

Veeam Backup for Microsoft Office 365

Version 4.0

User Guide

June, 2020

© 2020 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	9
ABOUT THIS DOCUMENT	10
ABOUT VEEAM BACKUP FOR MICROSOFT OFFICE 365	11
PLANNING AND PREPARATION	12
SYSTEM REQUIREMENTS	13
USED PORTS	16
REQUIRED PERMISSIONS	19
Microsoft SharePoint and OneDrive for Business	20
Microsoft Exchange Organizations	22
Azure AD Applications	24
CONSIDERATIONS AND LIMITATIONS	26
SUPPORTED AZURE STORAGE ACCOUNT TYPES	29
LICENSING AND LICENSE TYPES	30
SUBSCRIPTION LICENSE	32
RENTAL LICENSE	33
Monthly Usage Report	34
NOT FOR RESALE LICENSE	36
EVALUATION LICENSE	37
DEPLOYMENT	38
DOWNLOADING INSTALLATION PACKAGE	39
INSTALLING VEEAM BACKUP FOR MICROSOFT OFFICE 365	40
INSTALLING VEEAM EXPLORER FOR MICROSOFT EXCHANGE	42
INSTALLING VEEAM EXPLORER FOR MICROSOFT SHAREPOINT	44
INSTALLING IN UNATTENDED MODE	46
DEPLOYING TO AZURE AND AWS	48
CHECKING FOR UPDATES	49
INSTALLING AND UPDATING LICENSE	51
UPGRADING TO VEEAM BACKUP FOR MICROSOFT OFFICE 365 4.0	53
UNINSTALLING VEEAM BACKUP FOR MICROSOFT OFFICE 365	54
LAUNCHING VEEAM BACKUP FOR MICROSOFT OFFICE 365	55
USER INTERFACE	57
CURRENT SESSION	60
CONFIGURATION	61
GENERAL SETTINGS	62
Folder Exclusions	63
Session History	64

RESTful API Settings	65
Notification Settings	66
Authentication Settings.....	68
Update Notification Settings	69
Global Internet Proxy Server Settings.....	70
SSL Certificates	71
BACKUP INFRASTRUCTURE	74
Backup Proxy Servers	75
Backup Repositories	86
Object Storage Repositories	102
CREDENTIALS	125
Managing Cloud Credentials.....	126
Managing Encryption Passwords	129
ORGANIZATION MANAGEMENT	131
MICROSOFT OFFICE 365 ORGANIZATIONS	132
Adding Organizations with MFA	133
Adding Organizations with MFA and Legacy Protocols	141
Adding Organizations with Basic Authentication.....	147
ON-PREMISES MICROSOFT ORGANIZATIONS.....	152
Step 1. Launch Add Organization Wizard.....	153
Step 2. Select Organization Deployment Type.....	154
Step 3. Specify Microsoft Exchange Connection Settings.....	155
Step 4. Specify Microsoft SharePoint Connection Settings.....	157
Step 5. Finish Wizard	159
HYBRID ORGANIZATIONS.....	160
BACKUP ACCOUNTS	162
Adding Accounts	163
Changing Password and Removing Accounts	165
BACKUP APPLICATIONS	166
Adding Applications	167
Creating Applications	170
Updating Certificates and Removing Applications	173
EDITING ORGANIZATION PARAMETERS	174
RENAMING ORGANIZATIONS	175
REMOVING ORGANIZATIONS	177
DATA BACKUP	178
ORGANIZATION OBJECT TYPES	179
CREATING BACKUP JOB	182
Step 1. Launch New Backup Job Wizard	183

Step 2. Specify Backup Job Name	184
Step 3. Select Objects to Back Up	185
Step 4. Select Objects to Exclude	188
Step 5. Specify Backup Proxy and Repository	190
Step 6. Specify Scheduling Options	191
MANAGING BACKUP JOBS	193
Starting Backup Job	194
Stopping Backup Job	195
Enabling/Disabling Backup Job	196
Editing Backup Job Settings	197
Removing Backup Job	198
Exploring Backup Job	199
Upgrading Backup Job	200
DATA RESTORE	201
EXPLORING BACKUP JOBS	202
EXPLORING SINGLE ORGANIZATION	204
EXPLORING ALL ORGANIZATIONS	206
EXPLORING POINT-IN-TIME	208
BACKUP AND RESTORE STATISTICS	209
VIEWING BACKUP SESSION METRICS	210
VIEWING RESTORE SESSION METRICS	211
REPORTING	212
CREATING MAILBOX PROTECTION REPORTS	213
CREATING STORAGE CONSUMPTION REPORTS	215
CREATING LICENSE OVERVIEW REPORTS	217
LOG FILES EXPORT	219
CONFIGURING EXTENDED LOGGING MODE	221
OFFICE 365 BACKUP AS A SERVICE	222
FOR SERVICE PROVIDERS	223
Configuring Veeam Backup for Microsoft Office 365	224
FOR TENANTS	225
Exploring Backups in Veeam Explorers	226
VEEAM EXPLORER FOR MICROSOFT EXCHANGE	227
PLANNING AND PREPARATION	228
Used Ports	229
Required Permissions	230
Considerations and Limitations	232
LAUNCHING APPLICATION AND EXPLORING BACKUPS	233
Understanding User Interface	234

Browsing, Searching and Viewing Items	236
GENERAL APPLICATION SETTINGS	240
Extensible Storage Engine.....	241
SMTP Settings.....	242
Advanced Settings	243
STANDALONE DATABASES AND EXTERNAL SERVERS	244
Adding Microsoft Exchange Stores	245
Adding Veeam Backup for Microsoft Office 365 Server.....	246
Adding Veeam Backup for Microsoft Office 365 Service Provider.....	247
Removing Stores	249
RESTORE	250
Restore to Office 365 Organizations.....	251
Restore to On-Premises Microsoft Servers.....	262
1-Click Restore	270
EXPORT.....	274
Exporting to Custom Location	275
Using 1-Click Export	277
Receiving Export Reports	281
COMPARE	283
Compare to Office 365 Organizations.....	285
Compare to On-Premises Microsoft Servers.....	288
SAVING MICROSOFT EXCHANGE ITEMS	290
SENDING MICROSOFT EXCHANGE ITEMS	292
VEEAM EXPLORER FOR MICROSOFT SHAREPOINT.....	294
PLANNING AND PREPARATION	295
Used Ports	296
Required Permissions	297
Considerations and Limitations.....	298
LAUNCHING APPLICATION AND EXPLORING BACKUPS	302
Understanding User Interface.....	303
Browsing, Searching and Viewing Items	305
GENERAL APPLICATION SETTINGS	309
Staging SQL Server.....	310
Custom Lists	312
SMTP Settings.....	315
Advanced Settings	316
STANDALONE DATABASES	317
Adding Microsoft SharePoint Databases	318
Adding Veeam Backup for Microsoft Office 365 Databases.....	319

Adding Veeam Backup for Microsoft Office 365 Server.....	320
Adding Veeam Backup for Microsoft Office 365 Service Provider.....	321
Removing Databases	323
RESTORE	324
Restoring Sites	325
Restoring Document Libraries and Lists.....	330
Restoring Documents and List Items	336
EXPORT.....	342
Exporting Microsoft SharePoint Data.....	343
Importing Microsoft SharePoint Data	344
SAVING MICROSOFT SHAREPOINT DOCUMENTS AND LIBRARIES	345
SENDING MICROSOFT SHAREPOINT DOCUMENTS AND LIBRARIES	346
APPENDIX A: UNSUPPORTED SHAREPOINT LISTS	348
VEEAM EXPLORER FOR MICROSOFT ONEDRIVE FOR BUSINESS	351
PLANNING AND PREPARATION	352
LAUNCHING APPLICATION AND EXPLORING BACKUPS	353
Understanding User Interface.....	354
Browsing, Searching and Viewing Items	356
GENERAL APPLICATION SETTINGS	360
SMTP Settings.....	361
Advanced Settings	362
STANDALONE DATABASES	363
Adding Veeam Backup for Microsoft Office 365 Databases.....	364
Adding Veeam Backup for Microsoft Office 365 Server.....	365
Adding Veeam Backup for Microsoft Office 365 Service Provider.....	366
Removing Standalone Databases.....	368
RESTORE	369
Restoring Single OneDrive.....	370
Restoring Multiple OneDrives.....	374
COPY	378
Step 1. Launch Restore Wizard.....	379
Step 2. Select Authentication Method	380
Step 3. Log on to Office 365.....	382
Step 4. Specify Target User	383
Step 5. Specify Target Folder	384
Step 6. Specify Restore Options	385
SAVING MICROSOFT ONEDRIVES	386
SAVING MICROSOFT ONEDRIVE DOCUMENTS AND FOLDERS	388
SENDING MICROSOFT ONEDRIVE DOCUMENTS	389

Contacting Veeam Software

At Veeam Software we value the 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 at www.veeam.com/support.html 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 offices location, visit www.veeam.com/contacts.html.

Online Support

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

- Full documentation set: www.veeam.com/documentation-guides-datasheets.html
- Community forum at forums.veeam.com

About This Document

This document explains on how to use Veeam Backup for Microsoft Office 365 to back up and recover data of your Microsoft Office 365, on-premises Microsoft Exchange and on-premises Microsoft SharePoint organizations, including Microsoft OneDrive for Business.

Information hereinafter is applicable to Veeam Backup for Microsoft Office 365 version 4.0 until it is replaced with a newer version of the product.

Intended Audience

This guide is intended for IT specialists who want to provide 24/7/365 data protection and availability for Microsoft Office 365 and on-premises Microsoft organizations users.

About Veeam Backup for Microsoft Office 365

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

Planning and Preparation

Before you install Veeam Backup for Microsoft Office 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 requirements listed below.

- [Microsoft Exchange organizations](#)
- [Microsoft SharePoint organizations](#)
- [Veeam Backup for Microsoft Office 365 server](#)
- [Backup proxy servers](#)

Supported Microsoft Exchange Organizations

The following table lists supported Microsoft Exchange versions.

Microsoft Exchange	Comments
Microsoft Office 365 Exchange Online	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 Office 365, see this Microsoft article .
Microsoft Exchange Server 2019 (compatibility support), 2016 or 2013 (on-premises)	For more information about limitations for backup and restore of mail items, see the Considerations and Limitations section.

*Government support is experimental.

NOTE:

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

Supported Microsoft SharePoint Organizations

The following table lists supported Microsoft SharePoint versions.

Microsoft SharePoint	Comments
Microsoft Office 365 SharePoint Online	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 Office 365, see this Microsoft article .
Microsoft SharePoint Server 2019, 2016	For more information about hardware and software requirements for Microsoft SharePoint Server 2019/2016, see: <ul style="list-style-type: none">▪ Hardware and software requirements for SharePoint Server 2016▪ Hardware and software requirements for SharePoint Server 2019

*Government support is experimental.

Veeam Backup for Microsoft Office 365 Server

The following table lists system requirements for the host machine with Veeam Backup for Microsoft Office 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, 4 cores minimum.▪ <i>Memory</i>: 8 GB RAM minimum. Additional RAM and CPU resources improve backup, restore and search performance. Veeam Backup for Microsoft Office 365 also requires a minimum size of 8 GB of RAM for VMs with dynamic memory allocation.▪ <i>Disk Space</i>: 500 MB for product installation and additional free space for the configuration database (depending on the amount of organizations, jobs and sessions) and product logs.
OS	<p>Only 64-bit version of the following operating systems are supported:</p> <ul style="list-style-type: none">▪ Microsoft Windows Server 2019▪ Microsoft Windows Server 2016▪ Microsoft Windows Server 2012 R2▪ Microsoft Windows Server 2012▪ Microsoft Windows Server 2008 R2 SP1▪ Microsoft Windows 10▪ Microsoft Windows 8.x▪ Microsoft Windows 7 SP1
Software	<p>The following software is required:</p> <ul style="list-style-type: none">▪ Microsoft .NET Framework 4.7.2 or higher.▪ Windows C Runtime and Update (UCRT) in Windows. For more information, see this Microsoft article.▪ Mail restore requires Veeam Explorer for Microsoft Exchange that is part of Veeam Backup & Replication 9.5 Update 4 or Veeam Backup for Microsoft Office 4.0.▪ To use PowerShell cmdlets for backup and/or restore, Windows PowerShell 2.0 or higher is required. When using Windows 2012 or 2012R2, Windows PowerShell 2.0 Engine must be installed regardless of the current PowerShell version.▪ For more information about Microsoft Office 365 system requirements and limitations, see this Microsoft article.

IMPORTANT!

Consider the following:

- When you install Veeam Explorer for Microsoft Exchange, Veeam Explorer for Microsoft SharePoint (including Veeam Explorer for Microsoft OneDrive for Business) and Veeam Backup for Microsoft Office 365 on different servers, the OS version on computers with Veeam Explorers must be the same or higher than the OS version on a computer with Veeam Backup for Microsoft Office 365.
- Veeam Explorers can only be installed on a machine hosting Veeam Backup for Microsoft Office 365 4.0 or the *Veeam Backup for Microsoft Office 365 Console* component. You can also use a machine with Veeam Backup & Replication 9.5 Update 4 (or higher) that is deployed either along with any of the above components, or as an independent solution.

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 x64 processor, 4 cores minimum.▪ <i>Memory</i>: 8 GB RAM minimum. Additional RAM and CPU resources improve backup, restore and search performance.▪ <i>Disk space</i>: 300 MB for backup proxy installation and additional free space for configuration database (depending on the amount of organizations, jobs and sessions) and backup proxy logs.
OS	<p>Only 64-bit version of the following operating systems are supported:</p> <ul style="list-style-type: none">▪ Microsoft Windows Server 2019▪ Microsoft Windows Server 2016▪ Microsoft Windows Server 2012 R2▪ Microsoft Windows Server 2012▪ Microsoft Windows Server 2008 R2 SP1▪ Microsoft Windows 10▪ Microsoft Windows 8.x▪ Microsoft Windows 7 SP1 <p>Proxy servers can be deployed to the following core editions:</p> <ul style="list-style-type: none">▪ Microsoft Windows Server 2019▪ Microsoft Windows Server 2016 LTSC, 1709▪ Microsoft Windows Server 2012 R2
Other	<p>The following components are required:</p> <ul style="list-style-type: none">▪ Microsoft .NET Framework 4.7.2 or higher.▪ Windows C Runtime and Update (UCRT) in Windows. For more information, see this Microsoft article.

Used Ports

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

NOTE:

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

From	To	Protocol	Port	Description
Veeam Backup for Microsoft Office 365 Server	Microsoft Exchange Online	TCP	80, 443	Required to connect to Microsoft Exchange Online organizations.
	Microsoft SharePoint Online	TCP	80, 443	Required to connect to Microsoft SharePoint Online organizations.
	On-premises Microsoft SharePoint Server	HTTP (HTTPS)	5985 (5986 – used by default)	Required to connect to on-premises Microsoft SharePoint organizations via the WinRM port.
	On-premises Microsoft Exchange Server	TCP	80, 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 Office 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	HTTPS	443	Required to access the auto-update server and licensing server. For more information, see Checking for Updates and Installing License . The end point is: <i>https://vbo.butler.veeam.com/json-rpc.php</i>
	S3 Compatible object storage	HTTPS	443 (used by default)	Required to work with any of the object storage repositories.

	Amazon S3 object storage / IBM Cloud Object Storage			
	Azure blob storage			
Components	Veeam Backup for Microsoft Office 365 Server	TCP	9191	<p>Required to manage inbound/outbound traffic when interacting with the following components:</p> <ul style="list-style-type: none"> ▪ RESTful API ▪ PowerShell ▪ Veeam.Archiver.Shell (UI) ▪ (optionally) A remote management server (if any) <p>Make sure to open this port on a Veeam Backup for Microsoft Office 365 server.</p>
Veeam Explorer for Microsoft Exchange Veeam Explorer for Microsoft SharePoint (including Veeam Explorer for Microsoft OneDrive for Business)	Veeam Backup for Microsoft Office 365 Server	TCP	9194	<p>Required to manage inbound/outbound traffic when interacting with:</p> <ul style="list-style-type: none"> ▪ Veeam Explorer for Microsoft Exchange ▪ Veeam Explorer for Microsoft SharePoint <p>Make sure to open this port on a Veeam Backup for Microsoft Office 365 server.</p>
Backup Proxy Server	Veeam Backup for Microsoft Office 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 a Veeam Backup for Microsoft Office 365 server.</p> <p>You can also change this port, as described in Editing Backup Proxy Server.</p>
	Microsoft Exchange Online	TCP	80, 443	Required to connect to Microsoft Exchange Online via EWS (Exchange Web Services).
	On-premises Microsoft SharePoint	HTTP (HTTPS)	5985 (5986)	Required to connect to on-premises Microsoft SharePoint organizations via the WinRM port.

Cloud Gateway	A server that hosts Veeam Backup & Replication and Veeam Backup for Microsoft Office 365	TCP	9194	Required to maintain inbound/outbound traffic.
---------------	--	-----	------	--

Required Permissions

This section explains required permissions for user accounts.

Microsoft SharePoint and OneDrive for Business

This section lists required permissions to work with Microsoft SharePoint and OneDrive for Business organizations.

Consider the following:

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

To enable this setting, use the following cmdlet.

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

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

- The account you are using to add on-premises Microsoft SharePoint and Microsoft SharePoint Online organizations must be a member of these organizations.

On-premises Microsoft SharePoint

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

Role	Description	Misc.
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

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

Role	Description	Misc.
SharePoint Administrator	Required to back up Microsoft SharePoint Sites.	You can assign the Global Administrator role that overrides these roles.
View-only Configuration	Required to get a list of available groups and users.	
View-Only Recipients		

Assigning SharePoint Service Administrator role in PowerShell

To assign the *SharePoint Service Administrator* role using PowerShell (for Microsoft SharePoint Online organizations), use the following code snippet.

```
Connect-MsolService
```

```
$role=Get-MsolRole -RoleName "SharePoint Service 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 Exchange Organizations

The following table lists required roles that must be assigned to the account that you want to use to add Microsoft Exchange organizations.

Consider the following:

- The account you are using to add an organization must be a member of this organization.
- The account you are using to add an organization is not required to have a mailbox in such an organization.

Role	Description
Role Management	Required to grant the <i>ApplicationImpersonation</i> role.
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.
Reviewer or Owner	Required to use impersonation to backup/restore public folders under the <i>Default</i> user.

Granting ApplicationImpersonation via 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, as described in [this Microsoft article](#).
2. Run the following cmdlet to grant the role.

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

For Microsoft Office 365 Exchange Organizations

To grant the *ApplicationImpersonation* role for Microsoft Office 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
```

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
```

Azure AD Applications

This section explains required permissions for Azure AD applications that you use to [back up](#) and [restore](#) data from/to your [Microsoft Office 365 organizations](#).

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

Veeam Backup for Microsoft Office 365 Version 4c

The following table lists permissions for AD applications that are granted automatically by Veeam Backup for Microsoft Office 365 when you add organizations using the [modern authentication method](#).

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

API	Permission name	Type	Usage
Microsoft Graph	Directory.Read.All	Application/Delegated	Backup/Restore
	Group.Read.All	Application	Backup
	Group.ReadWrite.All	Delegated	Restore
	offline_access	Delegated	Restore
	Site.ReadWrite.All	Application	Backup
Exchange	EWS,AccessAsUser.All	Delegated	Restore
	full_access_as_app	Application	Backup
	full_access_as_user This permission is only required when you add an organization in the <i>German</i> region.	Delegated	Backup
SharePoint	AllSitesFullControl	Delegated	Restore
	Sites.FullControl.All	Application	Backup
	User.Read.All	Application	Backup
	User.ReadWrite.All	Delegated	Backup

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

API	Permission name	Type	Usage
Microsoft Graph	Site.ReadWrite.All	Application	Backup

SharePoint	Sites.FullControl.All	Application	
	User.Read.All	Application	

Veeam Backup for Microsoft Office 365 Version 4

The following table lists required permissions that must be granted to AD applications for backup operations for organizations with [modern authentication](#) and [legacy authentication protocols](#).

API	Permission name	Type	Usage
Microsoft Graph	Directory.Read.All	Application	Backup
	Group.Read.All	Application	
Exchange	full_access_as_app	Application	
SharePoint	Sites.FullControl.All	Application	
	User.Read.All	Application	

Considerations and Limitations

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

Infrastructure

- The *Veeam Backup for Microsoft Office 365 RESTful API Service*, *Veeam Backup for Microsoft Office 365 Service* and *Veeam Backup Proxy for Microsoft Office 365 Service* must be started using the *Local System* account.
- You cannot change the name of the Veeam Backup for Microsoft Office 365 server or change domains of the server without resetting the configuration.
- If the organization has multiple domains, they must be configured as a mesh to cross authenticate in order to download content from all domains with the service account. For more information, see [this Microsoft article](#).
- Microsoft Windows 2008 operating system is not supported; Windows 2008 R2 SP1 is the minimum supported version.
- Veeam Backup for Microsoft Office 365 does not support encryption at-rest for the following types of 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 3.0 shares).
- Backup proxy servers and the Veeam Backup for Microsoft Office 365 server must be deployed within the same or a trusted domain.
- [For Microsoft Outlook] Preliminary releases such as *Insider releases* or releases provided by *Monthly Channel Updates* are not supported; Veeam Backup for Microsoft Office 365 supports only RTM/GA versions. For more information, see [this Microsoft article](#).
- If the Veeam Backup for Microsoft Office 365 console and a management server are deployed on different machines, make sure that the management 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 Office 365 components have 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 above has occurred on a server that acts as a backup proxy server, then such a server becomes *Offline* in the Veeam Backup for Microsoft Office 365 console. To make a server available, re-add it, as described in [Adding Backup Proxy Servers](#).
- IPv6 is not supported for Microsoft Azure *China* region.
- Notifications about backup jobs completion results may not work properly for Microsoft Azure *China* and *Germany* regions.

Backup Repositories

- Backup repositories with enabled volume deduplication are not supported.
- A symbolic link that is configured as a mapped drive is not supported.

Object Storage Repositories

- Veeam Backup for Microsoft Office 365 does not support the *\$root* container in Azure blob storage.
- Veeam Backup for Microsoft Office 365 does not support Glacier or Lifecycle policy in Amazon AWS Data Management or Azure Archive storage class.
- Make sure the S3 Compatible device you are adding supports AWS v4 signature. For more information about authentication requests, see [this Amazon article](#).
- Veeam Backup for Microsoft Office 365 allows you to migrate data from a local backup repository to an object storage repository, but not vice versa. For more information, see the [Move-VBOEntityData](#) section of the Veeam Backup for Microsoft Office 365 PowerShell Reference.

Backup

- To back up mailboxes, make sure that a mailbox has a valid Microsoft Office 365 license. Otherwise a backup job will fail with the following error: *"Error: Mailbox doesn't have a valid Microsoft Office 365 license"*
- Veeam Backup for Microsoft Office 365 backs up public folders that are located under the *IPM_SUBTREE* folder only.
- Project Web Apps are not supported for backup.
- On-premises service accounts cannot be used for multi-factor authentication.
- Backup of *In-Place Hold Items* is not supported for on-premises Microsoft Exchange 2013.
- 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 Office 365 will perform full synchronization of that folder during the subsequent backup job session. For more information, see [this Microsoft article](#).
- 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.*
- When backing up Microsoft Exchange mailboxes, Veeam Backup for Microsoft Office 365 does not create a new version of an item the *Read/Unread* property of which 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.

Restore

- 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 Office 365 restores public folders that are located under the *IPM_SUBTREE* folder only.
- Restore of multiple objects is not supported for public folders.

- Cross-tenant restores in Office 365 is only possible for Exchange Online objects, not for SharePoint sites.
- 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](#).

Supported Azure Storage Account Types

This section explains supported Azure [storage account types](#) for:

- [Standard performance tier](#)
- [Premium performance tier](#)

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
General-purpose V1	Blob	N/A
BlobStorage	Blob (block blobs and append blobs only)	Hot, Cool

Premium Performance Tier

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

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

Licensing and License Types

Licensing in Veeam Backup for Microsoft Office 365 is based on user accounts that you back up; each backed-up user account consumes one unit of the license.

A user account consists of:

- **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 license per user.

A license is consumed by mailboxes that have at least one restore point created within the last 31 days. If a mailbox was not backed-up for 31 days, its license is automatically revoked.

- **Microsoft OneDrive for Business**

OneDrive for Business licenses are associated with email accounts. This means you cannot use the same license to back up one user email and another user OneDrive for Business account.

Consider that OneDrive (without *for Business*) is an independent storage service and is not supported by Veeam Backup for Microsoft Office 365.

- **Microsoft SharePoint Online and on-premises Microsoft SharePoint**

Each SharePoint user in your Office 365 subscription (or on-premises deployment) that has been granted access to the SharePoint sites needs to be licensed to back up your SharePoint environment. If you have 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.

A license is not required for:

- **Shared, resource and group mailboxes**

- **SharePoint team sites**

For more information, see [this Microsoft article](#).

- **External SharePoint users**

An external SharePoint user is a user from outside your Office 365 subscription to whom you have given 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 when given specific permissions.

NOTE:

After you install Veeam Backup for Microsoft Office 365, you will be prompted to provide a product license. You can dismiss this step and continue using the product without any [license installed](#). In this case, you will have Community Edition mode that allows you to process up to 10 user accounts in all organizations including 1TB of Microsoft SharePoint data. *Community Edition* mode suggests using the community license, which is not limited in time, nor imposes any limitations in terms of program functionality.

License Types

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

- [Subscription License](#)

Paid, fully-functional license that expires at the end of the subscription term which is 1 or 3 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 which is the last day of the month and normally 1 month from the contract start date. 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.

Subscription License

Subscription License is a paid and fully-functional license that expires at the end of the subscription term which is 1 or 3 years from the contract start date (depending on the subscription length).

License Expired

A grace period of 1 month is granted after the expiration of license for purpose of renewal. During this period, the program functionality is not limited. After this period, processing of all user accounts in all organizations will be stopped; scheduled jobs will be terminated with failure. In both cases, a notification message will be shown to notify you that the license is either about to be expired 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 by up to 10 user accounts or up to 10% of the license count.

If you exceed the license by more than 10 user accounts or more than 10% of the license count (whichever is greater), Veeam Backup for Microsoft Office 365 lets you process these 10 (or 10%) extra user accounts according to the FIFO queue logic (that is, "first in - first out"); no additional accounts are allowed.

The grace period in this case 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 which is the last day of the month and normally 1 month from the contract start date. Such a license type is distributed only to service providers.

Understanding Trial State

A trial state is given to each user account that is being backed up for the first time and lasts until the first day of the following month. During this period your rental license remains unconsumed by such accounts.

For example, you have three user accounts A, B and C to be backed up and the first session of a backup job is scheduled on January 13, 2019. In such a scenario, after the backup session, all three user accounts (A, B and C) will be given a trial state until February 1, 2019. On February 1, 2019, a trial state for each of these accounts will be automatically reset. After the trial state is reset, upon the next backup job session all three user accounts (A, B and C) start consuming a rental license immediately.

You can avoid consuming a rental license by trial accounts that you no longer want to process. For example, you may not want to continue backing up the account *B* from the example above. For that, you can simply remove this account from the backup job processing list.

License Expired

A grace period of 2 month is granted after the expiration of license for purpose of renewal. During this period, the program functionality is not limited. After this period, processing of all user accounts in all organizations will be stopped; scheduled jobs will be terminated with failure. In both cases, a notification message will be shown to notify you that the license is either about to be expired 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 by up to 20 user accounts or up to 20% of the license count.

If you exceed the license by more than 20 user accounts or more than 20% of the license count (whichever is greater), Veeam Backup for Microsoft Office 365 lets you process these 20 (or 20%) extra user accounts according to the FIFO queue logic (that is, "first in - first out"); no additional accounts are allowed.

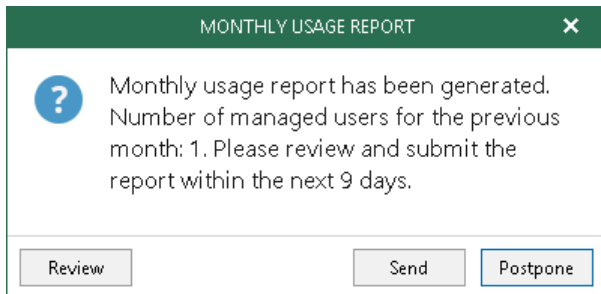
The grace period in this case is 2 months. After this period, processing of excessive user accounts (in FIFO queue) will be stopped; no more extra accounts will be queued for processing.

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

Monthly Usage Report

When using a rental license, you can submit a monthly usage report on the first day of each month. Such reports contain information on processed user accounts per each organization added to the Veeam Backup for Microsoft Office 365 backup infrastructure.

On the first day of each month and for the next 9 days you will be receiving the following notification message.



You can send the report immediately by clicking the **Send** button or you can skip this step by clicking **Postpone**.

In the latter case, on each subsequent launch of the application, the message above will continue to appear for the next 9 days. After this period, you will not be able to send a monthly usage report using the functionality described herein, but you can still review the report, as Veeam Backup for Microsoft Office 365 automatically saves it to the `%programdata%\Veeam\Backup365\Reports` directory in the `.pdf` and `.csv` formats.

Managing Reports

To review details of a report, click **Review** in the lower-left corner of the **Monthly Usage Report** dialog.

By default, Veeam Backup for Microsoft Office 365 will list each backed up user account of every organization added to the application scope.

You can do the following while in the **Monthly Usage Report** dialog to manage filters and perform other required actions:

- To view backed up accounts of a particular organization, select an organization in the drop-down list in the upper-left corner.
- To find accounts of the selected organization, use the search field in the upper-right corner.
- To prevent accounts from being added to the report, select such accounts and click **Remove**, then provide the removal reason (optional) and click **OK**.

To undo removing, click **Reset**.

- To save the report as a `.pdf` or `.csv` file, click **Save As** in the lower-left corner and specify a location.

MONTHLY USAGE REPORT

×

Monthly report for February 2019

All organizations

[Type in an object name to search for]

ACCOUNT ↑	ORGANIZATION NAME	LAST PROCESSED	
admin@abc.onmicrosoft.com	abc.onmicrosoft.com	2/4/2019 4:47 PM	

Remove

Reset

Save As

Send

Cancel

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 be receiving a notification message stating that your license is about to be expired. During this period, the program functionality will not be limited by any means. After your license has expired, processing of all user accounts will be stopped.

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 be receiving a notification message stating that your license is about to be expired. During this period, the program functionality will not be limited by any means. After your license has expired, processing of all user accounts will be stopped.

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.

Deployment

This section explains how to deploy Veeam Backup for Microsoft Office 365 to your environment.

Consider the following:

- If you have been participating in the public beta testing of Veeam Backup for Microsoft Office 365, make sure to uninstall the pre-release (BETA) versions of Veeam Backup for Microsoft Office 365, Veeam Explorer for Microsoft Exchange and Veeam Explorer for Microsoft SharePoint.
- 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 Office 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 Azure or Amazon Web Services (AWS).

Downloading Installation Package

You can download the Veeam Backup for Microsoft Office 365 installation package from the official [Veeam Website](#).

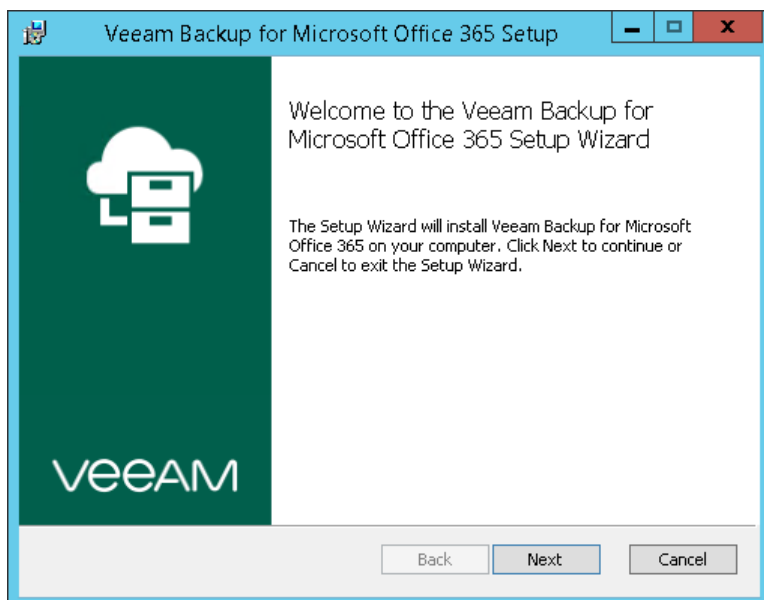
The installation package consists of the following MSI files:

- `Veeam.Backup365.msi` — installs Veeam Backup for Microsoft Office 365 with the following services:
 - *Veeam Backup for Microsoft Office 365 Service*
Controls global configuration settings.
 - *Veeam Backup Proxy for Microsoft Office 365 Service*
Manages backup proxy servers.
 - *Veeam Backup for Microsoft Office 365 RESTful API Service*
Processes RESTful commands. This component is disabled by default and can be enabled, as described in [Configuring RESTful API Settings](#).
- `VeeamExplorerForExchange.msi` — installs Veeam Explorer for Microsoft Exchange.
For more information, see the [Veeam Explorer for Microsoft Exchange](#) section of the Veeam Explorers User Guide.
- `VeeamExplorerForSharePoint.msi` — installs Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft OneDrive for Business.
For more information, see the [Veeam Explorer for Microsoft SharePoint](#) and [Veeam Explorer for Microsoft OneDrive for Business](#) sections of the Veeam Explorers User Guide.

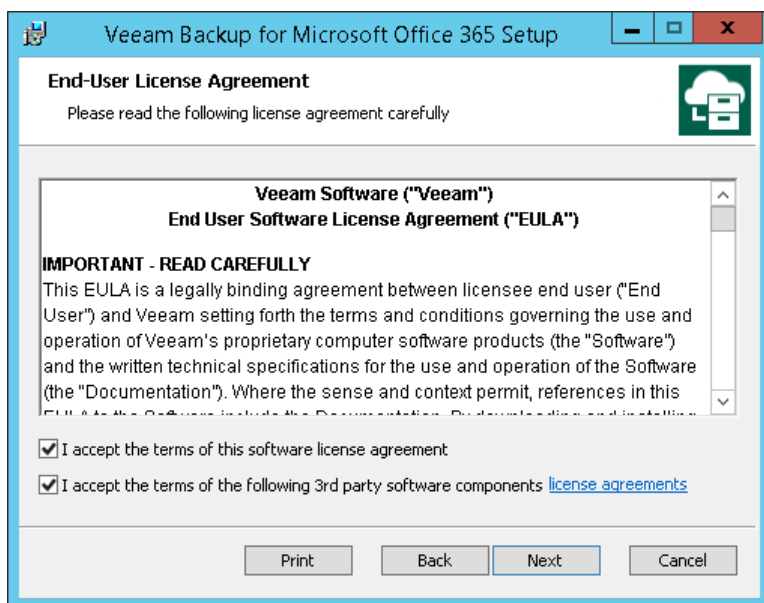
Installing Veeam Backup for Microsoft Office 365

To install Veeam Backup for Microsoft Office 365, do the following:

1. Run the `Veeam.Backup365.msi` file from the *Veeam Backup for Microsoft Office 365* distribution package.

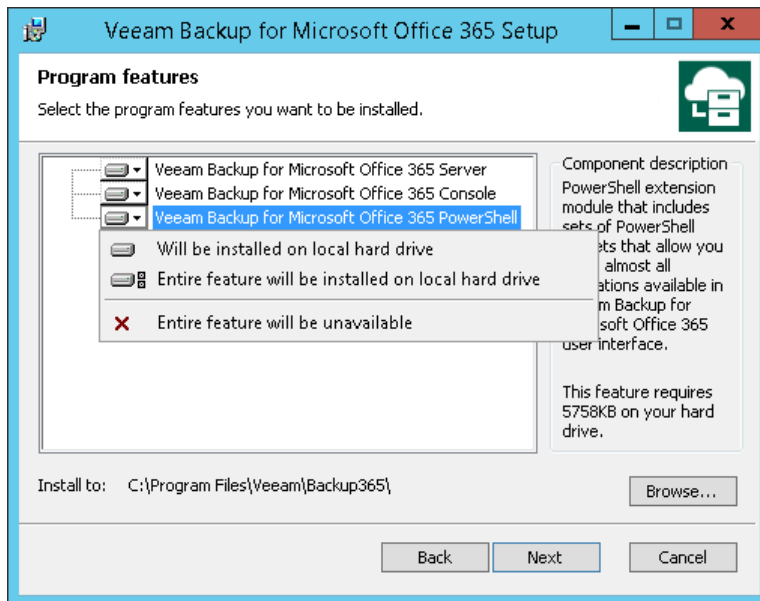


2. Read and accept **License Agreement**.

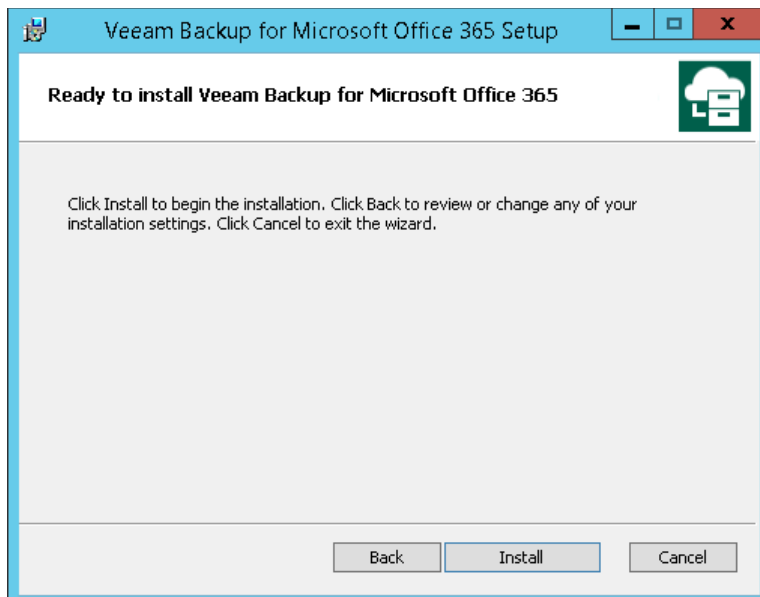


3. Select system components to install.

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



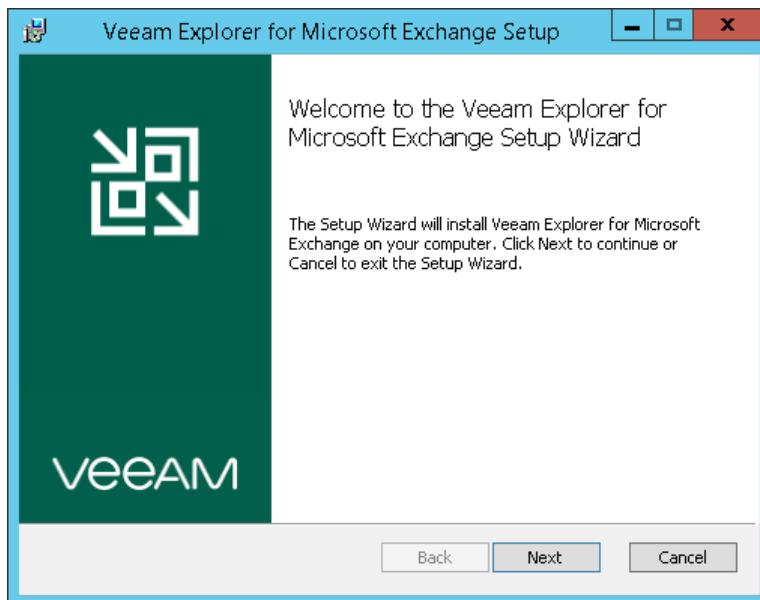
4. Click **Install**.



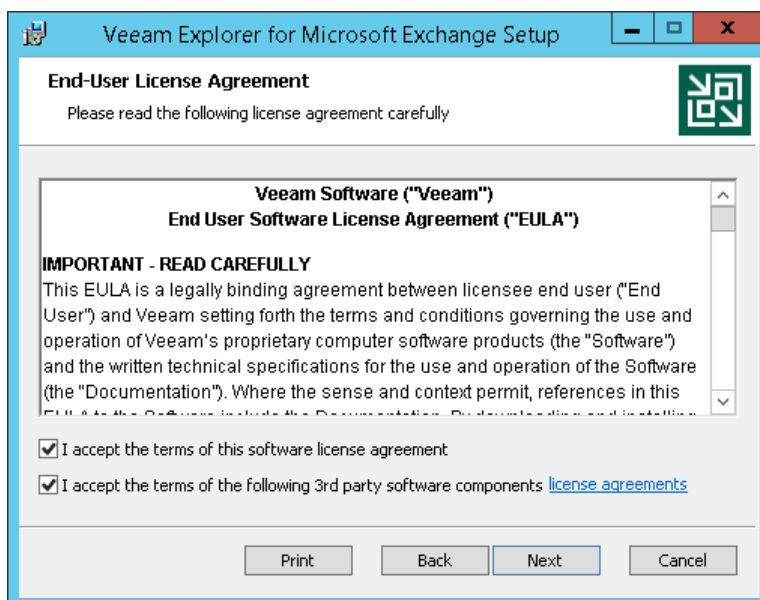
Installing Veeam Explorer for Microsoft Exchange

To install Veeam Explorer for Microsoft Exchange, do the following:

1. Run the `VeeamExplorerForExchange.msi` file from the *Veeam Backup for Microsoft Office 365* distribution package.

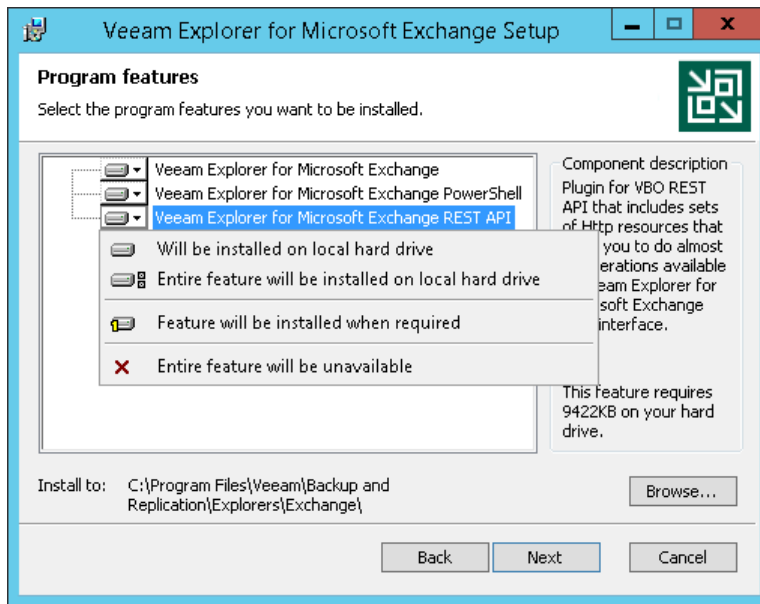


2. Read and accept **License Agreement**.

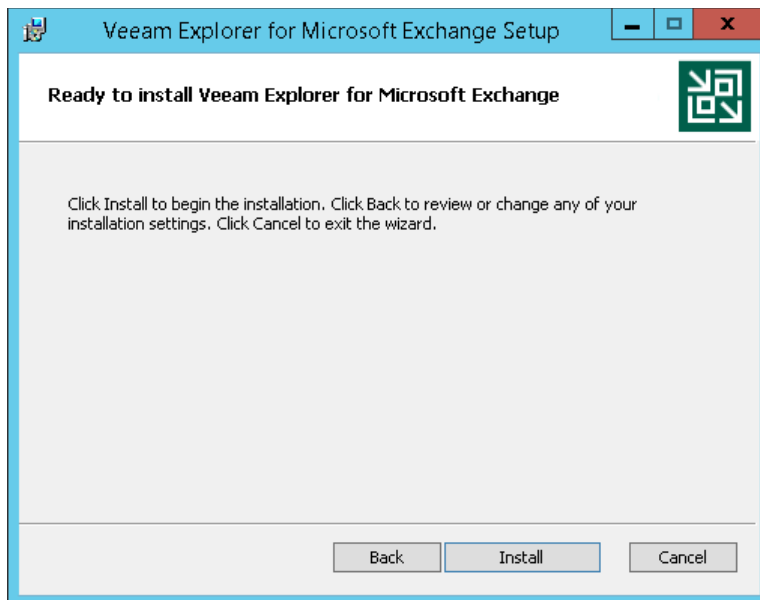


3. Select system components to install.

By default, Veeam Explorer for Microsoft Exchange will be installed to the `C:\Program Files\Veeam\Backup and Replication\Explorers\Exchange\` directory. To install to a different location, click **Browse** and specify a destination directory.



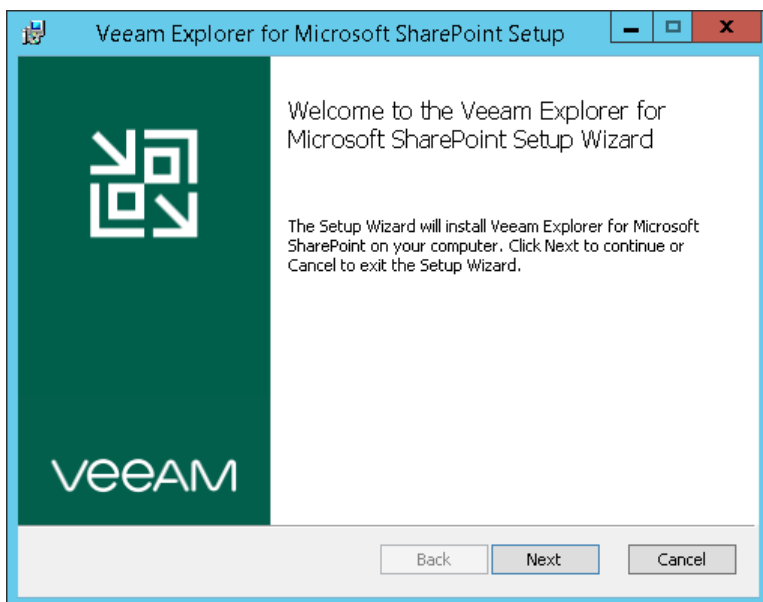
4. Click **Install**.



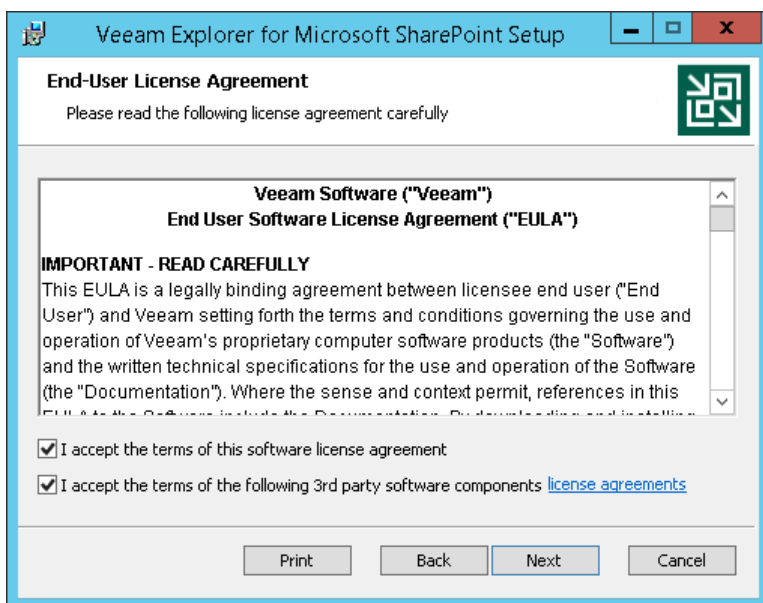
Installing Veeam Explorer for Microsoft SharePoint

To install Veeam Explorer for Microsoft SharePoint, do the following:

1. Run the `VeeamExplorerForSharePoint.msi` file from the *Veeam Backup for Microsoft Office 365* distribution package.

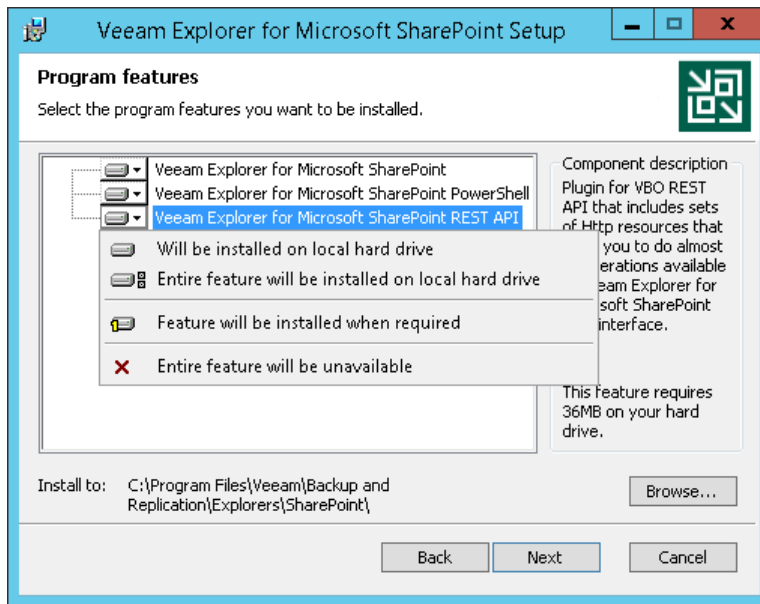


2. Read and accept **License Agreement**.

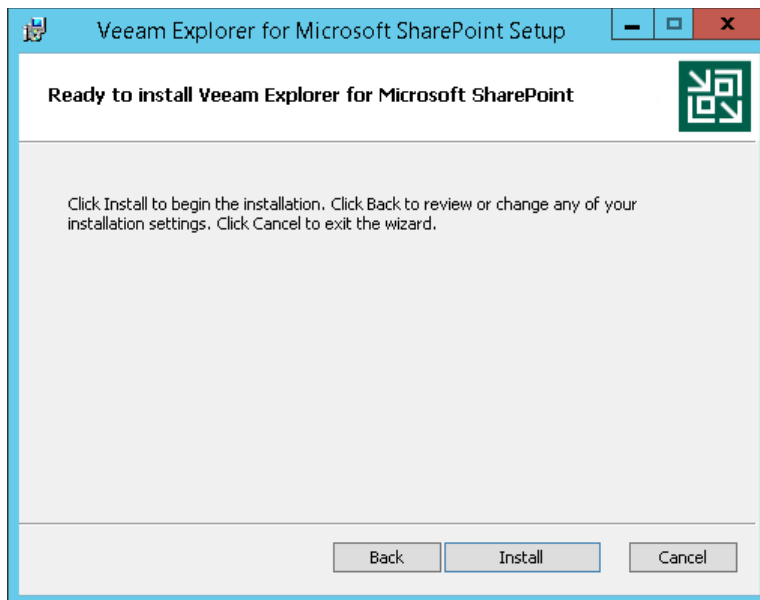


3. Select system components to install.

By default, Veeam Explorer for Microsoft SharePoint will be installed to the `C:\Program Files\Veeam\Backup and Replication\Explorers\SharePoint\` directory. To install to a different location, click **Browse** and specify a destination directory.



4. Click **Install**.



NOTE:

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

Installing in Unattended Mode

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

The syntax of running an *MSI* package is as follows:

```
msiexec /i <path_to_msi> /qn ADDLOCAL=<feature1, feature2>  
ACCEPT_THIRDPARTY_LICENSES=1 ACCEPT_EULA=1
```

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

Component	Feature name
Server	BR_OFFICE365
Console	CONSOLE_OFFICE365
PowerShell	PS_OFFICE365

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*.

Component	Feature name
UI	BR_SHAREPOINTEXPLORER
PowerShell	PS_SHAREPOINTEXPLORER

Examples

To install the *Veeam Backup for Microsoft Office 365* and *PowerShell* components.

```
msiexec /i Veeam.Backup365.msi /qn  
ADDLOCAL=BR_OFFICE365,CONSOLE_OFFICE365,PS_OFFICE365 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_SHAREPOINTEXPLORER,PS_SHAREPOINTEXPLORER 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.

Deploying to Azure and AWS

Veeam Backup for Microsoft Office 365 can be deployed to Azure or Amazon Web Services (AWS) cloud platforms according to the following steps:

1. Install Veeam Backup for Microsoft Office 365 on an Azure or AWS virtual machine, as described in [Installing Veeam Backup for Microsoft Office 365](#).

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

When deploying to Azure, we recommend using [F-Series VM Sizes](#) for better performance.

2. Configure additional backup proxy servers, as described in [Configuring Backup Proxy Servers](#).
3. Configure backup repositories, as described in [Configuring Backup Repositories](#).
4. Install Veeam Explorer for Microsoft Exchange and Veeam Explorer for Microsoft SharePoint, as described in [Installing Veeam Explorer for Microsoft Exchange](#) and [Installing Veeam Explorer for Microsoft SharePoint](#).

After deployment is complete, you can:

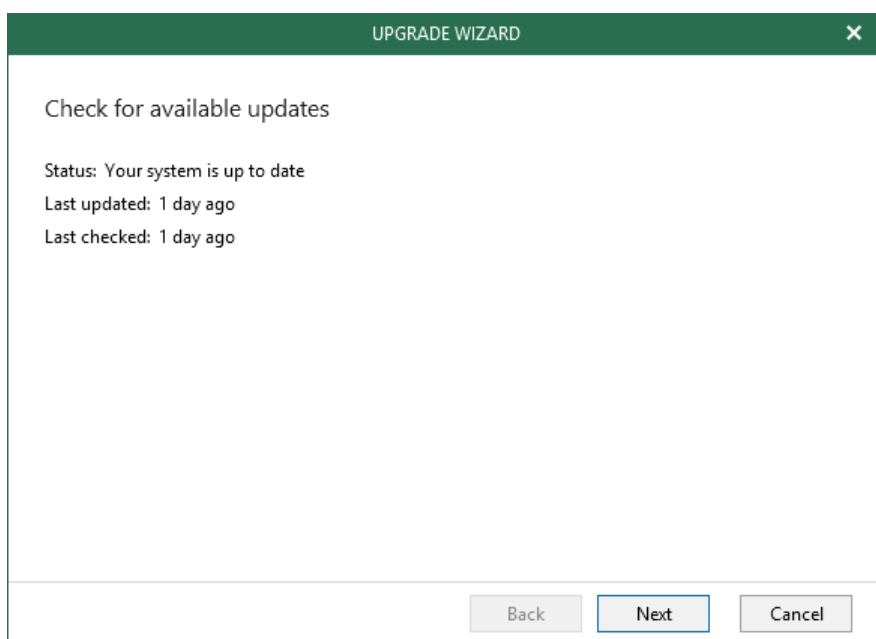
- Add Microsoft Office 365 and on-premises Microsoft organizations to the program scope, as described in [Microsoft Organizations Management](#).
- Create new backups, as described in [Data Backup](#).
- View and restore your data, as described in [Data Restore](#).

Checking for Updates

To perform an upgrade of Veeam Backup for Microsoft Office 365, do the following:

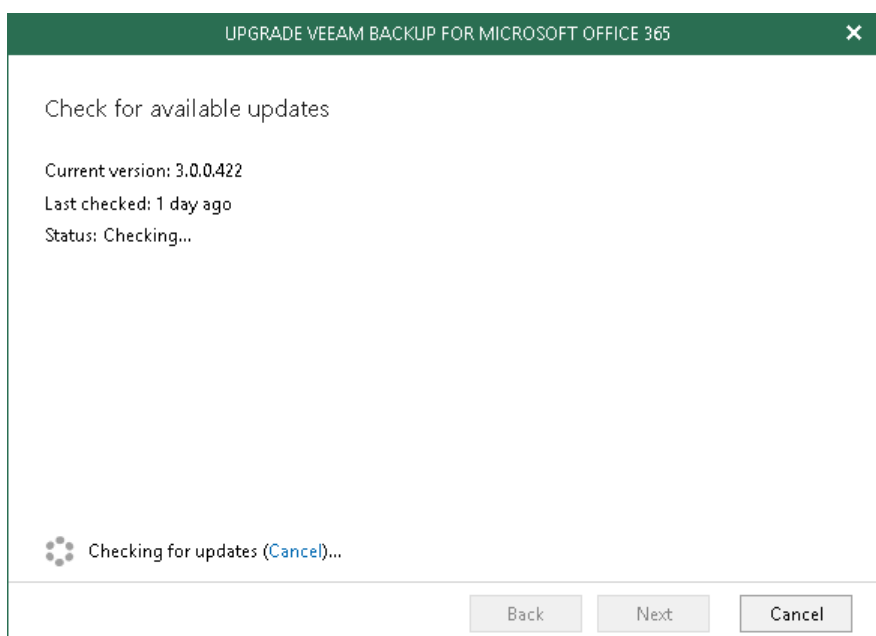
1. In the main menu, click **Upgrade**.
2. In the **Check for available updates** step, click **Next**.

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



3. Wait until Veeam Backup for Microsoft Office 365 checks whether a newer version is available.

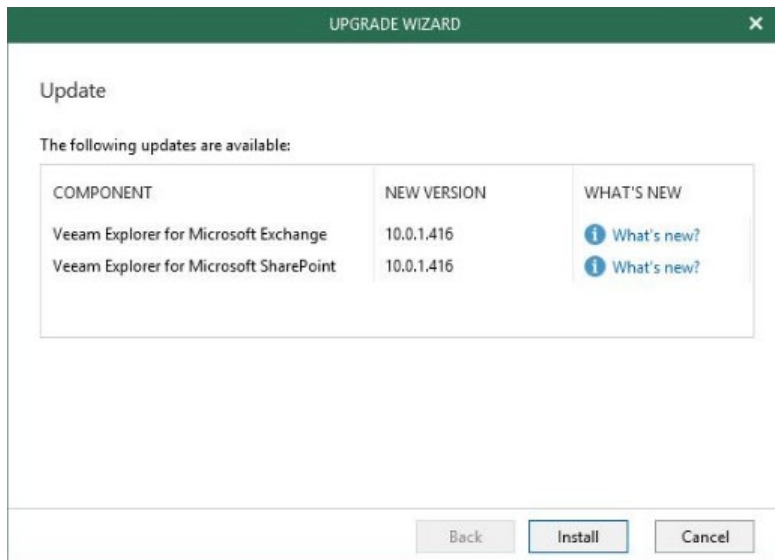
To abort the request, click **Cancel**.



4. If available, review details about new features and enhancements and click **Upgrade**.

During upgrade, the Veeam Backup for Microsoft Office 365 console will be closed, whereupon you will be offered to go through the setup steps, as described in [Installing Veeam Backup for Microsoft Office 365](#).

5. Once installation is complete, launch Veeam Backup for Microsoft Office 365, as described in [Launching Veeam Backup for Microsoft Office 365](#).
6. After you launch the Veeam Backup for Microsoft Office 365 console, you will be offered to upgrade Veeam Explorer for Microsoft Exchange and Veeam Explorer for Microsoft SharePoint.



NOTE:

Veeam Backup for Microsoft Office 365 is also capable of checking for a newer version of the application automatically. For that, select the **Automatically check and notify me on available updates** check box on the **Updates** tab, as described in [Configuring Update Notifications](#).

Installing and Updating License

After you install Veeam Backup for Microsoft Office 365, you will be prompted to provide a product license. You can dismiss this step and continue using the product without any license installed. In this case, you will have *Community Edition* mode that allows you to process up to 10 user accounts in all organizations including 1TB of Microsoft SharePoint data. *Community Edition* mode suggests using the community license, which is not limited in time, nor imposes any limitations in terms of program 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 or more than 1TB of Microsoft SharePoint data. For more information about available license types in Veeam Backup for Microsoft Office 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 see how many accounts are available 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** dialog, click **Install** and specify the path to the *.lic* file.

Updating License

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

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

To automatically update 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 [Used Ports](#).

LICENSE INFORMATION

Installed license

Status	Valid
Expiration date	1/17/2019 (36 days left)
Type	Subscription
Licensed to	Veeam Software AG
Contact person	Dev and QA Departments
Users	9999 (2 used)
Support ID	00782619
Support expiration date	1/17/2019 (36 days left)

Install...

Update Now

☒ Update license automatically (enables usage reporting)

OK

Cancel

Upgrading to Veeam Backup for Microsoft Office 365 4.0

Veeam Backup for Microsoft Office 365 application upgrade to version 4.0 is supported for the following versions:

- Veeam Backup for Microsoft Office 365 2.0 (product builds 2.0.0.567, 2.0.0.594 and 2.0.0.814).
- Veeam Backup for Microsoft Office 365 3.0 (product builds 3.0.0.422).

Consider the following:

- All modifications made to the `Config.xml` file manually will be lost.
- Upgrade of backup jobs created with version 2.0 is only required if these jobs contain Microsoft SharePoint sites.
- Backup jobs that have not been upgraded to Veeam Backup for Microsoft Office 365 version 2.0 will be removed.

For example, if you are still using Veeam Backup for Microsoft Office 365 version 1.5 or 1.0 and have not upgraded to version 2.0 prior to upgrading to version 4.0.

- The *Veeam Backup for Microsoft Office 365 RESTful API Service* must be enabled manually after the upgrade using the `services.msc` console.

Upgrading Application

To upgrade Veeam Backup for Microsoft Office 365, install Veeam Backup for Microsoft Office 365 version 4.0, as described in the following sections:

- [Installing Veeam Backup for Microsoft Office 365](#)
- [Installing Veeam Explorer for Microsoft Exchange](#)
- [Installing Veeam Explorer for Microsoft SharePoint](#)

Once installed, the following system components will be marked as **Out of Date**:

- *Backup repositories*

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

- *Backup jobs*

For more information on how to upgrade backup jobs, see [Upgrading Backup Job](#).

- *Backup proxy servers*

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

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

Uninstalling Veeam Backup for Microsoft Office 365

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

1. Stop all restore sessions (if any) in Veeam Explorer for Microsoft Exchange, Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft OneDrive for Business.
2. Open the Veeam Backup for Microsoft Office 365 console, go to **Backup Infrastructure > Backup Proxies** and remove all configured backup proxy servers, as described in [Removing Backup Proxy Server](#).
3. Open **Control Panel > Programs and Features**, select **Veeam Backup for Microsoft Office 365** and click **Uninstall**.
4. In the **Control Panel > Programs and Features**, select **Veeam Backup & Replication** and click **Uninstall** to uninstall Veeam Explorers.

Launching Veeam Backup for Microsoft Office 365

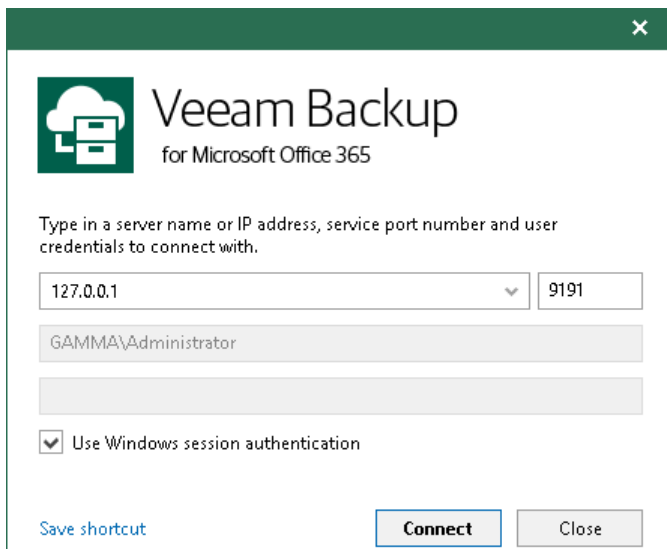
To launch Veeam Backup for Microsoft Office 365, go to **Start**, select **Veeam Backup for Microsoft Office 365** and specify the following:

1. A name or IP-address of the Veeam Backup for Microsoft Office 365 server.
2. A port number via which to connect to the specified Veeam Backup for Microsoft Office 365 server.
3. Authentication credentials that you want to use to connect to the specified Veeam Backup for Microsoft Office 365 server.

The account you are using must be a member of the *Local Administrator* group on the specified Veeam Backup for Microsoft Office 365 server.

To use your current account, select **Use Windows session authentication**.

To save a connection shortcut to the desktop, click **Save shortcut** in the bottom-left corner.



Launching via Command Line

To launch the application via 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 Office 365 that is installed on a local machine using the *Local System* account.

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 Office 365 that is installed on a remote machine using the **/host** and **/port** parameters.

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 Office 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 Office 365 using the **/account=<domain\accountName>** format.

Example:

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

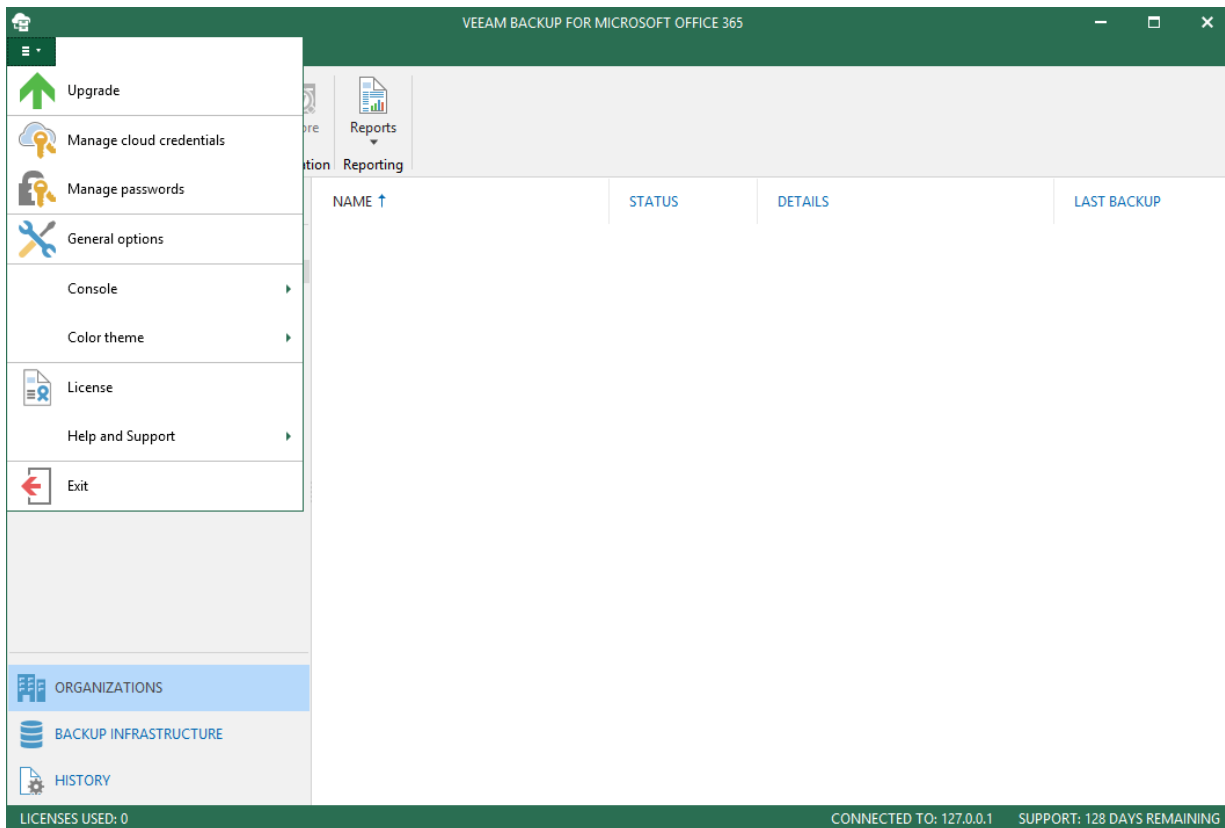

User Interface

Continue with this section to learn more about the Veeam Backup for Microsoft Office 365 user interface.

Main Menu

The main menu comprises the following:

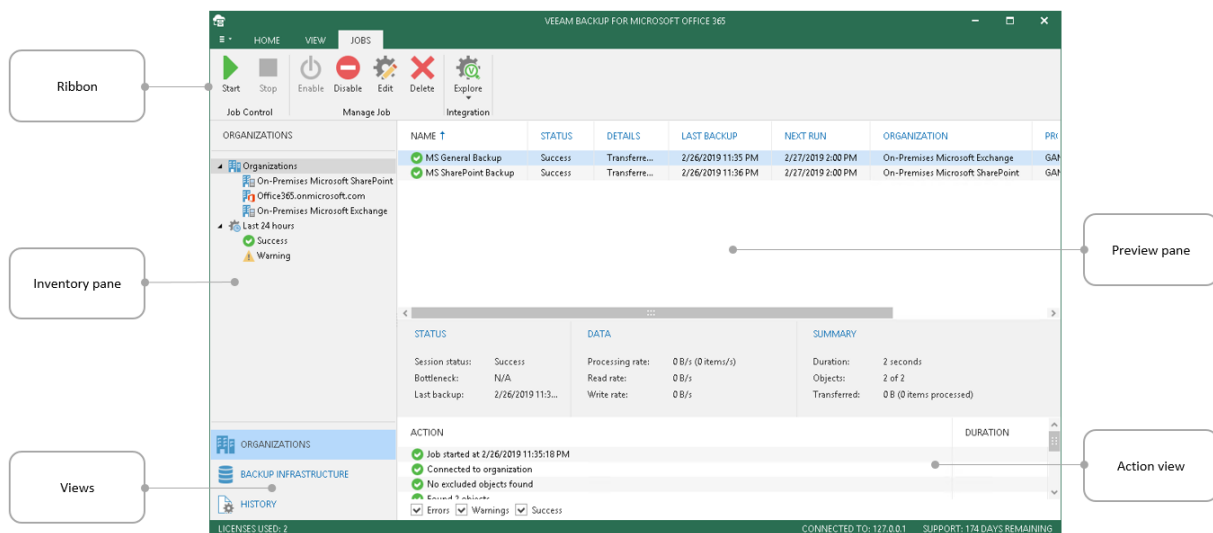
- **Upgrade.** Allows you to upgrade Veeam Backup for Microsoft Office 365.
For more information, see [Checking for Updates](#).
- **Managing cloud credentials.** Allows you to manage cloud passwords.
For more information, see [Managing Cloud Credentials](#).
- **Managing passwords.** Allows you to manage encryption passwords.
For more information, see [Managing Encryption Passwords](#).
- **General Options.** Allows you to configure general application options.
For more information, see [General Settings](#).
- **Console.**
 - **PowerShell.** Opens the PowerShell toolkit.
 - **Swagger.** Opens **Swagger Website**. Unavailable until you enable the REST service. For more information, see [Configuring RESTful API Settings](#).
- **Color Theme.** Contains four different color schemes that you can select for your application console.
- **License.** Shows license information.
For more information, see [Installing License](#).
- **Help and Support.**
 - **Online help.** Opens the online web help page.
 - **Support Information.** Launches the support information collection wizard.
For more information, see [Log Files Export](#).
 - **About.** Shows product information.
- **Exit.** Closes the program.



Main Application Window

The main application window can be divided into five categories:

1. The ribbon, which contains general commands organized into logical groups represented as tabs:
 - The **Home** tab provides quick access to common application operations.
 - 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 and backup repositories.
2. The inventory pane, which shows you a list of organizations added to the scope.
3. The preview pane, which shows you a list of backup jobs configured for the selected organization.
4. The views switch, which allows you to switch among the infrastructure views such as **Organizations**, **Backup Infrastructure** and **History**.
5. The action view, which allows you to view details about backup jobs results.



TIP:

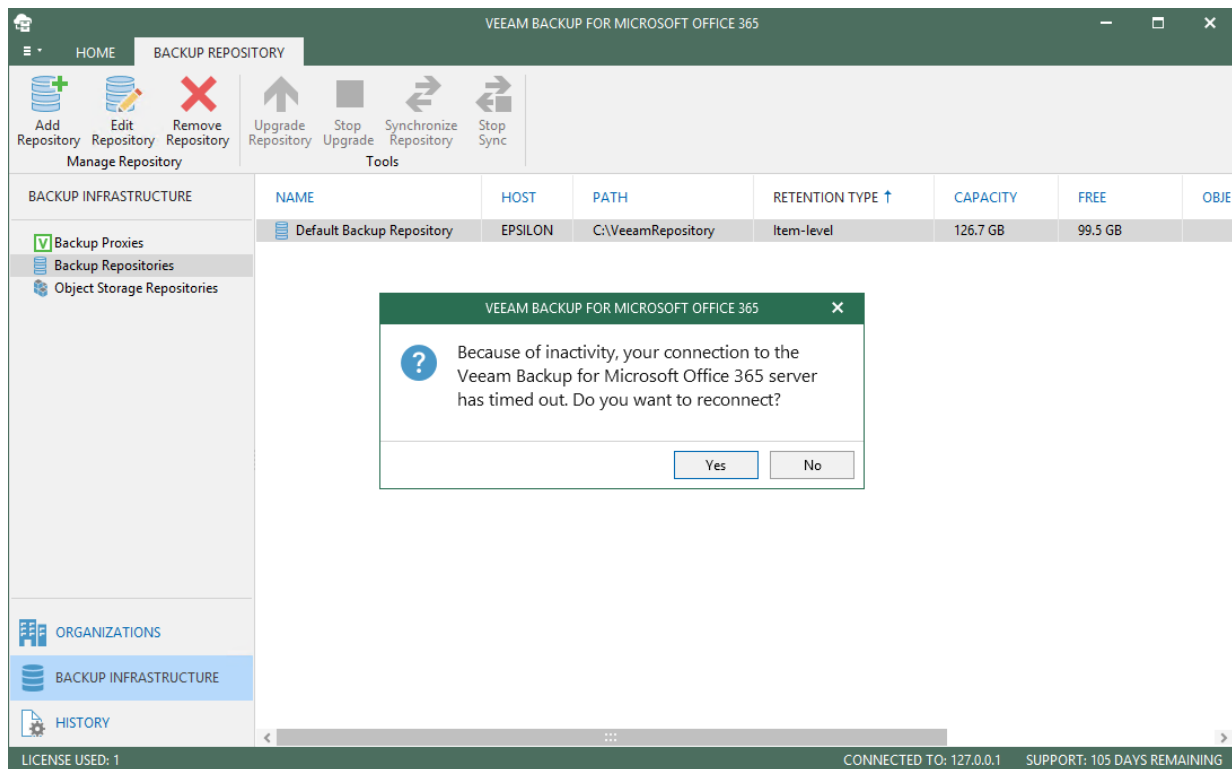
To open online help, press F1 in any Veeam Backup for Microsoft Office 365 wizard or window.

