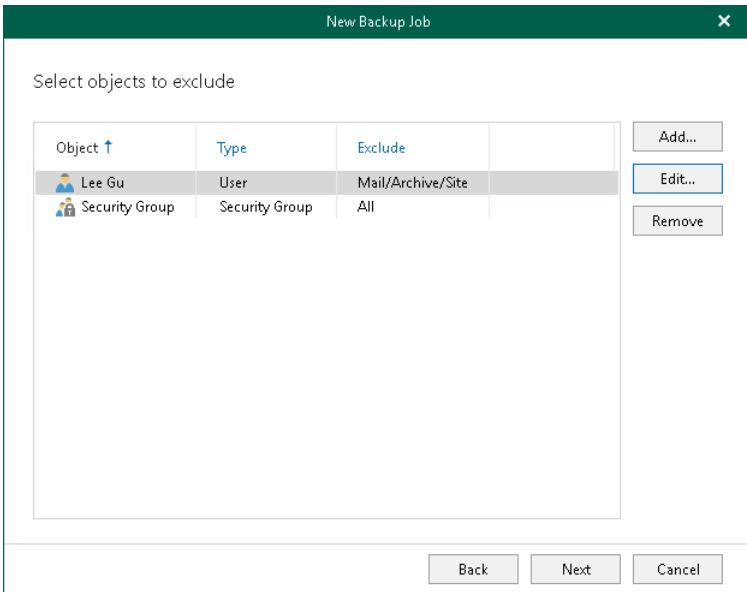
NOTE

You cannot edit exclusion options for the *Sites*, *Teams* and *Public Mailbox* objects.

The following is an example where the *Mail*, *Archive* and *Site* are excluded from the backup for the selected user. Veeam Backup for Microsoft 365 will only back up *OneDrive* data for this user.



To see what Veeam Backup for Microsoft 365 will exclude for the selected object to exclude, refer to the **Exclude** column. In this example, Veeam Backup for Microsoft 365 will exclude *Mail*, *Archive* and *Site*.



Step 5. Specify Backup Proxy and Repository

At this step of the wizard, specify a [backup proxy server](#) that you want to use to process data during a backup job session and a [backup repository](#) where you want to store your backups.

To specify a backup proxy server and backup repository, do the following:

1. From the **Backup proxy** drop-down list, select a backup proxy server that you want to use to process data during a backup job session.
2. From the **Backup repository** drop-down list, select a backup repository to which you want to save your data.

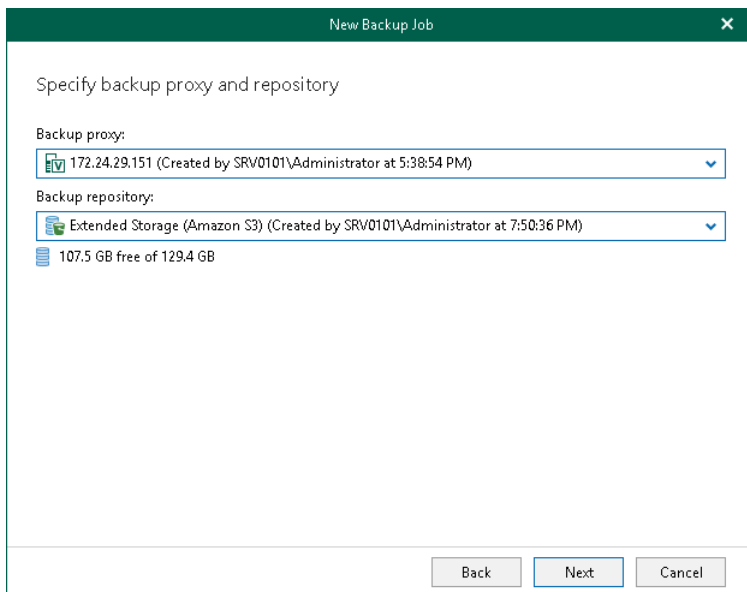
You can select a JET-based backup repository or backup repository that was [extended with object storage](#).

If you selected an extended backup repository, all data will be compressed and backed up directly to object storage; Veeam Backup for Microsoft 365 saves only [cache](#) to the extended backup repository.

NOTE

Consider the following:

- If you want to extend a backup job with backup copy capabilities, you must specify an [extended backup repository](#).
- Backup repositories extended with Azure Blob Storage Archive access tier and all Amazon S3 Glacier storage classes are not listed.



Step 6. Specify Scheduling Options

At this step of the wizard, configure a schedule for your backup job and actions that will be performed after completion of the wizard.

To configure a schedule, do the following:

1. If you want Veeam Backup for Microsoft 365 to run your backup job automatically in accordance with the schedule, select the **Run the job automatically** check box and customize a schedule. You can select one of the following options:
 - **Daily at this time.** Select this option if you want to run the job on the specified days at the specified hours. Keep in mind that the *Workdays* option means that Veeam Backup for Microsoft 365 will run the job every day from Monday to Friday at the specified time.
 - **Periodically every.** Select this option if you want to run the job every *N* minutes or hours. If you select the period in hours, click **Schedule** and specify allowed and prohibited hours for the backup job to run. For more information, see [Selecting Time Periods](#).
2. Select the **Retry failed objects processing** check box and specify the maximum number of retry attempts. You can also set an interval between subsequent retries.
3. Select the **Terminate the job if it exceeds allowed backup window** check box, click **Window** and specify allowed and prohibited hours for the backup job. For more information, see [Selecting Time Periods](#).
4. In the **When I click Create** section, do the following:
 - a. Select the **Start the job** check box if you want to start a backup job right after completion of the wizard.

If you do not want to start the job immediately, you can start it later. For more information, see [Starting Backup Job](#).
 - b. Select the **Create a backup copy for this job** check box if you want to configure creating backup copies.

Right after you click **Create**, you will be taken to the [Select Target Backup Repository](#) step of the **New Backup Copy Job** wizard.

Keep in mind that this check box is available only if the following conditions are met:

 - You have specified a [backup repository that was extended with object storage](#) to store your backups.

- You have added at least one more extended backup repository to the Veeam Backup for Microsoft 365 backup infrastructure. For more information, see [Backup Repositories](#) and [Backup Copy](#).

If you do not want to configure a backup copy job immediately, you can launch the **New Backup Copy Job** wizard later. For more information, see [Launch New Backup Copy Job Wizard](#).

The screenshot shows the 'New Backup Job' dialog box with the following settings:

- Run the job automatically
 - Daily at this time: 2:00 AM, Everyday
 - Periodically every: 5 minutes, Schedule...
- Retry failed objects processing: 3 times
 - Wait before each retry attempt for: 10 minutes
- Terminate the job if it exceeds allowed backup window, Window...
- When I click Create:
 - Start the job
 - Create a backup copy for this job

Buttons at the bottom: Back, Create, Cancel.

Selecting Time Periods

When you click **Schedule** or **Window**, the **Time Periods** dialog appears in which you can:

- Set the **Permitted** execution time frame for the backup job.
- Set the **Denied** execution time frame for the backup job.
- [In the **Schedule** window only] Specify a number of minutes for which you want to shift starting of the backup job within an hour if several backup jobs are scheduled to be started simultaneously. Using this option allows you to decrease the load on the Veeam Backup for Microsoft 365 backup infrastructure.

The main area of the dialog is divided into two axes:

- The vertical axis represents days of the week from Sunday to Saturday.
- The horizontal axis represents time intervals from 12 AM to 11:59 PM.

Within these axes a matrix is placed consisting of blocks. Each block represents a 59 minutes interval for each day of the week. The total number of blocks is 168 (24 blocks per each day of the week).

To set up an execution frame for the backup job, do the following:

1. Select a block that corresponds to the day of the week (vertical axis) and to the time interval (horizontal axis) on which you want to allow or prohibit the execution of a backup job.

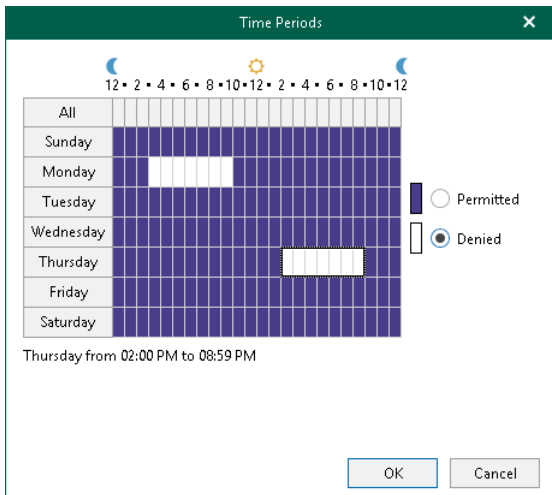
In addition, you can:

- a. Select multiple blocks simultaneously by clicking and holding the mouse pointer on the first block and dragging it until the last one that you want to use, including different days of the week.
- b. Click a day of the week in the vertical axis to select all the blocks of the day.
- c. Click **All** in the vertical axis to select all the blocks of the entire week.

2. On the right-hand side, select either the **Permitted** or **Denied** option to set up the execution rule for the selected blocks.

The following is an example in which it is prohibited to run a backup job on the following days of the week:

- Monday from 03:00 AM up until 09:59 AM.
- Thursday from 02:00 PM up until 08:59 PM.



Managing Backup Jobs

You can manage backup jobs that you created in Veeam Backup for Microsoft 365. For example, you can edit the settings of a backup job, start, stop, disable, remove backup jobs, explore backups created by backup jobs.

Starting Backup Job

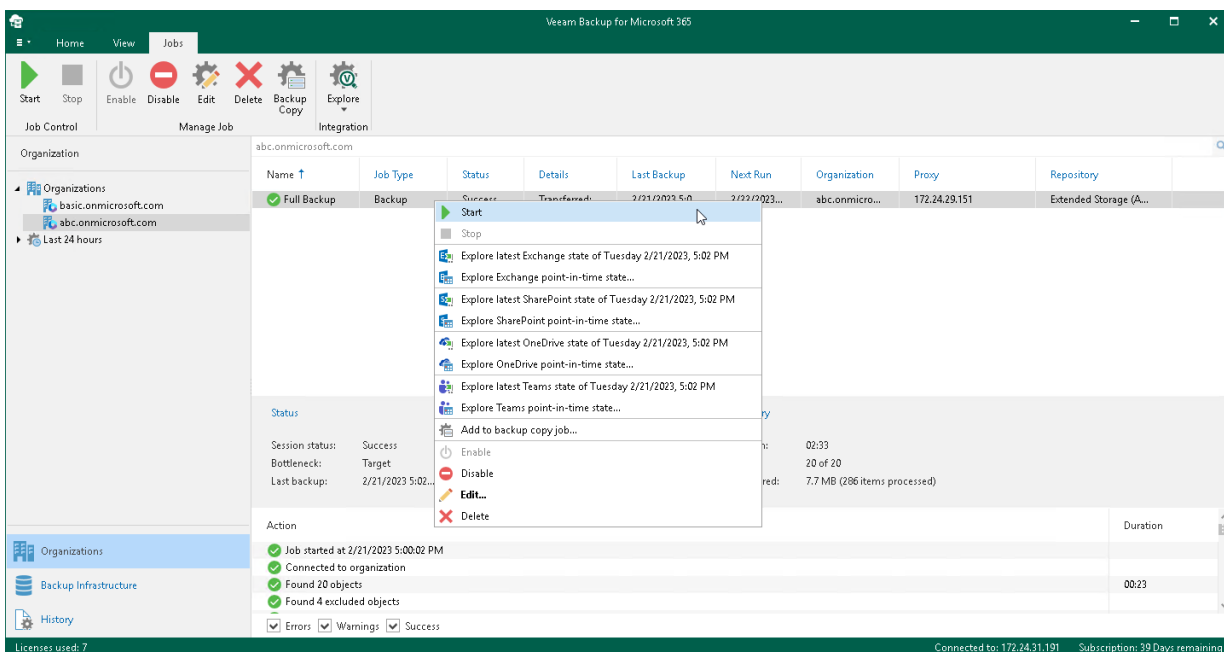
To start a backup job, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select an organization.

TIP

You can also select the root **Organizations** node to see all backup and backup copy jobs that were created for all organizations added to the scope.

3. In the preview pane, do one of the following:
 - Select a backup job and click **Start** on the ribbon.
 - Right-click a backup job and select **Start**.



Stopping Backup Job

When Veeam Backup for Microsoft 365 stops a backup job, it preserves the data that has already been backed up. If you want to continue, use the **Start** command. For more information, see [Starting Backup Job](#).

Keep in mind that when you restart the backup job, Veeam Backup for Microsoft 365 starts data processing from the beginning and may need additional time to re-identify the state of the backed-up data. After that Veeam Backup for Microsoft 365 continues with the remaining data to back up.

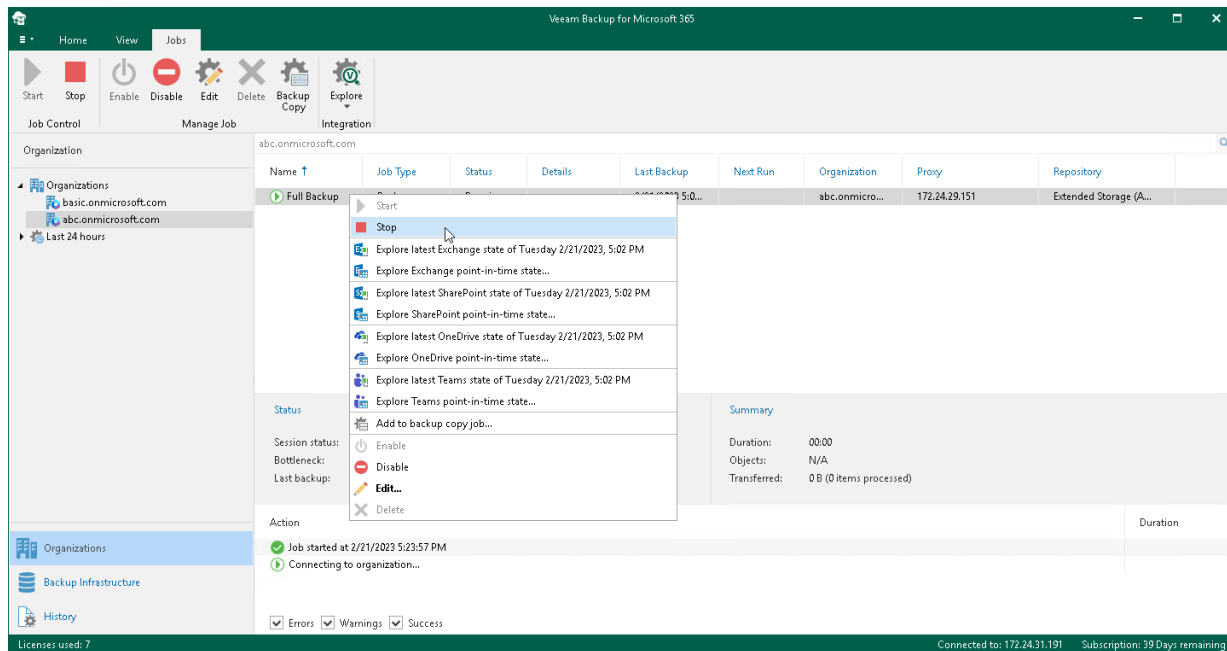
To stop a backup job, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select an organization.

TIP

You can also select the root **Organizations** node to see all backup and backup copy jobs that were created for all organizations added to the scope.

3. In the preview pane, do one of the following:
 - Select a backup job and click **Stop** on the ribbon.
 - Right-click a backup job and select **Stop**.



Enabling or Disabling Backup Job

You can enable or disable a backup job.

Consider the following:

- If a backup job is enabled, it can be executed on schedule.
- If a backup job is disabled, it cannot be executed on schedule but you can run it manually using the **Start** command. For more information, see [Starting Backup Job](#).

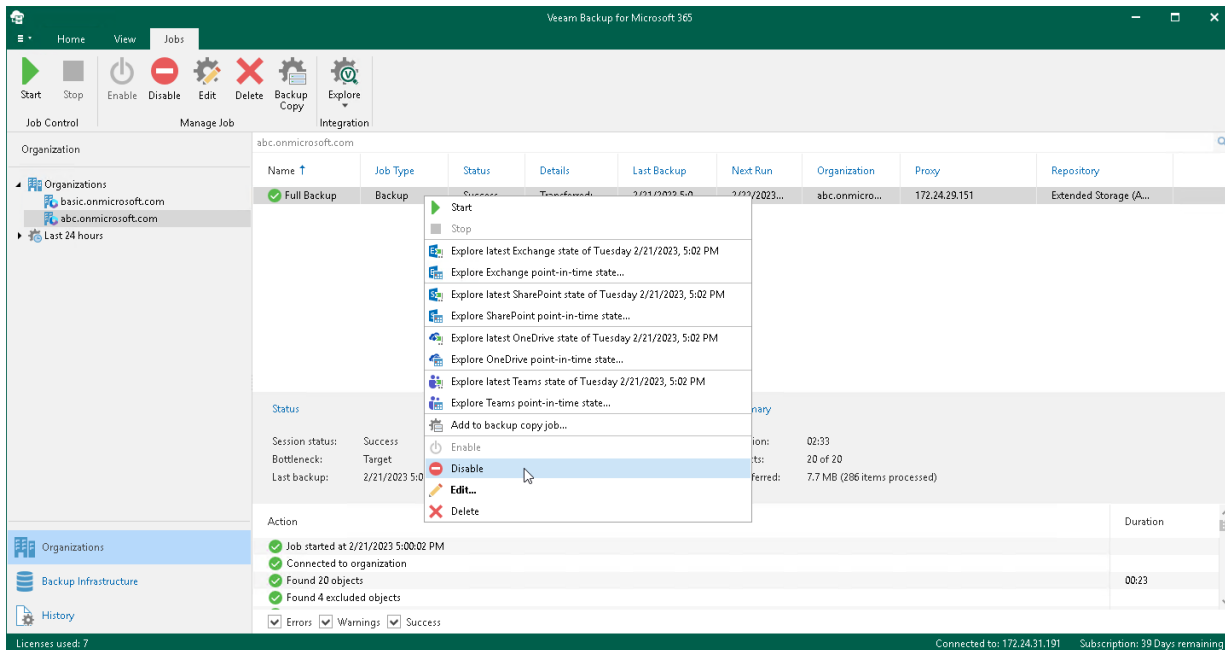
To enable or disable a backup job, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select an organization.

TIP

You can also select the root **Organizations** node to see all backup and backup copy jobs that were created for all organizations added to the scope.

3. In the preview pane, do one of the following:
 - Select a backup job and click **Enable** or **Disable** on the ribbon.
 - Right-click a backup job and select **Enable** or **Disable**.



Editing Backup Job Settings

Veeam Backup for Microsoft 365 allows you to edit a backup job settings.

To edit settings of a backup job, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select an organization.

TIP

You can also select the root **Organizations** node to see all backup and backup copy jobs that were created for all organizations added to the scope.

3. In the preview pane, do one of the following:
 - Select a backup job and click **Edit** on the ribbon.
 - Right-click a backup job and select **Edit**.
4. Modify the required settings.

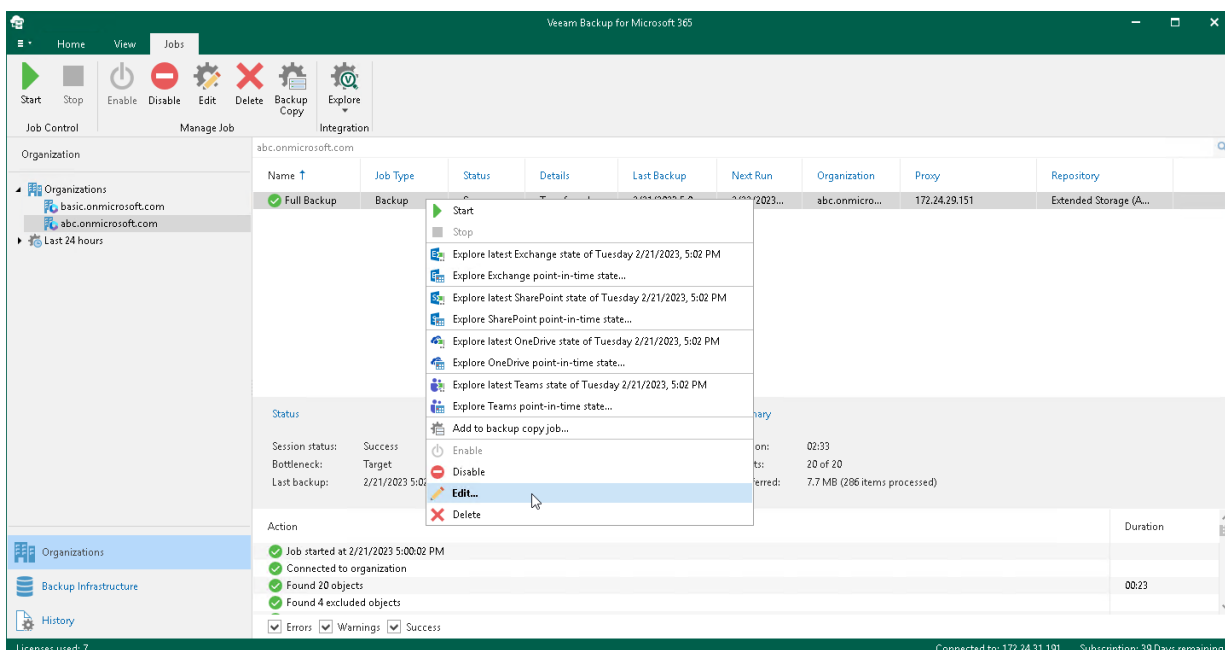
You can change the following parameters:

- The name and description of a backup job.
- The list of objects to back up and their processing options.
- The list of objects to exclude and their exclusion options.

Also, you can select another backup proxy server and backup repository, and reconfigure a backup job scheduling options.

NOTE

You cannot select another backup proxy server and backup repository with a different retention type if you edit a backup job for which a backup copy job is already created.



Removing Backup Job

You can remove a backup job from the Veeam Backup for Microsoft 365 configuration.

NOTE

Consider the following:

- When you remove a backup job, Veeam Backup for Microsoft 365 keeps the backup data in the backup location.
- When you remove a backup job, Veeam Backup for Microsoft 365 removes a backup copy job as well if such job was created for a backup job.

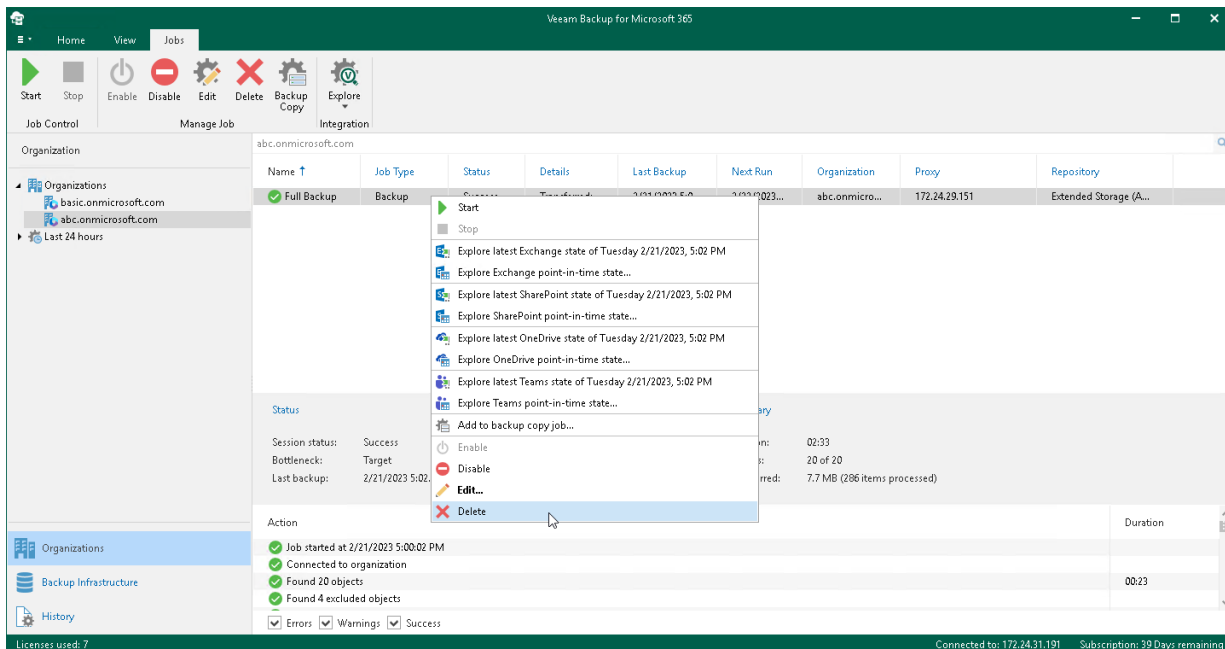
To remove a backup job from the Veeam Backup for Microsoft 365 configuration, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select an organization.

TIP

You can also select the root **Organizations** node to see all backup and backup copy jobs that were created for all organizations added to the scope.

3. In the preview pane, do one of the following:
 - Select a backup job and click **Delete** on the ribbon.
 - Right-click a backup job and select **Delete**.



Exploring Backup Job

You can open backups created by a backup job.

To open backups created by a backup job, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select an organization.

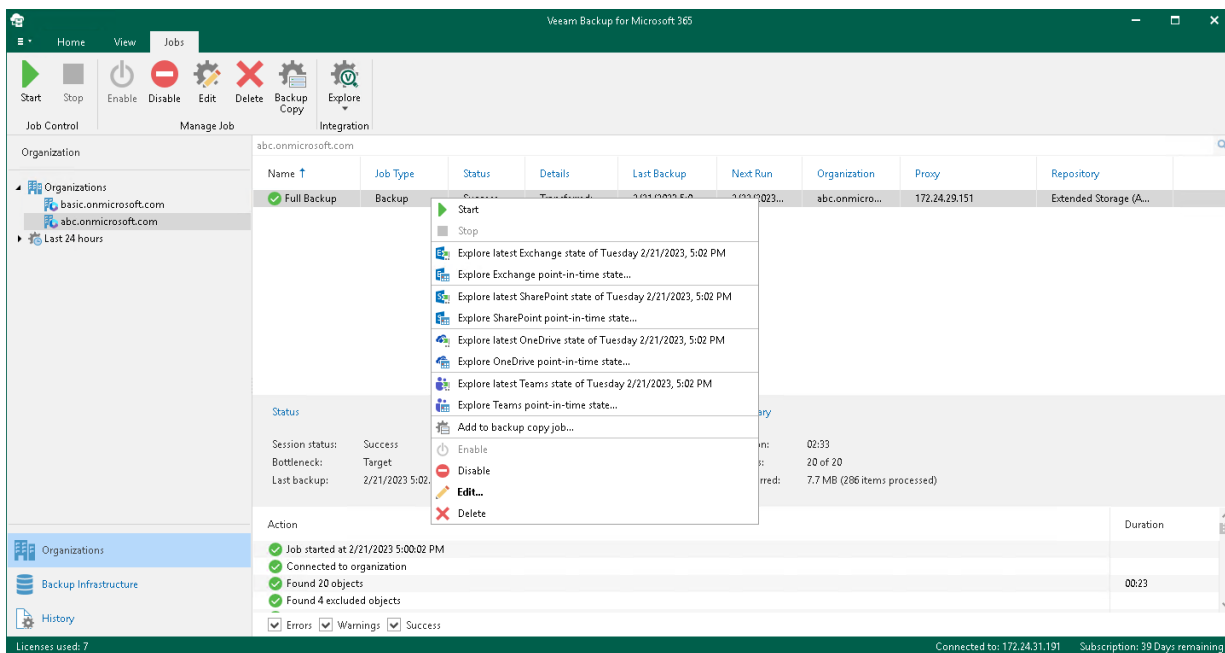
TIP

You can also select the root **Organizations** node to see all backup and backup copy jobs that were created for all organizations added to the scope.

3. In the preview pane, do one of the following:
 - Select a backup job and click **Explore** on the ribbon and then select **Explore latest <product> state of <date_and_time>** or **Explore <product> point-in-time state**.
 - Right-click a backup job and select **Explore latest <product> state of <date_and_time>** or **Explore <product> point-in-time state**.

where **<product>** is one of the following services: *Exchange*, *SharePoint*, *OneDrive*, or *Teams*.

4. Proceed to [Data Restore](#).



Backup Copy

To enhance protection of your data against disasters, you can extend your backup jobs with backup copy capabilities. With backup copy, you can transfer backups created by backup jobs from a source backup repository to target backup repository for long-term storage.

Both source and target backup repositories for backup copy must be [extended with object storage](#) and located on the same backup proxy server and have the same retention type. For more information on how to extend a backup repository with object storage, see [Specify Object Storage](#).

NOTE

Veeam Backup for Microsoft 365 does not support JET-based backup repositories as source or target backup repositories for backup copy. For more information, see [JET-Based Backup Repositories](#).

As well as backup, backup copy is a job-driven process. You can create a backup copy job right after configuring a backup job or at any time later. Keep in mind that an extended backup repository that you configure as a target for your backup job becomes a source backup repository for backup copies. A target backup repository to store backup copies must be specified when you configure a backup copy job. For more information, see [Creating Backup Copy Job](#).

The following table lists cloud and on-premises storage systems that Veeam Backup for Microsoft 365 supports as a source and target for backup copy jobs.

	Source for backup copy	Target for backup copy
Azure Blob Storage Hot access tier	✓	✓
Azure Blob Storage Cool access tier	✓	✓
Azure Blob Storage Archive access tier		✓
Amazon S3 Standard storage class	✓	✓
Amazon S3 Standard-Infrequent Access storage class	✓	✓
Amazon S3 Glacier Instant Retrieval storage class		✓
Amazon S3 Glacier Flexible Retrieval storage class		✓
Amazon S3 Glacier Deep Archive storage class		✓

	Source for backup copy	Target for backup copy
S3 Compatible object storage (if applicable)	✓	✓

Storage format of backup copies differs from storage format of backups: maximum size of blob files increases from 5 MB for backups to 256 MB for backup copies. Repacking of backed-up data is performed by either Veeam Backup for Microsoft 365 backup proxy or an auxiliary archiver appliance that Veeam Backup for Microsoft 365 can create in Microsoft Azure or Amazon EC2. Processing larger blobs helps you reduce costs incurred by your cloud storage provider for retrieving backed-up data from backup copies.

Veeam Backup for Microsoft 365 allows you to protect data in backup copies from loss as a result of attacks, malware activity or other injurious actions that may be performed by 3rd party applications. For more information about protecting data in backup copies, see [Immutability](#).

Getting Started with Backup Copy

In general, the process of creating backup copies in Veeam Backup for Microsoft 365 involves the following steps:

1. [Planning and preparation.](#)

You can skip this step in whole or in part if necessary backup infrastructure components are already added to Veeam Backup for Microsoft 365.

2. [Creating a backup job.](#)

3. [Creating a backup copy job.](#)

After Veeam Backup for Microsoft 365 created backup copies, you can explore and restore, or retrieve backup copies. For more information, see [What You Do with Backup Copies](#).

Planning and Preparation

Before you start creating a backup copy job to protect your backups, you must perform the following actions in the Veeam Backup for Microsoft 365 backup infrastructure:

1. Add object storage to Veeam Backup for Microsoft 365. Do the following:
 - a. Add object storage where you want to store your backups.
 - b. Add object storage that you want to use as a target for backup copy jobs.

For more information, see [Object Storage Usage Scenarios](#) and [Adding Object Storage](#).

NOTE

Azure Blob Storage Archive access tier, Amazon S3 Glacier Instant Retrieval, Amazon S3 Glacier Flexible Retrieval and Amazon S3 Glacier Deep Archive storage classes are supported only to store backup copies. For more information, see [Adding Amazon S3 Object Storage](#) and [Adding Microsoft Azure Blob Storage](#).