Current Session

Each time you open the Veeam Backup for Microsoft Office 365 console, a new connection is established to the [specified backup server](#). After 30 minutes of idleness, such a connection is timed out prompting you whether to continue using the product, thereby reestablishing a connection, or exit the console.

Consider the following:

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



Configuration

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

General Settings

You can configure general settings for Veeam Backup for Microsoft Office 365. General settings are applied to all [backup jobs](#) and [backup infrastructure](#) components.

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:

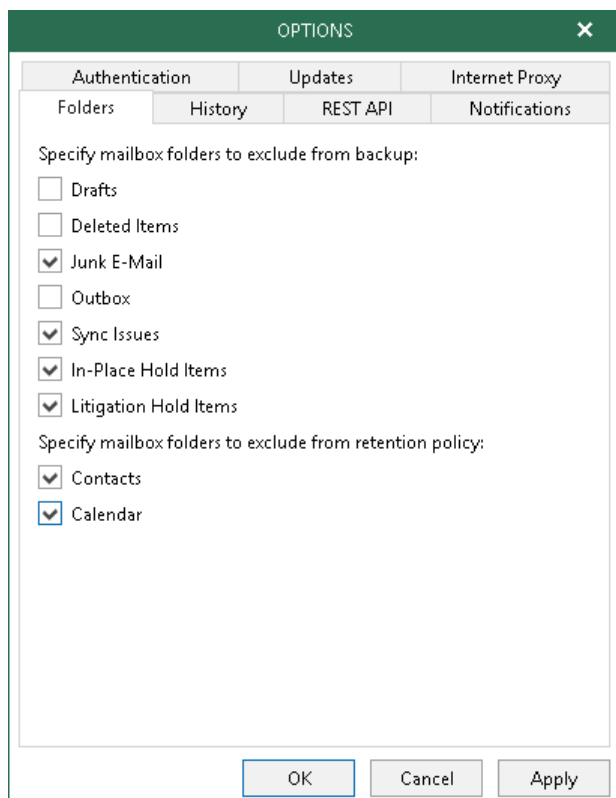
1. In the main menu, click **General Options**.
2. Open the **Folders** tab.
3. In the **Specify mailbox folders to exclude from backup** section, select folders that you want to exclude from a backup.
4. Click **OK**.

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**.

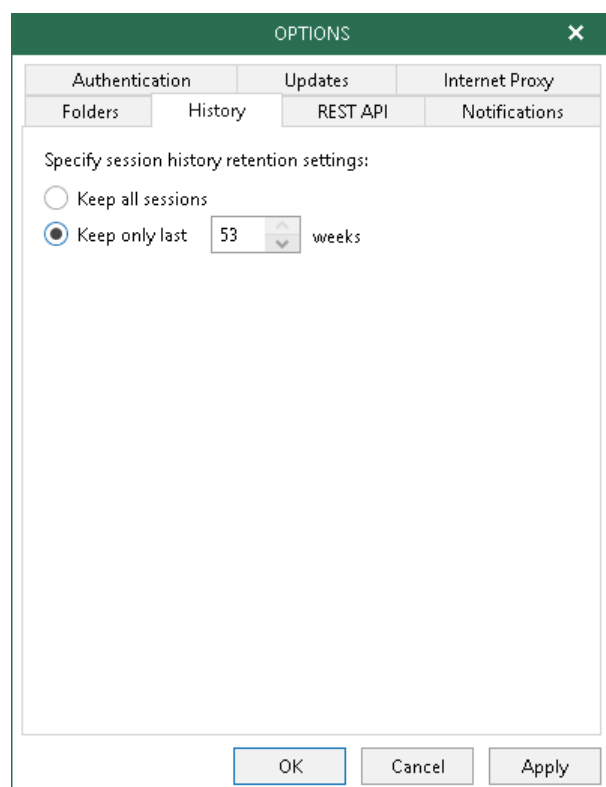


Session History

Veeam Backup for Microsoft Office 365 saves its backup and restore sessions to the configuration database. You can review such sessions, as described in [Backup and Restore Statistics](#).

To configure a period during which to keep backup and restore sessions log data, do the following:

1. In the main menu, click **General Options**.
2. Open the **History** tab.
3. Specify for how long the history of your backup and restore sessions should be kept. You can select **Keep all sessions** or specify a custom value in the **Keep only last** field.



RESTful API Settings

You can use the RESTful API to communicate with Veeam Backup for Microsoft Office 365.

To configure Veeam Backup for Microsoft Office 365 RESTful 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 (in minutes)** field, specify the lifetime value for an authentication token.

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

5. In the **HTTPS port** field, specify a port number via which you can access the RESTful service.
6. Click **Install** to specify an SSL certificate.

You can generate a new certificate or select an existing one using the **Select Certificate** wizard, as described in [SSL Certificate](#).

The screenshot shows the 'OPTIONS' dialog box with the 'REST API' tab selected. The dialog has a title bar with a close button. Below the title bar are tabs for 'Authentication', 'Updates', 'Internet Proxy', 'Folders', 'History', 'REST API', and 'Notifications'. The 'REST API' tab is active, displaying the following settings:

- A descriptive text: 'Specify the port configuration and SSL certificate to be used by Veeam Backup for Microsoft Office 365 RESTful API Service.'
- A checked checkbox labeled 'Enable REST service'.
- A numeric spinner for 'Authentication token lifetime (in minutes)' set to 60.
- A numeric spinner for 'HTTPS port' set to 4443.
- A section titled 'Installed certificate' containing:
 - 'Issued to:' and 'Issued by:' fields, both showing 'CN=Veeam Software, O=Veeam Software, OU='.
 - 'Friendly name:' field showing 'Veeam Software'.
 - 'Expiration date:' field showing '12/12/2028 5:06 AM'.
 - An 'Install...' button.

At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

Notification Settings

Continue with this section to learn how to configure Veeam Backup for Microsoft Office 365 to send email notifications about backup job completion results.

Consider the following:

- Notifications about backup job completion results are sent by a backup proxy server.
Such a server is selected in the [Specify Backup Proxy and Repository](#) step of the new backup job wizard.
- By default, system notifications are sent every time a backup job completes its sessions with any of the following states: *Success*, *Warning* and *Failure*. To turn off unwanted notifications, deselect check boxes that correspond to the events you do not want to be notified about.
- If a backup job is configured to perform retry attempts, you can select the **Suppress notifications until last retry** check box to send email notifications only after the last attempt.

To configure email notifications, do the following:

1. In the main menu, click **General Options**.
2. Go to the **Notifications** tab.
3. Select the **Enable e-mail notifications** check box.
4. Specify the address of a server you want to use as an SMTP server.
5. To provide advanced settings, click **Advanced** and specify the following:
 - A port number of an SMTP server you want to use.
By default, Veeam Backup for Microsoft Office 365 establishes a connection to *smtp.office365.com* via port *587*. For more information, see [this Microsoft article](#).
 - Select the **Connect Using SSL** check box to establish a secure connection.
 - Select the **The SMTP server requires authentication** check box and provide authentication credentials.
6. In the **From** field, specify the email address to be shown as a sender.
7. In the **To** field, specify the email address for a notification recipient.
To specify multiple email addresses, use semicolon.
8. By default, a notification subject will be as follows: *[%JobResult%] %OrgName% - %JobName% (%ObjectCount% objects), %Issues% issues*:
 - *%JobResult%*. A backup job result (*Success*, *Warning*, *Failed*).
 - *%OrgName%*. An Office 365 organization for which the job was configured.
 - *%JobName%*. The backup job name.
 - *%ObjectCount%*. The number of processed items.
 - *%Issues%*. The number of items with *Failed* or *Warning* states.
 - *%Time%*. Date and time of backup job completion.
9. In the **Attachment** drop-down list, select whether to include a detailed report as an attachment to the email.

Mind that such a report is only sent if contains more than 1000 users.

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

The screenshot shows the 'OPTIONS' dialog box with the 'Notifications' tab selected. The 'Enable e-mail notifications' checkbox is checked. The SMTP server is set to 'smtp.office365.com'. The 'From' field is 'Administrator@tech.org' and the 'To' field is 'Recipient@tech.org'. The 'Subject' field contains the template string '[%JobResult%] %OrgName% - %JobName% (%ObjectCount%)'. The 'Attachment' dropdown is set to 'Include detailed report as an attachment'. The 'Test Message' button is visible. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Authentication	Updates	Internet Proxy
Folders	History	REST API

☒ Enable e-mail notifications

SMTP server:
smtp.office365.com Advanced...

From:
Administrator@tech.org

To:
Recipient@tech.org

Subject:
[%JobResult%] %OrgName% - %JobName% (%ObjectCount%)

Attachment:
Include detailed report as an attachment ▼

Test Message

☒ Notify on success
☒ Notify on warning
☒ Notify on failure
☒ Suppress notifications until the last retry

OK Cancel Apply

Authentication Settings

Tenant authentication is required to view and recover backups that are located on the service provider side.

To enable tenant authentication, do the following:

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

You can generate a new certificate or select an existing one using the **Select Certificate** wizard, as described in [SSL Certificate](#).

TIP:

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

The screenshot shows the 'OPTIONS' dialog box with the 'Authentication' tab selected. The 'Enable tenants authentication with organization credentials' checkbox is checked. Below this, the 'Installed certificate' section displays the following details:

Field	Value
Issued to:	CN=Veeam Software, O=Veeam Software, OU=
Issued by:	CN=Veeam Software, O=Veeam Software, OU=
Friendly name:	Veeam Software certificate
Expiration date:	12/12/2028 5:12 AM

An 'Install...' button is located to the right of the expiration date field. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

Update Notification Settings

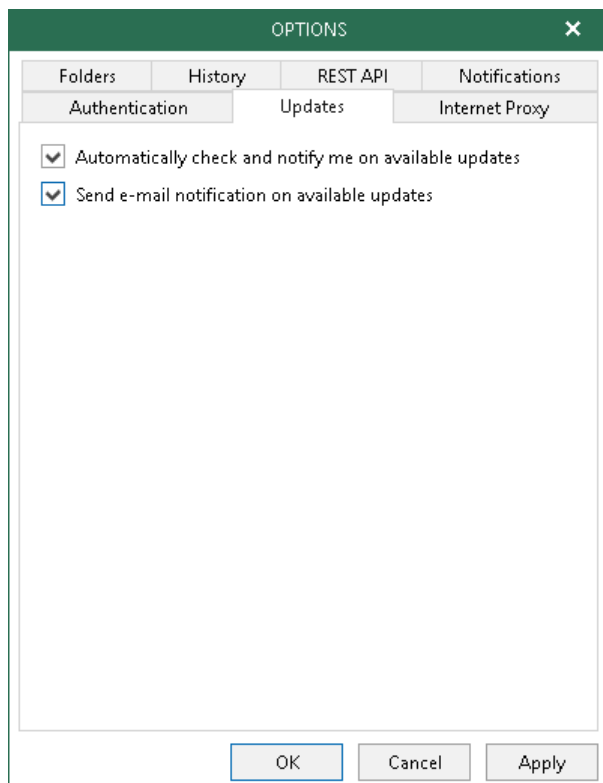
You can configure notifications about new versions of Veeam Backup for Microsoft Office 365.

To configure notifications, do the following:

1. In the main menu, click **General Options**.
2. Open the **Updates** tab.
3. Select the following check boxes:
 - **Automatically check and notify me on available updates.**
To be notified via a dialog message that appears in the user interface.
 - **Send e-mail notification on available updates.**
To be notified via an email message. The recipient address will be taken from the SMTP configuration settings. For more information, see [Configuring Notification Settings](#).

TIP:

To manually check for a new version, see [Checking for Updates](#).



Global Internet Proxy Server Settings

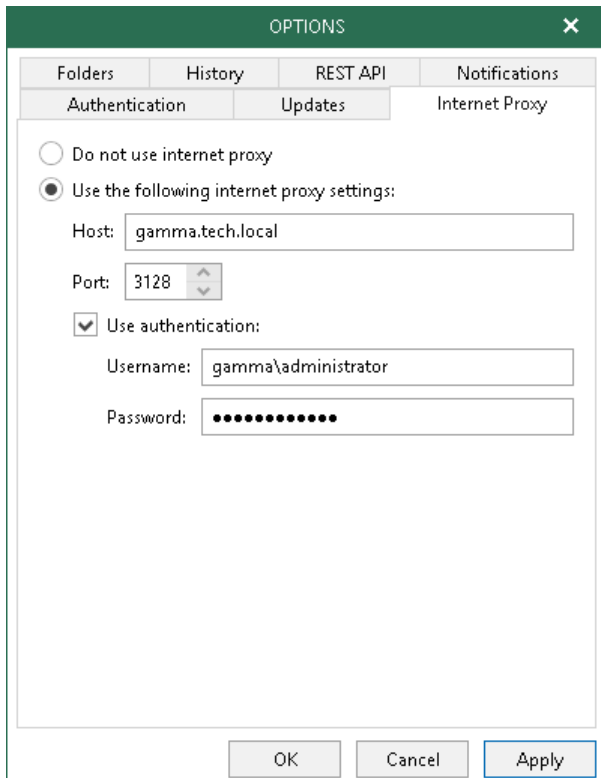
If a server on which Veeam Backup for Microsoft Office 365 is deployed does not have a direct access to the internet, you can assign an internet proxy server to be used as a gateway.

To set an internet proxy server, do the following:

1. In the main menu, click **General Options**.
2. Go to 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 via 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** to save the settings.

TIP:

In addition to configuring an internet proxy server for the Veeam Backup for Microsoft Office 365 server, you can configure such a server for each of your backup proxies, as described in [Configuring Internet Proxy Server for Backup Proxies](#).



The screenshot shows the 'OPTIONS' dialog box with the 'Internet Proxy' tab selected. The 'Do not use internet proxy' radio button is unselected, and the 'Use the following internet proxy settings:' radio button is selected. The 'Host' field contains 'gamma.tech.local'. The 'Port' field is set to '3128'. The 'Use authentication:' checkbox is checked, and the 'Username' field contains 'gamma\administrator'. The 'Password' field is masked with dots. At the bottom, there are 'OK', 'Cancel', and 'Apply' buttons.

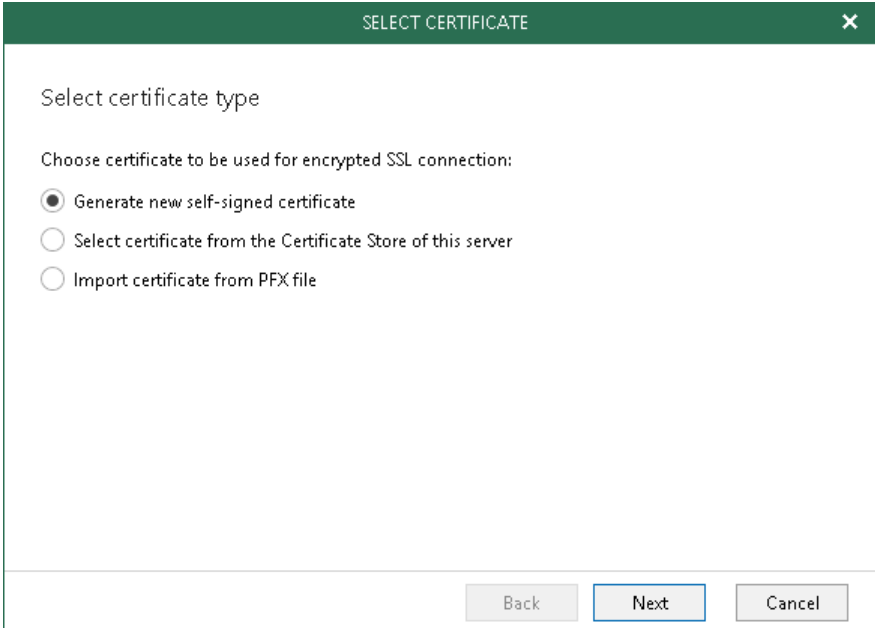
SSL Certificates

An SSL certificate is required in the following cases:

- To configure RESTful API settings.
For more information, see [RESTful API Settings](#).
- To enable user authentication with organization credentials for tenants.
For more information, see [Authentication Settings](#).
- To add Microsoft Office 365 organizations.
For more information, see [Microsoft Office 365 Organizations](#).
- To add backup applications to the backup configuration.
For more information, see [Backup Applications](#).

To install a new certificate, proceed with any of the following options:

- [Generate new self-signed certificate](#)
- [Select certificate from the Certificate Store of this server](#)
- [Import certificate from the PFX file](#)



SELECT CERTIFICATE

Select certificate type

Choose certificate to be used for encrypted SSL connection:

☒ Generate new self-signed certificate

☐ Select certificate from the Certificate Store of this server

☐ Import certificate from PFX file

Back Next Cancel

Generating New Certificate

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

SELECT CERTIFICATE

Generate certificate

Friendly name:

Veeam Software certificate

The certificate created by this feature will not originate from a trusted certification authority (CA). Users will be notified about this fact when establishing the initial connection to your service.

Back

Finish

Cancel

Selecting Certificate

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

SELECT CERTIFICATE

Pick certificate

Search:

[Type in an object name to search for]

ISSUED TO	EXPIRATION DATE	FRIENDLY NAME
epsilon.tech.local	5/14/2028 8:17:25 AM	Veeam Backup Server Certi
Veeam Backup Server Certificate	5/16/2019 8:36:38 AM	Veeam Backup Server Certi
WMSvc-EPSILON	10/8/2028 10:12:11 AM	WMSVC

<

...

>

Back

Finish

Cancel

Importing Certificate

To import a certificate, click **Browse** and select a *.pfx* file to use.

SELECT CERTIFICATE

×

Import certificate

Certificate:

C:\Certificate.pfx

Browse...

Password:

●●●●●●●●●●

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

Back

Finish

Cancel

Backup Infrastructure

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

- [Backup proxy servers](#)

Backup proxy servers are auxiliary machines that you can configure to effectively manage network traffic.

- [Backup repositories](#)

Backup repositories are storage systems that you can add to the Veeam Backup for Microsoft Office 365 backup infrastructure to keep your backup data.

- [Object storage repositories](#)

Object storage repositories are cloud-based and on-premises storage systems that you can employ to keep your backup data.

Backup Proxy Servers

A backup proxy server is an auxiliary physical or virtual machine that you can employ to leverage network traffic when [backing up](#) or [restoring](#) data.

Consider the following:

- A default backup proxy server is a machine with Veeam Backup for Microsoft Office 365.
It is recommended that after you install Veeam Backup for Microsoft Office 365, you 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.
- A server with Veeam Backup for Microsoft Office 365 and backup proxy servers must be deployed within the same or a trusted domain.
- 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 job completion results.

To send email notifications, backup proxy servers use an SMTP server that is configured, as described in [Configuring Notification Settings](#).

IMPORTANT!

Backup proxy servers and the machine hosting Veeam Backup for Microsoft Office 365 must be deployed within the same or a trusted domain.

Adding Backup Proxy Servers

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

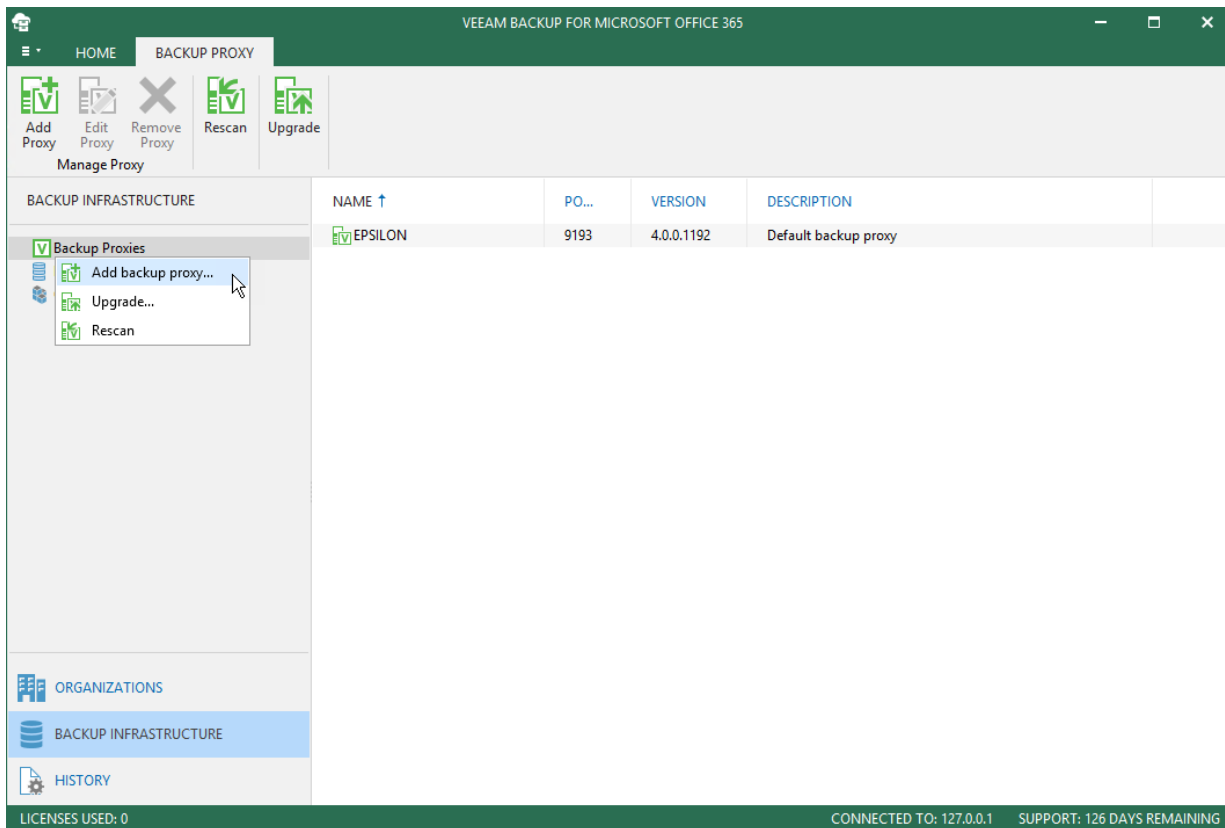
1. [Launch the New Backup Proxy wizard](#).
2. [Specify a backup proxy server address](#).
3. [Specify credentials](#).

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. On the **Backup Proxy** tab, click **Add Proxy**.

Alternatively, in the inventory pane, 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 the 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. In the **Description** field, enter a description (optional).

NEW BACKUP PROXY

Specify DNS name or IP address of the proxy server

Host: Port:

Description:

Back Next 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 Administrator* group.

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, as described in [Adding Backup Repository](#).

NEW BACKUP PROXY

Specify credentials to connect to the proxy server

Specify user account to connect to Windows server:

☐ Use current account (EPSILON\Administrator)

☒ Use the following account:

Username:

Password:

Back Next Cancel

Editing Backup Proxy Server Settings

Veeam Backup for Microsoft Office 365 allows you to edit settings of your backup proxy servers.

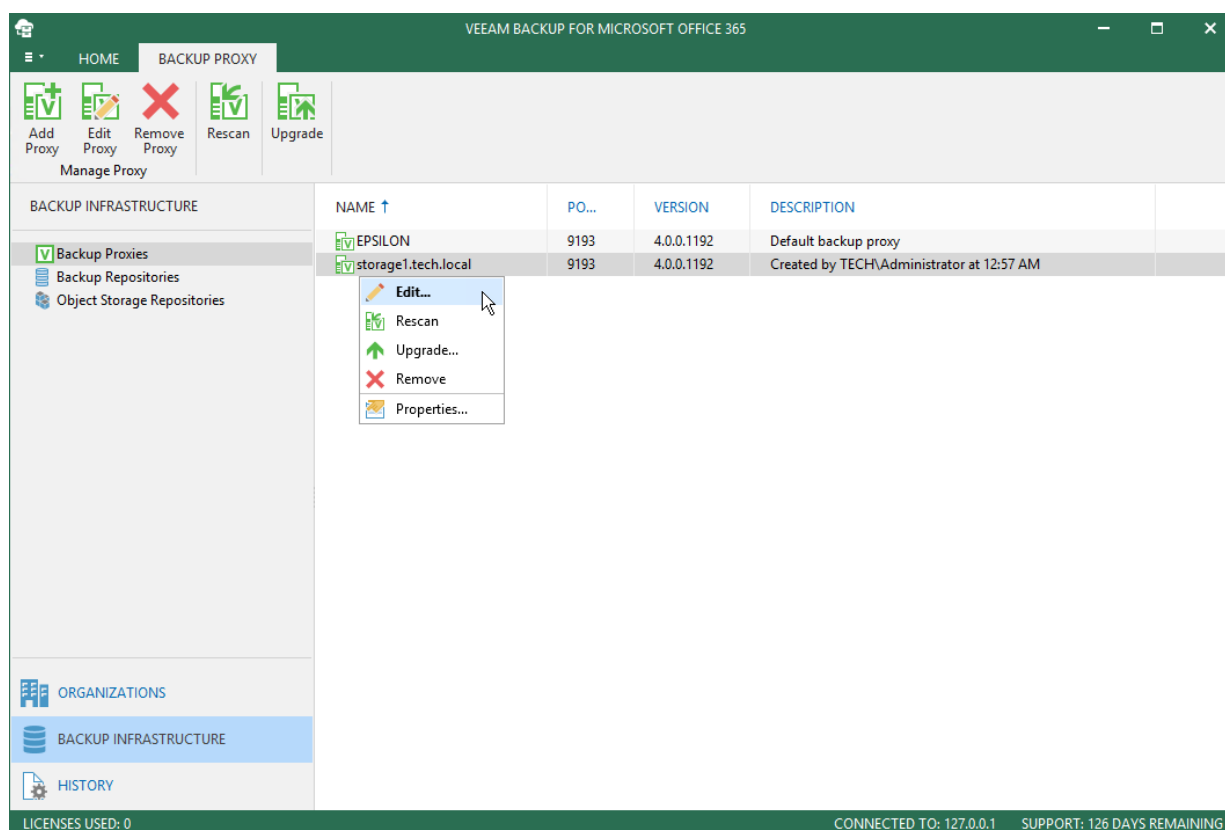
To edit backup proxy server settings, do the following:

1. Open the **Backup Infrastructure** view.

2. In the inventory pane, select the **Backup Proxies** node.
3. In the preview pane, select a backup proxy server.
4. On the **Backup Proxy** tab, click **Edit Proxy** on the ribbon.
Alternatively, in the preview pane, right-click a backup proxy server and select **Edit**.
5. Modify settings as required.

Consider the following:

- Editing a host server name is prohibited once it is set.
- The **Edit** command is unavailable if a backup proxy server needs to be upgraded, as described in [Upgrading Backup Proxy Servers](#).



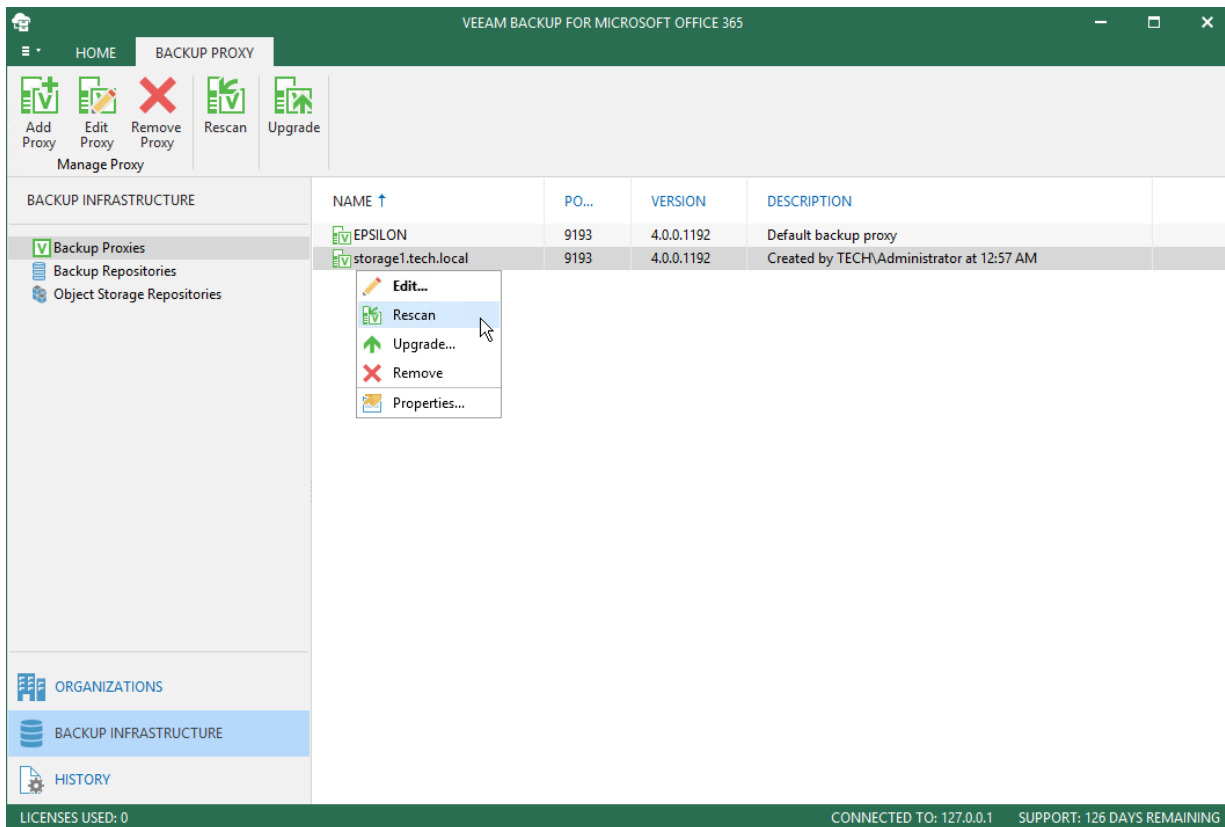
Rescanning Backup Proxy Servers

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, select a backup proxy server.
4. On the **Backup Proxy** tab, click **Rescan** on the ribbon.
Alternatively, in the preview pane, right-click a backup proxy server and select **Rescan**.

To rescan each backup proxy server in your environment, right-click the root **Backup Proxies** node and select **Rescan**.



Upgrading Backup Proxy Servers

To communicate with backup proxy servers, Veeam Backup for Microsoft Office 365 uses the proprietary service – *Veeam Backup Proxy for Microsoft Office 365 Service* that is installed on the target proxy machine. If this service becomes outdated, make sure to upgrade it manually.

To upgrade backup proxy servers, do the following:

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

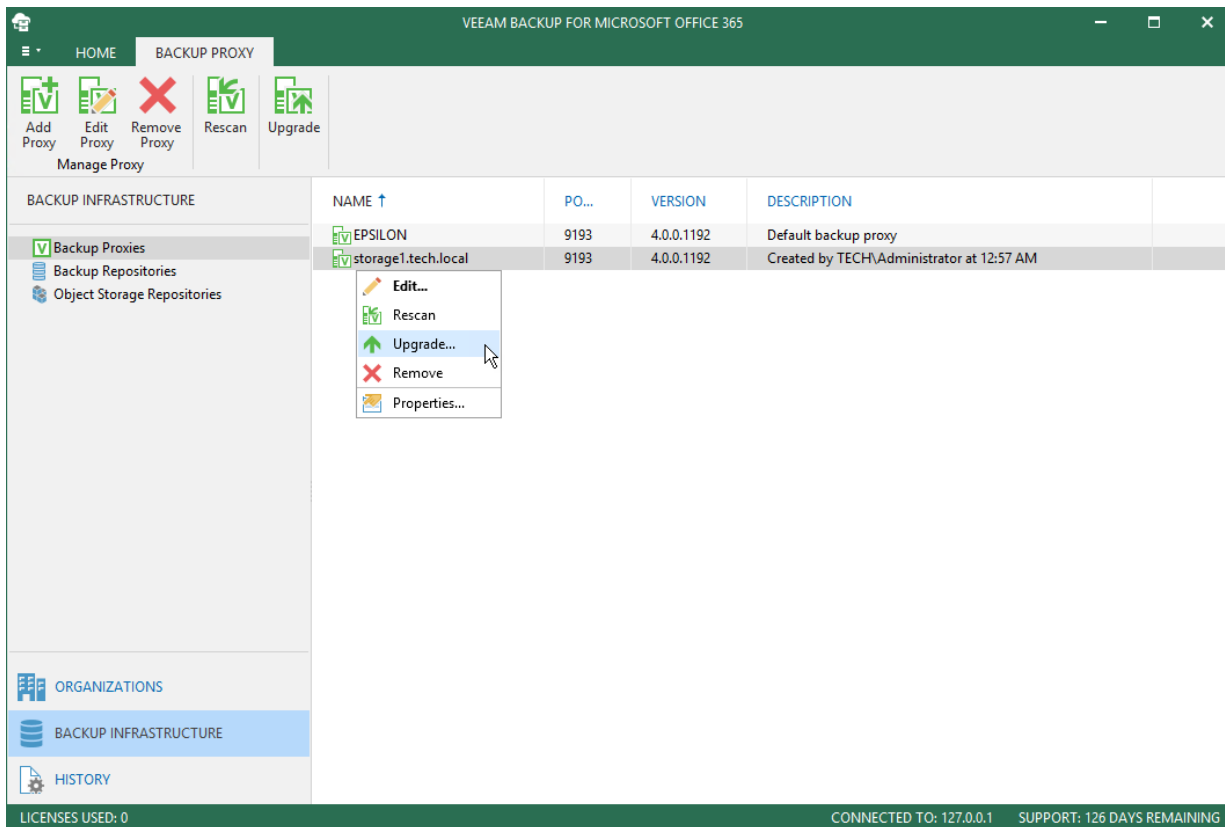
Step 1. Launch New Proxy Upgrade Wizard

To launch the new **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, select a backup proxy server.
4. On the **Backup Proxy** tab, click **Upgrade**.

Alternatively, in the preview pane, right-click a backup proxy server and select **Upgrade**.

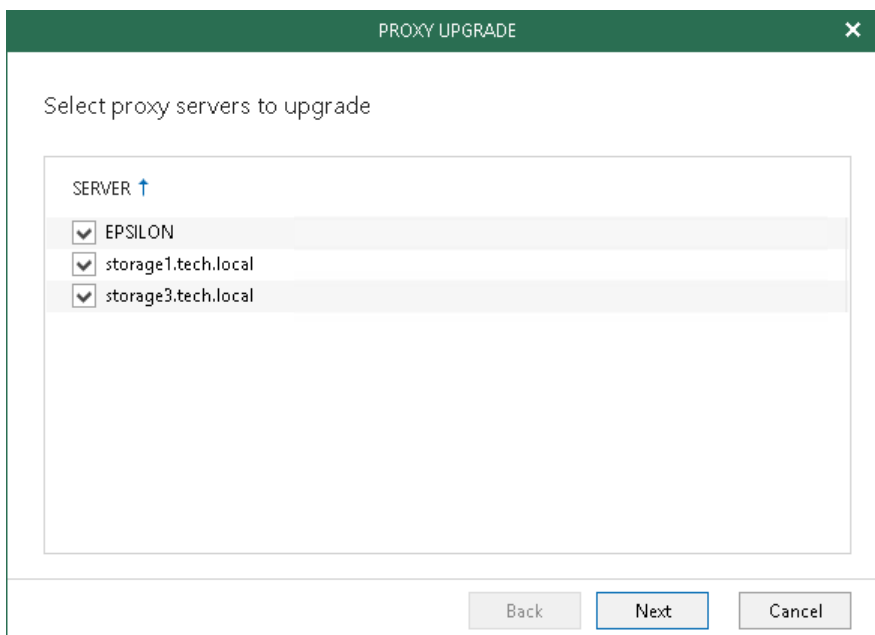
To upgrade all backup proxy servers at the same time, select the **Backup Proxies** node and click **Upgrade**.



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.

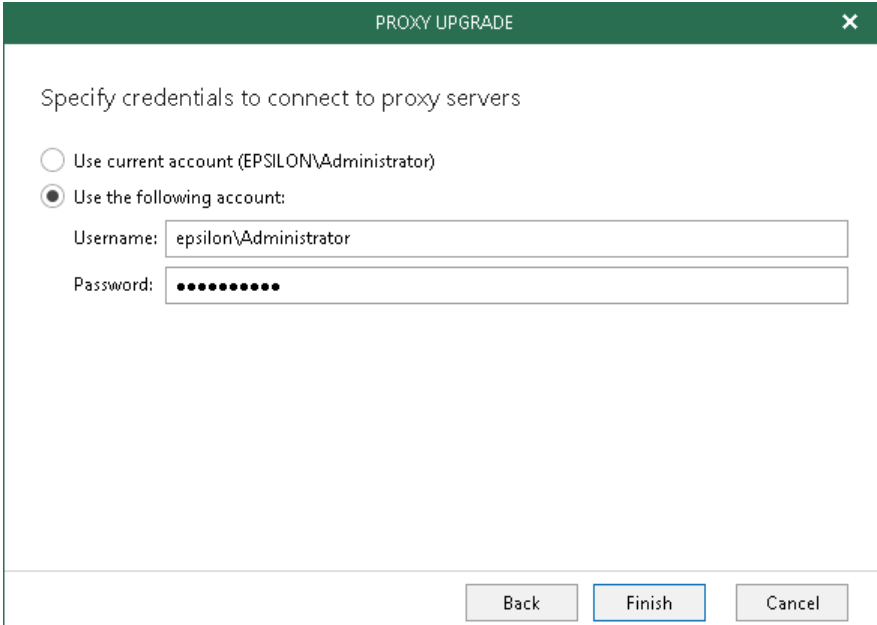
The default backup proxy server will be upgraded automatically.



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 Administrator* group.



PROXY UPGRADE

Specify credentials to connect to proxy servers

☐ Use current account (EPSILON\Administrator)

☒ Use the following account:

Username:

Password:

Back Finish Cancel

Removing Backup Proxy Servers

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

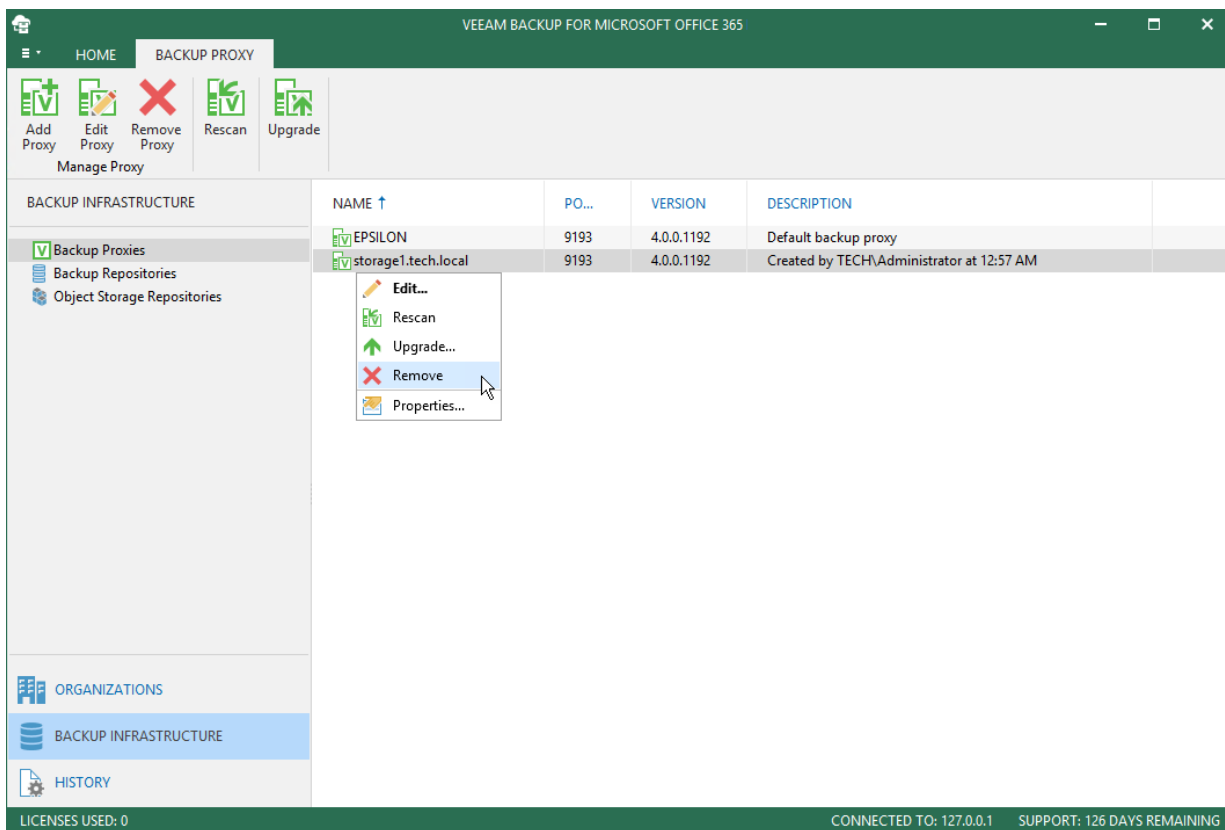
Consider the following:

- A default backup proxy server cannot be removed.
- The *Veeam Backup Proxy for Microsoft Office 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, select a backup proxy server.
4. On the **Backup Proxy** tab, click **Remove Proxy** on the ribbon.

Alternatively, in the preview pane, right-click a backup proxy server and select **Remove**.



Modifying Backup Proxy Server Properties

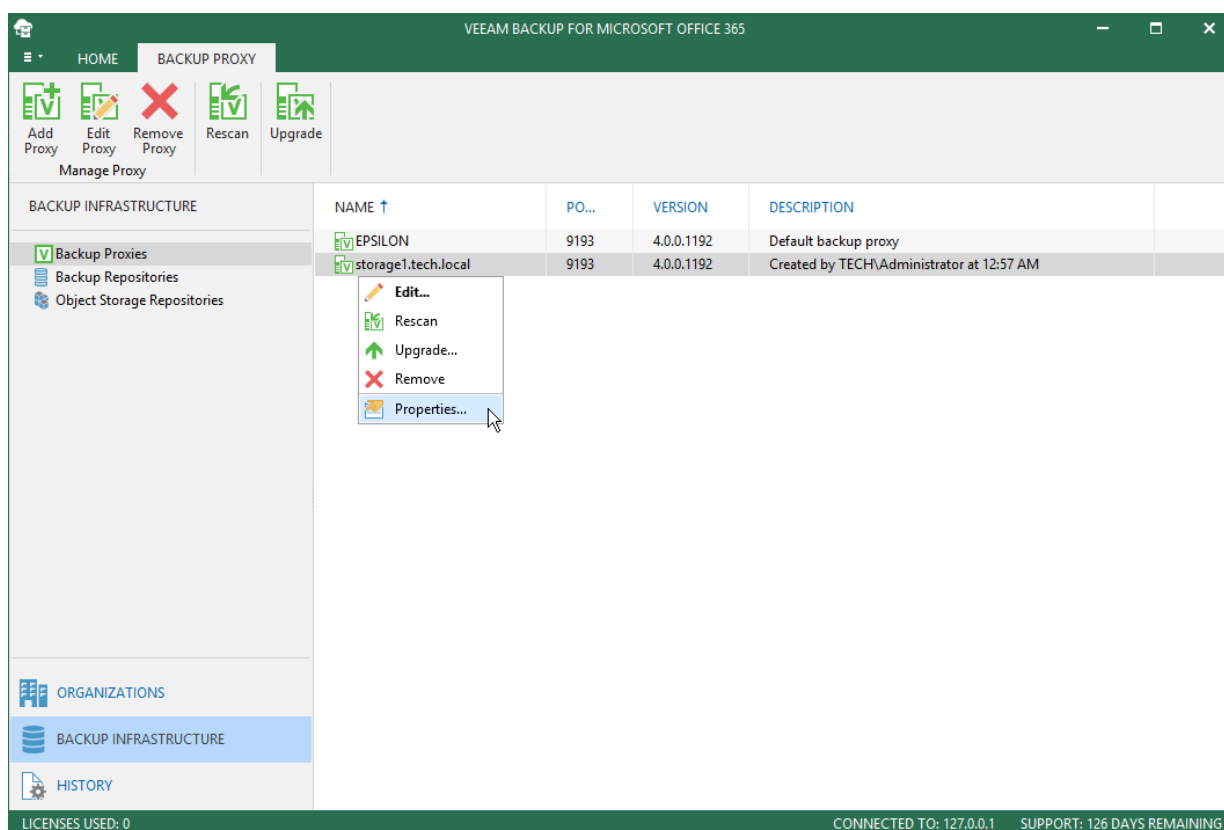
This section explains how to configure backup proxy server properties.

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** command is unavailable if a backup proxy server needs to be upgraded, as described in [Upgrading Backup Proxy Servers](#).



Configuring Threads and Network Bandwidth

Continue with this section to learn how to configure threads and how to limit download speed.

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

1. On the **General** tab:

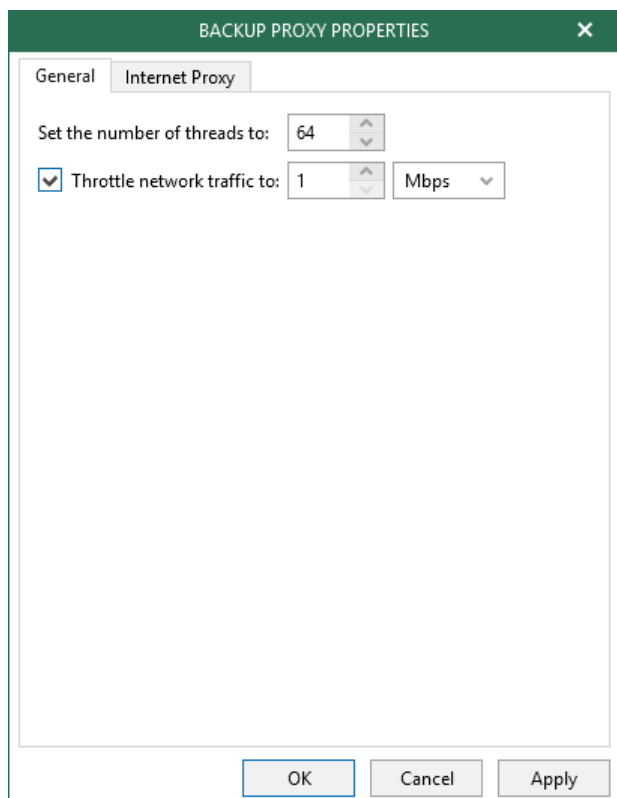
- In the **Set the number of threads to** field, specify the allowed number of threads.

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 Office 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 Office 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 Office 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** to save the settings.



Configuring Internet Proxy Server for Backup Proxies

Veeam Backup for Microsoft Office 365 lets you assign an internet proxy server to backup proxies that do not have direct access to the internet.

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

1. Go to the **Internet Proxy** tab.
2. Select an option to use:
 - **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 [Configuring Global Internet Proxy Server Settings](#).
 - **Use the following internet proxy settings.** Select this option to set up 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 via which to connect to the specified server.
 - Select the **Use authentication** check box to authenticate yourself on a server and provide authentication credentials.
3. Click **OK** to save the settings.

NOTE:

A default backup proxy server always uses the settings of the management server.

The screenshot shows a dialog box titled "BACKUP PROXY PROPERTIES" with a close button (X) in the top right corner. The "Internet Proxy" tab is selected, and the "General" tab is also visible. The "Internet Proxy" section contains three radio buttons: "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 the radio buttons, there are fields for "Host" (containing "delta.tech.local") and "Port" (containing "3128"). A checkbox labeled "Use authentication:" is checked. Below this checkbox, there are fields for "Username" (containing "Administrator") and "Password" (containing a series of dots). At the bottom of the dialog box, there are three buttons: "OK", "Cancel", and "Apply".

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

A backup repository is a storage system where you can keep backups created by your [backup jobs](#).

You can add the following types of backup repositories to the Veeam Backup for Microsoft Office 365 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 Office 365.
- Direct Attached Storage (DAS) connected to the backup proxy server.
- Storage Area Network (SAN).
A backup server must be connected to the SAN fabric via hardware, virtual HBA or software iSCSI initiator.
- Network Attached Storage (SMB 3.0 shares).
Experimental support.

Consider the following:

- Backup repositories with enabled volume deduplication are not supported.
- Storage volumes that host backup repositories must be formatted with NTFS or ReFS.
- Backups in backup repositories must not be encrypted by 3rd party encryption software as it leads to unpredictable system behavior and inevitable data loss.

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 backed up.

Each folder contains `repository.adb` — a backup file with the Office 365 organization data — along with a number of auxiliary files required to retain checkpoint information and repository configuration settings. To determine the period during which backup data must be stored in a backup repository, Veeam Backup for Microsoft Office 365 applies retention policy settings specified while adding the repository.

NOTE:

If a backup repository is [extended with object storage](#), only [cache](#) will be saved to such an extended backup repository.

Consider the following example. A Microsoft organization owns 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 will store backed-up files in a specific backup repository. When running backup job sessions, Veeam Backup for Microsoft Office 365 will add items to the backup repository in the following way:

1. During the initial backup job session, Veeam Backup for Microsoft Office 365 will collect all data from the Microsoft organization and save the data to folders in the backup repository.

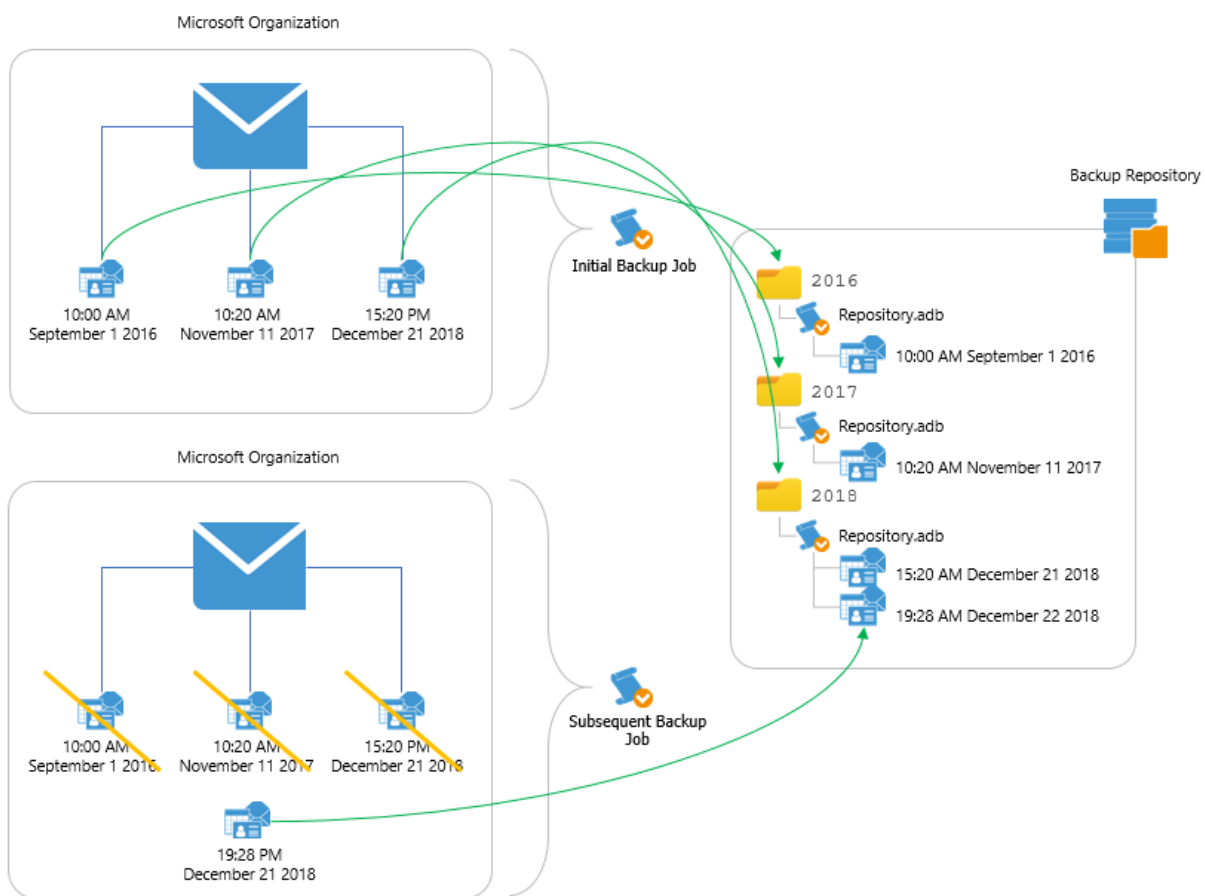
As each email item has been modified on a different date, Veeam Backup for Microsoft Office 365 will create 3 different folders in the backup repository: 2016, 2017 and 2018. Each folder will contain its own backup file `repository.adb`.

2. During subsequent backup job sessions, Veeam Backup for Microsoft Office 365 will back up only those email items that have 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 Office 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 and Microsoft OneDrive for Business items.



Retention Policy

A retention policy defines how long and under which retention type your data should be stored in a repository.

Veeam Backup for Microsoft Office 365 provides the following types of retention:

- **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**

Select this type if you want to keep an item until its latest restore point is within the retention coverage.

Item-Level Retention Type

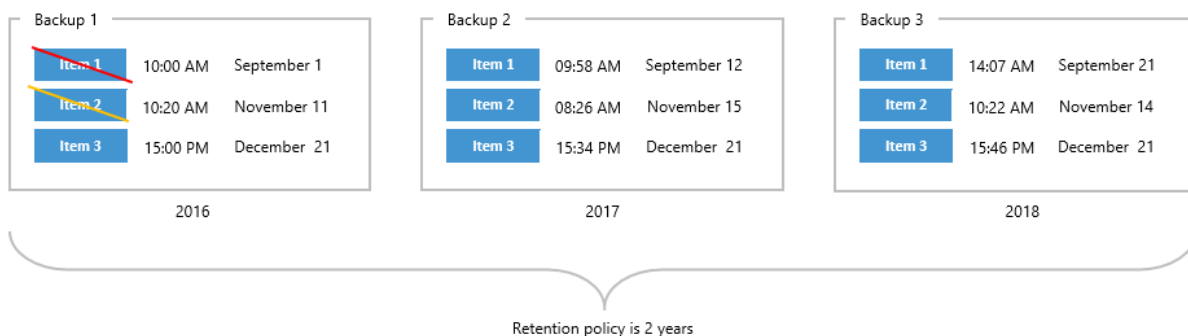
Data removal from backup repositories with the *Item-Level Retention* type occurs every time the creation time or last modification time of an item in a backup file goes beyond the retention coverage.

The following is an example that demonstrates three backup files; each file contains Microsoft Office 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, 2018. In such a scenario, Veeam Backup for Microsoft Office 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, 2016. That said, when a retention policy is being applied, for example, at 10:30 AM on November 11, 2018, Veeam Backup for Microsoft Office 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, whereupon Veeam Backup for Microsoft Office 365 completely removes such a repository from the hard drive.



Snapshot-Based Retention Type

Data removal from backup repositories with the *Snapshot-Based Retention* type occurs every time the latest restore point of an item in a backup file goes beyond the retention coverage.

Mind that each item in a backup file might have its own different version, which is also considered by the retention policy.

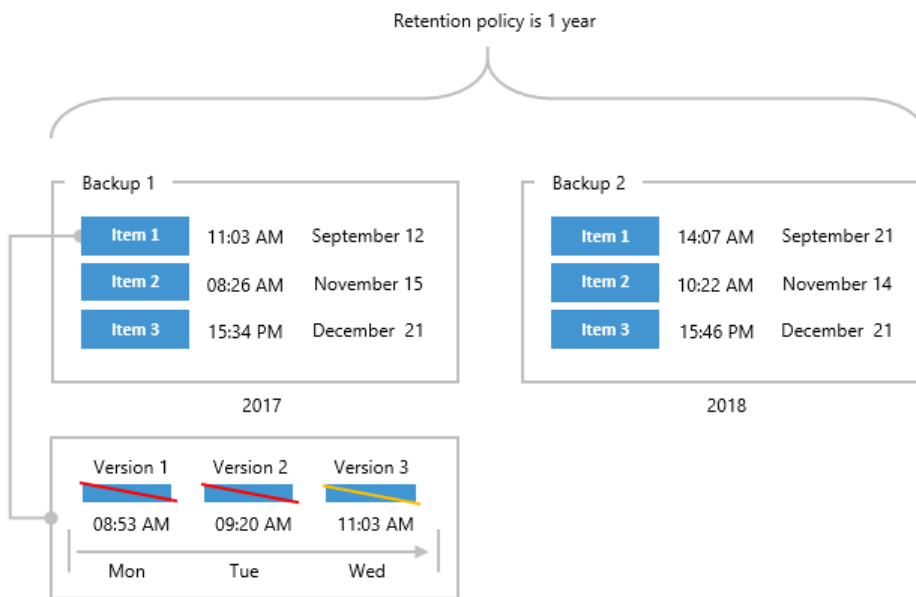
A different version means that the user could have changed any attribute in the production environment; for instance, he could have assigned a new category to an email in the mailbox. Such an action leads to a new version of an item to be created during the subsequent backup job session.

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 *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 (Mon, Tue, and Wed) and each modification was successfully backed up.

That said, there are three different versions of the same item in a backup repository.

According to the example, if the retention policy is 1 year and said to be applied at 10:00 AM on September 12, 2018, then all the item versions that exceed the specified retention threshold will be removed from the backup repository. As per example, these versions would be the *Version 1* and *Version 2*. The next version to be removed is the *Version 3*, the removal of which is about to occur right after 11:03:01 AM September 12, 2018.

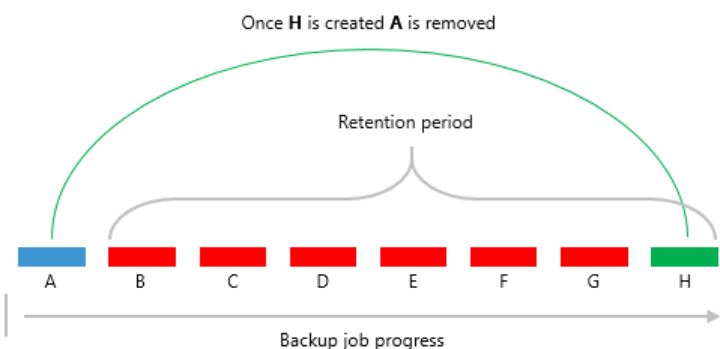
Such an approach repeats itself until no other items (or versions of items) left in a repository, whereupon Veeam Backup for Microsoft Office 365 completely removes such a repository from the hard drive.



Removing Unresolved Data

If a backup job fails to resolve organization mailboxes, SharePoint or OneDrive items, Veeam Backup for Microsoft Office 365 preserves the latest backup state until the next successful backup of such a mailbox, SharePoint or OneDrive item is created.

The following is an example that demonstrates a backup of the mailbox *A* which is followed by 6 consecutive unsuccessful attempts (*B* through *G*) of backing up that same mailbox during subsequent backup job sessions. In such a scenario, the mailbox *A* will not be removed until this mailbox is successfully backed up during the attempt *H*.

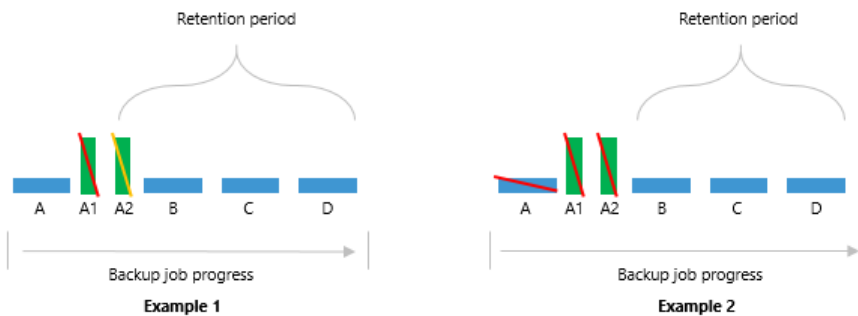


Removing Restore Points

Each version of an item can have its own 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.

Consider the following example with 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 scope, 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 scope 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*).

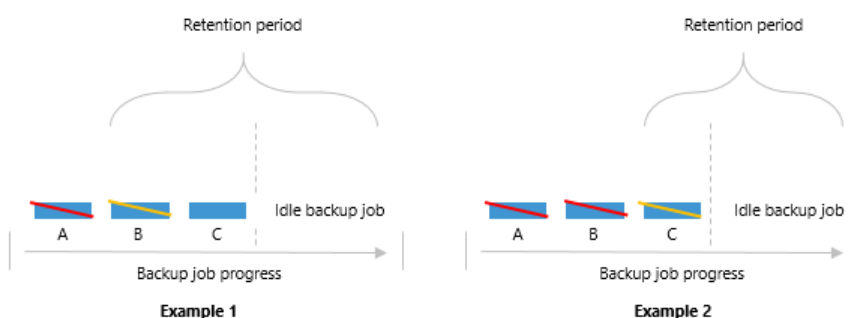


Backup Job Idleness

If a backup job has created a successful backup and then went idle for an indefinite period of time (for example, it might have become disabled), then all the data created by such a job will be removed once it is out of the retention coverage.

The following is an example in which the mailbox *A* has been removed because it was already out of the retention scope (*Example 1*), and the next mailbox to 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 and OneDrive for Business.



Direct Attached Storage (DAS)

In Veeam Backup for Microsoft Office 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 Office 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 server VM as a volume in the guest OS.

Network Attached Storage (SMB Shares)

Veeam Backup for Microsoft Office 365 lets you use network attached storage (NAS) as backup repositories. Such NAS storage can be a shared folder on your computer, or any other physical device that can be accessed via 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, make sure you are using Microsoft Windows 8 or Microsoft Windows 2012 and higher.

To access and use a shared folder, do the following:

- Configure NTFS permissions.
- Configure share permissions.

For more information, see [this Microsoft article](#).

After you share a folder, you can access it via 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>`.

NEW BACKUP REPOSITORY

Specify location for backup repository

Backup proxy:
EPSILON (Default backup proxy)

Path:
\\gamma.tech.local\share Browse...

106.9 GB free of 126.7 GB

Back Next Cancel

Adding Backup Repositories

To add a new backup repository, do the following:

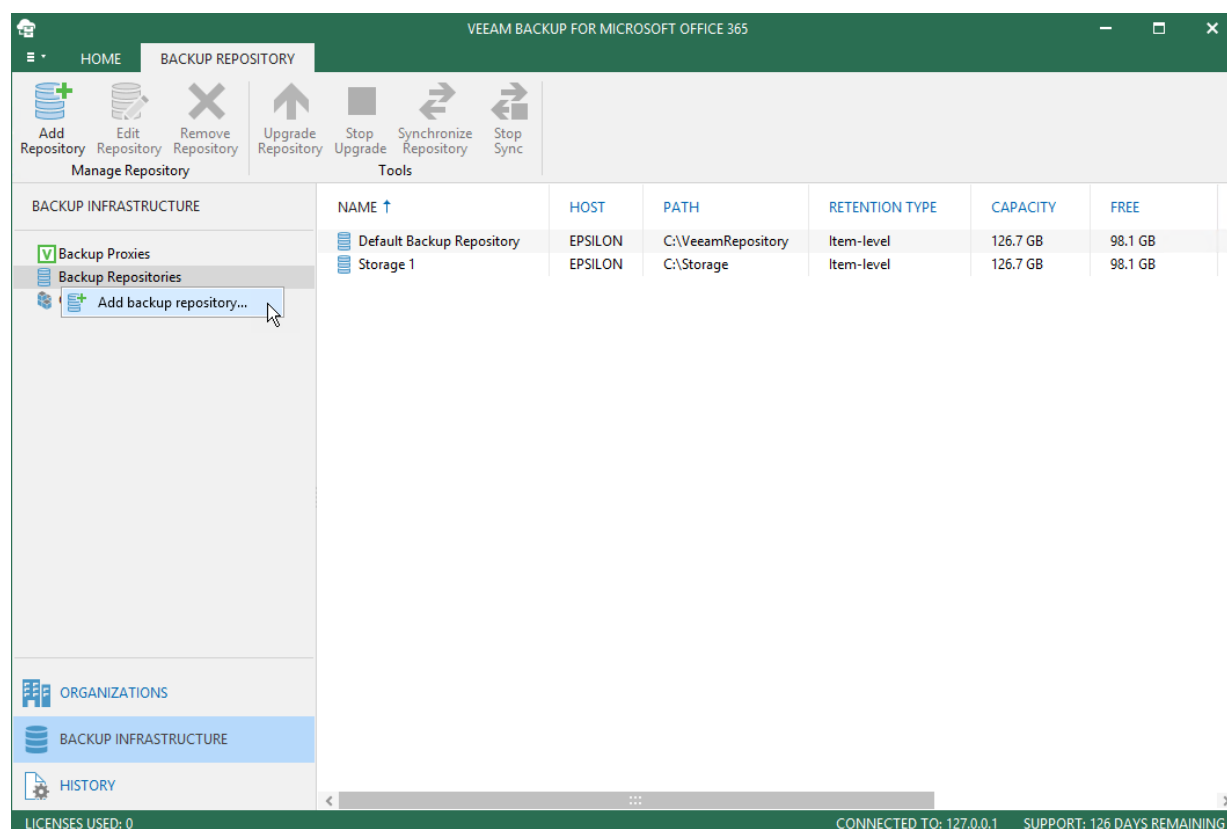
1. [Launch the New Backup Repository wizard.](#)
2. [Specify a backup repository name.](#)
3. [Specify a backup proxy server.](#)
4. [Specify an object storage repository.](#)
5. [Specify retention policy settings.](#)

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. On the **Backup Repository** tab, click **Add Repository**.

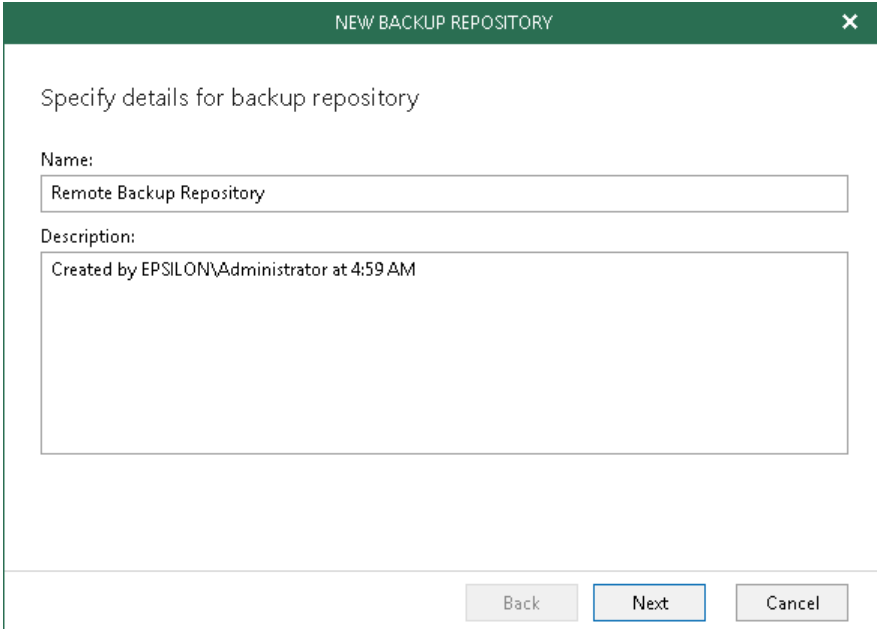
Alternatively, in the inventory pane, right-click the **Backup Repositories** node and select **Add backup repository**.



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 new name for the backup repository.
2. In the **Description** field, enter a description (optional).



NEW BACKUP REPOSITORY

Specify details for backup repository

Name:
Remote Backup Repository

Description:
Created by EPSILON\Administrator at 4:59 AM

Back Next Cancel

Step 3. 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.

To specify a backup proxy server and directory for storing backups, do the following:

1. In the **Backup proxy** drop-down list, select a backup proxy server. For more information, see [Backup Proxy Servers](#).
2. In the **Path** field, specify a directory to store your backup data. Click **Browse** to choose a directory.

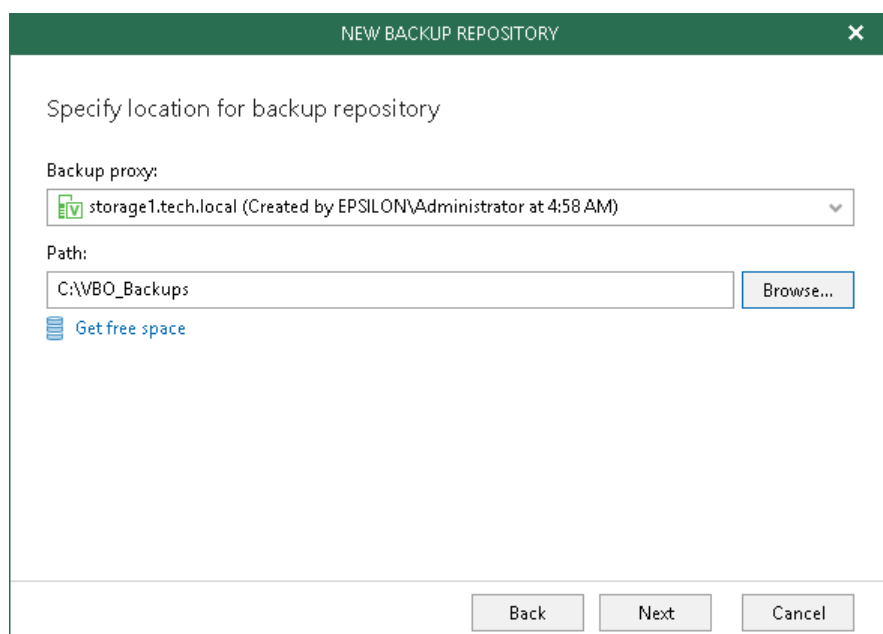
When planning to extend a backup repository with object storage, this directory will only be keeping cache consisting of required metadata, as described in [Cache](#). The actual data will be compressed and backed up directly to object storage that you specify in the next step.

When specifying a directory that already contains cache, in the next step, make sure to select the same exact object storage repository for which this cache was created.

3. Click **Get free space** if you want to know the available space on the selected backup proxy server.

NOTE:

To use a shared folder, provide the path manually. For more information about shared folders, see [Network Attached Storage \(SMB Shares\)](#).



Step 4. Specify Object Storage Repository

At this step of the wizard, you can optionally extend a backup repository with object storage to back up data directly to the cloud. For more information about object storage, see [Object Storage Repositories](#).

If you do not want to use object storage as your backup repository, skip this step and click **Next**.

Consider the following:

- You cannot extend a backup repository with object storage which 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, as described in [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. Select the **Offload backup data to object storage** check box.
2. In the drop-down list, select an object storage repository to which you want to offload your data.

Make sure that an object storage repository has been added to your environment in advance. Otherwise, click **Add** and follow the steps of the wizard, as described in [Adding Object Storage Repositories](#).

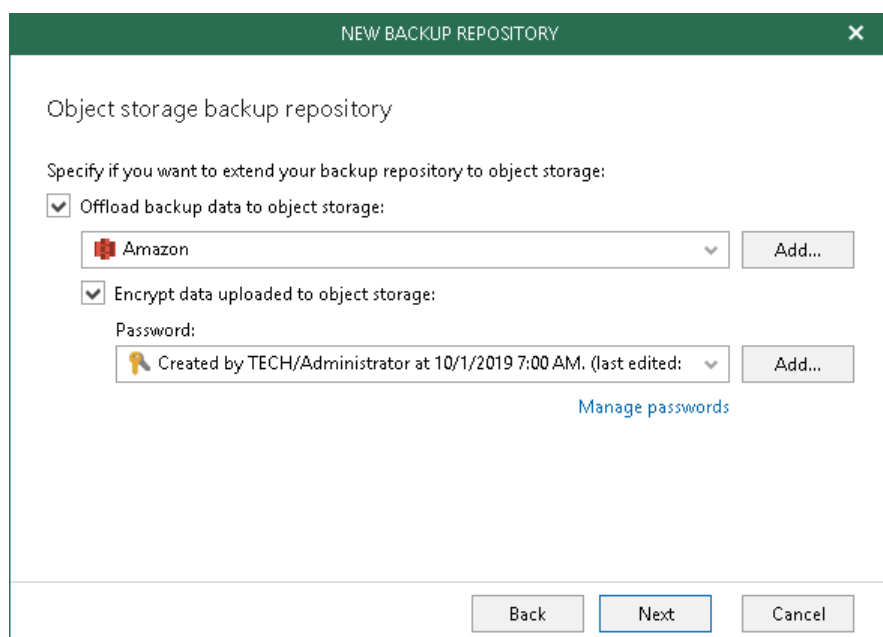
3. To offload data encrypted, select **Encrypt data uploaded to object storage** and provide a password.

If you have not created a password beforehand, click **Add** or use the [Manage passwords](#) link to specify a new password.

A password can be changed in the [Password Manager](#) 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.



Step 5. Specify Retention Policy Settings

At this step of the wizard, specify [retention policy](#) settings.

To specify retention settings, do the following:

1. In the **Retention policy** drop-down list, specify how long your data should be stored in a backup repository.
2. Choose a retention type:
 - **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.**
Select this type if you want to keep an item until its latest restore point 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 in the [previous step](#).

- A retention policy configured in this step removes outdated restore points located in object storage repositories.

The screenshot shows a dialog box titled "NEW BACKUP REPOSITORY" with a close button (X) in the top right corner. The main heading inside is "Specify retention policy settings". Below this, there is a label "Retention policy:" followed by a dropdown menu currently showing "3 years". There are two radio button options: "Item-level retention" (which is selected) and "Snapshot-based retention". Each option has a descriptive paragraph below it. At the bottom left, there is a text prompt "Click Advanced to customize how often the retention policy should be applied" and an "Advanced" button. At the very bottom, there are three buttons: "Back", "Finish", and "Cancel".

Editing Backup Repository Settings

Veeam Backup for Microsoft Office 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 Office 365 backup infrastructure.

For more information on how to extend a backup repository with object storage, see [Specify Object Storage Repository](#).

- 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.

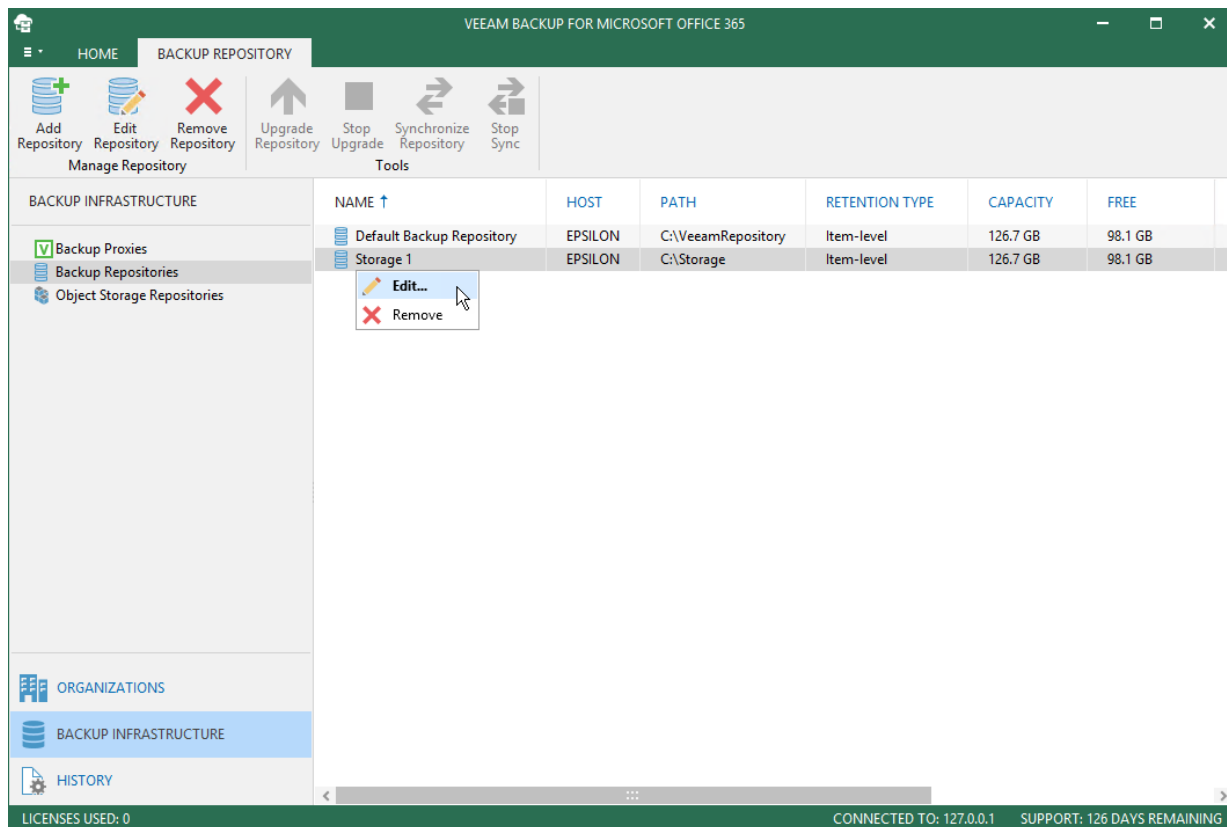
For more information about retention policies, see [Retention Policy](#).

- The **Edit** command is unavailable if a backup repository is out of date.

For more 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 the **Backup Repositories** node.
3. In the preview pane, select a backup repository.
4. On the **Backup Repository** tab, click **Edit Repository** on the ribbon.
Alternatively, in the preview pane, right-click a backup repository and select **Edit**.
5. Modify settings as required.



Removing Backup Repositories

Veeam Backup for Microsoft Office 365 allows you to remove backup repositories from the backup infrastructure if you no longer need them.

Consider the following:

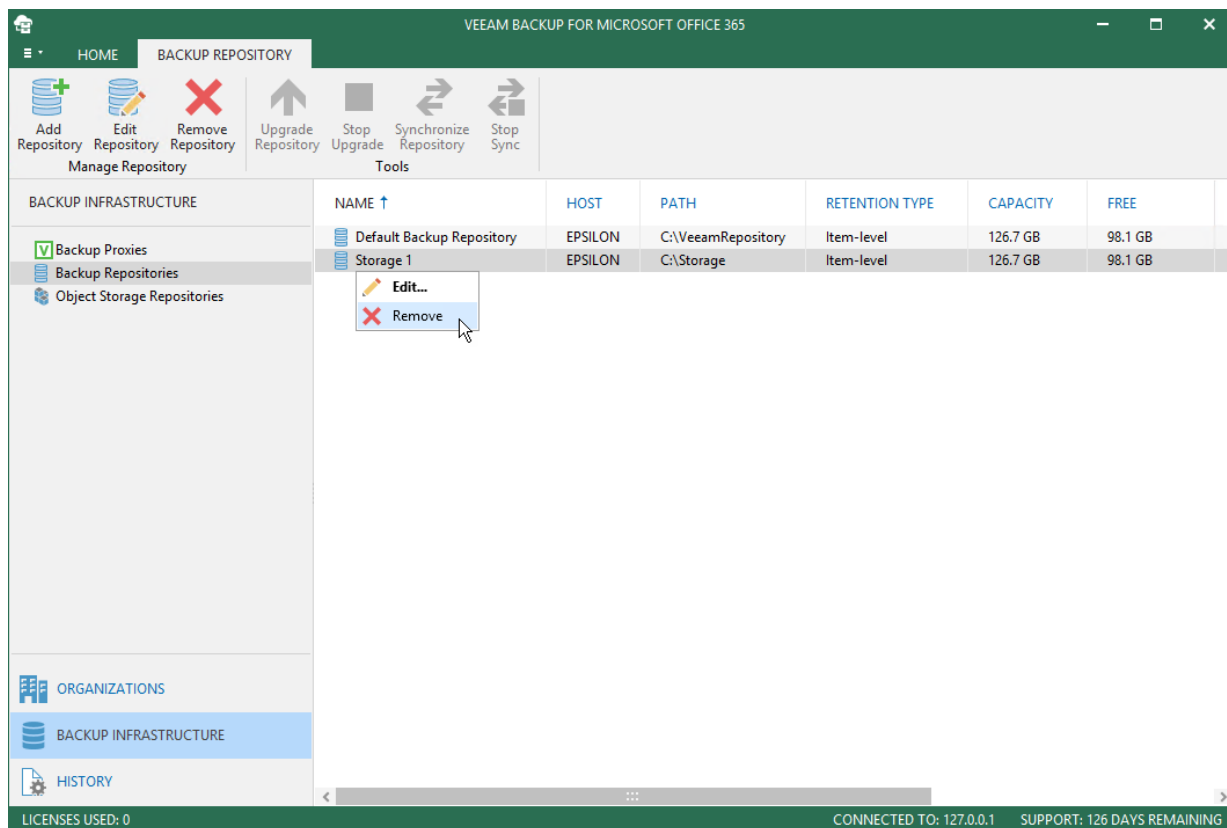
- When removing a backup repository, backup files that reside in such a repository will not be removed.
- The last remaining backup repository cannot be removed.
- When removing an extended backup repository that was synchronized, as described in [Synchronizing Repositories](#), the backup data located in associated object storage becomes unavailable.
- The backup repository that is in use by backup jobs cannot be removed

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:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Backup Repositories** node.
3. In the preview pane, select a backup repository.
4. On the **Backup Repository** tab, click **Remove Repository** on the ribbon.

Alternatively, in the preview pane, right-click a backup repository and select **Remove**.



Upgrading Backup Repositories

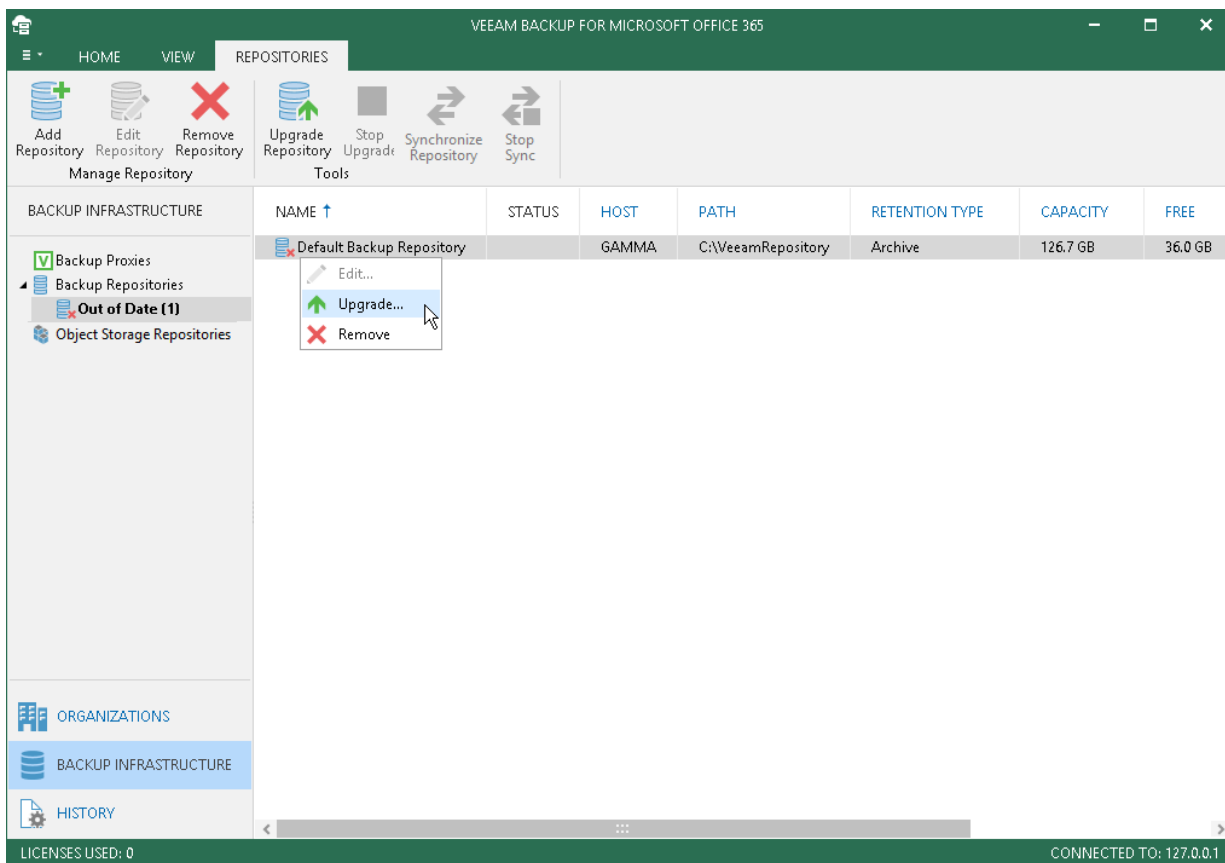
When you upgrade Veeam Backup for Microsoft Office 365 to a newer version, all backup repositories configured in your environment are marked as *Out of Date* and have to be upgraded manually.

To upgrade backup repositories, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Backup Repositories > Out of Date** node.
3. In the preview pane, select a backup repository.
4. On the **Backup Repository** tab, click **Upgrade Repository** on the ribbon.

Alternatively, in the preview pane, right-click a backup repository and select **Upgrade**.

To cancel an 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, as described in [Exploring Single Organization](#) and [Exploring All Organizations](#).
- Create new backups and offload these backups to object storage, as described in [Data Backup](#).

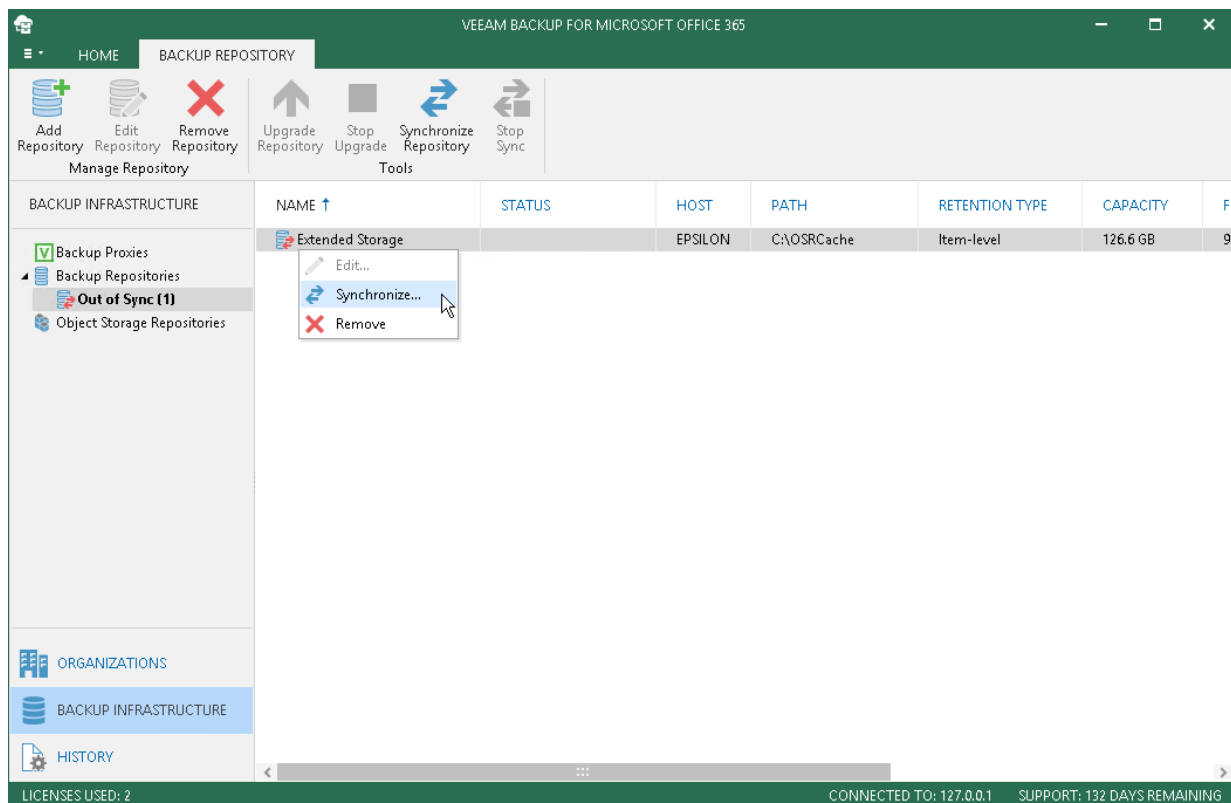
To synchronize cache between object storage and extended backup repositories, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Backup Repositories > Out of Sync** node.
3. In the preview pane, select a backup repository.
4. On the **Backup Repository** tab, click **Synchronize Repository** on the ribbon.

Alternatively, in the preview pane, right-click a backup repository and select **Synchronize**.

During synchronization, Veeam Backup for Microsoft Office 365 downloads metadata (cache) from object storage to the selected backup repository. For more information about cache, see [Cache](#).

To stop synchronization, click **Stop Sync** on the ribbon.



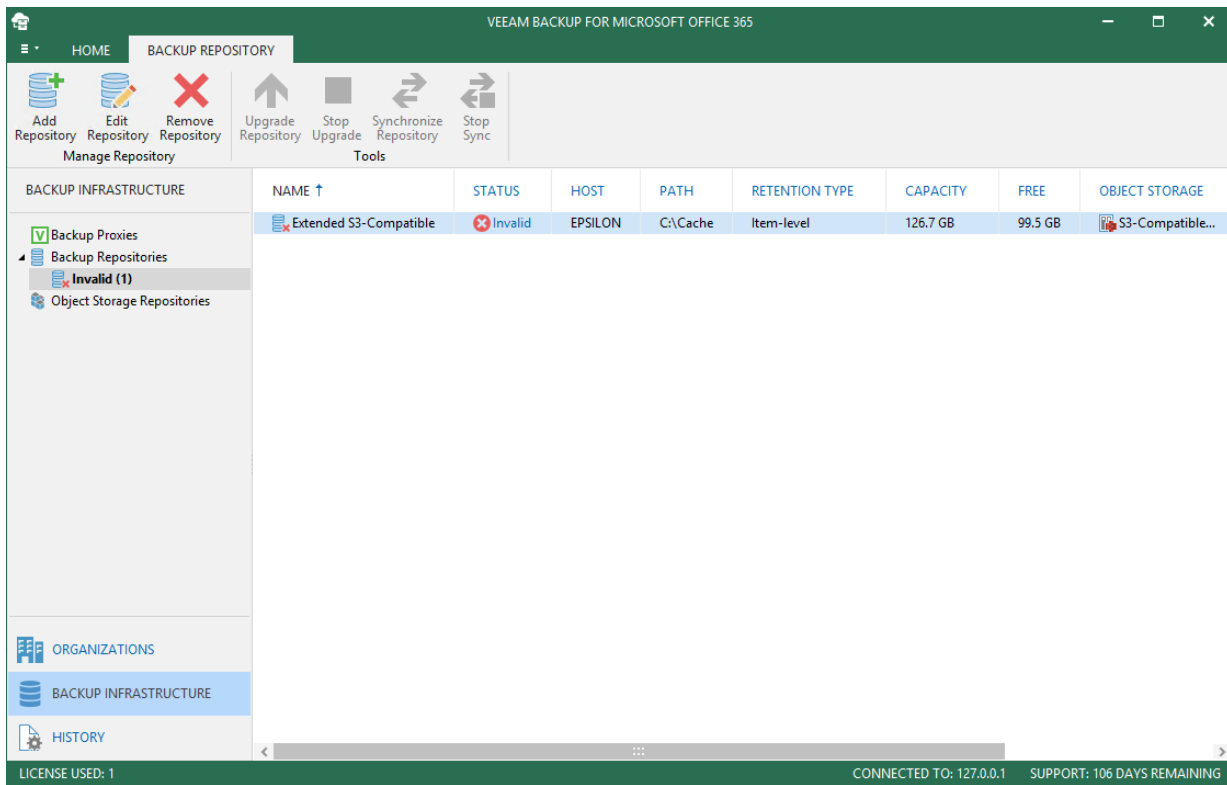
Invalid State

In Veeam Backup for Microsoft Office 365, a backup repository can be put into an *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, as described in [Object Storage Repository 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.
- If the connection to DAS or NFS is missing.
Such an invalid backup repository becomes available after your DAS or NFS storage is online.

Once a repository is put into an *Invalid* state, restore or backup from/to such a repository is not possible.

Invalid backup repositories can be found in the **Backup Infrastructure** view under the **Backup Repositories > Invalid** node.



Object Storage Repositories

Object storage repositories are used to store Microsoft Office 365 and on-premises Microsoft organization backups using the following cloud and on-premises services:

- S3 Compatible object storage

S3 Compatible storage is any device that conforms to the Amazon S3 protocol.

- Amazon S3 object storage

For more information about Amazon S3 object storage, see [this Amazon article](#).

- Microsoft Azure Blob storage

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

- IBM Cloud Object Storage

For more information about IBM cloud object storage, see [this IBM article](#).

To back up data to object storage, you can simply extend a backup repository with any of the storage listed above, as described in [Specify Object Storage Repository](#), and map a backup job to such an extended repository, as described in [Specify Backup Proxy and Repository](#).

Object Storage Repository Structure

The following structure is created and maintained by Veeam Backup for Microsoft Office 365 in 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 Office 365 does not support creating new buckets or containers.</p>
<bucket_name/container_name>/Veeam/Backup365/	<p>A set of mandatory folders created by Veeam Backup for Microsoft Office 365.</p>
<repository_folder_name>	<p>A repository folder that you create when adding a new object storage repository.</p> <p>For more information on how to add a new object storage repository, see Adding Object Storage Repositories.</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. 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 and so on. ▪ <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 might have set during extension of a backup repository with object storage.
<repository_folder_name>/Encryption	<p>Contains a <i>BackupKeys</i> blob file that holds information about the encryption keys that you might have 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 Repository.</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 <organization_Id> 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.
<organization_Id>/Mailboxes/<mailbox_Id>	<p>The <i>Mailboxes</i> directory contains backed-up 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>Folders</i>. Contains backed-up Exchange folders such as <i>Inbox</i>, <i>Drafts</i>, <i>Sent Items</i>, and so on. ▪ <i>FoldersHistory</i>. Contains folder changes. For example, you may have renamed a folder. In such a scenario, after the subsequent backup session, Veeam Backup for Microsoft Office 365 will update information about the renamed folders and save each new folder version to the <i>FoldersHistory</i> directory. ▪ <i>ItemsChanges</i>. Contains incremental backup data. ▪ <i>ItemsData</i>. Contains blob data of the backed-up Exchange messages. For example, attachments are saved to this folder. ▪ <i>ItemsPreview</i>. Contains required data to load the backup contents into the Veeam Explorer for Microsoft Exchange scope.

<organization_Id>/Sites	Contains a blob file with a list of backed-up SharePoint sites.
<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	Contains backup dates of SharePoint sites. Required for a snapshot-based retention policy.
<organization_Id>/Webs/<web_Id>	A set of folders that contain backed-up SharePoint sites and OneDrive Items. The <web_Id> directory contains the following directories: <ul style="list-style-type: none"> ▪ <i>Files</i>. Contains files of your 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>ListViews</i>. Contains SharePoint list views.
<repository_folder_name>/RepositoryLock	Contains a lock file that tells that this storage is already an extension to a backup repository. Object storage can only be owned by one owner (a backup repository) at a time. For more information on how to extend a backup repository with object storage, see Specify Object Storage Repository .

Cache

Cache helps you reduce cost expensive operations incurred by your cloud storage provider when reading or writing data to/from object storage repositories.

For example, when you use Veeam Explorers to open backups located in object storage, Veeam Backup for Microsoft Office 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 though 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 the object storage repository.

Replication gives Veeam Backup for Microsoft Office 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 Repository](#).

- 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 in the [Specify Backup Proxy Server](#) step.

Compression

Compression in Veeam Backup for Microsoft Office 365 helps you save storage space and reduce costs incurred by your cloud storage provider for maintaining backup data.

Compression works as follows:

- 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 Office 365 uses the *Gzip* algorithm. For more information about this algorithm, see [this Gzip article](#).

- Compression is done by the backup proxy server that you specify in the [Specify Backup Proxy Server](#) step.
- Certain types of data such as images or other media files cannot be compressed properly, thereby making an output compressed blob file larger than it would have been had it not been compressed at all. In such a scenario, the uncompressed version of the file will be saved.

Object Storage Retention

Obsolete restore points are removed from object storage automatically by Veeam Backup for Microsoft Office 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 Office 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.

Adding Object Storage Repositories

This section explains how to add the following types of object storage repositories to the Veeam Backup for Microsoft Office 365 backup infrastructure:

- [S3 Compatible Object Storage Repositories](#)
- [Amazon S3 Object Storage Repositories](#)
- [Microsoft Azure Blob Storage Repositories](#)
- [IBM Cloud Object Storage Repositories](#)

Adding S3 Compatible Object Storage Repositories

To add a new S3 Compatible object storage repository to the Veeam Backup for Microsoft Office 365 backup infrastructure, do the following:

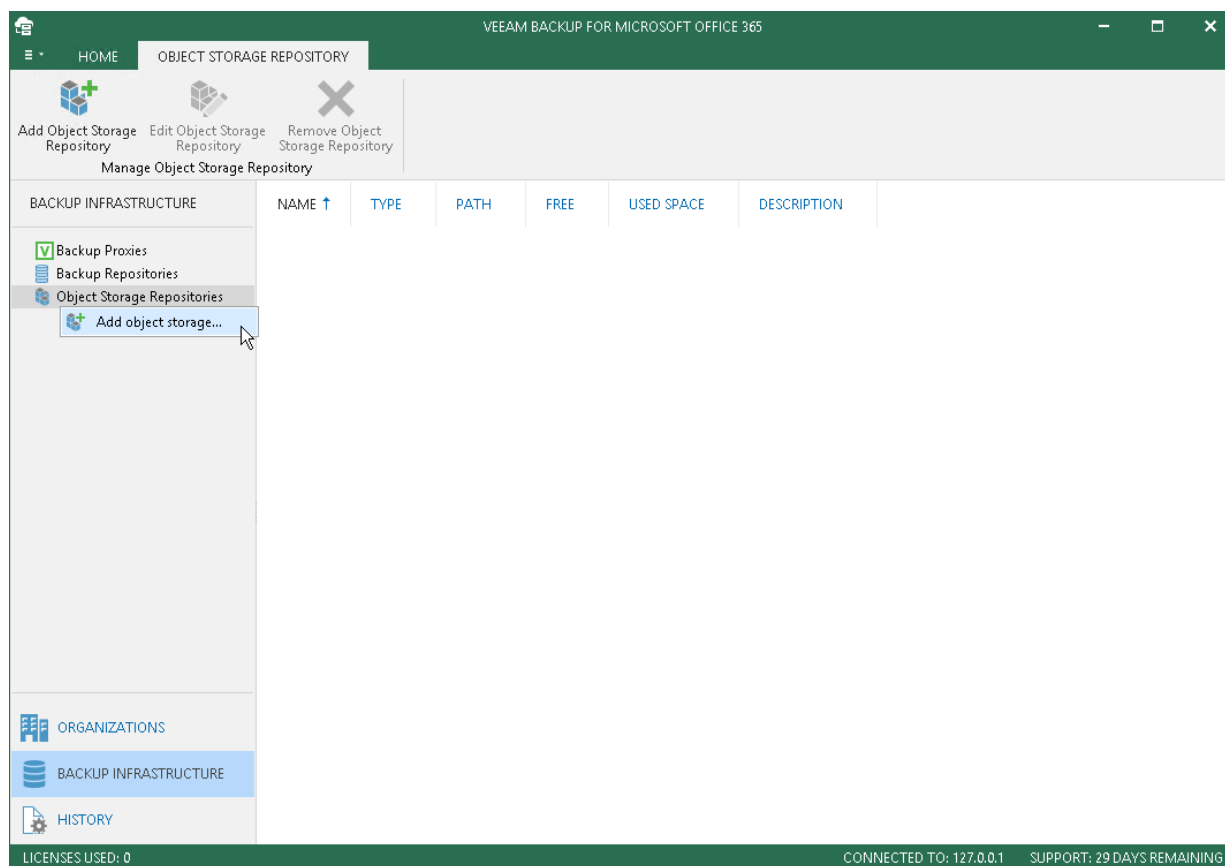
1. [Launch the New Object Storage Repository wizard.](#)
2. [Specify an object storage repository name.](#)
3. [Select an object storage type.](#)
4. [Specify an object storage service point and account.](#)
5. [Specify an object storage bucket.](#)

Step 1. Launch New Object Storage Repository Wizard

To launch the **New Object Storage Repository** wizard, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Object Storage Repositories** node.
3. On the **Object Storage Repository** tab, click **Add Object Storage Repository**.

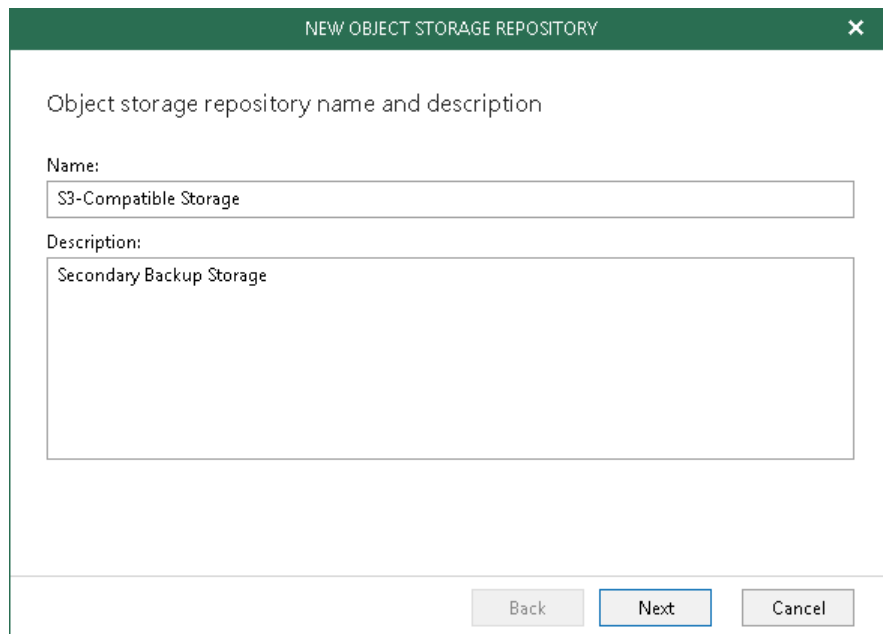
Alternatively, in the inventory pane, right-click the **Object Storage Repositories** node and select **Add object storage**.



Step 2. Specify Object Storage Repository Name

At this step of the wizard, enter a name for the object storage repository and provide optional description:

1. In the **Name** field, specify a new name for the object storage repository.
2. In the **Description** field, enter a description (optional).



NEW OBJECT STORAGE REPOSITORY

Object storage repository name and description

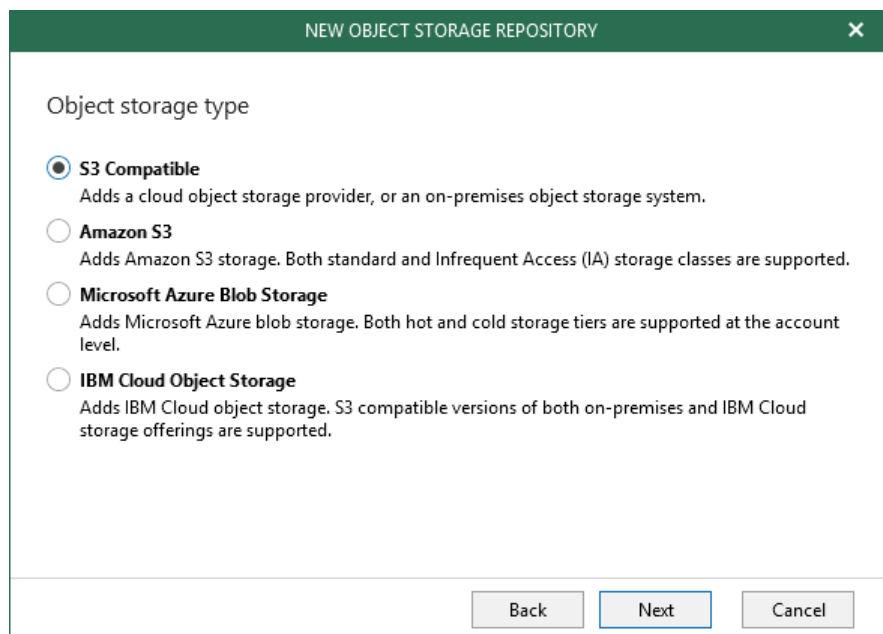
Name:
S3-Compatible Storage

Description:
Secondary Backup Storage

Back Next Cancel

Step 3. Select Object Storage Type

At this step of the wizard, select **S3 Compatible**.



NEW OBJECT STORAGE REPOSITORY

Object storage type

☒ **S3 Compatible**
Adds a cloud object storage provider, or an on-premises object storage system.

☐ **Amazon S3**
Adds Amazon S3 storage. Both standard and Infrequent Access (IA) storage classes are supported.

☐ **Microsoft Azure Blob Storage**
Adds Microsoft Azure blob storage. Both hot and cold storage tiers are supported at the account level.

☐ **IBM Cloud Object Storage**
Adds IBM Cloud object storage. S3 compatible versions of both on-premises and IBM Cloud storage offerings are supported.

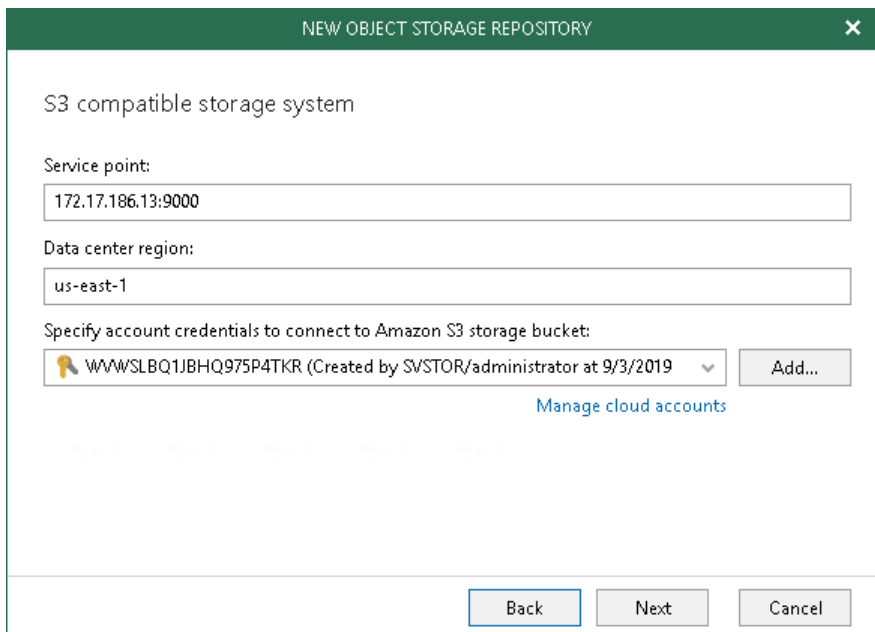
Back Next Cancel

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 data center 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. In the **Specify account credentials to connect to Amazon S3 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 in the drop-down list. Otherwise, click **Add** and provide your access and secret keys, as described in [Adding S3-Compatible Access Key](#). You can also click **Manage cloud accounts** to manage existing credentials records.



Step 5. Specify Object Storage Bucket

At this step of the wizard, specify an object storage bucket and folder where you want to keep your backup data.

1. In 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 Office 365 does not support creating new buckets.

2. In the **Folder** field, select a folder to which you want to map your object storage repository, and which will be used to store backups.

To select a folder, click **Browse** and either select an existing folder or create a new one by clicking **New Folder**.

For more information about how data is stored, see [Object Storage Repository Structure](#).

3. Click **Advanced** if you want to configure storage consumption limitations.

Veeam Backup for Microsoft Office 365 will display the **Advanced Settings** window.

NEW OBJECT STORAGE REPOSITORY

S3 compatible storage system bucket

Bucket:
bucket1

Folder:
S3 Storage Browse...

Click Advanced to customize object storage consumption Advanced

Back Finish Cancel

4. In the **Advanced Settings** window, do the following:
 - a. Select the **Limit object storage consumption to** check box if you want to allow Veeam Backup for Microsoft Office 365 to exceed the storage limit.
 - b. Set the limit.
 - c. Click **OK**.

ADVANCED SETTINGS

☒ Limit object storage consumption to: 1024 GB

This is a soft limit to help control your storage spend. If the specified limit is exceeded, the already running backup job will be allowed to complete, but no new jobs will start.

OK Cancel

Adding Amazon S3 Object Storage Repositories

To add a new Amazon S3 object storage repository to the Veeam Backup for Microsoft Office 365 backup infrastructure, do the following:

1. [Launch the New Object Storage Repository wizard.](#)
2. [Specify an object storage repository name.](#)
3. [Select an object storage type.](#)

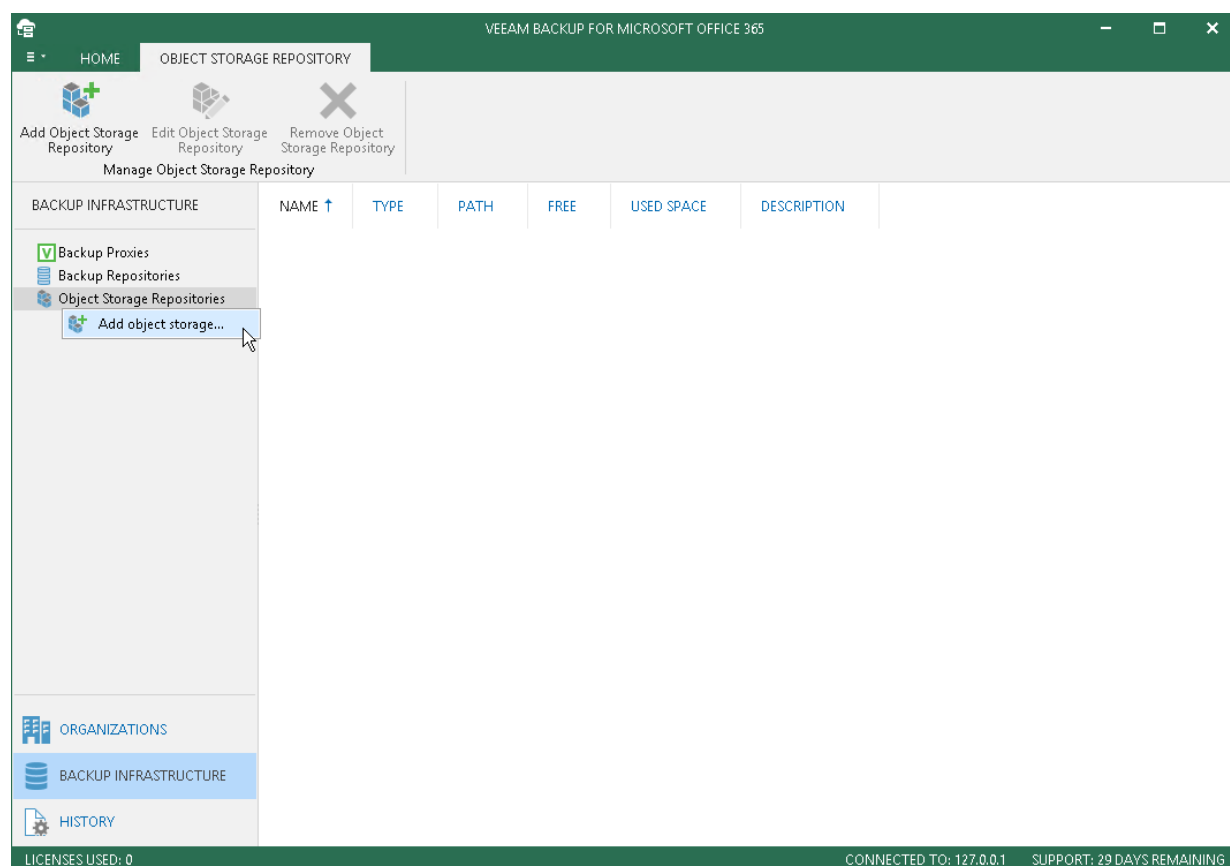
4. [Specify an object storage account.](#)
5. [Specify object storage settings.](#)

Step 1. Launch New Object Storage Repository Wizard

To launch the **New Object Storage Repository** wizard, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Object Storage Repositories** node.
3. On the **Object Storage Repository** tab, click **Add Object Storage Repository**.

Alternatively, in the inventory pane, right-click the **Object Storage Repositories** node and select **Add object storage**.



Step 2. Specify Object Storage Repository Name

At this step of the wizard, enter a name for the object storage repository and provide optional description:

1. In the **Name** field, specify a new name for the object storage repository.
2. In the **Description** field, enter a description (optional).

NEW OBJECT STORAGE REPOSITORY

Specify details for object storage repository

Name:
Amazon Object Storage

Description:
Secondary Backup Storage

Back Next Cancel

Step 3. Select Object Storage Type

At this step of the wizard, select **Amazon S3**.

NEW OBJECT STORAGE REPOSITORY

Object storage type

☐ **S3 Compatible**
Adds a cloud object storage provider, or an on-premises object storage system.

☒ **Amazon S3**
Adds Amazon S3 storage. Both standard and Infrequent Access (IA) storage classes are supported.

☐ **Microsoft Azure Blob Storage**
Adds Microsoft Azure blob storage. Both hot and cold storage tiers are supported at the account level.

☐ **IBM Cloud Object Storage**
Adds IBM Cloud object storage. S3 compatible versions of both on-premises and IBM Cloud storage offerings are supported.

Back Next Cancel

Step 4. Specify Object Storage Account

At this step of the wizard, specify an Amazon account and select a data center region.

1. In 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 in the drop-down list. Otherwise, click **Add** and provide your access and secret keys, as described in [Adding S3-Compatible Access Key](#). You can also click **Manage cloud accounts** to manage existing credentials records.
2. In the **Data center region** drop-down list, select a data center region.

Step 5. 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 keep backup data.

1. In the **Data center location** drop-down list, select a region that contains available buckets.
2. In 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 Office 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 repository, and which will be used to store backups.
To select a folder, click **Browse** and either select an existing folder or create a new one by clicking **New Folder**.
For more information about how data is stored, see [Object Storage Repository Structure](#).
3. Click **Advanced** if you want to configure storage consumption limitations.
Veeam Backup for Microsoft Office 365 will display the **Advanced Settings** window.

NEW OBJECT STORAGE REPOSITORY

Amazon S3 bucket

Data center location:
US East (Ohio)

Bucket:
veeam-bw

Folder:
Object Storage Directory Browse...

Click Advanced to customize object storage consumption Advanced

Back Finish Cancel

4. In the **Advanced Settings** window, do the following:

- Select the **Limit object storage consumption to** check box if you want to allow Veeam Backup for Microsoft Office 365 to exceed the storage limit.
- Set the limit.
- 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 Standard IA (Standard Infrequent Access). For more information about infrequent access, see [this Amazon article](#).
- Click **OK**.

ADVANCED SETTINGS

☒ Limit object storage consumption to: 1024 GB

This is a soft limit to help control your storage spend. If the specified limit is exceeded, the already running backup job will be allowed to complete, but no new jobs will start.

☒ Use infrequent access storage class (may result in additional costs)

Provides lower price per GB at the cost of higher retrieval and early deletion fees, and so is best suited for storing older backups which you are unlikely to have to restore from.

OK Cancel

Adding Microsoft Azure Blob Storage Repositories

To add a new Microsoft Azure blob storage repository to the Veeam Backup for Microsoft Office 365 backup infrastructure, do the following:

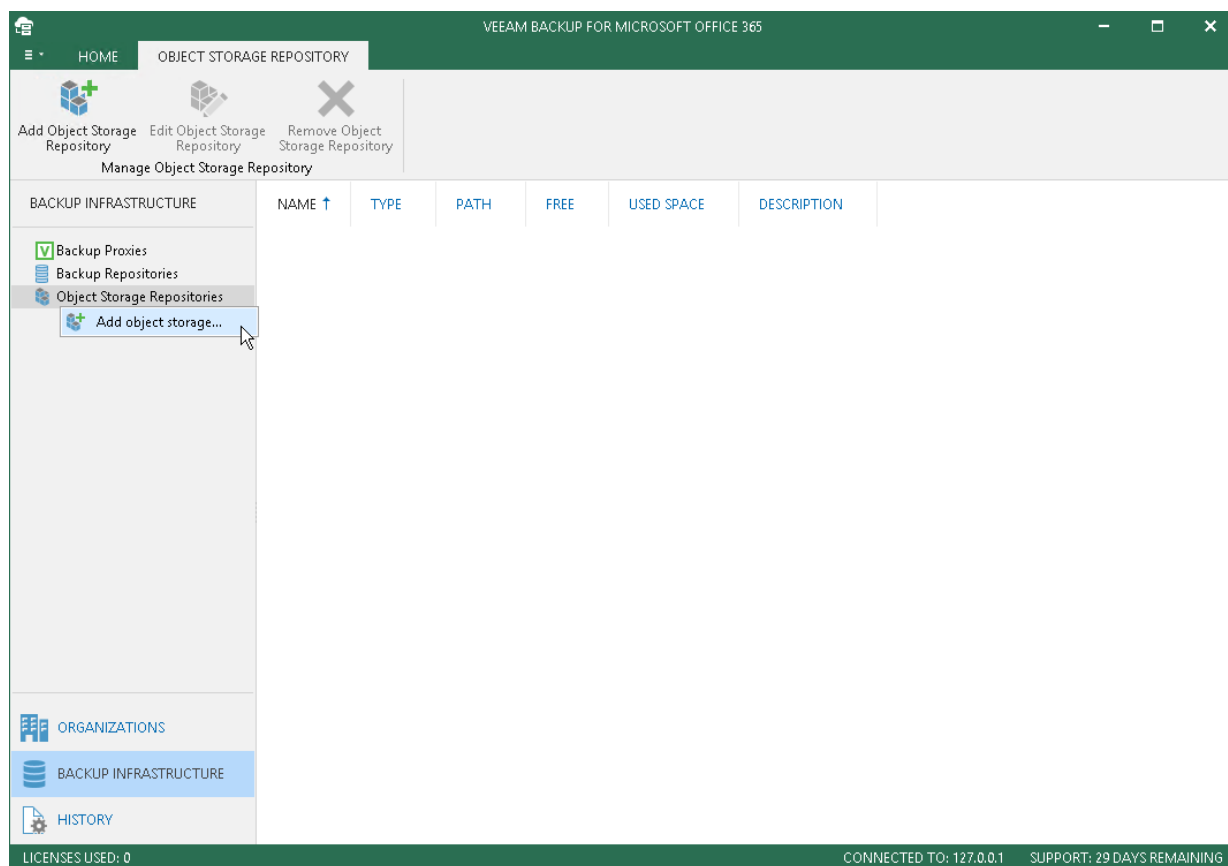
1. [Launch the New Object Storage Repository wizard.](#)
2. [Specify an object storage repository name.](#)
3. [Select an object storage type.](#)
4. [Specify an object storage account.](#)
5. [Specify object storage settings.](#)

Step 1. Launch New Object Storage Repository Wizard

To launch the **New Object Storage Repository** wizard, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Object Storage Repositories** node.
3. On the **Object Storage Repository** tab, click **Add Object Storage Repository**.

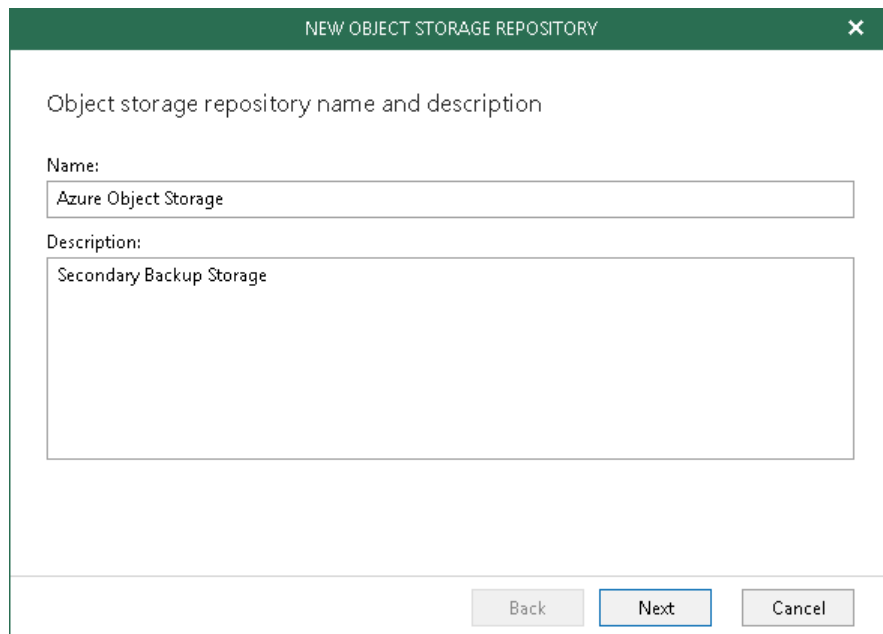
Alternatively, in the inventory pane, right-click the **Object Storage Repositories** node and select **Add object storage**.



Step 2. Specify Object Storage Repository Name

At this step of the wizard, enter a name for the object storage repository and provide optional description:

1. In the **Name** field, specify a new name for the object storage repository.
2. In the **Description** field, enter a description (optional).



NEW OBJECT STORAGE REPOSITORY

Object storage repository name and description

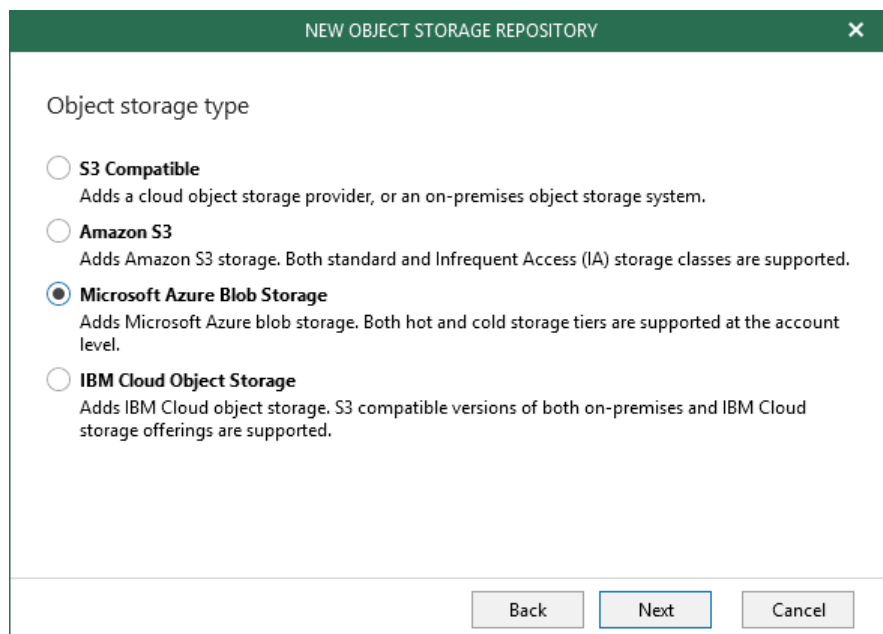
Name:
Azure Object Storage

Description:
Secondary Backup Storage

Back Next Cancel

Step 3. Select Object Storage Type

At this step of the wizard, select **Microsoft Azure Blob Storage**.



NEW OBJECT STORAGE REPOSITORY

Object storage type

☐ **S3 Compatible**
Adds a cloud object storage provider, or an on-premises object storage system.

☐ **Amazon S3**
Adds Amazon S3 storage. Both standard and Infrequent Access (IA) storage classes are supported.

☒ **Microsoft Azure Blob Storage**
Adds Microsoft Azure blob storage. Both hot and cold storage tiers are supported at the account level.

☐ **IBM Cloud Object Storage**
Adds IBM Cloud object storage. S3 compatible versions of both on-premises and IBM Cloud storage offerings are supported.

Back Next Cancel

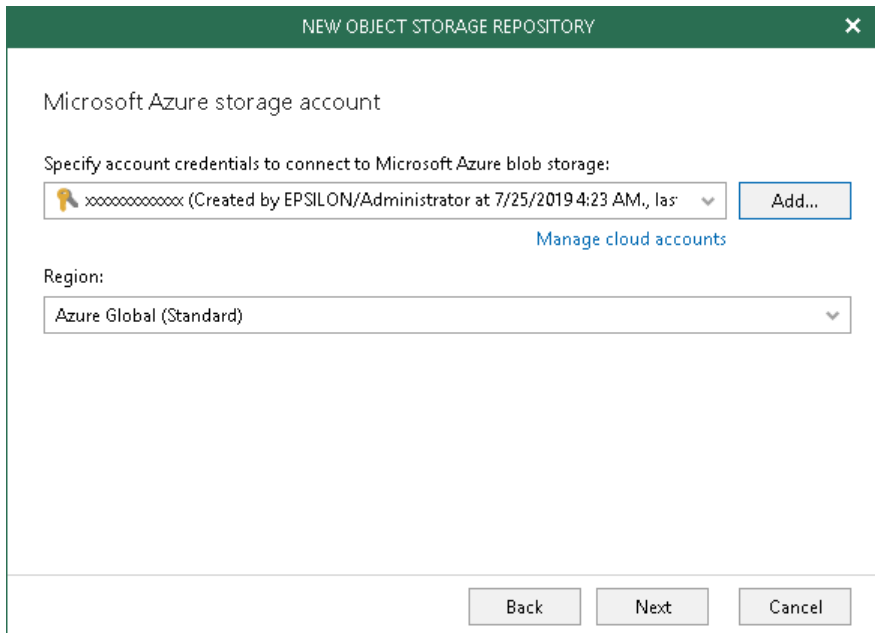
Step 4. Specify Object Storage Account

At this step of the wizard, specify a Microsoft Azure account and select a region.

1. In 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 in the drop-down list. Otherwise, click **Add** and provide your account and a shared key, as described in [Adding Microsoft Azure Storage Account](#). You can also click **Manage cloud accounts** to manage existing credentials records.

2. In the **Region** drop-down list, select a region.



Step 5. Specify Object Storage Settings

At this step of the wizard, specify an object storage container and folder where you want to keep your backup data.

1. In 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 Office 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 repository, 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 about how data is stored, see [Object Storage Repository Structure](#).

3. Click **Advanced** if you want to configure storage consumption limitations.

Veeam Backup for Microsoft Office 365 will display the **Advanced Settings** window.

NEW OBJECT STORAGE REPOSITORY

Microsoft Azure blob container

Container:
container1

Folder:
Azure Storage Browse...

Click Advanced to customize object storage consumption Advanced

Back Finish Cancel

4. In the **Advanced Settings** window, do the following:
 - a. Select the **Limit object storage consumption to** check box if you want to allow Veeam Backup for Microsoft Office 365 to exceed the storage limit.
 - b. Set the limit.
 - c. Click **OK**.

ADVANCED SETTINGS

☒ Limit object storage consumption to: 1024 GB

This is a soft limit to help control your storage spend. If the specified limit is exceeded, the already running backup job will be allowed to complete, but no new jobs will start.

OK Cancel

Adding IBM Cloud Object Storage Repositories

To add a new IBM cloud object storage repository to the Veeam Backup for Microsoft Office 365 backup infrastructure, do the following:

1. [Launch the New Object Storage Repository wizard.](#)
2. [Specify an object storage repository name.](#)
3. [Select an object storage type.](#)

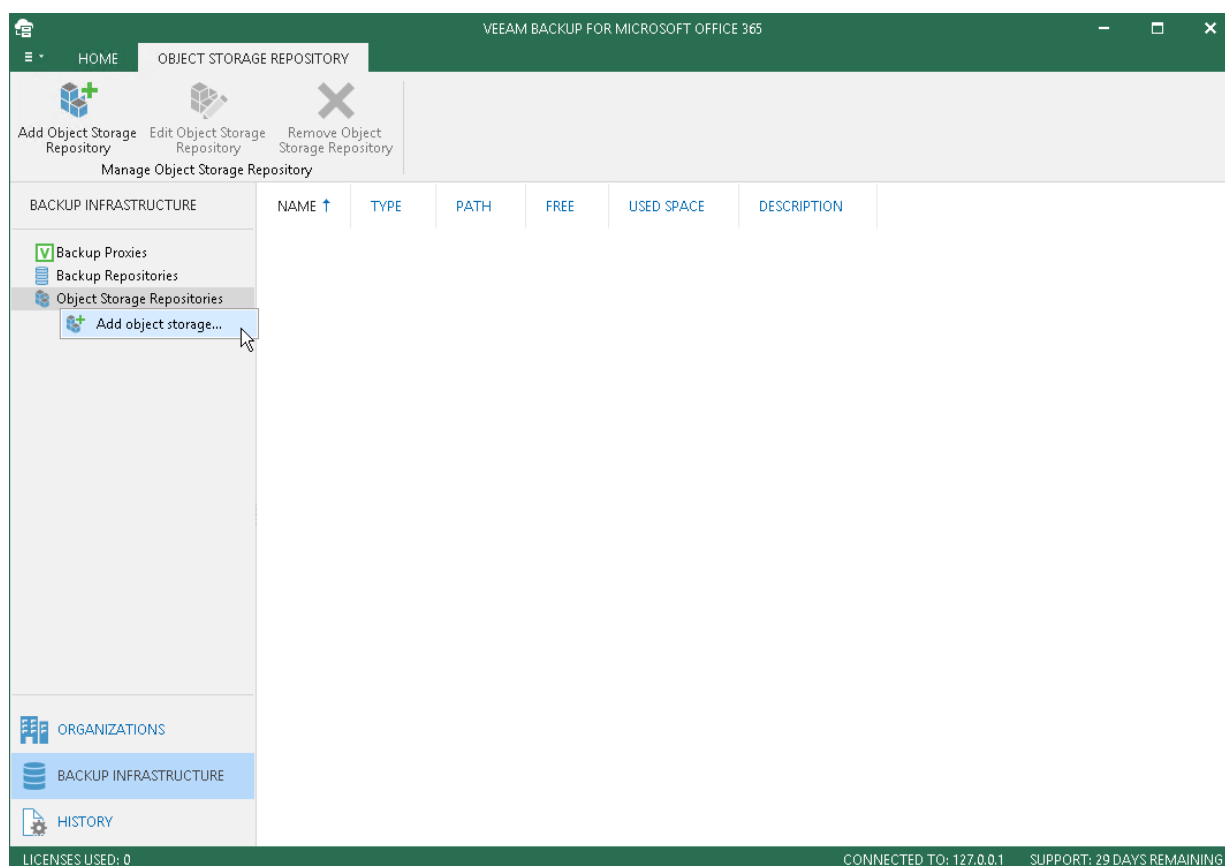
4. [Specify an object storage service point and account.](#)
5. [Specify object storage settings.](#)

Step 1. Launch New Object Storage Repository Wizard

To launch the **New Object Storage Repository** wizard, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Object Storage Repositories** node.
3. On the **Object Storage Repository** tab, click **Add Object Storage Repository**.

Alternatively, in the inventory pane, right-click the **Object Storage Repositories** node and select **Add object storage**.



Step 2. Specify Object Storage Repository Name

At this step of the wizard, enter a name for the object storage repository and provide optional description:

1. In the **Name** field, specify a new name for the object storage repository.
2. In the **Description** field, enter a description (optional).

NEW OBJECT STORAGE REPOSITORY

Object storage repository name and description

Name:
IBM Cloud Object Storage

Description:
Created by TECH\Administrator at 10/31/2019 12:14:23 AM

Back Next Cancel

Step 3. Select Object Storage Type

At this step of the wizard, select **IBM Cloud Object Storage**.

NEW OBJECT STORAGE REPOSITORY

Object storage type

☐ **S3 Compatible**
Adds a cloud object storage provider, or an on-premises object storage system.

☐ **Amazon S3**
Adds Amazon S3 storage. Both standard and Infrequent Access (IA) storage classes are supported.

☐ **Microsoft Azure Blob Storage**
Adds Microsoft Azure blob storage. Both hot and cold storage tiers are supported at the account level.

☒ **IBM Cloud Object Storage**
Adds IBM Cloud object storage. S3 compatible versions of both on-premises and IBM Cloud storage offerings are supported.

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 data center region and specify account credentials.

- In the **Service point** field, specify an endpoint address of your IBM cloud object storage.
- In the **Data center region** field, specify a region.
- In 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 in the drop-down list. Otherwise, click **Add** and provide your access and secret keys, as described in [Adding S3-Compatible Access Key](#). You can also click **Manage cloud accounts** to manage existing credentials records.

The screenshot shows a dialog box titled "NEW OBJECT STORAGE REPOSITORY" with a close button (X) in the top right corner. The main heading is "IBM Cloud Object Storage". Below it, there are three input fields: "Service point:" with the value "s3.us-west-1.wasabisys.com:443", "Data center region:" with the value "us-east-1", and "Specify account credentials to connect to IBM Cloud Object Storage bucket:". The third field contains a dropdown menu showing a key icon and the text "QRTI2W5R7VIOVA8E3UQ6 (Created by TECH/Administrator at 10/25/2019 5)" with a downward arrow, and an "Add..." button to its right. Below the dropdown is a blue link "Manage cloud accounts". At the bottom of the dialog are three buttons: "Back", "Next", and "Cancel".

Step 5. Specify Object Storage Settings

At this step of the wizard, specify an object storage bucket and folder where you want to keep your backup data.

1. In 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 Office 365 does not support creating new buckets.

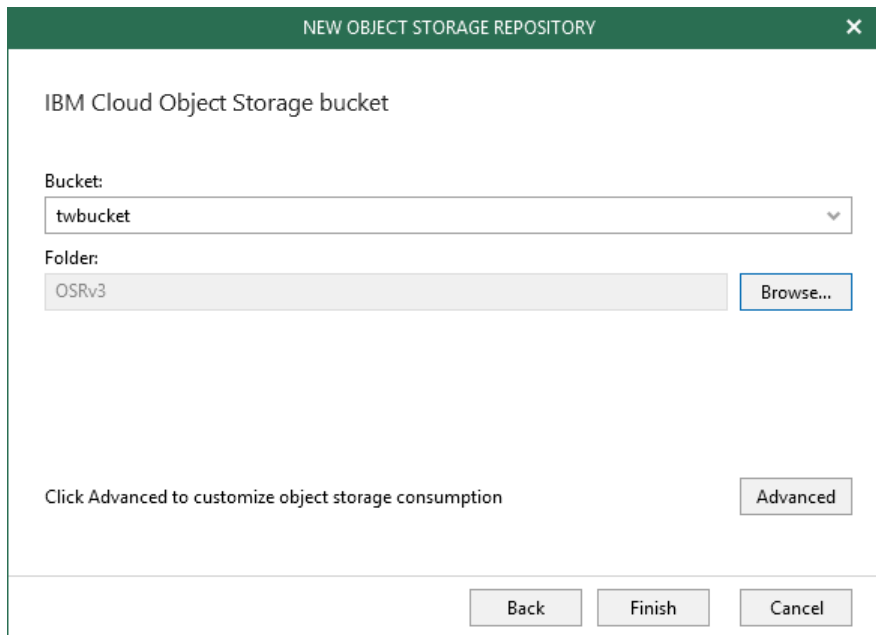
2. In the **Folder** field, select a folder to which you want to map your object storage repository, and which will be used to store backups.

To select a folder, click **Browse** and either select an existing folder or create a new one by clicking **New Folder**.

For more information about how data is stored, see [Object Storage Repository Structure](#).

3. Click **Advanced** if you want to configure storage consumption limitations.

Veeam Backup for Microsoft Office 365 will display the **Advanced Settings** window.



NEW OBJECT STORAGE REPOSITORY

IBM Cloud Object Storage bucket

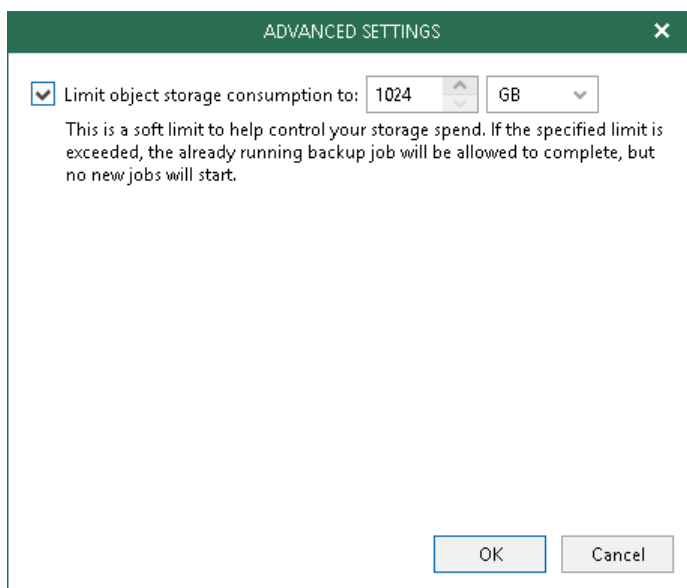
Bucket:
twbucket

Folder:
OSRv3 Browse...

Click Advanced to customize object storage consumption Advanced

Back Finish Cancel

4. In the **Advanced Settings** window, do the following:
 - a. Select the **Limit object storage consumption to** check box if you want to allow Veeam Backup for Microsoft Office 365 to exceed the storage limit.
 - b. Set the limit.
 - c. Click **OK**.



ADVANCED SETTINGS

☒ Limit object storage consumption to: 1024 GB

This is a soft limit to help control your storage spend. If the specified limit is exceeded, the already running backup job will be allowed to complete, but no new jobs will start.

OK Cancel

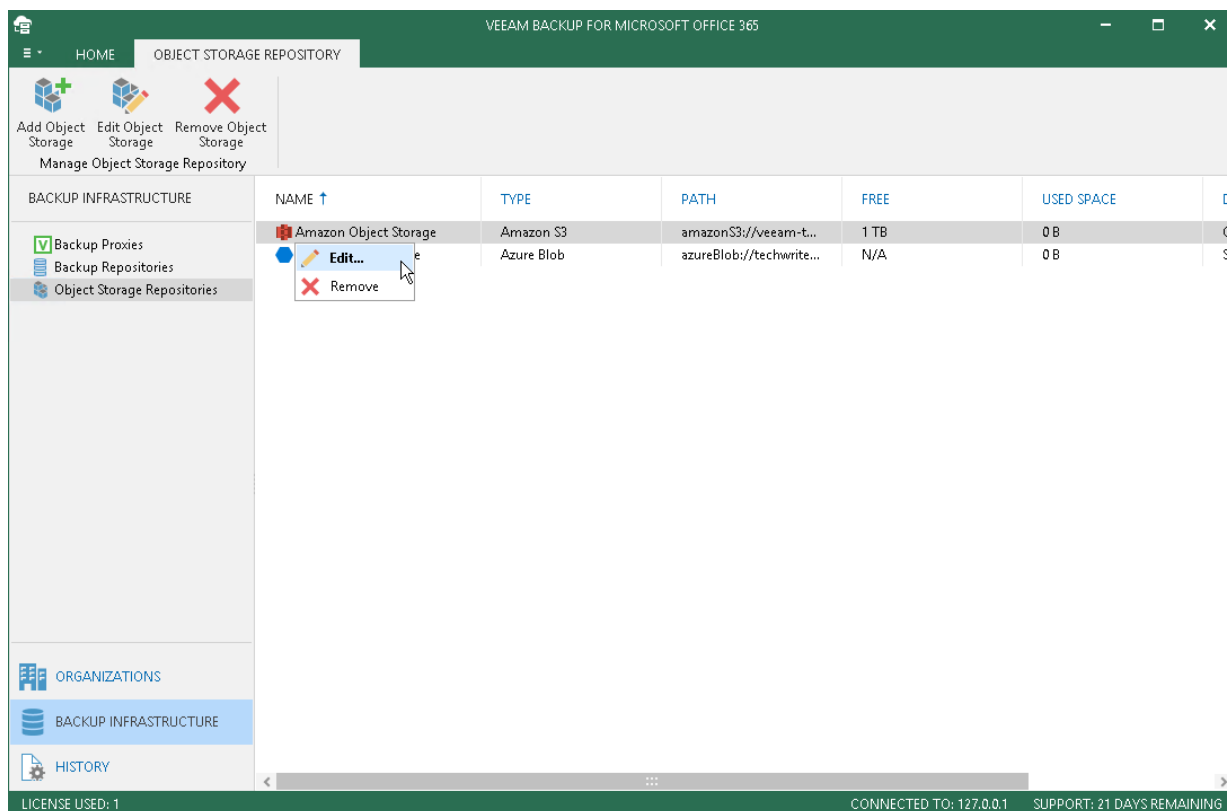
Editing Object Storage Settings

Veeam Backup for Microsoft Office 365 allows you to edit object storage repository settings such as the name of an object storage repository and its consumption limit.

To edit object storage repository settings, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Object Storage Repositories** node.

3. In the preview pane, select an object storage repository.
4. On the **Object Storage Repository** tab, click **Edit Object Storage** on the ribbon.
Alternatively, in the preview pane, right-click an object storage repository and select **Edit**.
5. Modify the name as required.



Removing Object Storage Repositories

Veeam Backup for Microsoft Office 365 allows you to remove object storage repositories from the backup infrastructure if you no longer need them.

Consider the following:

- You cannot remove an object storage repository 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 an object storage repository from the Veeam Backup for Microsoft Office 365 infrastructure, the backup data will not be removed from this storage.

To remove an object storage repository from the Veeam Backup for Microsoft Office 365 backup infrastructure, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Object Storage Repositories** node.
3. In the preview pane, select an object storage repository.
4. On the **Object Storage Repository** tab, click **Remove Object Storage** on the ribbon.
Alternatively, in the preview pane, right-click an object storage repository and select **Remove**.

VEEAM BACKUP FOR MICROSOFT OFFICE 365

HOMEOBJECT STORAGE REPOSITORY

Add Object Storage

Edit Object Storage

Remove Object Storage

Manage Object Storage Repository

BACKUP INFRASTRUCTURE

Backup Proxies

Backup Repositories

Object Storage Repositories

ORGANIZATIONS

BACKUP INFRASTRUCTURE

HISTORY

NAME ↑	TYPE	PATH	FREE	USED SPACE	D
Amazon Object Storage	Amazon S3	amazonS3://veeam-t...	1 TB	0 B	C
	Azure Blob	azureBlob://techwrite...	N/A	0 B	S

Edit...

Remove

CONNECTED TO: 127.0.0.1SUPPORT: 21 DAYS REMAINING

124 | Veeam Backup for Microsoft Office 365 | User Guide

Credentials

In Veeam Backup for Microsoft Office 365, you can use the following types of credentials:

- [Cloud credentials](#)

You can use this type of credentials to work with [object storage repositories](#).

- [Encryption passwords](#)

You can use this type of credentials to [encrypt data](#) in object storage repositories.

Managing Cloud Credentials

Veeam Backup for Microsoft Office 365 allows you to configure cloud credentials that you can use to access the following object storage:

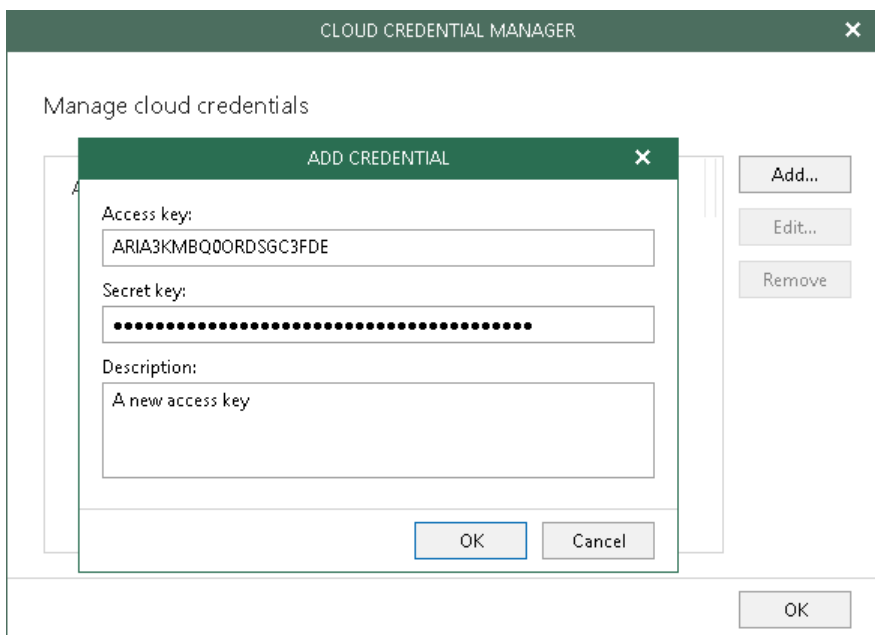
- [S3-Compatible and IBM storage](#)
- [Amazon AWS object storage](#)
- [Microsoft Azure Storage](#)

Adding S3-Compatible and IBM Storage Access Key

This section explains how to add new credentials for [S3-Compatible](#) or [IBM cloud object storage](#).

To add credentials, do the following:

1. In the main menu, click **Manage cloud credentials**.
2. In the **Cloud Credential Manager** dialog, click **Add > S3 Compatible access key**.
3. In the **Access key** field, enter your access key.
4. In the **Secret key** field, enter your secret key.
5. In the **Description** field, enter optional description.
6. Click **OK**.