2. Add extended backup repositories to Veeam Backup for Microsoft 365. Do the following:
 - a. Add a backup repository extended with object storage where you want to store your backups. You will use this backup repository as a target for your backup jobs.
 - b. Add a backup repository extended with object storage where you want to store your backup copies. You will use this backup repository as a target for your backup copy jobs.

For more information, see [Extended Backup Repositories](#) and [Adding Backup Repositories](#).

NOTE

An extended backup repository where you store your backups and a backup repository where you store backup copies must be located on the same backup proxy server and have the same retention type.

Creating Backup Job

Create a backup job. In the backup job settings, specify the extended backup repository where you want to store your backups. For more information, see [Specify Backup Proxy and Repository](#).

Creating Backup Copy Job

Create a backup copy job for the backup job created at the [Creating Backup Job](#) step. In the backup copy job settings, specify the target repository where Veeam Backup for Microsoft 365 will copy your backed-up data. For more information, see [Select Target Backup Repository](#).

What You Do with Backup Copies

After Veeam Backup for Microsoft 365 created backup copies, you can do the following:

- Retrieve your backup copies.

Retrieving backed-up data from backup copies is required before data explore and restore if Veeam Backup for Microsoft 365 stores this data in backup repositories extended with Azure Blob Storage Archive access tier, Amazon S3 Glacier Flexible Retrieval, or Amazon S3 Glacier Deep Archive storage classes. For more information, see [Retrieving Backed-Up Data](#), [Exploring Retrieved Data](#) and [Data Restore](#).

NOTE

If you store backup copies in a backup repository extended with Amazon S3 Glacier Instant Retrieval storage class, you can explore and restore your backed-up data directly from the repository. You do not need to retrieve backed-up data from this repository.

- Explore and restore backup copies.

You can start exploring and restoring data at any time you want if you have copied your backed-up data to a backup repository extended with the following object storage:

- Azure Blob Storage Hot/Cool access tier
- Amazon S3 Standard storage class
- Amazon S3 Standard-Infrequent Access storage class
- Amazon S3 Glacier Instant Retrieval storage class
- S3 Compatible object storage

For more information, see [Exploring Backup Copies](#) and [Data Restore](#).

NOTE

You cannot explore and restore both the retrieved backed-up data and backup copies using Restore Portal.

Creating Backup Copy Job

To create a backup copy job, do the following:

1. [Launch the New Backup Copy Job wizard.](#)
2. [Select a target backup repository.](#)
3. [Specify scheduling options.](#)

Step 1. Launch New Backup Copy Job Wizard

NOTE

Backup copy capabilities are only available if you have specified an [extended backup repository](#) as a target for your backup jobs. For more information, see [Specify Backup Proxy and Repository](#).

To launch the **New Backup Copy Job** wizard, do the following:

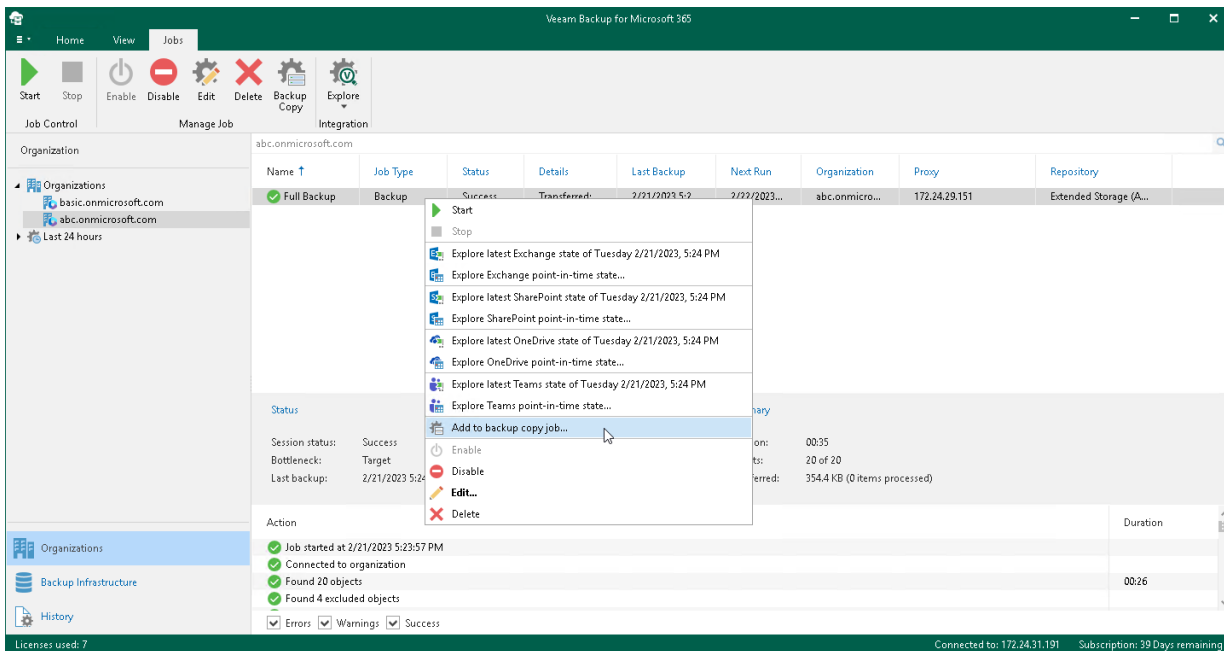
1. Open the **Organizations** view.
2. In the inventory pane, select an organization.

TIP

You can also select the root **Organizations** node to see all backup and backup copy jobs that were created for all organizations added to the scope.

3. In the preview pane, do one of the following:
 - Select a backup job for which you want to create a backup copy job and click **Backup Copy** on the ribbon.
 - Right-click a backup job and select **Add to backup copy job**.

Keep in mind that you can create only one backup copy job per backup job.



Step 2. Select Target Backup Repository

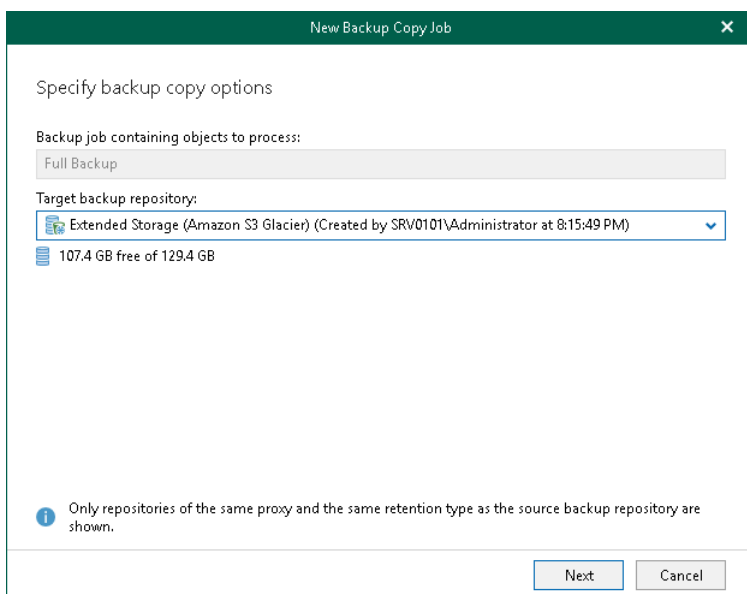
At this step of the wizard, specify an extended backup repository that you want to use as a target for the backup copy job.

NOTE

An extended backup repository where you store your backups and a target backup repository must be located on the same backup proxy server and have the same retention type.

To specify a target backup repository, do the following:

1. In the **Backup job containing objects to process** field, check the backup job name.
2. From the **Target backup repository** drop-down list, select a target backup repository to which you want to copy your backed-up data.



The screenshot shows a dialog box titled "New Backup Copy Job" with a close button (X) in the top right corner. The main heading is "Specify backup copy options". Below this, there are two sections:

- Backup job containing objects to process:** A text field containing "Full Backup".
- Target backup repository:** A dropdown menu showing "Extended Storage (Amazon S3 Glacier) (Created by SRV0101\Administrator at 8:15:49 PM)" with a downward arrow. Below the dropdown, it indicates "107.4 GB free of 129.4 GB".

At the bottom left, there is a blue information icon (i) followed by the text: "Only repositories of the same proxy and the same retention type as the source backup repository are shown." At the bottom right, there are two buttons: "Next" and "Cancel".

Step 3. Specify Scheduling Options

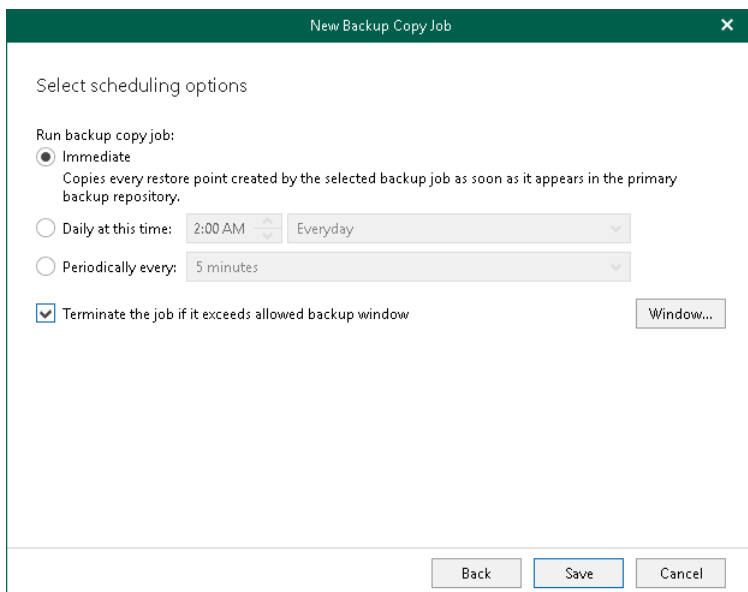
At this step of the wizard, configure a schedule for your backup copy job.

To configure a schedule, do the following:

1. In the **Run backup copy job** section, select one of the following options:
 - **Immediate.** Select this option if you want to run the backup copy job right after the latest restore point appears in the source backup repository. During the first run of the copy job, Veeam Backup for Microsoft 365 copies the latest restore point created by the source backup job (backup job for which you create a backup copy job). During next runs – each subsequent restore point.
 - **Daily at this time.** Select this option if you want to run the backup copy job on the specified days at the specified hours.
 - **Periodically every.** Select this option if you want to run the backup copy job every N minutes or hours.

Keep in mind that if you run your backup copy job daily or periodically, Veeam Backup for Microsoft 365 copies only the latest restore point that appeared in the source backup repository since the last run of this backup copy job.

2. Select the **Terminate the job if it exceeds allowed backup window** check box, click **Window** and specify allowed and prohibited hours for the backup copy job. For more information, see [Selecting Time Periods](#).



Selecting Time Periods

When you click **Window**, the **Time Periods** dialog appears in which you can:

- Set the **Permitted** execution time frame for the backup copy job.
- Set the **Denied** execution time frame for the backup copy job.

The main area of the dialog is divided into two axes:

- The vertical axis represents days of the week from Sunday to Saturday.
- The horizontal axis represents time intervals from 12 AM to 11:59 PM.

Within these axes a matrix is placed consisting of blocks. Each block represents a 59 minutes interval for each day of the week. The total number of blocks is 168 (24 blocks per each day of the week).

To set up an execution frame for the backup copy job, do the following:

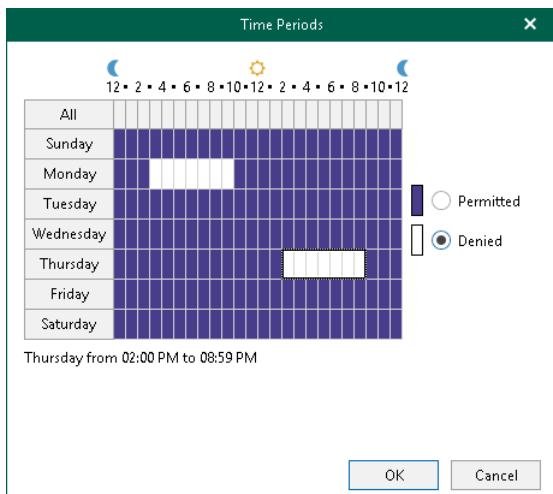
1. Select a block that corresponds to the day of the week (vertical axis) and to the time interval (horizontal axis) on which you want to allow or prohibit the execution of a backup copy job.

In addition, you can:

- a. Select multiple blocks simultaneously by clicking and holding the mouse pointer on the first block and dragging it until the last one that you want to use, including different days of the week.
 - b. Click a day of the week in the vertical axis to select all the blocks of the day.
 - c. Click **All** in the vertical axis to select all the blocks of the entire week.
2. On the right-hand side, select either the **Permitted** or **Denied** option to set up the execution rule for the selected blocks.

The following is an example in which it is prohibited to run a backup copy job on the following days of the week:

- Monday from 03:00 AM up until 09:59 AM.
- Thursday from 02:00 PM up until 08:59 PM.



Managing Backup Copy Jobs

You can manage backup copy jobs that you created for your backup jobs in Veeam Backup for Microsoft 365. For example, you can edit the settings of a backup copy job, start, stop, enable, disable and remove backup copy jobs.

Starting Backup Copy Job

By default, a backup copy job starts automatically either right after appearing of the latest restore point in the source backup repository or if you configure to run your backup copy job periodically - right after its creation and then in the specified time interval.

You can start your backup copy job manually. Manual start can be helpful if the backup copy job was disabled for some time or if a new restore point has already appeared in the source backup repository but the backup copy job was configured to run daily or periodically.

NOTE

Consider the following:

- Veeam Backup for Microsoft 365 processes only the latest restore point that appeared in the source backup repository since this backup copy job was created.
- Restore points created by the previous versions of Veeam Backup for Microsoft 365 are not processed.

To start a backup copy job manually, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select an organization.

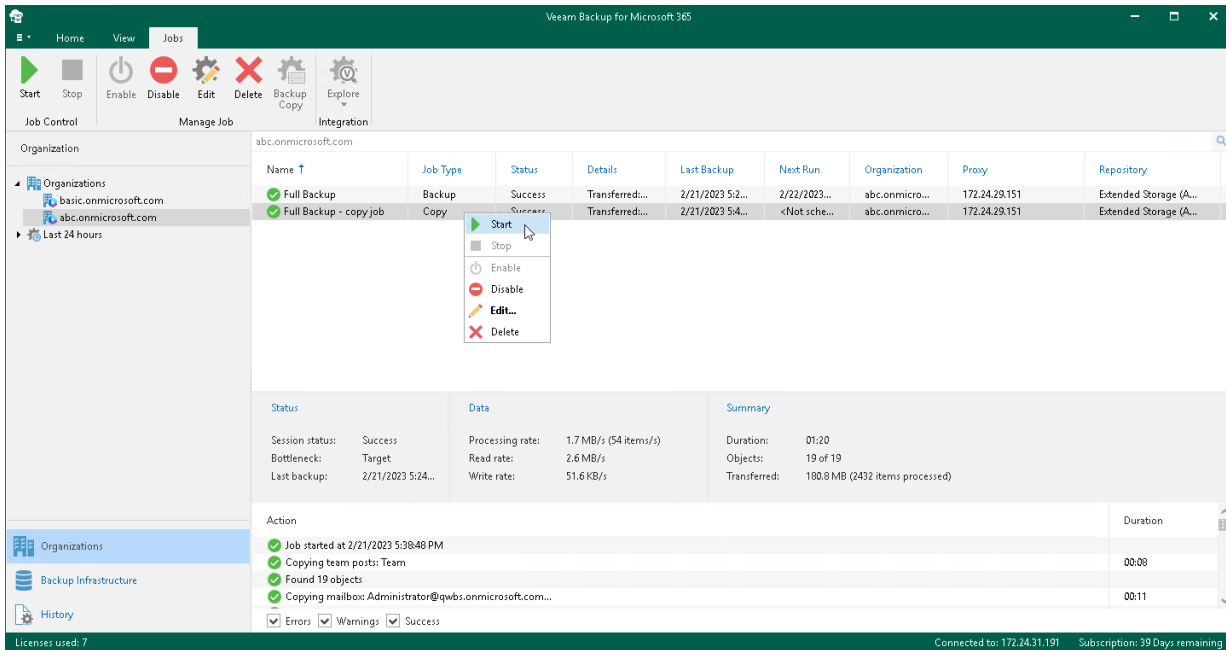
TIP

You can also select the root **Organizations** node to see all backup and backup copy jobs that were created for all organizations added to the scope.

3. In the preview pane, do one of the following:
 - Select a backup copy job and click **Start** on the ribbon.

- Right-click a backup copy job and select **Start**.

A backup copy job name consists of a backup job name for which a backup copy job is created and the *copy job* postfix.



Stopping Backup Copy Job

To stop a backup copy job, do the following:

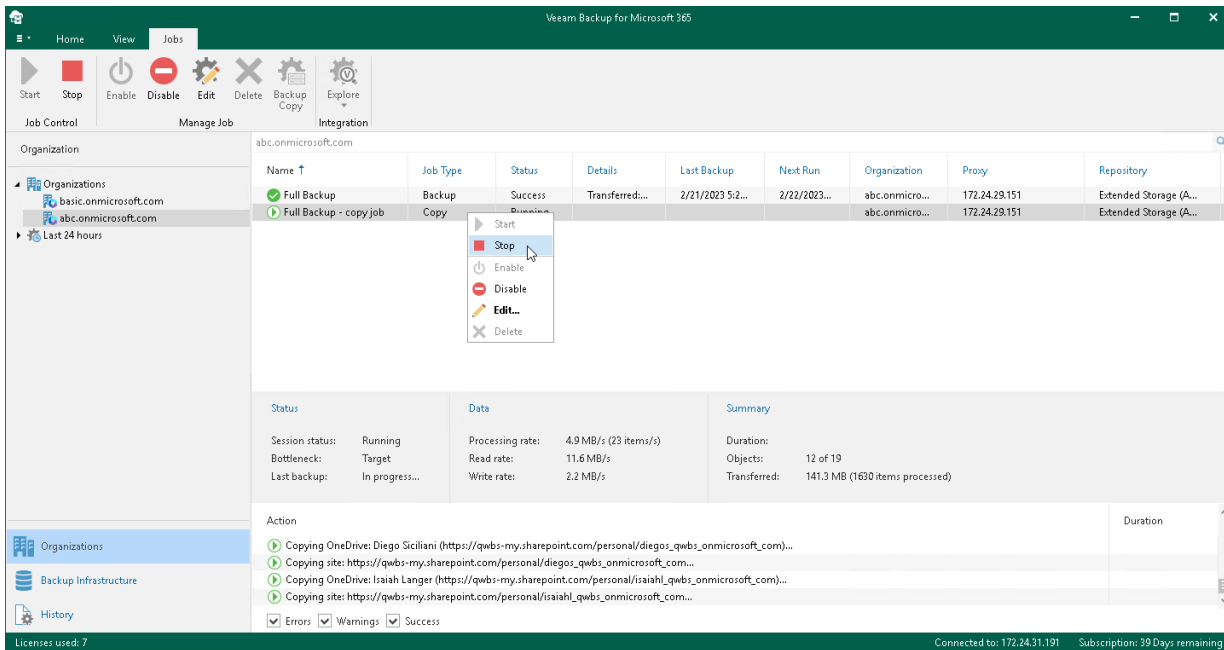
1. Open the **Organizations** view.
2. In the inventory pane, select an organization.

TIP

You can also select the root **Organizations** node to see all backup and backup copy jobs that were created for all organizations added to the scope.

3. In the preview pane, do one of the following:
 - Select a backup copy job and click **Stop** on the ribbon.
 - Right-click a backup copy job and select **Stop**.

A backup copy job name consists of a backup job name for which a backup copy job is created and the *copy* job postfix.



Enabling or Disabling Backup Copy Job

You can enable or disable a backup copy job.

Consider the following:

- If a backup copy job is enabled, it can be executed on schedule.
- If a backup copy job is disabled, it cannot be executed on schedule but you can run it manually using the **Start** command. For more information, see [Starting Backup Copy Job](#).

To enable or disable a backup copy job, do the following:

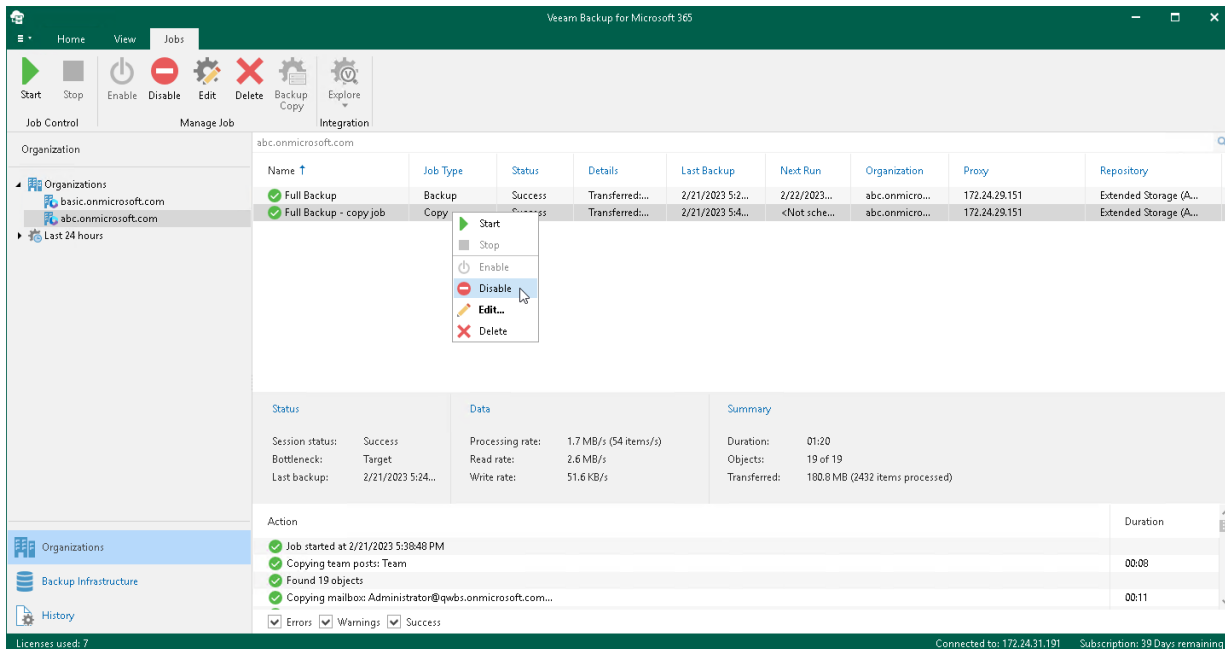
1. Open the **Organizations** view.
2. In the inventory pane, select an organization.

TIP

You can also select the root **Organizations** node to see all backup and backup copy jobs that were created for all organizations added to the scope.

3. In the preview pane, do one of the following:
 - Select a backup copy job and click **Enable** or **Disable** on the ribbon.
 - Right-click a backup copy job and select **Enable** or **Disable**.

A backup copy job name consists of a backup job name for which a backup copy job is created and the *copy job* postfix.



The screenshot shows the Veeam Backup for Microsoft 365 interface. The 'Jobs' tab is active, displaying a table of backup jobs. A context menu is open over the 'Full Backup - copy job' entry, with the 'Disable' option selected. The interface includes a ribbon with 'Job Control' and 'Manage Job' sections, and a preview pane showing job details and an action log.

Name	Job Type	Status	Details	Last Backup	Next Run	Organization	Proxy	Repository
Full Backup	Backup	Success	Transferred:...	2/21/2023 5:2...	2/22/2023...	abc.onmicro...	172.24.29.151	Extended Storage (A...
Full Backup - copy job	Copy	Success	Transferred:...	2/21/2023 5:4...	<Not sche...	abc.onmicro...	172.24.29.151	Extended Storage (A...

Status	Data	Summary
Session status: Success	Processing rate: 1.7 MB/s (54 items/s)	Duration: 01:20
Bottleneck: Target	Read rate: 2.6 MB/s	Objects: 19 of 19
Last backup: 2/21/2023 5:24...	Write rate: 51.6 KB/s	Transferred: 180.8 MB (2432 items processed)

Action	Duration
Job started at 2/21/2023 5:38:48 PM	
Copying team posts: Team	00:08
Found 19 objects	
Copying mailbox: Administrator@qws.onmicrosoft.com...	00:11

Editing Backup Copy Job Settings

Veeam Backup for Microsoft 365 allows you to edit a backup copy job settings.

To edit settings of a backup copy job, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select an organization.

TIP

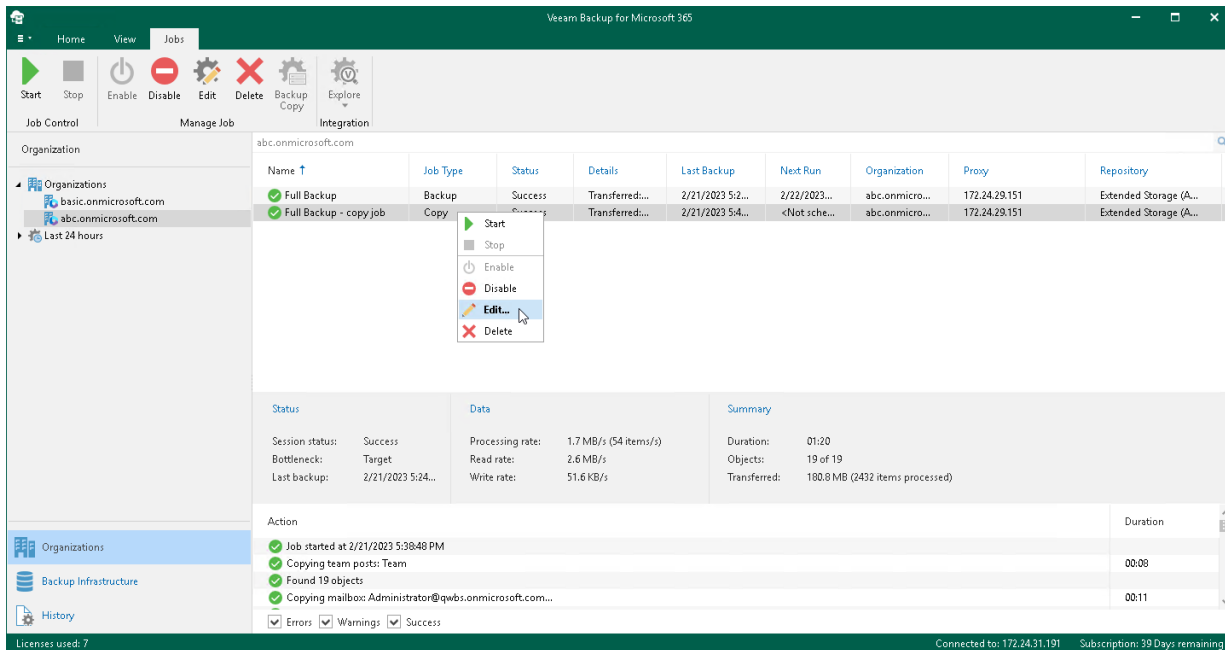
You can also select the root **Organizations** node to see all backup and backup copy jobs that were created for all organizations added to the scope.

3. In the preview pane, do one of the following:
 - Select a backup copy job and click **Edit** on the ribbon.
 - Right-click a backup copy job and select **Edit**.

A backup copy job name consists of a backup job name for which a backup copy job is created and the *copy job* postfix.

4. Modify the required settings.

You can change a [target backup repository](#) and reconfigure a backup copy job scheduling options.



Removing Backup Copy Job

You can remove a backup copy job from the Veeam Backup for Microsoft 365 configuration.

NOTE

When you remove a backup copy job, Veeam Backup for Microsoft 365 keeps the backed-up files in the target backup repository where backup copies were created. You can retrieve your backed-up data from the target backup repository or explore backup copies. For more information, see [Retrieving Backed-Up Data](#) and [Exploring Backup Copies](#).

To remove a backup copy job from the Veeam Backup for Microsoft 365 configuration, do the following:

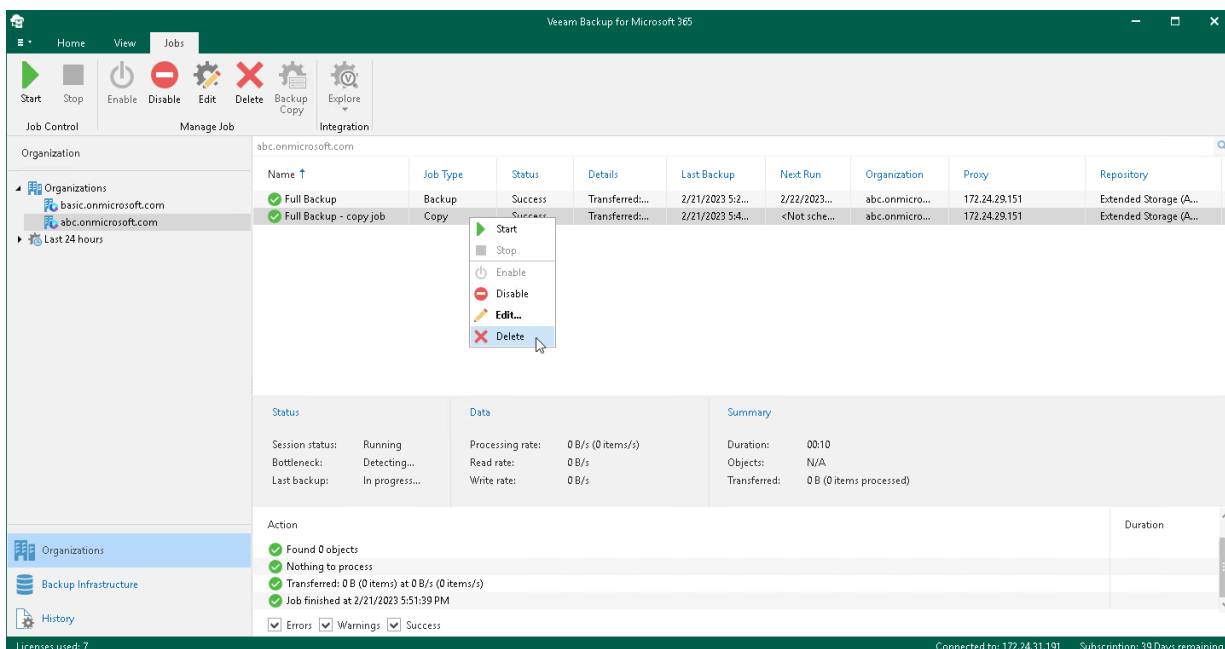
1. Open the **Organizations** view.
2. In the inventory pane, select an organization.

TIP

You can also select the root **Organizations** node to see all backup and backup copy jobs that were created for all organizations added to the scope.

3. In the preview pane, do one of the following:
 - Select a backup copy job and click **Delete** on the ribbon.
 - Right-click a backup copy job and select **Delete**.

A backup copy job name consists of a backup job name for which a backup copy job is created and the *copy* job postfix.



Retrieving Backed-Up Data

Data retrieval is the process of receiving temporary access to backup copies, so that backed-up data can be explored. You can retrieve backed-up data from a backup repository extended with Azure Blob Storage Archive access tier, Amazon S3 Glacier Flexible Retrieval or Amazon S3 Glacier Deep Archive storage classes.

As well as data backup and backup copy, data retrieval is a job-driven process. When you want to access your data in backup copies stored in Azure Blob Storage Archive, Amazon S3 Glacier Flexible Retrieval and Amazon S3 Glacier Deep Archive, you create a retrieval job. For more information, see [Creating Retrieval Job](#).

NOTE

Consider the following:

- You do not need to retrieve backed-up data from a backup repository extended with Amazon S3 Glacier Instant Retrieval storage class. For more information, see [Exploring Backup Copies](#).
- If you want to view the created retrieval jobs and their statuses, in the inventory pane, open the **Organizations** view, select the **Data retrieval** node and view the list in the preview pane.

When the retrieval job is complete, the retrieved data will be available for a specified period of time, during which you can [explore](#) and [restore](#) your data using Veeam Explorers. You can extend the availability period for data that Veeam Backup for Microsoft 365 has retrieved. For more information, see [Editing Retrieval Job Settings](#) and [Extending Availability of Retrieved Data](#).