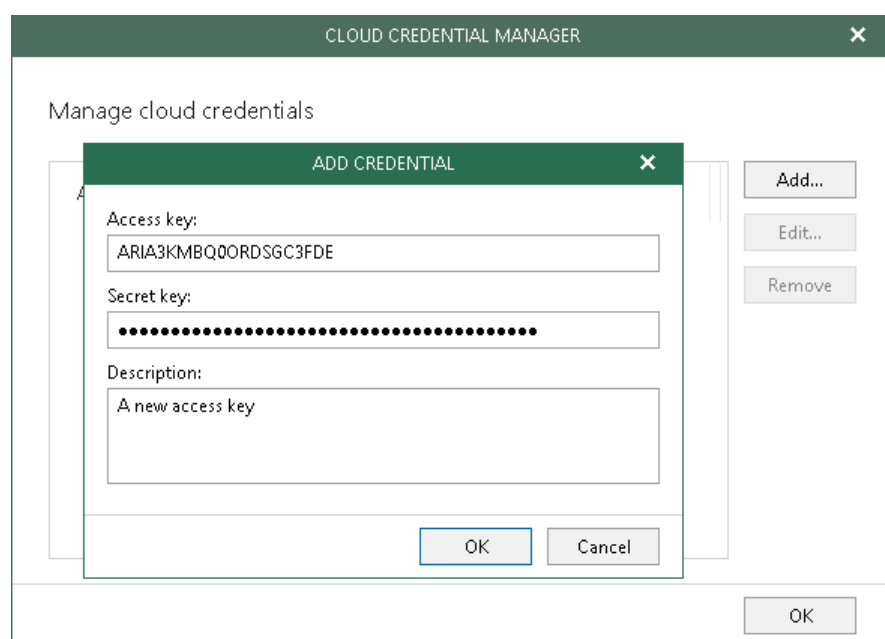


Adding Amazon AWS Access Key

This section explains how to add new credentials for [Amazon AWS object storage](#).

To add credentials, do the following:

1. In the main menu, click **Manage cloud credentials**.
2. In the **Cloud Credential Manager** dialog, click **Add > Amazon AWS access key**.
3. In the **Access key** field, enter your access key.
4. In the **Secret key** field, enter your secret key.
5. In the **Description** field, enter optional description.
6. Click **OK**.

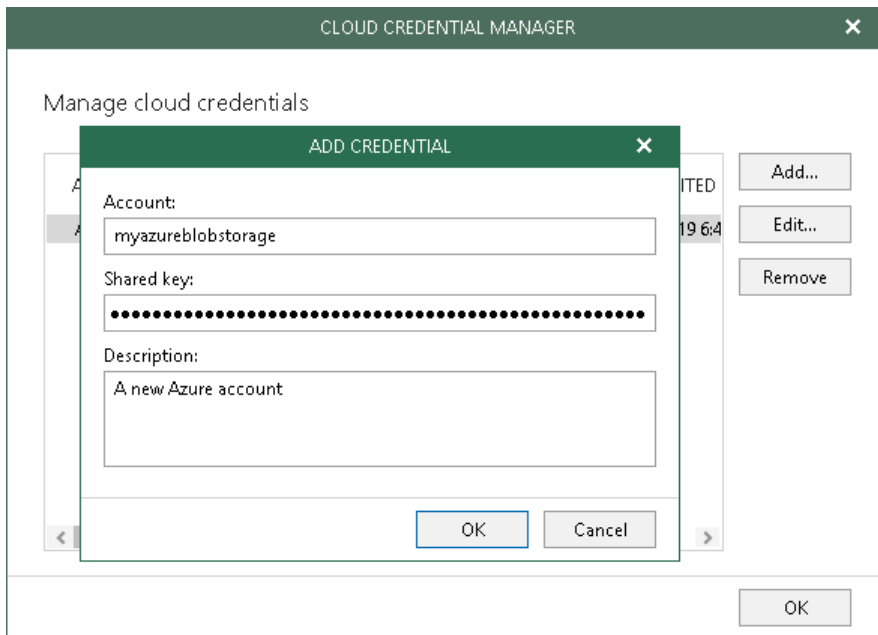


Adding Microsoft Azure Storage Account

This section explains how to 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** dialog, 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**.



Editing and Removing Cloud Credentials

Veeam Backup for Microsoft Office 365 allows you to edit and remove object storage credentials.

Editing Credentials

To edit credentials, do the following:

1. In the main menu, click **Manage cloud credentials**.
2. In the **Cloud Credential Manager** dialog, select credentials and click **Edit**.
3. Modify the selected credentials as required.

When editing Azure accounts, only the shared key can be changed.

Removing Credentials

To remove credentials, do the following:

1. In the main menu, click **Manage cloud credentials**.
2. In the **Cloud Credential Manager** dialog, select credentials and click **Remove**.

NOTE:

You cannot remove credentials that are in use.

Managing Encryption Passwords

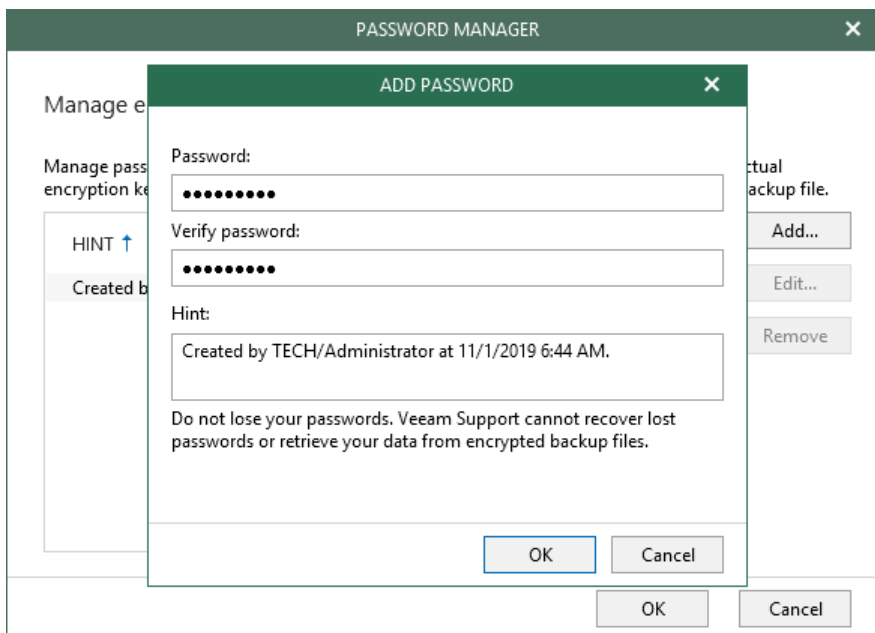
Veeam Backup for Microsoft Office 365 allows you to configure passwords that you can use to encrypt data in object storage repositories using the AES-256 specification.

To configure a password, do the following:

1. In the main menu, click **Manage passwords**.
2. In the **Password Manager** dialog, 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 might help you remember the password.

IMPORTANT!

Make sure to remember your password because, if lost, it cannot be restored.



Editing and Removing Password Records

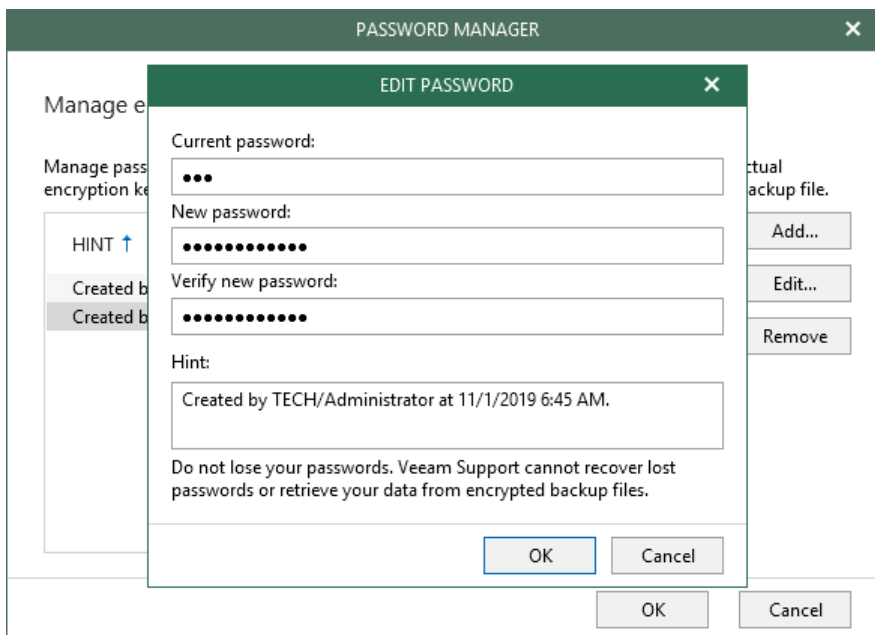
Veeam Backup for Microsoft Office 365 allows you to edit and remove passwords.

Editing Records

To edit a password, do the following:

1. In the main menu, click **Manage passwords**.
2. In the **Manage passwords** dialog, 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 might help you remember the password.



Removing Records

To remove a password, do the following:

1. In the main menu, click **Manage passwords**.
2. In the **Manage passwords** dialog, 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 Office 365 environment:

- [Microsoft Office 365 organizations](#)
- [On-Premises Microsoft organizations](#)
- [Hybrid organizations](#)

To connect to Microsoft Office 365 and on-premises Microsoft organizations, Veeam Backup for Microsoft Office 365 uses the following components:

- *Exchange Web Services* (EWS) and *PowerShell* to connect to Microsoft Office 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* to connect to Microsoft Office 365 organizations.

Microsoft Office 365 Organizations

You can add Microsoft Office 365 organizations to the Veeam Backup for Microsoft Office 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 Office 365 organizations, you can use the following authentication methods:

- **Modern authentication**

When you use this method, Veeam Backup for Microsoft Office 365 uses an Azure AD application for an authentication process against your Office 365 organizations with enabled security defaults; you cannot use a user account when using a modern authentication method.

- **Modern authentication with legacy authentication protocols**

When you use this method, you can use both the user account and the Azure AD application to authenticate against your Office 365 organizations with disabled security defaults.

- **Basic authentication**

When you use this method, you are required to provide a user account and its password to authenticate against your Office 365 organization.

Adding Organizations with MFA

[Information in this section is applicable to Veeam Backup for Microsoft Office 365 version 4c only.]

When you add an organization using the [modern authentication method](#), you are required to provide [Azure AD application](#) settings. Veeam Backup for Microsoft Office 365 uses such an application to establish a connection to your Office 365 organizations with enabled [security defaults](#) and maintain data transfer during [backup](#) and [restore](#) sessions.

With modern authentication, you cannot use a user account; only communications via an AD application is possible.

To add a new Microsoft Office 365 organization, do the following:

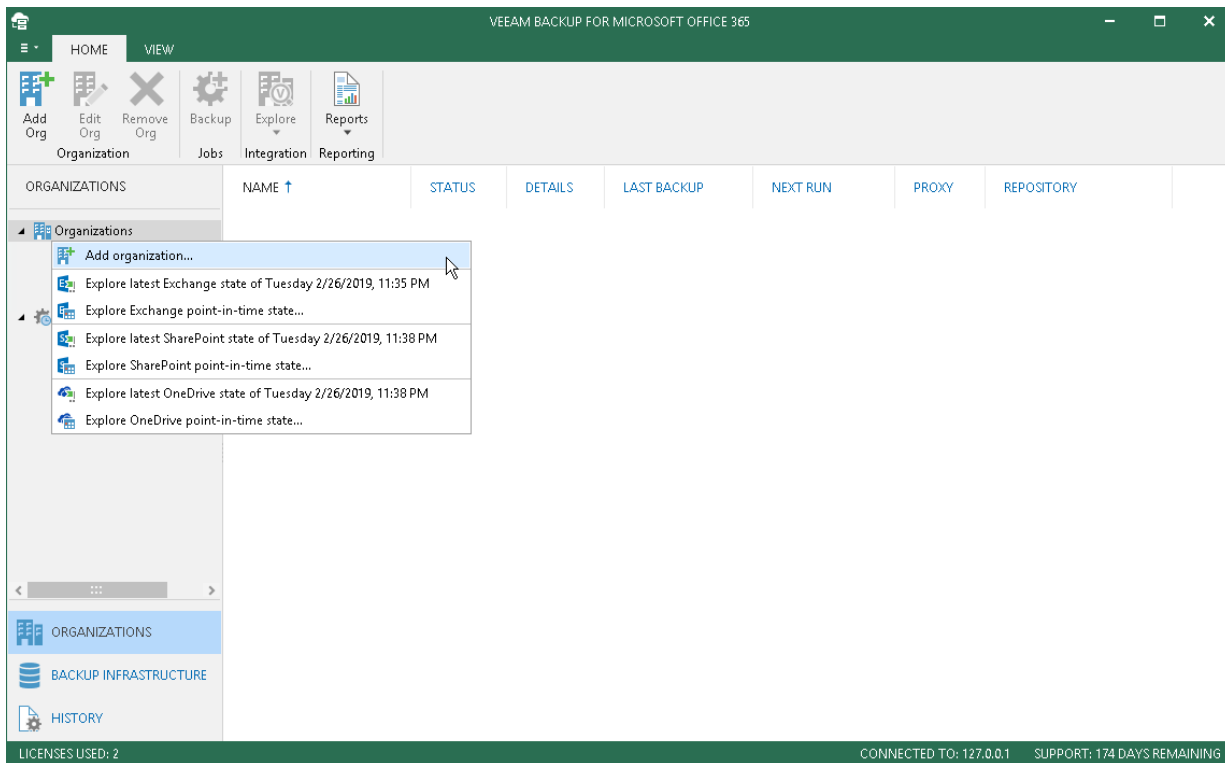
1. [Launch the Add Organization wizard.](#)
2. [Select an organization deployment type.](#)
3. [Specify connection settings.](#)
4. [Choose an Azure AD application.](#)
5. [Register an Azure AD Application.](#)
6. [Log on to Office365.](#)
7. [Finish the wizard.](#)

Step 1. Launch Add Organization Wizard

To launch the **Add Organization** wizard, do the following:

1. Open the **Organizations** view.
2. On the **Home** tab, click **Add Org** on the ribbon.

Alternatively, 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 that you want to protect.

To select a deployment type and services, do the following:

1. In the **Select organization deployment type** drop-down list, select **Microsoft Office 365**.
2. Select services that you want to protect:
 - **Exchange Online**
Select this check box if you want to back up Microsoft Exchange Online data.
 - **SharePoint Online and OneDrive for Business**
Select this check box if you want to back up Microsoft SharePoint Online and Microsoft OneDrive for Business data.

Organization deployment type

Select organization deployment type:

Microsoft Office 365

Select the services you want to protect:

☒ Exchange Online

☒ SharePoint Online and OneDrive for Business

Back Next Cancel

Step 3. Specify Connection Settings

At this step of the wizard, select a region and authentication method.

To select a region and authentication method, do the following:

1. In the **Region** drop-down list, select a Microsoft Azure region your Office 365 organization belongs to.

[Applicable to Veeam Backup for Microsoft Office 365 version 4. To select a *Government Community Cloud (GCC)* region, select **Default** in the drop-down list. For more information about Microsoft Office 365 endpoints, see [this Microsoft article](#).]

When you select *China*, you can use the *Basic Authentication* method only, as described in [Adding Organizations with Basic Authentication](#).

2. Select the **Modern authentication** option to connect to your Microsoft Office 365 organization with enabled [security defaults](#).

Make sure to leave the **Allow for using legacy authentication protocols** check box unchecked. This check box allows you to add an Office 365 organization with disabled security defaults, as described in [Adding Organizations with MFA and Legacy Protocols](#).

ADD ORGANIZATION

Office 365 connection settings

Region:

Default

Select authentication method:

☒ Modern authentication

Access Office 365 using an Azure AD application and certificate-based authentication for extra security.

☐ Allow for using legacy authentication protocols

Provides extended backup functionality, including protection of Discovery Search and Public Folder mailboxes, Dynamic Distribution groups, [and more](#).

☐ Basic authentication

Legacy authentication to access the Office 365 services on behalf of a user.

Back

Next

Cancel

Step 4. Choose Azure AD Application

At this step of the wizard, choose whether you want to register a new [Azure AD application](#) to connect to your Microsoft Office 365 organization or use an existing AD application.

You can select either of the following options:

- Register a new Azure AD application automatically**

With this option selected, Veeam Backup for Microsoft Office 365 requires to provide an application name and certificate to register a new AD application in Microsoft Azure Active Directory, as described in [Registering New Application](#).
- Use an existing Azure AD application**

With this option selected, Veeam Backup for Microsoft Office 365 requires to provide connection parameters to the existing AD application, as described in [Using Existing Application](#).

ADD ORGANIZATION

Office 365 connection settings

Select how to connect to the Office 365 organization:

☒ Register a new Azure AD application automatically

A new Veeam Backup for Microsoft Office 365 application will be registered in the specified Office 365 organization and granted with required permissions.

☐ Use an existing Azure AD application

Use an existing pre-configured Azure AD application.

Back

Next

Cancel

Step 5. Register Azure AD Application

At this step of the wizard, you can create a new application in Microsoft Azure Active Directory or select an existing one, as described in:

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

Registering New Azure AD Application

You can register a new AD application in Microsoft Azure Active Directory. Veeam Backup for Microsoft Office 365 will use this application for data exchange with your Microsoft Office 365 organizations during backup and restore sessions.

When registering a new AD application, Veeam Backup for Microsoft Office 365 automatically grants [required permissions](#) to this application.

To register a new application, do the following:

1. In the **Application Name** field, enter a name that you want to use to register a new AD application in your Microsoft Azure Active Directory.
2. Click **Install** to choose an SSL certificate that you want to use for data exchange between Veeam Backup for Microsoft Office 365 and an AD application.
3. In the **Select Certificate** wizard, select a certificate, as described in [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 Azure Active Directory, as described in [this Microsoft article](#). When generating a new self-signed certificate, Veeam Backup for Microsoft Office 365 will register it automatically.

4. Select the **Allow this application to change the export mode for SharePoint Web parts** check box to allow Veeam Backup for Microsoft Office 365 to back up web parts of your Microsoft SharePoint web sites. For more information about web parts, see [this Microsoft article](#).

By default, web parts of Microsoft SharePoint sites that belong to Office 365 organization with enabled [security defaults](#) have the *allowexport* property set to *false*, which prevents Veeam Backup for Microsoft Office 365 from having a direct access to such web parts.

If this check box is selected, Veeam Backup for Microsoft Office 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.

Using Existing Azure AD Application

You can specify an existing AD application in your Microsoft Azure Active Directory. Veeam Backup for Microsoft Office 365 will use this application for data exchange with your Microsoft Office 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 Office 365 organization using the following format: *name@<domain_name>.<domain>*. For example, *user@abc.com*.

Mind that if you select to protect only SharePoint Online and OneDrive for Business services at the [Select Organization Deployment Type](#) step, Veeam Backup for Microsoft Office 365 displays the **Specify organization name** field instead. In this field, specify a domain name of your Office 365 organization without the user name. For example, *abc.com*.

2. In the **Application ID** field, specify an identification number of an AD application that you want to use to access your Microsoft Office 365 organization.

You can find this number in the application settings of your Microsoft Azure Active Directory, as described in [this Microsoft article](#).

5. Click **Install** to choose an SSL certificate that you want to use for data exchange between Veeam Backup for Microsoft Office 365 and the specified AD application.

6. In the **Select Certificate** wizard, select a certificate, as described in [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 Azure Active Directory, as described in [this Microsoft article](#). When generating a new self-signed certificate, Veeam Backup for Microsoft Office 365 will register it automatically.

7. Select the **Grant this application required permissions and register its certificate in Azure AD** check box to automatically grant [required permissions](#) to the AD application.

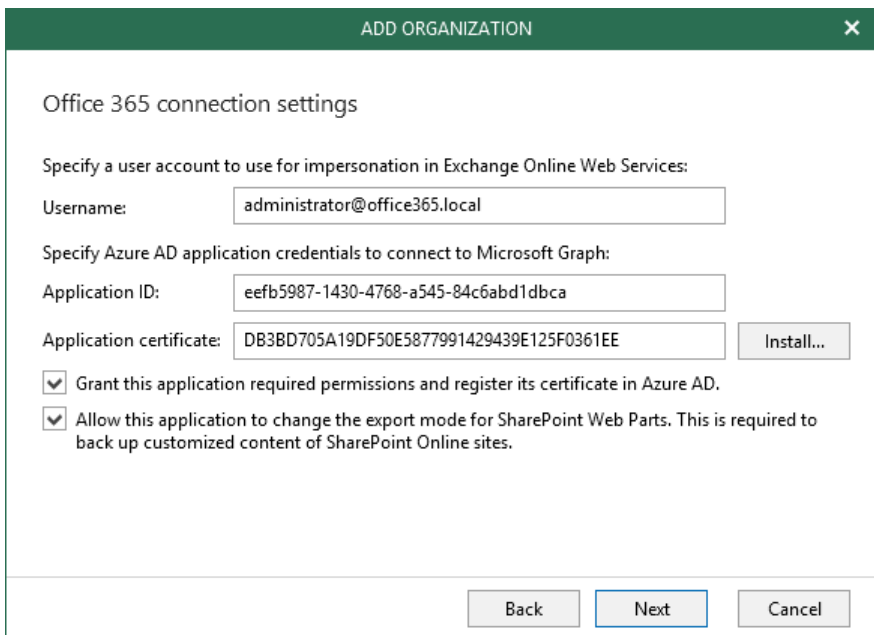
Veeam Backup for Microsoft Office 365 will also register the specified certificate in your Microsoft Azure Active Directory.

Mind that if this check box is not selected, Veeam Backup for Microsoft Office 365 skips the [Logon to Microsoft Office365 Organization](#) step and proceeds to [Finish Wizard](#).

8. Select the **Allow this application to change the export mode for SharePoint Web parts** check box to allow Veeam Backup for Microsoft Office 365 to back up web parts of your Microsoft SharePoint web sites. For more information about web parts, see [this Microsoft article](#).

By default, web parts of Microsoft SharePoint sites that belong to Office 365 organization with enabled security defaults have the *allowexport* property set to *false*, which prevents Veeam Backup for Microsoft Office 365 from having a direct access to such web parts.

If this check box is selected, Veeam Backup for Microsoft Office 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 "Office 365 connection settings". Below this, there are three sections for specifying credentials:

- Specify a user account to use for impersonation in Exchange Online Web Services:**
Username:
- Specify Azure AD application credentials to connect to Microsoft Graph:**
Application ID:
- Application certificate:

Below these fields are two checked checkboxes:

- ☒ Grant this application required permissions and register its certificate in Azure AD.
- ☒ Allow this application to change the export mode for SharePoint Web Parts. This is required to back up customized content of SharePoint Online sites.

At the bottom of the dialog are three buttons: "Back", "Next" (highlighted with a blue border), and "Cancel".

Step 6. Log on to Office 365

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

To sign in to the Microsoft Office 265 organization, do the following:

1. Click **Copy Code** to copy an authentication code.
Mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.
2. Click the link to the Microsoft portal.
3. On the **Microsoft Azure device logon** page, paste the code that you have copied and sign in to Azure.
Make sure to log 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** window and click **Next**.

ADD ORGANIZATION


Logon to Office 365


Provided account must have permissions to authenticate to the Office 365 organization.

To sign in, use a web browser and authenticate by entering a code below to the page:
<https://microsoft.com/devicelogin>

CBQFG2Z34

Copy Code

 Refresh code

 You are authenticated to Office 365 as administrator@tech.club

Back

Next






Cancel

Step 7. Finish Wizard

At this step of the wizard, wait for a connection to be established and click **Finish**.

ADD ORGANIZATION

Verifying connection and organization parameters...

ACTION	DURATION
 Connect to Microsoft Graph	00:48
 Connect to EWS	
 Connect to SharePoint	00:01
 Check Exchange Online plan	
 Check SharePoint Online plan	

Back

Finish

Cancel

Adding Organizations with MFA and Legacy Protocols

[Information in this section is applicable to Veeam Backup for Microsoft Office 365 version 4 and 4c.]

When you add an organization using the [modern authentication method](#) with legacy authentication protocols, you can use either a user account or an [Azure AD application](#) for authentication. Veeam Backup for Microsoft Office 365 uses a user account or an application to establish a connection to your Office 365 organizations with disabled [security defaults](#) and maintain data transfer during [backup](#) and [restore](#) sessions.

To add a new Microsoft Office 365 organization, [check prerequisites](#) and do the following:

1. [Launch the Add Organization wizard.](#)
2. [Select an organization deployment type.](#)
3. [Specify connection settings.](#)
4. [Specify Azure AD application credentials.](#)
5. [Specify SharePoint Online credentials.](#)
6. [Finish the wizard.](#)

Before You Begin

Before you start adding a new Microsoft Office 365 organization with enabled [multi-factor authentication](#) (MFA), you must register a new [Azure AD application](#) in your Microsoft 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 Office 365 organizations and to perform a backup and restore from/to such organizations.

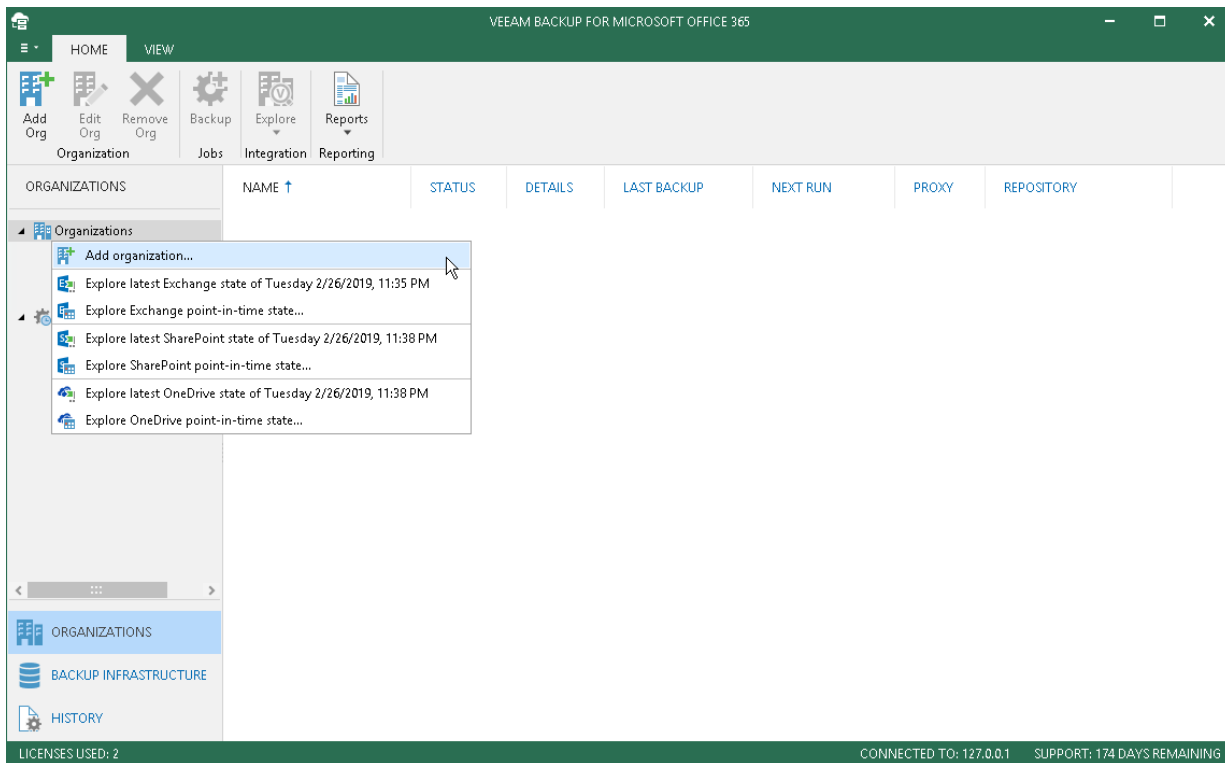
Make sure to grant your AD application [required permissions](#).

Step 1. Launch Add Organization Wizard

To launch the **Add Organization** wizard, do the following:

1. Open the **Organizations** view.
2. On the **Home** tab, click **Add Org** on the ribbon.

Alternatively, 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 that you want to protect.

To select a deployment type and services, do the following:

1. In the **Select organization deployment type** drop-down list, select **Microsoft Office 365**.
2. Select services that you want to protect:
 - **Exchange Online**
Select this check box if you want to back up Microsoft Exchange Online data.
 - **SharePoint Online and OneDrive for Business**
Select this check box if you want to back up Microsoft SharePoint Online and Microsoft OneDrive for Business data.

Organization deployment type

Select organization deployment type:

Microsoft Office 365

Select the services you want to protect:

☒ Exchange Online

☒ SharePoint Online and OneDrive for Business

Back Next Cancel

Step 3. Specify Connection Settings

At this step of the wizard, select a region and authentication method.

To select a region and authentication method, do the following:

1. In the **Region** drop-down list, select a Microsoft Azure region your Office 365 organization belongs to.

[Applicable to Veeam Backup for Microsoft Office 365 version 4. To select a *Government Community Cloud (GCC)* region, select **Default** in the drop-down list. For more information about Microsoft Office 365 endpoints, see [this Microsoft article](#).]

When you select *China*, you can use the *Basic Authentication* method only, as described in [Adding Organizations with Basic Authentication](#).

2. Select the **Modern authentication** option and the **Allow for using legacy authentication protocols** check box to connect to your Microsoft Office 365 organization.

Office 365 connection settings

Region:

Default

Select authentication method:

☒ Modern authentication

Access Office 365 using an Azure AD application and certificate-based authentication for extra security.

☒ Allow for using legacy authentication protocols

Provides extended backup functionality, including protection of Discovery Search and Public Folder mailboxes, Dynamic Distribution groups, and more.

☐ Basic authentication

Legacy authentication to access the Office 365 services on behalf of a user.

Back Next Cancel

Step 4. Specify Azure AD Application Credentials

At this step of the wizard, specify connection parameters to the Microsoft Azure AD application that you want to use to access your Microsoft Office 365 resources.

To specify connection parameters, do the following:

1. In the **Application ID** field, specify an identification number of the AD application.

You can find this number in the application settings of your Microsoft Azure Active Directory, as described in [this Microsoft article](#).

2. Choose an AD application authentication type. You can select either **Application secret** or **Application certificate**:

- a. To use a secret key, in the **Application secret** field, enter a secret key to access your custom application.

To obtain a secret key, you will need to generate it first, as described in [this Microsoft article](#).

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.

- b. To use a certificate, switch to the **Application certificate** option and click **Install**. For more information, see [SSL Certificates](#).

To be able to use a certificate, you must upload it to the Azure portal, as described in [this Microsoft article](#).

3. In the **Username** and **App password** fields, specify Exchange Online credentials of your Microsoft Office 365 organization.

The user account must be provided in either 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 Office 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 and OneDrive for Business** check box if you want to use the same credentials to access your Microsoft SharePoint Online and OneDrive for Business organizations. This check box is only available if both organization types have been selected at the [Select Organization Deployment Type](#) step.

If the **Use the same credentials for SharePoint Online and OneDrive for Business** check box is not selected, you will be offered to provide required credentials for the Microsoft SharePoint Online and OneDrive for Business organizations at the [Specify SharePoint Online Credentials](#) step.

ADD ORGANIZATION

Exchange Online credentials

Application ID: 63caebf0-2624-48d0-9ece-de1db611dc98

☒ Application secret:

☐ Application certificate: Install...

Username: administrator@abc.onmicrosoft.com

App password:

☒ Grant this account required roles and permissions

☒ Use the same credentials for SharePoint Online and OneDrive for Business

Back Next Cancel

Step 5. Specify SharePoint Online Credentials

[This step is only available if the **Use the same credentials for SharePoint Online and OneDrive for Business** check box has not been selected at the [Specify Azure Active Directory Credentials](#) step.]

At this step of the wizard, enter credentials to connect to the Microsoft SharePoint Online organization.

To enter credentials, do the following:

1. In the **Application ID** field, specify an identification number of the AD application.
You can find this number in the application settings of your Microsoft Azure Active Directory, as described in [this Microsoft article](#).
2. Choose an AD application authentication type. You can select either **Application secret** or **Application certificate**:
 - a. To use a secret key, in the **Application secret** field, enter a secret key to access your custom application.
To obtain a secret key, you will need to generate it first, as described in [this Microsoft article](#).
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.
 - b. To use a certificate, switch to the **Application certificate** option and click **Install**. For more information, see [SSL Certificates](#).
To be able to use a certificate, you must upload it to the Azure portal, as described in [this Microsoft article](#).
3. In the **Username** and **Password** fields, specify authentication credentials to connect to the Microsoft Office 365 organization.
The user account must be provided in either 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.

ADD ORGANIZATION

SharePoint Online and OneDrive for Business credentials

Application ID:

63caebf0-2624-48d0-9ece-de1db611dc98

☒ Application secret:

.....

☐ Application certificate:

Install...

Username:

administrator@abc.onmicrosoft.com

App password:

.....

☒ Grant this account required roles and permissions

Back

Next

Cancel

Step 6. Finish Wizard

At this step of the wizard, wait for a connection to be established and click **Finish**.

ADD ORGANIZATION

Verifying connection and organization parameters...

ACTION	DURATION
<input checked="" type="checkbox"/> Connect to Microsoft Graph	
<input checked="" type="checkbox"/> Connect to EWS	
<input checked="" type="checkbox"/> Connect to PowerShell	00:02
<input checked="" type="checkbox"/> Check Exchange Online plan	
<input checked="" type="checkbox"/> Check SharePoint Online plan	
<input checked="" type="checkbox"/> Check Required cmdlets access	00:02
<input checked="" type="checkbox"/> Check View-Only Recipients role	
<input checked="" type="checkbox"/> Check Mailbox Search role	
<input checked="" type="checkbox"/> Check ApplicationImpersonation role	00:01

Back

Finish

Cancel

Adding Organizations with Basic Authentication

[Information in this section is applicable to Veeam Backup for Microsoft Office 365 version 4 and 4c.]

When you add an organization using the basic authentication method, you are required to provide a user name and password to authenticate against your Office 365 organizations.

To add a new Microsoft Office 365 organization, do the following:

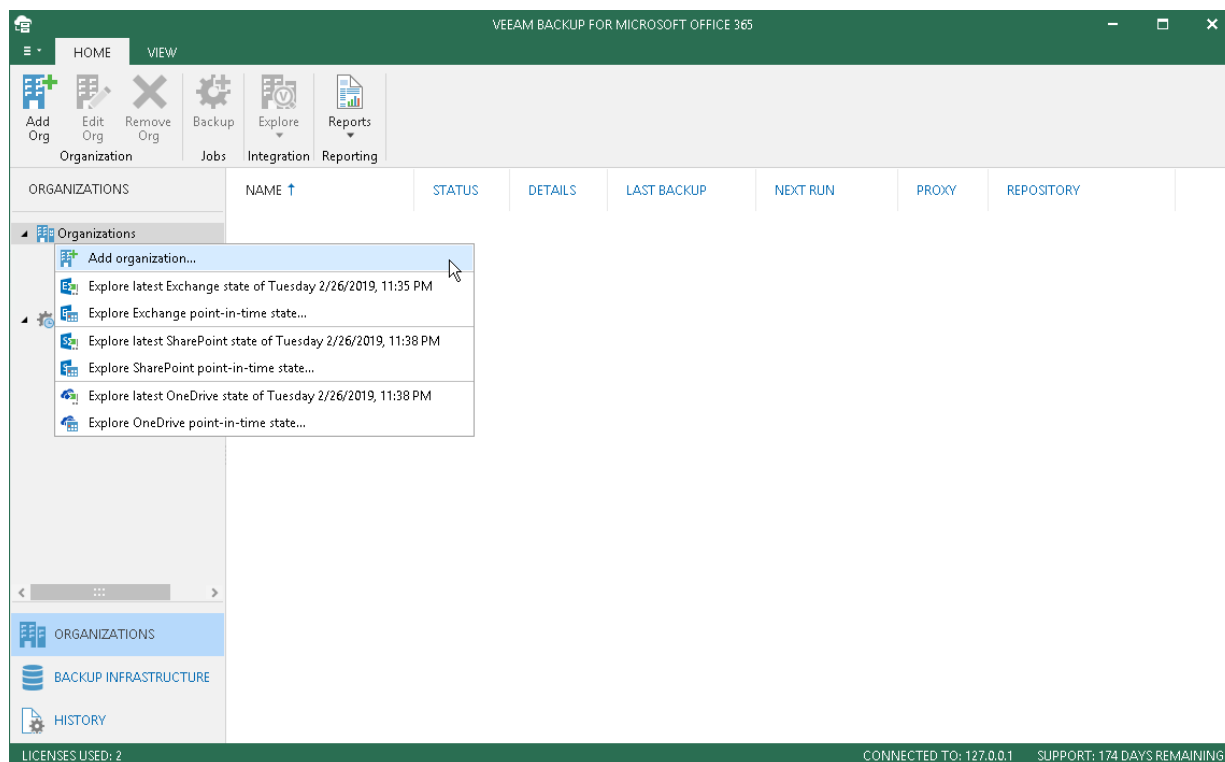
1. [Launch the Add Organization wizard.](#)
2. [Select an organization deployment type.](#)
3. [Specify connection settings.](#)
4. [Specify Exchange Online credentials.](#)
5. [Specify SharePoint Online credentials.](#)
6. [Finish the wizard.](#)

Step 1. Launch Add Organization Wizard

To launch the **Add Organization** wizard, do the following:

1. Open the **Organizations** view.
2. On the **Home** tab, click **Add Org** on the ribbon.

Alternatively, in the inventory pane, right-click the **Organizations** node and select **Add organization**.

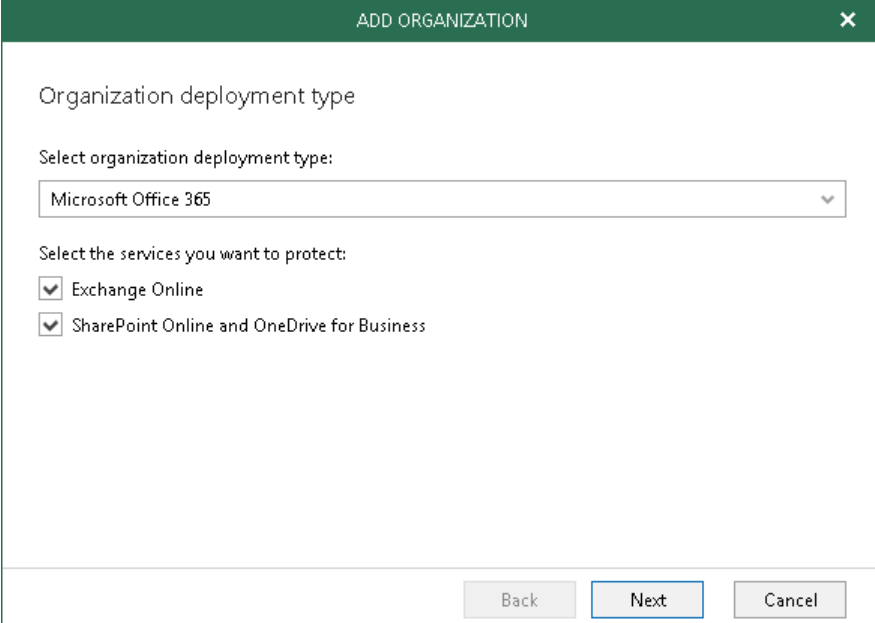


Step 2. Select Organization Deployment Type

At this step of the wizard, select a deployment type and Microsoft Online services that you want to protect.

To select a deployment type and services, do the following:

1. In the **Select organization deployment type** drop-down list, select **Microsoft Office 365**.
2. Select services that you want to protect:
 - **Exchange Online**
Select this check box if you want to back up Microsoft Exchange Online data.
 - **SharePoint Online and OneDrive for Business**
Select this check box if you want to back up Microsoft SharePoint Online and Microsoft OneDrive for Business data.



Step 3. Specify Connection Settings

At this step of the wizard, select a region and authentication method.

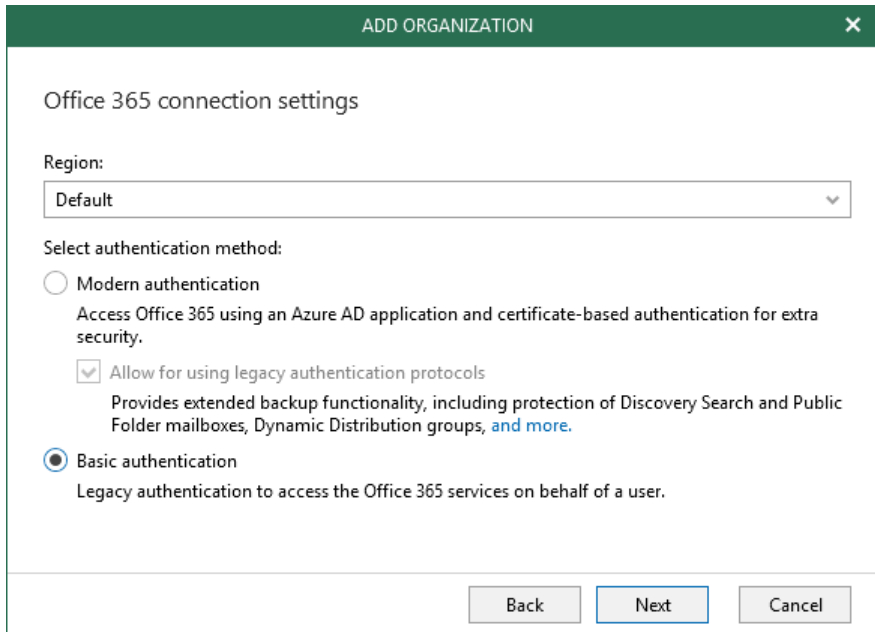
To select a region and authentication method, do the following:

1. In the **Region** drop-down list, select a Microsoft Azure region your Office 365 organization belongs to.
[Applicable to Veeam Backup for Microsoft Office 365 version 4. To select a *Government Community Cloud (GCC)* region, select **Default** in the drop-down list. For more information about Microsoft Office 365 endpoints, see [this Microsoft article](#).]
When you select *China*, you can use the *Basic Authentication* method only.
2. Select the **Basic authentication** option to connect to your Microsoft Office 365 organization using the basic authentication method.

NOTE:

To connect to Microsoft Office 365 organizations that belong to *China* or *Germany* regions, Veeam Backup for Microsoft Office 365 requires an Azure AD application that is automatically deployed to your Azure Active Directory. To be able to deploy this application, Veeam Backup for Microsoft Office 365 requires the following roles to be granted to your Microsoft Office 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 "Office 365 connection settings". Below this title, there is a "Region:" label followed by a dropdown menu currently set to "Default". Underneath, the text "Select authentication method:" is followed by two radio button options. The first option is "Modern authentication", which is currently unselected. It includes a description: "Access Office 365 using an Azure AD application and certificate-based authentication for extra security." Below this description is a checked checkbox labeled "Allow for using legacy authentication protocols", with a sub-description: "Provides extended backup functionality, including protection of Discovery Search and Public Folder mailboxes, Dynamic Distribution groups, and more." The second option is "Basic authentication", which is currently selected. It includes a description: "Legacy authentication to access the Office 365 services on behalf of a user." At the bottom of the dialog box, there are three buttons: "Back", "Next", and "Cancel".

Step 4. Specify Exchange Online Credentials

At this step of the wizard, enter credentials to connect to the Microsoft SharePoint Online organization.

To enter credentials, do the following:

1. In the **Username** and **Password** fields, specify authentication credentials to connect to the Microsoft Office 365 organization.

The user account must be provided in either 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 Office 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 and OneDrive for Business** check box if you want to use the same credentials to access your Microsoft SharePoint Online and OneDrive for Business organizations. This check box is only available if both organization types have been selected at the [Select Organization Deployment Type](#) step.

If the **Use the same credentials for SharePoint Online and OneDrive for Business** check box is not selected, you will be offered to provide required credentials for the Microsoft SharePoint Online and OneDrive for Business organizations at the [Specify SharePoint Online 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 two input fields: 'Username:' containing 'administrator@abc.onmicrosoft.com' and 'Password:' containing a series of dots. Below the password field are two checked checkboxes: 'Grant this account required roles and permissions' and 'Use the same credentials for SharePoint Online and OneDrive for Business'. At the bottom of the dialog are three buttons: 'Back', 'Next' (which is highlighted with a blue border), and 'Cancel'.

Step 5. Specify SharePoint Online Credentials

[This step is only available if the **Use the same credentials for SharePoint Online and OneDrive for Business** check box have not been selected at the [Specify Exchange Online Credentials](#) step.]

At this step of the wizard, enter credentials to connect to the Microsoft SharePoint Online organization.

To enter credentials, do the following:

1. In the **Username** and **Password** fields, specify authentication credentials to connect to the Microsoft Office 365 organization.

The user account must be provided in either 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.

ADD ORGANIZATION

SharePoint Online and OneDrive for Business credentials

Username:

administrator@abc.onmicrosoft.com

Password:

••••••••

☒ Grant this account required roles and permissions

Back

Next

Cancel

Step 6. Finish Wizard

At this step of the wizard, wait for a connection to be established and click **Finish**.

ADD ORGANIZATION

Verifying connection and organization parameters...

ACTION	DURATION
<input checked="" type="checkbox"/> Connect to Microsoft Graph	
<input checked="" type="checkbox"/> Connect to EWS	
<input checked="" type="checkbox"/> Connect to PowerShell	00:02
<input checked="" type="checkbox"/> Check Exchange Online plan	
<input checked="" type="checkbox"/> Check SharePoint Online plan	
<input checked="" type="checkbox"/> Check Required cmdlets access	00:02
<input checked="" type="checkbox"/> Check View-Only Recipients role	
<input checked="" type="checkbox"/> Check Mailbox Search role	
<input checked="" type="checkbox"/> Check ApplicationImpersonation role	00:01

Back

Finish

Cancel

On-Premises Microsoft Organizations

To add on-premises Microsoft Exchange and on-premises Microsoft SharePoint organizations, do the following:

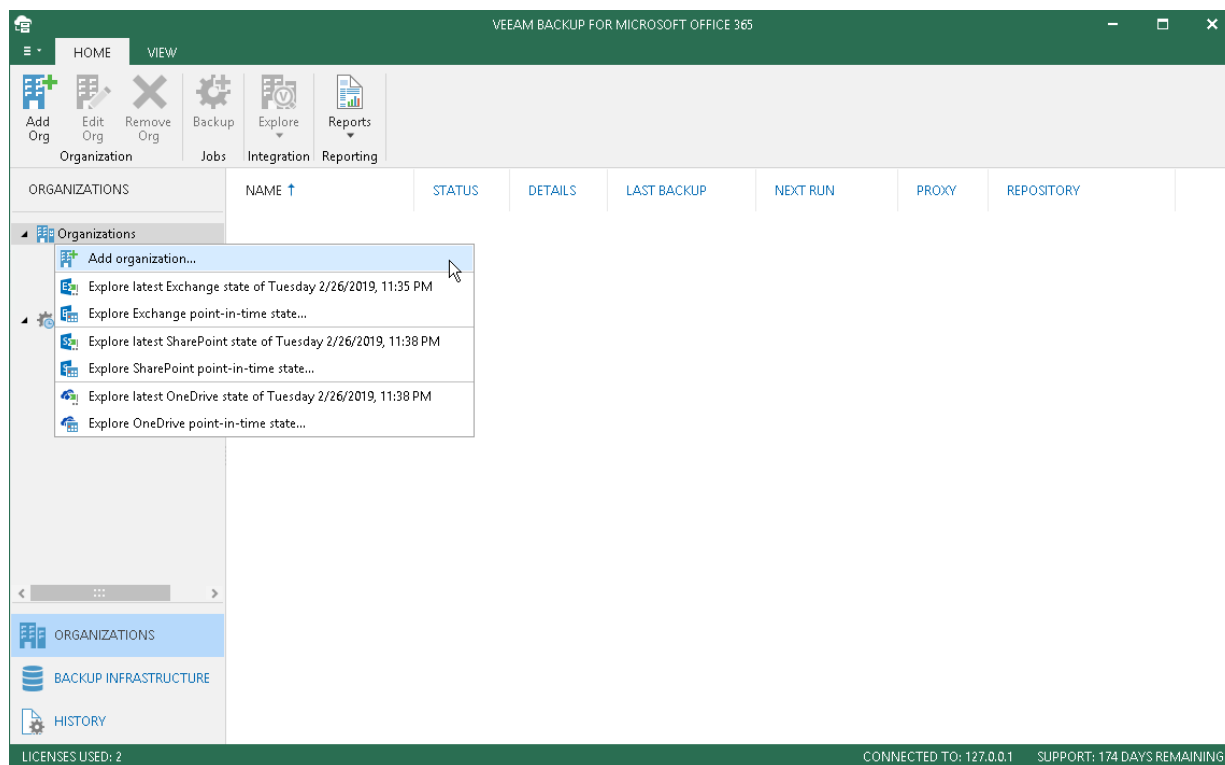
1. [Launch the Add Organization wizard.](#)
2. [Select an organization deployment type.](#)
3. [Specify Microsoft Exchange connection settings.](#)
4. [Specify Microsoft SharePoint connection settings.](#)
5. [Finish the Wizard.](#)

Step 1. Launch Add Organization Wizard

To launch the **Add Organization** wizard, do the following:

1. Open the **Organizations** view.
2. On the **Home** tab, click **Add Org** on the ribbon.

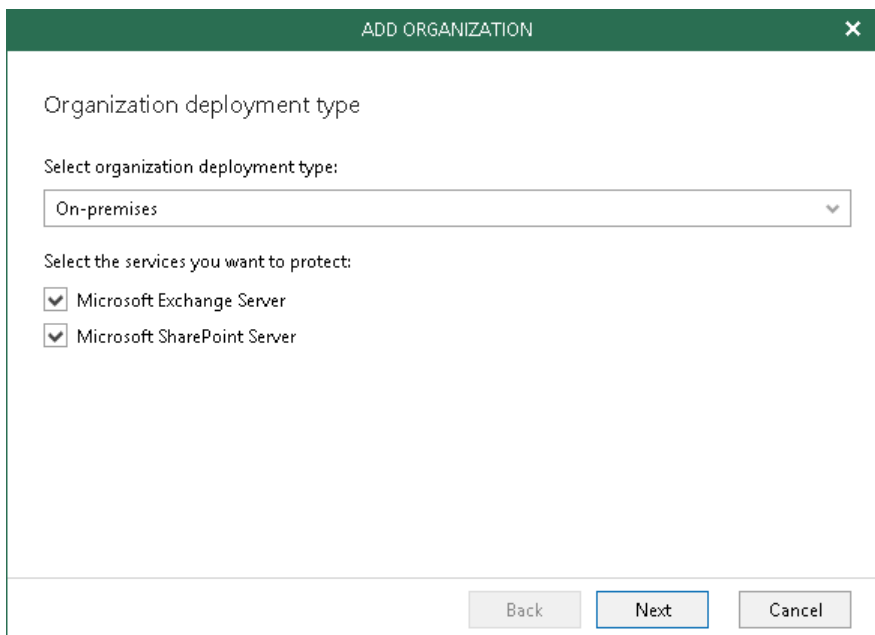
Alternatively, in the inventory pane, right-click the **Organizations** node and select **Add organization**.



Step 2. Select Organization Deployment Type

At this step of the wizard, select a deployment type and on-premises service that you want to protect.

1. In 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.



Organization deployment type

Select organization deployment type:

On-premises

Select the services you want to protect:

☒ Microsoft Exchange Server

☒ Microsoft SharePoint Server

Back Next 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 user credentials, assign appropriate permissions and configure advance 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 using either of the following formats: *domain\account* or *account@domain*.

For more information, see [Required Permissions](#).

Consider that using ADFS accounts to add on-premises Microsoft organizations is not possible. Only Office 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 upfront. Otherwise, the automatic assignment of the *ApplicationImpersonation* role will fail; an organization will not be added.
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 three input fields: "Server name:" with the text "Exchange", "Username:" with the text "exchange\administrator", and "Password:" with masked characters "••••••••". Below the password field are two checked checkboxes: "Grant this account required roles and permissions" and "Configure throttling policy". At the bottom left, there is a text prompt "Click Advanced to configure additional connection security settings" and an "Advanced..." button. At the bottom right, there are three buttons: "Back", "Next" (highlighted with a blue border), and "Cancel".

5. Click **Advanced** if you want to skip one or more SSL verifications and select any of the following check boxes:
 - Skip certificate trusted authority verification
 - Skip certificate common name verification
 - Skip revocation check

ADVANCED SETTINGS

☒ Connect using SSL

☐ Skip certificate trusted authority verification

☒ Skip certificate common name verification

☐ Skip revocation check

OK

Cancel

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 user credentials, assign appropriate permissions and configure advance settings.

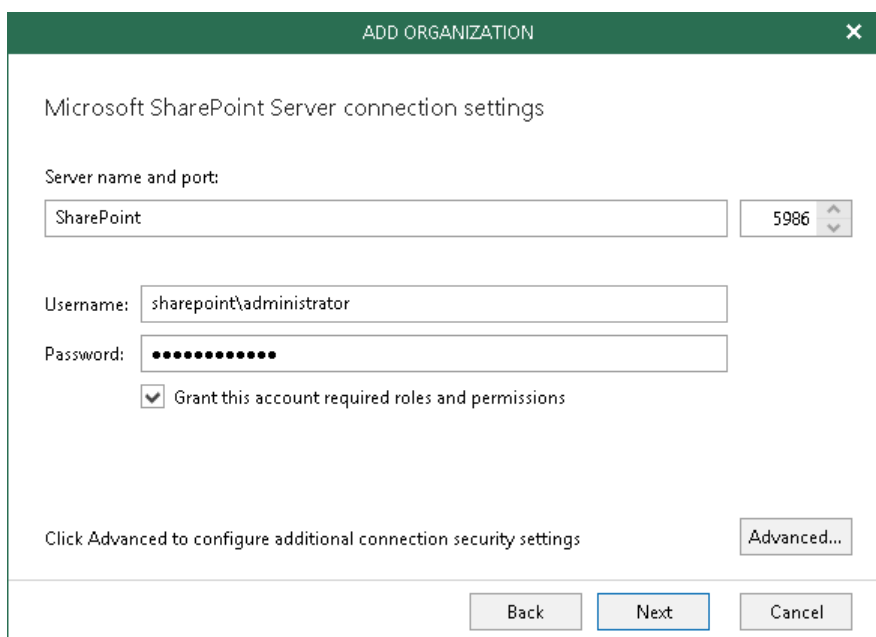
To specify connection settings to the on-premises Microsoft SharePoint server, do the following:

1. In the **Server name and port** field, specify a Microsoft SharePoint server name and the WinRM port.
For the server name, 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 using either of the following formats: *domain\account* or *account@domain*.

For more information, see [Required Permissions](#).

Consider that using ADFS accounts to add on-premises Microsoft organizations is not possible. Only Office 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 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.



The screenshot shows a dialog box titled "ADD ORGANIZATION" with a close button (X) in the top right corner. The main heading inside is "Microsoft SharePoint Server connection settings". Below this, there are three input fields: "Server name and port" with the text "SharePoint" and a port dropdown set to "5986"; "Username" with the text "sharepoint\administrator"; and "Password" with masked characters. Below the password field is a checked checkbox labeled "Grant this account required roles and permissions". At the bottom left, there is a text prompt "Click Advanced to configure additional connection security settings" and an "Advanced..." button. At the very bottom, there are three buttons: "Back", "Next" (highlighted with a blue border), and "Cancel".

4. Click **Advanced** if you want to skip one or more SSL verifications and select any of the following check boxes:
 - **Skip certificate trusted authority verification**
 - **Skip certificate common name verification**
 - **Skip revocation check**

ADVANCED SETTINGS ✕

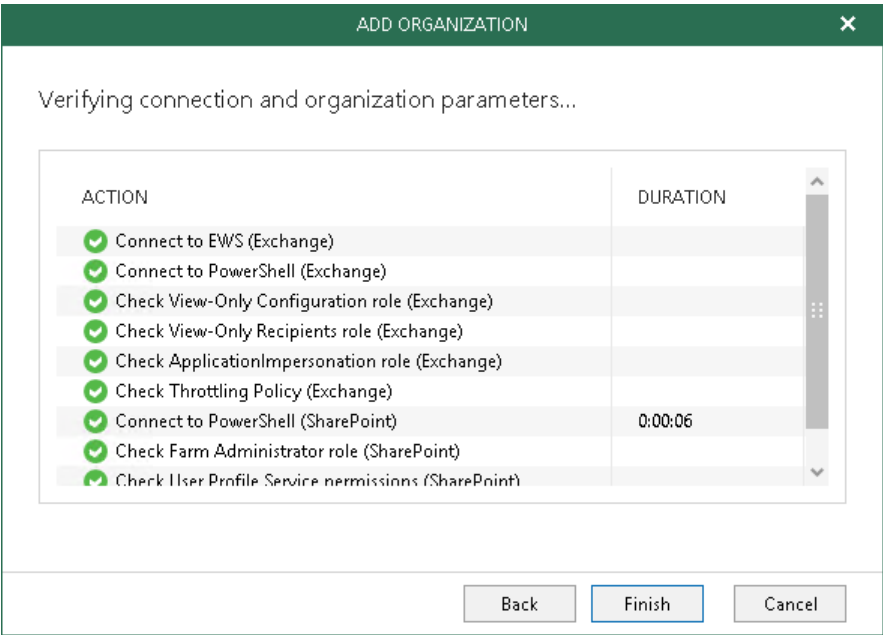
☒ Connect using SSL

- ☐ Skip certificate trusted authority verification
- ☒ Skip certificate common name verification
- ☐ Skip revocation check

OK Cancel

Step 5. Finish Wizard

At this step of the wizard, wait for a connection to be established and click **Finish**.



Hybrid Organizations

This section explains how to create hybrid configurations consisting of Microsoft Office 365 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 + on-premises Microsoft SharePoint.
- 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.

To select services that you want to add to a hybrid organization, combine the following check boxes based on the scenarios above:

- **Exchange Online**
To back up Microsoft Exchange Online data.
- **Microsoft Exchange Server**
To back up on-premises Microsoft Exchange data.
- **SharePoint Online and OneDrive for Business**
To back up Microsoft SharePoint Online and OneDrive for Business data.
- **Microsoft SharePoint Server**
To back up on-premises Microsoft SharePoint data.

Depending on the types of services that you have selected, do the following:

- Specify connection settings for the Microsoft Office 365 organization, as described in [Adding Microsoft Office 365 Organizations](#).
- Specify connection settings for the on-premises Microsoft Exchange and/or Microsoft SharePoint organization, as described in [Adding on-premises Organizations](#).

NOTE:

Consider the following:

- To create a hybrid organization, services that you select must belong to the same Microsoft Office 365 organization.
- You can use a non-MFA enabled ADFS account to add a Microsoft Office 365 organization. Using ADFS accounts to add on-premises Microsoft organizations is not possible.

ADD ORGANIZATION

Organization deployment type

Select organization deployment type:

Hybrid

Select Exchange services you want to protect:

☒ Exchange Online

☒ Microsoft Exchange Server

Select SharePoint services you want to protect:

☒ SharePoint Online and OneDrive for Business

☒ Microsoft SharePoint Server

Back Next Cancel

Backup Accounts

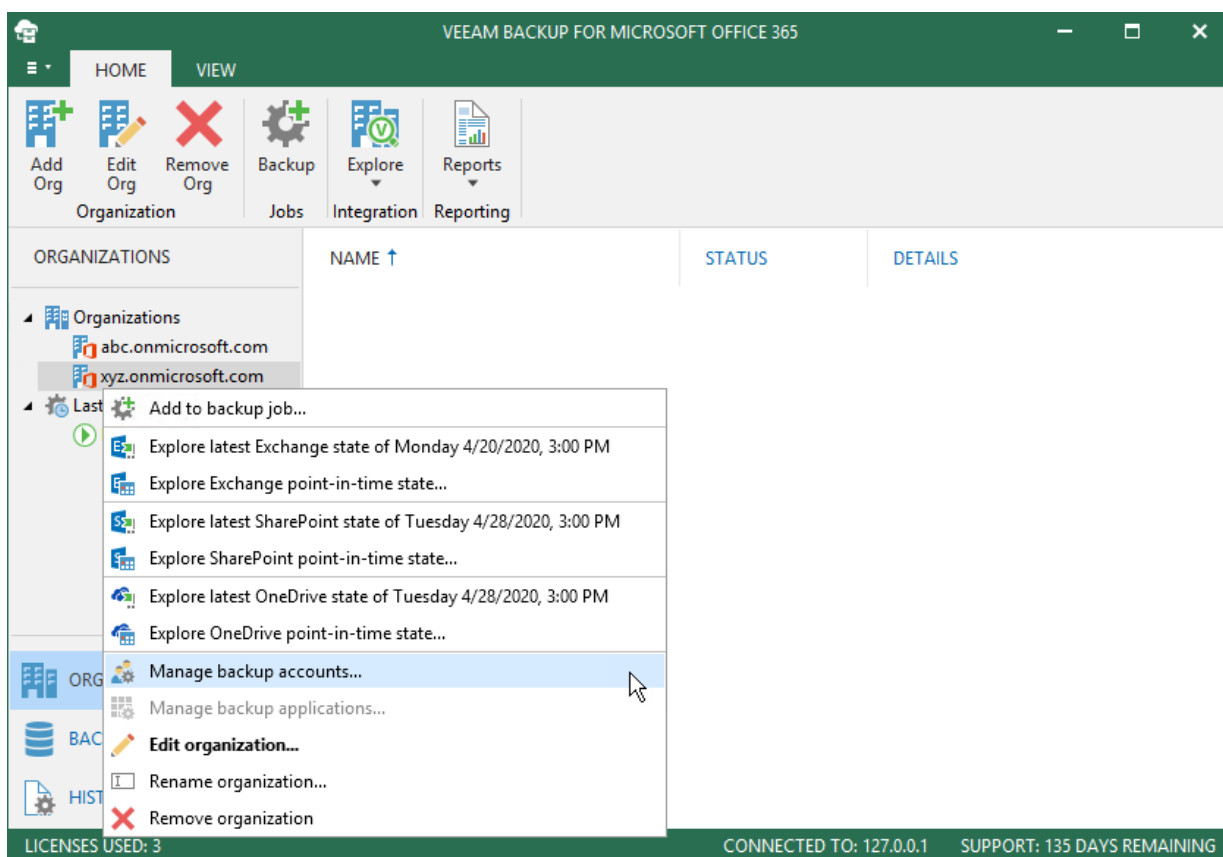
You can configure auxiliary backup accounts for Microsoft Office 365 organizations with disabled [security defaults](#) to minimize throttling when backing up Microsoft SharePoint and OneDrive for Business data.

Adding 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**.

Mind that the **Manage backup account** option is unavailable for organizations with enabled [security defaults](#).



3. In the **Backup Accounts Manager** window, click **Select**.
4. In the **Select 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.

It is recommended not to 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 Office 365 ignores an account under which your Microsoft Office 365 organization was [added](#); such accounts are never used to reduce throttling.

5. In the **Select accounts and configure their passwords** list, select check boxes next to accounts that you want to add as backup applications.
6. In the **Password** column, click **Not configured**.

The dialog box is titled "BACKUP ACCOUNTS MANAGER" with a close button (X) in the top right corner. It contains the following elements:

- A header text: "Add auxiliary backup accounts to process SharePoint Online and OneDrive for Business data. Using multiple accounts allows to increase backup performance and avoid throttling."
- A section "Select Office 365 security group:" with a text box containing "VBOWorkGroupTW" and a "Select..." button.
- A section "Select accounts and configure their passwords:" containing a table with two columns: "ACCOUNT" and "PASSWORD".

ACCOUNT	PASSWORD
<input type="checkbox"/> ACCOUNT ↑	
<input type="checkbox"/> account1@abc.onmicrosoft.com	✖ Not configured
<input type="checkbox"/> account1@abc.onmicrosoft.com	✖ Not configured
<input type="checkbox"/> account1@abc.onmicrosoft.com	✖ Not configured
<input type="checkbox"/> account1@abc.onmicrosoft.com	✖ Not configured

Below the table, it says "0 accounts selected". At the bottom of the dialog are "OK" and "Cancel" buttons.

7. In the **Add Password** window, enter the password for the account and click **OK**.

Make sure to provide an **AD application** password instead of a user account password when adding MFA-enabled accounts.

The dialog box is titled "ADD PASSWORD" with a close button (X) in the top right corner. It contains the following elements:

- A text box labeled "Account:" containing "account1@office365.onmicrosoft.com".
- A text box labeled "Password:" with a masked password (dots).
- An information icon (i) with a note: "For an account enabled for multi-factor authentication (MFA), use an app password instead of a user password."
- "OK" and "Cancel" buttons at the bottom.

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** dialog, in the **Password** column, click **Configured**.
4. In the **Edit Password** dialog, modify the password and 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** dialog, in the **Account** column, deselect accounts that you no longer want to use and click **OK**.

Backup Applications

[Backup applications are available in Veeam Backup for Microsoft Office 365 version 4c only.]

You can configure [Microsoft Azure AD applications](#) for Microsoft Office 365 organizations with enabled [security defaults](#) to minimize throttling when backing up Microsoft SharePoint and OneDrive for Business data. You can add existing applications to the backup configuration or create new applications in your Microsoft Azure Active Directory using Veeam Backup for Microsoft Office 365 capabilities.

To minimize throttling, Veeam Backup for Microsoft Office 365 iterates through each added application and uses it to access Microsoft Office 365 resources and to fetch data from your organizations.

For security purposes, data exchange between applications in Azure and Veeam Backup for Microsoft Office 365 is maintained via SSL certificates only; you cannot use an [AD application secret](#).

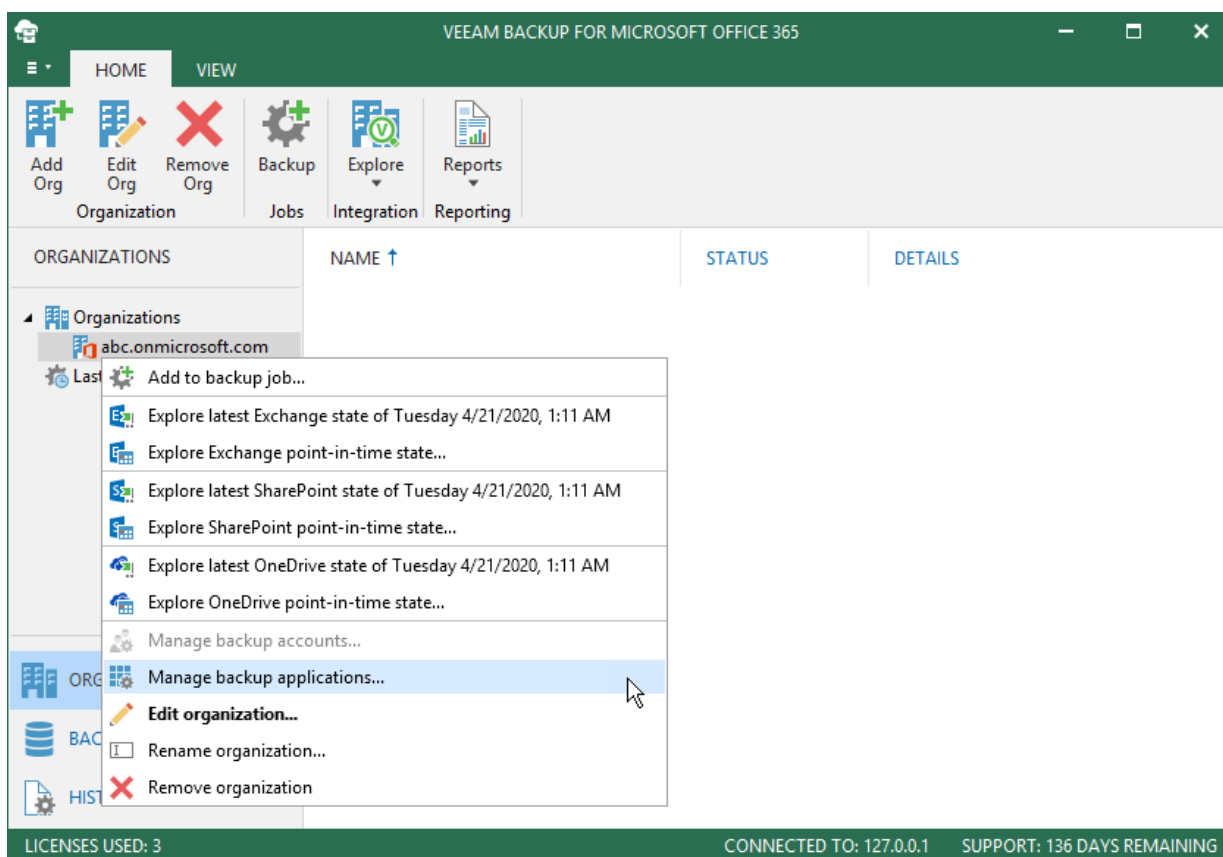
Adding Applications

When you add AD applications to the backup configuration, Veeam Backup for Microsoft Office 365 retrieves a list of existing applications from your Microsoft Azure Active Directory. From this list, you can select as many applications as you need. Each added application helps you reduce throttling during a backup of Microsoft SharePoint and OneDrive for Business data. For more information about AD applications, see [this Microsoft article](#).

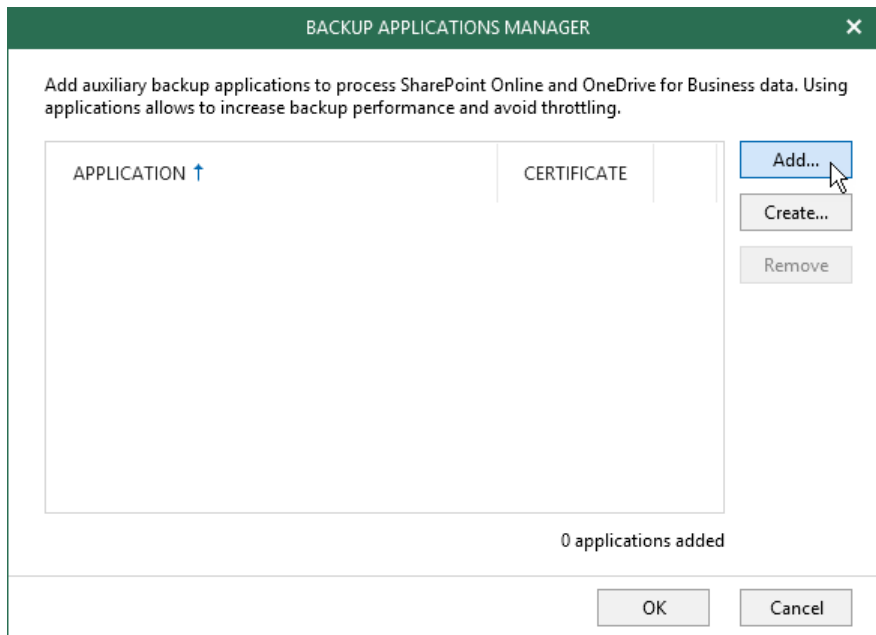
To add AD applications to the backup configuration, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, right-click a Microsoft Office 365 organization with enabled [security defaults](#) and select **Manage backup applications**.

Mind that the **Manage backup applications** option is unavailable for organizations with disabled security defaults.



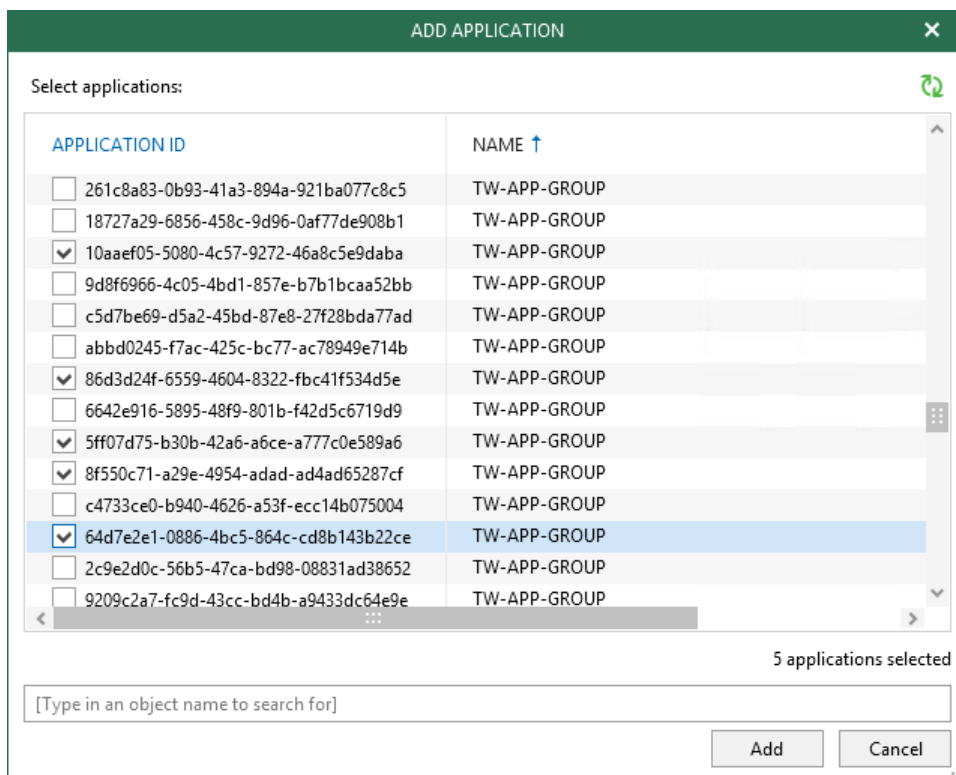
3. In the **Backup Applications Manager** window click **Add**.