Data retrieval cost varies depending on the desired speed of the process. You can select an option that you prefer at the [Select Retrieval Mode](#) step of the **Retrieve Backup Copy** wizard. Keep in mind that options differ for Azure Blob Storage Archive, Amazon S3 Glacier Flexible Retrieval and Amazon S3 Glacier Deep Archive storage classes.

Creating Retrieval Job

To create a retrieval job, do the following:

1. [Launch the Retrieve Backup Copy wizard.](#)
2. [Specify a retrieval job name.](#)
3. [Specify point in time.](#)
4. [Select an organization.](#)
5. [Select objects.](#)
6. [Select a retrieval mode.](#)
7. [Specify data availability period.](#)

Step 1. Launch Retrieve Backup Copy Wizard

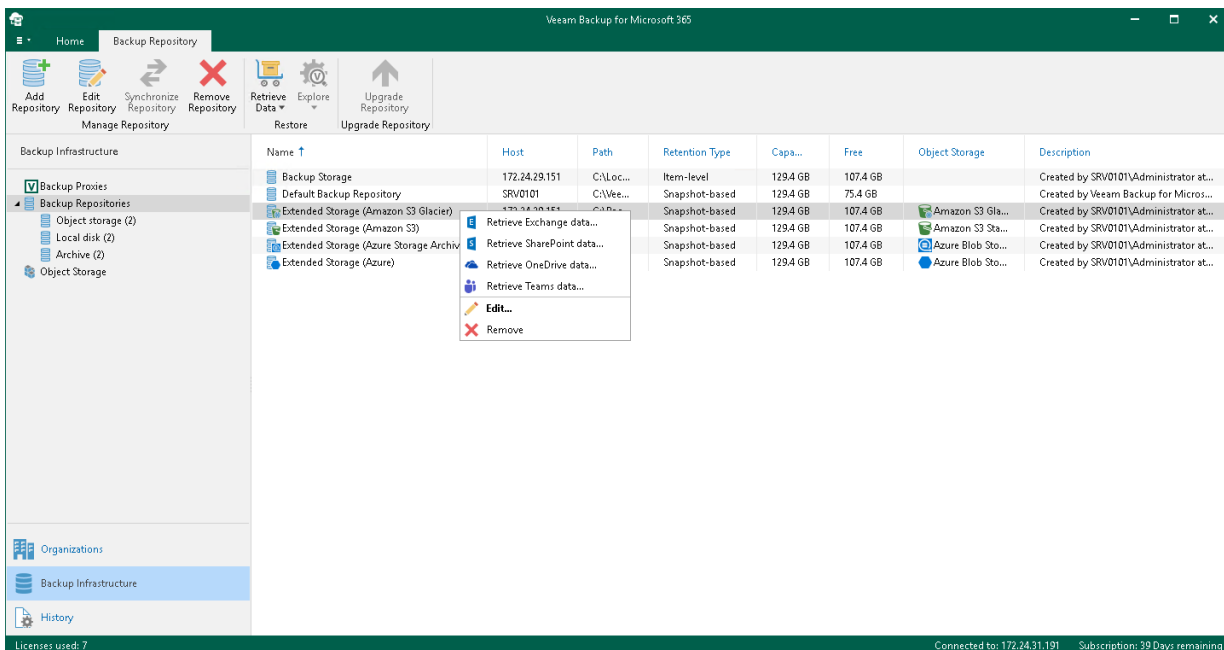
To launch the **Retrieve Backup Copy** wizard, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Backup Repositories** or **Backup Repositories > Archive** node.
3. In the preview pane, do one of the following:
 - Select a backup repository from which you want to retrieve backed-up data and click **Retrieve Data** on the ribbon and then select **Retrieve <product> data**.
 - Right-click a backup repository from which you want to retrieve backed-up data and select **Retrieve <product> data**.

NOTE

The **Retrieve <product> data** option is one of the following:

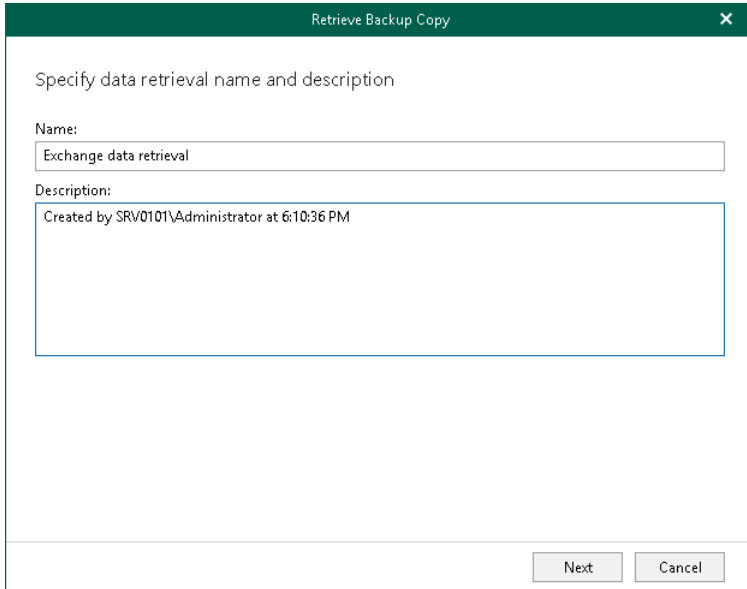
- **Retrieve Exchange data.** Use this option to create a retrieval job for the subsequent explore and restore of the retrieved data using Veeam Explorer for Microsoft Exchange.
- **Retrieve SharePoint data.** Use this option to create a retrieval job for the subsequent explore and restore of the retrieved data using Veeam Explorer for Microsoft SharePoint.
- **Retrieve OneDrive data.** Use this option to create a retrieval job for the subsequent explore and restore of the retrieved data using Veeam Explorer for Microsoft OneDrive for Business.
- **Retrieve Teams data.** Use this option to create a retrieval job for the subsequent explore and restore of the retrieved data using Veeam Explorer for Microsoft Teams.



Step 2. Specify Retrieval Job Name

At this step of the wizard, edit the suggested name for the retrieval job if needed and provide optional description:

1. In the **Name** field, edit the retrieval job name that Veeam Backup for Microsoft 365 suggests.
2. In the **Description** field, enter optional description.



Retrieve Backup Copy

Specify data retrieval name and description

Name:
Exchange data retrieval

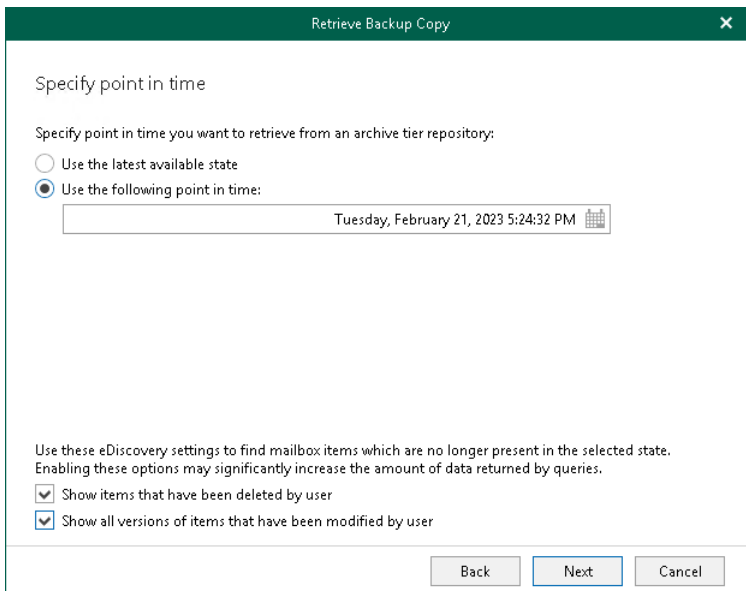
Description:
Created by SRV0101\Administrator at 6:10:36 PM

Next Cancel

Step 3. Specify Point In Time

At this step of the wizard, select a backup state of the backed-up data that you want to retrieve from the extended backup repository:

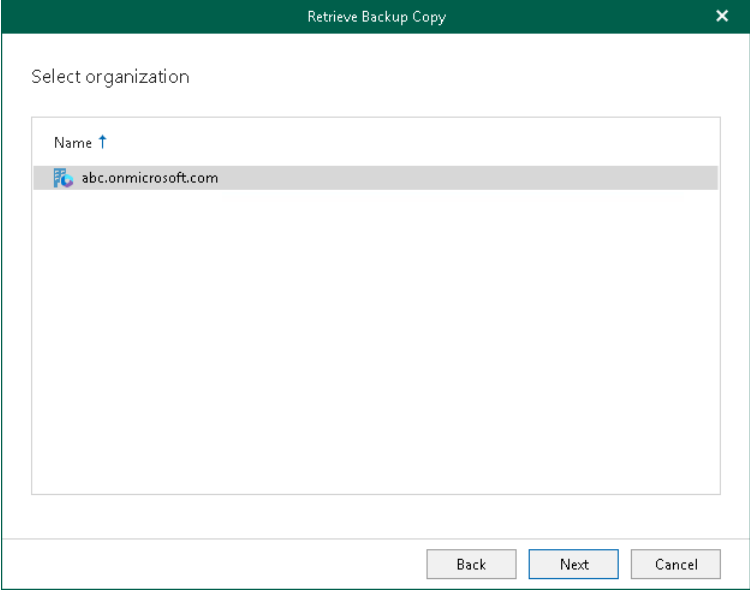
1. Select one of the following options:
 - **Use the latest available state.** Select this option to retrieve the latest state of the backed-up data.
 - **Use the following point in time.** Select this option to retrieve the backed-up data of the selected date.
2. If you want to view historic data, select the following check boxes:
 - **Show items that have been deleted by user.** Select this option to show items that have been removed by the user before the specified date.
 - **Show all versions of items that have been modified by user.** Select this option to show all versions of items that have been modified by the user before the specified date.



The screenshot shows a dialog box titled "Retrieve Backup Copy" with a close button (X) in the top right corner. The main heading is "Specify point in time". Below it, the text reads "Specify point in time you want to retrieve from an archive tier repository:". There are two radio button options: "Use the latest available state" (which is unselected) and "Use the following point in time:" (which is selected). Below the selected option is a text input field containing the date and time "Tuesday, February 21, 2023 5:24:32 PM" and a small calendar icon to its right. At the bottom of the dialog, there is a section titled "Use these eDiscovery settings to find mailbox items which are no longer present in the selected state. Enabling these options may significantly increase the amount of data returned by queries." with two checked checkboxes: "Show items that have been deleted by user" and "Show all versions of items that have been modified by user". At the very bottom, there are three buttons: "Back", "Next" (which is highlighted with a blue border), and "Cancel".

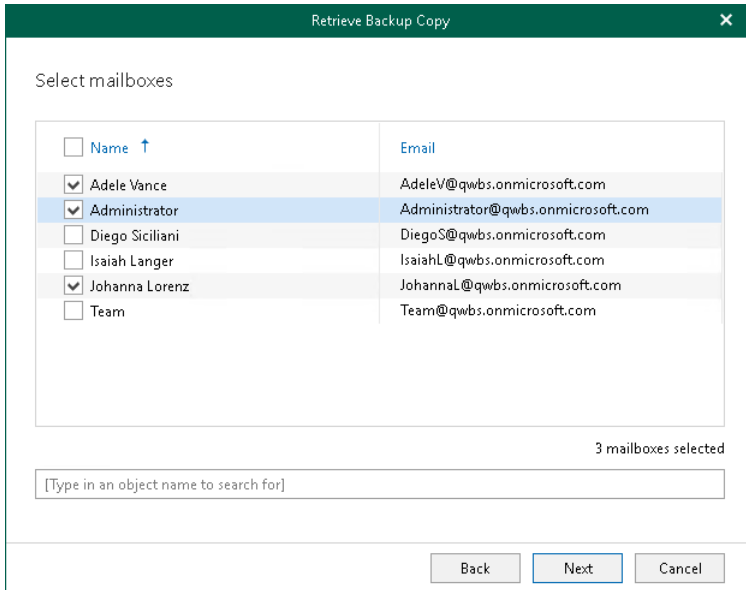
Step 4. Select Organization

At this step of the wizard, select an organization. Veeam Backup for Microsoft 365 will retrieve from the backed-up data of objects that are belong to the selected organization.



Step 5. Select Objects

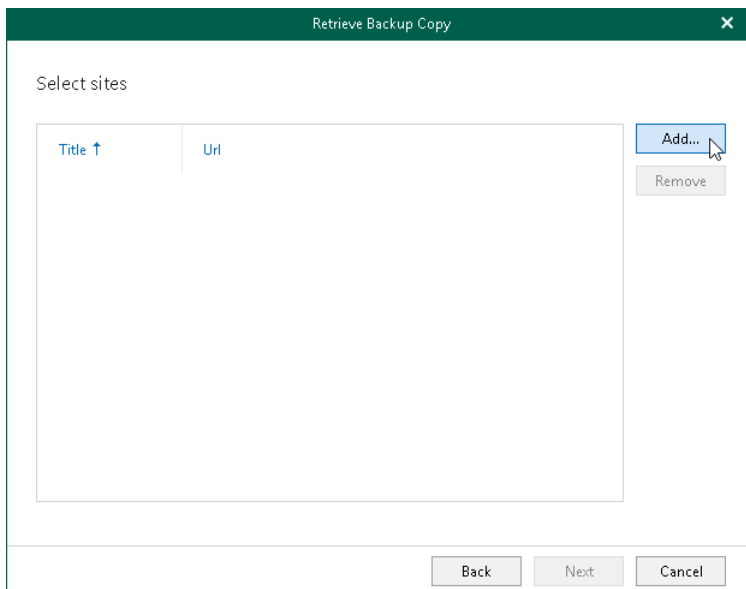
At this step of the wizard, select check boxes next to the objects (mailboxes, OneDrives, teams) whose backed-up data you want to retrieve from the extended backup repository.



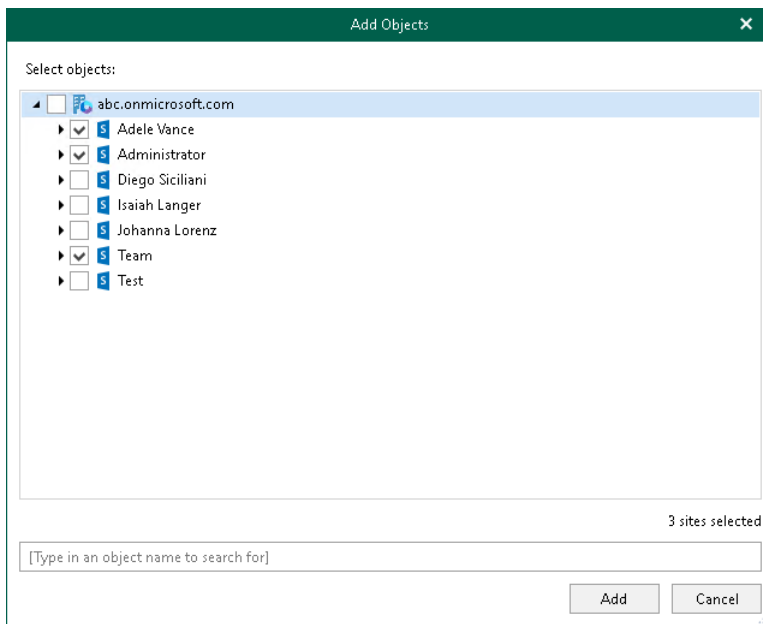
Selecting SharePoint Sites

If you want to retrieve backed-up data of the SharePoint sites, do the following:

1. Click **Add**.



- In the **Add Objects** window, select check boxes next to the sites or subsites whose backed-up data you want to retrieve.



- Click **Add**.

The selected objects appear in the list of SharePoint sites whose backed-up data you want to retrieve.

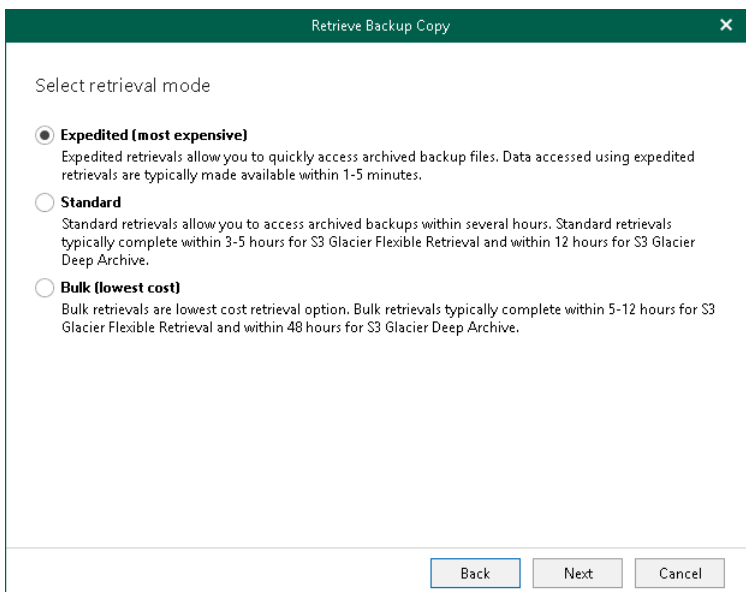
Step 6. Select Retrieval Mode

At this step of the wizard, select a retrieval mode that you want to use. Data retrieval cost varies depending on the desired speed of the process. Options differ for Azure Blob Storage Archive, Amazon S3 Glacier Flexible Retrieval and Amazon S3 Glacier Deep Archive.

Amazon S3 Glacier Flexible Retrieval / Amazon S3 Glacier Deep Archive

Select one of the following options:

- **Expedited**
Use this option to access your backed-up data within several minutes.
- **Standard**
Use this option to access your backed-up data within several hours.
- **Bulk**
Use this option to access your backed-up data within the longer time period.



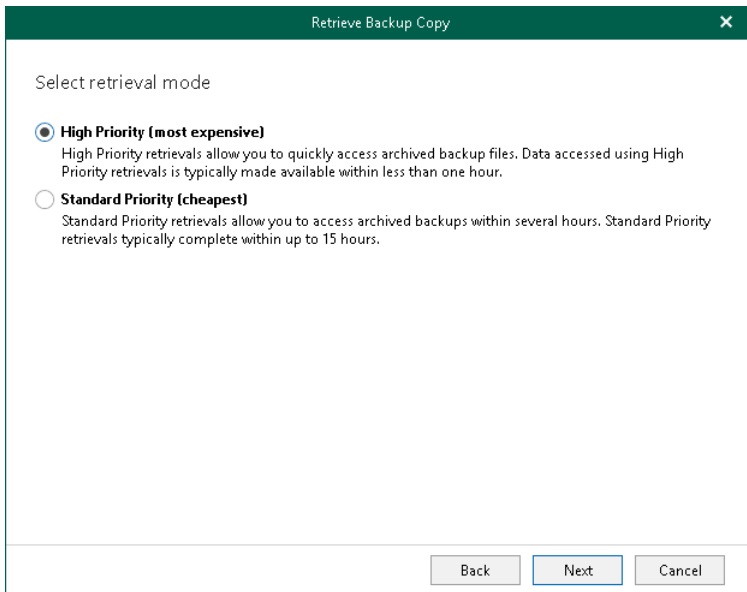
Azure Blob Storage Archive

Select one of the following options:

- **High Priority**
Use this option to access your backed-up data within 1 hour.

- **Standard Priority**

Use this option to access your backed-up data within several hours.



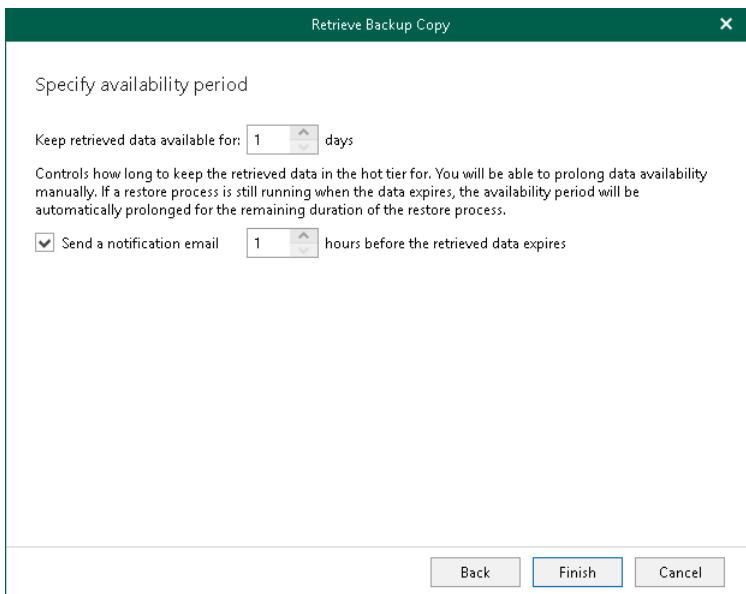
Step 7. Specify Availability Period

At this step of the wizard, specify the availability period that you want to apply for the retrieved backed-up data. During this period you will be able to explore and restore your data using Veeam Explorers. For more information, see [Exploring Retrieved Data](#).

If you want to receive a notification that the availability period is about to end, select the **Send a notification email N hours before the retrieved data expires** check box and specify the time for the notification.

NOTE

You can extend the availability period if necessary. For more information, see [Editing Retrieval Job Settings](#) and [Extending Availability of Retrieved Data](#).



The screenshot shows a dialog box titled "Retrieve Backup Copy" with a close button (X) in the top right corner. The main content area is titled "Specify availability period". It contains the following elements:

- A label "Keep retrieved data available for:" followed by a spinner control set to "1" and the text "days".
- A paragraph of text: "Controls how long to keep the retrieved data in the hot tier for. You will be able to prolong data availability manually. If a restore process is still running when the data expires, the availability period will be automatically prolonged for the remaining duration of the restore process."
- A checked checkbox labeled "Send a notification email" followed by a spinner control set to "1" and the text "hours before the retrieved data expires".

At the bottom of the dialog box, there are three buttons: "Back", "Finish" (which is highlighted with a blue border), and "Cancel".

Editing Retrieval Job Settings

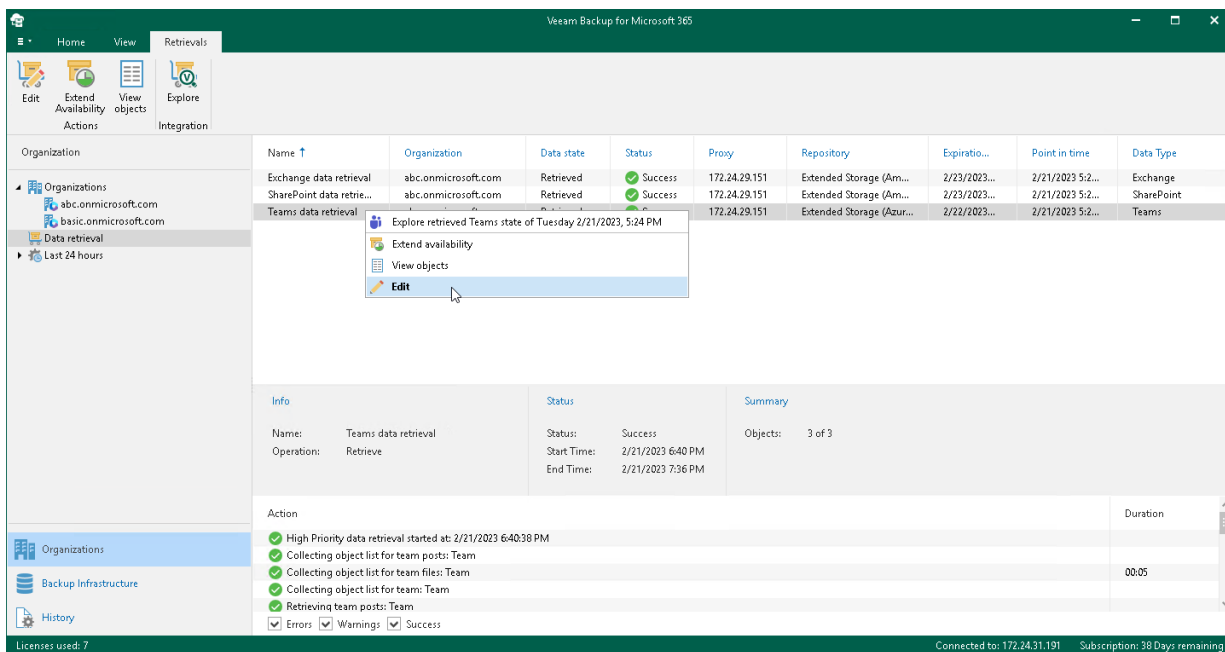
Veeam Backup for Microsoft 365 allows you to edit a retrieval job settings.

To edit settings of a retrieval job, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select the **Data retrieval** node.
3. In the preview pane, do one of the following:
 - Select a retrieval job and click **Edit** on the ribbon.
 - Right-click a retrieval job and select **Edit**.
4. Modify the required settings.

You can change the following parameters:

- The name and description of a retrieval job.
- The availability period of the retrieved backed-up data.



Extending Availability of Retrieved Data

You can extend the availability period of the retrieved backed-up data.

To extend the availability period of the retrieved backed-up data, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select the **Data retrieval** node.
3. In the preview pane, do one of the following:
 - Select a retrieval job with backed-up data which availability period you want to extend and click **Extend Availability** on the ribbon.
 - Right-click a retrieval job and select **Extend Availability**.
4. In the wizard window that opens, specify number of days during which the retrieved backed-up data will be available to explore and restore using Veeam Explorers.
5. If you want to receive a notification that the availability period is about to end, select the **Send a notification email N hours before the retrieved data expires** check box and specify the time for the notification.

Extend availability data retrieve wizard

Specify availability period

Keep retrieved data available for: 10 days (expiration date: 3/3/2023 7:36:21 PM)

Controls how long to keep the retrieved data in the hot tier for. You will be able to prolong data availability manually. If a restore process is still running when the data expires, the availability period will be automatically prolonged for the remaining duration of the restore process.

Send a notification email 1 hours before the retrieved data expires

Finish Cancel

Data Restore

To restore Microsoft organization data, you can use Veeam Explorers and Restore Portal:

- [Veeam Explorer for Microsoft Exchange](#)
To explore and restore Microsoft Exchange mailboxes, folders, messages, tasks, contacts and items.
- [Veeam Explorer for Microsoft SharePoint](#)
To explore and restore Microsoft SharePoint sites, libraries and items.
- [Veeam Explorer for Microsoft OneDrive for Business](#)
To explore and restore Microsoft OneDrive for Business items and folders.
- [Veeam Explorer for Microsoft Teams](#)
To explore and restore Microsoft Teams teams, channels, tabs, posts and files.
- [Restore Portal](#)
To explore and restore Microsoft Exchange, Microsoft SharePoint, Microsoft OneDrive for Business and Microsoft Teams data using Restore Portal. Restore Portal allows users to perform self-service restore.

TIP

When you use Veeam Explorers to explore backups, you can search for required items in a backup file. In particular, you can use the **Advanced Find** mechanism that allows you to configure search criteria using filters. For more information, see the *Searching for Objects in Backup File* sections of the [Veeam Explorers User Guide](#) for each Veeam Explorer.

To launch Veeam Explorers, you use the **Explore** option. For more information, see the following sections:

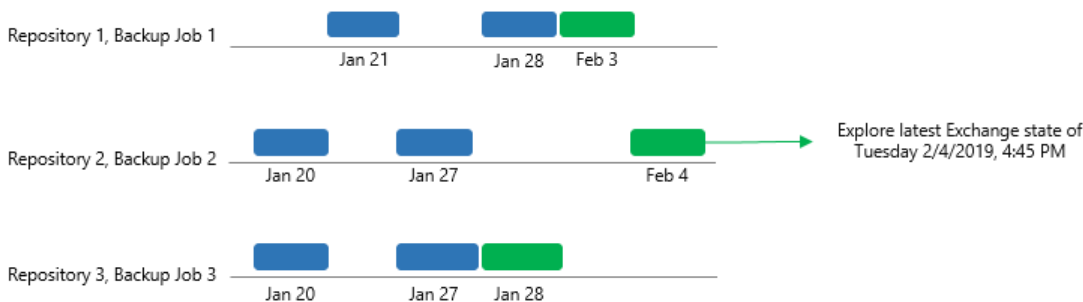
- [Exploring Backup Jobs](#)
To open backups created by the selected backup job.
- [Exploring Single Organization](#)
To open backups created by all backup jobs of a specific organization.
- [Exploring All Organizations](#)
To open backups of all organizations.
- [Exploring Retrieved Data](#)
To open backups that you have retrieved from backup copies located in backup repositories extended with Azure Blob Storage Archive access tier, Amazon S3 Glacier Flexible Retrieval or Amazon S3 Glacier Deep Archive storage classes.
- [Exploring Backup Copies](#)
To open backup copies stored in backup repositories extended with Azure Blob Storage, Amazon S3 Standard, Amazon S3 Standard-Infrequent Access and Amazon S3 Glacier Instant Retrieval storage classes or S3 Compatible object storage.

You can also restore Microsoft organization data from backups created for the Veeam Backup for Microsoft 365 server by Veeam Backup & Replication. For more information, see the [Application Items Restore](#) section of the Veeam Backup & Replication User Guide.

Exploring Backup Jobs

When exploring backup jobs, Veeam Backup for Microsoft 365 loads the latest restore point that was created by the selected job.

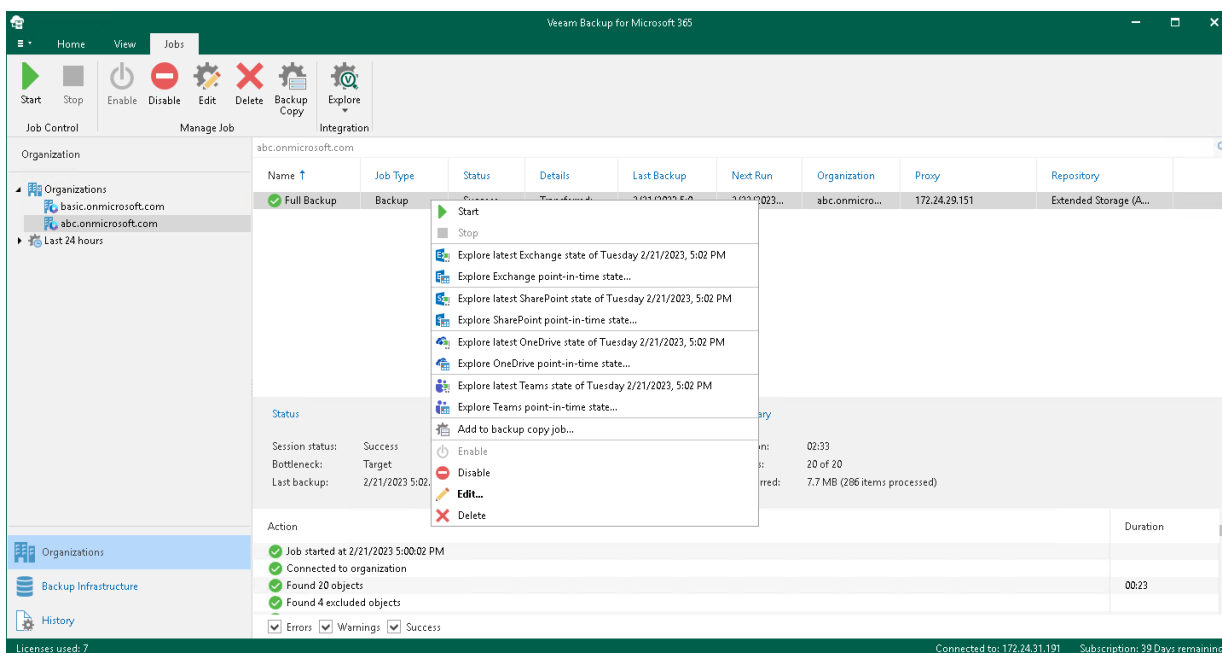
The following is an example of exploring the *Backup Job 2* from the *Repository 2*. This job has three restore points created on January 20, January 27 and February 4. In such a scenario, Veeam Backup for Microsoft 365 loads only the latest restore point (created on February 4) into the Veeam Explorers scope.



To open backups created by the selected backup job, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select an organization.
3. In the preview pane, select a backup job that contains backups that you want to open.
4. On the **Jobs** tab, click **Explore**, or right-click a backup job and select one of the following options:
 - **Explore latest <product> state of <date_and_time>**. To explore the latest backup state.
 - **Explore <product> point-in-time state**. To select a point-in-time state. For more information, see [Exploring Point In Time](#).

where **<product>** is one of the following services: *Exchange*, *SharePoint*, *OneDrive*, or *Teams*.



Exploring Single Organization

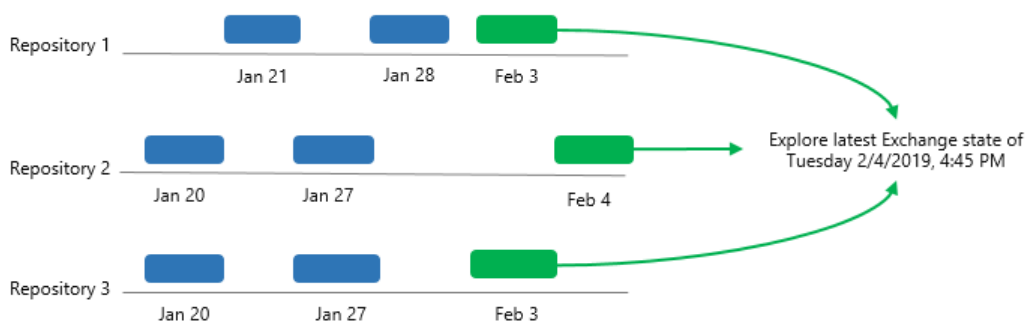
When exploring a single organization, Veeam Backup for Microsoft 365 merges and loads the latest restore points that have been created by each backup job of the selected organization.

NOTE

If you remove specific objects from a backup job scope or remove a backup job from the Veeam Backup for Microsoft 365 configuration, all backup data created by this job remains in a backup repository and will be loaded into the Veeam Explorers scope.

The following is an example of exploring a single organization with backups that are stored in three different [backup repositories](#). In such a scenario, the following restore points will be merged and loaded into the Veeam Explorers scope:

- For *Repository 1*, only the restore point created on February 3.
- For *Repository 2*, only the restore point created on February 4.
- For *Repository 3*, only the restore point created on February 3.

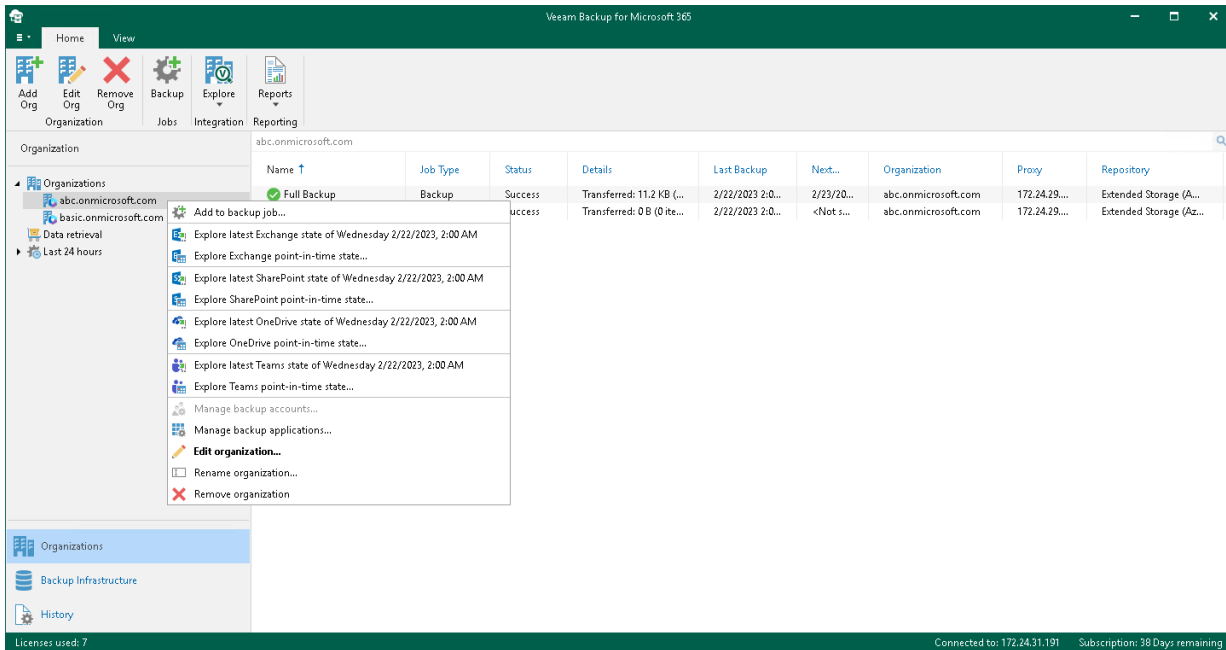


To open backups created by all backup jobs of a specific organization, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, right-click an organization and select one of the following options:
 - **Explore latest <product> state of <date_and_time>**. To explore the latest backup state.

- **Explore <product> point-in-time state.** To select a point-in-time state. For more information, see [Exploring Point In Time](#).

where <product> is one of the following services: *Exchange*, *SharePoint*, *OneDrive*, or *Teams*.



Exploring All Organizations

When exploring all organizations, Veeam Backup for Microsoft 365 merges and loads the latest restore points of each backup job of every organization.

NOTE

If you remove specific objects from a backup job scope or remove a backup job from the Veeam Backup for Microsoft 365 configuration, all backup data created by this job remains in a backup repository and will be loaded into the Veeam Explorers scope.

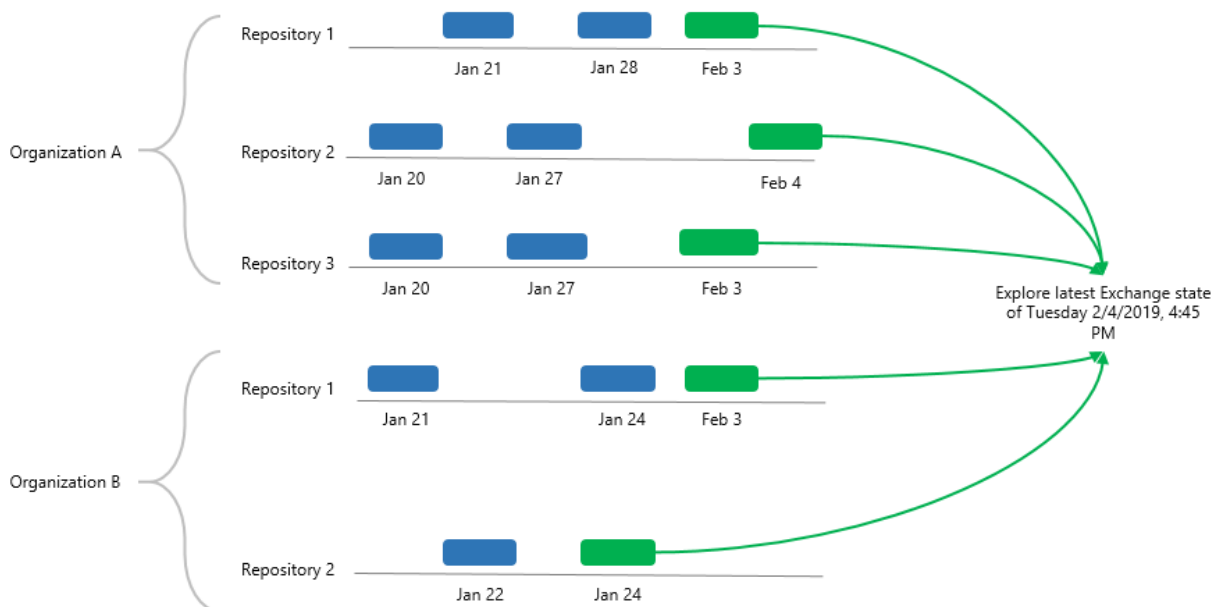
The following is an example of exploring two organizations: *A* and *B*. The organization *A* has three backup jobs and the organization *B* has two backup jobs.

When exploring the organization *A*, the following restore points will be merged and loaded into the Veeam Explorers scope:

- For *Repository 1*, only the restore point created on February 3.
- For *Repository 2*, only the restore point created on February 4.
- For *Repository 3*, only the restore point created on February 3.

When exploring the organization *B*, the following restore points will be merged and loaded into the Veeam Explorers scope:

- For *Repository 1*, only the restore point created on February 3.
- For *Repository 2*, only the restore point created on January 24.

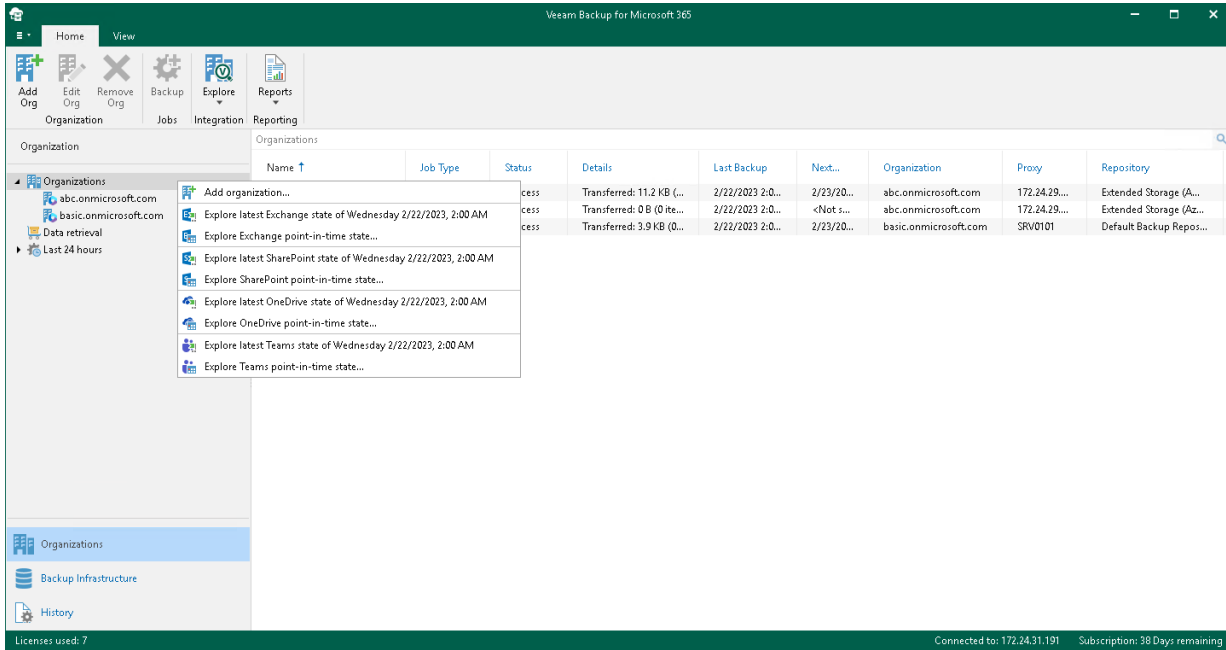


To open backups of all organizations, do the following:

1. Open the **Organizations** view.
2. Right-click the root **Organizations** node and select one of the following options:
 - **Explore latest <product> state of <date_and_time>**. To explore the latest backup state.

- **Explore <product> point-in-time state.** To select a point-in-time state. For more information, see [Exploring Point In Time](#).

where <product> is one of the following services: *Exchange*, *SharePoint*, *OneDrive*, or *Teams*.

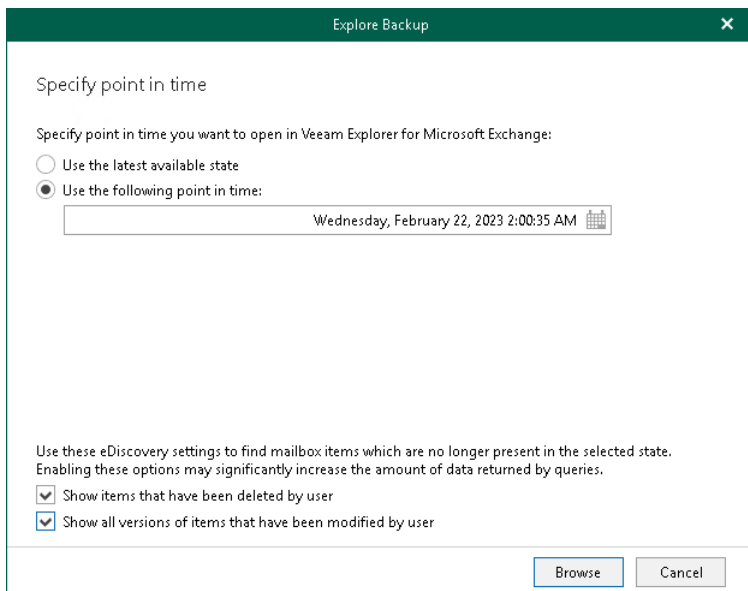


Exploring Point In Time

When exploring a point-in-time state, Veeam Backup for Microsoft 365 runs the **Explore Backup** wizard.

At the **Specify point in time** step of the wizard, select a backup state that you want to open:

1. Select one of the following options:
 - **Use the latest available state.** Select this option to load the latest state of items in the backup file.
 - **Use the following point in time.** Select this option to load a backup as of the selected date.
2. If you want to view historic data, select the following check boxes:
 - **Show items that have been deleted by user.** Select this option to show items that have been removed by the user before the specified date.
 - **Show all versions of items that have been modified by user.** Select this option to show all versions of items that have been modified by the user before the specified date.



The screenshot shows a dialog box titled "Explore Backup" with a close button (X) in the top right corner. The main heading is "Specify point in time". Below this, it says "Specify point in time you want to open in Veeam Explorer for Microsoft Exchange:". There are two radio button options: "Use the latest available state" (which is unselected) and "Use the following point in time:" (which is selected). Below the second option is a text input field containing "Wednesday, February 22, 2023 2:00:35 AM" and a calendar icon. At the bottom of the dialog, there is a note: "Use these eDiscovery settings to find mailbox items which are no longer present in the selected state. Enabling these options may significantly increase the amount of data returned by queries." Below the note are two checked checkboxes: "Show items that have been deleted by user" and "Show all versions of items that have been modified by user". At the very bottom, there are two buttons: "Browse" and "Cancel".

Exploring Retrieved Data

You can explore backed-up data you have retrieved from a backup repository extended with Azure Blob Storage Archive access tier, Amazon S3 Glacier Flexible Retrieval or Amazon S3 Glacier Deep Archive storage classes. For more information on how to retrieve backed-up data, see [Retrieving Backed-Up Data](#).

NOTE

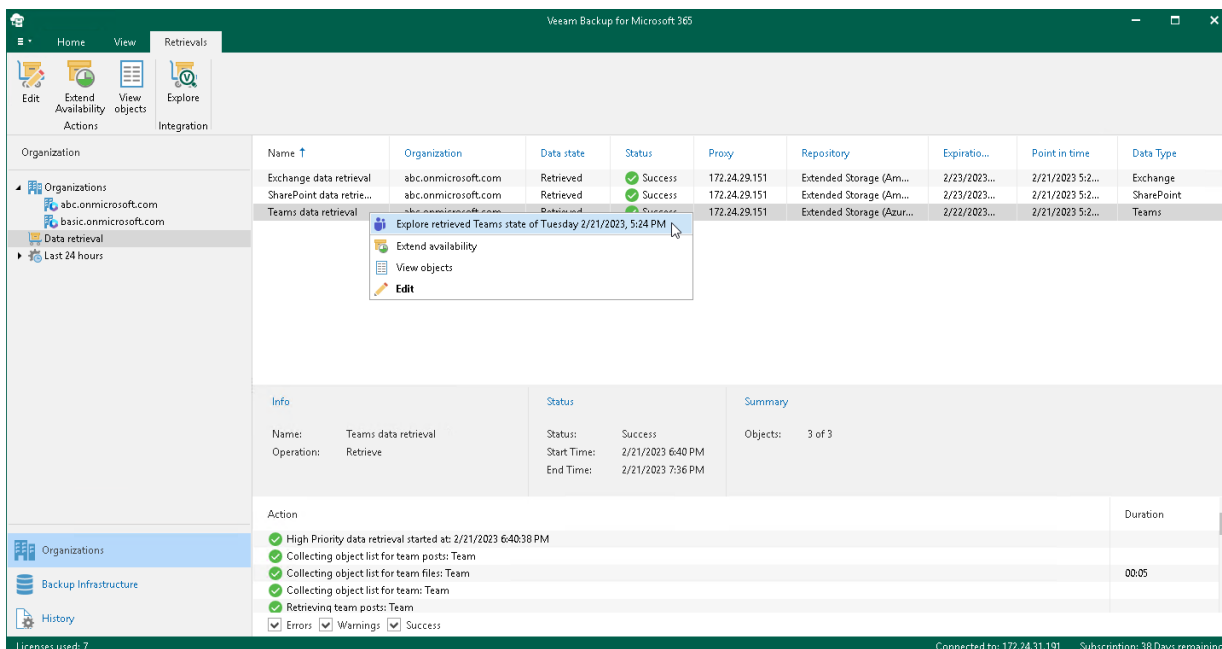
By default, the retrieved data is available for explore during 1 day. You can specify the availability period at the [Specify Availability Period](#) step of the **Retrieve Backup Copy** wizard.

If the retrieved data is restored by Veeam Explorers, the availability period is prolonged automatically for the remaining duration of the restore process. You can extend the availability period. For more information, see [Editing Retrieval Job Settings](#) and [Extending Availability of Retrieved Data](#).

To open backups that you have retrieved, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select the **Data retrieval** node.
3. In the preview pane, do one of the following:
 - Select a retrieval job that contains backed-up data that you want to open and click **Explore** on the ribbon.
 - Right-click a retrieval job and select **Explore retrieved <product> state**.

where **<product>** is one of the following services: *Exchange*, *SharePoint*, *OneDrive*, or *Teams*.



The screenshot displays the Veeam Backup for Microsoft 365 interface. The main window shows a table of retrieved data with columns for Organization, Name, Organization, Data state, Status, Proxy, Repository, Expiration, Point in time, and Data Type. A context menu is open over the 'Teams data retrieval' row, showing options like 'Explore retrieved Teams state of Tuesday 2/21/2023, 5:24 PM', 'Extend availability', 'View objects', and 'Edit'. Below the table, there is an 'Info' section with details for the 'Teams data retrieval' job, including its name, operation, status, start and end times, and a summary of objects. At the bottom, an 'Action' log shows the progress of the retrieval process, including steps like 'High Priority data retrieval started at: 2/21/2023 6:40:38 PM' and 'Collecting object list for team posts: Team'. The status bar at the bottom indicates 'Licenses used: 7', 'Connected to: 172.24.31.191', and 'Subscription: 38 Days remaining'.

Organization	Name	Organization	Data state	Status	Proxy	Repository	Expiration	Point in time	Data Type
abc.onmicrosoft.com	Exchange data retrieval	abc.onmicrosoft.com	Retrieved	Success	172.24.29.151	Extended Storage (Am...	2/23/2023...	2/21/2023 5:2...	Exchange
abc.onmicrosoft.com	SharePoint data retrie...	abc.onmicrosoft.com	Retrieved	Success	172.24.29.151	Extended Storage (Am...	2/23/2023...	2/21/2023 5:2...	SharePoint
basic.onmicrosoft.com	Teams data retrieval	basic.onmicrosoft.com	Retrieved	Success	172.24.29.151	Extended Storage (Azur...	2/22/2023...	2/21/2023 5:2...	Teams

Info

Name:	Teams data retrieval	Status:	Success	Objects:	3 of 3
Operation:	Retrieve	Start Time:	2/21/2023 6:40 PM		
		End Time:	2/21/2023 7:36 PM		

Action

Action	Duration
High Priority data retrieval started at: 2/21/2023 6:40:38 PM	
Collecting object list for team posts: Team	
Collecting object list for team files: Team	
Collecting object list for team: Team	
Retrieving team posts: Team	00:05

Exploring Backup Copies

You can start exploring and restoring data from backup copies stored in backup repositories extended with the following object storage:

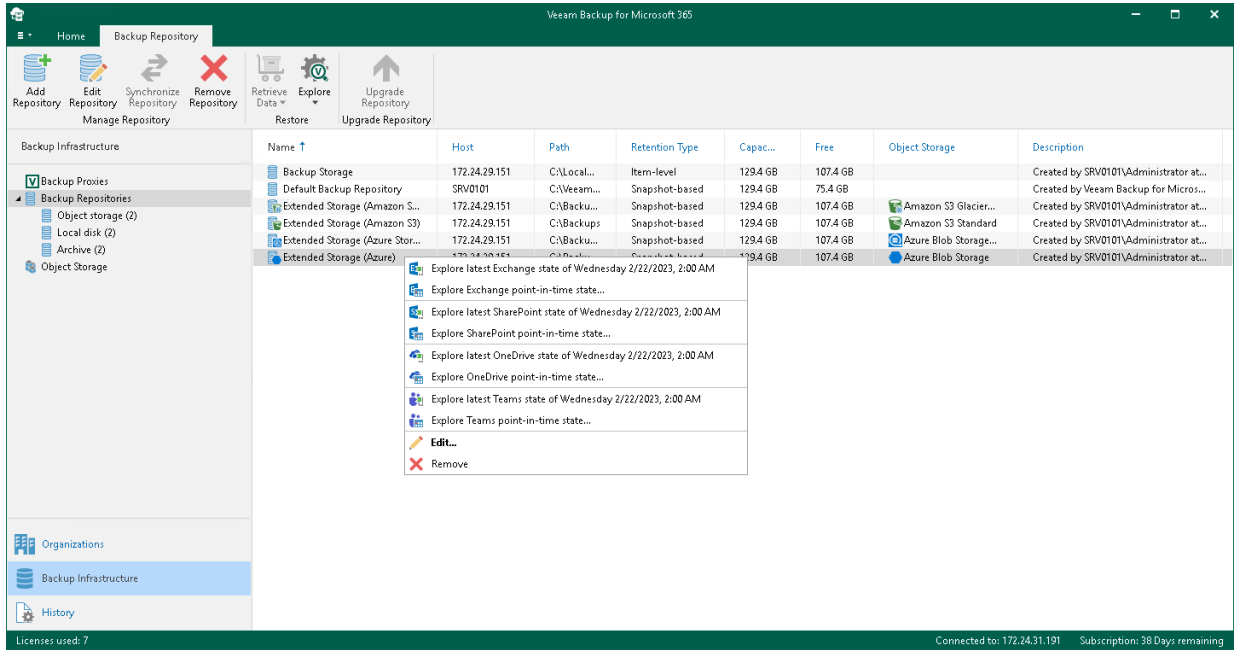
- Azure Blob Storage Hot/Cool access tier
- Amazon S3 Standard storage class
- Amazon S3 Standard-Infrequent Access storage class
- Amazon S3 Glacier Instant Retrieval storage class
- S3 Compatible object storage

To open backup copies stored in the selected backup repository, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select one of the following nodes:
 - **Backup Repositories**. Contains all backup repositories added to the Veeam Backup for Microsoft 365 backup infrastructure.
 - **Backup Repositories > Object Storage**. Contains backup repositories extended with Azure Blob Storage, Amazon S3 Standard and Amazon S3 Standard-Infrequent Access storage classes or S3 Compatible object storage.
 - **Backup Repositories > Archive**. Contains backup repositories extended with Amazon S3 Glacier Instant Retrieval storage class.
3. In the preview pane, select a backup repository that contains backup copies that you want to open.
4. Do one of the following:
 - On the **Backup Repository** tab, click **Explore** on the ribbon.
 - Right-click a backup repository.
5. Select one of the following options:
 - **Explore latest <product> state of <date_and_time>**. To explore the latest backup state.

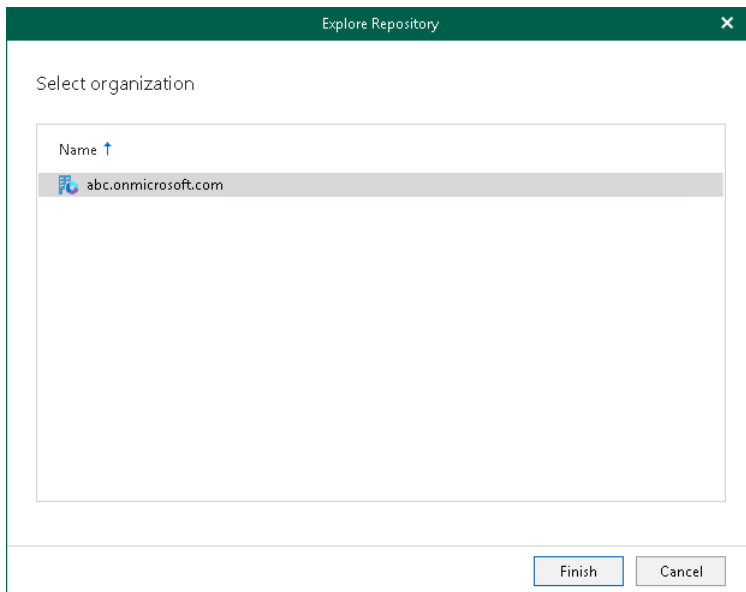
- **Explore <product> point-in-time state.** To select a point-in-time state. For more information, see [Exploring Point In Time](#).

where <product> is one of the following services: *Exchange*, *SharePoint*, *OneDrive*, or *Teams*.



6. If you selected the **Explore latest <product> state of <date_and_time>** option, in the **Explore Repository** wizard window, select an organization.

Veeam Backup for Microsoft 365 will open backed-up data from backup copies created for the selected organization.



Backup, Backup Copy, Retrieve and Restore Statistics

Each backup, backup copy, retrieve or restore session saves its results and metrics to the Veeam Backup for Microsoft 365 configuration database.

To review backup, backup copy, retrieve and restore sessions, open the **History** view and select one of the following nodes:

- **Jobs.** To see all backup and backup copy sessions.
 - **Backup.** To see both completed and running backup sessions.
 - **Copy.** To see both completed and running backup copy sessions.
- **Retrieve.** To see both completed and running retrieve sessions.
- **Restore.** To see Veeam Explorers restore sessions.

To stop a running session, select it in the preview pane and click **Stop** on the ribbon. For more information, see [Stopping Backup Job](#) and [Stopping Backup Copy Job](#).

To review a specific session results of only particular type, use the *Success*, *Warnings* or *Errors* check boxes at the bottom.

The screenshot shows the Veeam Backup for Microsoft 365 interface in the History view. The main area displays a table of backup jobs with columns for Name, Organization, Session Type, Status, Details, Start/End times, Proxy, Repository, and Res... (Restore). The table lists several jobs, including Full Backup - copy job, Full Backup (Incremental), New Backup (Incremental), and Full Backup (Full). One job is highlighted in blue, showing a 'Warning' status with '2 objects failed'.

Name	Organi...	Ses...	Status	Details	Start...	End...	Proxy	Repository	Res...
Full Backup - copy job	abc.onmi...	Copy	Success	Transferred: 180.8...	2/22/2...	2/22/2...	172.24.29.1...	Extended Storage (Azure)	
Full Backup - copy job	abc.onmi...	Copy	Success	Transferred: 0 B (0...	2/22/2...	2/22/2...	172.24.29.1...	Extended Storage (Azure Stora...	
Full Backup (Incremental)	abc.onmi...	Backup	Success	Transferred: 11.2 K...	2/22/2...	2/22/2...	172.24.29.1...	Extended Storage (Amazon S3)	
New Backup (Incremental)	basic.on...	Backup	Success	Transferred: 3.9 KB...	2/22/2...	2/22/2...	SRV0101	Default Backup Repository	
Full Backup - copy job	abc.onmi...	Copy	Success	Transferred: 180.8...	2/21/2...	2/21/2...	172.24.29.1...	Extended Storage (Azure Stora...	
Full Backup - copy job	abc.onmi...	Copy	Success	Transferred: 0 B (0...	2/21/2...	2/21/2...	172.24.29.1...	Extended Storage (Amazon S3...	
Full Backup - copy job	abc.onmi...	Copy	Success	Transferred: 180.8...	2/21/2...	2/21/2...	172.24.29.1...	Extended Storage (Amazon S3...	
Full Backup (Incremental)	abc.onmi...	Backup	Success	Transferred: 354.4...	2/21/2...	2/21/2...	172.24.29.1...	Extended Storage (Amazon S3)	
New Backup (Full)	basic.on...	Backup	Success	Transferred: 3.5 GB...	2/21/2...	2/21/2...	SRV0101	Default Backup Repository	
Full Backup (Incremental)	abc.onmi...	Backup	Success	Transferred: 7.7 M...	2/21/2...	2/21/2...	172.24.29.1...	Extended Storage (Amazon S3)	
Full Backup (Full)	abc.onmi...	Backup	Warning	2 objects failed	2/21/2...	2/21/2...	172.24.29.1...	Extended Storage (Amazon S3)	

Below the table, there is a 'Status' section with 'Session status: Success' and 'Bottleneck: Target'. A 'Data' section shows 'Processing rate: 24.5 KB/s (0 items/s)', 'Read rate: 3.3 MB/s', and 'Write rate: 0 B/s'. A 'Summary' section shows 'Duration: 00:35', 'Objects: 20 of 20', and 'Transferred: 354.4 KB (0 items processed)'. An 'Action' section lists: 'Job started at 2/21/2023 5:23:57 PM', 'Connected to organization', 'Found 20 objects', and 'Found 4 excluded objects'. At the bottom, there are checkboxes for 'Errors', 'Warnings', and 'Success'.

Viewing Backup and Backup Copy Session Metrics

You can view a backup and backup copy session metrics in one of the following ways:

- Open the **Organizations** view and in the inventory pane, select an organization and then select a backup or backup copy job in the preview pane.
- Open the **History** view and in the inventory pane, select the **Jobs > Backup** or **Jobs > Copy** node and then select a backup or backup copy session in the preview pane.

Status		Data		Summary	
Session status:	Success	Processing rate:	584.4 KB/s (72 items/s)	Duration:	38:33
Bottleneck:	Target	Read rate:	2.1 MB/s	Objects:	5 of 5
		Write rate:	86.4 KB/s	Transferred:	2.3 GB (4948 items processed)

Metrics of a backup or backup copy session consist of the following sections:

- The **Status** section that shows the following fields:
 - **Session status.** The current state of the selected session.
 - **Bottleneck.** A bottleneck value.

This value may be: **Detecting**, **Source**, **Target** and **N/A**.

 - The **Detecting** state is displayed when a backup or backup copy job is started and Veeam Backup for Microsoft 365 has not calculated the bottleneck value.
 - The **Source** state is displayed when a bottleneck occurs during download.

For example, if you have a slow connection or problems occur on the internet provider side and your connection speed drops significantly, the bottleneck value will typically be shown as **Source**.
 - The **Target** state is displayed when a bottleneck occurs during writing data to disk.

For example, if you are using a hard drive that is fragmented or an old type of the hard drive, the bottleneck value will typically be shown as **Target**.
 - The **N/A** state is displayed when no bottleneck occurs.
 - **Last Backup.** The date and time of the last backup or backup session.
- The **Data** section that shows the following fields:
 - **Processing rate.** Shows the processing rate.
 - **Read rate.** Shows the download speed.
 - **Write rate.** Shows the writing speed.
- The **Summary** section that shows the following fields:
 - **Duration.** The duration of the backup or backup copy session.

- **Objects.** Shows how many objects have been backed up or copied during the session.

An object is an OneDrive account, SharePoint site, Microsoft Teams team, mailbox and archive mailbox, including group mailboxes, public folders and discovery search mailboxes.

- **Transferred.** Shows how many bytes have been downloaded.