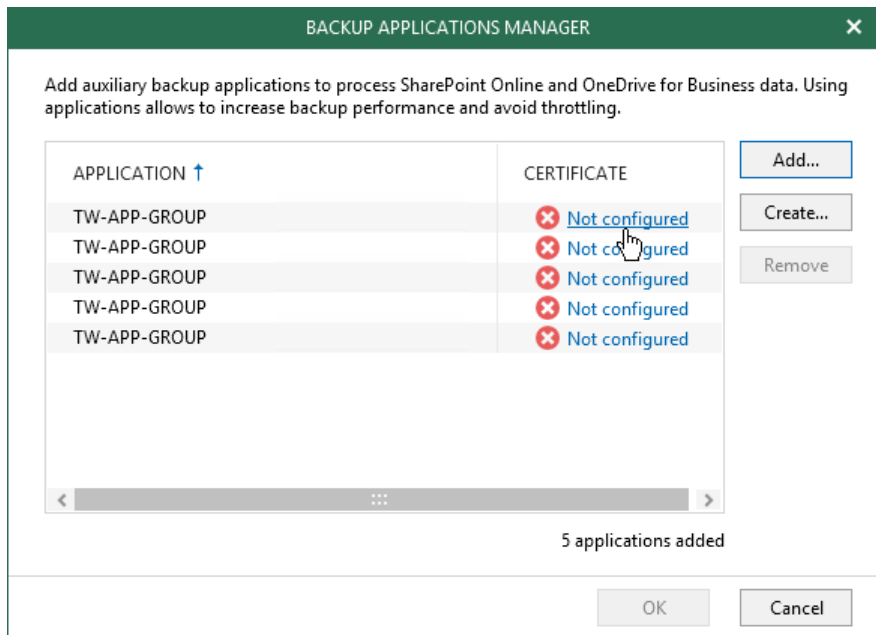
4. In the **Add Applications** window, select AD applications that you want to add and click **Add**.

Make sure to manually grant applications [required permissions](#) in advance.

Also mind that Veeam Backup for Microsoft Office 365 ignores an AD application under which your Microsoft Office 365 organization was [added](#); such applications are never used to reduce throttling.



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 Office 365 and your AD application.



6. In the **Select Certificate** wizard, select an SSL certificate, as described in [SSL Certificates](#).

Before selecting a certificate in Veeam Backup for Microsoft Office 365, you must assign this certificate to the application on the Azure portal, as described in [this Microsoft article](#).

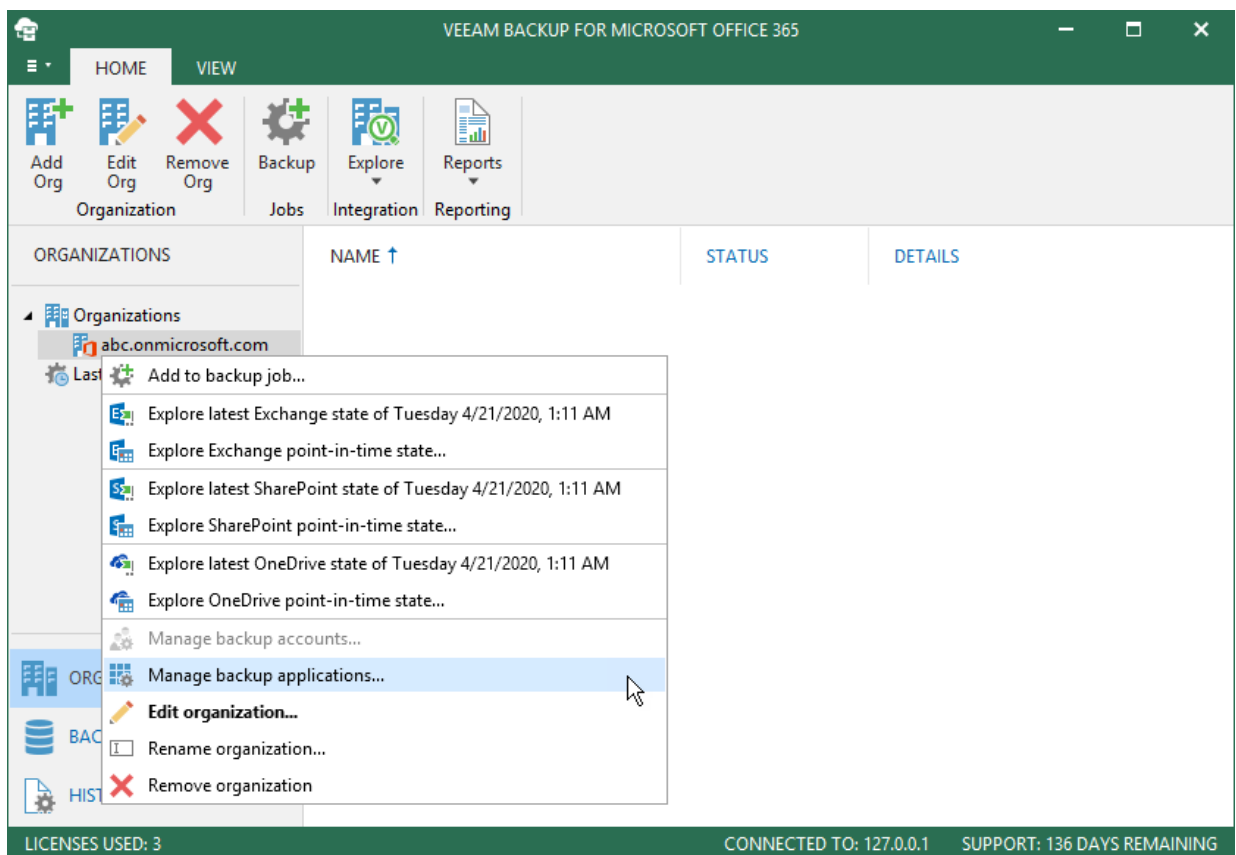
Creating Applications

When you create a new AD application, Veeam Backup for Microsoft Office 365 automatically registers this application in Microsoft Azure Active Directory of your Office 365 organization. After you create an application, Veeam Backup for Microsoft Office 365 automatically adds this application to the backup configuration. Each added application helps you reduce throttling during a backup of Microsoft SharePoint and OneDrive for Business data. For more information about AD applications, see [this Microsoft article](#).

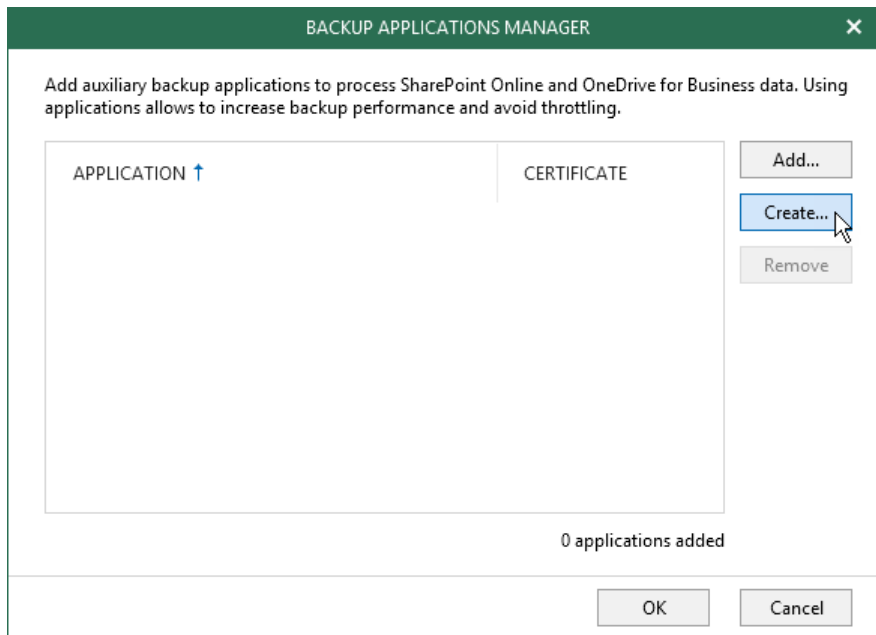
To create AD applications and add them to the backup configuration, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, right-click a Microsoft Office 365 organization with enabled [security defaults](#) and select **Manage backup applications**.

Mind that the **Manage backup applications** option is unavailable for organizations with disabled security defaults.



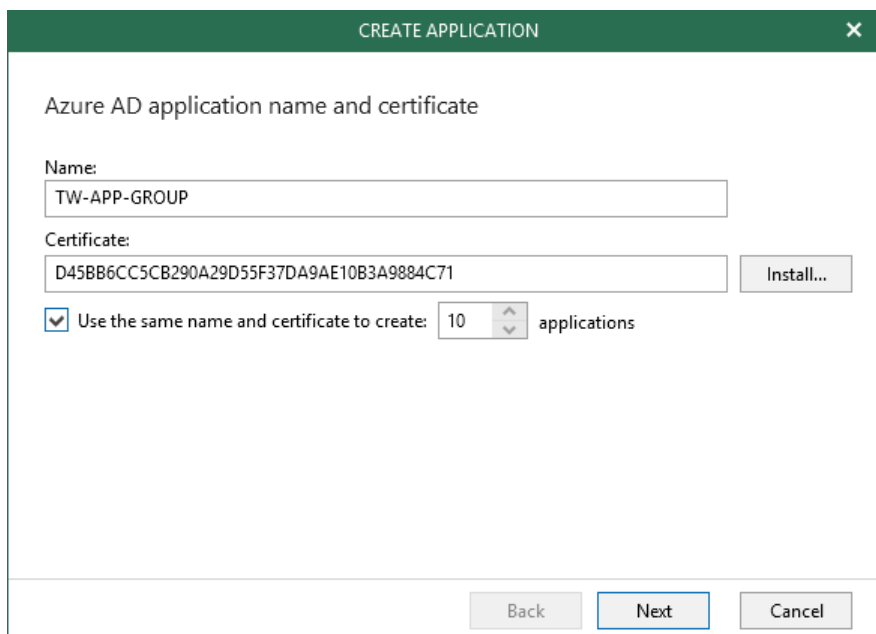
3. In the **Backup Applications Manager** click **Create**.



4. In the **Create Application** window, enter a name that you want to use for the Azure AD application and choose an SSL certificate for secure communications between Veeam Backup for Microsoft Office 365 and your application. For more information on how to install a certificate, see [SSL Certificates](#).

Veeam Backup for Microsoft Office 365 will automatically register the specified certificate in your Microsoft Azure Active Directory and assign this certificate to the AD application. In addition, Veeam Backup for Microsoft Office 365 automatically grants the *Sites.FullControl.All* permission to the application.

If you want to create more than one 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 Office 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. In the **Create Application** window, click **Copy Code** to copy an authentication code. Mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.

6. Click the link to the Microsoft portal.
7. On the **Microsoft Azure device login** page, paste the code that you have copied and sign in to Azure.
Make sure to log 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** window and click **Finish**.

CREATE APPLICATION

Logon to Office 365

Provided account must have permissions to authenticate to the Office 365 organization.

To sign in, authenticate with the below code at:
<https://microsoft.com/devicelogin>

CV8GSEK8U

Copy code

Refresh code

✔ You are authenticated to Office 365 as administrator@tech.club

Back

Finish

Cancel

Updating Certificates and Removing Applications

You can update a certificate of each configured 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** dialog, in the **Certificate** column, click **Configured**.
4. Update the certificate using the **Select Certificate** wizard. For more information about this wizard, see [SSL Certificates](#).

Removing Application

To remove 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 list, select an application and click **Remove**.

You can select multiple applications using the CTRL button.

Editing Organization Parameters

You can edit the following organization parameters:

- Organization deployment type.

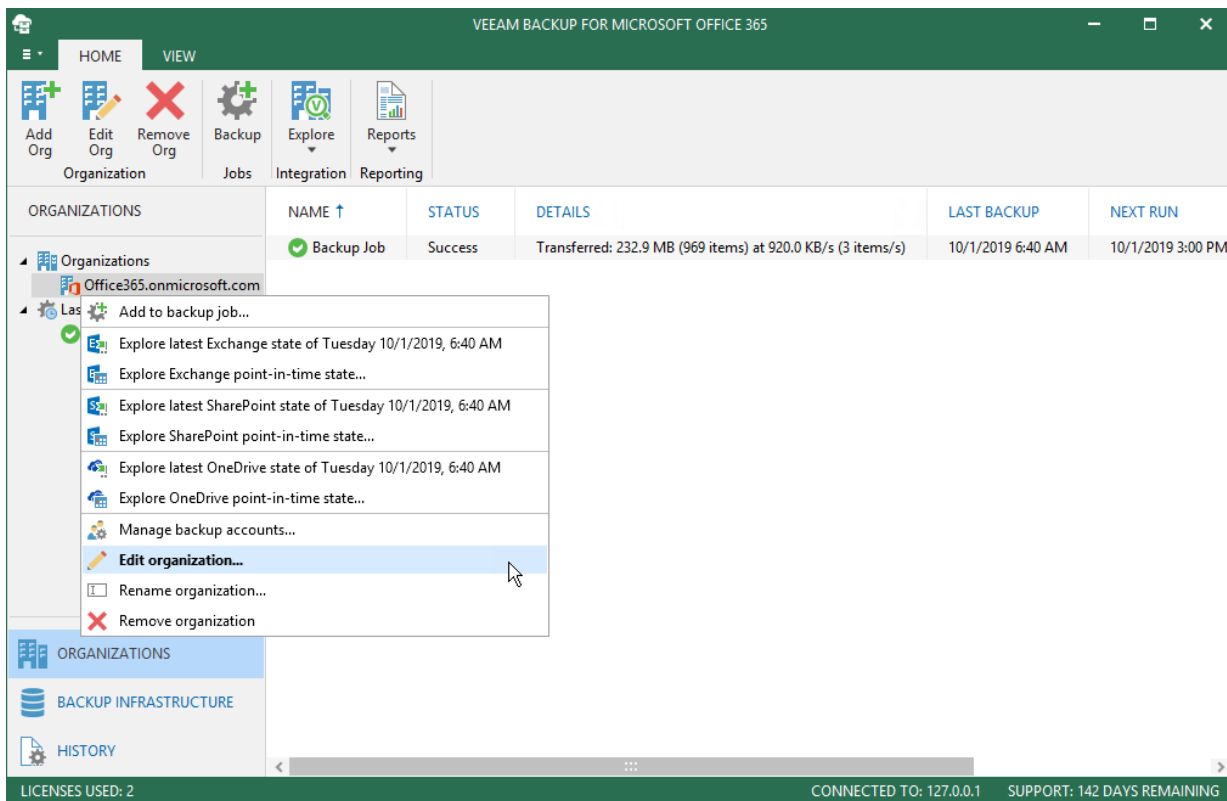
Consider that you cannot change *Microsoft Office 365* organization deployment type to the *On-premises* type.

- User name and/or password.

To edit organization parameters, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select an organization.
3. On the **Home** tab, click **Edit Org** on the ribbon.

Alternatively, in the inventory pane, right-click an organization and select **Edit organization**.

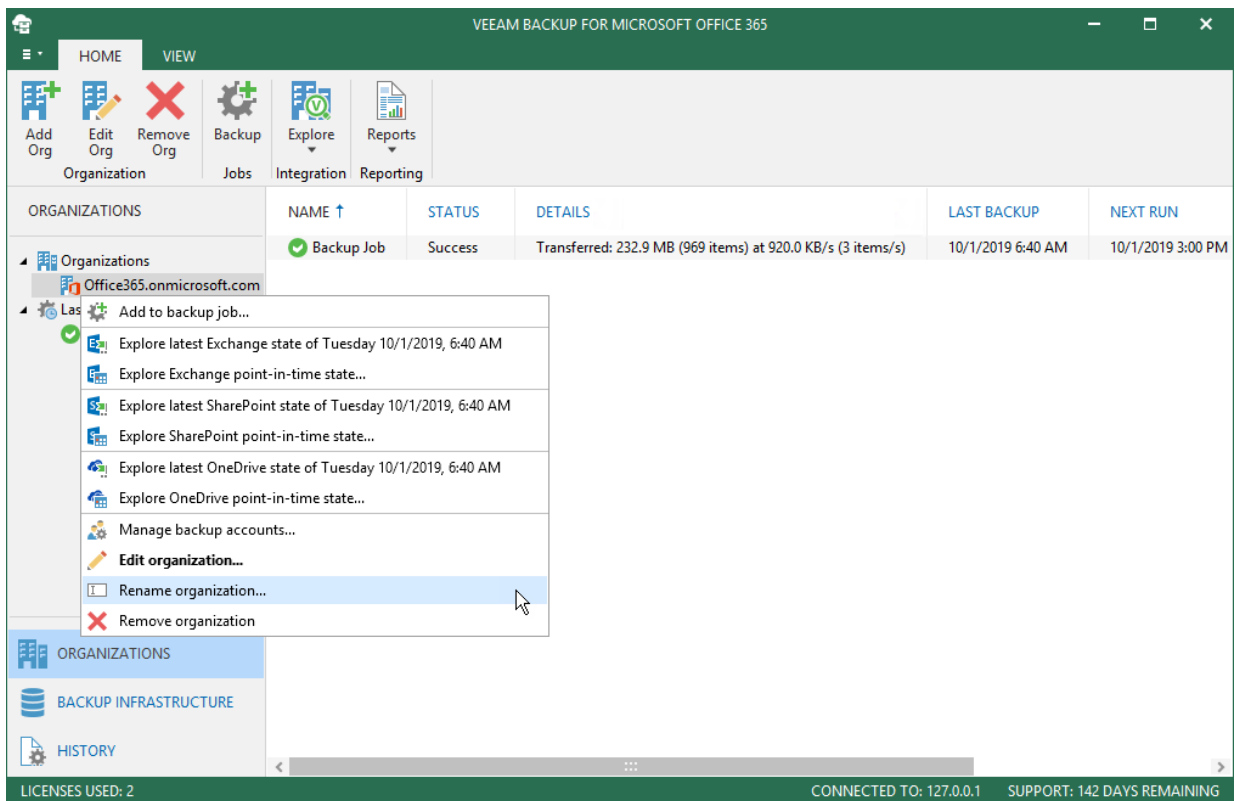


Renaming Organizations

You can rename your Microsoft Office 365 and on-premises Microsoft organizations in the Veeam Backup for Microsoft Office 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, select either 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 and click **Rename**.

Consider that when creating a [Mailbox Protection Reports](#), organizations will be shown with their original names.

RENAME ORGANIZATION

×

Specify organization name

Specify organization name to use in Veeam Backup for Microsoft Office 365:

☐ Use the default name (beta)

☒ Use the following name:

On-Premises Microsoft SharePoint

Back

Rename

Cancel

Removing Organizations

You can remove an organization from the Veeam Backup for Microsoft Office 365 console if you no longer need it.

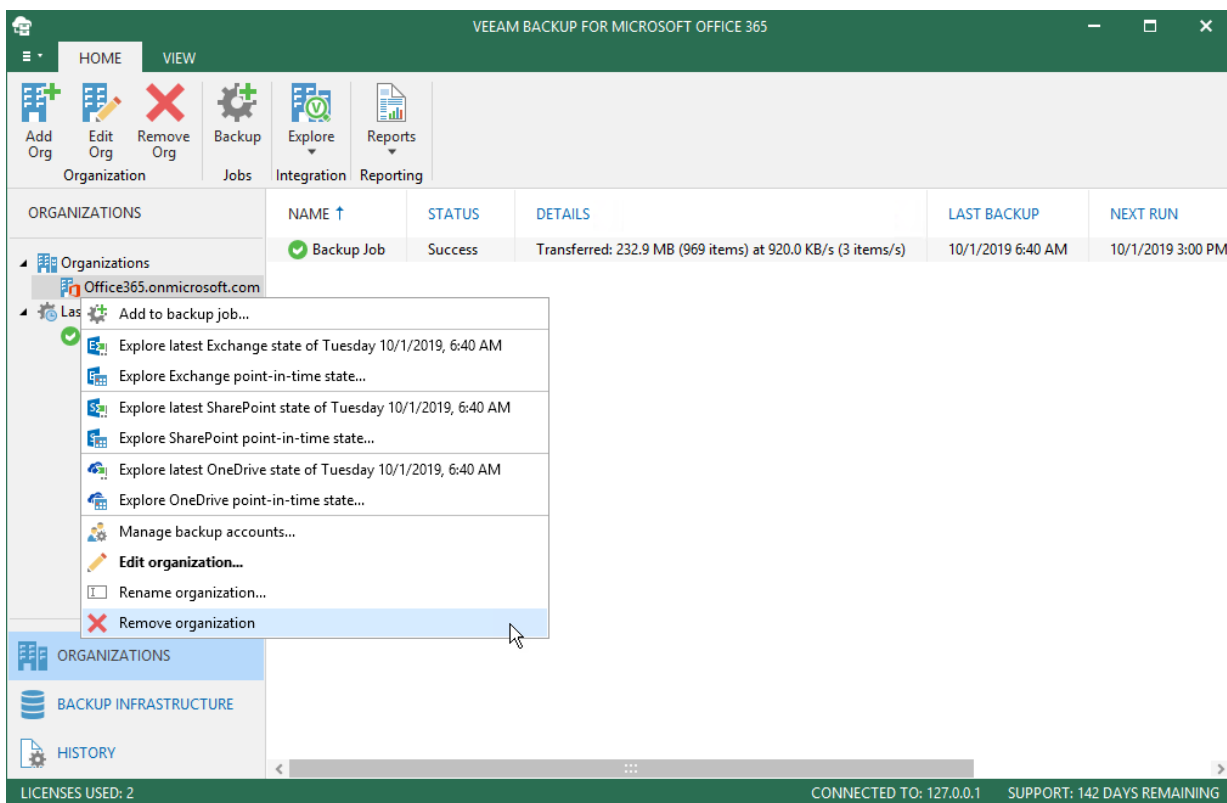
Consider the following:

- When removing an organization, its backups will not be removed.
- Backup jobs configured for the organization that you are removing will be permanently deleted.

To remove an organization, do the following:

1. Open the **Organizations** view.
2. In the preview pane, select an organization.
3. On the **Home** tab, click **Remove Org** on the ribbon.

Alternatively, in the inventory pane, right-click an organization and select **Remove organization**.



Data Backup

To back up data of your [Office 365 and on-premises organizations](#), you use backup jobs.

A backup job is a set of configuration parameters that define a list of users, groups, sites and organizations to back up, a location where to store backups, a schedule according to which new backups must be created and so on.

Organization Object Types

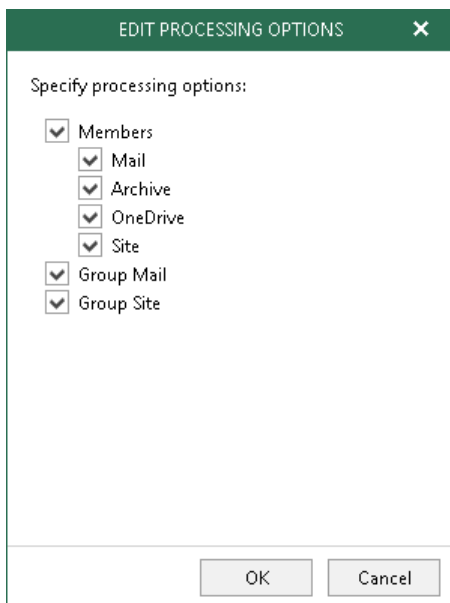
This section explains object types and their processing and exclusion options that you can select when creating and configuring backup jobs.

The following object types are available:

- **Groups**
Consists of Office 365 groups (available only in Microsoft Office 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.
- **Organizations**
Consists of organization objects and their processing options.

Each of these object types consists of a set of processing/exclusion options such as **Mail**, **Archive**, **OneDrive**, **Site**, **Group Mail** and **Group Site** which you can select/deselect to make data retrieval even more precise.

Processing and exclusion options can be selected at the [Select Objects to Backup](#) and [Select Objects to Exclude](#) steps respectively.



EDIT PROCESSING OPTIONS

Specify processing options:

- ☒ Members
 - ☒ Mail
 - ☒ Archive
 - ☒ OneDrive
 - ☒ Site
- ☒ Group Mail
- ☒ Group Site

OK Cancel

Groups

The following table lists available *Group* types and their processing/exclusion options.

Group Type	Microsoft Office 365 Organizations	On-premises Microsoft Exchange Organizations
O365 group (available only in Office 365 organizations)	When configuring Office 365 organizations, the following set of processing/exclusion options is available: <ul style="list-style-type: none"> Members with <i>Mail</i>, <i>Archive</i>, <i>OneDrive</i> and <i>Site</i> <i>Group Mail</i> <i>Group Site</i> 	N/A
Security Group	Members with <i>Mail</i> , <i>Archive</i> , <i>OneDrive</i> and <i>Site</i>	Members with <i>Mail</i> and <i>Archive</i> options
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.

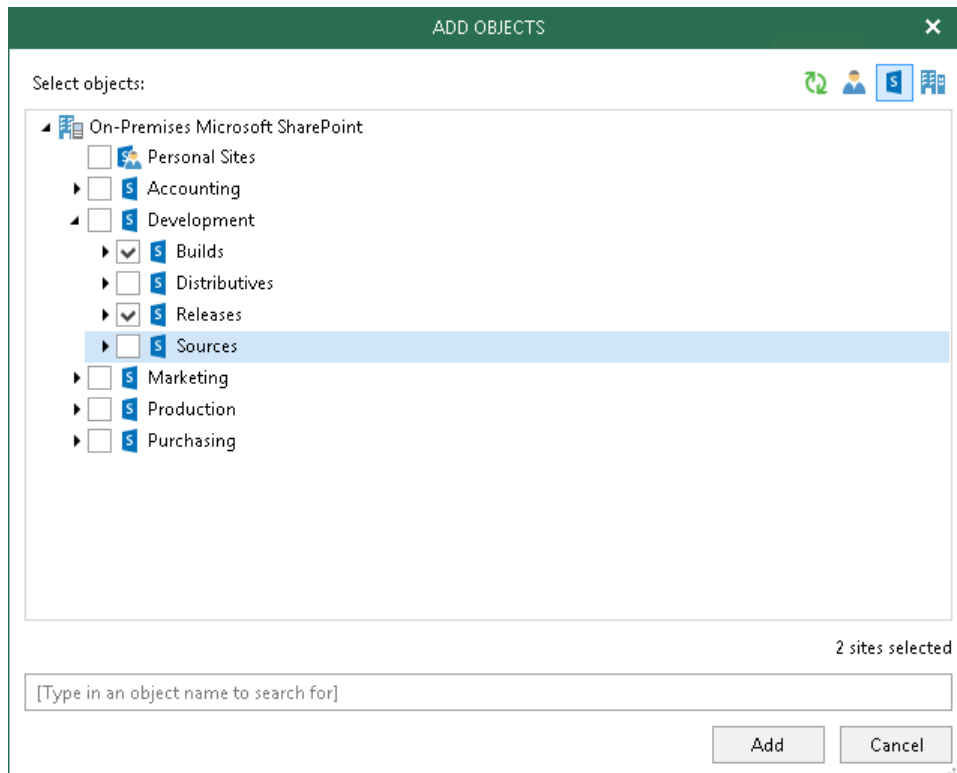
User Type	Microsoft Office 365 Organizations	On-premises Microsoft Exchange Organizations	On-premises Microsoft SharePoint Organizations
User	<i>Mail</i> , <i>Archive</i> , <i>OneDrive</i> and <i>Site</i>	<i>Mail</i> and <i>Archive</i>	<i>OneDrive</i> and <i>Site</i>
Shared mailbox (available only in Office 365 and Exchange organizations)			N/A
Public mailbox (available only in Office 365 and Exchange organizations)			

Sites

Consider the following:

- Objects of this type do not have any processing/exclusion options.
- Objects of this type are not available in on-premises Microsoft Exchange organizations.
- 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 be deselected.



Organizations

The following table lists processing/exclusion options available for *Organization* types.

Microsoft Office 365 Organizations	On-premises Microsoft Exchange Organizations	On-premises Microsoft SharePoint Organizations
<i>Mail, Archive, OneDrive and Site</i>	<i>Mail and Archive</i>	<i>OneDrive and Site</i>

Creating Backup Job

To create a backup job, do the following:

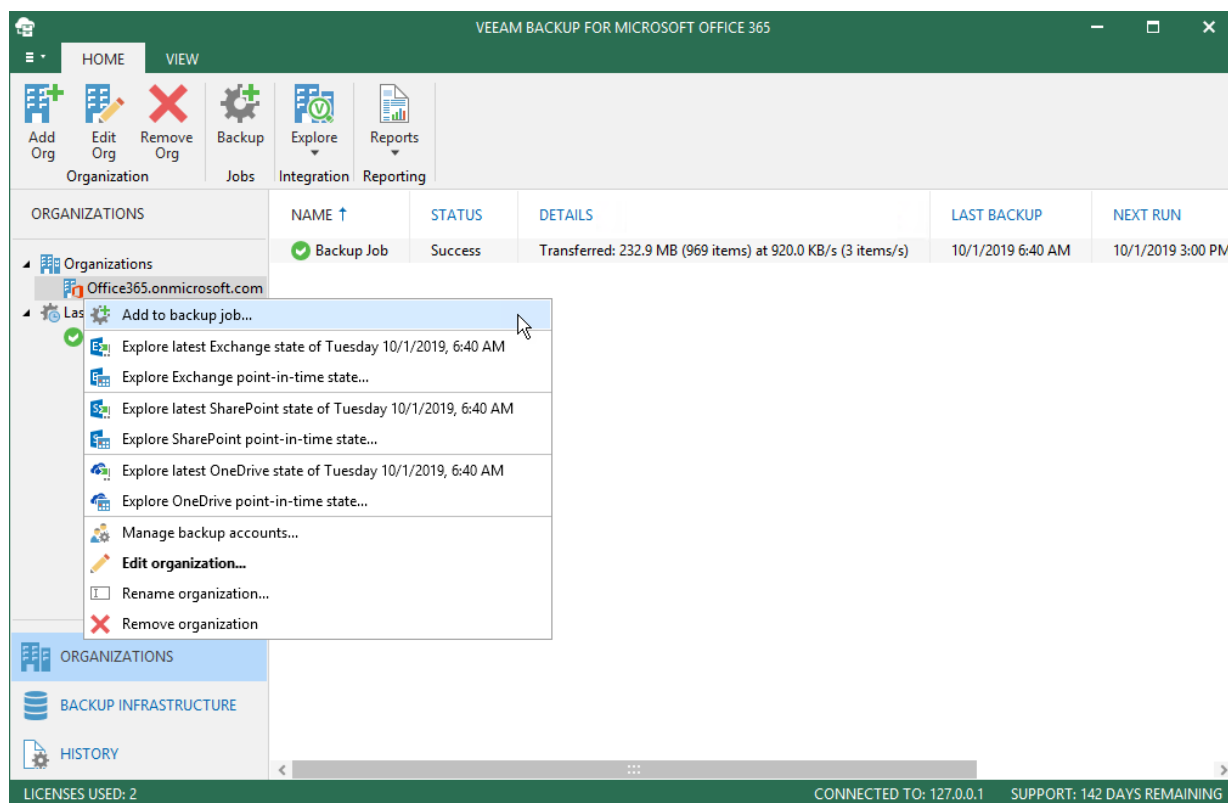
1. [Launch the New Backup Job wizard.](#)
2. [Specify a backup job name.](#)
3. [Select objects to back up.](#)
4. [Select objects to exclude.](#)
5. [Specify a backup proxy and repository.](#)
6. [Specify scheduling options.](#)

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 to back up.
3. On the **Home** tab, click **Backup** on the ribbon.

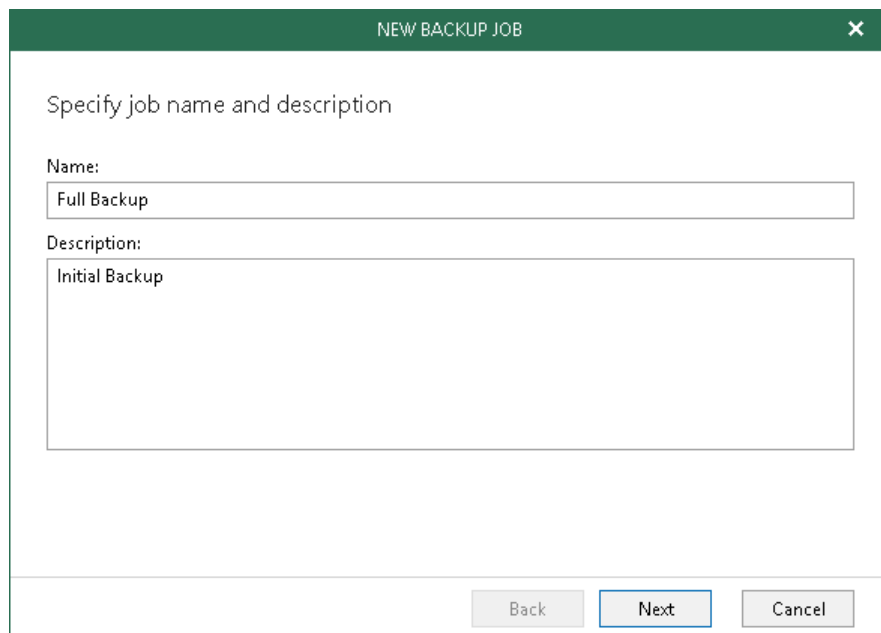
Alternatively, in the inventory pane, right-click an organization and select **Add to backup job**.



Step 2. Specify Backup Job Name

At this step of the wizard, specify a name and description for the backup job.

1. In the **Name** field, enter a new name for the backup job.
2. In the **Description** field, enter a description (optional).



NEW BACKUP JOB

Specify job name and description

Name:
Full Backup

Description:
Initial Backup

Back Next Cancel

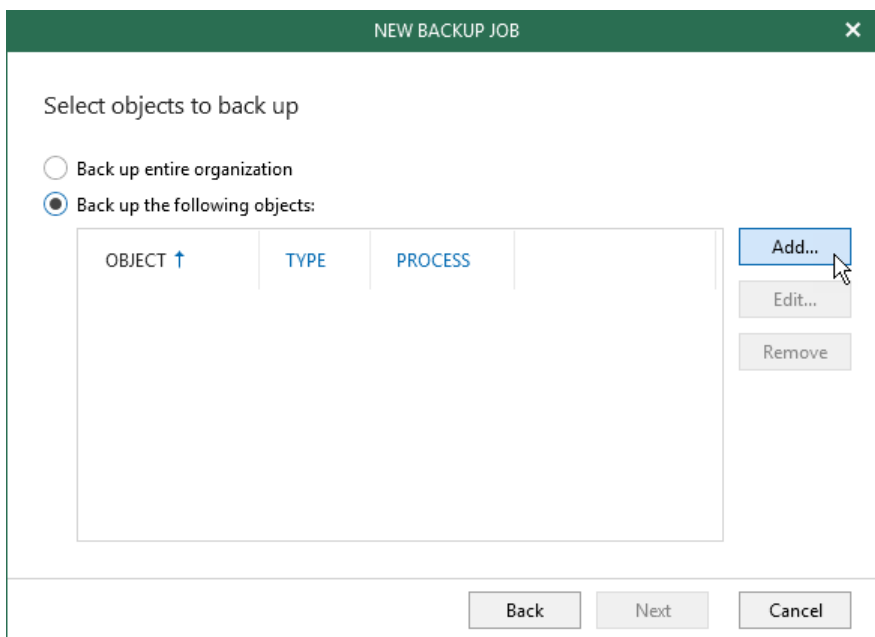
Step 3. Select Objects to Back Up

At this step of the wizard, select objects that you want to back up.

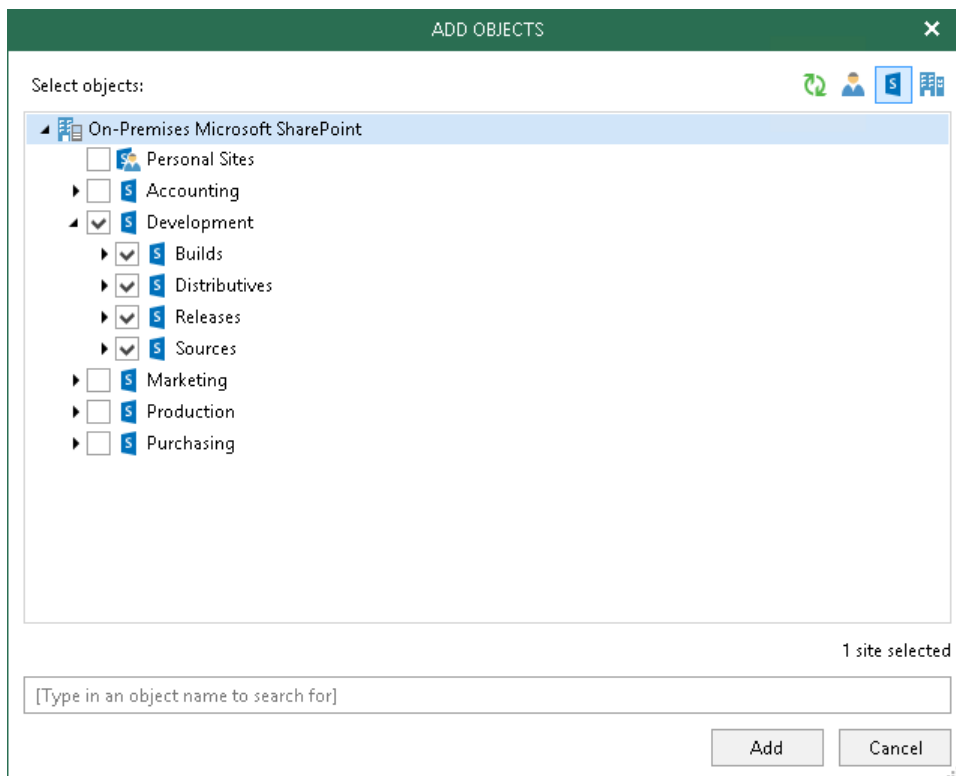
In Veeam Backup for Microsoft Office 365, you can select to back up an entire organization or specify users, sites, groups and organizations.

To select objects to back up, do the following:

1. Select the **Backup the following objects** option.
2. Click **Add**.



3. In the **Add Objects** window, select users, groups, sites and organizations that you want to back up.
To add objects of different types, use the switch group in the upper-right corner.
To quickly find necessary objects, use the search field at the bottom.
4. Click **Add**.



NOTE:

Mind the following:

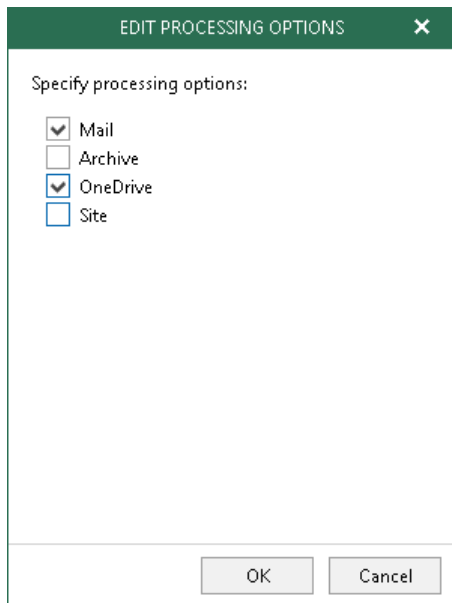
- You can create only one entire organization backup job per organization.
- Objects that are already processed by any of your backup jobs will be skipped from the entire organization processing list.
- Due to possible access limitations some *Sites* objects might be unavailable.
- Due to Microsoft limitations, you cannot add the following objects for [Microsoft Office 365 organizations](#) with enabled [security defaults](#): *Discovery Search Mailboxes*, *Public Folder Mailboxes* and *Dynamic Distribution Groups*.
- When you add an *Organization* object type, [processing options](#) are applied to all users, groups and sites in the selected organization.

4. If you want to specify processing options, select an object in the table, click **Edit** and in the **Edit Processing Options** window, select options that you need.

For more information about available object types and their processing options, see [Organization Object Types](#).

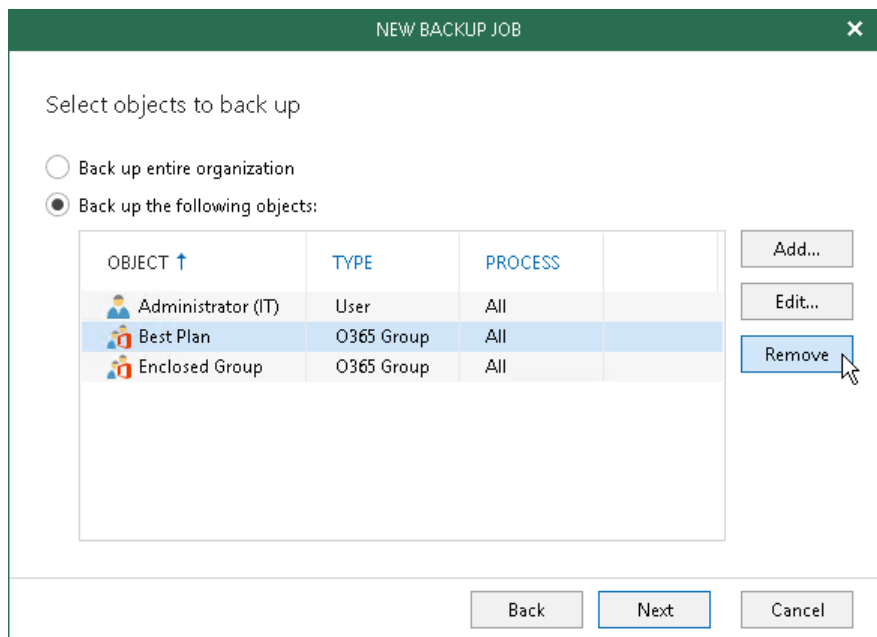
NOTE:

You cannot edit processing options of the *Sites* and *Public Mailbox* objects.



The dialog box titled "EDIT PROCESSING OPTIONS" has a close button (X) in the top right corner. Below the title bar, it says "Specify processing options:". There are four checkboxes: "Mail" (checked), "Archive" (unchecked), "OneDrive" (checked), and "Site" (unchecked). At the bottom, there are "OK" and "Cancel" buttons.

To remove an object from the list, select it and click **Remove**.



The dialog box titled "NEW BACKUP JOB" has a close button (X) in the top right corner. Below the title bar, it says "Select objects to back up". There are two radio buttons: "Back up entire organization" (unchecked) and "Back up the following objects:" (checked). Below the radio buttons is a table with three columns: "OBJECT", "TYPE", and "PROCESS". The table has three rows: "Administrator (IT)" (User, All), "Best Plan" (O365 Group, All), and "Enclosed Group" (O365 Group, All). To the right of the table are three buttons: "Add...", "Edit...", and "Remove". A mouse cursor is pointing at the "Remove" button. At the bottom of the dialog box are three buttons: "Back", "Next", and "Cancel".

OBJECT	TYPE	PROCESS
Administrator (IT)	User	All
Best Plan	O365 Group	All
Enclosed Group	O365 Group	All

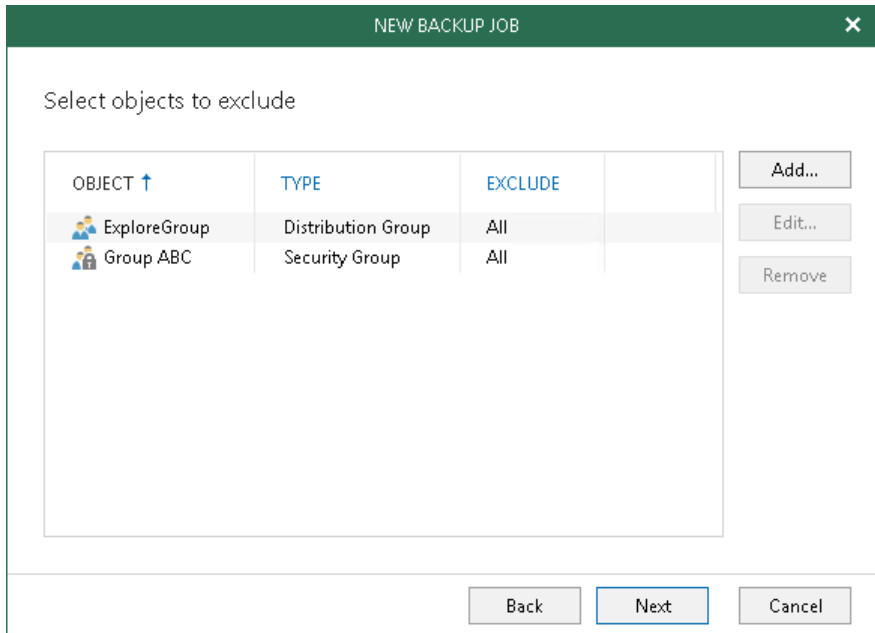
Step 4. Select Objects to Exclude

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 and sites that you do not want to back up.

NOTE:

Due to Microsoft limitations, Veeam Backup for Microsoft Office 365 does not back up the following objects for [Microsoft Office 365 organizations](#) with enabled [security defaults](#): *Discovery Search Mailboxes*, *Public Folder Mailboxes* and *Dynamic Distribution Groups*.



OBJECT ↑	TYPE	EXCLUDE
ExploreGroup	Distribution Group	All
Group ABC	Security Group	All

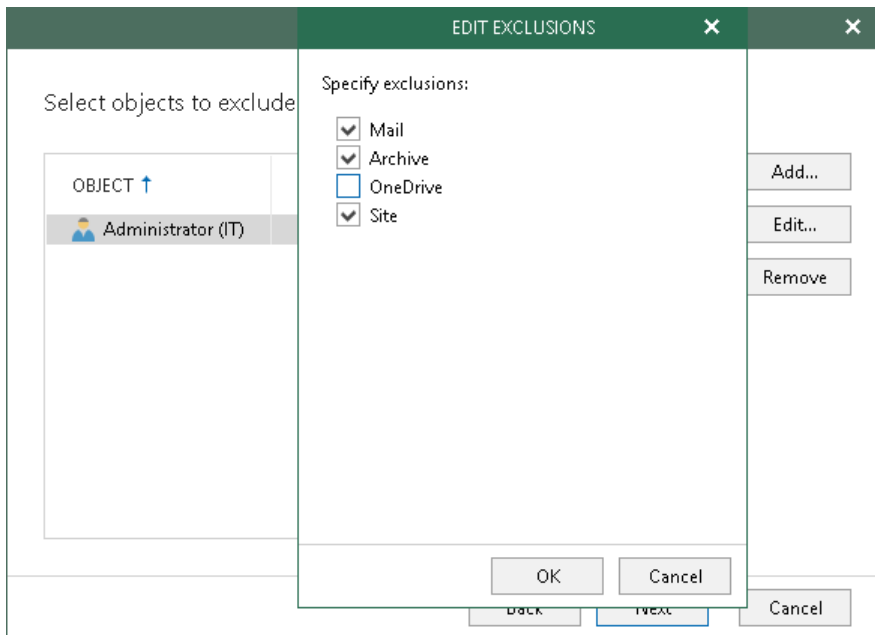
If you want to specify exclusion options, select an object in the table, click **Edit** and in the **Edit Processing Options** window, select options that you need.

For more information about available object types and their exclusion options, see [Organization Object Types](#).

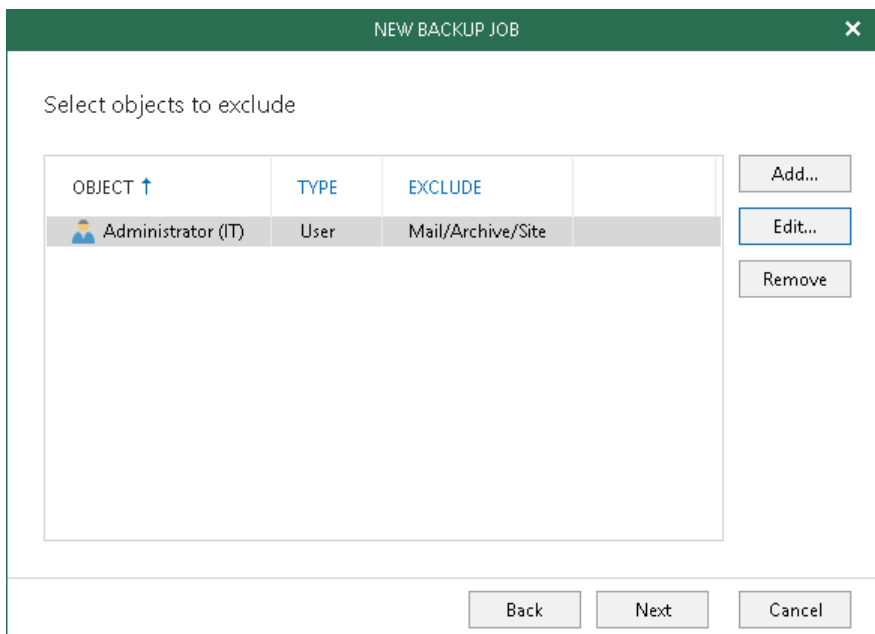
NOTE:

You cannot edit exclusion options of the *Sites* and *Public Mailbox* object types.

The following is an example where the *Mail*, *Archive* and *Site* objects are excluded from the backup for the *Administrator (IT)* user; Veeam Backup for Microsoft Office 365 will only back up OneDrive data for this user.



To see what objects are excluded, refer to the **Exclude** column. As per example, the excluded objects are *Mail*, *Archive* and *Site*.



Step 5. Specify Backup Proxy and Repository

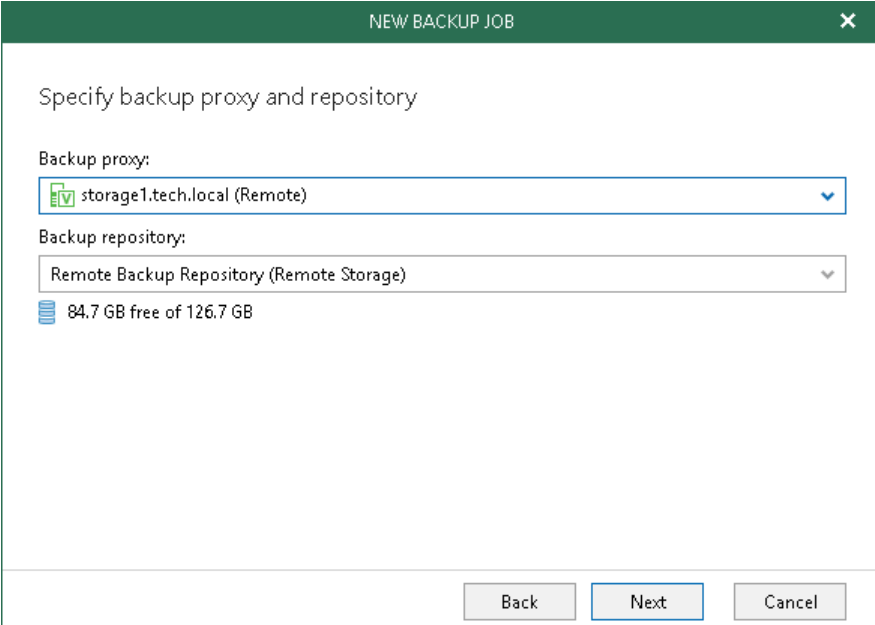
At this step of the wizard, specify a [backup proxy server](#) that you want to use to process data during a backup session and a [backup repository](#) where you want to keep your backups.

To specify a backup proxy server and backup repository, do the following:

1. From the **Backup proxy** drop-down, select a backup proxy server that you want to use to process data during a backup session.
2. From the **Backup repository** drop-down, select a backup repository to which you want to save your data.

You can select a standard backup repository or backup repository that was [extended with object storage](#).

When selecting a backup repository that was extended with object storage, all data will be compressed and backed up directly to object storage; Veeam Backup for Microsoft Office 365 saves only [cache](#) to the extended backup repository.



The screenshot shows a window titled "NEW BACKUP JOB" with a close button (X) in the top right corner. The main heading is "Specify backup proxy and repository".

Under "Backup proxy:", there is a dropdown menu with a green icon and the text "storage1.tech.local (Remote)".

Under "Backup repository:", there is a dropdown menu with the text "Remote Backup Repository (Remote Storage)". Below this dropdown, it says "84.7 GB free of 126.7 GB".

At the bottom of the window, there are three buttons: "Back", "Next" (which is highlighted with a blue border), and "Cancel".

Step 6. Specify Scheduling Options

At this step of the wizard, configure a schedule for the backup job.

To configure a schedule, do the following:

1. Select the **Run the job automatically** check box and customize a schedule for your backup job.

You can select:

- **Daily at this time**

Select this option if you want to run the job daily at the specified hours.

- **Periodically every**

Select this option if you want to run the job every *N* minutes.

2. Select the **Retry failed objects processing** check box and specify the maximum number of retry attempts. You can also set an interval before attempting subsequent retries.
3. Select the **Terminate 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. Select the **Start the job when I click Create** check box if you want to start a backup job upon 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](#).

The screenshot shows the 'NEW BACKUP JOB' dialog box with the title bar in green. The main area is titled 'Select scheduling options'. It contains several settings:

- ☒ Run the job automatically
 - ☒ Daily at this time: 2:00 PM (dropdown), Everyday (dropdown)
 - ☐ Periodically every: 5 minutes (dropdown)
- ☒ Retry failed objects processing: 3 (spinner) times
 - Wait before each retry attempt for: 10 (spinner) minutes
- ☒ Terminate the job if it exceeds allowed backup window [Window... button]
- ☒ Start the job when I click Create

At the bottom are three buttons: 'Back' (highlighted with a blue border), 'Create', and 'Cancel'.

Selecting Time Periods

When you click **Window**, the **Time Period** 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.

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:

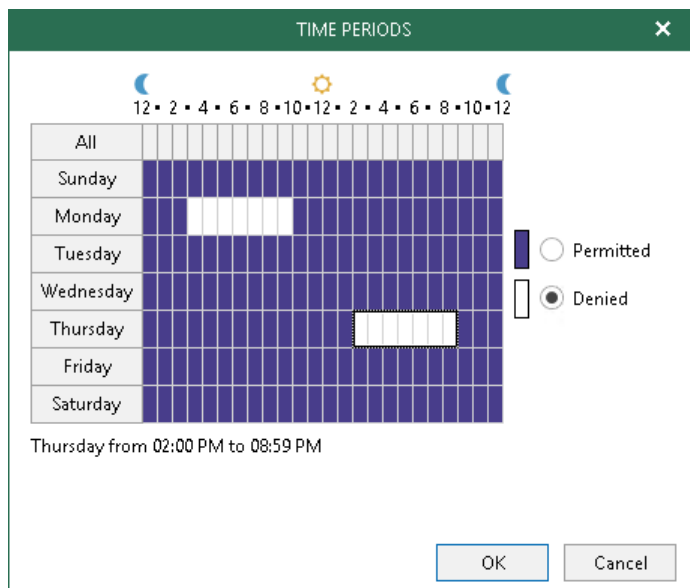
1. Select a block that corresponds to the day of the week (vertical axis) and to the time interval (horizontal axis) on which you want to allow or prohibit the execution of a backup job.

In addition, you can:

- 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.
 - Click a day of the week in the vertical axis to select all the blocks of the day thereof.
 - 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

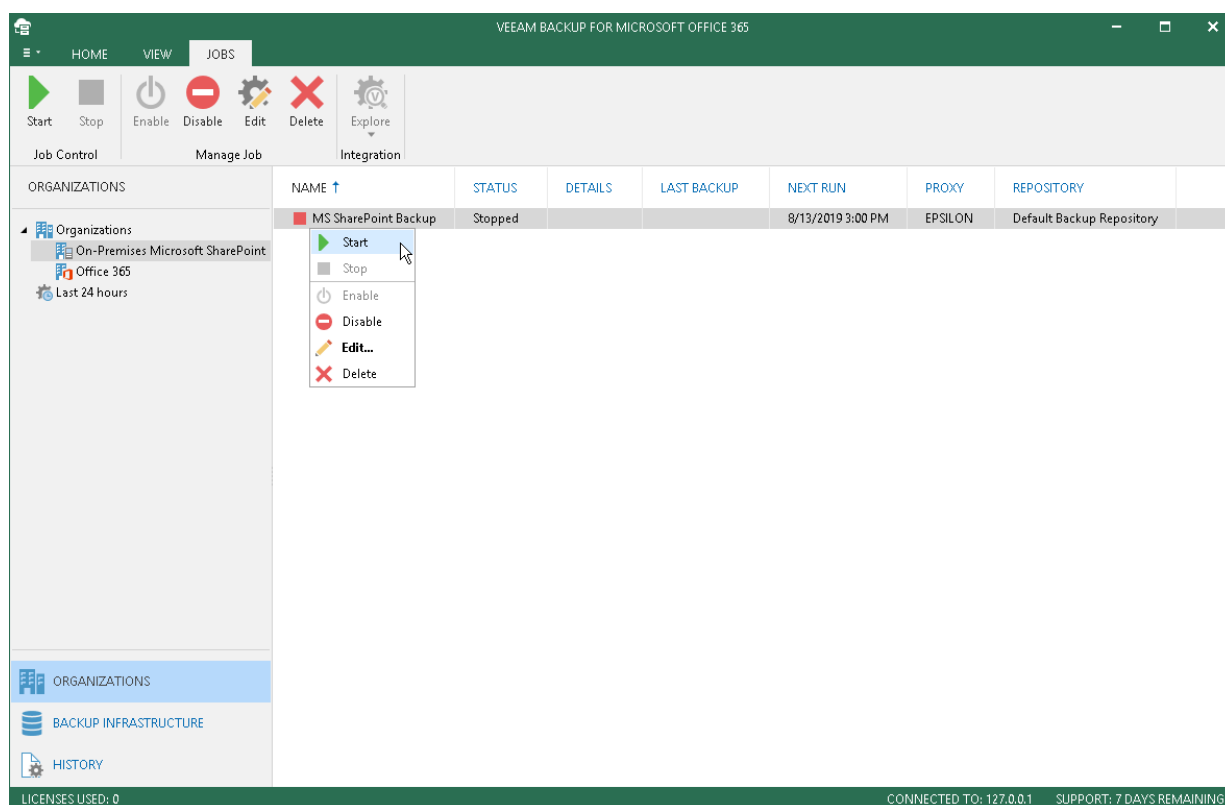
You can manage backup jobs that you created in Veeam Backup for Microsoft Office 365. You can edit the settings of a backup job, start, stop, disable, remove backup jobs, and so on.

Starting Backup Job

To start a backup job, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select an organization.
Select the root **Organizations** node to see backup jobs of every organization added to the scope.
3. In the preview pane, select a backup job.
4. On the **Jobs** tab, click **Start** on the ribbon.

Alternatively, in the preview pane, right-click a backup job and select **Start**.

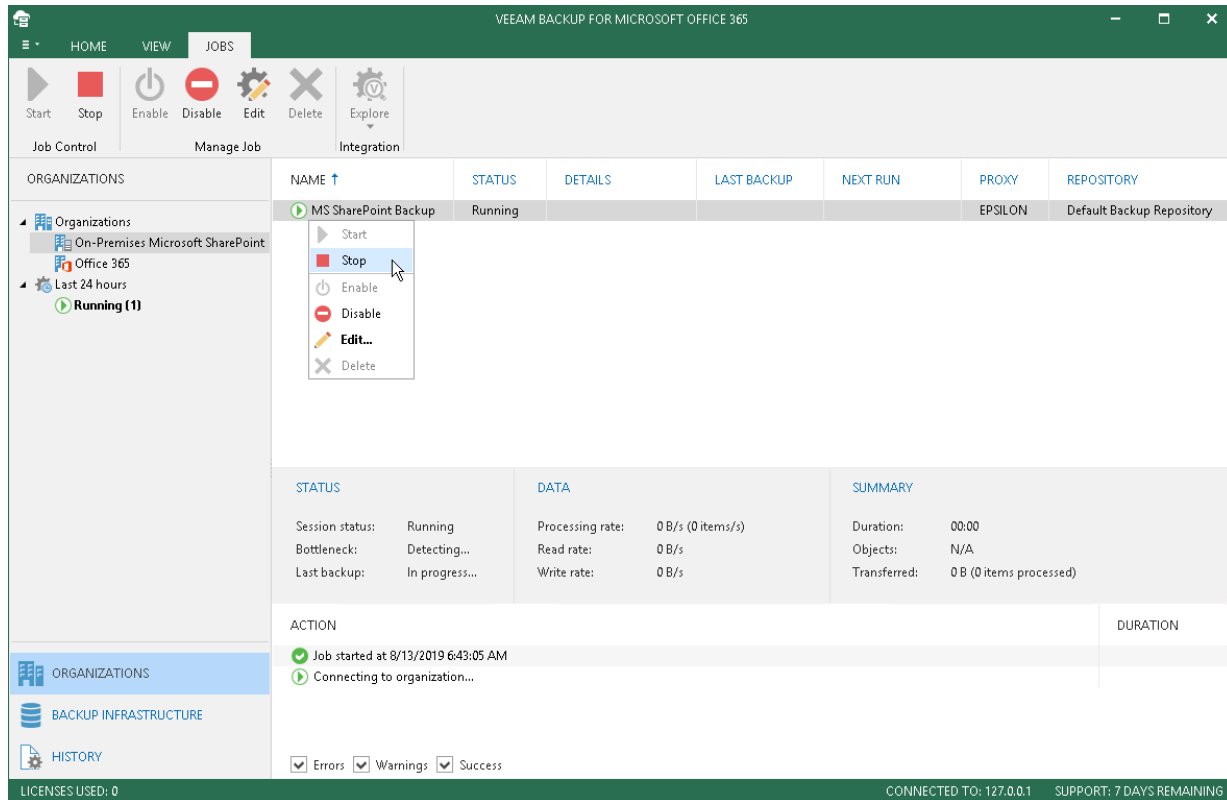


Stopping Backup Job

When Veeam Backup for Microsoft Office 365 stops a backup job, it freezes the current backup state preserving what has already been backed up so that you can continue where you left off. To continue, use the **Start** command, as described in [Starting Backup Job](#).

To stop a backup job, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select an organization.
Select the root **Organizations** node to see backup jobs of every organization added to the scope.
3. In the preview pane, select a backup job.
4. On the **Jobs** tab, click **Stop** on the ribbon.
Alternatively, in the preview pane, right-click a backup job and select **Stop**.



Enabling/Disabling Backup Job

This section explains how to enable or disable a backup job.

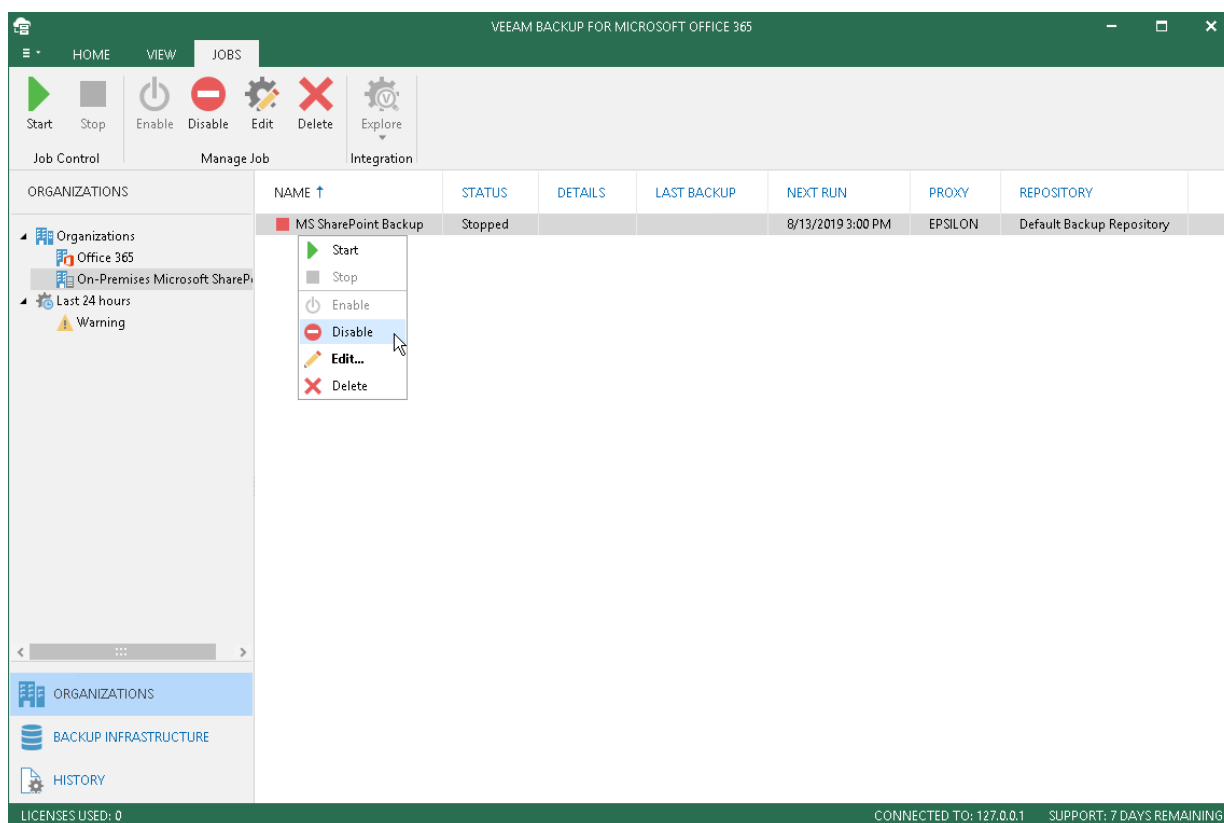
Consider the following:

- 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 can be executed manually, using the **Start** command.

To enable or disable a backup job, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select an organization.
Select the root **Organizations** node to see backup jobs of every organization added to the scope.
3. In the preview pane, select a backup job.
4. On the **Jobs** tab, click **Enable/Disable** on the ribbon.

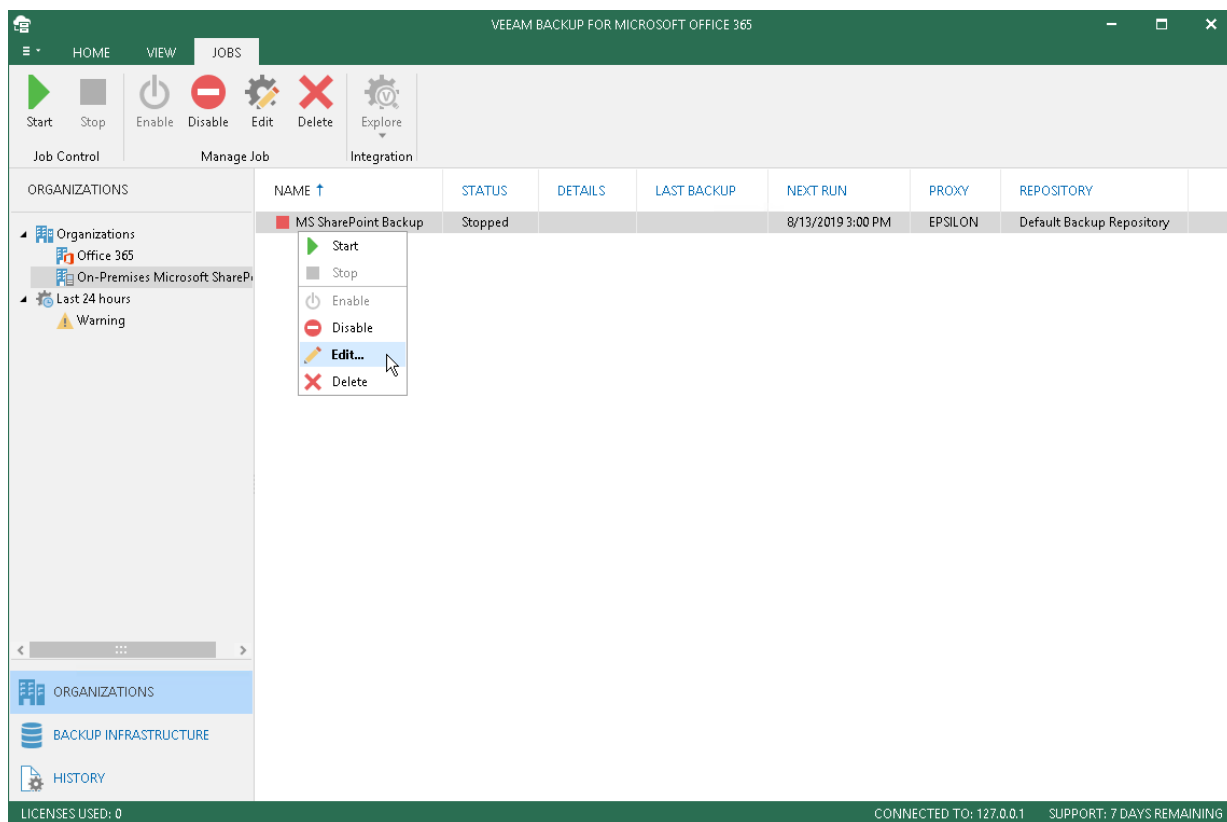
Alternatively, in the preview pane, right-click a backup job and select **Enable/Disable**.



Editing Backup Job Settings

To edit settings a backup job, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select an organization.
Select the root **Organizations** node to see backup jobs of every organization added to the scope.
3. In the preview pane, select a backup job.
4. On the **Jobs** tab, click **Edit** on the ribbon.
Alternatively, in the preview pane, right-click a backup job and select **Edit**.
5. Modify settings as required.



Removing Backup Job

This section explains how remove a backup job from the Veeam Backup for Microsoft Office 365 configuration.

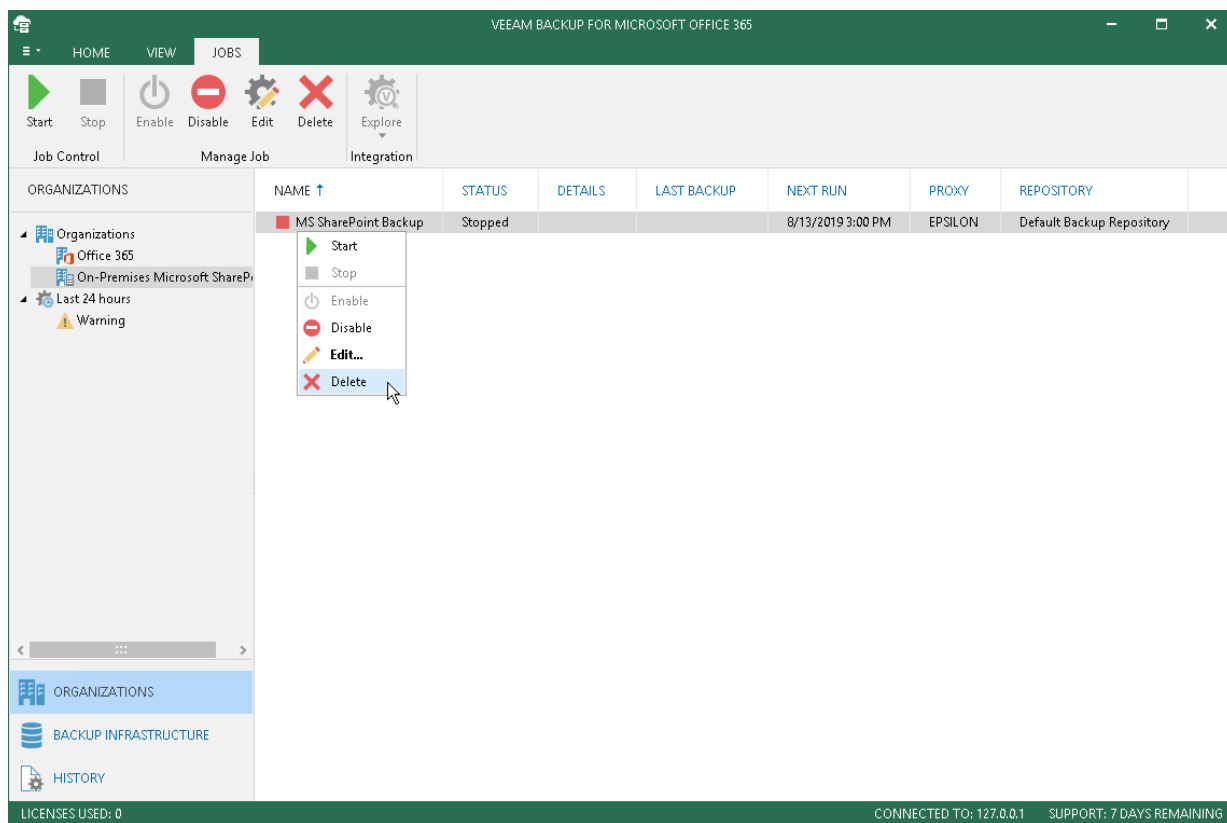
NOTE:

Consider that when removing a backup job from the configuration, the backup data will not be removed.

To remove a backup job from the Veeam Backup for Microsoft Office 365 configuration, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select an organization.
Select the root **Organizations** node to see backup jobs of every organization added to the scope.
3. In the preview pane, select a backup job.
4. On the **Jobs** tab, click **Remove** on the ribbon.

Alternatively, in the preview pane, right-click a backup job and select **Remove**.



Exploring Backup Job

To open backups created by Veeam Backup for Microsoft Office 365, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select an organization.
Select the root **Organizations** node to see the backup jobs of each organization added to the scope.
3. In the preview pane, select a backup job.
4. On the **Jobs** tab, click **Explore** on the ribbon and select **Explore latest <product> state of <date_and_time>** or **Explore <product> point-in-time state**.

Alternatively, in the preview pane, right-click a backup job and select **Explore latest <product> state of <date_and_time>** or **Explore <product> point-in-time state**.