Viewing Retrieve Session Metrics

You can view a retrieve session metrics in one of the following ways:

- Open the **Organizations** view and in the inventory pane, select the **Data retrieval** node and then select a retrieval job in the preview pane.
- Open the **History** view and in the inventory pane, select the **Retrieve** node and then select a retrieve session in the preview pane.

Info	Status	Summary
Name: Exchange data retrieval	Status: Success	Objects: 3 of 3
Operation: Retrieve	Start Time: 2/21/2023 6:29 PM	
	End Time: 2/22/2023 2:52 AM	

Metrics of a retrieve session consist of the following sections:

- The **Info** section that shows the following fields:
 - **Name.** The name of the retrieve session.
 - **Operation.** The name of the operation.
Can be *Retrieve* or *Remove*.
- The **Status** section that shows the following fields:
 - **Status.** The status of the session.
Can be *Running*, *Success*, *Warning*, or *Error*.
 - **Start Time.** The start time of the session.
 - **End Time.** The end time of the session.
- The **Summary** section that shows the following fields:
 - **Objects.** Shows how many objects have been selected for retrieval of their backed-up data.
An object is an OneDrive account, SharePoint site, Microsoft Teams team, mailbox and archive mailbox, including group mailboxes, public folders and discovery search mailboxes.
 - **Processed.** Shows how many blob files have been downloaded.

Viewing Restore Session Metrics

To view a restore session metrics, do the following:

1. Open the **History** view.
2. In the inventory pane, select the **Restore** node.
3. In the preview pane, select a restore session.

Info	Status
Name: Exchange restore (Job: New Backup - 2/22/2023 2:00:13 A...	Status: Running
Session type: Restore	Start Time: 2/22/2023 6:07 PM
Initiated by: SRV0101\Administrator	

Metrics of a restore session consist of the following sections:

- The **Info** section that shows the following fields:
 - **Name**. The name of the restore session.
 - **Session type**. The session type.
 - **Initiated by**. The user name under which the session has been executed or is still in progress.
- The **Status** section that shows the following fields:
 - **Status**. The status of the session.
Can be *Running*, *Success*, *Warning*, or *Error*.
 - **Start Time**. The start time of the session.
 - **End Time**. The end time of the session.

Performing Search

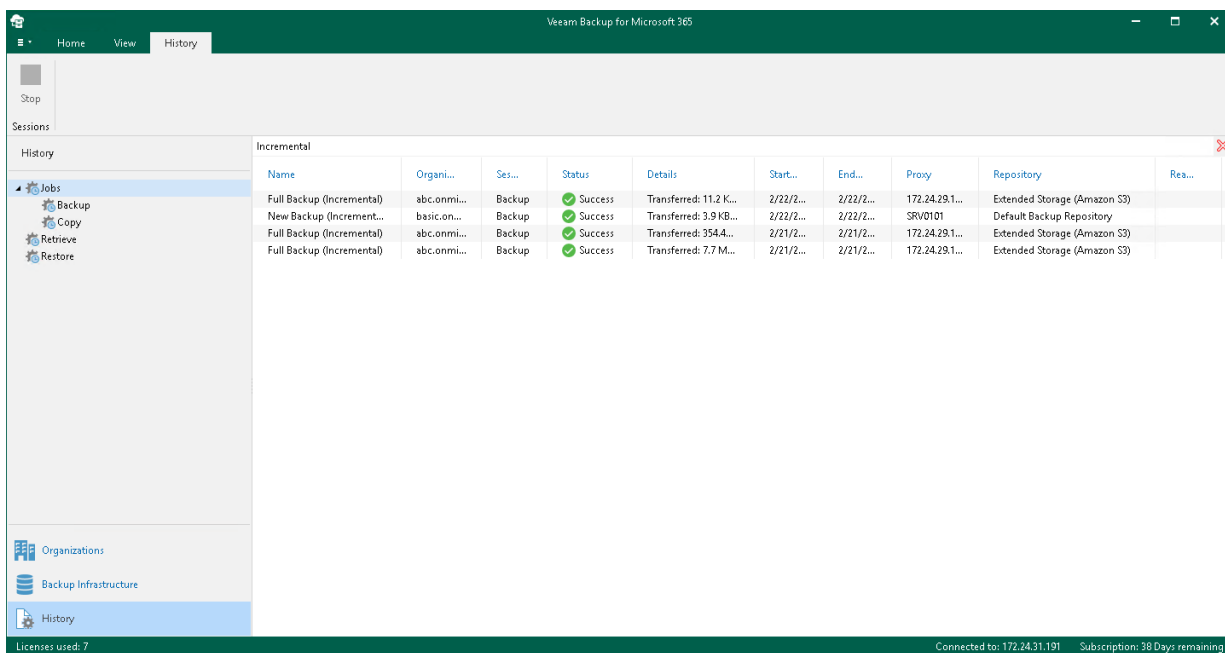
In the History view of the Veeam Backup for Microsoft 365 console, you can search for backup, backup copy, retrieve and restore sessions using keywords.

To search for backup, backup copy, retrieve and restore sessions, do the following:

1. Open the **History** view.
2. Select one of the following nodes:
 - **Jobs**. To search for both backup and backup copy sessions.
 - **Backup**. To search only for backup sessions.
 - **Copy**. To search only for backup copy sessions.
 - **Retrieve**. To search for retrieve sessions.
 - **Restore**. To search for restore sessions.
3. Enter a search query in the search field at the top of the preview pane.

Veeam Backup for Microsoft 365 will display only sessions whose names include keywords that you are searching for.

To remove a keyword, click the cross mark.



Reporting

Veeam Backup for Microsoft 365 allows you to create the following data protection reports:

- [Mailbox Protection Reports](#)
- [Storage Consumption Reports](#)
- [License Overview Reports](#)
- [User Protection Reports](#)

Creating Mailbox Protection Reports

The **Mailbox Protection** reports show statistical information on protected and unprotected mailboxes of your Microsoft 365 and on-premises Microsoft Exchange organizations.

Each report consists of the following fields and shows information per mailbox.

Field	Description
Description	Shows a description of the report.
Reporting Date	Shows the date when the report was created.
License Information	Shows the following: <ul style="list-style-type: none">• Product name• Company name• License type• License expiration date• Support identification number
Summary	<p>Shows the total number of protected and unprotected mailboxes per each organization added to the scope:</p> <ul style="list-style-type: none">• A mailbox is considered protected if it was backed up at least once within the last 31 days.• A mailbox is considered unprotected if it was not backed up at least once within the last 31 days, or if it was not backed up at all. <p>The following types of mailboxes are included in the report:</p> <ul style="list-style-type: none">• <i>Group mailbox</i>• <i>Public mailbox</i>• <i>Shared mailbox</i>• <i>Resource (Equipment and Room) mailbox</i> <p>Renamed organizations will be shown with their original names. For more information about renaming organizations, see Renaming Organizations.</p>

To generate a report, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select an organization for which you want to create a report.

TIP

You can also select the root **Organizations** node to generate a report for all organizations added to the scope.

3. On the **Home** tab, click **Reports > Mailbox Protection**.

The **Generate Report** wizard runs.

4. Click **Browse** to specify a location to save the report.

Use the **Save as type** drop-down list in the **Save As** dialog to select PDF or CSV format in which you want to save the report.

5. Select the **Open report after publishing** check box to open the generated report using the default application.
6. Click **Finish**.

Generate Report

Specify report parameters

Reporting date: 2/22/2023

Save as:

C:\Users\Administrator\Documents\MailboxProtectionReport_2023_02_22_18_25_36.pdf

Browse...

Open report after publishing

Finish Cancel

Creating Storage Consumption Reports

The **Storage Consumption** reports show statistical information on used space in backup repositories and object storage.

Each report consists of the following fields and shows information per repository.

Field	Description
Description	Shows a description of the report.
Reporting Interval	Shows the time interval for which the report was generated.
License Information	Shows the following: <ul style="list-style-type: none">• Product name• Company name• License type• License expiration date• Support identification number
Summary	Shows occupied storage space of all backup repositories added to the scope.
Top 5 Repositories by Storage Usage	Shows top 5 repositories in which data in backups or backup copies occupies the most disk space.
Top 5 Repositories by Growth	Shows top 5 repositories in which the space is occupied most frequently.
Daily Change (GB)	Information is shown per standalone backup repositories and backup repositories that were extended with object storage. For extended backup repositories, Veeam Backup for Microsoft 365 shows the following statistical information: <ul style="list-style-type: none">• Used space that is occupied by cache.• Used space that is occupied by data in backups or backup copies that stored in object storage.
Repository Growth (GB)	

Consider the following:

- Repositories that have no statistical information are not included in the report. No information is available when you added a new backup repository. For more information on how to add a new backup repository, see [Adding Backup Repositories](#).

Since nothing has been placed to a backup repository after it was added, no statistical information is available, therefore, this repository is not included in the report.

- Repositories whose **Daily Change** and **Total Size** values are less than 10 MB are not included in the report.

For example, a report is said to be built starting from *09/01/2021* to *09/30/2021* and the period from *09/01/2021* to *09/09/2021* is empty (both the **Daily Change** and **Total Size** values are less than 10 MB). In this scenario, such a report will only show statistical information starting from *09/10/2021*.

To generate a report, do the following:

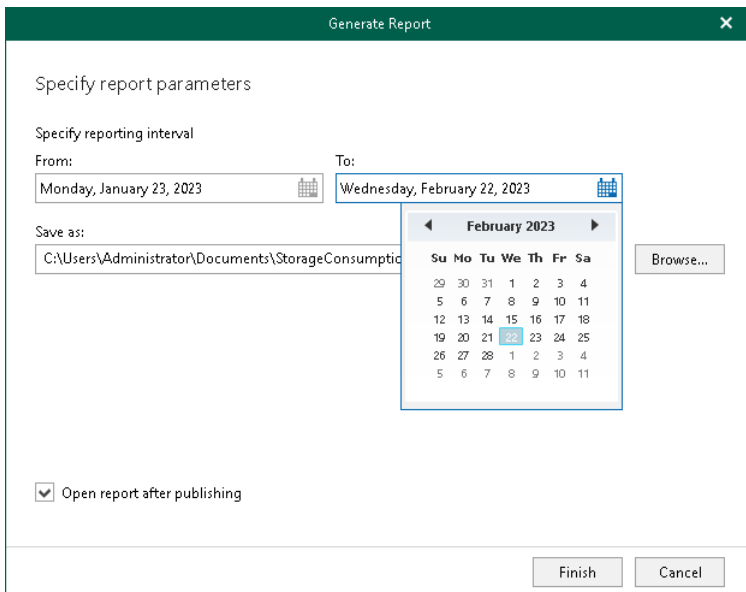
1. Open the **Organizations** view.
2. In the inventory pane, select an organization.
3. On the **Home** tab, click **Reports > Storage Consumption**.

The **Generate Report** wizard runs.

4. Specify a time interval for reporting.
5. Click **Browse** to specify a location to save the report.

Use the **Save as type** drop-down list in the **Save As** dialog to select PDF or CSV format in which you want to save the report.

6. Select the **Open report after publishing** check box to open the generated report using the default application.
7. Click **Finish**.



Creating License Overview Reports

The **License Overview** reports show statistical information on how many licenses are in use and by which organization.

Each report consists of the following fields and shows information per organization consuming the license.

Field	Description
Description	Shows a description of the report.
Reporting Interval	Shows the time interval for which the report is generated. Note: By default, the report is generated for 30 days. If the reporting interval that you set is more than 1 day, the report includes all organizations that consumed the license within the specified period. Even if an organization license expired within the specified period, such organization is included in the report as well.
License Information	Shows the following: <ul style="list-style-type: none">• Product name• Company name• License type• License expiration date• Support identification number
Summary	Shows how many licenses are in use, including licenses for user accounts whose status is <i>new user</i> .
Top 5 Organizations by License Usage	Shows top 5 organizations that consume the license the most.

NOTE

When using a rental license, the *License Overview* report also shows a number of *new user* accounts per each organization. For more information, see [Rental License](#).

To generate a report, do the following:

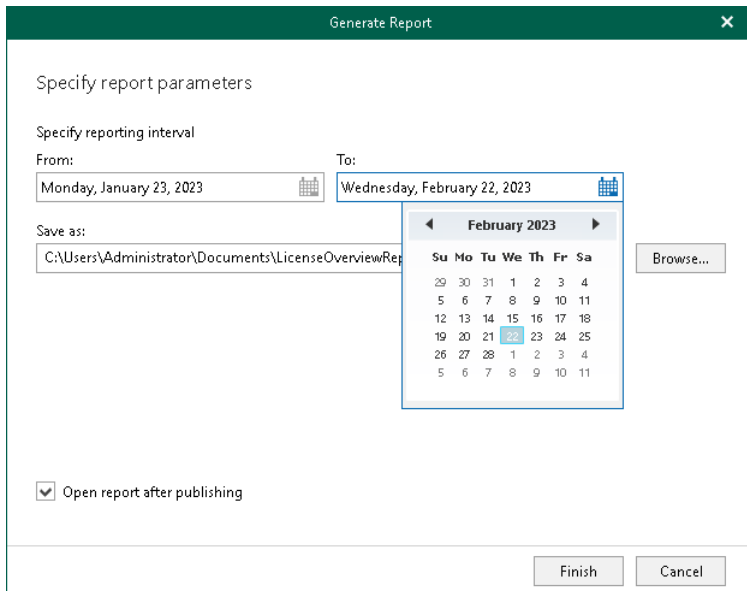
1. Open the **Organizations** view.
2. In the inventory pane, select an organization.
3. On the **Home** tab, click **Reports > License Overview**.
The **Generate Report** wizard runs.
4. Specify a time interval for reporting.

5. Click **Browse** to specify a location to save the report.

Use the **Save as type** drop-down list in the **Save As** dialog to select PDF or CSV format in which you want to save the report.

6. Select the **Open report after publishing** check box to open the generated report using the default application.

7. Click **Finish**.



Creating User Protection Reports

The **User Protection** reports show statistical information on protected and unprotected user accounts of your Microsoft 365 and on-premises Microsoft organizations.

Each report consists of the following fields and shows information per user account.

Field	Description
Description	Shows a description of the report.
Reporting Date	Shows the date when the report was created.
License Information	Shows the following: <ul style="list-style-type: none">• Product name• Company name• License type• License expiration date• Support identification number
Summary	<p>Shows the total number of protected and unprotected users per each organization added to the scope:</p> <ul style="list-style-type: none">• A user is considered protected if both the user is currently added to a backup job and restore points are available for the user data in Veeam Backup for Microsoft 365.• A user is considered unprotected if the user is not added to a backup job and there are no restore points for the user data in Veeam Backup for Microsoft 365.• A user is considered unprotected with restore points if the user is not added to a backup job, but restore points are available for the user data in Veeam Backup for Microsoft 365. <p>Only user accounts are included in the report; group accounts are not included.</p> <p>If an organization was removed from Veeam Backup for Microsoft 365, the report shows information only about users whose data was backed up.</p> <p>Renamed organizations will be shown with their original names. For more information about renaming organizations, see Renaming Organizations.</p>

To generate a report, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select an organization for which you want to create a report.

TIP

You can also select the root **Organizations** node to generate a report for all organizations added to the scope.

3. On the **Home** tab, click **Reports > User Protection**.

The **Generate Report** wizard runs.

4. Click **Browse** to specify a location to save the report.

Use the **Save as type** drop-down list in the **Save As** dialog to select PDF or CSV format in which you want to save the report.

5. Select the **Open report after publishing** check box to open the generated report using the default application.
6. Click **Finish**.

Generate Report

Specify report parameters

Reporting date: 2/22/2023

Save as:

C:\Users\Administrator\Documents\UserProtectionReport_2023_02_22_18_28_14.pdf Browse...

Open report after publishing

Finish Cancel

Managing Log Files

Veeam Backup for Microsoft 365 allows you to collect log files generated by default and enable the extended logging mode. Log files help you and Veeam Customer Support specialists to troubleshoot product operation issues when working with Veeam Backup for Microsoft 365 and Veeam Explorers.

Logs for Veeam Backup for Microsoft 365 Installation and Upgrade

Veeam Backup for Microsoft 365 saves the installation and upgrade log files in the `%ProgramData%\Veeam\Backup365\Logs\Setup` folder. Autorun logs are saved in the `%ProgramData%\Veeam\Backup365\Logs` folder.

Logs for Veeam Backup for Microsoft 365 Components

Veeam Backup for Microsoft 365 creates a separate log file for each of its components and saves them in the `%ProgramData%\Veeam\Backup365\Logs` folder.

Logs for Veeam Backup for Microsoft 365 PowerShell

For PowerShell modules, Veeam Backup for Microsoft 365 saves log files in the `%ProgramData%\Veeam\Backup365\Logs\PowerShell` folder.

If you move a Microsoft organization data from one backup repository to another using the `Move-VBOEntityData` cmdlet, Veeam Backup for Microsoft 365 saves log files in the `%ProgramData%\Veeam\Backup365\Logs\Move` folder.

If you remove a Microsoft organization data from a backup repository using the `Remove-VBOEntityData` cmdlet, Veeam Backup for Microsoft 365 saves log files in the `%ProgramData%\Veeam\Backup365\Logs\Remove` folder.

Logs for Retention

For each backup repository, Veeam Backup for Microsoft 365 creates log files on the product retention activity in the `%ProgramData%\Veeam\Backup365\Logs\Retention\<RepositoryName>` folder.

This folder includes the `Retention_<RepositoryName>_<timestamp>.log` files, where `<RepositoryName>` is the backup repository name.

Logs for Backup and Backup Copy Jobs

For each backup or backup copy job, Veeam Backup for Microsoft 365 saves log files in the `%ProgramData%\Veeam\Backup365\Logs\<organization_name>\<job_name>` folder.

This folder includes the following log files:

- A separate log file for each job session.
- A separate log file for each performed task.

- A summary report file in the HTML format with information about all job sessions and all objects that were processed during each job session.
- An archiver appliance log file if Veeam Backup for Microsoft 365 uses archiver appliance when performing a backup copy job.

Logs for Data Retrieve

Veeam Backup for Microsoft 365 creates a separate log file for each retrieval job. Depending on type of the retrieved data, Veeam Backup for Microsoft 365 saves log files in the following subfolders of the `%ProgramData%\Veeam\Backup365\Logs\<organization_name>` folder:

- Exchange data retrieval
- SharePoint data retrieval
- OneDrive data retrieval
- Teams data retrieval

Logs for Restore Portal

For each restore session that is performed on Restore Portal, Veeam Backup for Microsoft 365 saves logs to the `Veeam.Archiver.Service_<timestamp>` and `Veeam.Archiver.REST_<timestamp>` files located in the `%ProgramData%\Veeam\Backup365\Logs` folder.

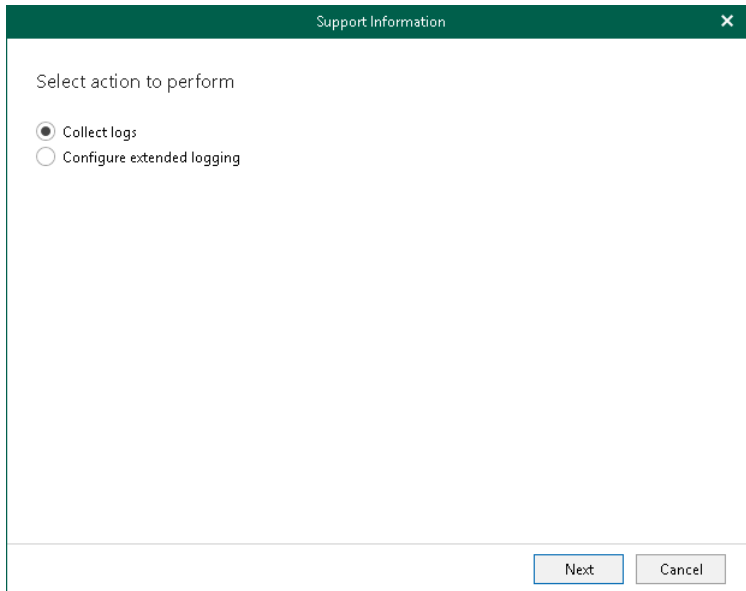
Logs for Veeam Explorers

Log files for Veeam Explorers are saved separately in the `%ProgramData%\Veeam\Backup\<Veeam_Explorer_Name>\Logs` folder.

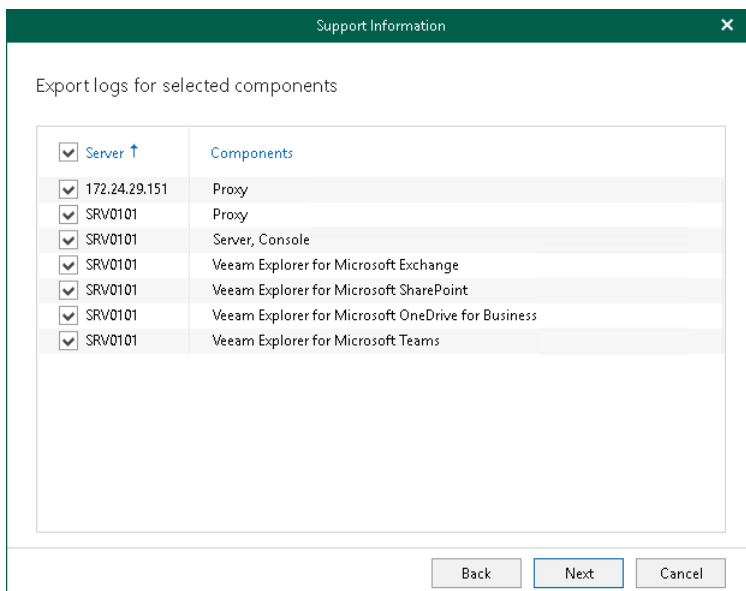
Collecting Log Files

To collect log files, do the following:

1. In the main menu, click **Help and Support > Support information**.
2. Select the **Collect logs** option.



3. Select Veeam Backup for Microsoft 365 infrastructure components for which to obtain log files. If Veeam Explorers are installed on the machine that runs Veeam Backup for Microsoft 365, you can select them as well.



4. Specify a time period for log export:
 - Select the **Collect logs for the last N days** option to specify the number of days for which to export your log files.
 - Select the **Collect logs for the specified time period** option to set up a period for log files export.

- Select the **Collect all logs** option to export all existing log files regardless of the time period.

Support Information

Specify the time period to perform logs export for

Collect logs for the last days

Collect logs for the specified time period

From: To:

Collect all logs

February 2023

Su	Mo	Tu	We	Th	Fr	Sa
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	1	2	3	4
5	6	7	8	9	10	11

Back Next Cancel

5. Specify the path.

Support Information

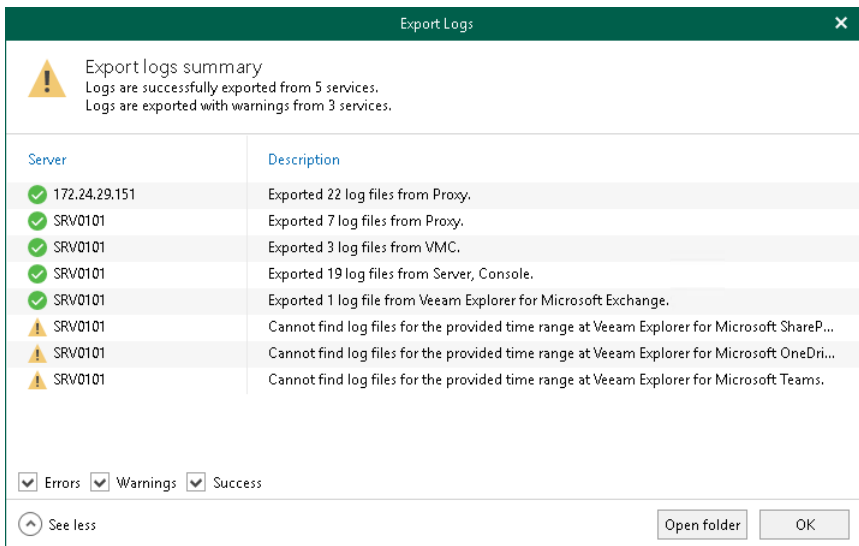
Select location to export the logs to

Path:

Back Finish Cancel

6. Click **Finish**.

Once log files are collected, Veeam Backup for Microsoft 365 prompts you to view logs collection statistics by expanding the **Export Logs** dialog. You can open a folder where log files were exported. To do this, click **Open folder**.



The screenshot shows the 'Export Logs' dialog box with a green header and a close button. It contains a summary section with a warning icon and a table of log export results. The table has two columns: 'Server' and 'Description'. Below the table are filter checkboxes for 'Errors', 'Warnings', and 'Success', and buttons for 'See less', 'Open folder', and 'OK'.

Export logs summary
Logs are successfully exported from 5 services.
Logs are exported with warnings from 3 services.

Server	Description
172.24.29.151	Exported 22 log files from Proxy.
SRV0101	Exported 7 log files from Proxy.
SRV0101	Exported 3 log files from VMC.
SRV0101	Exported 19 log files from Server, Console.
SRV0101	Exported 1 log file from Veeam Explorer for Microsoft Exchange.
SRV0101	Cannot find log files for the provided time range at Veeam Explorer for Microsoft ShareP...
SRV0101	Cannot find log files for the provided time range at Veeam Explorer for Microsoft OneDri...
SRV0101	Cannot find log files for the provided time range at Veeam Explorer for Microsoft Teams.

Errors Warnings Success

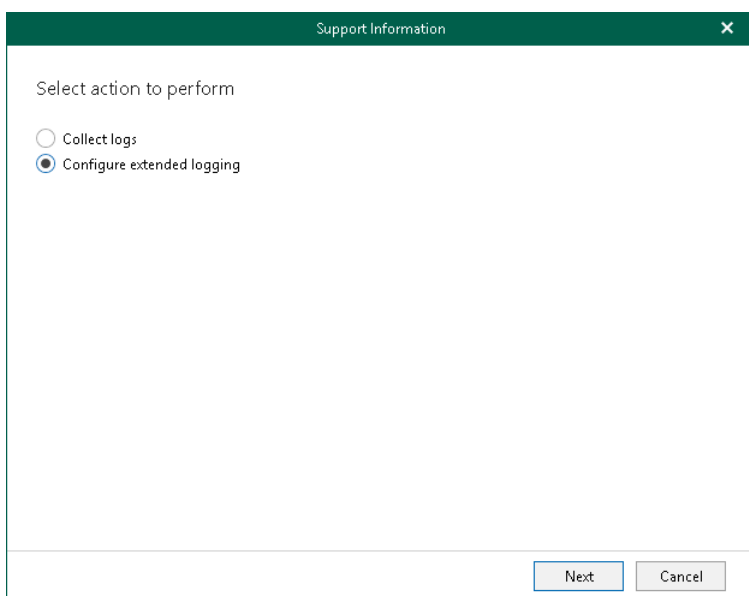
Enabling Extended Logging Mode

Extended logging mode augments log records generated during the Veeam Backup for Microsoft 365 operation. In comparison to log records generated by default, extended log records contain additional information such as more detailed description of operations performed during the backup and restore processes, as well as more detailed description of items processed during backup and restore.

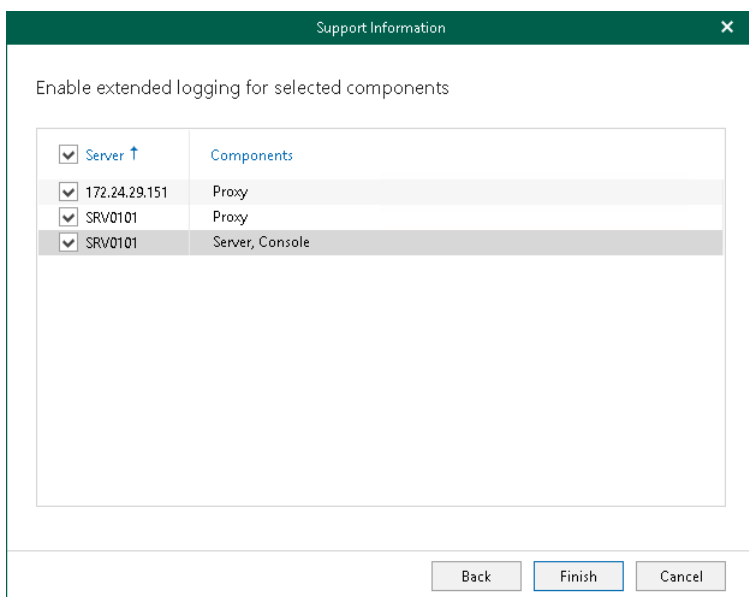
Veeam Customer Support specialists use log files generated in the extended logging mode to troubleshoot product operation issues and may ask you to enable this mode after you report a problem to Veeam Customer Support.

To enable extended logging mode, do the following:

1. In the main menu, click **Help and Support > Support information**.
2. Select the **Configure extended logging** option.



3. Select components (local or remote) to which you want to apply the extended logging mode.



4. Click **Finish**.

After you enable extended logging mode, you need to go back to the main application window and perform actions for which you want to collect additional information. Then you can collect logs. For more information, see [Collecting Log Files](#).

Backup as Service for Microsoft 365

You can configure *Backup as a Service for Microsoft 365* for service providers and tenants.

For Service Providers

To configure *Backup as a Service for Microsoft 365* for service providers, do the following:

1. Install Veeam Backup for Microsoft 365 on a server with Veeam Backup & Replication with the enabled *Cloud Connect* feature.

For more information, see the [Deployment](#) section of this guide and the [Installing Veeam Backup & Replication](#) section of the Veeam Backup & Replication User Guide.

2. Install Veeam Backup for Microsoft 365 and Veeam Backup & Replication licenses.

For more information, see the [Licensing and License Types](#) of this guide and the [Licensing for Service Providers](#) section of the Veeam Cloud Connect Guide.

3. Configure a TLS certificate. For more information, see the [Managing TLS Certificates](#) section of the Veeam Cloud Connect Guide.

Without a certificate, you will not be able to add a *Cloud Gateway* component.

4. Configure a cloud gateway. For more information, see the [Adding Cloud Gateways](#) section of the Veeam Cloud Connect Guide.

5. Add new tenants. For more information, see the [Registering Tenant Accounts](#) section of the Veeam Cloud Connect Guide.

6. Configure your Veeam Backup for Microsoft 365 environment. For more information, see [Configuring Veeam Backup for Microsoft 365](#).

To allow end users from tenant organizations to browse and restore their backups without using Veeam Explorers, a service provider can use the following:

- Restore Portal. For more information, see [Data Restore Using Restore Portal](#).
- Web portal created using Veeam Backup for Microsoft 365 REST API. For more information, see [REST API Reference](#).

NOTE

Consider the following:

- Make sure to install Veeam Explorer for Microsoft Exchange, Veeam Explorer for Microsoft SharePoint, Veeam Explorer for Microsoft OneDrive for Business and Veeam Explorer for Microsoft Teams that come as part of the Veeam Backup for Microsoft 365 7 installation package. For more information, see [Installing Veeam Backup for Microsoft 365](#).
- Make sure to install Veeam Backup for Microsoft 365 on a server with Veeam Backup & Replication 10 or later.

Configuring Veeam Backup for Microsoft 365

To configure Veeam Backup for Microsoft 365 on a service provider side, the following actions must be performed:

1. Configure the Veeam Backup for Microsoft 365 environment. For more information on how to configure Veeam Backup for Microsoft 365 settings, see [General Settings](#).
2. Enable tenant authentication to the Veeam Backup for Microsoft 365 server to perform self-restore procedures. For more information, see [Authentication Settings](#).
3. Configure backup proxy servers. For more information, see [Backup Proxy Servers](#).
4. Configure backup repositories. For more information, see [Backup Repositories](#).
5. Add tenant organizations to the Veeam Backup for Microsoft 365 scope. For more information, see [Organization Management](#).
6. Configure backup and backup copy for data in tenant organizations. For more information, see [Data Backup](#) and [Backup Copy](#).
7. Configure data restore using Restore Portal for end users and restore operators from tenant organizations. For more information, see [Configuring Restore Portal for Multiple Tenants](#).

NOTE

As a service provider, you must obtain Microsoft organization credentials of your tenants. The same credentials will be used by tenants to connect to the Veeam Backup for Microsoft 365 server on a service provider side for self-restore procedures using Veeam Explorers.

For Tenants

To configure *Backup as a Service for Microsoft 365* for tenants, do the following:

1. Add a service provider in Veeam Backup & Replication. For more information, see the [Connecting to Service Providers](#) section of the Veeam Cloud Connect Guide.
2. Add backups to the Veeam Explorer scope. For more information, see [Exploring Backups in Veeam Explorers](#).

NOTE

Consider the following:

- Make sure to install Veeam Explorer for Microsoft Exchange, Veeam Explorer for Microsoft SharePoint, Veeam Explorer for Microsoft OneDrive for Business and Veeam Explorer for Microsoft Teams that come as part of the Veeam Backup for Microsoft 365 7 installation package. For more information, see [Installing Veeam Explorers](#).
- By default, tenants cannot restore anything without the service provider assistance. To be able to perform self-restore procedures, a service provider must configure authentication settings for tenants. For more information, see [Authentication Settings](#).
- Tenants must provide service providers with their Microsoft organization credentials. Tenants can use the same credentials when adding a Veeam Backup for Microsoft 365 service provider server to the Veeam Explorers scope. For more information, see [Exploring Backups in Veeam Explorers](#).

Exploring Backups in Veeam Explorers

To explore backups located on the service provider side, add such backups in Veeam Explorers. For more information, see the following sections of the Veeam Explorers User Guide:

- [Adding Organization Backups in Veeam Explorer for Microsoft Exchange](#)
- [Adding Organization Backups in Veeam Explorer for Microsoft SharePoint](#)
- [Adding Organization Backups in Veeam Explorer for Microsoft OneDrive for Business](#)
- [Adding Organization Backups in Veeam Explorer for Microsoft Teams](#)

NOTE

Consider the following:

- Make sure to have access to the service provider server to be able to explore your backups. For more information on how to grant access, see [Authentication Settings](#).
- [For connection to a service provider using the modern app-only authentication method] The account that you plan to use to log in to Microsoft 365 must be assigned the *Global Administrator* role.

Data Restore Using Restore Portal

Restore Portal is a web-based solution that allows users to perform self-service restore of backed-up data. They can explore and restore Microsoft Exchange, Microsoft SharePoint, Microsoft OneDrive for Business and Microsoft Teams data from backups created by Veeam Backup for Microsoft 365.

Restore Portal offers two scenarios for data restore: *self-service restore* and *operator restore*. For more information about available usage scenarios, see [Restore Portal Usage Scenarios](#).

Veeam Backup for Microsoft 365 users who take part in the Restore Portal usage scenarios can be divided into three groups:

- **Veeam Backup for Microsoft 365 administrators** – IT specialists who use Veeam Backup for Microsoft 365 to protect data in Microsoft organizations. They maintain the Veeam Backup for Microsoft 365 backup infrastructure, configure general application settings including the [REST API](#), [Authentication Settings](#) and [Restore Portal](#) settings, and [assign permissions](#) to users who act as restore operators.
- **Restore operators** – a service provider representatives or other users who restore data from backups created by Veeam Backup for Microsoft 365 for other users.
- **End users** – users of a Microsoft 365 organization who perform self-service restore of their own backed-up data.

If the Veeam Backup for Microsoft 365 administrator in a Microsoft 365 organization has configured the REST API and Restore Portal settings in Veeam Backup for Microsoft 365, restore operators and end users access Restore Portal from any computer and perform all operations in a web browser window. For more information, see [Launching Restore Portal](#) and [Performing Restore](#).

Restore Portal Usage Scenarios

Restore Portal offers users two scenarios for data restore:

- *Self-service restore.* In this scenario, users explore and restore their own data from backups created by Veeam Backup for Microsoft 365. After a user logs in to Restore Portal, only data that Veeam Backup for Microsoft 365 has backed up for this user account is available to explore and restore.
- *Operator restore.* In this scenario, the Veeam Backup for Microsoft 365 administrator specifies a user (or a group in which this user is included) as a *restore operator*.

Restore operators have permissions to explore and restore data from backups for specific organization object types: users, groups (group members only), sites, teams, or the entire Microsoft 365 organization. Permissions are assigned to restore operators when the Veeam Backup for Microsoft 365 administrator adds a *restore operator role*. For more information on how to add a restore operator role, see [Adding Restore Operator Role](#).

After a restore operator logs in to Restore Portal, the product shows backed-up data for objects that the restore operator is allowed to manage – that is, to explore and restore data from backups created by Veeam Backup for Microsoft 365 for these objects.

Restore operators can work separately with data of the managed objects. Restore Portal allows them to switch between the managed objects. For more information on how to select an object whose backed-up data a restore operator will explore and restore, see [Changing Restore Operator Scope](#).

Restore operations that end users and restore operators can perform with the backed-up data are the same in both usage scenarios.

How Restore Portal Works

The following components are involved in the Restore Portal operation:

- Veeam Backup for Microsoft 365 server
- *Veeam Backup for Microsoft 365 REST API Service*
- Microsoft 365 organization
- Restore Portal
- *Veeam Backup Proxy for Microsoft 365 Service*

Veeam Backup for Microsoft 365 uses REST API and Azure AD application when authenticating users to Restore Portal with their Microsoft 365 user account credentials. REST API authorization is based on the [OAuth 2.0 Authorization Framework](#). For more information on how to create and configure Azure AD application to access Restore Portal, see [Creating or Configuring Azure AD Application](#).

Restore Portal uses REST API to communicate with the Veeam Backup for Microsoft 365 server. For more information on how to configure REST API, see [REST API Settings](#).

Data exchange between the Veeam Backup for Microsoft 365 server, Microsoft 365 organization, Azure AD application, *Veeam Backup for Microsoft 365 REST API Service* and Restore Portal is performed using SSL certificates. For more information, see [Installing SSL Certificates](#).

Considerations and Limitations

This section lists considerations and known limitations of Restore Portal.

- Restore Portal is supported only for organizations added to Veeam Backup for Microsoft 365 using the modern app-only authentication method. Azure AD application that you have used to add your Microsoft 365 organization must have [permissions](#) for data restore using an application certificate.
- Backups created for on-premises Microsoft organizations cannot be restored using Restore Portal. For hybrid organizations, Restore Portal allows you to restore only data from backups created for Microsoft 365 organizations.
- Group mailboxes data is not supported for explore and restore using Restore Portal.
- Items of different types that you added to the restore list (for example, mailbox items, OneDrive and SharePoint files) will not be restored simultaneously. You must configure and run different restore operations for Exchange, SharePoint, OneDrive and Teams items.
- Backup copies and backups that were retrieved from backup copies cannot be explored and restored using Restore Portal.
- If you want to restore your backed-up data using Restore Portal in different regions, you must use a separate installation of the Veeam Backup for Microsoft 365 REST API component and a separate Azure AD application in each Microsoft Azure region.

Configuration

Restore Portal is deployed automatically along with the Veeam Backup for Microsoft 365 REST API component installation.

The Veeam Backup for Microsoft 365 administrator can configure Restore Portal for the following backup infrastructures:

- [Single Microsoft 365 Organization](#)
- [Multiple Tenants on Service Provider Side](#)

Configuring Restore Portal for Single Microsoft 365 Organization

If the Veeam Backup for Microsoft 365 administrator wants to allow end users and restore operators in a Microsoft 365 organization to explore and restore data from backups using Restore Portal, the following actions must be performed before users start using the web application:

1. Check that the Veeam Backup for Microsoft 365 REST API component is installed either on the Veeam Backup for Microsoft 365 server or on a separate machine.

Deployment of the Veeam Backup for Microsoft 365 REST API component on a separate machine decreases the load on the backup infrastructure when exploring and restoring data from backups using Restore Portal. For more information, see [Installing Veeam Backup for Microsoft 365](#) to deploy the solution to the Veeam Backup for Microsoft 365 server and [Installing REST API](#) to deploy the Veeam Backup for Microsoft 365 REST API component separately.

2. Enable *Veeam Backup for Microsoft 365 REST API Service*.

This service processes REST API commands and allows Restore Portal to communicate with Veeam Backup for Microsoft 365. For more information, see [REST API Settings](#) if you have deployed the solution on the Veeam Backup for Microsoft 365 server and [Configuring REST API and Restore Portal on Separate Machine](#) if you have installed REST API separately.

3. Enable restore operator authentication to the Veeam Backup for Microsoft 365 server. For more information, see [Authentication Settings](#).

4. Enable Restore Portal and configure access to it. For more information, see [Restore Portal Settings](#) if you have deployed the solution on the Veeam Backup for Microsoft 365 server and [Configuring REST API and Restore Portal on Separate Machine](#) if you have installed REST API separately.

5. Add restore operator roles to assign permissions to users who act as restore operators. For more information, see [Adding Restore Operator Role](#).

6. Provide end users and restore operators with the Restore Portal web address.

Configuring Restore Portal for Multiple Tenants

NOTE

Follow these steps as a part of *Backup as a Service for Microsoft 365* usage scenario. For more information, see [Backup as Service for Microsoft 365](#).

On Service Provider Side

To configure access for end users and restore operators from tenant organizations to Restore Portal, the following actions must be performed on a service provider side before users start using the web application:

1. Check that the Veeam Backup for Microsoft 365 REST API component is installed either on the Veeam Backup for Microsoft 365 server or on a separate machine.

Deployment of the Veeam Backup for Microsoft 365 REST API component on a separate machine decreases the load on the backup infrastructure when exploring and restoring data from backups using Restore Portal. For more information, see [Installing Veeam Backup for Microsoft 365](#) to deploy the solution to the Veeam Backup for Microsoft 365 server and [Installing REST API](#) to deploy the Veeam Backup for Microsoft 365 REST API component separately.

2. Enable *Veeam Backup for Microsoft 365 REST API Service*.

This service processes REST API commands and allows Restore Portal to communicate with Veeam Backup for Microsoft 365. For more information, see [REST API Settings](#) if you have deployed the solution on the Veeam Backup for Microsoft 365 server and [Configuring REST API and Restore Portal on Separate Machine](#) if you have installed REST API separately.

3. Enable tenant and restore operator authentication to the Veeam Backup for Microsoft 365 server. For more information, see [Authentication Settings](#).
4. Enable Restore Portal and configure access to it. For more information, see [Restore Portal Settings](#) if you have deployed the solution on the Veeam Backup for Microsoft 365 server and [Configuring REST API and Restore Portal on Separate Machine](#) if you have installed REST API separately.

IMPORTANT

Azure AD application that end users and restore operators from tenant organizations will use to access Restore Portal must be created for a Microsoft 365 organization on a service provider side.

5. Run the [Install-Module](#) cmdlet to install the Microsoft Graph PowerShell module. For more information, see [this Microsoft article](#).
6. Share the configured Azure AD application with all tenant organizations.

To do this, authenticate to Microsoft Entra ID (formerly Azure Active Directory) using the [Connect-AzureAD](#) cmdlet and then run the [New-AzureADServicePrincipal](#) cmdlet. Specify an application ID of Azure AD application configured for authentication to Restore Portal as the `AppId` parameter value.

```
Connect-AzureAD  
New-AzureADServicePrincipal -AppId "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX"
```

7. Configure access to Restore Portal on each tenant side. For more information, see [On Tenant Side](#).
8. Add restore operator roles to assign permissions to users who act as restore operators. For more information, see [Adding Restore Operator Role](#).
9. Provide end users and restore operators with the Restore Portal web address.

On Tenant Side

Perform the following actions for all tenant organizations before users start using the web application:

1. Run the [Install-Module](#) cmdlet to install the Microsoft Graph PowerShell module. For more information, see [this Microsoft article](#).

2. Authenticate to Microsoft Entra ID (formerly Azure Active Directory) using the [Connect-AzureAD](#) cmdlet and then run the [New-AzureADServicePrincipal](#) cmdlet. Specify an application ID of Azure AD application configured by a service provider for authentication to Restore Portal as the `AppId` parameter value.

```
Connect-AzureAD  
New-AzureADServicePrincipal -AppId "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX"
```

3. Sign in to the tenant organization Azure portal.
4. Go to **Microsoft Entra ID > Enterprise applications**.
5. Search for Azure AD application configured for authentication to Restore Portal by *ObjectID* that you have obtained at step 2. Alternatively, you can get ObjectID by running the following command:

```
Get-AzureADServicePrincipal -Filter "AppId eq 'XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX'"
```

Specify an application ID of Azure AD application configured by a service provider for authentication to Restore Portal as the `AppId` parameter value.

6. Go to the application permissions and grant admin consent to this application on behalf of all users in the tenant organization. For more information, see [this Microsoft article, Permissions for Authentication to Restore Portal](#) and contact Veeam Customer Support.

Adding Restore Operator Role

In the operator restore scenario, Veeam Backup for Microsoft 365 administrators must add restore operator roles.

When adding a restore operator role, they select organization users or groups and assign permissions to them. Such users or groups become restore operators. Restore operators are allowed to explore and restore data from backups created by Veeam Backup for Microsoft 365 for specific organization object types: users, groups (group members only), sites, teams, or the entire Microsoft 365 organization.

To add a restore operator role, [check prerequisites](#) and do the following:

1. [Launch the New Restore Operator Role wizard](#).
2. [Specify a role name](#).
3. [Select Microsoft organization](#).
4. [Select restore operators](#).
5. [Select objects to manage](#).
6. [Select objects to exclude](#).

Before You Begin

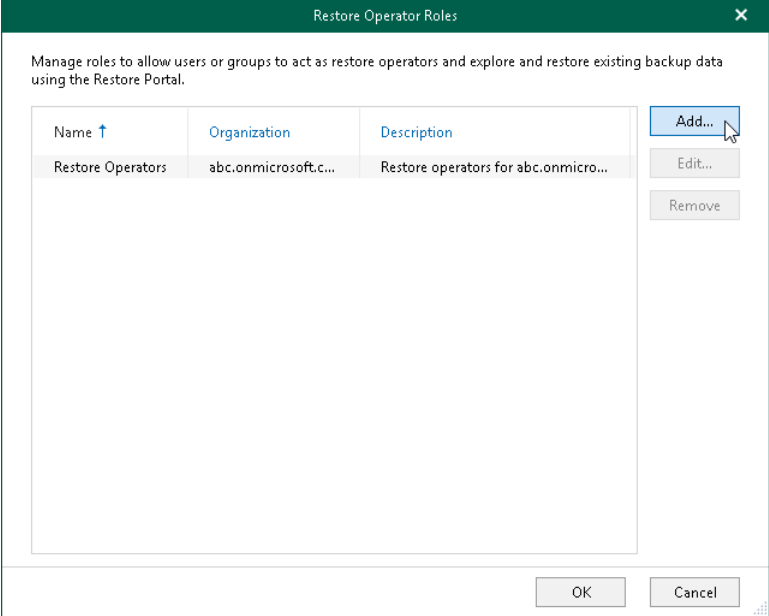
Before you add a restore operator role, check the following prerequisites:

- You can add restore operator roles for users and groups of Microsoft 365 organizations and hybrid organizations. Keep in mind that for hybrid organizations, only Microsoft 365 objects can be processed.
- The organization for which you want to add a restore operator role must be added to Veeam Backup for Microsoft 365 using the modern app-only authentication method.

Step 1. Launch New Restore Operator Role Wizard

To launch the **New Restore Operator Role** wizard, do the following:

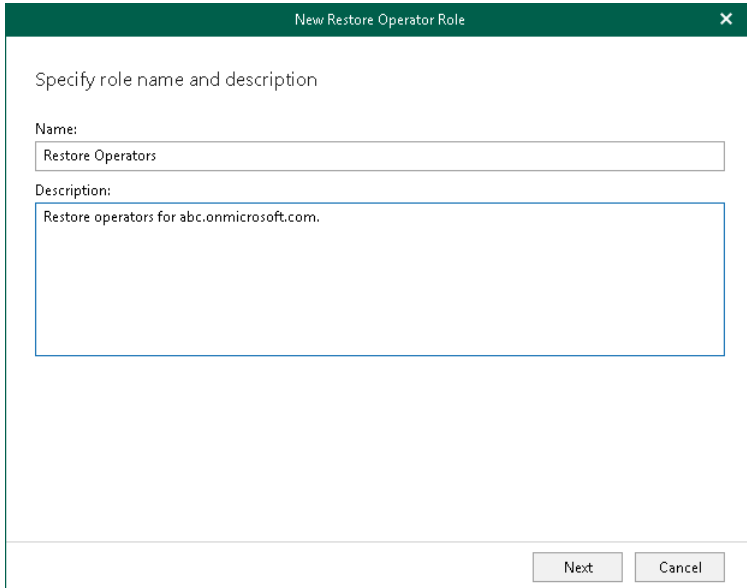
- 1. In the main menu, click **Restore Operator Roles**.
- 2. In the **Restore Operator Roles** window, click **Add**.



Step 2. Specify Role Name

At this step of the wizard, enter a name for the restore operator role and provide optional description:

1. In the **Name** field, enter a name for the restore operator role.
2. In the **Description** field, enter optional description.



New Restore Operator Role

Specify role name and description

Name:
Restore Operators

Description:
Restore operators for abc.onmicrosoft.com.

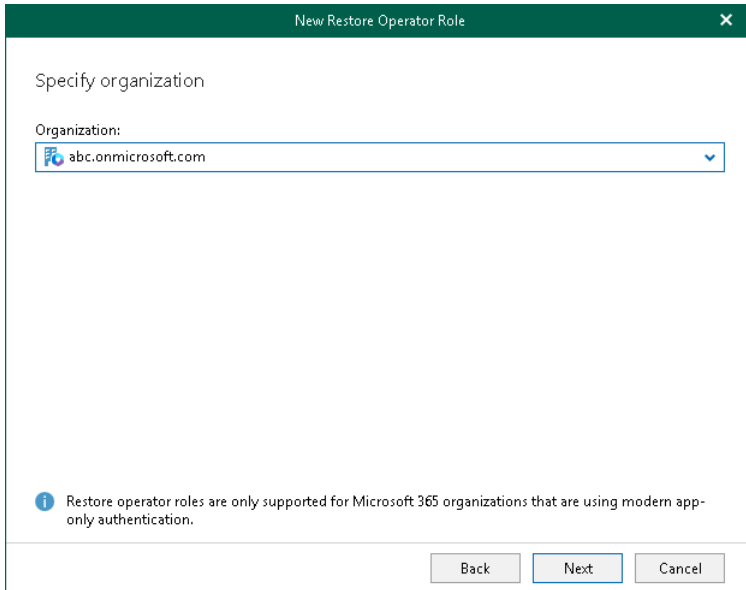
Next Cancel

Step 3. Select Organization

At this step of the wizard, from the **Organization** drop-down list, select an organization whose users or groups will act as restore operators.

Consider the following:

- You can add restore operator roles only for Microsoft 365 organizations and hybrid organizations.
- The organization for which you want to add a restore operator role must be added to Veeam Backup for Microsoft 365 using the modern app-only authentication method.



New Restore Operator Role

Specify organization

Organization:

abc.onmicrosoft.com

Restore operator roles are only supported for Microsoft 365 organizations that are using modern app-only authentication.

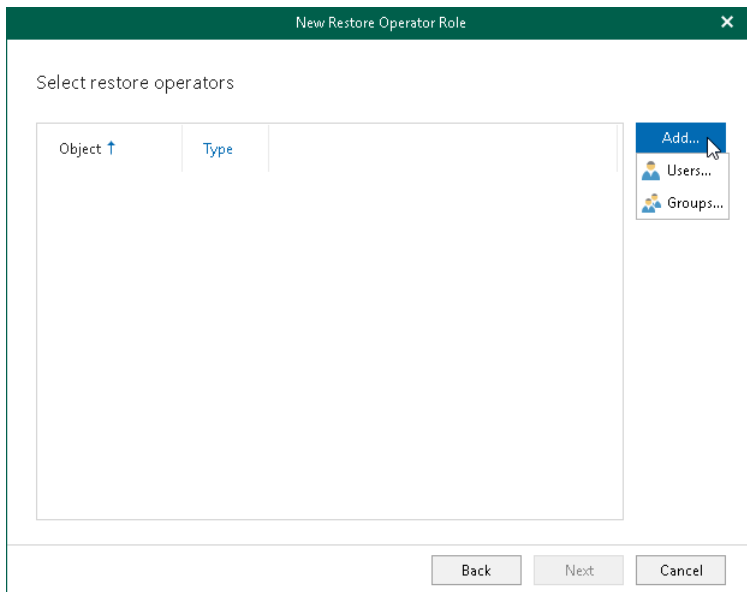
Back Next Cancel

Step 4. Select Restore Operators

At this step of the wizard, select users or groups that you want to act as restore operators. Keep in mind that for hybrid organizations, only Microsoft 365 objects can be processed.

To select restore operators, do the following:

1. Click **Add** and select either *Users* or *Groups*.

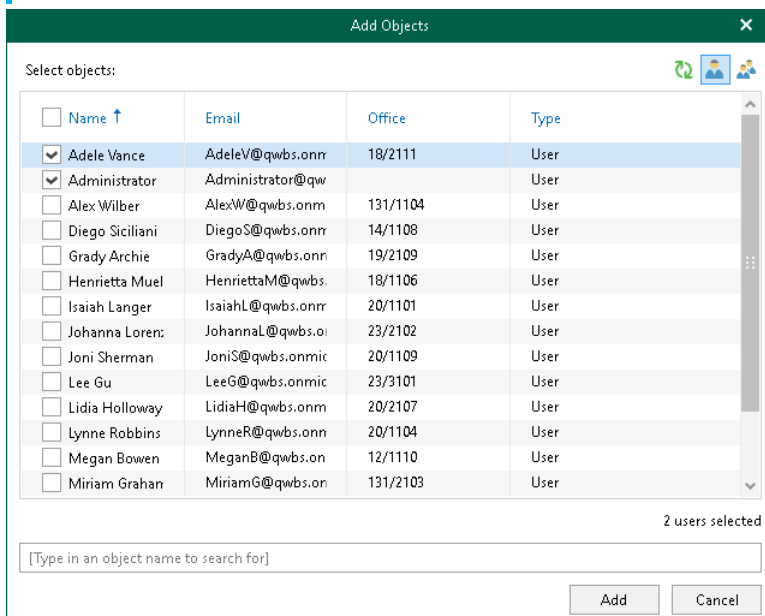


2. In the **Add Objects** window, select check boxes next to the users or groups that you want to act as restore operators.

TIP

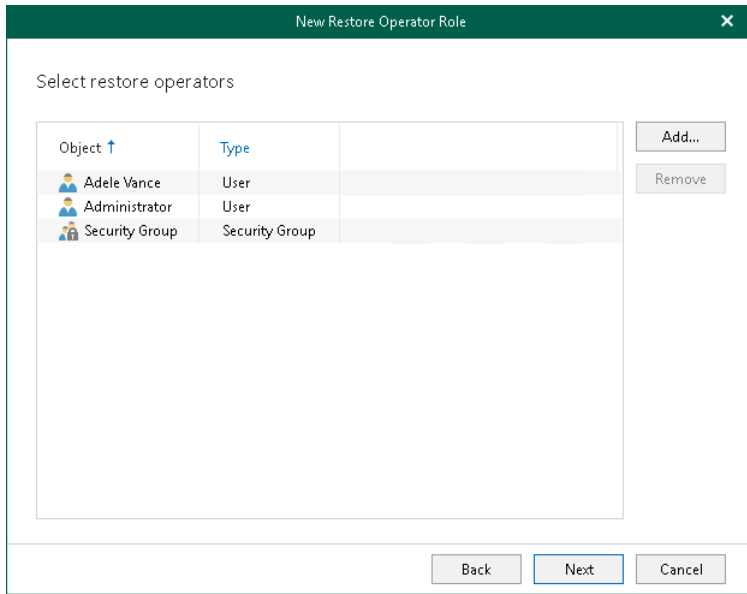
Consider the following:

- To switch between objects of different types, you can click the buttons in the upper-right corner.
- To refresh the objects list, you can click **Refresh**.
- To quickly find necessary objects, you can use the search field at the bottom.



3. Click **Add**.

The selected objects appear in the list of restore operators.



Step 5. Select Objects to Manage

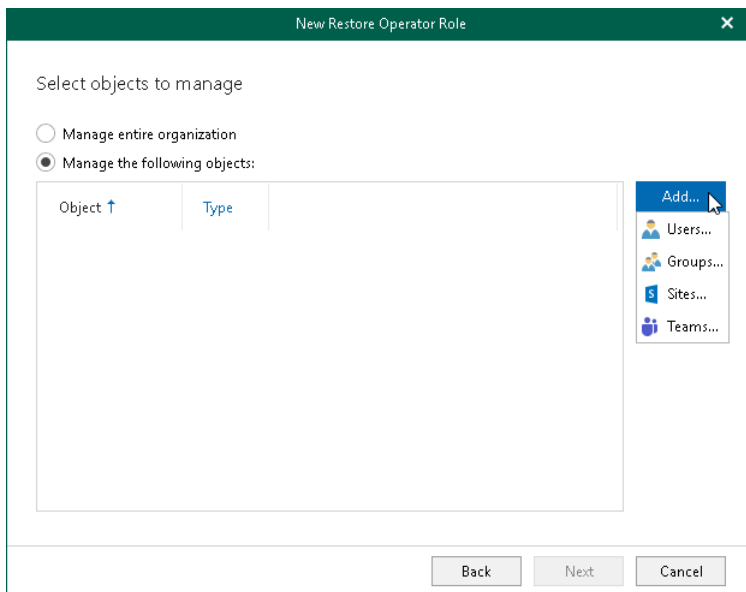
At this step of the wizard, select objects to manage. Restore operators will be able to explore and restore backed-up data of these objects using Restore Portal.

You can select either the entire organization or specific users, groups, sites, and teams.

To select objects to manage, do the following:

1. Select one of the following options:
 - **Manage entire organization** to allow restore operators to explore and restore data from backups created by Veeam Backup for Microsoft 365 for all objects within the selected Microsoft 365 organization.

Keep in mind that if a restore operator is allowed to explore and restore data from backups created by Veeam Backup for Microsoft 365 for the entire Microsoft 365 organization, changing a restore operator scope may take a considerable time.
 - **Manage the following objects** to allow restore operators to explore and restore data from backups created by Veeam Backup for Microsoft 365 for specific users, groups, sites, or teams.
2. If you selected the **Manage the following objects** option, click **Add** and select one of the following options: *Users*, *Groups*, *Sites*, or *Teams*.

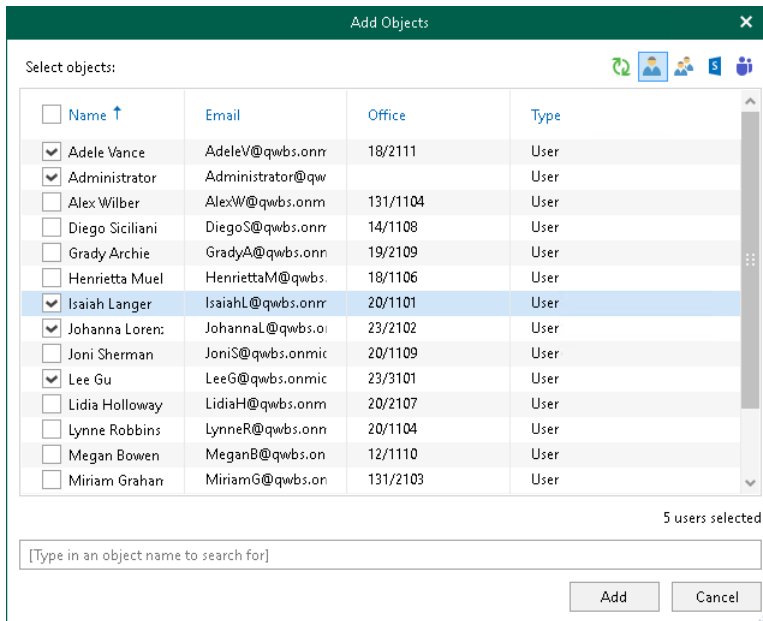


3. In the **Add Objects** window, select check boxes next to the users, groups, sites, or teams whose backed-up data the restore operators will be able to explore and restore using Restore Portal.

TIP

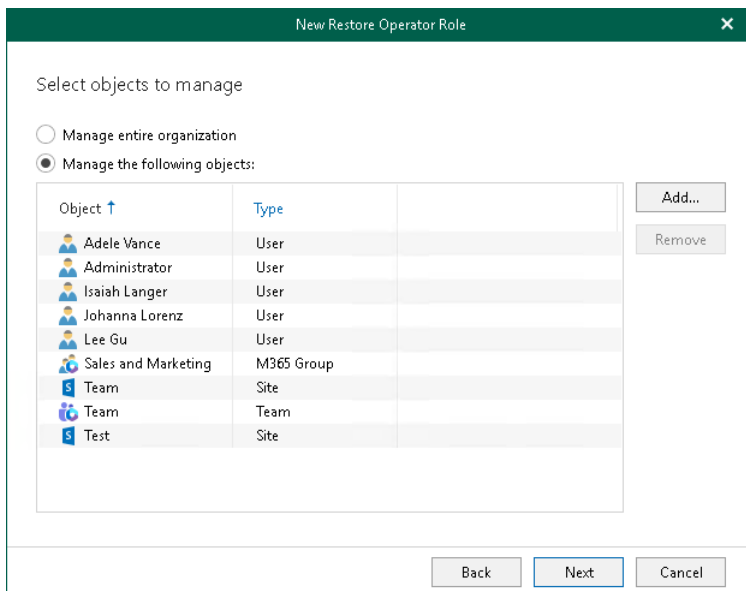
Consider the following:

- To switch between objects of different types, you can click the buttons in the upper-right corner.
- To refresh the objects list, you can click **Refresh**.
- To quickly find necessary objects, you can use the search field at the bottom.



4. Click **Add**.

The selected objects appear in the list of objects to manage.



Step 6. Select Objects to Exclude

At this step of the wizard, select objects to exclude. Restore operators will be prohibited to explore and restore backed-up data of these objects using Restore Portal.

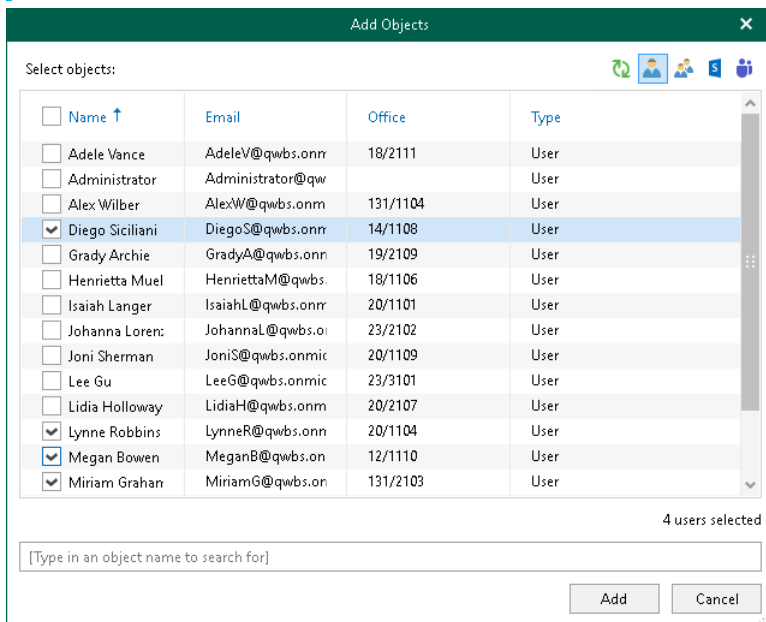
To exclude objects, do the following:

1. Click **Add** and select one of the following options: *Users, Groups, Sites, or Teams*.
2. In the **Add Objects** window, select check boxes next to the users, groups, sites, or teams whose backed-up data the restore operators will be prohibited to explore and restore using Restore Portal.