5. Proceed to [Data Restore](#).

The screenshot displays the Veeam Backup for Microsoft Office 365 software interface. The top navigation bar includes 'HOME', 'VIEW', and 'JOBS' tabs, with 'JOBS' currently selected. Below the navigation bar is a ribbon with buttons for 'Start', 'Stop', 'Enable', 'Disable', 'Edit', 'Delete', and 'Explore'. The main area is divided into three panes. The left pane, titled 'ORGANIZATIONS', shows a tree view with 'Organizations' expanded, listing 'Office365.onmicrosoft.com', 'On-Premises Microsoft Exchange', and 'On-Premises Microsoft SharePoint'. The middle pane shows a table of backup jobs. The first job, 'Primary Backup', is selected, and a context menu is open over it, showing options like 'Start', 'Stop', 'Explore latest Exchange state of Wednesday 10/23/2019, 12:46 AM', 'Explore Exchange point-in-time state...', 'Explore latest SharePoint state of Wednesday 10/23/2019, 12:46 AM', 'Explore SharePoint point-in-time state...', 'Explore latest OneDrive state of Wednesday 10/23/2019, 12:46 AM', 'Explore OneDrive point-in-time state...', 'Enable', 'Disable', 'Edit...', and 'Delete'. The right pane shows a 'SUMMARY' section with details: Duration: 07:49, Objects: 3 of 3, Transferred: 247.8 MB (998 items processed). At the bottom, there is an 'ACTION' section with a list of events: 'Job started at 10/23/2019 12:38:16 AM', 'Connected to organization', 'No excluded objects found', and 'Found 3 objects'. The bottom status bar shows 'LICENSES USED: 2', 'CONNECTED TO: 127.0.0.1', and 'SUPPORT: 120 DAYS REMAINING'.

NAME	STATUS	DETAILS	LAST BACKUP	NEXT RUN	PROXY
Primary Backup	Success	Transferred: 247.8 MB (998 items) at 543....	10/23/2019 12:46 AM	10/23/2019 3:00 PM	EPSILON

ACTION	DURATION
Job started at 10/23/2019 12:38:16 AM	
Connected to organization	
No excluded objects found	
Found 3 objects	00:15

Upgrading Backup Job

After you install a new version of Veeam Backup for Microsoft Office 365, the existing backup jobs that were created with version 2.0 and have more than 20 Microsoft SharePoint sites must be upgraded manually.

To upgrade backup jobs, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select the **Out of Date** node.
3. In the preview pane, select a backup job.
4. On the **Jobs** tab, click **Upgrade** on the ribbon.

Alternatively, in the preview pane, right-click a backup job and select **Upgrade**.

The screenshot displays the Veeam Backup for Microsoft Office 365 application window. The 'JOBS' tab is active, showing a list of backup jobs. The 'On-Premises Exchange' job is selected, and its context menu is open, with the 'Upgrade...' option highlighted. The job's status is 'Success', and it is marked as 'Out of Date (1)'. The interface includes a ribbon with various job control and management options, and a detailed preview pane showing job statistics and a log of actions.

NAME	STATUS	DETAILS	LAST BACKUP	NEXT RUN	PROXY	REPOSITORY
On-Premises Exchange	Success			<Disabled>	EPSILON	Default Backup Repository

STATUS	DATA	SUMMARY
Session status: Success	Processing rate: 2.4 KB/s (0 items/s)	Duration: 14 seconds
Bottleneck: Source	Read rate: 16.4 KB/s	Objects: 1 of 1
Last backup: Never	Write rate: 103.5 KB/s	Transferred: 35.3 KB (3 items processed)

ACTION	DURATION
Job started at 12/29/2018 4:12:52 AM	
Connected to organization	
Found 1 mailboxes	

Errors: ☒ Warnings: ☒ Success: ☒

LICENSES USED: 0 CONNECTED TO: 127.0.0.1 SUPPORT: 20 DAYS REMAINING

Data Restore

To restore data, you can use the abilities of Veeam Explorers, as described in:

- [Veeam Explorer for Microsoft Exchange](#)
To explore and recover Microsoft Exchange mailboxes, folders, messages, tasks, contacts and items.
- [Veeam Explorer for Microsoft SharePoint](#)
To explore and recover Microsoft SharePoint sites, libraries and items.
- [Veeam Explorer for Microsoft OneDrive for Business](#)
To explore and recover Microsoft OneDrive for Business items and folders.

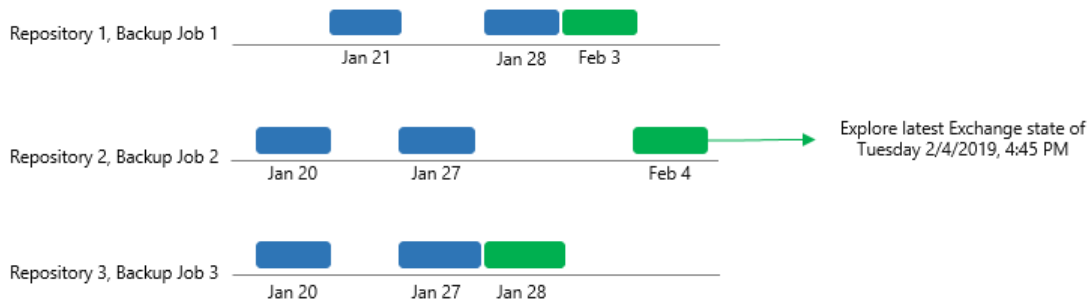
To launch Veeam Explorers, use the **Explore** option, as described in the following sections:

- [Exploring Backup Jobs](#)
To open backups created by the selected backup job.
- [Exploring Single Organization](#)
To open backups created by all backup jobs of the selected organization.
- [Exploring All Organizations](#)
To open backups of all organizations.

Exploring Backup Jobs

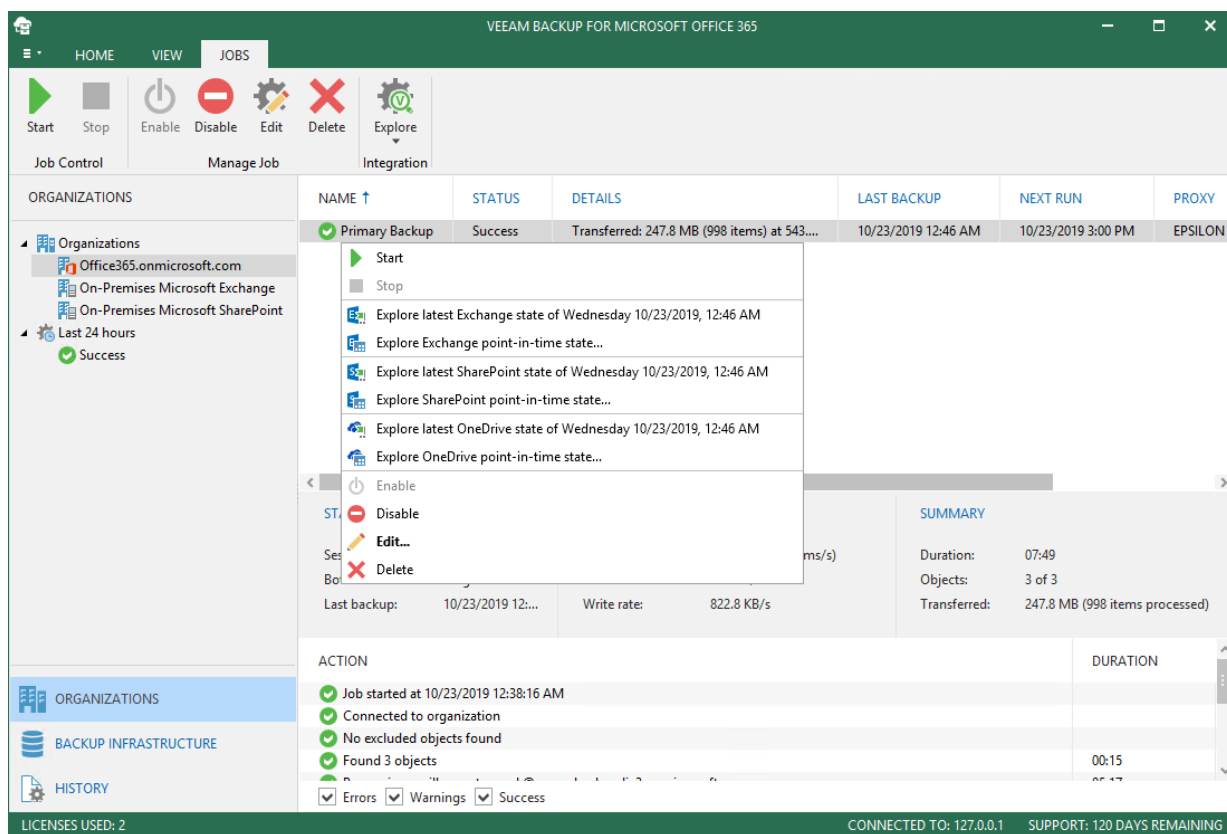
When exploring backup jobs, Veeam Backup for Microsoft Office 365 loads the latest restore point that was created by the selected job.

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 Office 365 loads only the latest one (created on February 4) into the Veeam Explorer 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 that contains backups that you want to open.
3. In the preview pane, select a backup job and click **Explore** on the ribbon, or right-click a backup job and select either of the following options:
 - a) **Explore latest <Product> state of <date_and_time>**. To explore the latest backup state.
 - b) **Explore point-in-time state**. To select a point-in-time state. For more information, see [Exploring Point-In-Time](#).



Exploring Single Organization

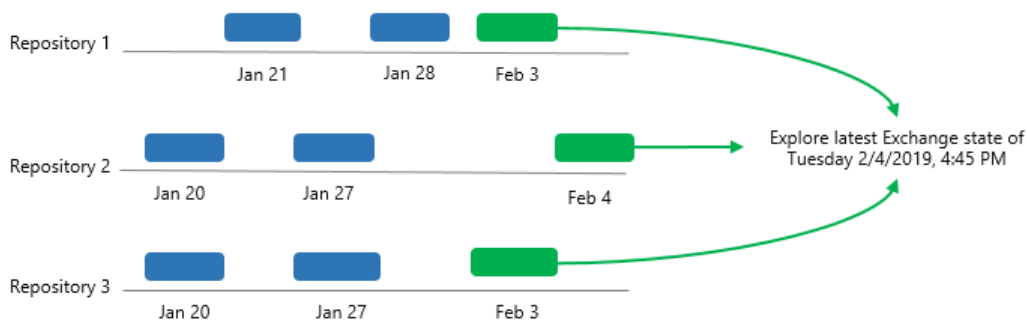
When exploring a single organization, Veeam Backup for Microsoft Office 365 merges and loads the latest restore points that have been created by each backup job of the selected organization.

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 Explorer 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.

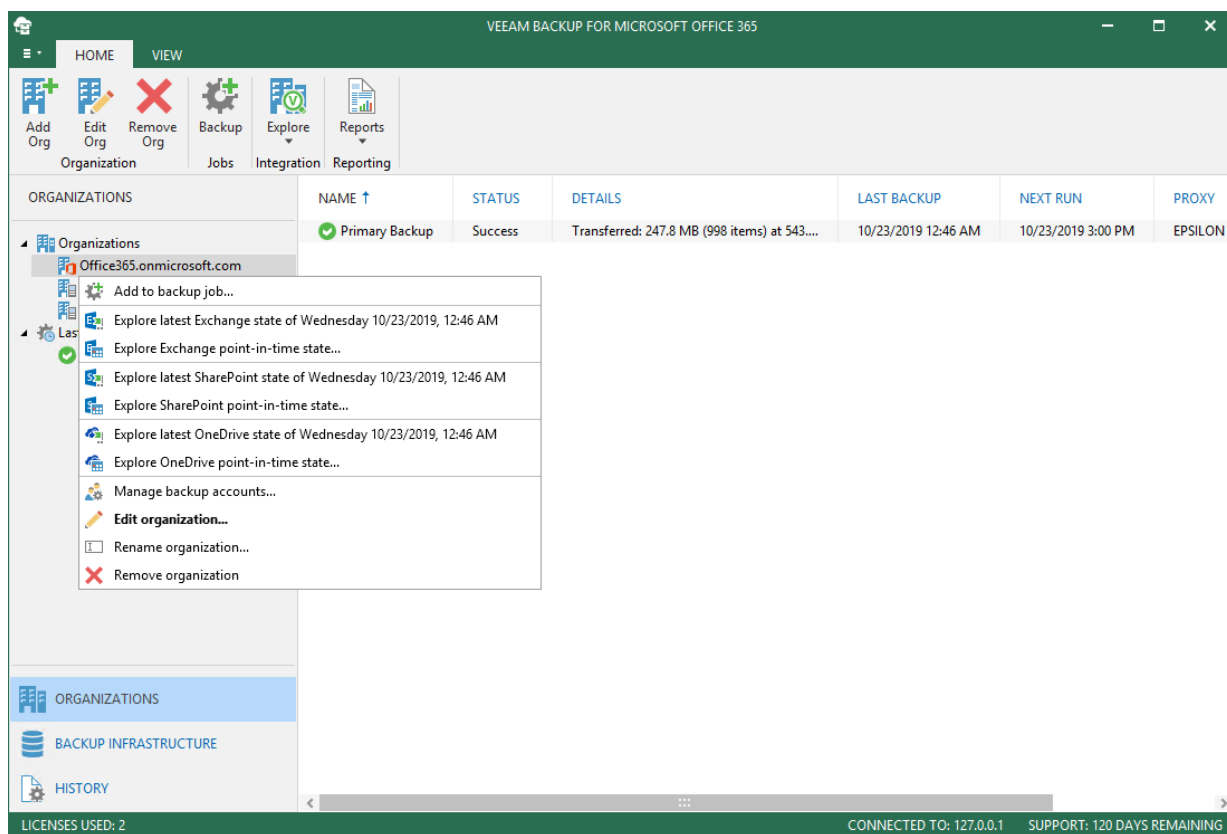
NOTE:

Consider that if you have removed a backup job from the Veeam Backup for Microsoft Office 365 backup configuration, the backup data created by such a job continues to remain in a backup repository and is also loaded into the Veeam Explorer scope.



To open backups created by all backup jobs of the selected organization, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, right-click an organization and select either of the following options:
 - a) **Explore latest <Product> state of <date_and_time>**. To explore the latest backup state.
 - b) **Explore point-in-time state**. To select a point-in-time state. For more information, see [Exploring Point-in-Time](#).



Exploring All Organizations

When exploring all organizations, Veeam Backup for Microsoft Office 365 merges and loads the latest restore points of each backup job of every organization.

The following is an example of exploring two organizations *A* and *B*. An organization *A* has three backup jobs and an organization *B*, two backup jobs.

When exploring an organization *A*, the following restore points will be merged and loaded into the Veeam Explorer scope:

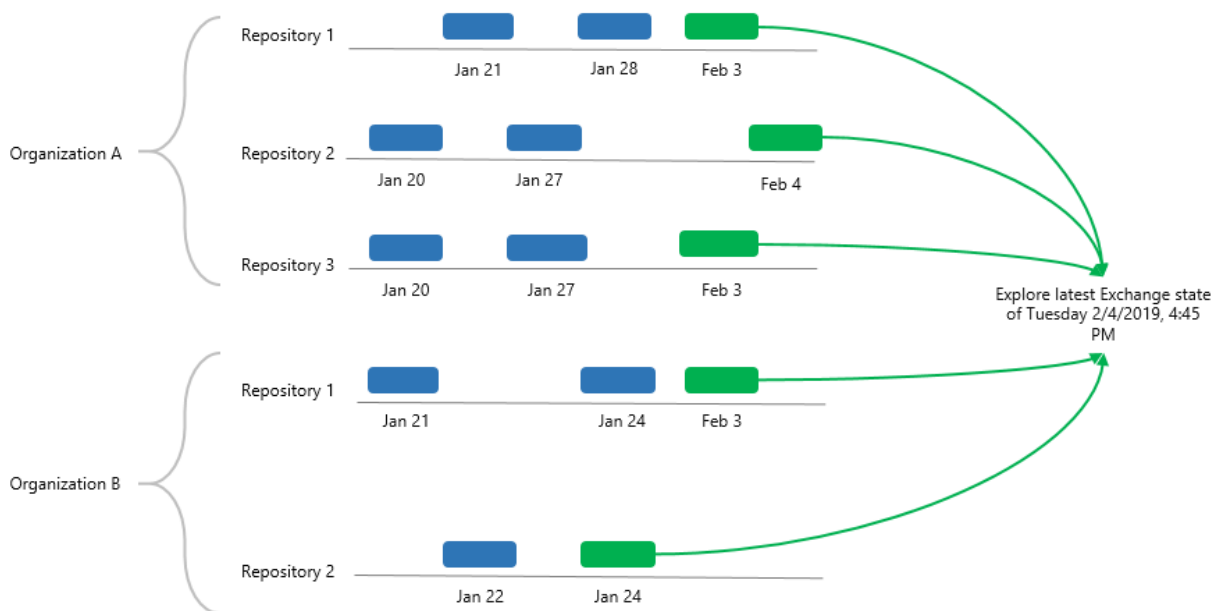
- For *Repository 1* only the restore point created on February 3.
- For *Repository 2* only the restore point created on February 4.
- For *Repository 3* only the restore point created on February 3.

When exploring an organization *B*, the following restore points will be merged and loaded into the Veeam Explorer scope:

- For *Repository 2* only the restore point created on February 3.
- For *Repository 2* only the restore point created on January 24.

NOTE:

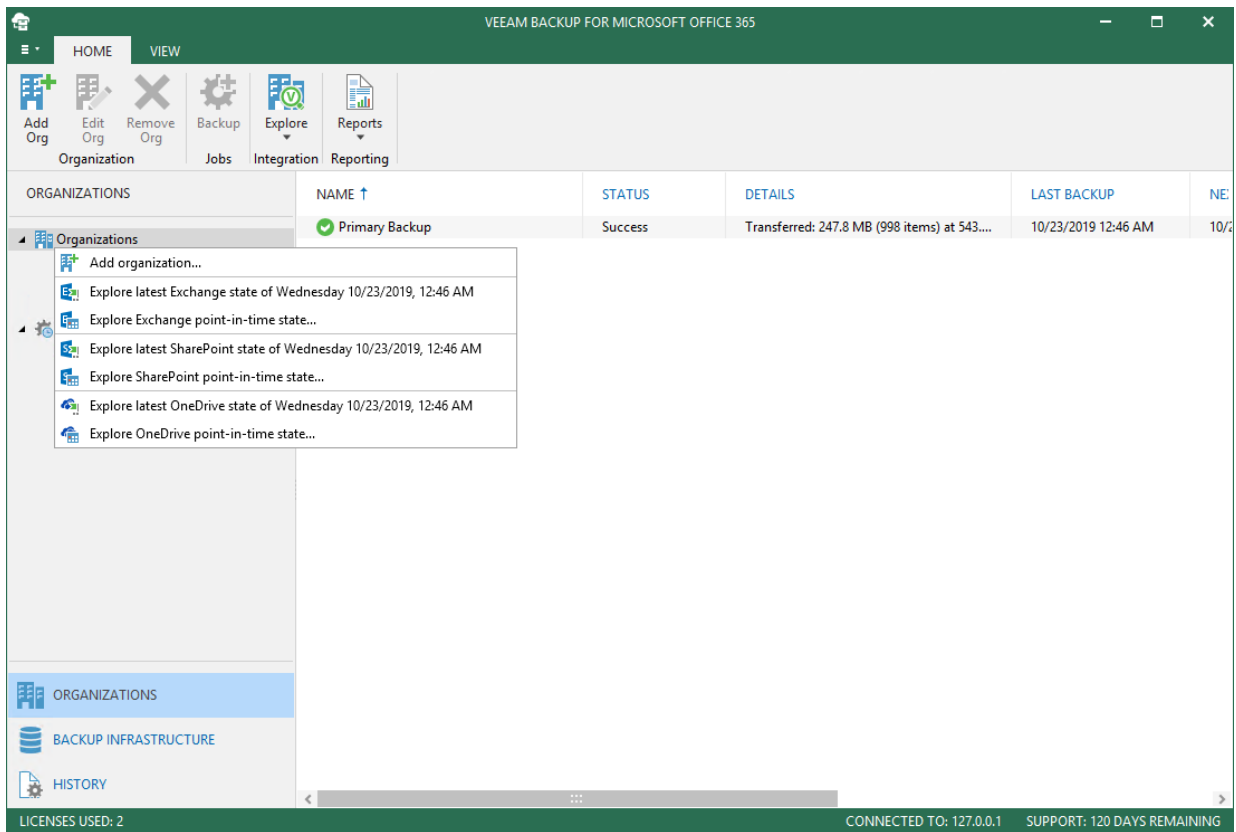
Consider that if you have removed a backup job from the Veeam Backup for Microsoft Office 365 backup configuration, the backup data created by such a job continues to remain in a backup repository and is also loaded into the Veeam Explorer scope.



To open backups of all organizations, do the following:

1. Open the **Organizations** view.
2. Right click the root **Organizations** node and select either of the following options:
 - a) **Explore latest <Product> state of <date_and_time>**. To explore the latest backup state.

- b) **Explore point-in-time state.** To select a point-in-time state. For more information, see [Exploring Point-in-Time](#).



Exploring Point-In-Time

When exploring a point in time state, choose a backup state that you want to open:

- **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.

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.
- **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.

EXPLORE BACKUP

Specify point in time

Specify point in time you want to open in Veeam Explorer for Microsoft Exchange:

☐ Use the latest available state

☒ Use the following point in time:

Monday, December 17, 2018 4:37:34 AM

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.

☒ Show items that have been deleted by user

☒ Show all versions of items that have been modified by user

Back Finish Cancel

Backup and Restore Statistics

Each backup or restore session saves its results and metrics to the Veeam Backup for Microsoft Office 365 configuration database.

To review backup and restore sessions, go to the **History** view and select either of the following nodes:

- **Jobs > Backup.** To see both completed and running backup 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](#).

To review 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 Office 365 interface. The top navigation bar includes 'HOME', 'VIEW', and 'HISTORY'. The left sidebar has a 'Stop' button and a 'Sessions' section with 'Jobs', 'Backup', and 'Restore' nodes. The main area displays a table of backup sessions.

HISTORY	NAME	ORGANIZATION	SESSION TYPE	STATUS	DETAILS
Jobs > Backup	Complete Backup (Incremental)	Office365.onmicrosoft.com	Backup	Success	Transferred: 0 B (0 items) at 0 B/s (0 ite...
	Complete Backup (Incremental)	Office365.onmicrosoft.com	Backup	Success	Transferred: 0 B (0 items) at 0 B/s (0 ite...
	Complete Backup (Incremental)	Office365.onmicrosoft.com	Backup	Success	Transferred: 0 B (0 items) at 0 B/s (0 ite...
	Complete Backup (Incremental)	Office365.onmicrosoft.com	Backup	Success	Transferred: 115.9 KB (1 item) at 2.8 KB/s.
	Complete Backup (Incremental)	Office365.onmicrosoft.com	Backup	Success	Transferred: 288.5 KB (4 items) at 9.3 KB/s.
	Complete Backup (Incremental)	Office365.onmicrosoft.com	Backup	Success	Transferred: 235.5 KB (2 items) at 9.8 KB/s.
	Complete Backup (Incremental)	Office365.onmicrosoft.com	Backup	Success	Transferred: 0 B (0 items) at 0 B/s (0 ite...
	Complete Backup (Incremental)	Office365.onmicrosoft.com	Backup	Success	Transferred: 204.9 KB (3 items) at 6.5 KB/s.
	Complete Backup (Incremental)	Office365.onmicrosoft.com	Backup	Success	Transferred: 0 B (0 items) at 0 B/s (0 ite...
	Complete Backup (Incremental)	Office365.onmicrosoft.com	Backup	Success	Transferred: 0 B (0 items) at 0 B/s (0 ite...
	Complete Backup (Incremental)	Office365.onmicrosoft.com	Backup	Success	Transferred: 0 B (0 items) at 0 B/s (0 ite...
	Complete Backup (Incremental)	Office365.onmicrosoft.com	Backup	Success	Transferred: 114.4 KB (47 items) at 3.3 K...

Below the table, there are three sections: STATUS, DATA, and SUMMARY.

STATUS	DATA	SUMMARY
Session status: Success	Processing rate: 0 B/s (0 items/s)	Duration: 00:28
Bottleneck: N/A	Read rate: 0 B/s	Objects: 1 of 1
	Write rate: 0 B/s	Transferred: 0 B (0 items processed)

At the bottom, there is an 'ACTION' section with a list of events and a 'DURATION' column.

ACTION	DURATION
Job started at 8/30/2019 12:51:57 AM	
Connected to organization	00:08
No excluded objects found	

At the very bottom, there are checkboxes for 'Errors', 'Warnings', and 'Success'. The status bar at the bottom shows 'LICENSE USED: 1', 'CONNECTED TO: 127.0.0.1', and 'LICENSE EXPIRED (21 DAYS OF GRACE PERIOD REMAINING)'.

Viewing Backup Session Metrics

You can view backup sessions as either of the following steps describes:

- Open the **Organizations** view and in the inventory pane, select an organization and then select a backup job in the preview pane.
- Open the **History** view and in the inventory pane, select the **Jobs > Backup** node and then select a backup session in the preview pane.

STATUS		DATA		SUMMARY	
Session status:	Success	Processing rate:	0 B/s (0 items/s)	Duration:	2 minutes, 58 seconds
Bottleneck:	Target	Read rate:	709.7 KB/s	Objects:	9 of 9
Last backup:	2/26/2019 2:02...	Write rate:	0 B/s	Transferred:	0 B (0 items processed)

Metrics of a backup session consist of the following sections:

- The **Status** section that shows the following fields:
 - **Session Status.** The current state of the selected backup job.
 - **Bottleneck.** A bottleneck value.

This value might be: **Detecting**, **Source**, **Target** and **N\A**.

 - **Detecting** state is displayed when a backup job is started and Veeam Backup for Microsoft Office 365 has not calculated the bottleneck value.
 - **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**.
 - **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**.
 - **N\A** state is displayed when no bottleneck occurs.
 - **Last Backup.** The date and time of the last 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 session.
 - **Objects.** Shows how many objects have been backed up during the session.

An object is an OneDrive account, SharePoint site, mailbox and archive mailbox, including group mailboxes, public folders and discovery search mailboxes.
 - **Transferred.** Shows how many bytes have been downloaded.

Viewing Restore Session Metrics

To review 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:	SharePoint restore (Job: Complete Backup - 9/4/2019 3:00...	Status:	Success
Session type:	Restore	Start Time:	9/5/2019 3:22 AM
Initiated by:	EPSILON\Administrator	End Time:	9/5/2019 3:30 AM

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 *Success*, *Warning* or *Error*.
 - **Start Time**. The start time of the session.
 - **End Time**. The end time of the session.

Reporting

Continue with this section to learn how to create the following data protection reports:

- [Mailbox Protection Reports](#)
- [Storage Consumption Reports](#)
- [License Overview Reports](#)

Creating Mailbox Protection Reports

Mailbox Protection reports show statistical information on protected and unprotected mailboxes of your Microsoft Office 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 product name and a license type.
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 to create a report.

You can also select the root **Organizations** node to generate a report for all organizations added to the scope.
3. In the **Organizations** view, on the **Home** tab, select **Reports > Mailbox Protection**.
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 specify the format (*.pdf* or *.csv*) in which 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: 12/21/2018

Save as:

C:\Users\Administrator\Documents\MailboxProtectionReport_2018_12_21_06_59_47.p

Browse...

☒ Open report after publishing

Back

Finish

Cancel

Creating Storage Consumption Reports

Storage Consumption reports show statistical information on used space in backup or object storage repositories.

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 product name and a license type.
Summary	Shows occupied storage space of all backup repositories added to the scope.
Top 5 repositories by storage usage	Shows top 5 repositories the backup data on which occupies the most disk space.
Top 5 repositories by growth	Shows top 5 repositories in which the space is occupied most frequently.
Daily Change Rate (in 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 Office 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 backup data in object storage.
Repository Growth (in GB)	

Consider the following:

- Repositories that have no statistical information will not be included in the report.

No information is available when:

- You have added a new backup repository, as described in [Adding Backup Repositories](#).

Since nothing has been placed to a backup repository after it was added, no statistical information is available, therefore, this repository will not be included in the report.

- You have upgraded a previous version of Veeam Backup for Microsoft Office 365 with a newer one, as described in [Upgrading to Veeam Backup for Microsoft Office 365 4.0](#).

In this case, all backup repositories in your environment will be excluded from the report.

- Repositories whose **Daily Change** and **Total Size** values are less than 10MB will not be included in the report.

For example, a report is said to be built starting from *01/01/2019* to *31/01/2019* and the period from *01/01/2019* to *09/01/2019* is empty (both the **Daily Change** and **Total Size** values are less than 10MB). In this scenario, such a report will only be showing statistical information starting from *10/01/2019*.

To generate a report for each organization added to the scope, do the following:

1. Open the **Organizations** view.
2. On the **Home** tab, select **Reports > Storage Consumption**.
3. Specify a time interval.
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 specify the format (*.pdf* or *.csv*) in which 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

Specify reporting interval

From: Wednesday, November 21, 2018 To: Friday, December 21, 2018

Save as: C:\Users\Administrator\Documents\StorageConsumptionReport_2018_12_21_06_57_1 Browse...

☒ Open report after publishing

Back Finish Cancel

Creating License Overview Reports

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 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 how many licenses are in use, including trial licenses.
Top 5 organizations per license usage	Shows top 5 organizations that consume the license the most.

NOTE:

When using a rental license, *License Overview* reports also show a number of trial licenses per each organization. For more information, see [Rental License](#).

To generate a report for each organization added to the scope, do the following:

1. Open the **Organizations** view.
2. On the **Home** tab, select **Reports > License Overview**.
3. Specify a time interval.
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 specify the format (*.pdf* or *.csv*) in which 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

Specify reporting interval

From:

Wednesday, November 21, 2018

To:

Friday, December 21, 2018

Save as:

C:\Users\Administrator\Documents\LicenseOverviewReport_2018_12_21_06_44_29.pdf

Browse...

☒ Open report after publishing

Back

Finish

Cancel

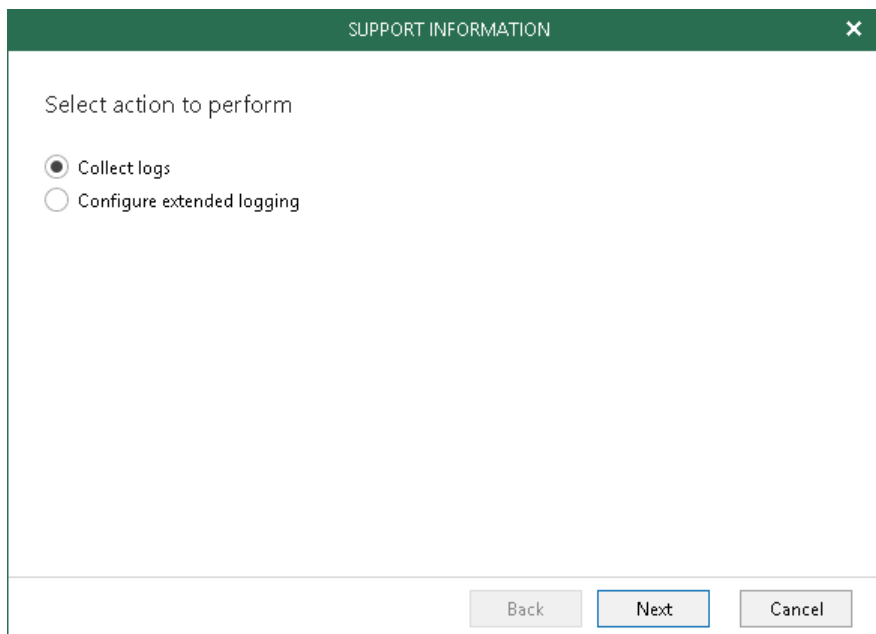
Log Files Export

This section explains how to collect log files that help you troubleshoot unexpected errors when working with Veeam Backup for Microsoft Office 365.

To collect log files, do the following:

1. In the main menu, click **Help and Support > Support Information**.
2. Select the **Collect logs** option.

To enable extended logging mode, select **Configure extended logging** and proceed with the [Configuring Extended Logging Mode](#) section.



SUPPORT INFORMATION

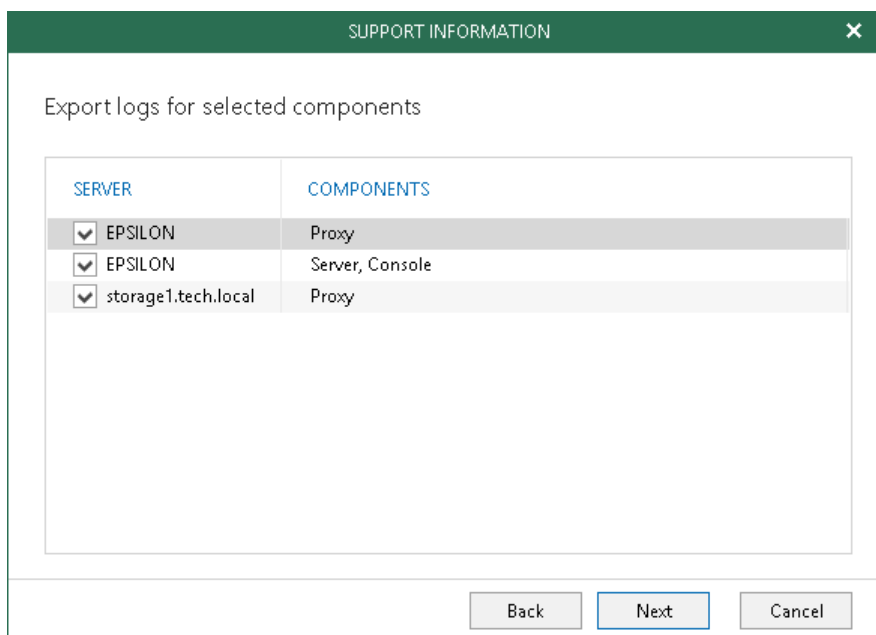
Select action to perform

☒ Collect logs

☐ Configure extended logging

Back Next Cancel

3. Select system components for which to obtain log files.



SUPPORT INFORMATION

Export logs for selected components

SERVER	COMPONENTS
<input checked="" type="checkbox"/> EPSILON	Proxy
<input checked="" type="checkbox"/> EPSILON	Server, Console
<input checked="" type="checkbox"/> storage1.tech.local	Proxy

Back Next Cancel

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

◀ December 2018 ▶

Su	Mo	Tu	We	Th	Fr	Sa
25	26	27	28	29	30	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	29
30	31	1	2	3	4	5

Back Next Cancel

5. Specify the path and click **Finish**.

SUPPORT INFORMATION ✕

Select location to export the logs to

Path:

Back Finish Cancel

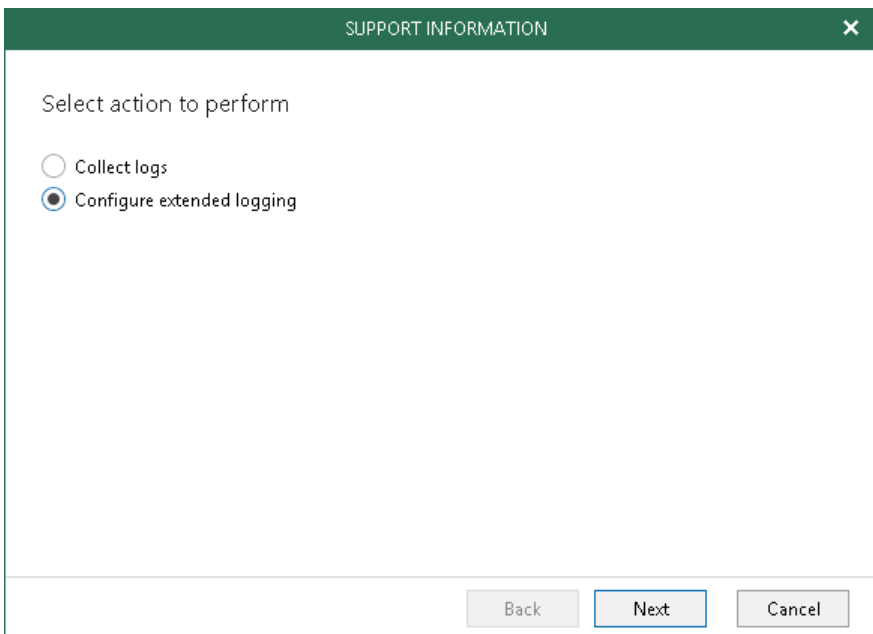
Configuring Extended Logging Mode

Extended logging mode augments log records collected by default and adds additional information on execution results that you might want to review to troubleshoot unexpected application errors.

After enabling extended logging mode, you can go back to the application and perform required actions, then collect logs, as described in [Log Files Export](#).

To configure extended logging mode, do the following:

1. In the main menu, click **Help and Support > Support Information**.
2. Select the **Configure extended logging** option.



SUPPORT INFORMATION

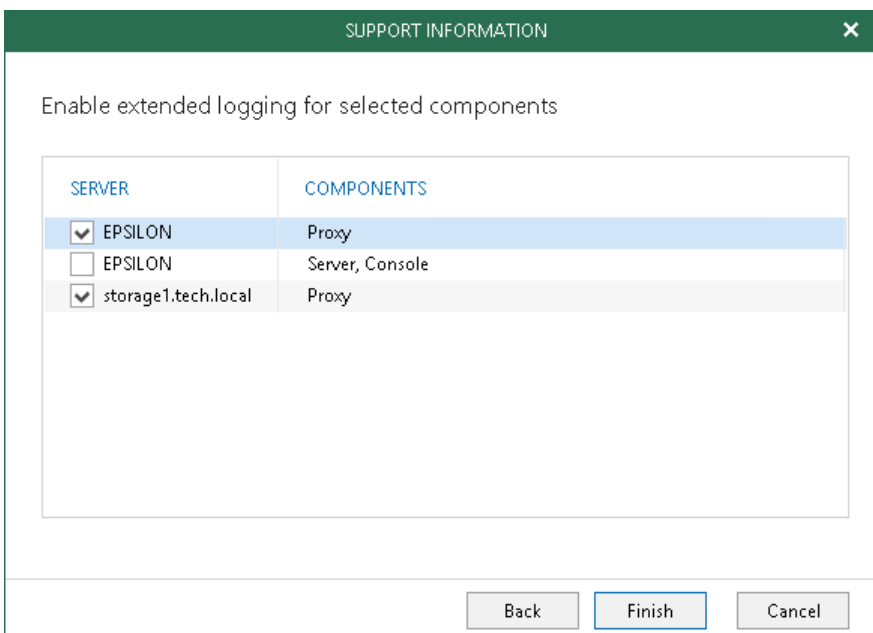
Select action to perform

☐ Collect logs

☒ Configure extended logging

Back Next Cancel

3. Select components (local or remote) to which you want to apply extended logging mode.



SUPPORT INFORMATION

Enable extended logging for selected components

SERVER	COMPONENTS
<input checked="" type="checkbox"/> EPSILON	Proxy
<input type="checkbox"/> EPSILON	Server, Console
<input checked="" type="checkbox"/> storage1.tech.local	Proxy

Back Finish Cancel

Office 365 Backup as a Service

This section explains how to configure *Office 365 Backup as a Service* for service providers and tenants.

For Service Providers

To configure *Office 365 Backup as a Service* for service providers, do the following:

1. Install Veeam Backup for Microsoft Office 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 & Replication and Veeam Backup for Microsoft Office 365 licenses.

For more information, see the [Licensing for Service Providers](#) section of the Veeam Cloud Connect Administrator Guide and the [Licensing and License Types](#) section of this guide.

3. Configure a TLS certificate, as described in the [Managing TLS Certificates](#) section of the Veeam Cloud Connect Administrator Guide.

Without a certificate, you will not be able to add a *Cloud Gateway* component.

4. Configure a cloud gateway, as described in the [Adding Cloud Gateways](#) section of the Veeam Cloud Connect Administrator Guide.

5. Add new tenants, as described in the [Registering Tenant Accounts](#) section of the Veeam Cloud Connect Administrator Guide.

6. Configure your Veeam Backup for Microsoft Office 365 environment, as described in [Configuring Veeam Backup for Microsoft Office 365](#).

A service provider can use Veeam Backup for Microsoft Office 365 RESTful API to build a web portal that will allow tenants to browse and restore their backups without using Veeam Explorers. For more information, see [RESTful API reference](#).

NOTE:

Consider the following:

- Make sure to install Veeam Explorer for Microsoft Exchange, Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft OneDrive for Business that come as part of the Veeam Backup for Microsoft Office 365 4.0 distribution package.
- Make sure to install Veeam Backup for Microsoft Office 365 on a server with Veeam Backup & Replication 9.5 Update 4 or higher.

Configuring Veeam Backup for Microsoft Office 365

For more information on how to configure Veeam Backup for Microsoft Office 365 for service providers, see the following sections:

- [Configuring Veeam Backup for Microsoft Office 365 Environment](#)
To learn how to configure Veeam Backup for Microsoft Office 365 settings.
- [Configuring Authentication Settings](#)
To learn how to allow tenants to perform self-restore procedures.
- [Configuring Backup Proxy Servers](#)
To learn how to configure backup proxy servers.
- [Configuring Backup Repositories](#)
To learn how to configure backup repositories.
- [Microsoft Organizations Management](#)
To learn how to add tenants organizations to the Veeam Backup for Microsoft Office 365 scope.
- [Data Backup](#)
To learn how to back up data of your 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 Office 365 server of a service provider via Veeam Explorers for self-service recovery.

For Tenants

To configure *Office 365 Backup as a Service* for tenants, do the following:

1. Add a service provider in Veeam Backup & Replication, as described in the [Connecting to Service Providers](#) section of the Veeam Cloud Connect User Guide.
2. Add backups to the Veeam Explorer scope, as described in [Exploring Backups in Veeam Explorers](#).

NOTE:

Mind the following:

- Make sure to install Veeam Explorer for Microsoft Exchange, Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft OneDrive for Business that come as part of the Veeam Backup for Microsoft Office 365 4.0 distribution package.
- By default, tenants are not able to restore anything without the service provider assistance. To be able to perform self-service recovery procedures, a service provider must configure authentication settings for tenants, as described in [Configuring 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 Office 365 service provider server to the Veeam Explorers scope, as described in [Working with Backups in Veeam Explorers](#).

Exploring Backups in Veeam Explorers

To explore backups located on the service provider side, add such backups in Veeam Explorers, as described in:

- [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](#)

NOTE:

Make sure to have access to the service provider server to be able to explore your backups. Access can be granted, as described in [Configuring Authentication Settings](#).

Veeam Explorer for Microsoft Exchange

Veeam Explorer for Microsoft Exchange allows you to restore and export Microsoft Exchange data from backups created in Veeam Backup for Microsoft Office 365 and Veeam Backup & Replication.

You can also compare data with the production environment to track differences in your backups and on production servers. In addition, you can save data from backups to a local computer and send data from backups via email.

Planning and Preparation

Continue with this section to learn how to configure your environment before start using Veeam Explorer for Microsoft Exchange.

Used Ports

Consider opening the following ports to perform a restore.

From	To	Protocol	Port	Notes
Veeam Backup Server / Standalone Console	Microsoft Exchange 2003/2007 CAS Server	TCP	80, 443	WebDAV connections
	Microsoft Exchange 2010/2013/2016/2019 CAS Server	TCP	443	Microsoft Exchange web services connections

Required Permissions

The following table lists required permissions for a restore.

Operation	Required Roles and Permissions
Restore to Microsoft Office 365 and on-premises Microsoft Exchange	<p>To restore data to Microsoft Office 365 and on-premises Microsoft Exchange, make sure to configure user accounts as follows:</p> <p>Restore to a Public Folder</p> <ul style="list-style-type: none">▪ The account being used must own a mailbox on a target Microsoft Exchange server.▪ The account must be assigned the <i>Organization Management</i> role on a target Microsoft Exchange server. See Assigning Organization Management Role.▪ To restore <i>In-Place Hold Items</i> to the original location: If the <i>In-Place Hold Items</i> folder already exists, make sure the account being used can create, modify and delete items. If the <i>In-Place Hold Items</i> folder does not exist, the account being used must be able to create folders under the <i>All Public Folders</i> root node. <p>Restore to a Mailbox</p> <ul style="list-style-type: none">▪ If the account owns a mailbox, make sure it has <i>Full Access</i>.▪ If the account does not own a mailbox, then access must be granted through impersonation. See Granting Full Access.

Examples

Assigning Organization Management Role

To assign the *Organization Management* role, use the following cmdlet.

```
Add-RoleGroupMember "Organization Management" -Member "<user_account>"
```

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

Granting Full Access

To grant *Full Access* to the account that owns a mailbox, use the following cmdlet.

```
Add-MailboxPermission -Identity "<target_mailbox>" -User "<user_account>" -  
AccessRights FullAccess -InheritanceType All
```

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

To grant *Full Access* to the account that do not own a mailbox (i.e. through impersonation), use the following cmdlet.

```
New-ManagementRoleAssignment -Name "<role_name>" -Role ApplicationImpersonation -User  
"<user_account>"
```

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

Recalling Given Permissions

To recall given access level, run either of the following cmdlets.

```
Remove-ManagementRoleAssignment "<role_name>"
```

```
Remove-ManagementRoleAssignment -Identity <role_name>
```

Considerations and Limitations

This section lists considerations and known limitations of Veeam Explorer for Microsoft Exchange.

General

- When Veeam Explorer for Microsoft Exchange is installed on a server on which both Veeam Backup & Replication and Veeam Backup for Microsoft Office 365 are installed, the notification settings will be inherited from the Veeam Backup and Replication Global Notification settings.

Restore

- Veeam Explorer for Microsoft Exchange does not support restore via *PSDirect*, *VIX* or *Sphere API*.
- Sending objects that exceed 3MB in size may fail. To fix this issue, install [this Microsoft update](#).
- Multiple restore is not supported for public folders. Use per-object restore.
- To restore *In-Place Hold Items* or *Litigation Hold Items* to the original location, consider the following:
 - *In-Place Hold Items* restore is not supported for On-Premises Exchange Server 2013 due to EWS limitations.
 - To restore *In-Place Hold Items* of Exchange 2016 mailboxes, these mailboxes must have *In-Place Hold* enabled and applied at least once with *DiscoveryHolds* system folder creation. Otherwise, restore 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 information on enabling *In-Place Hold* and *Litigation Hold*, see [this Microsoft article](#).

NOTE:

To use an internet proxy server to restore backups created in Veeam Backup for Microsoft Office 365, make sure to provide appropriate proxy server address and the port number. For that, go to the **Control Panel > Internet Options Connections** tab, click **LAN Settings**, select the **Use a proxy server for your LAN** check box and specify a proxy server you want to use. Credentials for such a proxy (if needed) will be taken from the **Control Panel > Credential Manager > Windows Credentials** console.

Consider that this functionality is only available in Veeam Explorer for Microsoft Exchange that comes as part of the Veeam Backup for Microsoft Office 365 distribution package.

Export

Consider the following:

- Export is only available if you have a 64-bit version of Microsoft Outlook 2019, Microsoft Outlook 2016, Microsoft Outlook 2013 or Microsoft Outlook 2010 installed on a computer with Veeam Explorer for Microsoft Exchange.
- To avoid conflicts during export, make sure to exclude .pst files from the indexing scope. Oftentimes conflicts may occur due to a file you are exporting is being indexed at the same time. When exporting to shared folders, exclude Outlook files or disable Windows search on the destination computer.

Launching Application and Exploring Backups

To open Veeam Explorer for Microsoft Exchange and load backups, you can use any of the following methods:

- The **Explore** option. For more information, see [Data Restore](#).

When loading backups located in object storage repositories, Veeam Explorer for Microsoft Exchange will notify you about the location of these backups. You can select the **Don't show this message again** check box to unsubscribe from such notifications. To enable notifications, select the **Reset disabled pop-up notifications** check box, as described in [Configuring Advanced Settings](#).

- Go to **Start** and click **Veeam Explorer for Microsoft Exchange**.

When you open Veeam Explorer for Microsoft Exchange from the **Start** menu, all backed-up databases will be loaded automatically.

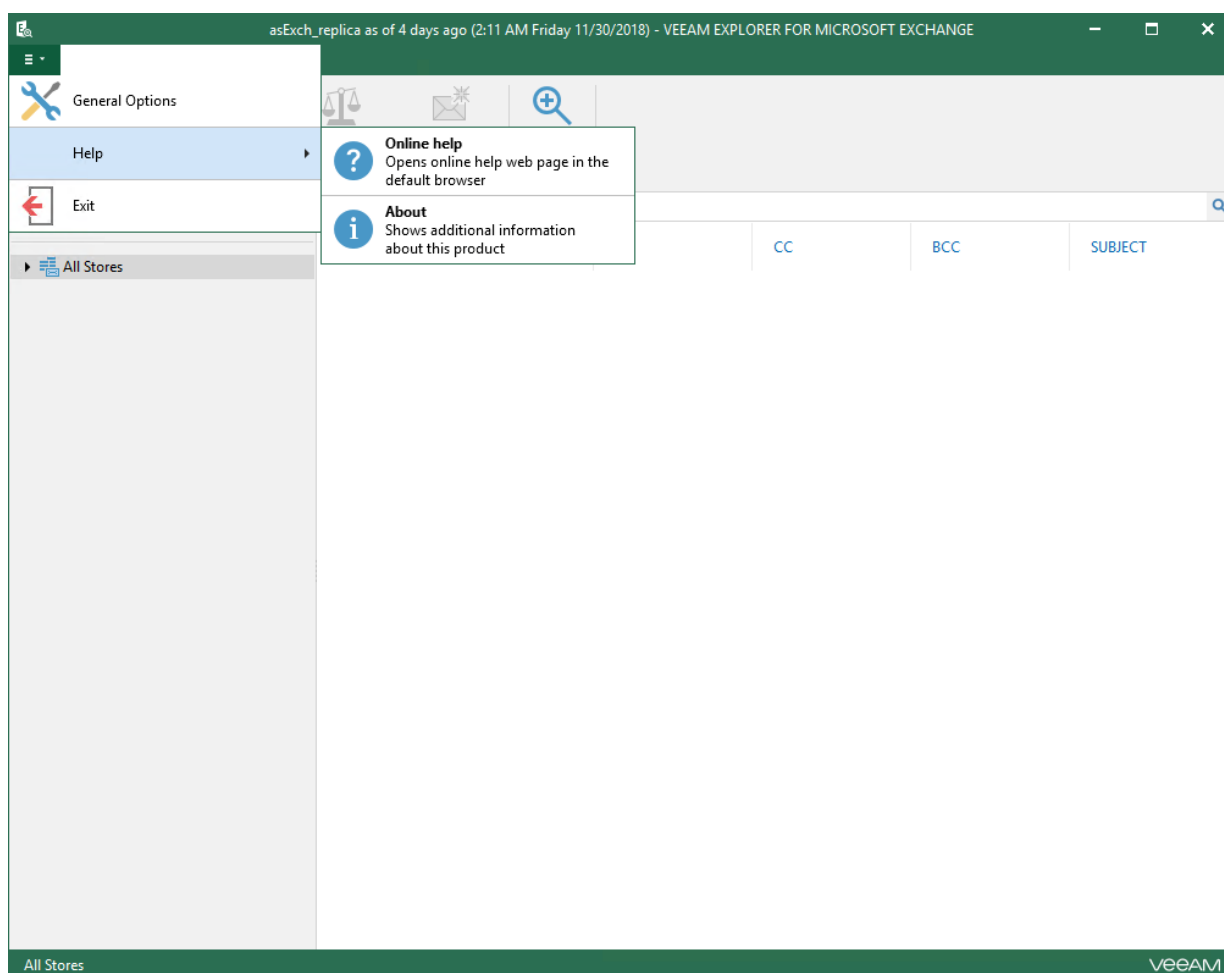
Understanding User Interface

Veeam Explorer for Microsoft Exchange provides you with the convenient user interface that allows you to perform required operations in a user-friendly manner.

Main Menu

The main menu comprises the following features:

- **General Options.** Allows you to configure program options.
- **Help.**
 - **Online help.** Opens the online web help page.
 - **About.** Shows information about the product.
- **Exit.** Closes the program.

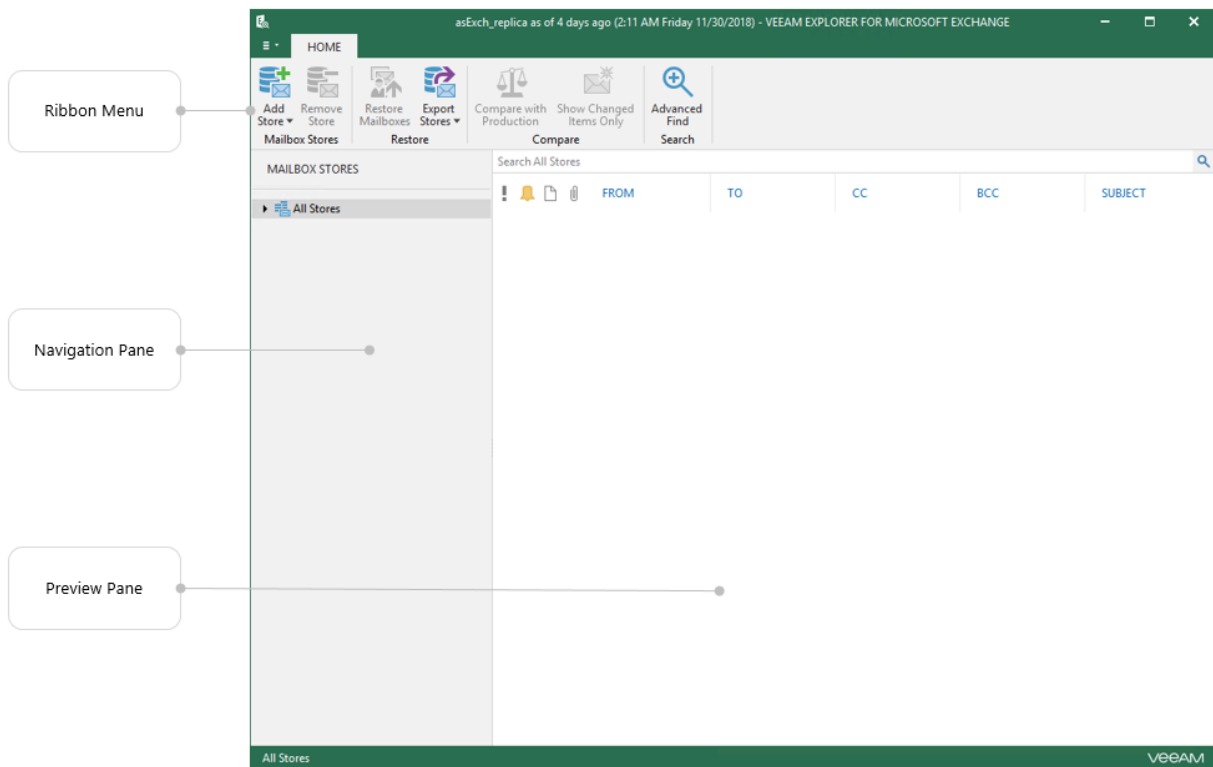


Main Application Window

The main application window can be divided into three categories:

- The ribbon menu, which contains general program commands organized into logical groups.
- The navigation pane, which allows you to browse through the hierarchy of your backup files.

- The preview pane, which shows you the details about objects you have selected in the navigation area.



Browsing, Searching and Viewing Items

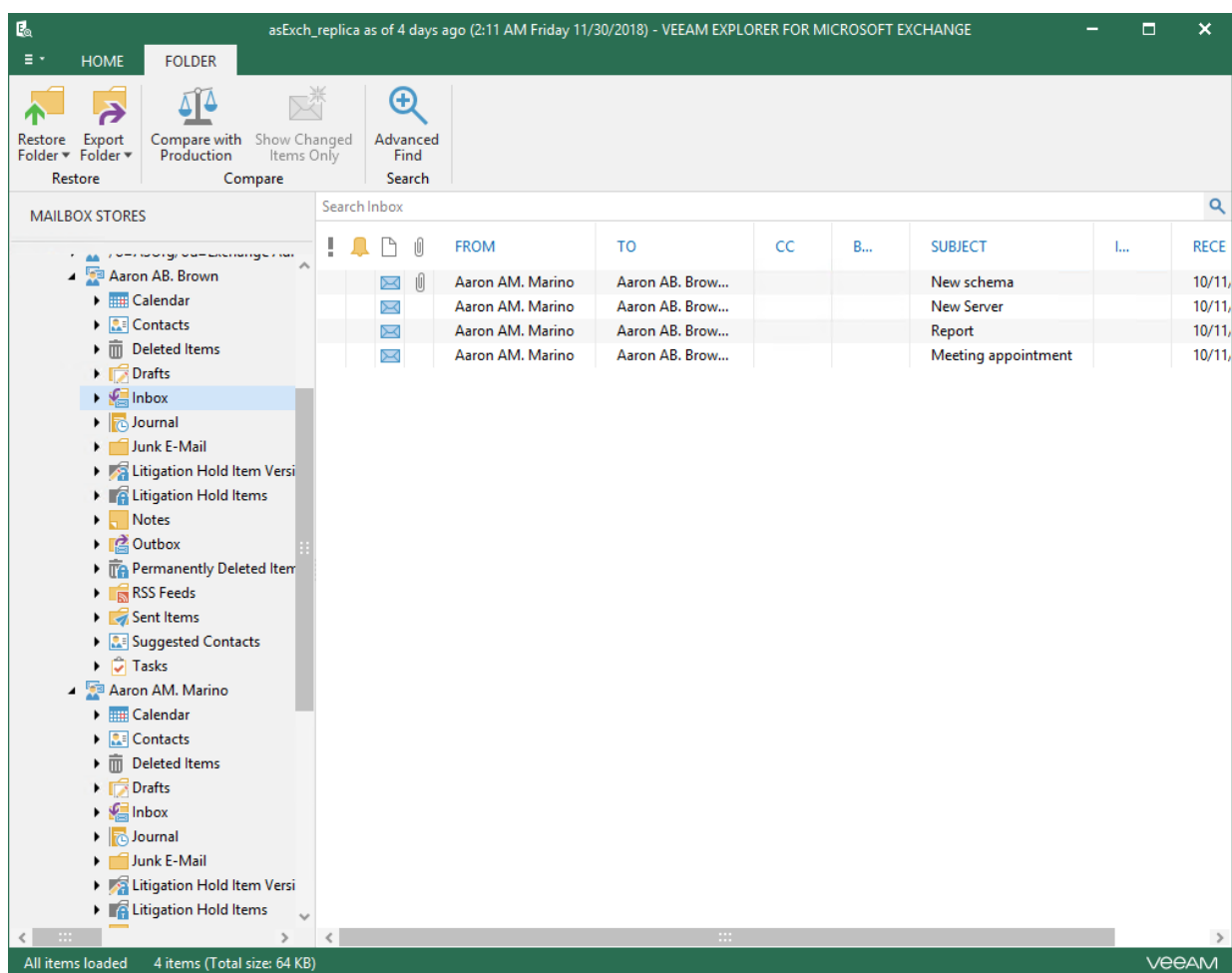
Continue with this section to learn more about:

- [Browsing backup content](#)
- [Opening Messages](#)
- [Searching for objects in a backup file](#)
- [Using advance search](#)

Browsing

To view the contents of a backup file, you use the navigation pane which shows you the database structure containing your Exchange objects.

After you select an object in the navigation pane, you can see its content in the preview pane.

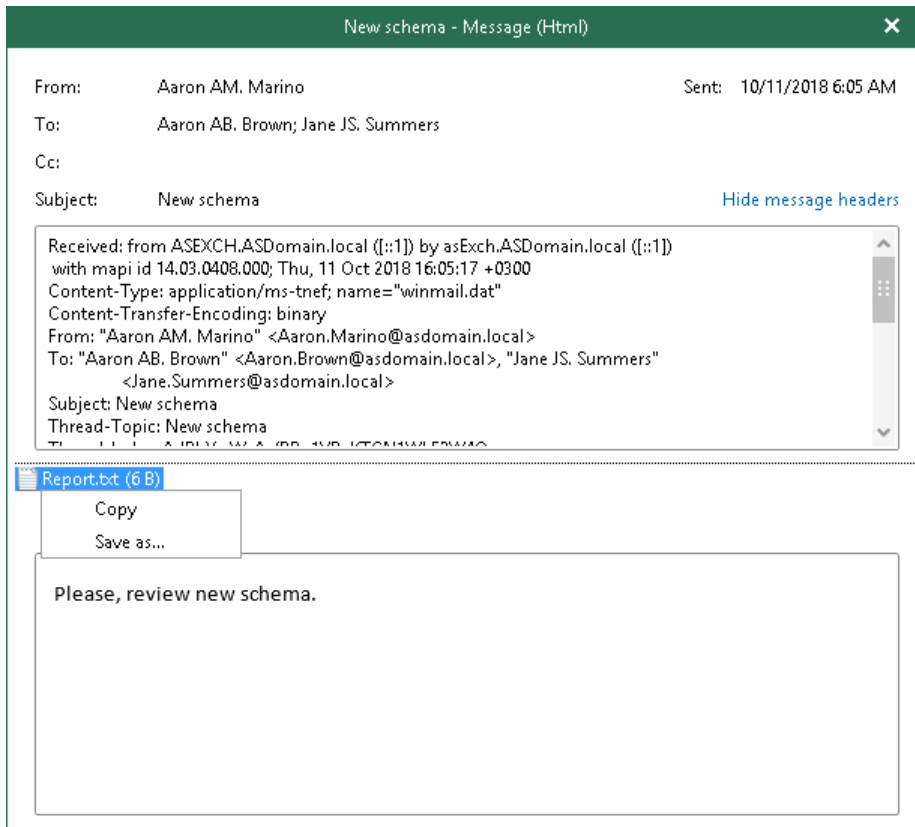


Opening Messages

To open a message, right-click a message in the preview pane and select **Open**. You can also double-click a message:

- To show message headers, click **Show message headers**.

- To open attachments, double-click an attachments or right-click an attachment and select **Open**.
- To save attachments, right-click an attachment and select **Save as**.



Searching

The search mechanism allows you to find items matching specified search criteria.

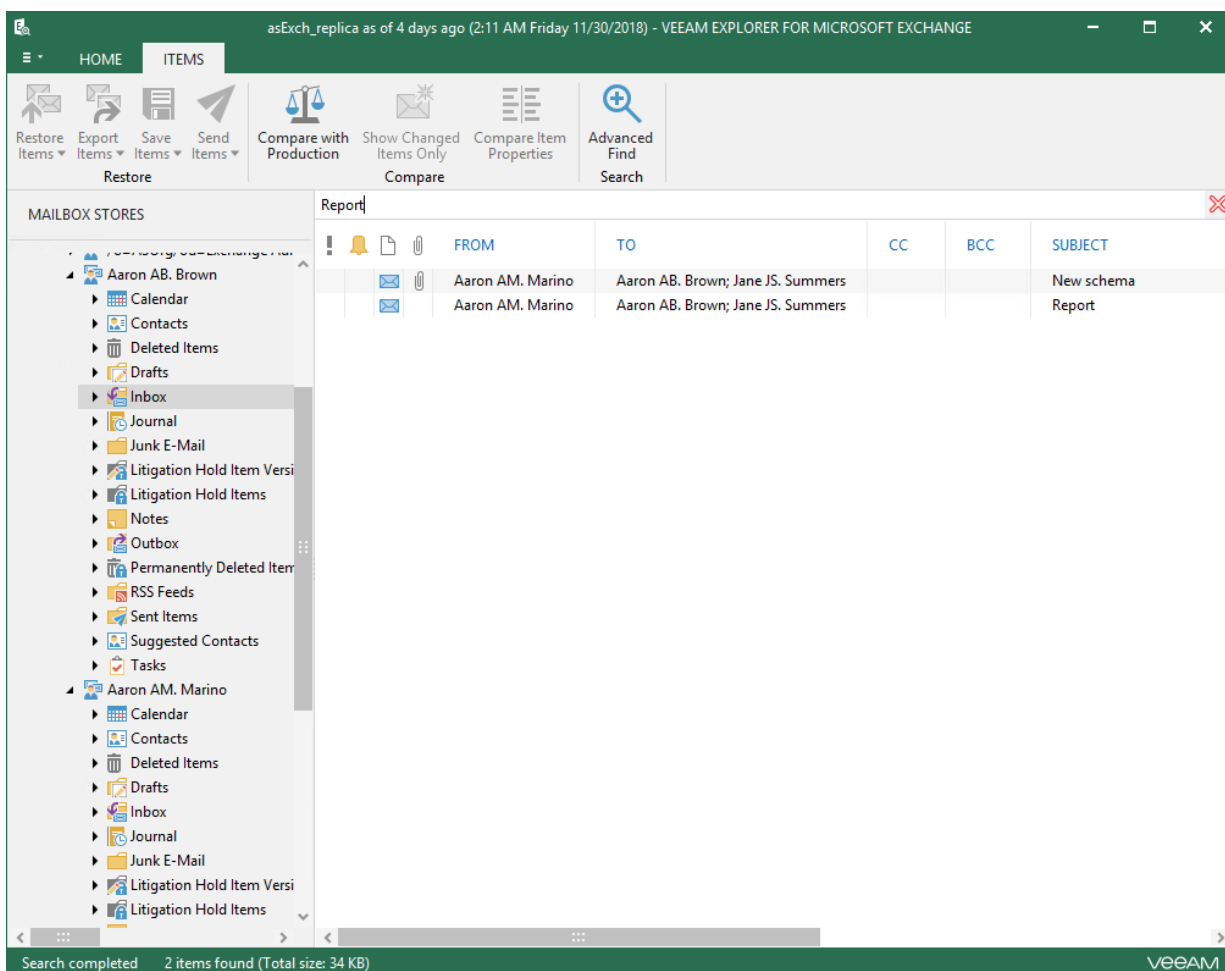
To search for required items, do the following:

1. In the navigation pane, select an object in which you want to find data.
2. Enter a search query to the search field at the top of the preview pane.

NOTE:

To find the exact phrase, use double quotes. For example, *"Office 365"*.

You can narrow search results by specifying various search criteria using the *criteria:value* format. You can also use logical upper-cased operators such as *AND*, *OR* and *NOT* along with wildcard characters such as *** and *?*.



Using Advanced Find Capabilities

The **Advanced Find** mechanism allows you to define your search criteria more precisely.

For example, to find messages with the subject *Report*, do the following:

1. In the preview pane, select a node and click **Advanced Find**.
2. In the **Define search criteria** section, select **Category > All fields**.
3. In the **Field** list, select **Subject**.
4. In the **Condition** list, select **Contains**.
5. In the **Value** field, specify a substring to look for.
6. Click **Start**.

To remove a filter, click the cross mark on the left. To remove all configured filters, click **Reset**.

asExch_replica as of 4 days ago (2:11 AM Friday 11/30/2018) - VEEAM EXPLORER FOR MICROSOFT EXCHANGE

HOME ITEMS

Restore Items Export Items Save Items Send Items Compare with Production Show Changed Items Only Compare Item Properties Advanced Find Search

MAILBOX STORES

- Aaron AB. Brown
 - Calendar
 - Contacts
 - Deleted Items
 - Drafts
 - Inbox
 - Journal
 - Junk E-Mail
 - Litigation Hold Item Versi
 - Litigation Hold Items
 - Notes
 - Outbox
 - Permanently Deleted Item
 - RSS Feeds
 - Sent Items
 - Suggested Contacts
 - Tasks
- Aaron AM. Marino
 - Calendar
 - Contacts
 - Deleted Items
 - Drafts
 - Inbox
 - Journal
 - Junk E-Mail
 - Litigation Hold Item Versi
 - Litigation Hold Items

Find items that match these criteria:

Subject contains Report

Define search criteria

Category: All Fields Field: Assistant's name

Condition: is exactly Value:

Add To List

	FROM	TO	CC	BCC	SUBJECT
	Aaron AM. Marino	Aaron AB. Brown; Jane JS. Summers			Report

Search completed 1 items found (Total size: 14 KB)

VEEAM

General Application Settings

Continue with this section to learn more about configuring general application settings and components.

Extensible Storage Engine

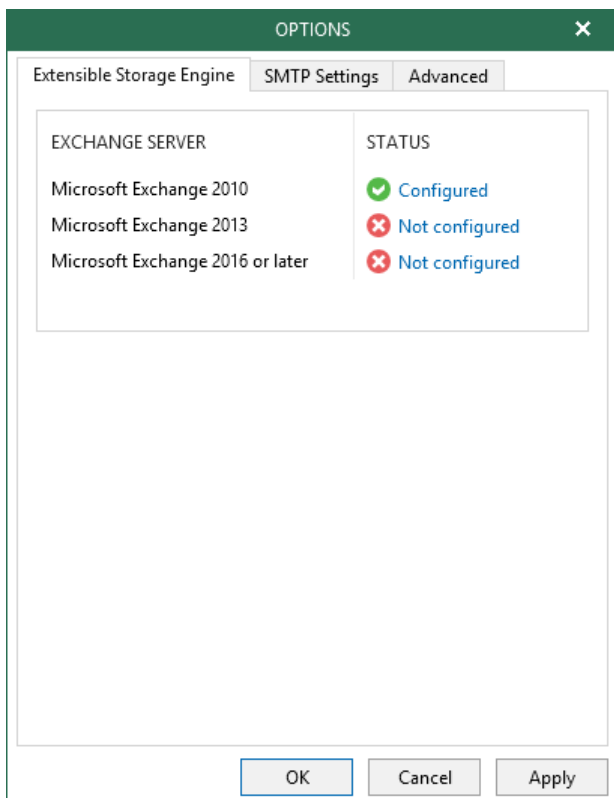
To work with database files, Veeam Explorer for Microsoft Exchange requires a dynamic link library `ese.dll` which is distributed with Microsoft Exchange.

The `ese.dll` file must be of the same version as the Microsoft Exchange application that was used to create a database. When restoring a VM that was backed up with application-aware image processing, the `ese.dll` file will be located automatically.

To specify the path to the `ese.dll` file, do the following:

1. Go to the main menu and click **General Options**.
2. Open the **Extensible Storage Engine** tab.
3. Click the link next to the Microsoft Exchange version and specify the path to the `ese.dll` file.

This file can be found on the Microsoft Exchange server distribution CD in the `X:\Setup\ServerRoles\Common\ese.dll` directory or in the installation directory of the Microsoft Exchange server.



SMTP Settings

Veeam Explorer for Microsoft Exchange allows you to send Exchange items that are located in a backup via email. For that, you must configure an SMTP server via which you want to send emails.

To configure SMTP settings, do the following:

1. Go to the main menu and click **General Options**.
2. Open the **SMTP Settings** tab.
3. Select the **Configure SMTP settings** check box and do the following:
 - a. In the **Server** field, specify a DNS name or IP address of the SMTP server.
 - b. In the **Port** field, specify a port number of the specified SMTP server.
 - c. In the **From** field, specify the sender email address.
 - d. Select the **Use authentication** check box. If the specified SMTP server requires an SMTP authentication for outgoing traffic and provide valid credentials.
 - e. Select the **Enable SSL security** check box to enable SSL data encryption.
3. Click **Send** to send a test email message.
4. Click **Apply**.

The screenshot shows the 'OPTIONS' dialog box with the 'SMTP Settings' tab selected. The 'Configure SMTP settings' checkbox is checked. The 'Server' field is 'smtp.office365.com', 'Port' is '25', and 'From' is 'administrator@abc.com'. The 'Use authentication' checkbox is checked, with 'User' set to 'Administrator' and 'Password' masked with dots. The 'Enable SSL security' checkbox is also checked. At the bottom, there is a 'Send test e-mail to:' section with 'E-mail' set to 'administrator@abc.com' and a 'Send' button. The 'OK', 'Cancel', and 'Apply' buttons are at the bottom right.

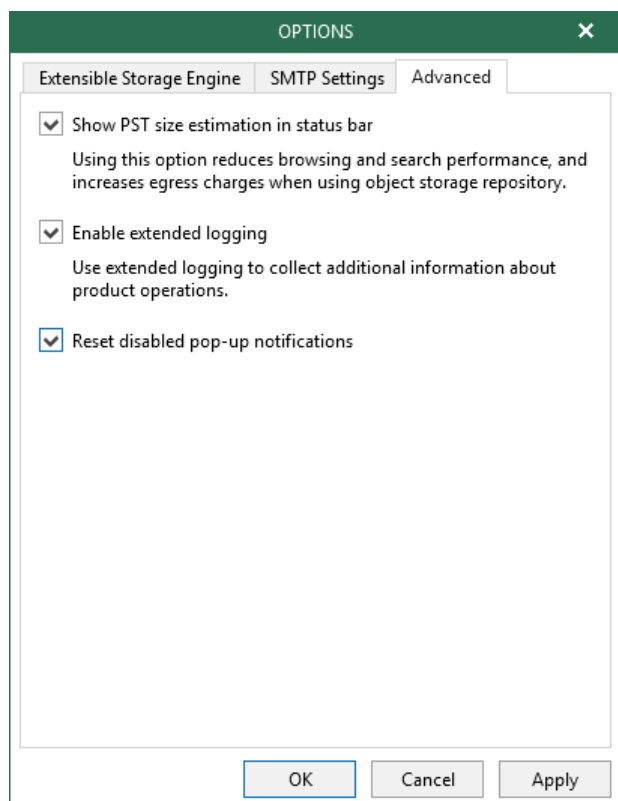
Advanced Settings

Veeam Explorer for Microsoft Exchange allows you to configure advanced settings such as extended logging mode, pop-up notifications and a PST size availability.

To configure advanced settings, do the following:

1. Go to the main menu and click **General Options**.
2. Open the **Advanced** tab and select the following check boxes:
 - **Show PST size estimation in status bar** if you want to see the estimated size of the Outlook database file in the status bar.
 - **Enable Extended logging** if you want to enable extended logging mode to collect logs that contain extended details on specific operations.

After enabling extended logging mode, you can go back to the application and perform required actions, then collect logs.
 - **Reset disabled pop-up notifications** if you want to enable notifications when loading backups from object storage repositories.



Standalone Databases and External Servers

This section explains how to add standalone databases to the Veeam Explorer for Microsoft Exchange scope and how to connect to a Veeam Backup for Microsoft Office 365 server and service provider server to view backups located on these servers.

Adding Microsoft Exchange Stores

This section explains how to add Microsoft Exchange databases manually.

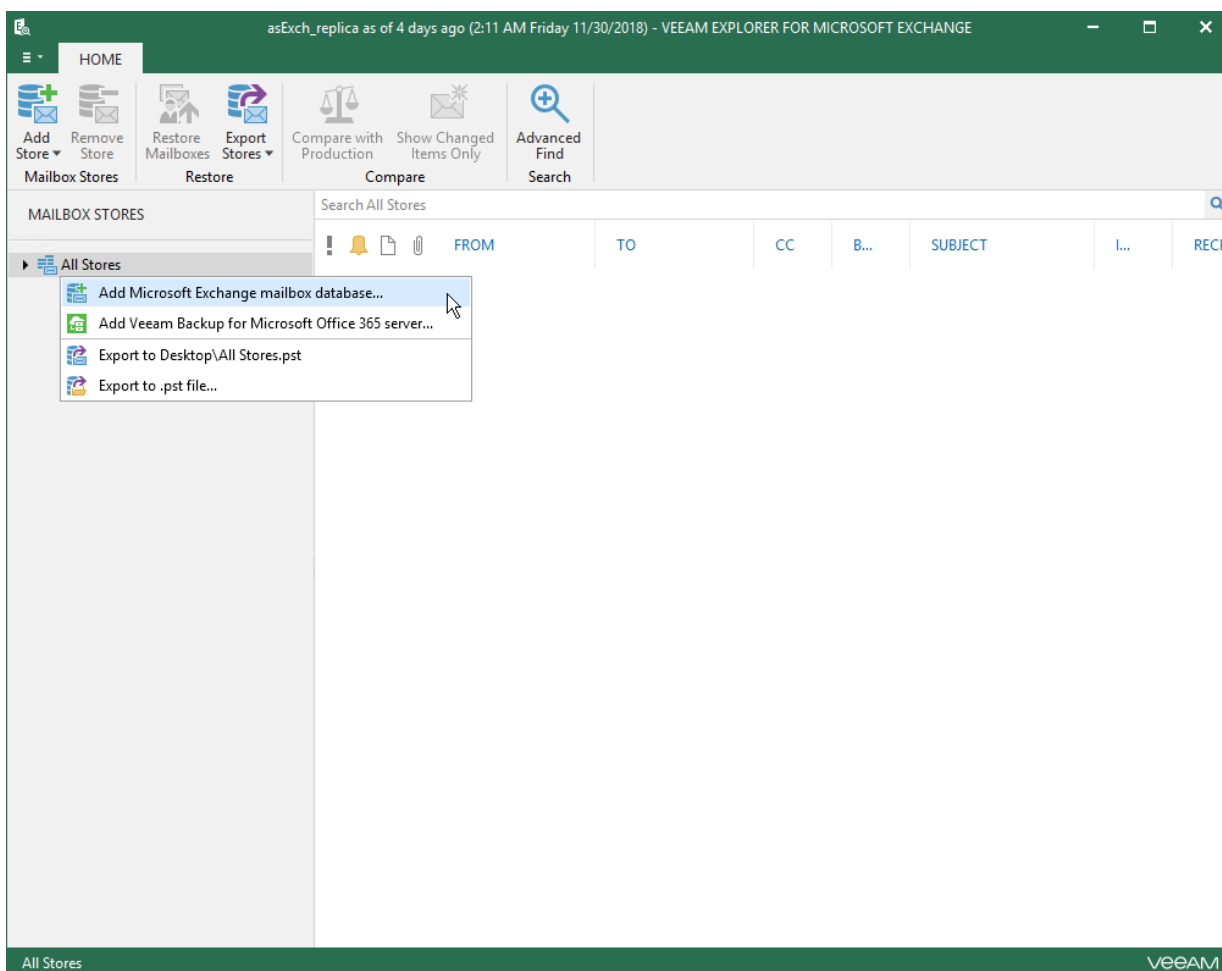
NOTE:

Before adding databases, make sure that Veeam Explorer for Microsoft Exchange has access to the `ese.dll` file. For more information, see [Configuring Extensible Storage Engine](#).

If a database is in *Dirty State*, you will have to recover it by applying log files. Click **Recover** and wait until log files are applied, then re-add the database. Make sure that the **Write** permission is granted to the account being used.

To manually add a Microsoft Exchange database, do the following:

1. On the **Home** tab, click **Add Store > Microsoft Exchange mailbox database** or right-click the **All Stores** node and select **Microsoft Exchange mailbox database**.
2. Click **Browse** to specify the path to the `.edb` file and Exchange logs folder.



Adding Veeam Backup for Microsoft Office 365 Server

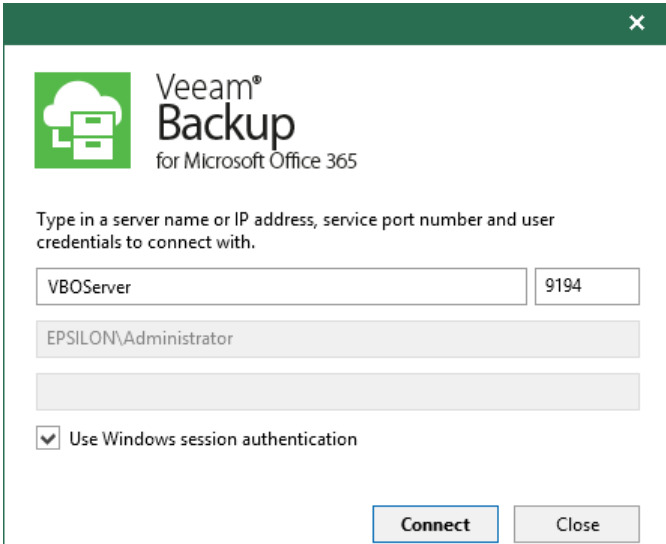
In Veeam Explorer for Microsoft Exchange, you can connect to a Veeam Backup for Microsoft Office 365 server to view backups located on this server.

To connect to a Veeam Backup for Microsoft Office 365 server, do the following:

1. On the **Home** tab, click **Add Store > Veeam Backup for Microsoft Office 365 server** or right-click the **All Stores** node in the navigation pane and select **Add Veeam Backup for Microsoft Office 365 server**.
2. Specify a server name or IP-address and enter credentials to access the specified server.

Select the **Use Windows session authentication** check box to connect with the user account under which you are currently logged in.

3. Click **Connect**.



The screenshot shows a dialog box titled "Veeam® Backup for Microsoft Office 365". It contains a text prompt: "Type in a server name or IP address, service port number and user credentials to connect with." Below this are three input fields: the first contains "VBOServer", the second contains "9194", and the third contains "EPSILON\Administrator". There is a checkbox labeled "Use Windows session authentication" which is checked. At the bottom right are two buttons: "Connect" and "Close".

Adding Veeam Backup for Microsoft Office 365 Service Provider

In Veeam Explorer for Microsoft Exchange, you can connect to a service provider server to add its backups to the application scope and perform a restore directly from such backups.


NOTE:

Make sure that both Veeam Explorer for Microsoft Exchange and Veeam Backup & Replication are installed on the same server and at least one service provider is added to Veeam Backup & Replication.

To add Veeam Backup for Microsoft Office 365 service providers, do the following:

1. On the toolbar, click **Add Store > Veeam Backup for Microsoft Office 365 Service Provider** or use the corresponding context menu command.
2. From the **Select service provider and authentication method** drop-down list, select a service provider that you want to add and choose an authentication method that can be either *Modern authentication* or *Basic authentication*.
4. [For *Modern authentication*] Select a region to which an Office 365 organization of the selected service provider belongs.
5. [For *Modern authentication*] Copy the device code and use it to sign in to Microsoft Azure Active Directory.

For *Basic authentication*, you must enter a user name and password to connect to the service provider server.
6. Select a point-in-time state as of which you want to load Office 365 backups.
To select a state, use the calendar control.
7. Select the **Show items that have been deleted by user** check box to see all the items that were removed.
8. Select the **Show all versions of items that have been modified by user** check box if you want to load modified versions.
9. Click **Connect**.



Veeam Backup

for Microsoft Office 365

Select service provider and authentication method:

office.tech.local (Tenant1)


Modern authentication


Select Office 365 organization region and sign in to Azure AD:

Default

To sign in, authenticate with the below code at:
<https://microsoft.com/devicelogin>

CGJF25HY5

 [Copy code](#)


 Waiting for user logon...

Specify point in time you want to open:

☒ Use the latest available state

☐ Use the following point in time:

Wednesday, May 27, 2020 4:57:23 AM



☒ Show items that have been deleted by user

☒ Show all versions of items that have been modified by user

☐ Hide

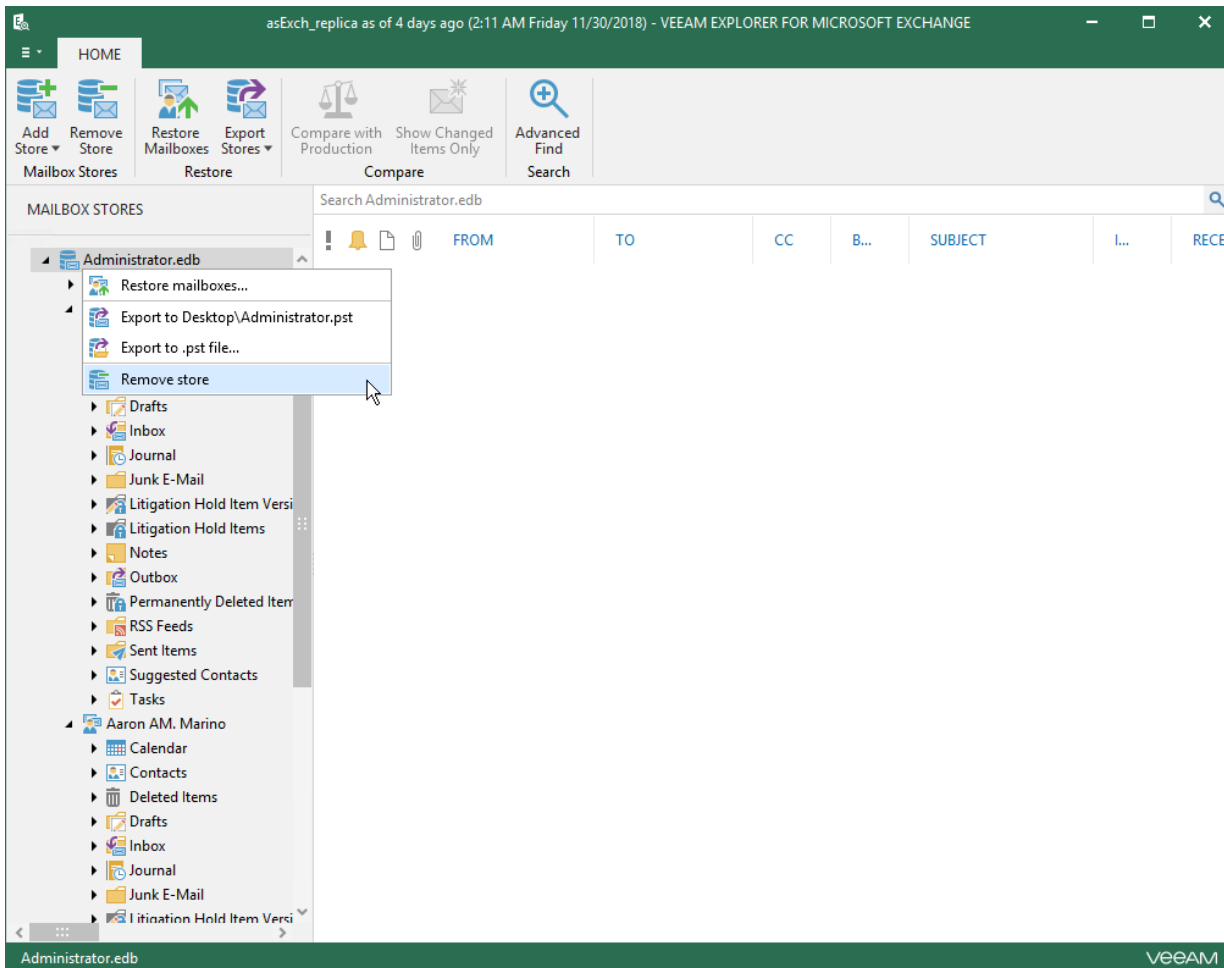
Connect

Close

Removing Stores

Veeam Explorer for Microsoft Exchange allows you to remove an Exchange store from the application scope when you no longer need it.

To remove a store from the application scope, right-click a store in the navigation pane and select **Remove Store**.



Restore

This section explains how to restore data to [Microsoft Office 365](#) and [on-premises Microsoft](#) organizations.

IMPORTANT!

This section explains how to perform a restore in Veeam Explorer for Microsoft Exchange that comes as part of Veeam Backup for Microsoft Office 365 version 4c. For more information on how to restore data in Veeam Explorer for Microsoft Exchange that comes with Veeam Backup for Microsoft Office 365 version 4, see [this section](#) of the Veeam Explorers User Guide.

Restore to Office 365 Organizations

This section explains how to restore data to Microsoft Office 365 organizations with enabled [multi-factor authentication](#) (MFA) and/or [security defaults](#).

For more information, see [Microsoft Office 365 Organizations](#).

When you perform a restore, you can specify a target mailbox, choose an authentication method that you want to use for a restore, specify a target folder to which you want to restore data and configure restore options.

You can also use [1-Click Restore](#) if you do not want to configure a restore session and prefer to use the default settings during a restore.

Restoring Single Mailbox, Folders and Items

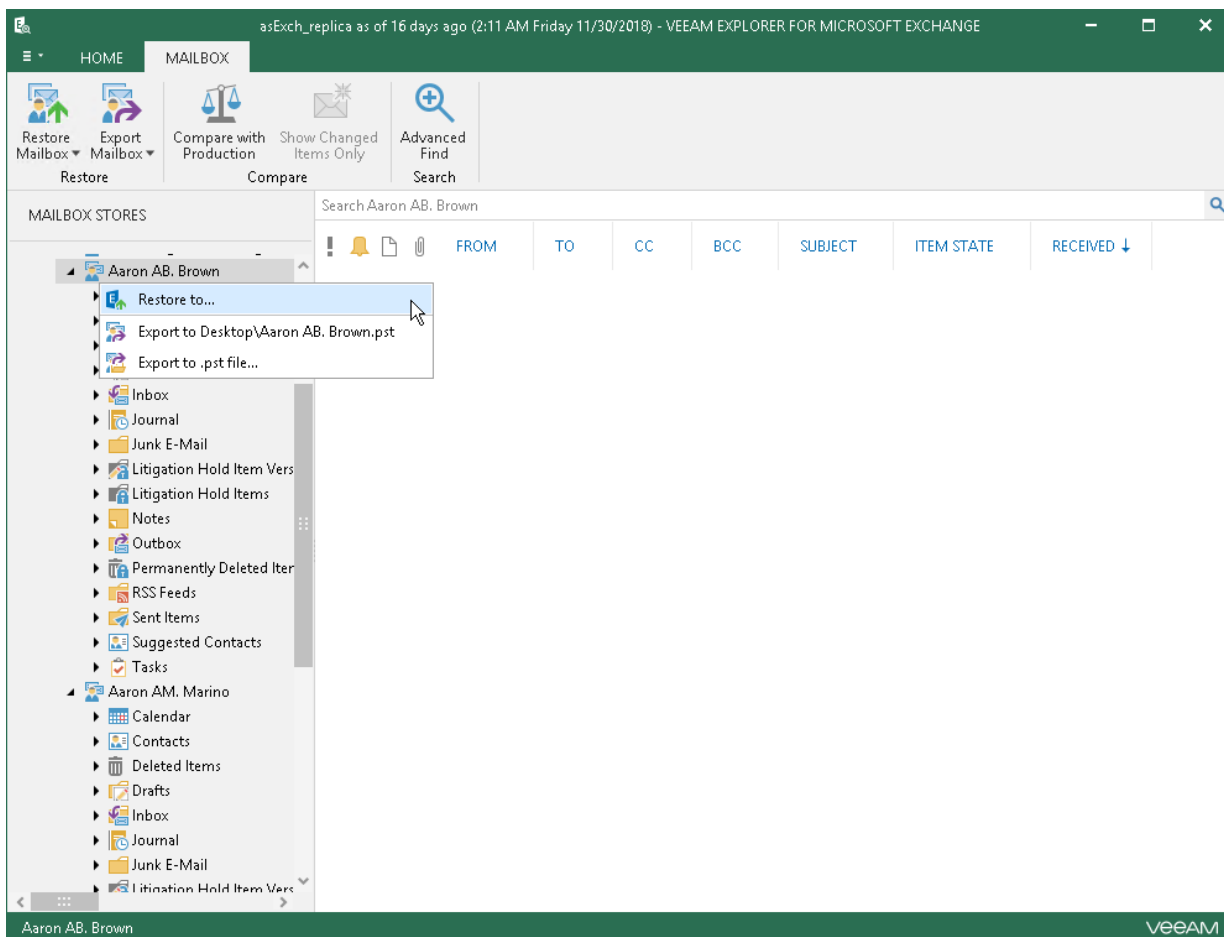
To restore the selected Exchange mailbox, do the following:

1. [Launch the Restore wizard](#).
2. [Specify a target mailbox](#).
3. [Select an authentication method](#).
4. [Log on to Office 365](#).
5. [Specify a CAS server](#).
6. [Specify a target folder](#).
7. [Specify restore options](#).

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. In the navigation panel, select a mailbox, folder or an item that you want to restore.
2. On the **Mailbox/Folder/Items** tab, select **Restore Mailbox/Restore Folder/Restore Item** > **Restore to** or right-click a mailbox, folder or an item and select **Restore to**.



Step 2. Specify Target Mailbox

At this step of the wizard, specify the target mailbox and mailbox location.

To specify mailbox settings, do the following:

1. In the **Mailbox** field, enter a mailbox name to which you want to restore data.

You can specify any name that you want. You can also restore a mailbox to a different organization. For example, you have backed up a mailbox *administrator@abc.onmicrosoft.com*. To restore such a mailbox to a different organization, you can specify, for instance, *administrator@xyz.onmicrosoft.com* to restore a mailbox to the *xyz.onmicrosoft.com* organization.

2. Select **Exchange Online** to restore the specified mailbox to an Exchange Online organization with enabled multi-factor authentication (MFA) and enabled or disabled security defaults. For more information, see [Microsoft Office 365 Organizations](#).

You can also perform a restore of backups created for Exchange Online organizations to on-premises Microsoft Exchange servers and vice versa, as described in [Restore to On-Premises Microsoft Servers](#).

RESTORE WIZARD

Target mailbox

Mailbox:

administrator@abc.onmicrosoft.com

Specify target mailbox location:

☒ Exchange Online

☐ On-premises Microsoft Exchange Server

Back Next Cancel

Step 3. Select Authentication Method

At this step of the wizard, choose whether you want to use modern or basic authentication.

Modern Authentication

To use modern authentication, do the following:

1. From the **Specify authentication method** drop-down list, select *Modern authentication*.
This will allow Veeam Backup for Microsoft Office 365 to use an Azure AD application for a restore. Such an application is used to restore the specified mailbox back to Office 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults. For more information, see [Microsoft Office 365 Organizations](#).
2. From the **Region** drop-down list, select a region to which your Exchange Online organization belongs.
3. In the **Organization name** field, enter a name of your Exchange Online organization.
Make sure that the organization name matches the name specified at the [previous step](#).
4. In the **Application ID** field, enter an identification number of the Azure AD application that you want to use for a restore.
By default, Veeam Explorer for Microsoft Exchange populates this field with an identification number of the application that was used during a backup session. If you want to use another application, make sure to grant this application required permissions, as described in [Azure AD Applications](#).

RESTORE WIZARD

Office 365 connection settings

Specify authentication method:

Modern authentication

Specify region, organization name and Azure AD application to connect with:

Region:

Default

Organization name:

abc.onmicrosoft.com

Application ID:

e7b9bd5b-f8de-4da5-aa4f-0a5f89ba0c79

Back Next Cancel

Basic Authentication

To use basic authentication, do the following:

1. From the **Specify authentication method** drop-down list, select *Basic Authentication*.
2. Enter credentials to connect to the Exchange organization.

When restoring to an on-premises Exchange server, make that the account that you use has both the *Exchange Admin* and the Global Admin roles.

RESTORE WIZARD

Office 365 connection settings

Specify authentication method:

Basic authentication

Specify user account to connect with:

☐ Use current account (TECH\Administrator)

☒ Use the following account:

Username: administrator@abc.onmicrosoft.com

Password:

To connect with an account enabled for multi-factor authentication (MFA), use an app password instead of a user password.

Back Next Cancel

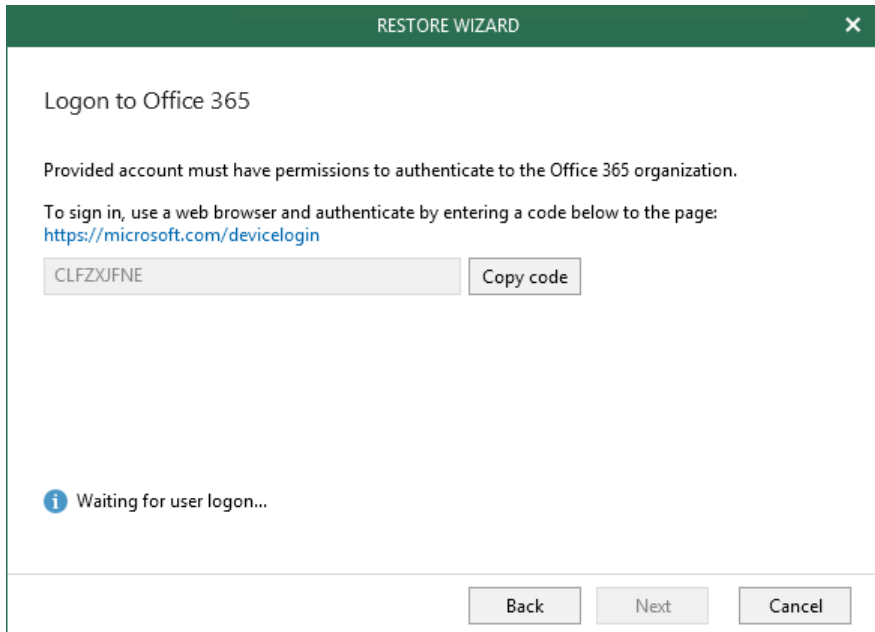
Step 4. Log on to Office 365

[This step is only available if you have selected the *Modern Authentication* option at the [previous step](#).]

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

To sign in to the Microsoft Office 265 organization, do the following:

1. Click **Copy Code** to copy an authentication code.
Mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.
2. Click the link to the Microsoft portal.
3. On the **Microsoft Azure device logon** page, paste the code that you have copied and sign in to Azure.
Make sure to log in with the user account that has both the *ApplicationImpersonation* role and the *Exchange admin* role. For more information, see [this Microsoft article](#).
4. Return to the **Restore Wizard** window and click **Next**.



The screenshot shows a window titled "RESTORE WIZARD" with a close button (X) in the top right corner. The main content area is titled "Logon to Office 365". Below the title, it states: "Provided account must have permissions to authenticate to the Office 365 organization. To sign in, use a web browser and authenticate by entering a code below to the page: <https://microsoft.com/devicelogin>". There is a text input field containing the code "CLFZXJFNE" and a "Copy code" button to its right. At the bottom left, there is an information icon (i) and the text "Waiting for user logon...". At the bottom right, there are three buttons: "Back", "Next", and "Cancel".

Step 5. Specify CAS Server and Folder

[This step is only available if you have selected the *Basic Authentication* option at the [Select Authentication Method](#) step.]

At this step of the wizard, specify a CAS server and provide a folder to which you want to restore data. You can perform a restore to the original folder or specify a custom folder.

To provide a CAS server and target folder, do the following:

1. Specify a CAS server name or its IP address.
This field is populated automatically with the CAS server address from your domain. You can also enter a CAS server manually.
2. Select a folder to which you want to restore data. You can perform a restore to the original folder or specify a custom folder.
When you select to restore to a customer folder, Veeam Explorer for Microsoft Exchange checks if the specified folder exists, if not, it creates a folder automatically. For example, if you specify a path like *Folder1/Folder2/Folder3*, Veeam Backup for Microsoft Office 365 will restore your data to the *Folder3*. You can use both the slash ("/") and the backslash ("\") characters when specifying a path.

RESTORE WIZARD

Target mailbox server and folder

Specify the mailbox server (CAS) to restore the selected items to:

outlook.office365.com

Specify the folder to restore items to:

☐ Restore to the original folder

☒ Restore to the following folder:

new_target_folder

Back Next Cancel

Step 6. Specify Target Folder

[This step is only available if you have selected the *Modern Authentication* option at the [Select Authentication Method](#).]

At this step of the wizard, select a target folder to which you want to restore the [specified mailbox](#). You can perform a restore to the original folder or specify a custom folder.

When you select to restore to a customer folder, Veeam Explorer for Microsoft Exchange checks if the specified folder exists, if not, it creates a folder automatically. For example, if you specify a path like *Folder1/Folder2/Folder3*, Veeam Backup for Microsoft Office 365 will restore your data to the *Folder3*. You can use both the slash ("/") and the backslash ("\") characters when specifying a path.

RESTORE WIZARD

Target folder

Specify the folder to restore items to:

☐ Restore to the original folder

☐ Restore to the following folder:

Back Next Cancel

Step 7. Specify Restore Options

At this step of the wizard, specify restore options:

- **Changed items**
To restore items that have been changed.
- **Missing Items**
To restore missing items.
- **Mark restored items as unread**
To mark restored items as unread.

To prevent certain folders from being restored, click the **Exclude folders** link and select folders to exclude.

Restoring Multiple Mailboxes

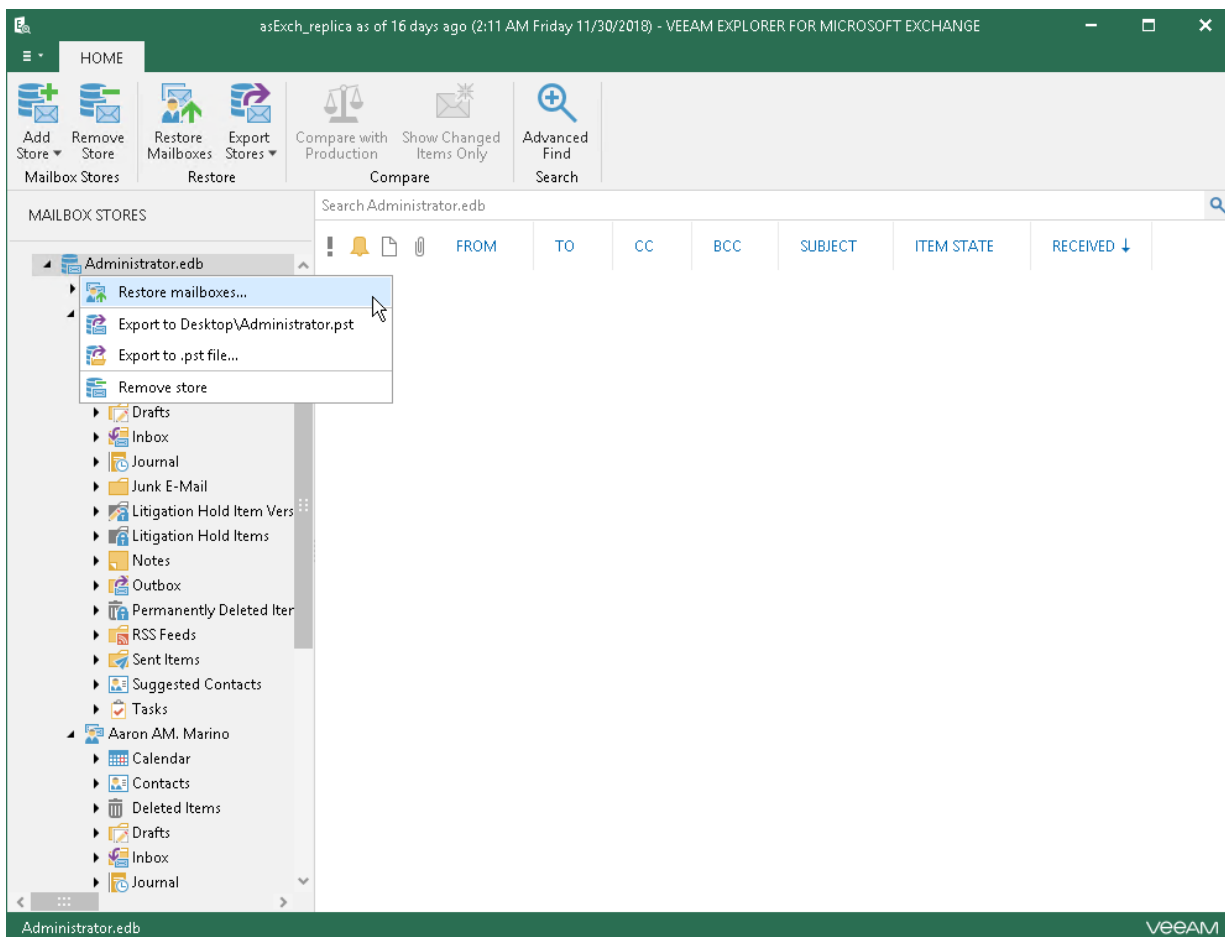
To restore multiple Exchange mailboxes, do the following:

1. [Launch the Restore wizard.](#)
2. [Select an authentication method.](#)
3. [Log on to Office 365.](#)
4. [Select mailboxes to restore.](#)
5. [Select restore options.](#)

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. In the navigation panel, select a mailbox that you want to restore.
2. On the **Home** tab, select **Restore Mailboxes** or right-click a container and select **Restore mailboxes**.



Step 2. Select Authentication Method

At this step of the wizard, choose whether you want to use modern or basic authentication.

Modern Authentication

To use modern authentication, do the following:

1. From the **Specify authentication method** drop-down list, select *Modern authentication*.

This will allow Veeam Backup for Microsoft Office 365 to use an Azure AD application for a restore. Such an application is used to restore the specified mailbox back to Office 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults.

For more information, see [Microsoft Office 365 Organizations](#).

2. In the **Application ID** field, enter an identification number of the Azure AD application that you want to use for a restore.

By default, Veeam Explorer for Microsoft Exchange populates this field with the identification number of the application that was used during a backup session. If you want to use another application, make sure to grant this application required permissions, as described in [Azure AD Applications](#).

RESTORE WIZARD

Specify Office 365 credentials

Specify authentication method:

Modern authentication

Specify an Azure AD application to connect with:

Application ID: e7b9bd5b-f8de-4da5-aa4f-0a5f89ba0c79

Back Next Cancel

Basic Authentication

To use basic authentication, do the following:

1. From the **Specify authentication method** drop-down list, select *Basic Authentication*.
2. Enter credentials to connect to the Exchange organization.

When restoring to an on-premises Exchange server, make that the account that you use has both the *Exchange Admin* and the Global Admin roles.

RESTORE WIZARD

Specify Office 365 credentials

Specify authentication method:

Basic authentication

Specify user account to connect with:

Username: administrator@abc.onmicrosoft.com

Password: [masked]

To connect with an account enabled for multi-factor authentication (MFA), use an app password instead of a user password.

Back Next Cancel

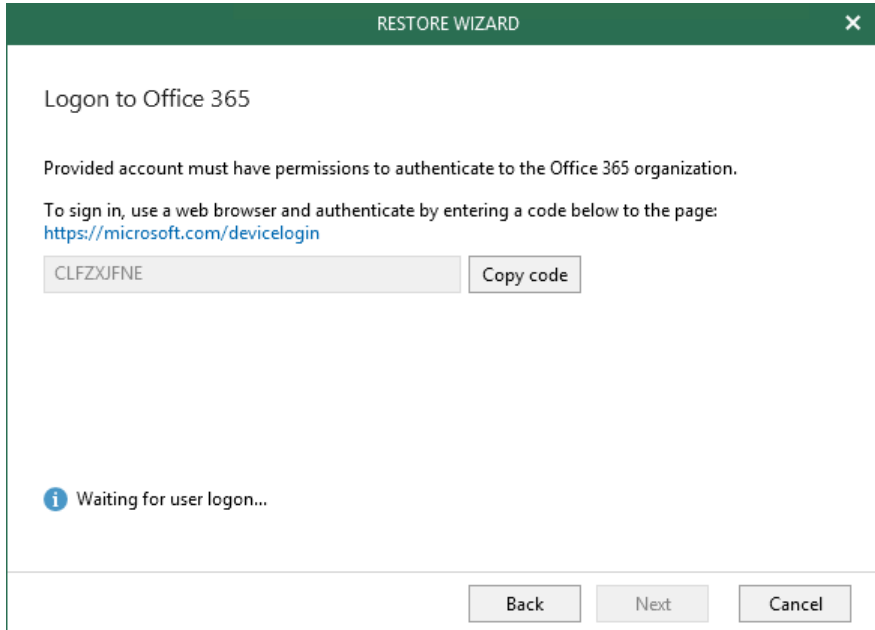
Step 3. Log on to Office 365

[This step is only available if you have selected the *Modern Authentication* option at the [previous step](#).]

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

To sign in to the Microsoft Office 265 organization, do the following:

1. Click **Copy Code** to copy an authentication code.
Mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.
2. Click the link to the Microsoft portal.
3. On the **Microsoft Azure device login** page, paste the code that you have copied and sign in to Azure.
Make sure to log in with the user account that has both the *ApplicationImpersonation* role and the *Exchange admin* role. For more information, see [this Microsoft article](#).
4. Return to the **Restore Wizard** window and click **Next**.



RESTORE WIZARD

Login to Office 365

Provided account must have permissions to authenticate to the Office 365 organization.

To sign in, use a web browser and authenticate by entering a code below to the page:
<https://microsoft.com/devicelogin>

CLFZXJFNE Copy code

i Waiting for user login...

Back Next Cancel

Step 4. Select Mailboxes to Restore

At this step of the wizard, select mailboxes that you want to restore.

To see the full email address in the **E-Mail** column, click **Resolve selected mailboxes**.

RESTORE WIZARD

Select mailboxes to restore

MAILBOX ↑	E-MAIL
<input checked="" type="checkbox"/> Administrator	administrator@abc.onmicrosoft.com
<input checked="" type="checkbox"/> IT	IT@abc.onmicrosoft.com

2 mailboxes selected
[Resolve selected mailboxes](#)

Back

Next

Cancel

Step 5. Select Restore Options

At this step of the wizard, specify restore options:

- **Changed items.** To restore items that have been changed.
- **Missing Items.** To restore missing items.
- **Mark restored items as unread.** To mark restored items as unread.

When restoring multiple mailboxes, select the **Finish the restore of recent items before restoring the remaining items** check box and set the value in the **Restore items for the last <N> days first** field to restore multiple mailboxes in "chunks", when the most recent items in the backup will be processed first.

To prevent certain folders from being recovered, click the **Exclude folders** link and select folders to exclude.

RESTORE WIZARD

Specify the restore options

Restore the following items:

☒ Changed items
☒ Missing items

Flag restored items:

☒ Mark restored items as unread

Mass mailbox restore

☒ Finish the restore of recent items before restoring the remaining items

Restore items for the last days first

[Exclude folders...](#)

Back

Restore

Cancel

Restore to On-Premises Microsoft Servers

This section explains how to restore data to on-premises Microsoft Exchange servers.

For more information, see [On-Premises Microsoft Organizations](#).

When you perform a restore, you can specify a target mailbox, choose an authentication method that you want to use for a restore, specify a target folder to which you want to restore data and configure restore options.

You can also use [1-Click Restore](#) if you do not want to configure a restore session and prefer to use the default settings during a restore.

Restoring Single Mailbox, Folders and Items

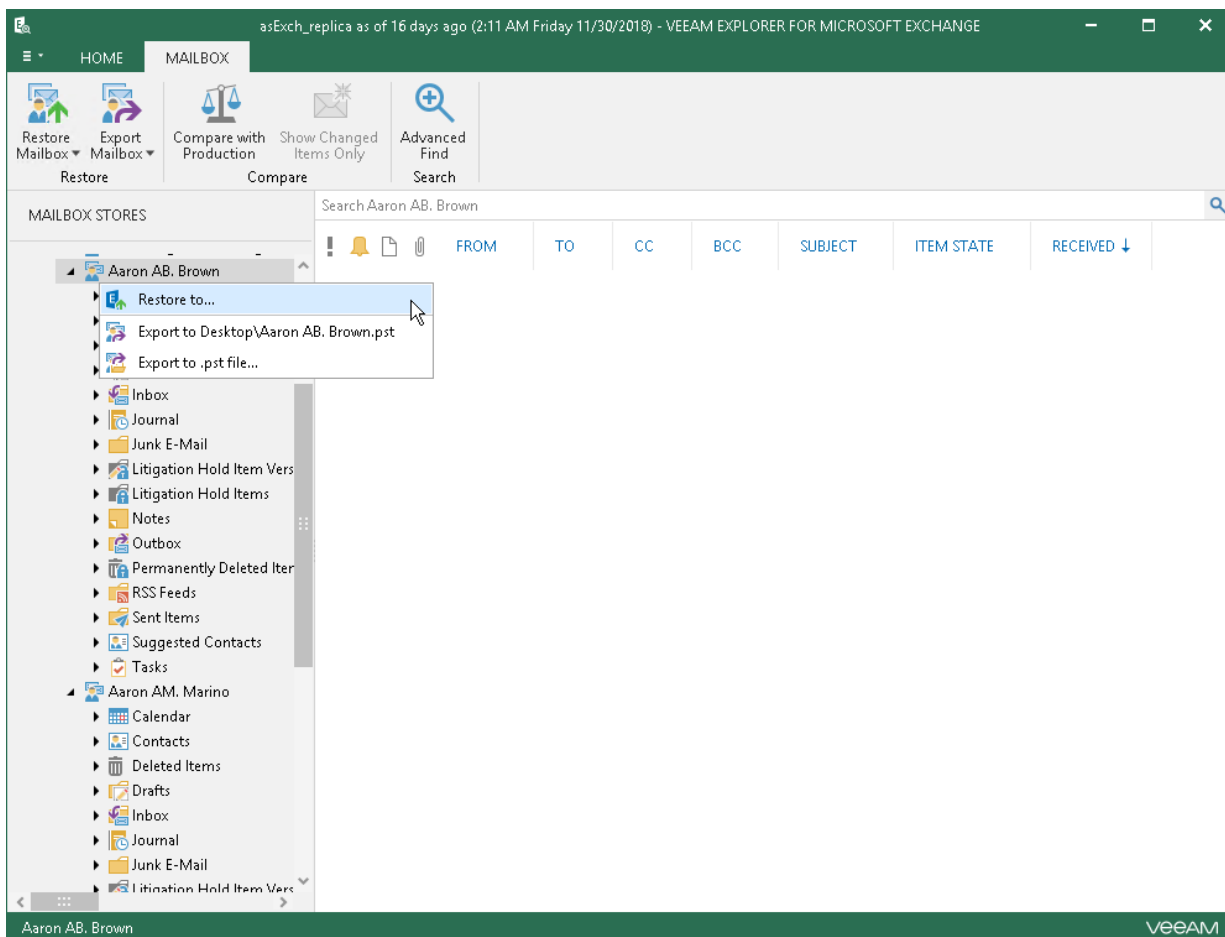
To restore mailboxes, folders and items, do the following:

1. [Launch the Restore wizard](#).
2. [Specify a target mailbox](#).
3. [Specify a user account](#).
4. [Specify a CAS server and target folder](#).
5. [Specify restore options](#).

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. In the navigation panel, select a mailbox that you want to restore.
2. On the **Mailbox** tab, select **Restore Mailbox > Restore to** or right-click a mailbox and select **Restore to**.



Step 2. Specify Target Mailbox

At this step of the wizard, specify the target mailbox and mailbox location.

To specify mailbox settings, do the following:

1. In the **Mailbox** field, enter a mailbox name to which you want to restore data.
2. Select **On-premises Microsoft Exchange Server** to restore the specified mailbox to an on-premises Microsoft Exchange organization. For more information, see [On-Premises Microsoft Organizations](#).

You can also perform a restore of backups created for on-premises Microsoft Exchange organizations to Exchange Online organizations and vice versa, as described in [Restore to Office 365 Organizations](#).

RESTORE WIZARD

Target mailbox

Mailbox:

administrator@tech.com

Specify target mailbox location:

☐ Microsoft Office 365

☒ On-premises Microsoft Exchange Server

Back Next Cancel

Step 3. Specify User Account

At this step of the wizard, specify an account that you want to use to connect to the Exchange server in your domain.

RESTORE WIZARD

On-Premises Microsoft Exchange Server settings

Specify user account to connect with:

☐ Use current account (TECH\Administrator)

☒ Use the following account:

Username: TECH\Restore

Password: ●●●●●●●●

Back Next Cancel

Step 4. Specify CAS Server and Target Folder

At this step of the wizard, specify a CAS server and provide a folder to which you want to restore data. You can perform a restore to the original folder or specify a custom folder.

To provide a CAS server and target folder, do the following:

1. Specify a CAS server name or its IP address.

This field is populated automatically with the CAS server address from your domain. You can also enter a CAS server manually.

2. Select a folder to which you want to restore data. You can perform a restore to the original folder or specify a custom folder.

When you select to restore to a customer folder, Veeam Explorer for Microsoft Exchange checks if the specified folder exists, if not, it creates a folder automatically. For example, if you specify a path like *Folder1/Folder2/Folder3*, Veeam Backup for Microsoft Office 365 will restore your data to the *Folder3*. You can use both the slash ("/") and the backslash ("\") characters when specifying a path.

The screenshot shows a window titled "RESTORE WIZARD" with a close button (X) in the top right corner. The main heading is "Specify target mailbox server and folder". Below this, there is a label "Specify the mailbox server (CAS) to restore the selected items to:" followed by a text input field containing "exchange2013". Underneath, there is a label "Specify the folder to restore items to" and two radio button options: "Restore to the original folder" (which is selected) and "Restore to the following folder:". Below the second option is an empty text input field. At the bottom of the window, there are three buttons: "Back", "Next" (which is highlighted with a blue border), and "Cancel".

Step 5. Specify Restore Options

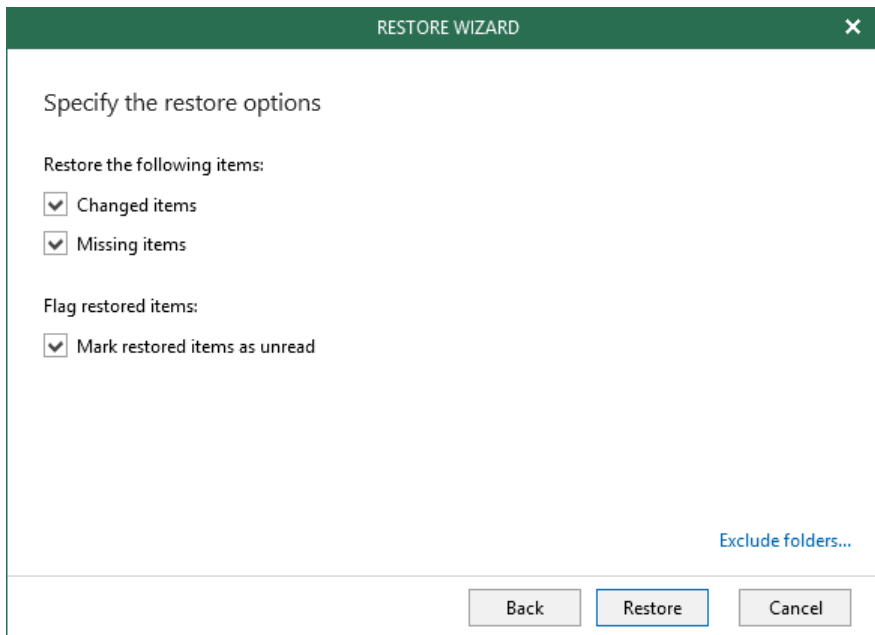
At this step of the wizard, specify restore options:

- **Changed items.** To restore items that have been changed.
- **Missing Items.** To restore missing items.
- **Mark restored items as unread.** To mark restored items as unread.

To prevent certain folders from being restored, click **Exclude folders** and select folders to exclude.

NOTE:

The **Exclude folders** link is not available when restoring folders and items.



Restoring Multiple mailboxes

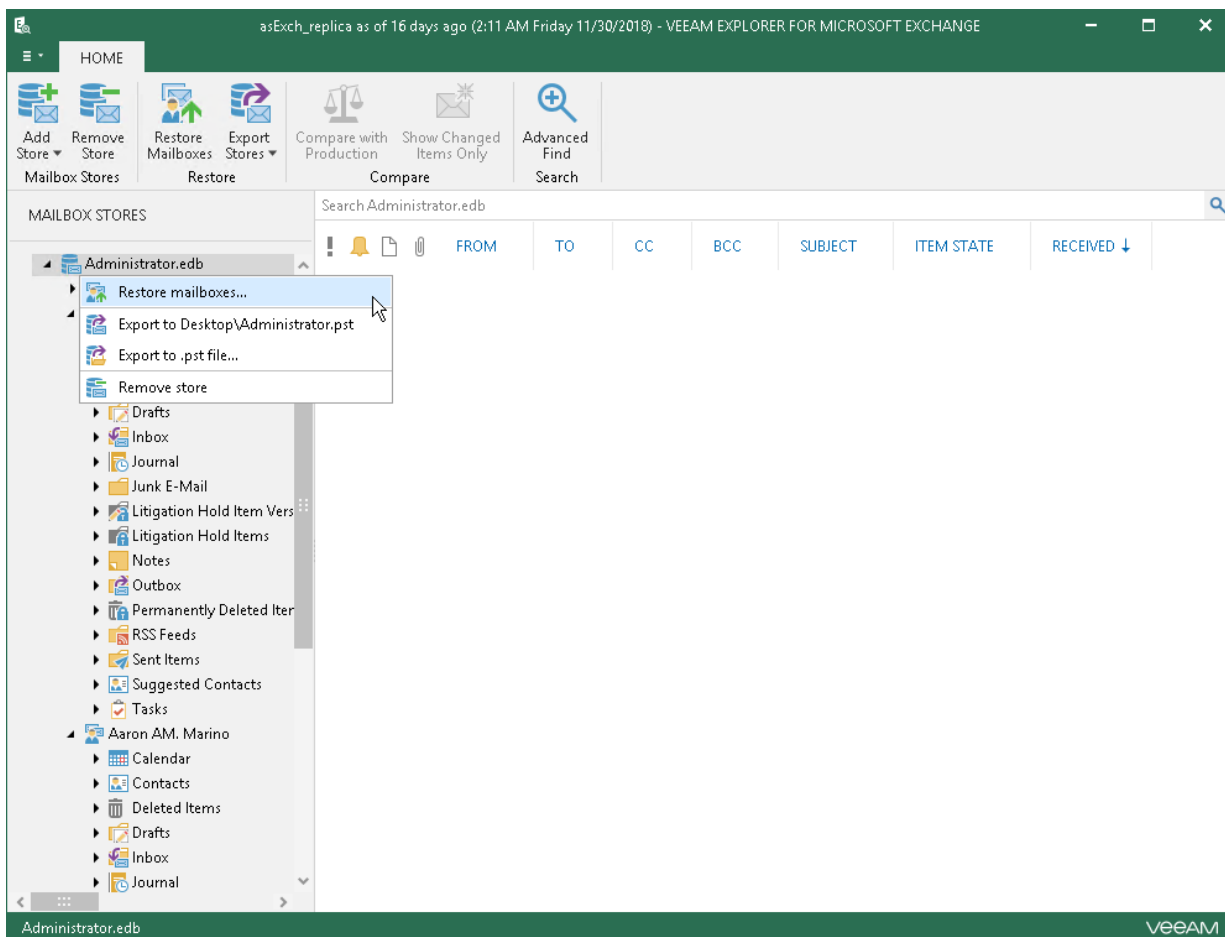
To restore multiple Exchange mailboxes, do the following:

1. [Launch the Restore wizard.](#)
2. [Specify a domain and credentials.](#)
3. [Select mailboxes to restore.](#)
4. [Specify a target mailbox server.](#)
5. [Select restore options.](#)

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. In the navigation panel, select a mailbox that you want to restore.
2. On the **Home** tab, select **Restore Mailboxes** or right-click a container and select **Restore mailboxes**.



Step 2. Specify Domain and Credentials

At this step of the wizard, enter a domain name where your CAS server resides and provide credentials.

Step 3. Select Mailboxes to Restore

At this step of the wizard, select mailboxes that you want to restore.

To see the full email address in the **E-Mail** column, click **Resolve selected mailboxes**.

The screenshot shows the 'RESTORE WIZARD' window with the title bar 'RESTORE WIZARD' and a close button. The main heading is 'Select mailboxes to restore'. Below it is a table with two columns: 'MAILBOX ↑' and 'E-MAIL'. The table contains three rows: a header row, a row for 'Administrator' with email 'administrator@abc.onmicrosoft.com', and a row for 'IT' with email 'IT@abc.onmicrosoft.com'. All three rows have a checked checkbox in the first column. Below the table, it says '2 mailboxes selected' and a blue link 'Resolve selected mailboxes'. At the bottom are three buttons: 'Back', 'Next' (highlighted with a blue border), and 'Cancel'.

MAILBOX ↑	E-MAIL
<input checked="" type="checkbox"/> Administrator	administrator@abc.onmicrosoft.com
<input checked="" type="checkbox"/> IT	IT@abc.onmicrosoft.com

2 mailboxes selected [Resolve selected mailboxes](#)

Back Next Cancel

Step 4. Specify Target Mailbox Server

At this step of the wizard, specify a target server to which you want to restore mailboxes.

The screenshot shows the 'RESTORE WIZARD' window with the title bar 'RESTORE WIZARD' and a close button. The main heading is 'Specify target mailbox server'. Below it is the text 'Specify the mailbox server (CAS) to restore the selected items to:'. Underneath is a text input field containing 'exchange2013'. At the bottom are three buttons: 'Back', 'Next' (highlighted with a blue border), and 'Cancel'.

Specify target mailbox server

Specify the mailbox server (CAS) to restore the selected items to:

exchange2013

Back Next Cancel

Step 5. Select Restore Options

At this step of the wizard, specify restore options:

- **Changed items.** To restore items that have been changed.
- **Missing Items.** To restore missing items.
- **Mark restored items as unread.** To mark restored items as unread.

When restoring multiple mailboxes, select the **Finish the restore of recent items before restoring the remaining items** check box and set the value in the **Restore items for the last <N> days first** field to restore multiple mailboxes in "chunks", when the most recent items in the backup will be processed first.

To prevent certain folders from being recovered, click the **Exclude folders** link and select folders to exclude.

RESTORE WIZARD

Specify the restore options

Restore the following items:

☒ Changed items

☒ Missing items

Flag restored items:

☒ Mark restored items as unread

Mass mailbox restore

☒ Finish the restore of recent items before restoring the remaining items

Restore items for the last

7

days first

Exclude folders...

Back

Restore

Cancel

1-Click Restore

The *1-Click Restore* feature allows you to quickly recover Exchange mailboxes, folders and items according to the following:

- The original Exchange server, original folder and the original mailbox name are restored.
- Both changed and missing items are restored.
- Restored items are marked as unread.
- No folders are excluded.

1-Click restore is a convenient feature when you do not want to configure a restore session and prefer to restore data with the default settings.

Restoring to Office 365 Organizations

To perform *1-Click Restore* to Office 365 organizations, do the following:

1. [Launch the Restore wizard.](#)
2. [Select an authentication method.](#)
3. [Log on to Office 365.](#)

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. In the navigation panel, select a mailbox, folder or item that you want to restore.
2. On the **Mailbox/Folder/Items** tab, select **Restore Mailbox/Restore Folder/Restore Item** > **Restore to <mailbox_name>** or right-click a mailbox/folder/item and select **Restore to <mailbox_name>**.

Step 2. Select Authentication Method

At this step of the wizard, choose whether you want to use modern or basic authentication.

Modern Authentication

To use modern authentication, do the following:

1. From the **Specify authentication method** drop-down list, select *Modern authentication*.

This will allow Veeam Backup for Microsoft Office 365 to use an Azure AD application for a restore. Such an application is used to restore the specified mailbox back to Office 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults.

For more information, see [Microsoft Office 365 Organizations](#).
2. In the **Application ID** field, enter an identification number of the Azure AD application that you want to use for a restore.

By default, Veeam Explorer for Microsoft Exchange populates this field with the identification number of the application that was used during a backup session. If you want to use another application, make sure to grant this application required permissions, as described in [Azure AD Applications](#).

RESTORE WIZARD

Specify Office 365 credentials

Specify authentication method:

Modern authentication

Specify an Azure AD application to connect with:

Application ID: e7b9bd5b-f8de-4da5-aa4f-0a5f89ba0c79

Back Next Cancel

Basic Authentication

To use basic authentication, do the following:

1. From the **Specify authentication method** drop-down list, select *Basic Authentication*.
2. Enter credentials to connect to the Exchange organization and click **Connect**.

Make that the account that you use has both the *Exchange Admin* and the *Global Admin* roles.

RESTORE WIZARD

Office 365 connection settings

Specify authentication method:

Basic authentication

Specify user account to connect with:

Username: administrator@abc.onmicrosoft.com

Password: [masked with dots]

i To connect with an account enabled for multi-factor authentication (MFA), use an app password instead of a user password.

Back Restore Cancel

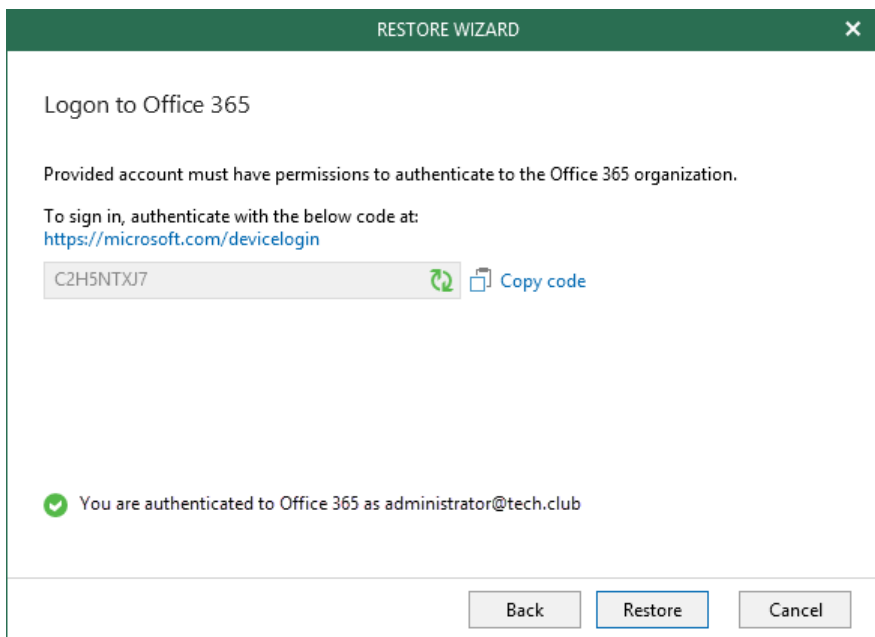
Step 3. Log on to Office 365

[This step is only available if you have selected the *Modern Authentication* option at the [previous step](#).]

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

To sign in to the Microsoft Office 265 organization, do the following:

1. Click **Copy Code** to copy an authentication code.
Mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.
2. Click the link to the Microsoft portal.
3. On the **Microsoft Azure device logon** page, paste the code that you have copied and sign in to Azure.
Make sure to log in with the user account that has both the *ApplicationImpersonation* role and the *Exchange admin* role. For more information, see [this Microsoft article](#).
4. Return to the **Restore Wizard** window and click **Restore**.



Restoring to On-Premises Microsoft Servers

To perform *1-Click Restore* to on-premises Microsoft servers, do the following:

1. [Launch the Restore wizard](#).
2. [Specify a user account](#).

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. In the navigation panel, select a mailbox, folder or item that you want to restore.
2. On the **Mailbox/Folder/Items** tab, select **Restore Mailbox/Restore Folder/Restore Item > Restore to <mailbox_name>** or right-click a mailbox/folder/item and select **Restore to <mailbox_name>**.

Step 2. Specify User Account

At this step of the wizard, specify an account that you want to use to connect to the Exchange server.

RESTORE WIZARD

×

On-Premises Microsoft Exchange Server settings

Specify user account to connect with:

Username: tech\Administrator

Password: ●●●●●●●●

Back

Restore

Cancel

Export

Continue with this section to learn more about exporting Microsoft Exchange data.

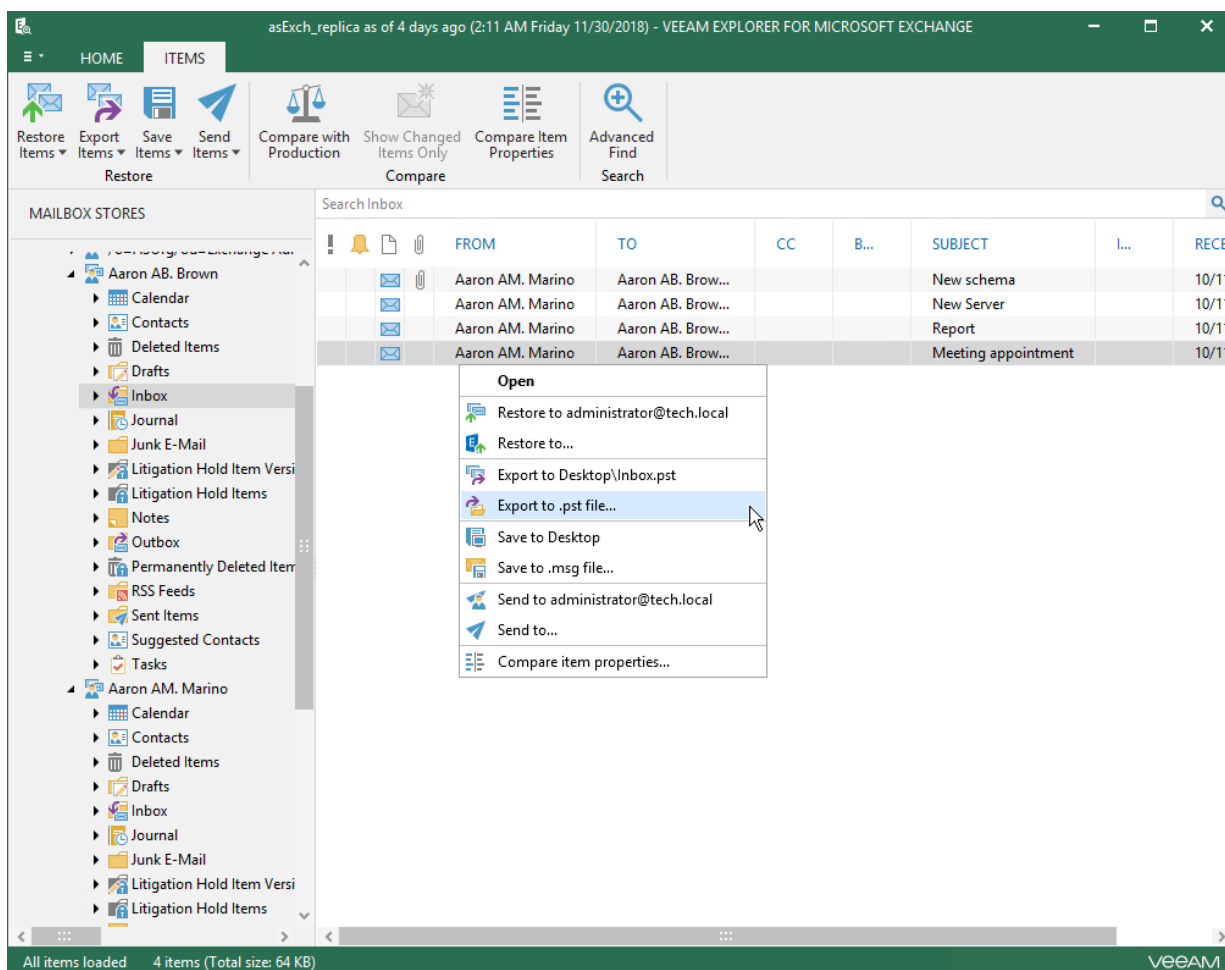
TIP:

Before exporting data, make sure to read [Considerations and Limitations](#).

Exporting to Custom Location

To export objects to the custom location, do the following:

1. In the navigation pane, select a folder or in the preview pane, select an item.
2. On the **Folder/Items** tab, select **Export Folder/Item > Export to .pst file** or right-click a folder/item and select **Export to .pst file**.



3. In the **Export Folder/Export Mail Item** dialog, do the following:
 - In the **Export location** field, specify the name and location for the new *.pst* file.
 - Select the **Apply filter** check box and enter keywords to export only those items that match specified criteria. To provide multiple keywords, use the *OR* logical operator as the delimiter.
Veeam Explorer for Microsoft Exchange will check for the specified keywords in all fields such as **From**, **To**, **Subject** and **Body**.
The **Apply filter** option is only available when exporting folders and mailboxes, not items.
 - Select the **Limit PST size to** check box and specify the size of which to export *.pst* files.
With this option, Veeam Explorer for Microsoft Exchange will create multiple *.pst* files as of the specified size.

EXPORT FOLDER

×

Specify the target path and optional settings:

Export location:

C:\Users\Administrator.TECH\Desktop\Inbox.pst

Browse...

☒ Apply filter:

task

☒ Limit PST size to:

1

GB (additional PST files will be created as needed)

Export

Cancel

Using 1-Click Export

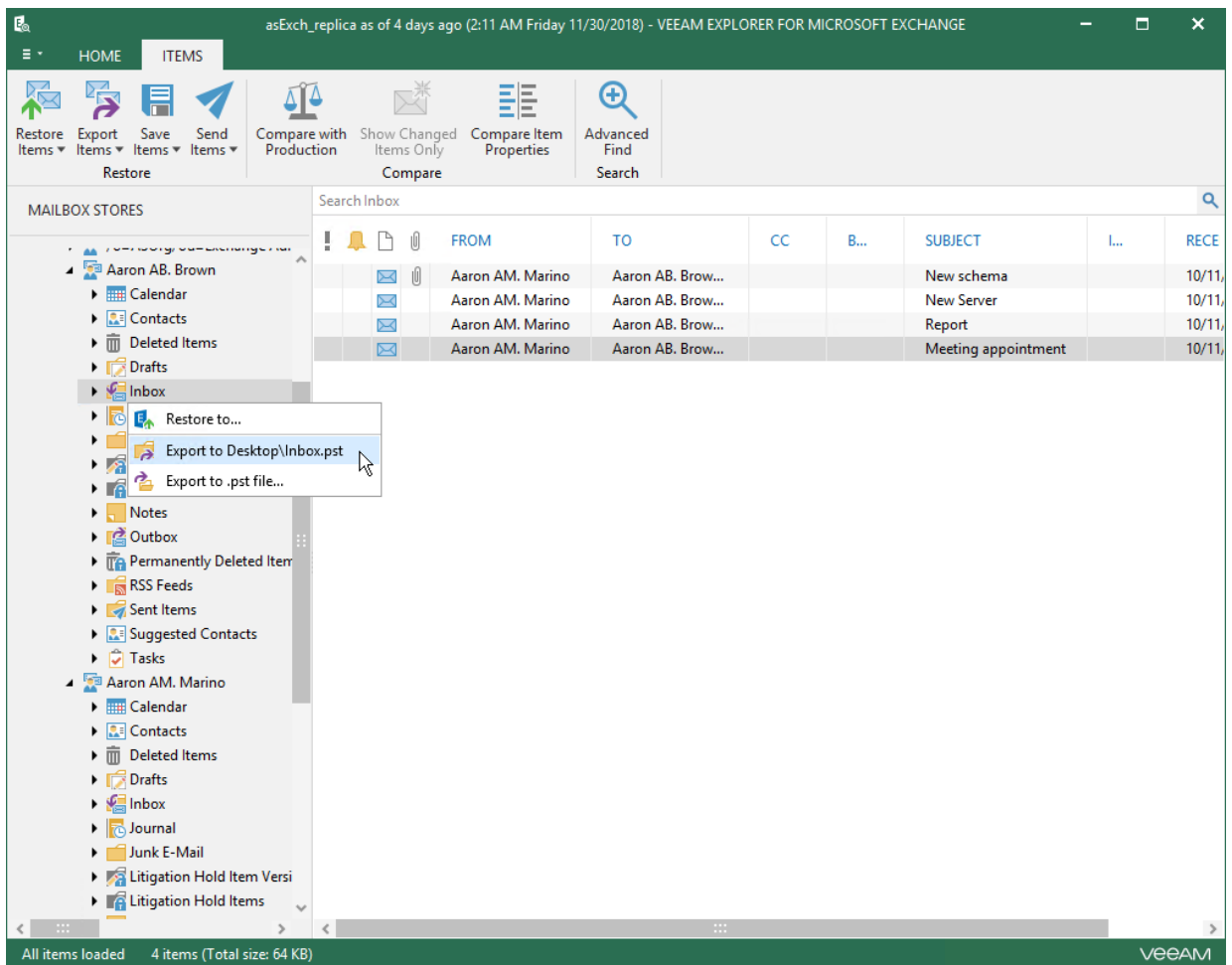
Veeam Explorer for Microsoft Exchange allows you to quickly export mailbox store data as *.pst* files.

NOTE:

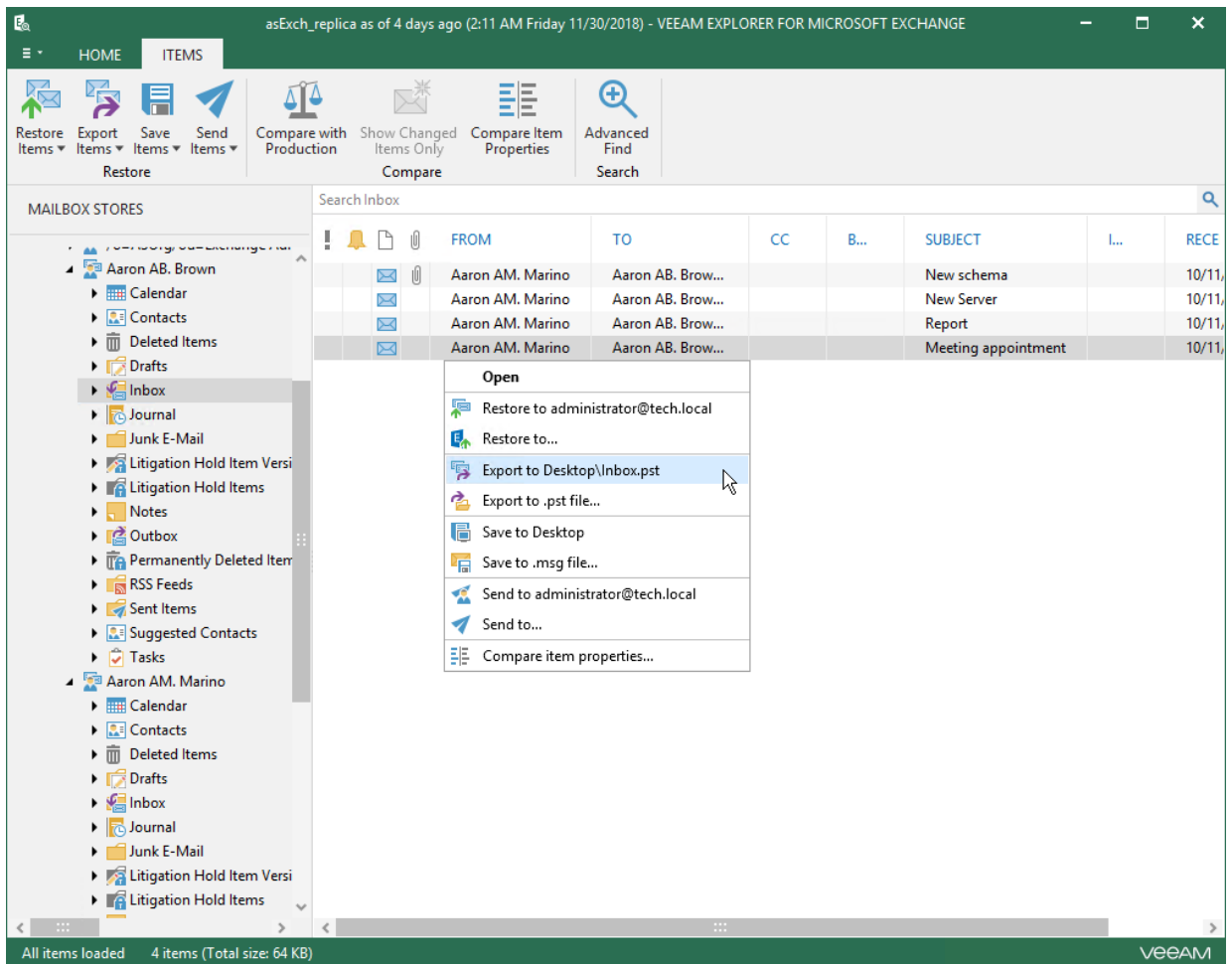
Export operations require Microsoft Outlook to be installed on a computer running Veeam Explorer for Microsoft Exchange.

Depending on the object type you want to export, do the following:

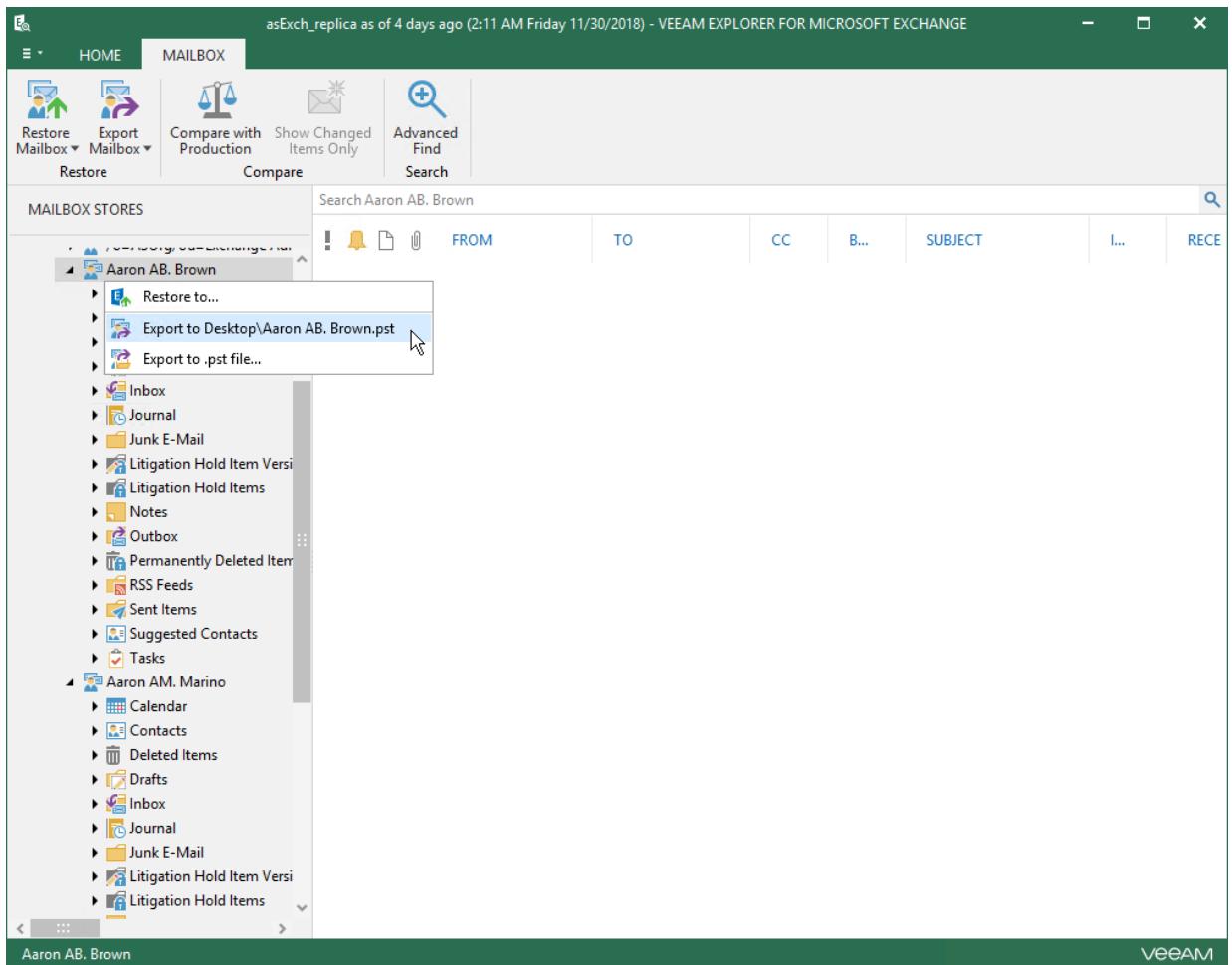
- To export a folder, select it in the navigation pane and on the **Folder** tab, click **Export Folder > Export to <default_location>\<original_folder_name>.pst** or use the corresponding context menu command.