TIP

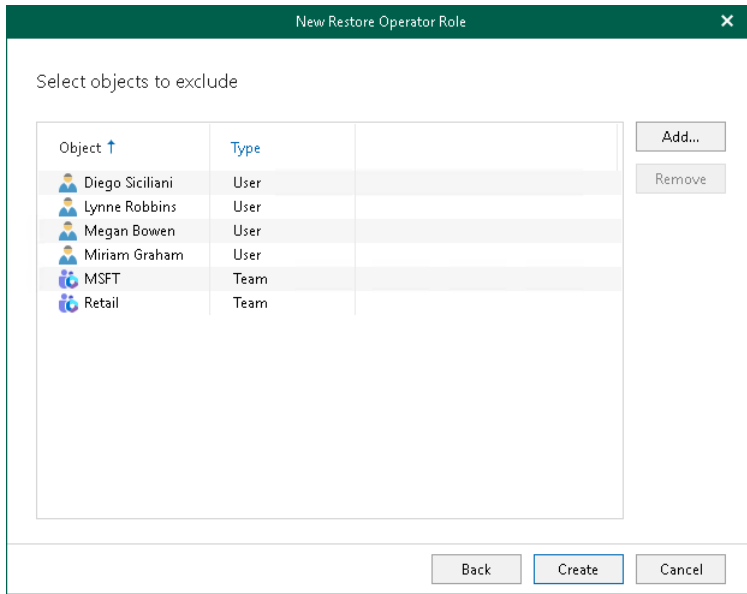
Consider the following:

- To switch between objects of different types, you can click the buttons in the upper-right corner.
- To refresh the objects list, you can click **Refresh**.
- To quickly find necessary objects, you can use the search field at the bottom.



3. Click **Add**.

The selected objects appear in the list of objects to exclude.



Editing Restore Operator Role Settings

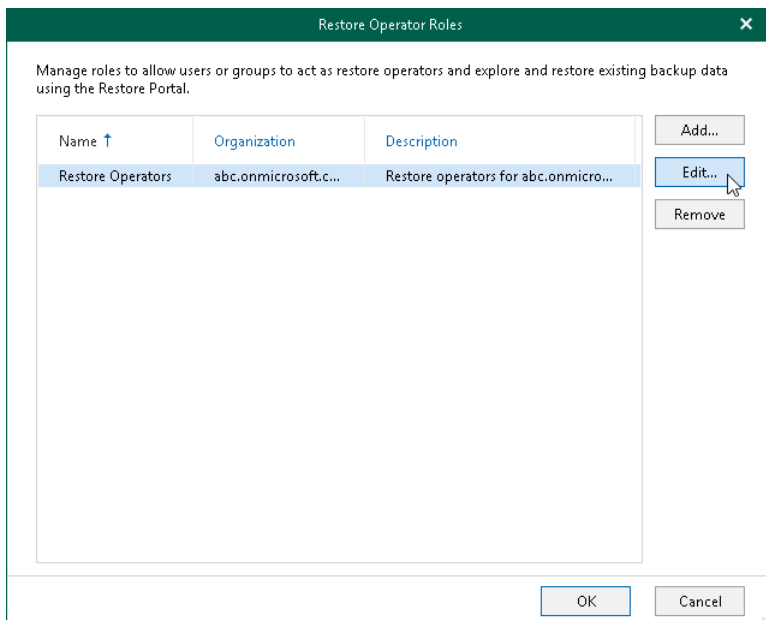
Veeam Backup for Microsoft 365 allows you to edit restore operator role settings.

To edit settings of a restore operator role, do the following:

1. In the main menu, click **Restore Operator Roles**.
2. In the **Restore Operator Roles** window, select a restore operator role and click **Edit**.
3. Modify the required settings.

You can change the following parameters:

- The name and description of a restore operator role.
- The list of restore operators.
- The lists of objects whose backed-up data the restore operators will and will not be able to explore and restore using Restore Portal.

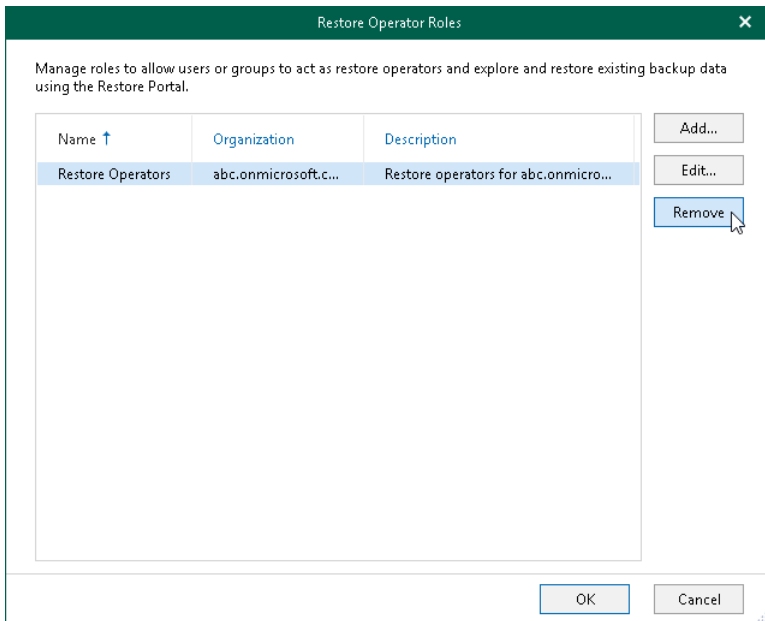


Removing Restore Operator Role

You can remove a restore operator role from the Veeam Backup for Microsoft 365 configuration if you no longer need it.

To remove a restore operator role, do the following:

1. In the main menu, click **Restore Operator Roles**.
2. In the **Restore Operator Roles** window, select a restore operator role and click **Remove**.



Launching Restore Portal

To launch Restore Portal, do the following:

1. Open a web browser on any computer and navigate to the Restore Portal web address.

Consider the following:

- The web address must be specified in one of the following formats:
 - `https://<IPv4 address>:<port number>`, where `<IPv4 address>` is a public IPv4 address of a machine with the Veeam Backup for Microsoft 365 REST API component installed. For example, `https://135.169.170.192:4443`.
 - `https://<DNS hostname>:<port number>`, where `<DNS hostname>` is DNS hostname of a machine with the Veeam Backup for Microsoft 365 REST API component installed. For example, `https://portal.abc.com:4443`.
- The Restore Portal web address must be provided by the Veeam Backup for Microsoft 365 administrator.

NOTE

You can access Restore Portal using the only URI that was specified by the Veeam Backup for Microsoft 365 administrator when registering a new Azure AD application for authentication to Restore Portal. To add another URI or edit the application, the Veeam Backup for Microsoft 365 administrator must configure the application settings in the Microsoft Entra ID (formerly Azure Active Directory). For more information on how to configure the Restore Portal web address, see [Creating or Configuring Azure AD Application](#).

- You do not need any Veeam Backup for Microsoft 365 components or Veeam Explorers installed on a computer that you use to access Restore Portal.
 - Internet Explorer is not supported. To access Restore Portal, use Microsoft Edge (version 79 or later), Mozilla Firefox (version 21 or later) or Google Chrome (version 24 or later).
2. On the welcome page, enter a user account that you use to connect to the Microsoft 365 organization.

You must provide a user account in one of the following formats: `user@domain.com` or `user@domain.onmicrosoft.com`.

3. Click **Log In**.

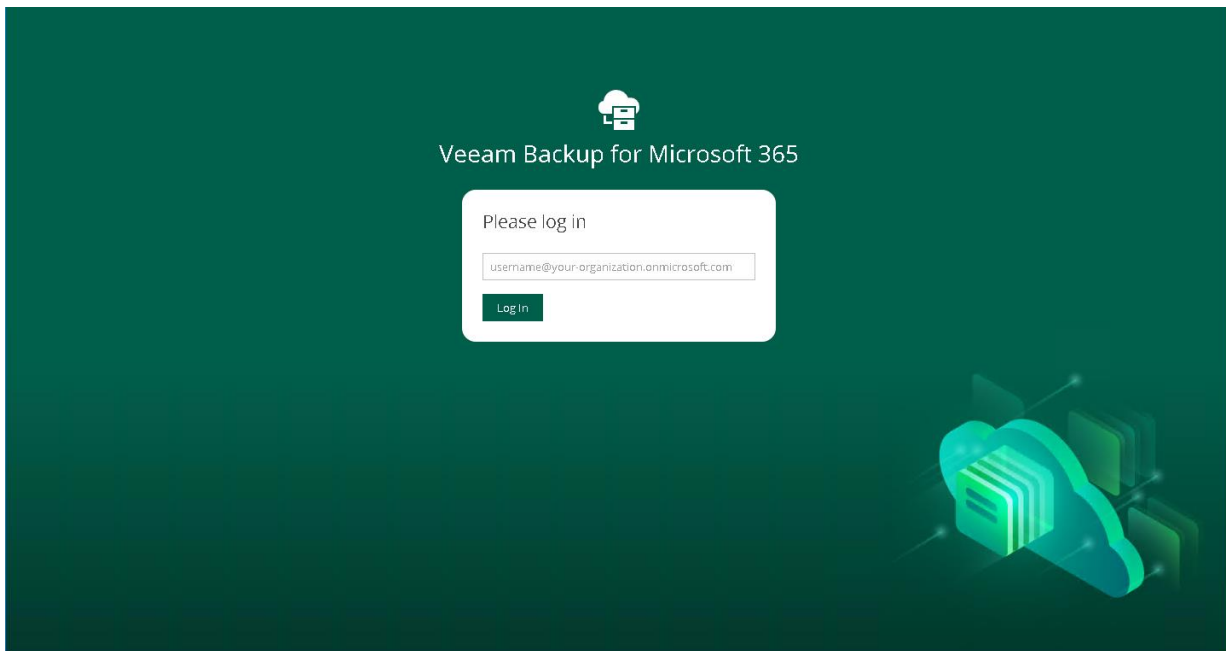
Restore Portal will redirect you to the Microsoft authentication portal where you will be prompted to enter your Microsoft 365 user account password.

NOTE

If multi-factor authentication (MFA) is enabled in the Microsoft 365 organization, the Microsoft authentication portal also will prompt the user to verify the user identity using an additional verification method.

4. If you are a restore operator, select an object that you want to manage. For more information, see [Changing Restore Operator Scope](#).

5. Select a restore point from which you want to explore and restore data from backups created by Veeam Backup for Microsoft 365. For more information on how to view and select available restore points in Restore Portal, see [Selecting Restore Point](#).



Logging Out

To log out of Restore Portal, in the upper-right corner of the Restore Portal window, click the user name and click **Log Out**.

After you log out, all sessions that were opened by Veeam Backup for Microsoft 365 to explore backed-up data are stopped. Restore sessions with restore operations that are running on Restore Portal will continue in the background till data restore completes.

User Interface

The web-based user interface of Restore Portal is designed to let you quickly explore backed-up Microsoft Exchange, Microsoft SharePoint, Microsoft OneDrive for Business and Microsoft Teams data in one window. Also, it allows you to perform restore operations without using Veeam Explorers and view details about restore sessions progress and results and the restore sessions history.

The main window consists of the **Explore**, **Restore Sessions** and **Restore List** tabs.

Explore Tab

This tab contains the navigation and preview panes.

Navigation Pane

The navigation pane allows you to do the following:

- If you are a restore operator, you can select an object that you want to manage. For more information, see [Changing Restore Operator Scope](#).
- Select a restore point from which you want to explore and restore data from backups created by Veeam Backup for Microsoft 365. For more information, see [Selecting Restore Point](#).
- Browse through the hierarchy of folders with backed-up data. Nodes with Microsoft Exchange, Microsoft OneDrive for Business, Microsoft SharePoint and Microsoft Teams data are displayed in the navigation pane separately. Availability of nodes differs depending on backups created by Veeam Backup for Microsoft 365 for an object whose backed-up data is explored at the moment.

For example, for a *user* object the following data can be displayed:

- Exchange Online mailbox
- Archive mailbox
- OneDrive for Business
- Personal Site (available only for restore operators)

For restore operators, Restore Portal displays data for user objects, SharePoint sites and teams that restore operators are allowed to explore.

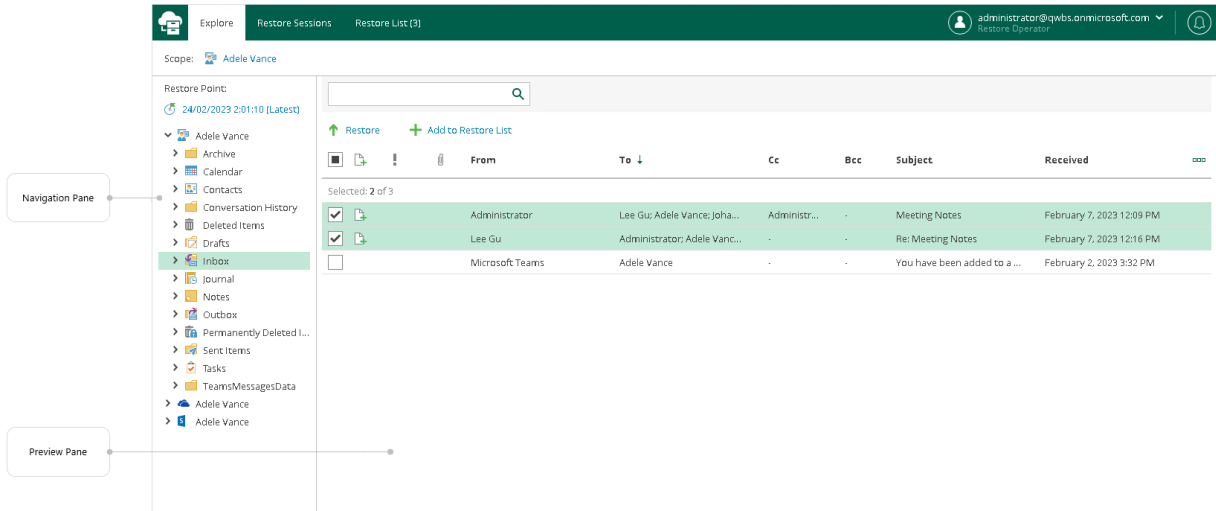
Preview Pane

The preview pane allows you to view details about items that are contained in a folder you have selected in the navigation pane. Items are displayed according to the selected restore point. You can search items and select items that you want to restore or add to the restore list.

NOTE

Consider the following:

- Restore Portal displays up to 2000 items, so search for specific items.
- You can use logical upper-cased operators such as *AND*, *OR* and *NOT*.

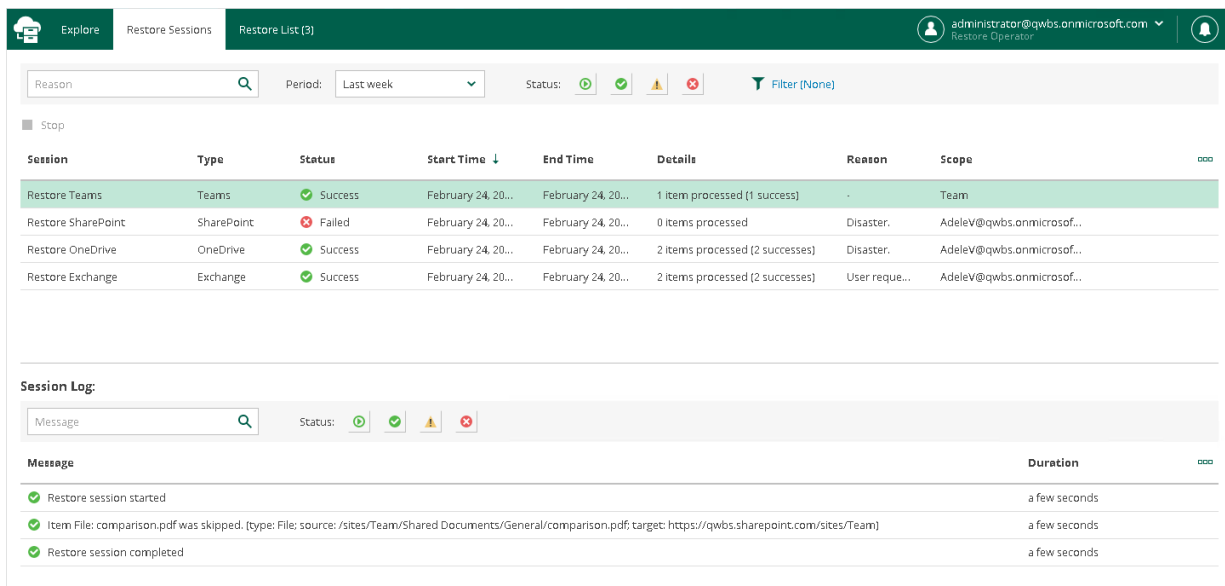


Restore Sessions Tab

On this tab, you view details about restore session progress and results.

You can do the following:

- Stop a restore session.
- Search and filter restore sessions by type, status and time period.
- View the list of events that occurred during a restore session, search and filter events by their status.

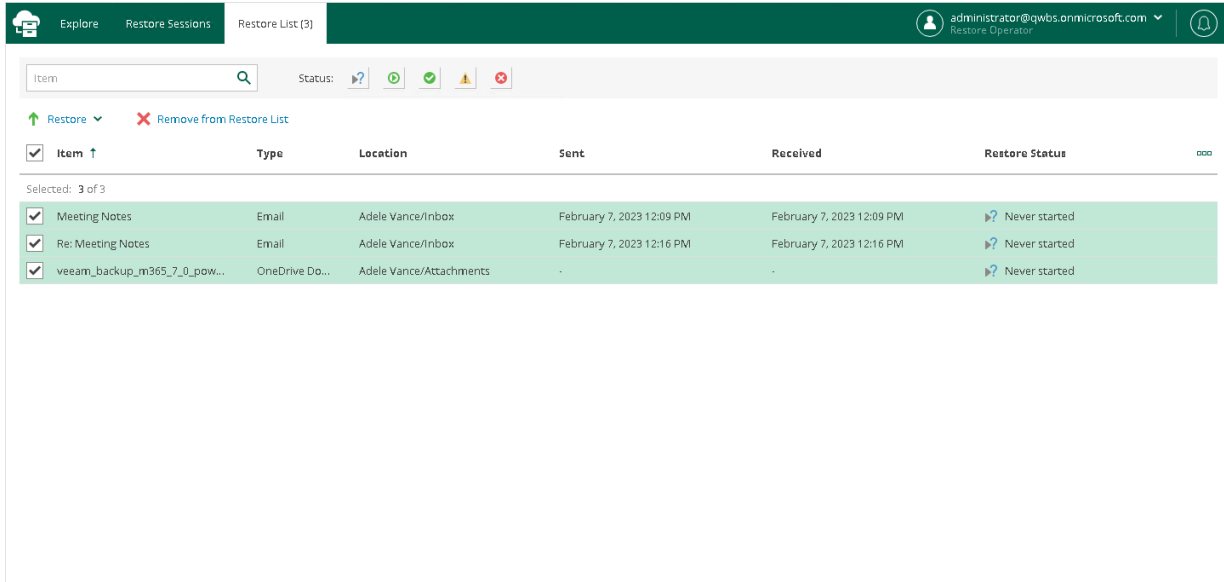


Restore List Tab

On this tab, you view and edit the content of the restore list. This tab appears only if a restore list is not empty.

You can do the following:

- Select items that you want to restore.
- Remove items from the restore list.
- Search and filter items by their restore status.



Notification Pane

Notification pane is hidden in the upper-right corner of the Restore Portal window under the *notification* icon shaped like a bell.

To expand the notification pane, click the notification icon.

For more information, see [Managing Notifications](#).

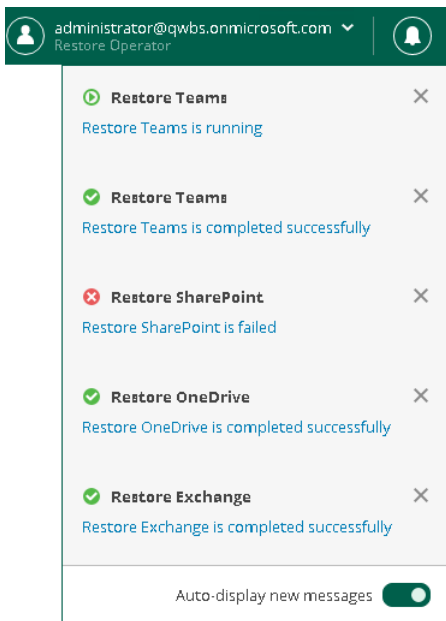
Managing Notifications

Restore Portal notifies you about restore sessions results. Notifications appear in the [notification pane](#).

Each notification includes a restore session name, a status icon, and a status link. If you click the restore session status link, Restore Portal opens the [Restore Sessions](#) tab and navigates you directly to the restore session record.

If you want the notification pane to expand automatically when a new notification appears, do the following:

1. Click the notification icon to expand the notification pane.
2. Enable the **Auto-display new messages** option.



Changing Restore Operator Scope

After logging in to Restore Portal, restore operators can view the list of objects available to them to manage — that is, to explore and restore data from backups created by Veeam Backup for Microsoft 365 for these objects. For more information on how assign permissions to a restore operator, see [Adding Restore Operator Role](#).

Restore operators can manage data of organization objects separately. Thus, they must switch between the managed objects: users, groups (group members only), sites, teams or the entire Microsoft 365 organization. In terms of Veeam Backup for Microsoft 365, this operation is called *Changing restore operator scope*.

NOTE

If a restore operator is allowed to explore and restore data from backups created by Veeam Backup for Microsoft 365 for all objects within a Microsoft 365 organization, loading of available objects may take a considerable time. To avoid this, the Veeam Backup for Microsoft 365 administrator can edit the restore operator role settings and select not the entire organization, but specific users, groups, sites, or teams as objects to manage. For more information, see [Editing Restore Operator Role Settings](#) and [Select Objects to Manage](#).

To select an object whose backed-up data a restore operator will explore and restore, do the following:

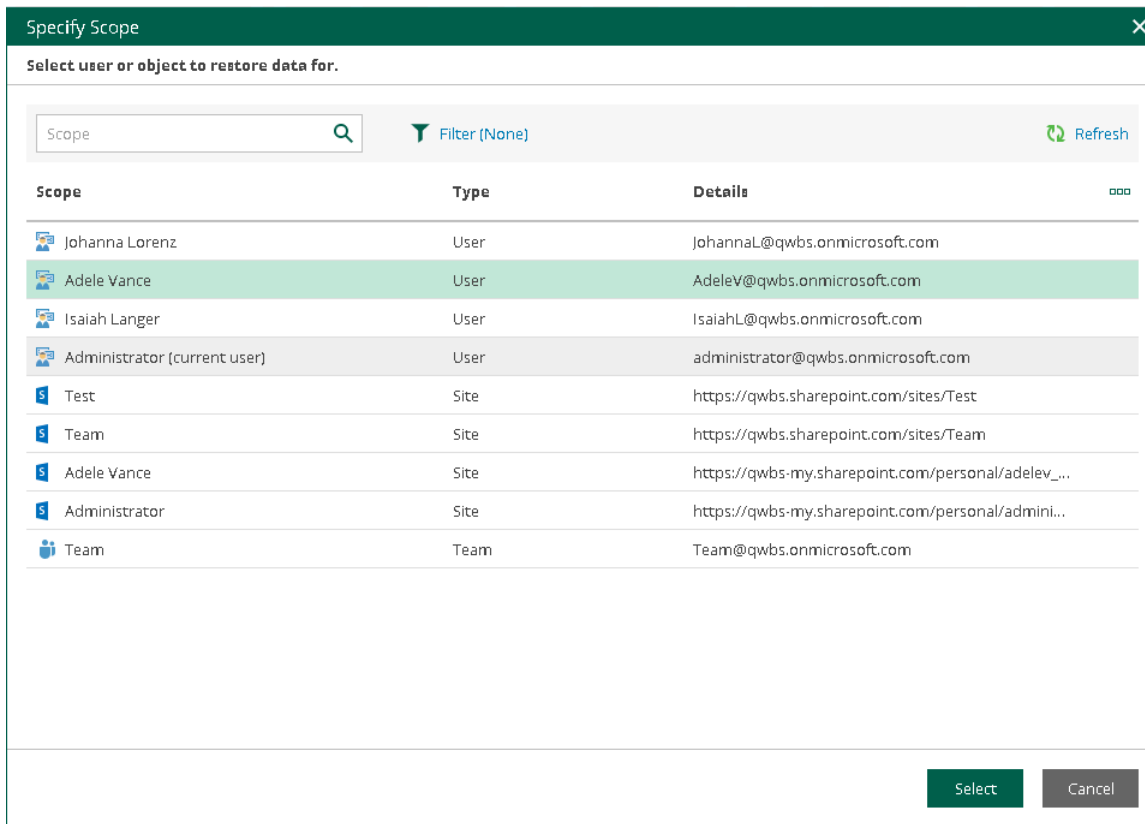
1. In the upper-left corner of the Restore Portal window, click **You** or the name of the object managed last.
2. In the **Specify Scope** window, select an object that you want to manage. You can search objects and filter them by their organization object type.

NOTE

You can select only objects that currently exist in Microsoft 365 organization. To explore and restore data from backups created for objects that do not exist in Microsoft 365 organization, use Veeam Explorers. For more information, see [Veeam Explorers User Guide](#).

3. Click **Select**.

The name of the selected object will appear in the upper-left corner of the Restore Portal window. The **Explore** tab will be displayed, on which you can browse through the hierarchy of folders with backed-up data of the selected object and [select a restore point](#).



Selecting Restore Point

After you log in to Restore Portal, you must select a restore point from which you want to explore and restore data from backups created by Veeam Backup for Microsoft 365.

NOTE

If you are a restore operator, you must first select an object that you want to manage and then select a restore point that is available for the selected object in a backup repository. For more information, see [Changing Restore Operator Scope](#).

To view available restore points and select a restore point that you want to use, do the following:

1. In the upper-left corner of the Restore Portal window, click **Select Restore Point** or the restore point timestamp.
2. In the displayed dialog box, do one of the following:
 - In the calendar, click the date for which Veeam Backup for Microsoft 365 has available restore points. Such dates are marked in bold. The list of available restore points for the selected date will be displayed on the right.

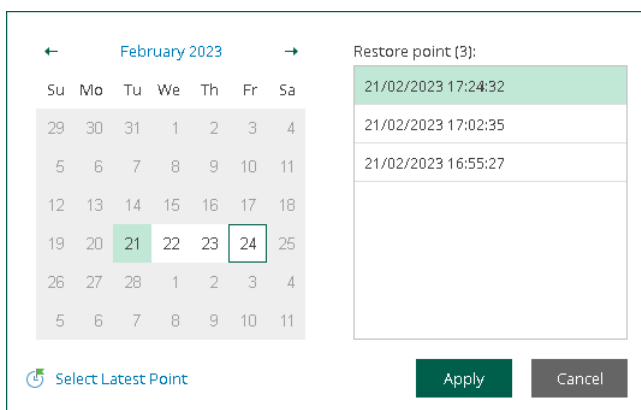
NOTE

Consider the following:

- You can select restore points that correspond to backups created by Veeam Backup for Microsoft 365 for an object whose backed-up data you want to explore and restore.
- If the latest backups of Exchange, SharePoint and OneDrive data of a user belong to different restore points, Veeam Backup for Microsoft 365 will display the backup data from the selected restore point and from the closest restore points prior to the selected restore point.
- Only restore points created by Veeam Backup for Microsoft 365 version 6.0 or later will be displayed.
- Veeam Backup for Microsoft 365 will not display restore points created by backup copy jobs.

- Click **Select Latest Point** to select the latest restore point that is available in a backup repository.

3. Click **Apply**.



Performing Restore

After logging in to Restore Portal, you can explore and restore data from backups created by Veeam Backup for Microsoft 365. If you act as an *end user*, you perform self-service restore of your own data. If you have a *restore operator* permissions, you explore and restore backed-up data for those objects that you are allowed to manage. For more information about Restore Portal usage scenarios, see [Restore Portal Usage Scenarios](#). For more information on how to assign permissions to a restore operator, see [Adding Restore Operator Role](#).

You can explore and restore data from backups created by Veeam Backup for Microsoft 365 for the following Microsoft Online services:

- [Microsoft Exchange Online](#)
- [Microsoft SharePoint Online](#)
- [Microsoft OneDrive for Business](#)
- [Microsoft Teams](#)

Using Restore List

If you want to select items located in different folders in the hierarchy of folders with backed-up data displayed in the navigation pane, you can add them to the restore list. For example, you can add to the restore list one by one items of different types: for a user – mailbox items, OneDrive and SharePoint files, for a team – Microsoft Teams files, tabs and posts, and proceed to their restore.

NOTE

You cannot add the following objects to the restore list:

- OneDrive and SharePoint folders
- Microsoft Teams teams, channels, tabs and folders

To add items to the restore list, do the following:

1. Open the **Explore** tab.
2. In the navigation pane, browse through the hierarchy of folders with backed-up data.
3. Select a folder that contains data you want to restore.
4. In the preview pane, select check boxes next to the necessary items.

For mailbox folders, documents, list items and files, you can select which version of an item you want to restore. To do this, in the **Version** column, click the most recent version number, and in the displayed window, select the earlier version to restore.

For Microsoft Teams posts, you can select which replies to the selected post you want to restore. To do this, in the **Replies** column, click **Show**, and in the displayed window, select check boxes next to replies that you want to restore.

NOTE

Consider the following:

- Restore Portal displays up to 2000 items, so search for specific items.
- You can use logical upper-cased operators such as *AND*, *OR* and *NOT*.

5. Click **Add to Restore List**.
6. Repeat steps 2-5 to add more items to the restore list.
7. On the **Restore List** tab, review the list of items that you added to the restore list.
8. To restore items, select check boxes next to the necessary items and click **Restore** and then select one of the following options:
 - **Restore Exchange Items**. This option runs the [Exchange Restore](#) wizard.
 - **Restore OneDrive Documents**. This option runs the [OneDrive Restore](#) wizard.
 - **Restore SharePoint List Items**. This option runs the [SharePoint Restore](#) wizard.
 - **Restore SharePoint Library Documents**. This option runs the [SharePoint Restore](#) wizard.
 - **Restore Teams Files**. This option runs the [Microsoft Teams Restore](#) wizard.
 - **Restore Teams Tabs**. This option runs the [Microsoft Teams Restore](#) wizard.
 - **Restore Teams Posts**. This option runs the [Microsoft Teams Restore](#) wizard.

TIP

To remove items from the restore list, select check boxes next to the necessary items and click **Remove from Restore List**.

9. Follow the steps of the wizard that you ran and configure restore operation options. Keep in mind that you must run wizards manually one after another.

The screenshot displays the 'Restore List (7)' interface. At the top, there are navigation tabs for 'Explore', 'Restore Sessions', and 'Restore List (7)'. The user is logged in as 'administrator@qws.onmicrosoft.com' with the role of 'Restore Operator'. Below the navigation, there is a search bar and a status bar with icons for help, refresh, success, warning, and error. A context menu is open over the first row, showing options: 'Restore Exchange Items', 'Restore SharePoint Library Documents', and 'Restore OneDrive Documents'. The main table lists the following items:

	Type	Location	Sent	Received	Restore Status
<input type="checkbox"/>	Library Document	Adele Vance/Content/Style Library/Media Player	-	-	Never started
<input checked="" type="checkbox"/>	Library Document	Adele Vance/Content/Style Library/Media Player	-	-	Never started
<input checked="" type="checkbox"/>	Email	Adele Vance/Inbox	February 7, 20...	February 7, 20...	Never started
<input checked="" type="checkbox"/>	OneDrive Document	Adele Vance	-	-	Never started
<input checked="" type="checkbox"/>	Email	Adele Vance/Inbox	February 7, 20...	February 7, 20...	Never started
<input checked="" type="checkbox"/>	OneDrive Document	Adele Vance	-	-	Success
<input checked="" type="checkbox"/>	OneDrive Document	Adele Vance/Attachments	-	-	Success

Exchange Restore

To restore Exchange items, do the following:

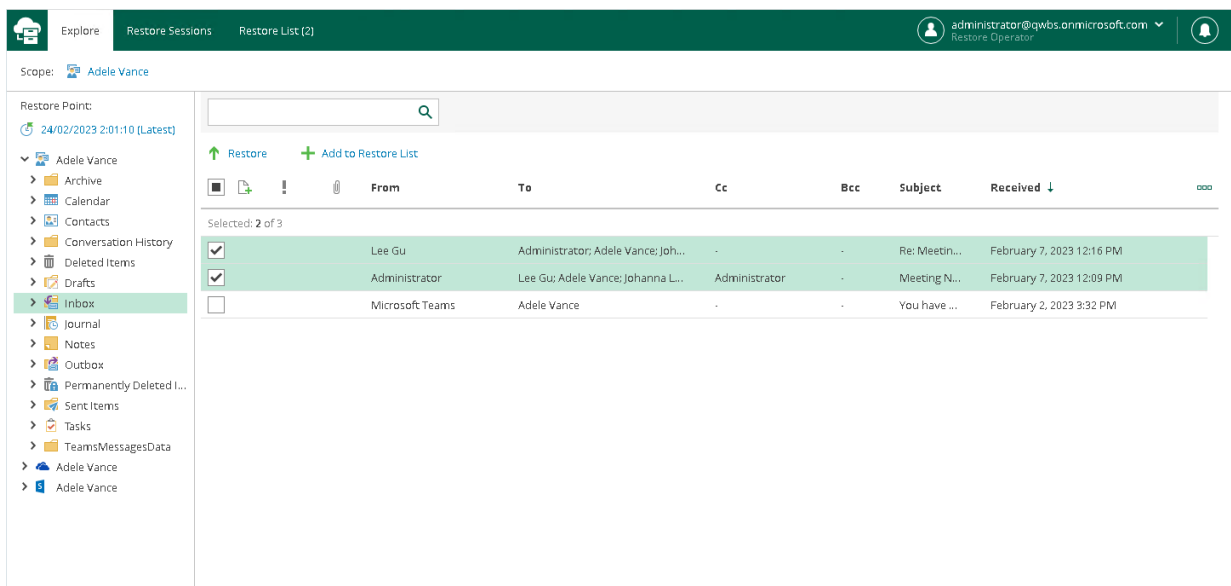
1. Open the **Explore** tab.
2. Select a restore point from which you want to explore and restore data. For more information, see [Selecting Restore Point](#).
3. In the navigation pane, browse through the hierarchy of folders with backed-up data.
4. Select a folder that contains data you want to restore.
5. In the preview pane, select check boxes next to the necessary Exchange items.

NOTE

Consider the following:

- Restore Portal displays up to 2000 items, so search for specific items.
- You can use logical upper-cased operators such as *AND*, *OR* and *NOT*.

6. Click **Restore**.



The screenshot shows the Exchange Restore interface. The top navigation bar includes 'Explore', 'Restore Sessions', and 'Restore List (2)'. The user is logged in as 'administrator@qwbsonmicrosoft.com'. The scope is set to 'Adele Vance'. The restore point is '24/02/2023 2:01:10 [Latest]'. The left navigation pane shows a tree view of folders, with 'Inbox' selected. The main area displays a table of items with columns: From, To, Cc, Bcc, Subject, and Received. Two items are selected, indicated by checkmarks in the first column.

	From	To	Cc	Bcc	Subject	Received
<input checked="" type="checkbox"/>	Lee Gu	Administrator; Adele Vance; Joh...	-	-	Re: Meetn...	February 7, 2023 12:16 PM
<input checked="" type="checkbox"/>	Administrator	Lee Gu; Adele Vance; Johanna L...	Administrator	-	Meeting N...	February 7, 2023 12:09 PM
<input type="checkbox"/>	Microsoft Teams	Adele Vance	-	-	You have ...	February 2, 2023 3:32 PM

The **Exchange Restore** wizard runs to configure the restore operation options.

- At the **Items** step, specify items that you want to restore. If you no longer want to restore an item, select it and click **Remove**.

Exchange Restore

Items

Specify items to restore.

Name

Name	Size	Type	Location
Meeting Notes	-	Email	Adele Vance/Inbox
Re: Meeting Notes	-	Email	Adele Vance/Inbox

- At the **Restore mode** step, select where you want to restore the selected items:
 - Restore to the original location.** Select this option if you want to restore the selected items to their original location.
 - Restore to a new location.** Select this option if you want to restore the selected items to another location and specify the folder name in the **Restore to the following folder** field. If the specified folder does not exist, it will be created automatically.

Exchange Restore

Restore mode

Specify whether you want to restore items to the original location or to another location.

Restore to the original location
Quickly initiate the restore of the selected items to their original location.

Restore to a new location
Restore to the following folder:

[Advanced options...](#)

- Click **Advanced options** to open the **Restore options** dialog.
- In the **Restore options** dialog, select check boxes next to the additional options that you want to apply during the restore operation and then click **Apply**:
 - Restore changed items.** Select this check box if you want to restore items that have been changed.
 - Restore missing items.** Select this check box if you want to restore items that are missing in the target folder.

- **Mark restored items as unread.** Select this check box if you want to mark each restored item as unread.

The screenshot shows the 'Exchange Restore' dialog box with the 'Restore mode' step selected. The left sidebar contains 'Items', 'Restore mode', 'Reason', and 'Summary'. The main area is titled 'Restore mode' and contains two radio button options: 'Restore to the original location' and 'Restore to a new location'. The 'Restore to a new location' option is selected, and a text box labeled 'Restore Folder' is visible. To the right, the 'Restore options' panel is open, showing checkboxes for 'Restore changed items', 'Restore missing items', and 'Mark restored items as unread' (which is checked). 'Apply' and 'Cancel' buttons are at the bottom of the options panel.

11. [Optional] At the **Reason** step, specify a restore reason. This information will be available in the **Reason** column on the **Restore Sessions** tab and you will be able to reference it later.

The screenshot shows the 'Exchange Restore' dialog box with the 'Reason' step selected. The left sidebar contains 'Items', 'Restore mode', 'Reason', and 'Summary'. The main area is titled 'Reason' and contains a text box labeled 'Restore reason:' with the text 'User request.' entered. At the bottom of the dialog, there are 'Previous', 'Next', and 'Cancel' buttons.

12. At the **Summary** step, review details of the restore operation and click **Finish**.

Restore Portal runs the restore operation immediately and opens the [Restore Sessions](#) tab, where you view details about restore session progress and results.

SharePoint Restore

To restore SharePoint items, do the following:

1. Open the **Explore** tab.
2. Select a restore point from which you want to explore and restore data. For more information, see [Selecting Restore Point](#).
3. In the navigation pane, browse through the hierarchy of folders with backed-up data.
4. Select a folder that contains data you want to restore.
5. In the preview pane, select check boxes next to the necessary SharePoint items.

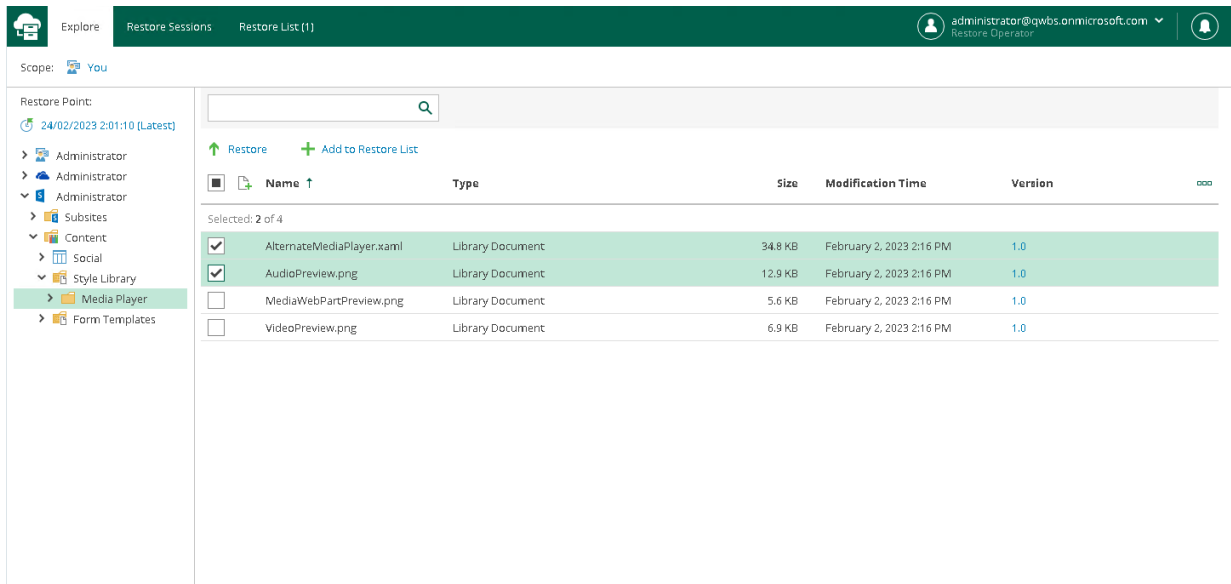
For SharePoint folders, documents and list items, you can select which version of an item you want to restore. To do this, in the **Version** column, click the most recent version number, and in the displayed window, select the earlier version to restore.

NOTE

Consider the following:

- Restore Portal displays up to 2000 items, so search for specific items.
- You can use logical upper-cased operators such as *AND*, *OR* and *NOT*.

6. Click **Restore**.



The **SharePoint Restore** wizard runs to configure the restore operation options.

7. At the **Items** step, specify items that you want to restore. If you no longer want to restore an item, select it and click **Remove**.

Name	Size	Type	Location
AudioPreview.png	12.9 KB	Library Document	Adele Vance/Content/Styl...
MediaWebPartPreview.png	5.6 KB	Library Document	Adele Vance/Content/Styl...

8. At the **Restore mode** step, select where you want to restore the selected items:
- **Restore to the original location.** Select this option if you want to restore the selected items to their original location.
 - **Restore to a new location.** Select this option if you want to restore the selected items to another location and specify the list name in the **Restore to the following list** field.

Keep in mind that if you restore documents or list items, you must specify a document library or a list that exists in the original SharePoint site.

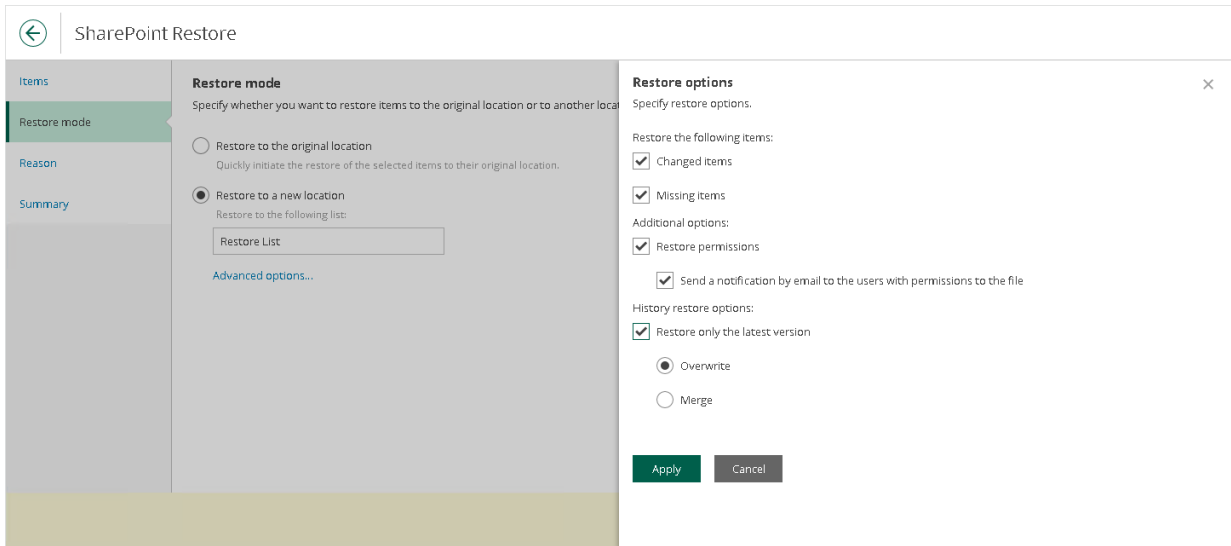
Restore to the original location
Quickly initiate the restore of the selected items to their original location.

Restore to a new location
Restore to the following list:

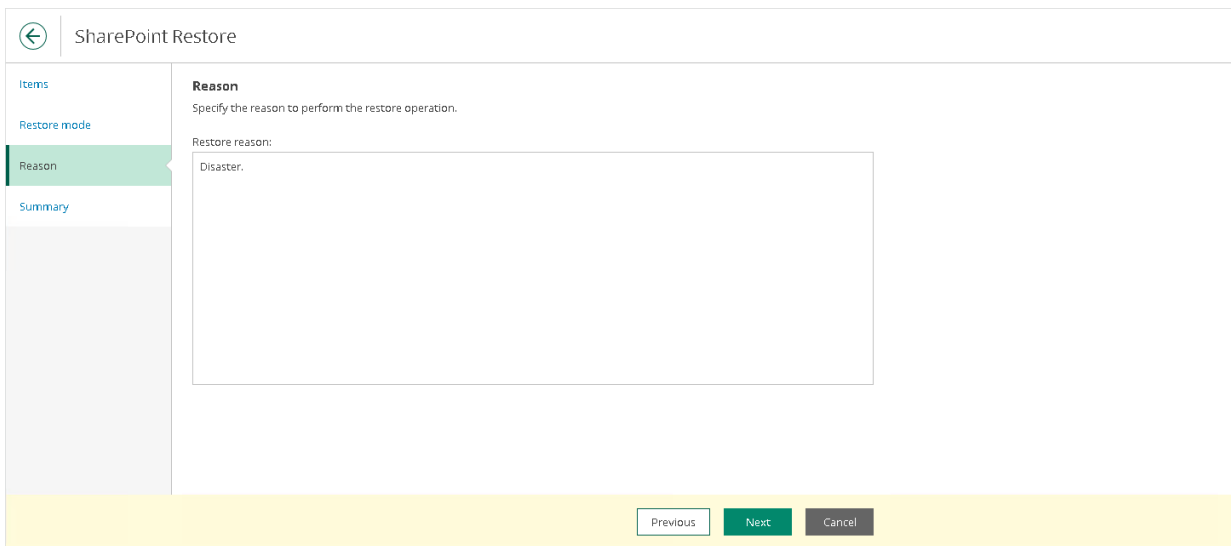
[Advanced options...](#)

9. Click **Advanced options** to open the **Restore options** dialog.
10. In the **Restore options** dialog, select check boxes next to the additional options that you want to apply during the restore operation and then click **Apply**:
- **Changed items.** Select this check box if you want to restore data that has been modified in the production environment.
 - **Missing items.** Select this check box if you want to restore missing items.
 - **Restore permissions.** Select this check box if you want to restore permissions.

- **Send a notification by email to the users with permissions to the file.** Select this check box if you want to notify users about items restore. Veeam Backup for Microsoft 365 will notify users with whom items have been shared. You can select this check box only if the **Restore permissions** check box is selected.
- **Restore only the latest version.** Select this check box if you want to restore only the latest version of items. If this check box is selected, you can select one of the following options:
 - **Overwrite.** Select this option to overwrite data in the production environment.
 - **Merge.** Select this option to merge an existing and a backup version of items.



11. [Optional] At the **Reason** step, specify a restore reason. This information will be available in the **Reason** column on the **Restore Sessions** tab and you will be able to reference it later.



12. At the **Summary** step, review details of the restore operation and click **Finish**.

Restore Portal runs the restore operation immediately and opens the **Restore Sessions** tab, where you view details about restore session progress and results.

OneDrive Restore

To restore OneDrive items, do the following:

1. Open the **Explore** tab.
2. Select a restore point from which you want to explore and restore data. For more information, see [Selecting Restore Point](#).
3. In the navigation pane, browse through the hierarchy of folders with backed-up data.
4. Select a folder that contains data you want to restore.
5. In the preview pane, select check boxes next to the necessary OneDrive items.

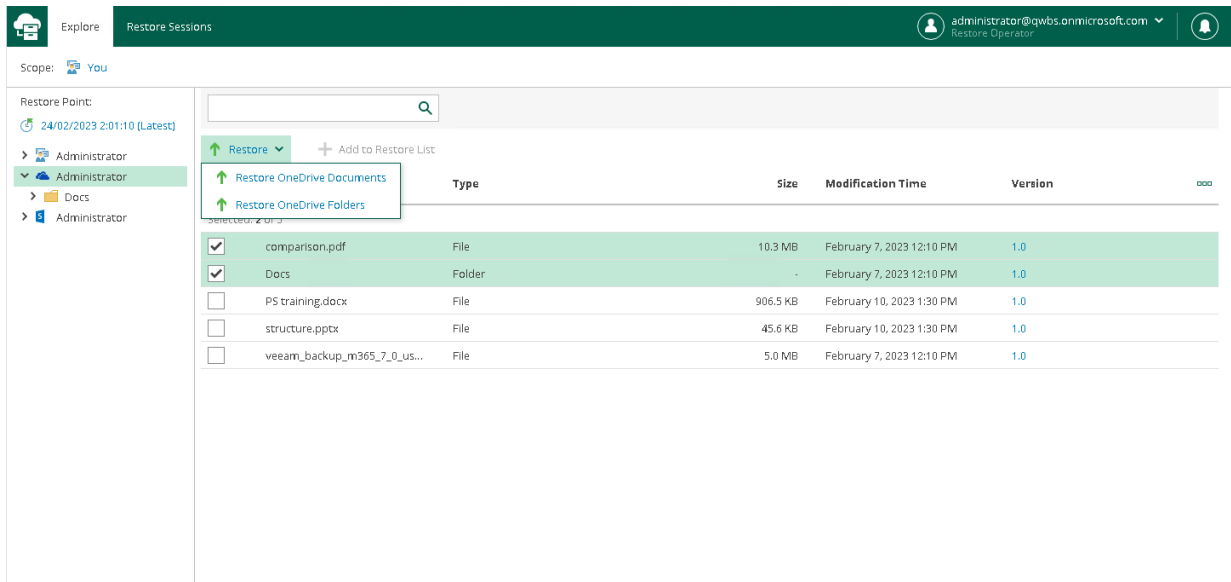
For OneDrive folders and documents, you can select which version of an item you want to restore. To do this, in the **Version** column, click the most recent version number, and in the displayed window, select the earlier version to restore.

NOTE

Consider the following:

- Restore Portal displays up to 2000 items, so search for specific items.
- You can use logical upper-cased operators such as *AND*, *OR* and *NOT*.

6. Click **Restore** and select one of the following options if necessary:
 - **Restore OneDrive Documents**. This option allows you to restore OneDrive documents.
 - **Restore OneDrive Folders**. This option allows you to restore OneDrive folders.



The **OneDrive Restore** wizard runs to configure the restore operation options.

7. At the **Items** step, specify items that you want to restore. If you no longer want to restore an item, select it and click **Remove**.

OneDrive Restore

Items

Specify items to restore.

Name

Name	Size	Type	Location
structure.pptx	45.6 KB	OneDrive Document	Adele Vance
veeam_backup_m365_7_0...	5.0 MB	OneDrive Document	Adele Vance/Attachments

8. At the **Restore mode** step, choose whether you want to overwrite the file or document in the original location or keep the restored one along with the original.

OneDrive Restore

Restore mode

Specify whether you want to overwrite the document in the original location or keep both documents.

Overwrite
Overwrite the selected documents.

Keep
Keep the restored document along with the original.

9. [Optional] At the **Reason** step, specify a restore reason. This information will be available in the **Reason** column on the **Restore Sessions** tab and you will be able to reference it later.

The screenshot shows a web interface for 'OneDrive Restore'. On the left, there is a vertical navigation menu with four items: 'Items', 'Restore mode', 'Reason', and 'Summary'. The 'Reason' item is highlighted with a green background. The main content area is titled 'Reason' and contains the instruction 'Specify the reason to perform the restore operation.' Below this, there is a text input field labeled 'Restore reason:' with the word 'Disaster.' entered. At the bottom of the interface, there is a yellow bar containing three buttons: 'Previous', 'Next', and 'Cancel'.

10. At the **Summary** step, review details of the restore operation and click **Finish**.

Restore Portal runs the restore operation immediately and opens the [Restore Sessions](#) tab, where you view details about restore session progress and results.

Teams Restore

To restore Microsoft Teams items, do the following:

1. Open the **Explore** tab.
2. Select a restore point from which you want to explore and restore data. For more information, see [Selecting Restore Point](#).
3. In the navigation pane, browse through the hierarchy of folders with backed-up data.
4. Select a folder that contains data you want to restore.
5. In the preview pane, select check boxes next to the necessary Microsoft Teams items.

For Microsoft Teams folders and files, you can select which version of an item you want to restore. To do this, in the **Version** column, click the most recent version number, and in the displayed window, select the earlier version to restore.

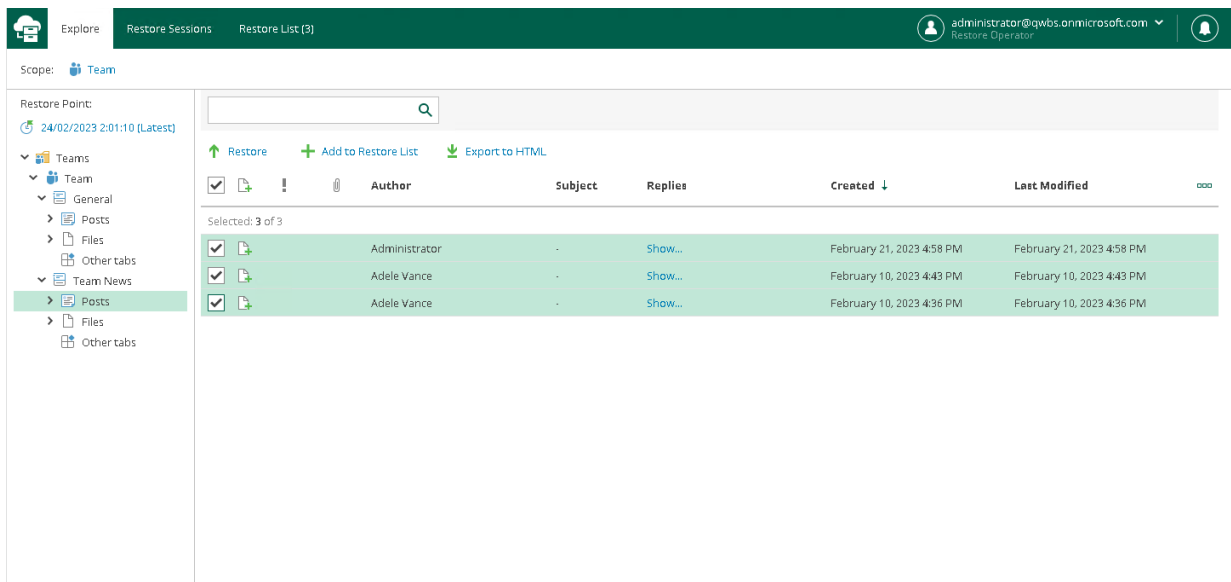
For Microsoft Teams posts, you can select which replies to the selected post you want to restore. To do this, in the **Replies** column, click **Show**, and in the displayed window, select check boxes next to replies that you want to restore.

NOTE

Consider the following:

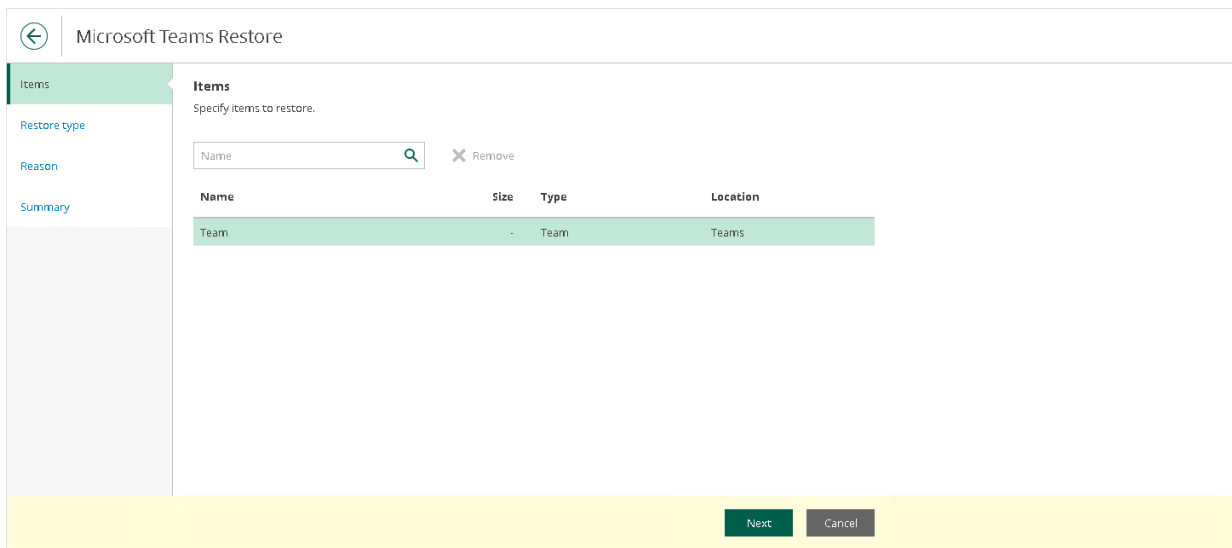
- Restore Portal displays up to 2000 items, so search for specific items.
- You can use logical upper-cased operators such as *AND*, *OR* and *NOT*.

6. Click **Restore**.



The **Microsoft Teams Restore** wizard runs to configure the restore operation options.

7. At the **Items** step, specify items that you want to restore. If you no longer want to restore an item, select it and click **Remove**.



8. [Unavailable for the **Posts** tab and posts] At the **Restore type** step, select check boxes next to the restore options that you want to apply during the restore operation:
- For teams:
 - **Changed items.** Select this check box if you want to restore data that has been modified in the production environment.
 - **Missing items.** Select this check box if you want to restore missing items.
 - **Team settings (guest permissions, @mentions, fun stuff).** Select this check box if you want to restore settings of the team.
 - **Membership and their permissions.** Select this check box if you want to restore members of the team along with their roles.
 - For team channels and the **Other tabs** tab:
 - **Changed items.** Select this check box if you want to restore data that has been modified in the production environment.
 - **Missing items.** Select this check box if you want to restore missing items.
 - For the **Files** tab and files:
 - **Changed items.** Select this check box if you want to restore data that has been modified in the production environment.
 - **Missing items.** Select this check box if you want to restore missing items.

- **Restore only the latest version.** Select this check box if you want to restore only the latest version of items.

The screenshot shows the 'Microsoft Teams Restore' wizard at the 'Restore type' step. The left sidebar contains 'Items', 'Restore type', 'Reason', and 'Summary'. The 'Restore type' section is active and contains the following options:

- Restore the following items:
 - Changed items
 - Missing items
- Restore the following settings:
 - Team settings (guest permissions, @mentions, fun stuff)
 - Membership and their permissions

At the bottom, there are three buttons: 'Previous', 'Next', and 'Cancel'.

9. [Optional] At the **Reason** step, specify a restore reason. This information will be available in the **Reason** column on the **Restore Sessions** tab and you will be able to reference it later.

The screenshot shows the 'Microsoft Teams Restore' wizard at the 'Reason' step. The left sidebar contains 'Items', 'Restore type', 'Reason', and 'Summary'. The 'Reason' section is active and contains the following text:

Specify the reason to perform the restore operation.

Restore reason:
User request.

At the bottom, there are three buttons: 'Previous', 'Next', and 'Cancel'.

10. At the **Summary** step, review details of the restore operation and click **Finish**.

Restore Portal runs the restore operation immediately and opens the [Restore Sessions](#) tab, where you view details about restore session progress and results.

Exporting Teams Posts

You can export Microsoft Teams posts to a file in the HTML format.

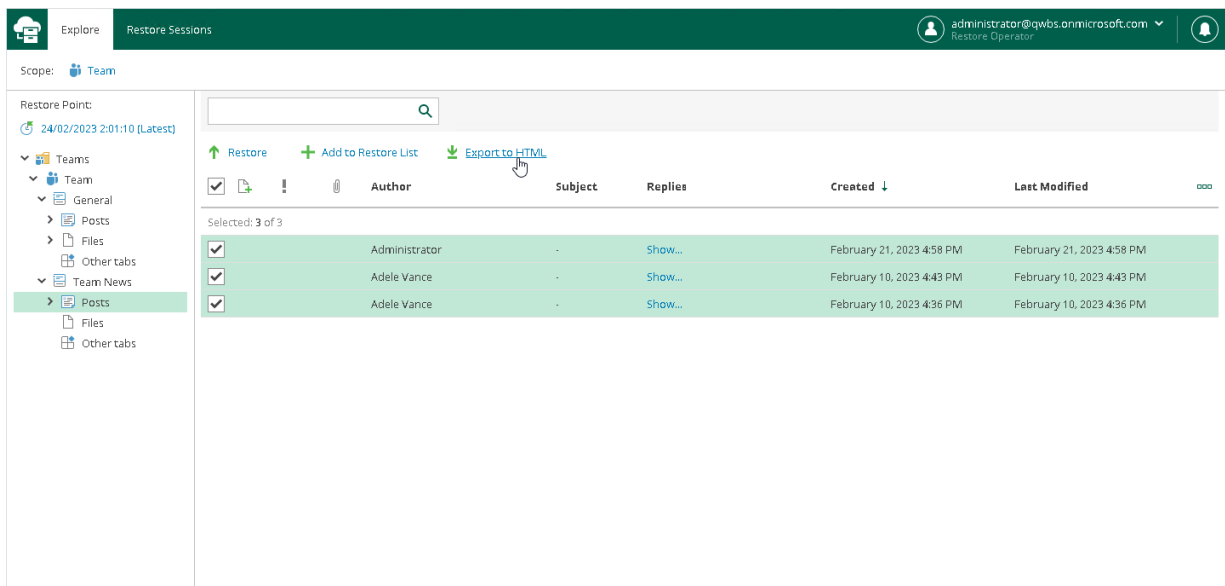
To export posts to a file in the HTML format, do the following:

1. Open the **Explore** tab.
2. Select a restore point from which you want to explore data. For more information, see [Selecting Restore Point](#).
3. In the navigation pane, browse through the hierarchy of folders with backed-up data.
4. Select the **Posts** folder that contains posts you want to export.
5. In the preview pane, select check boxes next to the necessary Microsoft Teams posts and click **Export to HTML**.

NOTE

Consider the following:

- Restore Portal displays up to 2000 items, so search for specific items.
- You can use logical upper-cased operators such as *AND*, *OR* and *NOT*.



The screenshot shows the 'Explore' tab in the Restore Portal. The 'Restore Point' is set to '24/02/2023 2:01:10 (Latest)'. The navigation pane on the left shows the hierarchy: Teams > Team > General > Posts. The main preview pane shows a table of posts with columns: Author, Subject, Replies, Created, and Last Modified. Three posts are selected, and the 'Export to HTML' button is highlighted.

	Author	Subject	Replies	Created	Last Modified
<input checked="" type="checkbox"/>	Administrator	-	Show...	February 21, 2023 4:58 PM	February 21, 2023 4:58 PM
<input checked="" type="checkbox"/>	Adele Vance	-	Show...	February 10, 2023 4:43 PM	February 10, 2023 4:43 PM
<input checked="" type="checkbox"/>	Adele Vance	-	Show...	February 10, 2023 4:36 PM	February 10, 2023 4:36 PM

Restore Portal creates the export file with a name that includes the channel name and the operation timestamp. You can view this file in a browser window.

Data Restore Using Veeam Explorers

Veeam Explorers extend the functionality of Veeam Backup for Microsoft 365 and allow you to explore and restore data from backups.

For more information on how to use Veeam Explorers, see [Veeam Explorers User Guide](#).