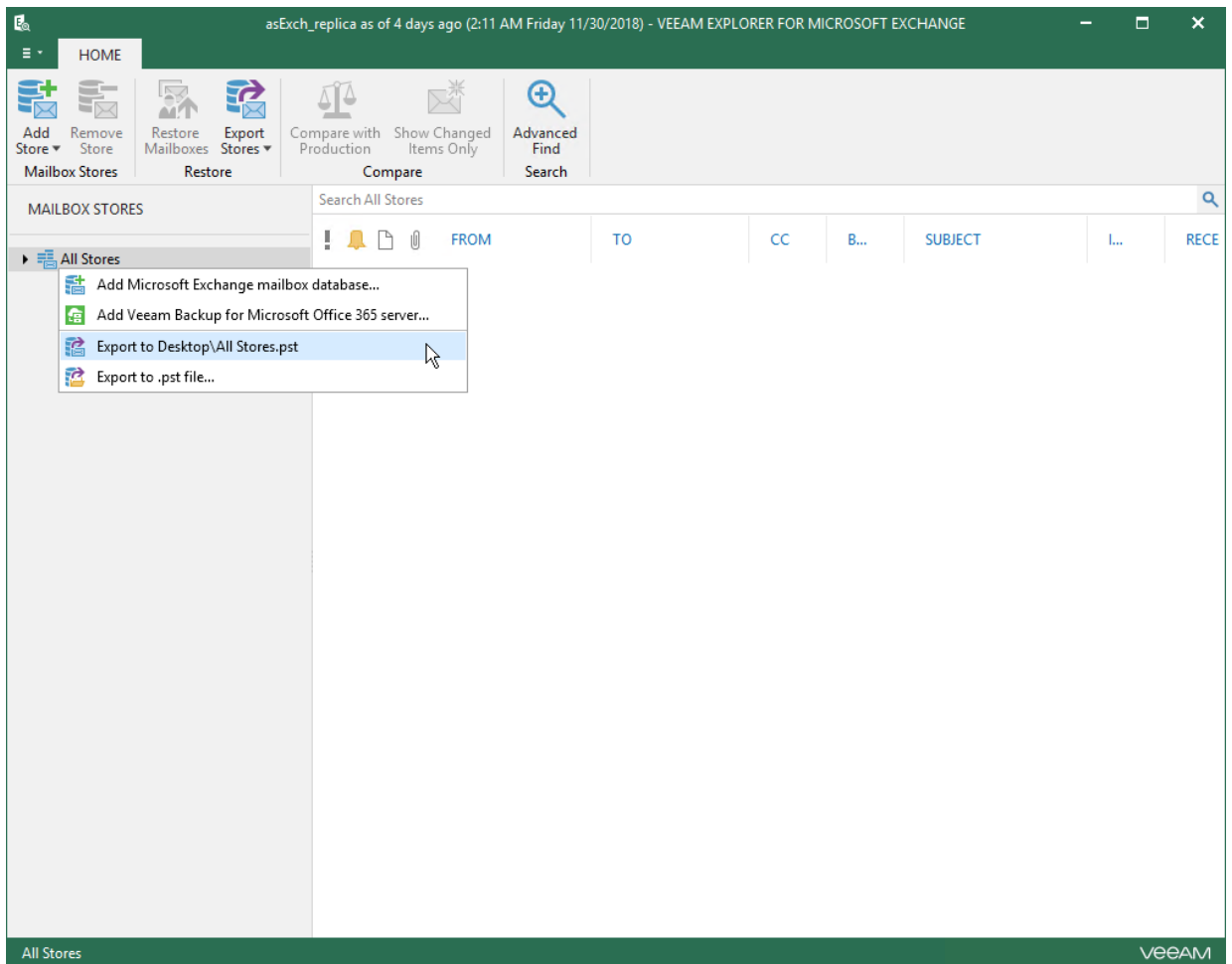
- To export an item, select it in the navigation pane and on the **Items** tab, click **Export Items > Export to <default_location>\<original_folder_name>.pst** or use the corresponding context menu command.



- To export a mailbox, select it in the navigation pane and on the **Mailbox** tab, click **Export mailbox > Export to <default_location>\<original_mailbox_name>.pst** or use the corresponding context menu command.



- To export a mailbox store or all stores added to the scope, select a store or select the **All Stores** node and click **Export** on the **Home** tab.



Receiving Export Reports

Veeam Explorer for Microsoft Exchange can deliver reports that show summary information about export operations.

Consider the following:

- If you want export reports to be delivered, make sure to configure an SMTP server in Veeam Explorer for Microsoft Exchange and/or Veeam Backup & Replication notification settings.

For more information, see the [Configuring SMTP Settings](#) section of this guide and the [Configuring Global Email Notification Settings](#) section of the Veeam Backup & Replication User Guide.

- A server with Veeam Explorer for Microsoft Exchange and Veeam Backup & Replication must be in a domain.
- Export reports are delivered automatically upon each export session.

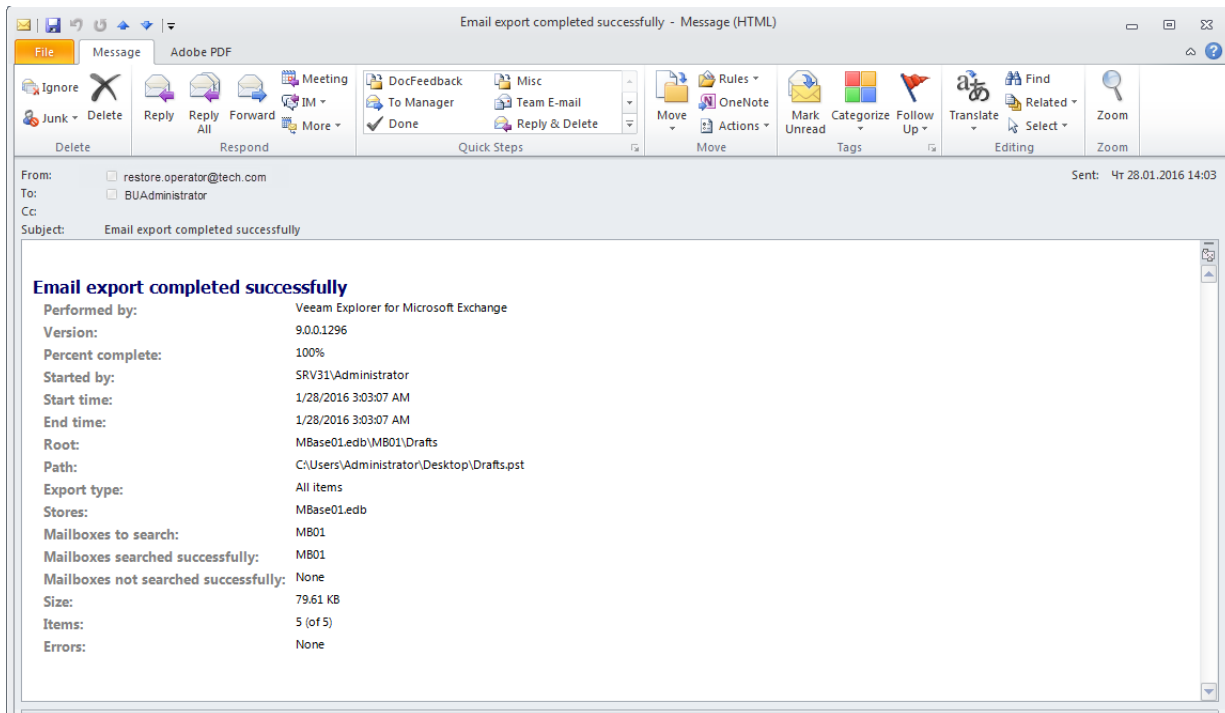
You can use [Export to Custom Location](#) or [1-Click Export](#).

- Recipients of the report are chosen as follows:
 - The recipient is always the current user account under which Veeam Explorer for Microsoft Exchange is running when using only Veeam Explorer for Microsoft Exchange notification settings.
 - The recipient is always the user account provided in Veeam Backup & Replication notification settings when using only Veeam Backup & Replication settings.
 - If you have configured both Veeam Explorer for Microsoft Exchange and Veeam Backup & Replication notification settings, the report will be sent to both recipients.

The following table lists fields that are shown in the report.

Report field	Description
Performed by	Veeam Explorer for Microsoft Exchange
Version	Shows the Veeam Explorer for Microsoft Exchange build number.
Percent complete	Shows the number of items included in the <i>.pst</i> file.
Started by	Shows the user account generated the report.
Start time, End time	Shows the creation time of a report.
Root	Shows the object path.
Path	Shows the path to the database file.
Export type	Shows the export type.
Stores	Shows a datastore name from which items have been exported.
Mailboxes to search	Shows a mailbox name from which items have been exported.

Mailboxes searched successfully, Mailboxes not searched successfully	Shows results for mailboxes to search.
Size	Shows the total size of exported items.
Items	Shows the number of exported items.
Errors	Shows errors that occurred during export.



Compare

IMPORTANT!

This section explains how to perform a compare in Veeam Explorer for Microsoft Exchange that comes as part of Veeam Backup for Microsoft Office 365 version 4c. For more information on how to compare data in Veeam Explorer for Microsoft Exchange that comes with Veeam Backup for Microsoft Office 365 version 4, see [this section](#) of the Veeam Explorers User Guide.

This section explains how to compare data in a backup file with that of the production state.

1. In the navigation pane, select an object and click **Compare with Production** on the toolbar.
2. Proceed to either [Compare to Office 365 Organizations](#) or [Compare to On-Premises Microsoft Servers](#).
3. After the authorization process is complete, click **Show Changed Items Only** on the toolbar to view only those items that have been changed.

To view the details on what exactly has changed since the last backup, right-click an item and select **Compare item properties**. The discrepancies will be shown in the **Compare Message Properties** window. If both objects are equal, nothing will be displayed.

To show unchanged objects, select **Show unchanged properties** in the top-right corner. To show system properties, select **Show system properties**.

Double-click **Body** to see the body message.

To compare a single item, right-click an item and select **Compare item properties**.

COMPARE MESSAGE PROPERTIES

×

Properties: ☒ Show unchanged properties ☒ Show system properties

NAME	BACKUP	PRODUCTION
Attachments (No changes)		
▾ Recipients		
▸ To	Aaron.Brown@asdomain.local	Aaron.Brown@asdomain.local
▸ To	Jane.Summers@asdomain.local	Jane.Summers@asdomain.local
▸ Properties		
Body	< double click to open >	< double click to open >

Close

Compare to Office 365 Organizations

To compare data with your production Office 365 organizations, do the following:

1. [Select an authentication method.](#)
2. [Log on to Office 365.](#)

Step 1. Select Authentication Method

At this step of the wizard, choose whether you want to use modern or basic authentication.

Modern Authentication

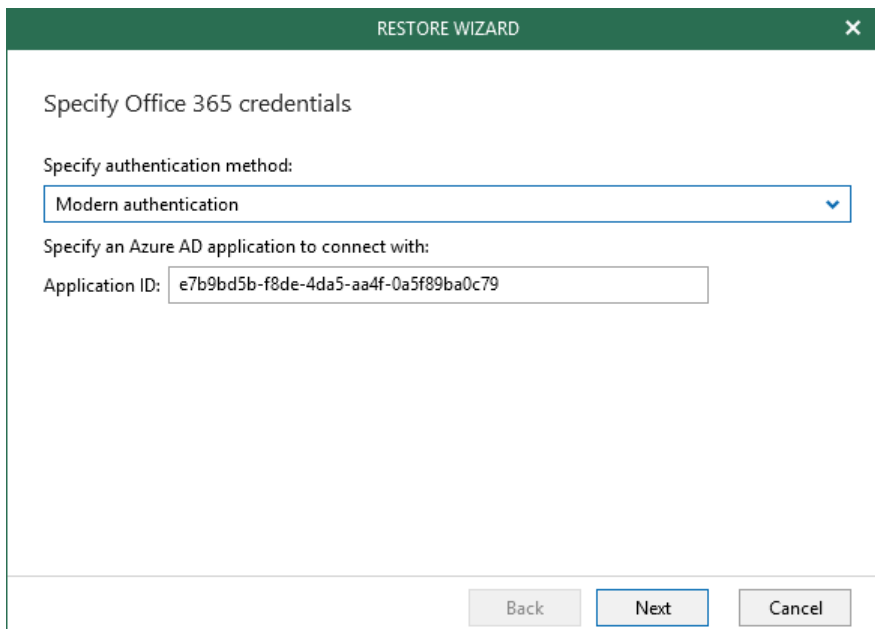
To use modern authentication, do the following:

1. From the **Specify authentication method** drop-down list, select *Modern authentication*.
This will allow Veeam Backup for Microsoft Office 365 to use an Azure AD application for a restore. Such an application is used to restore the specified mailbox back to Office 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults.

For more information, see [Microsoft Office 365 Organizations](#).

2. In the **Application ID** field, enter an identification number of the Azure AD application that you want to use for a restore.

By default, Veeam Explorer for Microsoft Exchange populates this field with the identification number of the application that was used during a backup session. If you want to use another application, make sure to grant this application required permissions, as described in [Azure AD Applications](#).



RESTORE WIZARD

Specify Office 365 credentials

Specify authentication method:

Modern authentication

Specify an Azure AD application to connect with:

Application ID: e7b9bd5b-f8de-4da5-aa4f-0a5f89ba0c79

Back Next Cancel

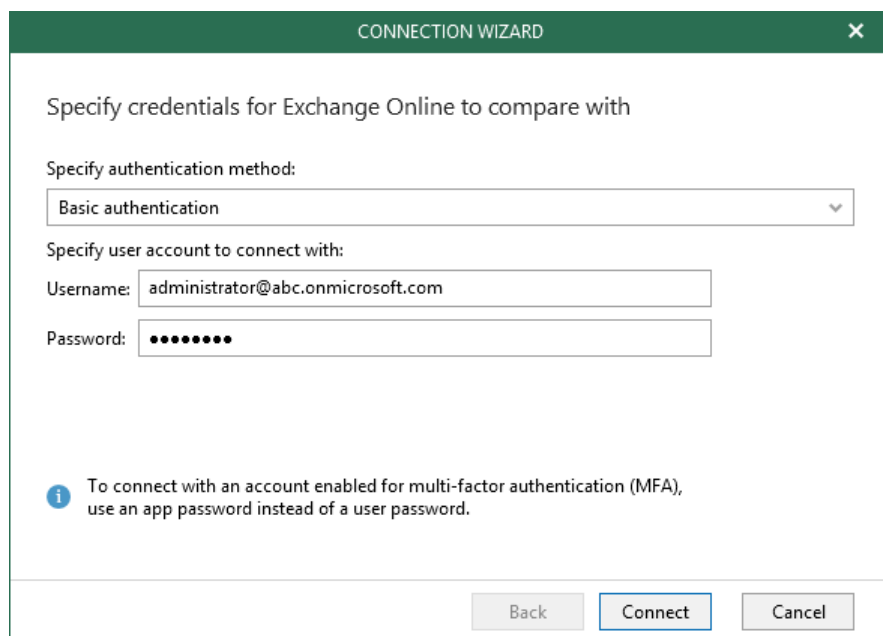
Basic Authentication

To use basic authentication, do the following:

1. From the **Specify authentication method** drop-down list, select *Basic Authentication*.

2. Enter credentials to connect to the Exchange organization and click **Connect**.

Make that the account that you use has both the *Exchange Admin* and the *Global Admin* roles.



CONNECTION WIZARD

Specify credentials for Exchange Online to compare with

Specify authentication method:

Basic authentication

Specify user account to connect with:

Username: administrator@abc.onmicrosoft.com

Password: ••••••••

To connect with an account enabled for multi-factor authentication (MFA), use an app password instead of a user password.

Back Connect Cancel

Step 2. Log on to Office 365

[This step is only available if you have selected the *Modern Authentication* option at the [previous step](#).]

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

To sign in to the Microsoft Office 265 organization, do the following:

1. Click **Copy Code** to copy an authentication code.
Mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.
2. Click the link to the Microsoft portal.
3. On the **Microsoft Azure device logon** page, paste the code that you have copied and sign in to Azure.
Make sure to log in with the user account that has both the *ApplicationImpersonation* role and the *Exchange admin* role. For more information, see [this Microsoft article](#).
4. Return to the **Connection Wizard** window and click **Connect**.


CONNECTION WIZARD


Logon to Office 365


Provided account must have permissions to authenticate to the Office 365 organization.

To sign in, authenticate with the below code at:
<https://microsoft.com/devicelogin>

CZ6W4DHK5



 Copy code

 You are authenticated to Office 365 as administrator@tech.club

Back

Connect

Cancel

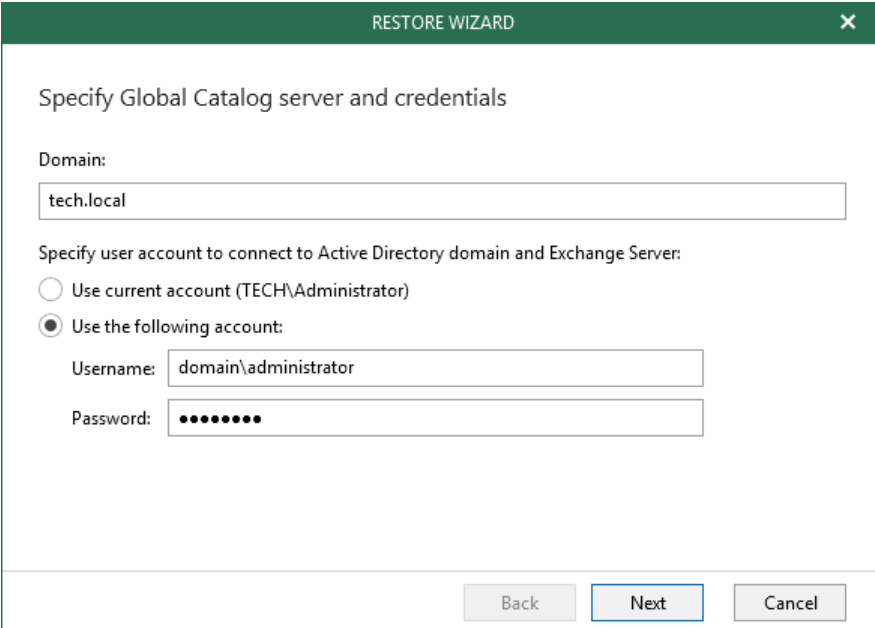
Compare to On-Premises Microsoft Servers

To compare data with your production on-premises Microsoft Exchange, do the following:

1. [Specify a domain and credentials.](#)
2. [Specify a target mailbox server.](#)

Step 1. Specify Domain and Credentials

At this step of the wizard, enter a domain name where your CAS server resides and provide credentials.



The screenshot shows a window titled "RESTORE WIZARD" with a close button (X) in the top right corner. The main heading inside the window is "Specify Global Catalog server and credentials". Below this heading, there is a "Domain:" label followed by a text input field containing "tech.local". Underneath, there is a label "Specify user account to connect to Active Directory domain and Exchange Server:" followed by two radio button options. The first option is "Use current account (TECH\Administrator)" and is unselected. The second option is "Use the following account:" and is selected. Below the selected option, there are two text input fields: "Username:" containing "domain\administrator" and "Password:" containing a series of dots. At the bottom of the window, there are three buttons: "Back", "Next" (which is highlighted with a blue border), and "Cancel".

Step 2. Specify Target Mailbox Server

At this step of the wizard, specify a target server to which you want to restore mailboxes and click **Connect**.

CONNECTION WIZARD

×

Specify target mailbox server

Specify the mailbox server (CAS) to restore the selected items to:

split.croatia.local

Back

Connect

Cancel

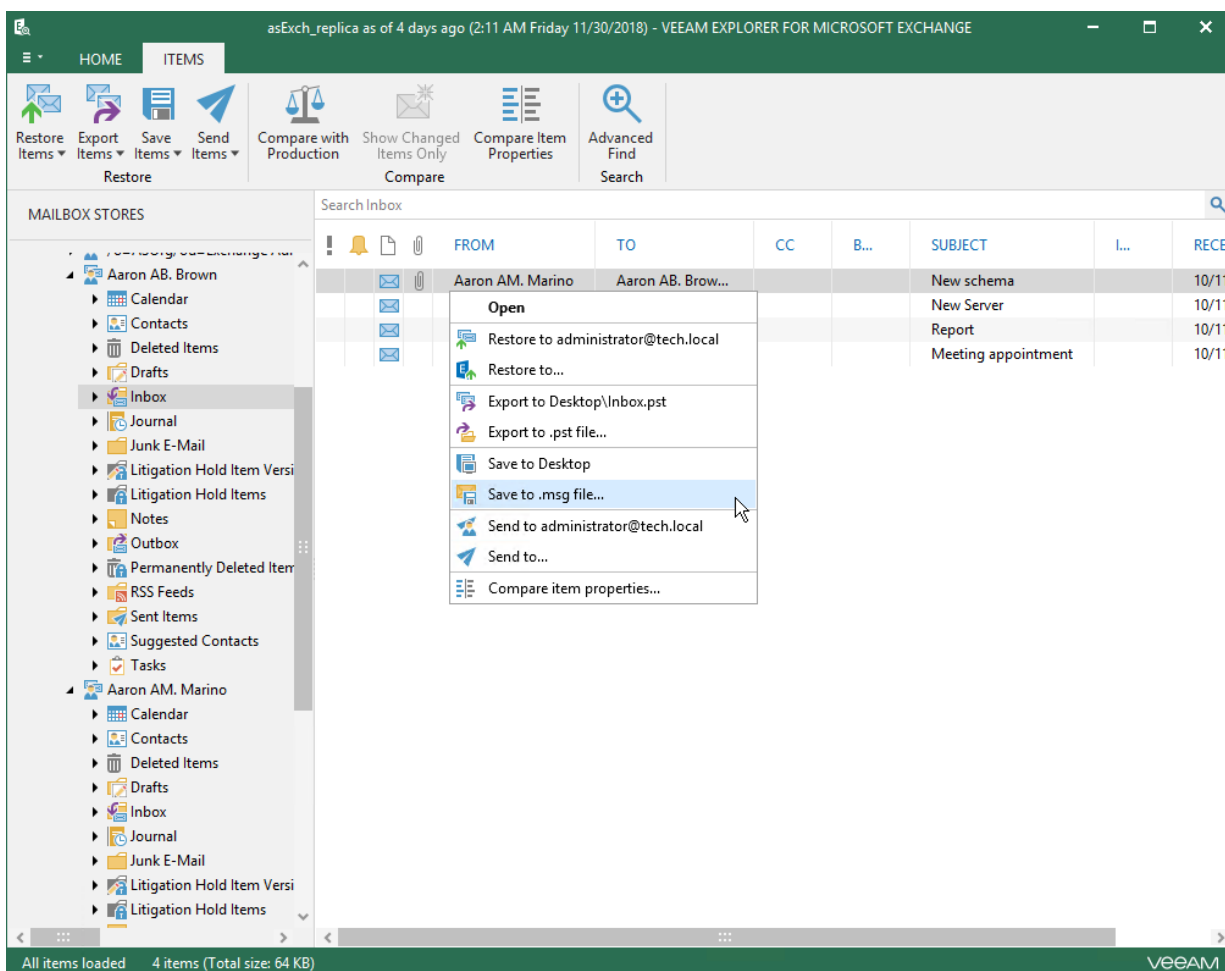
Saving Microsoft Exchange Items

Veeam Explorer for Microsoft Exchange allows you to save any item as *Microsoft Exchange Mail Document* (.msg) files.

Saving to Custom Location

To save items to a custom location, do the following:

1. In the navigation pane, select an item.
2. On the **Items** tab, select **Save Items > Save to .msg file** or right-click a folder/item and select **Save to .msg file**.

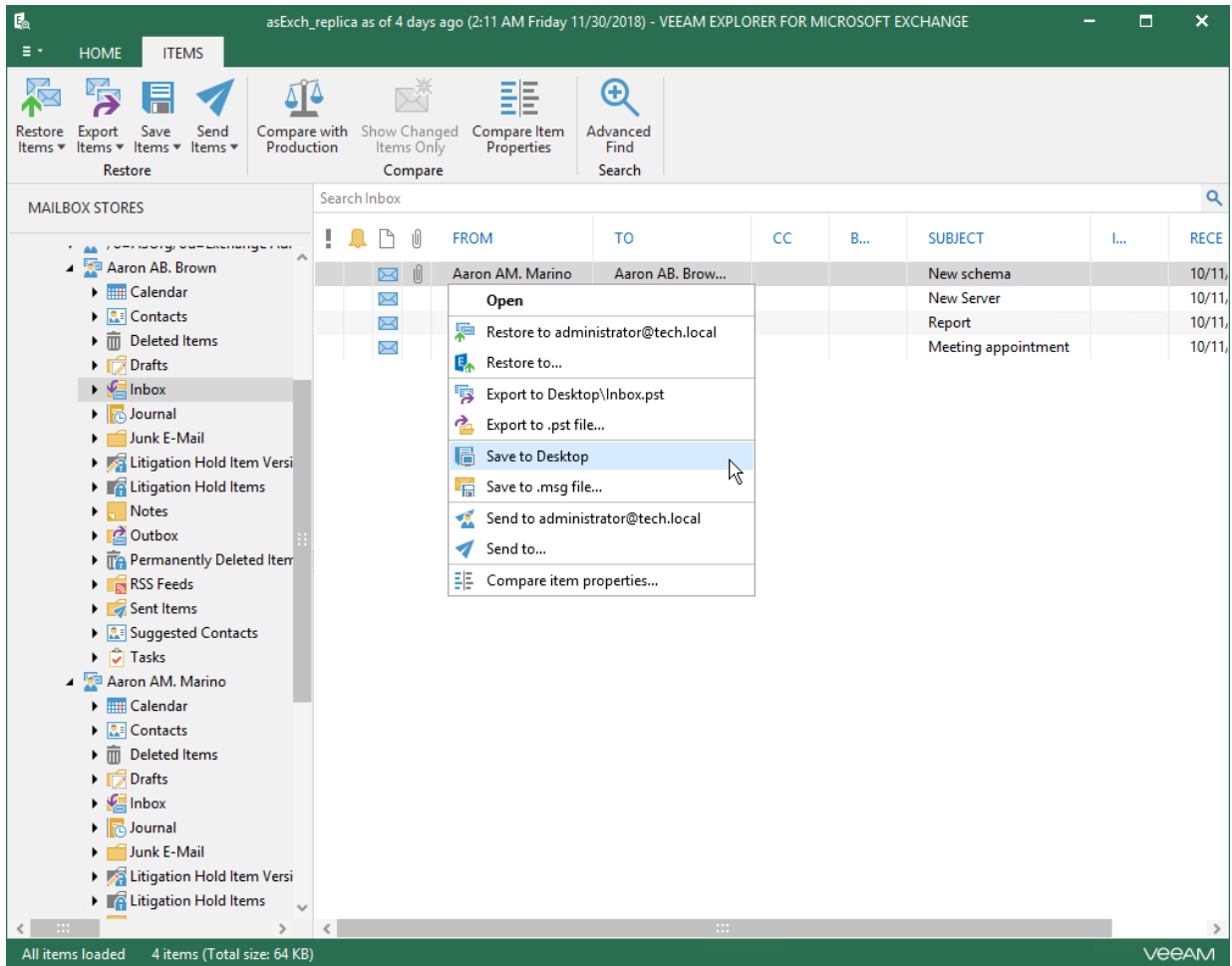


1-Click Save

To save your Exchange data, do the following:

1. In the navigation pane select a folder containing required items.
2. In the preview pane, select items.
Use the **Search** field to find particular items.
3. On the **Items** tab, select **Save Items > Save to <folder_name>** or right-click a folder/item and select **Save to <folder_name>**.

A <folder_name> name depends on the latest location that was used when saving items.



Sending Microsoft Exchange Items

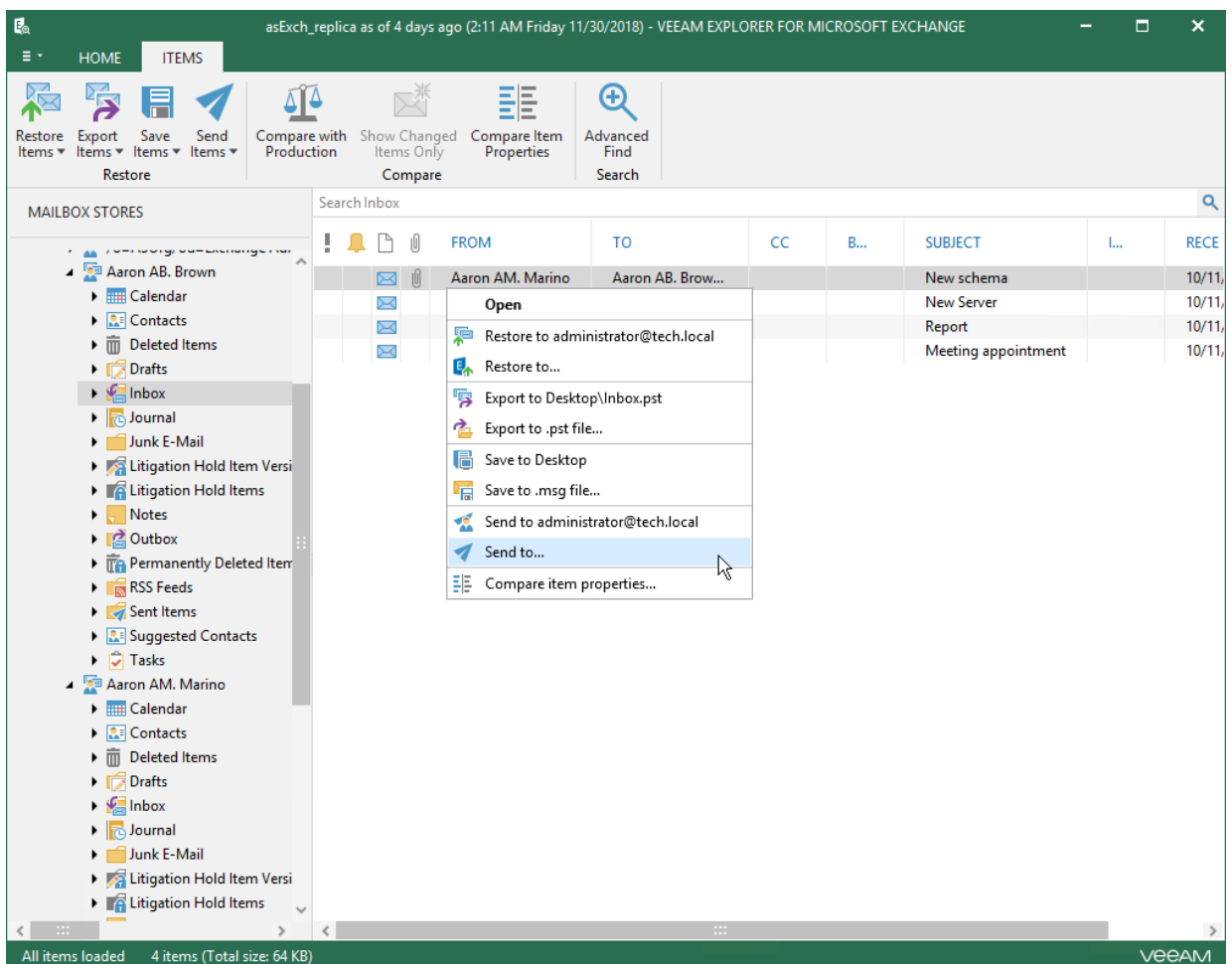
Veeam Explorer for Microsoft Exchange allows you to send Exchange items via email.

TIP:

Before sending documents, make sure to configure SMTP settings, as described in [Configuring SMTP Settings](#). The amount of data you can send at a time depends on your SMTP server configuration.

To send items, do the following:


1. In the navigation pane select a folder.
2. In the preview pane, select items to send.
Use the **Search** field to find particular items.
3. On the **Items** tab, select **Send Items > Send to** or right-click a folder/item and select **Send to**.



4. Provide a recipient address.

The **From** field is filled automatically based on the address you have provided when configuring SMTP settings. To edit the message body, click **More Details**.

SEND TO



Send

From:


administrator@tech.local

To:


Aaron.Brown@asdomain.local

Subject:

Mail Items Recovery

New schema

Sent by Veeam Explorer for Microsoft Exchange

Fewer details

Veeam Explorer for Microsoft SharePoint

Veeam Explorer for Microsoft SharePoint allows you to restore and export Microsoft SharePoint data.

You can also save data from backups to a local computer and send data from backups via email.

Planning and Preparation

Continue with this section to learn how to configure your environment before start using Veeam Explorer for Microsoft SharePoint:

Used Ports

Consider opening the following ports to perform a restore.

General

From	To	Protocol	Port	Notes
Veeam Explorer for Microsoft SharePoint	SQL Server	TCP	1433,1434 and other	To communicate with Microsoft SQL servers hosting content databases. Exact port numbers depend on the configuration of a Microsoft SQL server. For more information, see this Microsoft article .
	SharePoint Web Application	As recommended by Microsoft	As recommended by Microsoft	For more information on recommended port numbers and protocols for SharePoint web application, see this Microsoft article To discover ports currently used by your SharePoint web application, follow the steps described in this Microsoft article .

NOTE:

To restore database items or lists to a server that is running in a DMZ, the SharePoint web application ports will be used.

iSCSI Traffic

From	To	Protocol	Port	Notes
Target Server / Staging Server	Veeam Backup Server / Standalone Console	TCP	3260 - 3270	Used by iSCSI initiator to connect to the iSCSI target.

Required Permissions

The following table lists required permissions for a restore.

Operation	Required Roles and Permissions
Restore to on-premises Microsoft SharePoint	<p>To restore data to on-premises SharePoint, make sure to configure user accounts as follows:</p> <ul style="list-style-type: none">▪ The account must be granted <i>Full Control</i> to connect to the target SharePoint server.▪ The account must be assigned either the <i>Site Administrator</i> or <i>System Account</i> role to restore user permissions.▪ If permissions of items being restored are inherited from the parent one, the account must be granted <i>Full Control</i>.▪ If permissions of items being restored are not inherited from the parent one and items being restored replace the existing ones, the account must be granted <i>Contribute</i> and <i>Full Control</i>.
Restore to Microsoft Office 365	<p>To restore data to SharePoint Online, make sure to configure user accounts as follows:</p> <ul style="list-style-type: none">▪ The account must be granted the <i>SharePoint Administrator</i> role.▪ The account must be granted the <i>Site Collection Administrator</i> role.

Considerations and Limitations

This section covers considerations and known limitations of Veeam Explorer for Microsoft SharePoint.

General

- When Veeam Explorer for Microsoft SharePoint is installed on a server on which both Veeam Backup & Replication and Veeam Backup for Microsoft Office 365 are installed, the notification settings will be inherited from the Veeam Backup and Replication Global Notification settings.

Status Recovery Limitations

Consider the following when planning documents/list items recovery:

- If a document/item was in *Check Out* state when the backup was created, item's last version will not be restored to the target SharePoint and will be available for viewing only. Previous versions (if any) will be restored.
- If the *Declare this item as a record* action was originally applied to list item, the corresponding status will not be preserved. Instead, the restored item status will be set in accordance with the target list/library content approval workflow.
- Original status *On Hold* will not be restored

Restoring Documents, Libraries and Lists

- Versioning settings of SharePoint lists are not preserved during restore.
- Restoring Generic List and Pages Library may fail with the "*No content type 'XXX' found in web YYY*" error.
- *Modified By* field of restored documents is updated with the account performing restore.
- Some *Rating Settings* of *Discussion* lists values are not restored.
- Restore via PSDirect, VIX or Sphere API is not supported.

Restoring List Items

Consider that when restoring a list item, Veeam Explorer works in the following way:

- Deletes an existing item
- Creates item's latest version anew using data from the backup.
- Checks whether it is declared as a record.
- If the check is a success, the process finishes.
- If not, the created version is deleted and item versions are restored sequentially.
- Restore via PSDirect, VIX or Sphere API is not supported.

This logic leads to several peculiarities of list item restore, as described below.

If a list or list items column is used as a lookup column in the dependent list, consider that restoring an item from the source list causes corresponding items deletion in the dependent list.

If a lookup column in the dependent list has the enforced relationship behavior set to **Cascade Delete**, then restoring an item from the source list may cause item deletion in the dependent list due to Microsoft implementation. For more information, see [this Microsoft article](#).

To prevent this issue, it is recommended to turn off enforced relationship behavior. As a work-around, you can roll-back the SharePoint database using Veeam Explorer for Microsoft SQL Server (as described in the [corresponding section](#) of this guide) or roll-back the whole SharePoint server VM to the desired state using any Veeam Backup & Replication recovery option.

The following limitations should also be considered:

- If a lookup column in the dependent list has the enforced relationship behavior set to **Restrict Delete**, then item restore with Veeam Explorer will fail.
- If an .ASPX page references an item using ItemID, this reference may fail to restore (as the item will be created anew with a different ItemID).
- If a list item cannot be deleted (for example, site's "Welcome" page), consider that restore process will recover all versions of the item sequentially without deletions, adding them to *Version History*.
- *Restored Issue* list items are assigned new Issue ID.
- Restore of *Time Card* list is not supported.

Restoring List Items with Links (Attachments)

Consider the following when planning for the recovery of list items with links (attachments):

- If the retention policy for target list/document library was configured to **Declare record** automatically, only the last version of the item will be restored to target list/library. Target retention policy settings will be applied to restored item (**Declare record**). However, links (attachments) will not be restored.
- Alternatively (with different retention policy settings), all versions of the original item will be restored to target list/library; item links (attachments) will be restored only if such item does not exist on target SharePoint.
- If *Declare this item as a record* action was originally applied to list item, such item will not be restored.
- Restore via PSDirect, VIX or Sphere API is not supported.

Restoring Surveys

Consider the following limitations when planning for the recovery of surveys, survey questions and responses:

- Survey item(s) can be restored to a new survey, created automatically by Veeam Explorer for Microsoft SharePoint in the specified destination instead of the previously deleted survey. However, if a new survey is created by user from scratch (not replacing a deleted one) – items cannot be recovered to such a survey.
- A survey can be restored to an existing target survey only if that target survey includes at least one item (question) same as survey questions stored in the content database.
- If a survey question was not answered completely in the source survey, after restore the response status in the target survey will be set to *Completed*, anyway.
- When restoring a single response to a survey, target response item with the same number will be deleted and restored item will be placed in the target survey after the last numbered response.

For example, if the target survey has responses #1-15 and you try to restore a response that used to be #6 on source – then target response #6 will be deleted and restored response will be assigned #16.

- Restore via PSDirect, VIX or Sphere API is not supported.

Restoring Sites

- If you plan to restore SharePoint site pages, consider that Veeam Explorer does not support recovery of items which are not stored in the SharePoint content database (in particular, pages, page references and items based on default templates). Such items cannot be restored (neither by **Restore** nor by **Save** menu option), except for data from Wiki Content (text and images) which is stored in the database. Thus, site pages containing only text and/or images can be restored and displayed properly.

NOTE:

Consider the following:

- In case you attempt to restore such items, the following error message will be logged: "*Item <item> is skipped: restoration of items based on SharePoint default template is not supported.*"
- In case you attempt to save such items, the following error message will be logged: "*Unable to save document <item>. Document content is not available.*"
- Web features restore is not supported for SharePoint 2010 sites.

Export and Import

- Importing exported Picture Library may result in IDs changed for some items.
- Importing exported Project Tasks list does not preserve column order.
- Importing exported SharePoint list does not preserve Validation Settings.

Data Type Limitations

Consider the column (field) data type when planning for the recovery of your SharePoint libraries/lists:

- If source column (field) data type was set to *Lookup*, but the referenced list/library was deleted, such columns (fields) will not be restored even if you recover that referenced list. The reason is that if referenced list is deleted, the reference (link) to that list is no longer valid.
- If source column (field) data type was set to *Managed Metadata*, such columns (fields) will not be restored.

Workflow-related Considerations

You may need to restore the item(s) originally belonging to a list with no content approval required, to another list. If you try to restore such item(s) to a list that requires content approval, item version and status will be modified in the following way:

- a. If a target list is configured to include major versions only – then all versions of restored item will become major (despite the original versioning); item status will be set to Pending.
- b. If a target list is configured to include both major and minor versions – then all versions of restored item will become minor (despite the original versioning); item status will be set as follows:
 - If the last version (original) was major – status will be set to *Pending*

- If the last version was minor – status will be set to *Draft*

Also, consider the following when planning for the recovery of list items (with or without content approval originally required):

- a. If the retention policy for target list/document library is configured to **Declare record** automatically, only the last version of the item will be restored to target list/library. Target retention policy settings will be applied to restored item (**Declare record**).
Besides, if **Require content approval for submitted items** was enabled for the original list, then after recovery item status will be set to *Pending*.
- b. Alternatively (with different retention policy settings), all versions of the original item will be restored to target list/library.
Besides, if **Require content approval for submitted items** was enabled for the original list, then after recovery item status in the content approval workflow will be also restored, except for the states listed (see "Status Recovery Limitations" above).

Launching Application and Exploring Backups

To open Veeam Explorer for Microsoft SharePoint and load backups, you can use any of the following methods:

- The **Explore** option. For more information, see [Data Restore](#).

When loading backups located in object storage repositories, Veeam Explorer for Microsoft SharePoint will notify you about the location of these backups. You can select the **Don't show this message again** check box to unsubscribe from such notifications. To enable notifications, select the **Reset disabled pop-up notifications** check box, as described in [Configuring Advanced Settings](#).

- Go to **Start** and click **Veeam Explorer for Microsoft SharePoint**.

When you open Veeam Explorer for Microsoft SharePoint from the **Start** menu, all backed-up databases will be loaded automatically.

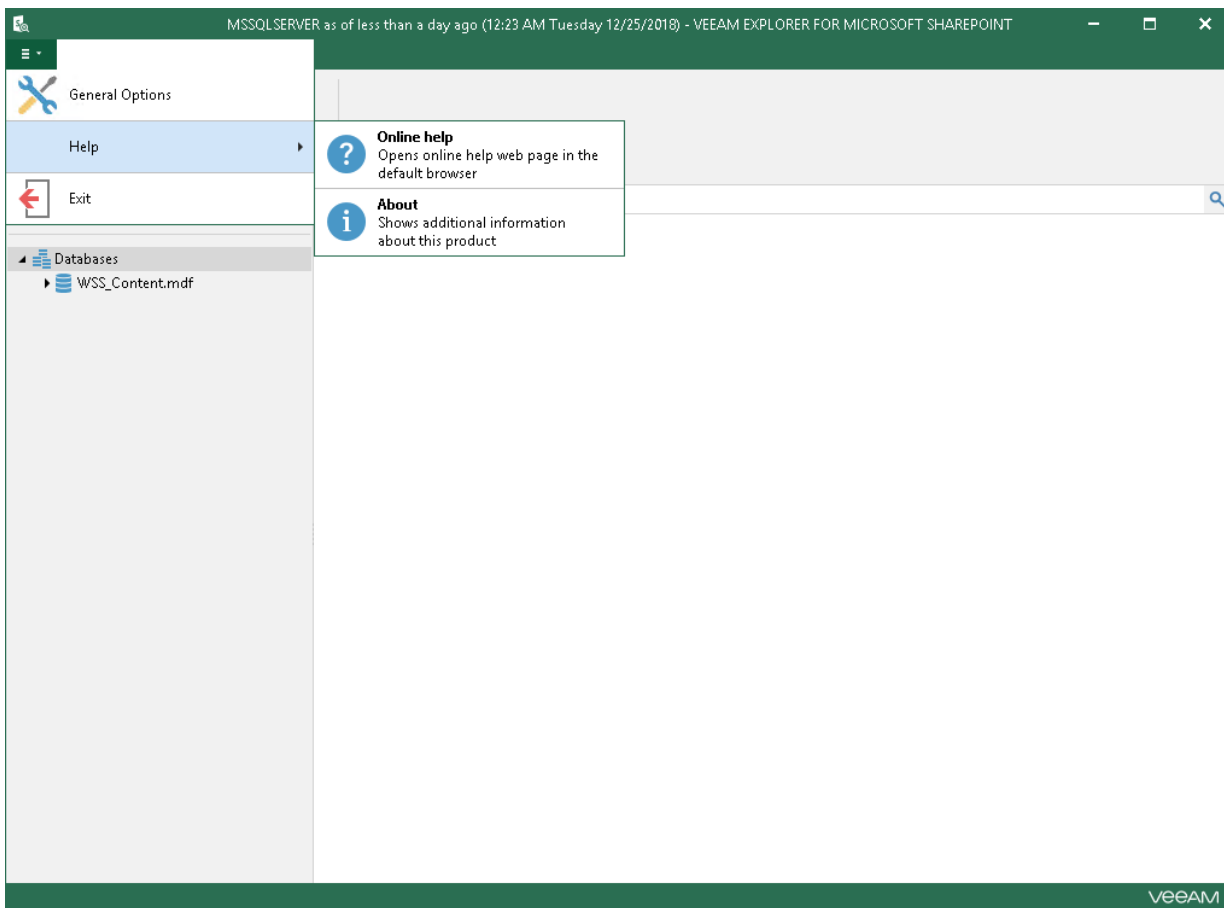
Understanding User Interface

Veeam Explorer for Microsoft SharePoint provides you with the convenient user interface that allows you to perform required operations in a user-friendly manner.

Main Menu

The main menu comprises the following features:

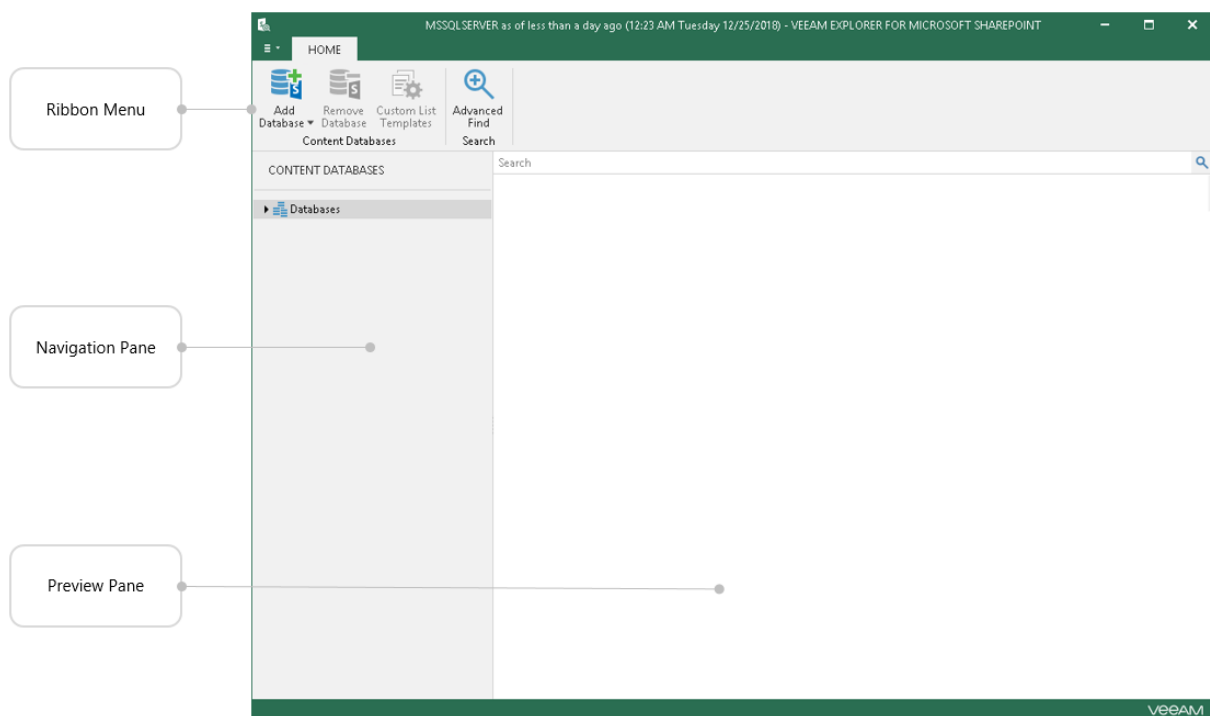
- **General Options.** Allows you to configure program options.
- **Help.**
 - **Online help.** Opens the online web help page.
 - **About.** Shows information about the product.
- **Exit.** Closes the program.



Main Application Window

The main application window can be divided into three categories:

- The ribbon menu, which contains general program commands organized into logical groups.
- The navigation pane, which allows you to browse through the hierarchy of your backup files.
- The preview pane, which shows you the details about objects you have selected in the navigation area.



Browsing, Searching and Viewing Items

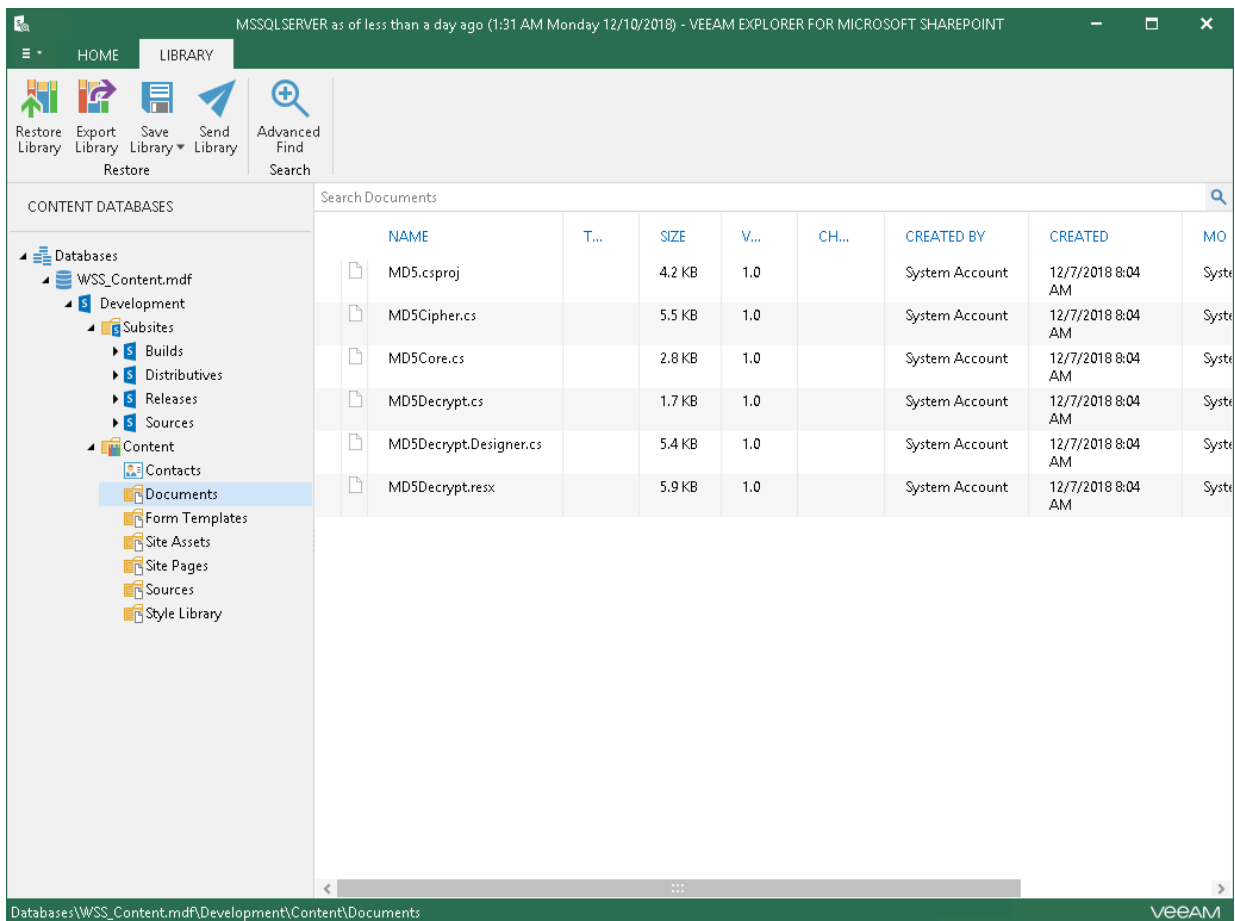
Continue with this section to learn more about:

- [Browsing backup content](#)
- [Viewing objects properties and open files](#)
- [Searching for objects in a backup file](#)
- [Using the advance search capabilities](#)

Browsing

To view the contents of a backup file, you use the navigation pane which shows you the database structure containing your site items such as libraries and subsites.

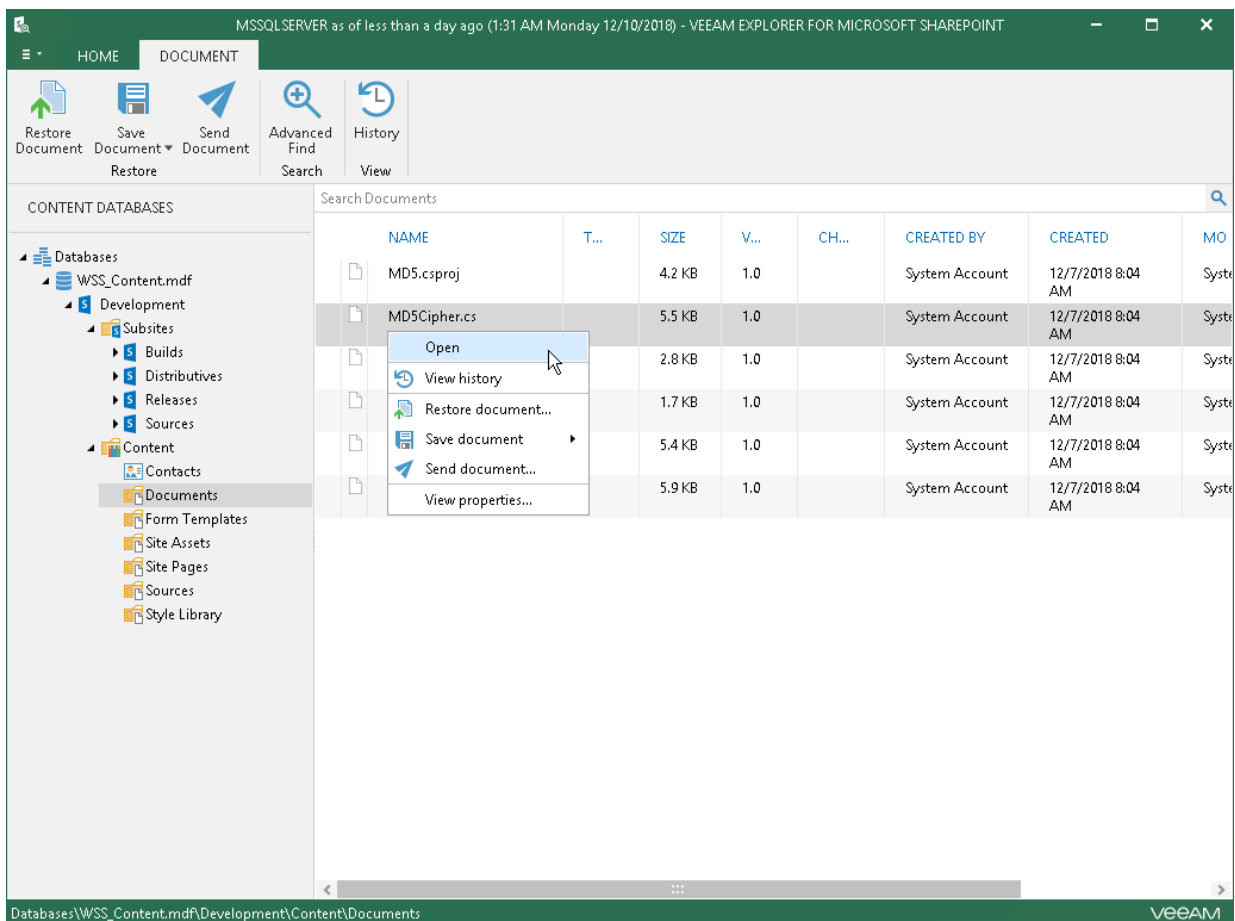
After you select an object in the navigation pane, you can see its content in the preview pane.



Viewing Properties and Opening Files

To view object properties, right-click an object in the preview pane and select **View Properties**.

To open a document using an associated application, right-click a document in the preview pane and select **Open**.



Searching

The search mechanism allows you to find items matching specified search criteria.

To search for required items, do the following:

1. In the navigation pane, select an object in which you want to find your data.
2. Enter a search query to the search field at the top of the preview pane.

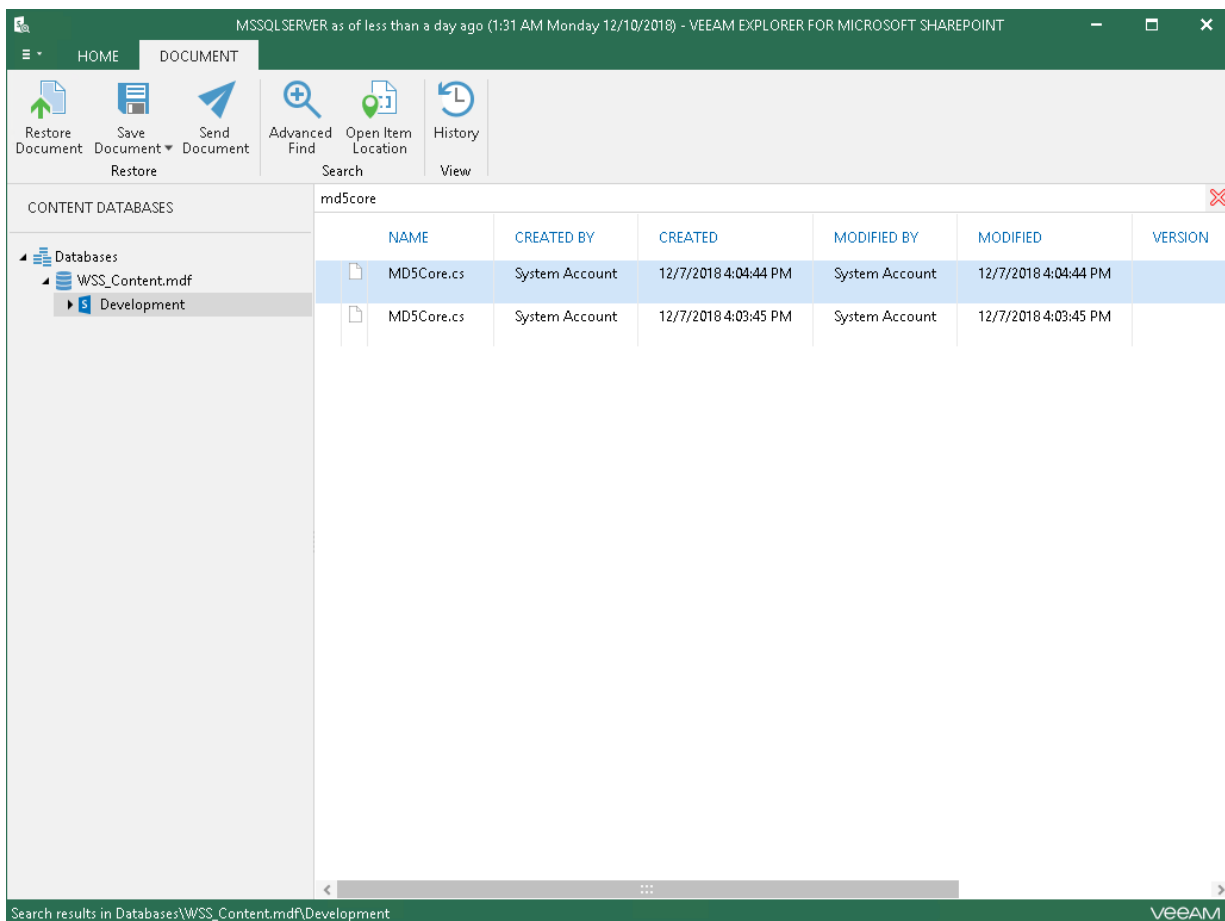
NOTE:

To find the exact phrase, use double quotes. For example, *"media player"*.

You can narrow your search results by specifying various search criteria using the *criteria:value* format.

For example, to find all items that require approval in the list of decisions, you can use the following search query: *status:pending approval*.

You can also use logical upper-cased operators such as *AND*, *OR* and *NOT* along with wildcard characters such as *** and *?*. The search criteria are similar to those used for searching in Microsoft SharePoint. For more information, see [this Microsoft article](#).



Using Advanced Find Capabilities

The **Advanced Find** mechanism allows you to define your search criteria more precisely.

For example, to find an object that starts with the word *Media*, do the following:

1. In the preview pane, select a content node and click **Advanced Find**.
2. In the **Define search criteria** section, select **Category > Document fields**.
3. In the **Field** list, select **File Name**.
4. In the **Condition** list, select **Starts With**.
5. In the **Value** field, specify a file name.
6. Click **Start**.

To remove a filter, click the cross mark next to it. To remove all configured filters, click **Reset**.

MSSQLSERVER as of less than a day ago (1:31 AM Monday 12/10/2018) - VEEAM EXPLORER FOR MICROSOFT SHAREPOINT

HOME DOCUMENT

Restore Document Save Document Send Document Advanced Find History

Restore Search View

CONTENT DATABASES

- Databases
 - WSS_Content.mdf
 - Development
 - Subsites
 - Builds
 - Distributives
 - Releases
 - Sources
 - Content
 - Contacts
 - Documents
 - Form Templates
 - Site Assets
 - Site Pages
 - Sources
 - Style Library

Find items that match these criteria:

File Name starts with md5c Start Reset

Define search criteria

Category: Frequently-used fields Field: Anniversary

Condition: between Value: Monday, December 10, 2018 Monday, December 10, 2018 Add To List

NAME	CREATED BY	CREATED	MODIFIED BY	MODIFIED	VERSION
MD5Cipher.cs	System Account	12/7/2018 4:04:44 PM	System Account	12/7/2018 4:04:44 PM	
MD5Cipher.cs	System Account	12/7/2018 4:03:43 PM	System Account	12/7/2018 4:03:43 PM	
MD5Core.cs	System Account	12/7/2018 4:04:44 PM	System Account	12/7/2018 4:04:44 PM	
MD5Core.cs	System Account	12/7/2018 4:03:45 PM	System Account	12/7/2018 4:03:45 PM	

Search results in Databases\WSS_Content.mdf\Development

veeam

General Application Settings

Continue with this section to learn more about configuring general application settings and components.

Staging SQL Server

To perform Microsoft SharePoint items recovery, Veeam Explorer requires a Microsoft SQL server to be used as a staging system.

Consider the following when configuring a staging SQL server:

- If a SQL server belongs to an untrusted domain, connection will not be possible.
- If a SQL server belongs to a trusted domain, only the *SQL Server authentication* method is available.
- If both a SQL server and the machine running Veeam Explorer belong to the same domain, then both *Windows* and *SQL Server authentication* methods are possible.

To use *Windows authentication*, make sure to configure the following delegation settings:

- a) In **Active Directory Users and Computers**, select the necessary staging SQL server.
- b) Open its properties and select the **Delegation** tab. Select **Trust this computer for delegation to specified services only** and **Use any authentication protocol** options for the **cifs** service on a computer with Veeam Explorer.
- c) Restart the staging SQL Server.
- d) Select a user account to connect to the staging SQL server. Also, select its properties on the **Account** tab and make sure the **Account is sensitive and cannot be delegated** check box is cleared.

To configure a staging server, do the following:

1. Go to the main menu and click **General Options**.
2. Go to the **SQL Server Settings** tab.
3. Click **Browse** to specify a SQL server you want to use as a staging system.
4. Specify the account to access the selected SQL server.
5. Specify the account to access a SQL server instance.

OPTIONS

×

Staging Server

Custom Lists

SMTP Settings

Advanced

SQL Server name:

SRV003\SQLEXPRESS

Browse...

Specify user account to connect to Windows server:

☐ Use current account (TECH\Administrator)

☒ Use the following account:

Username:

Administrator

Password:

●●●●●●●●●●

Specify user account to connect to SQL Server instance:

☐ Use the same Windows server account (Administrator)

☒ Use the following account:

Username:

Administrator

Password:

●●●●●●●●

☒ Use SQL Server authentication

OK

Cancel

Apply

Custom Lists

Veeam Explorer for Microsoft SharePoint supports obtaining custom list templates from backups created in Veeam Backup & Replication.

The actual information about templates is stored directly in a backup file and obtained automatically so that you can view the custom list data without having to perform any additional operations.

NOTE:

Configuring custom lists is not required when working with backups created in Veeam Backup for Microsoft Office 365.

To see templates with their corresponding names and features, go to the main menu > **General Options** and click the link under the **STATUS** column which also comprises the total number of available templates.

You can select **Automatically update custom list templates from backups** to automatically update existing templates. Also, you can select **Warn me if attached database has new custom list templates** to be notified if the database contains new templates other than those you already have.

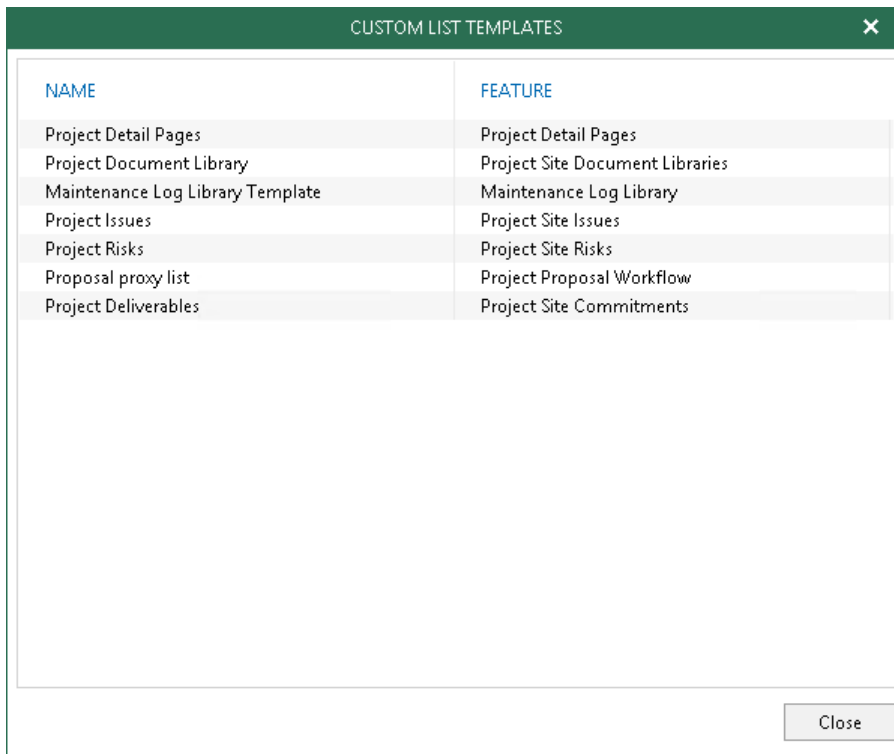
SHAREPOINT SERVER	STATUS	
Microsoft SharePoint 2010	No Templates	Clear
Microsoft SharePoint 2013	No Templates	Clear
Microsoft SharePoint 2016	No Templates	Clear
Microsoft SharePoint 2019	No Templates	Clear

☒ Automatically update custom list templates from backups

☒ Warn me if attached database has new custom list templates

OK Cancel Apply

See the figure below showing you what custom list templates are available.

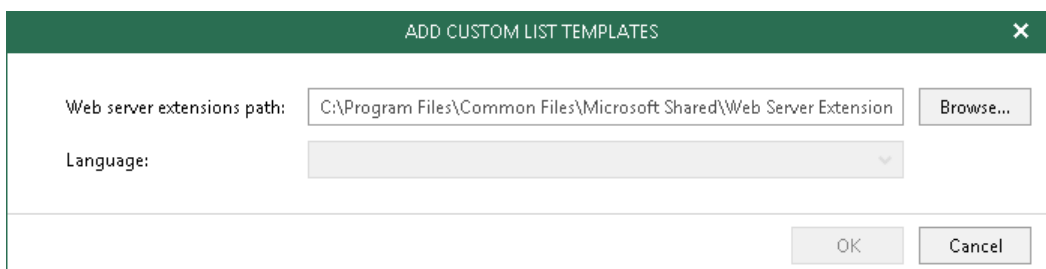


To remove templates, click **Clear**.

Importing Templates Manually

To import existing templates from the Microsoft SharePoint server manually, do the following:

1. Go to the main menu, select **General Options > Custom Lists** and click **Update**.
2. Specify the path to Microsoft SharePoint templates, select the language and click **OK**. The language set in the drop-down list depends on the installed language packages on a SharePoint server.



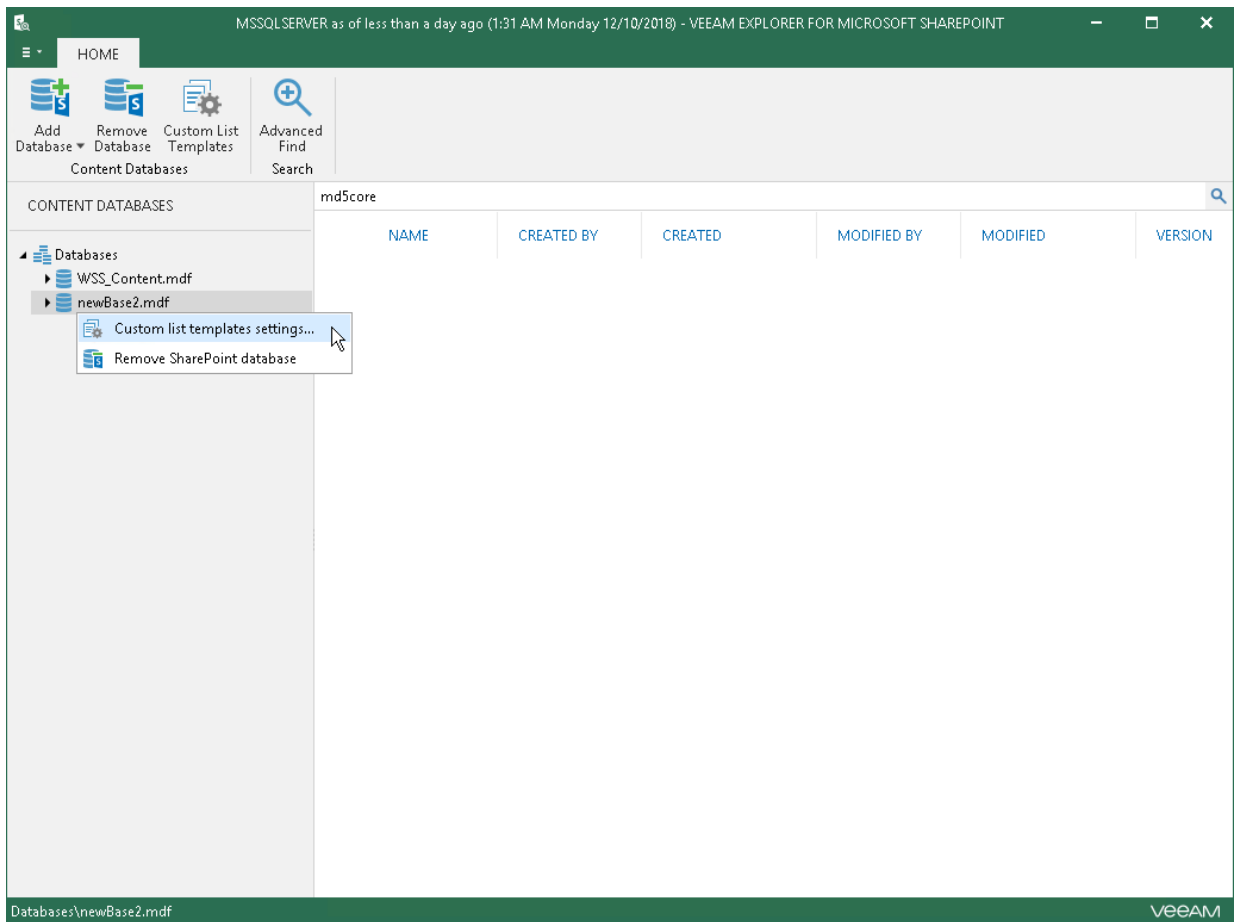
Importing Templates Using Ribbon Menu

NOTE:

Available only for Microsoft SQL Server databases and requires a staging SQL server. For more information on configuring a staging server, see [Configuring SQL Server Settings](#).

To import existing templates from the Microsoft SharePoint server using the ribbon menu, do the following:

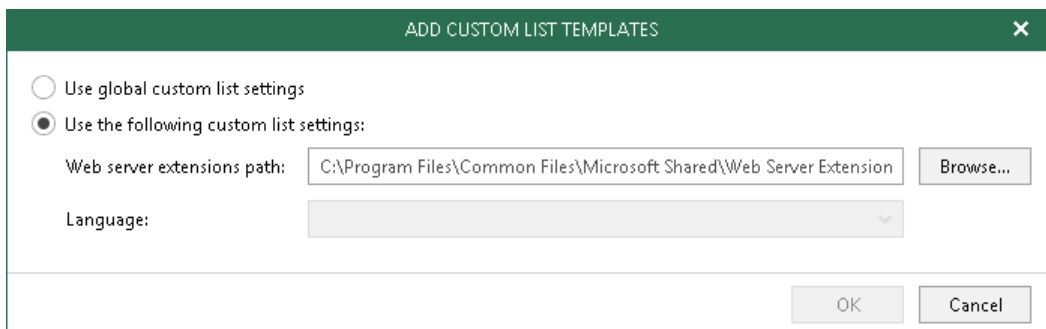
1. In the navigation pane, select a SQL database.
2. Click **Custom List Template** on the ribbon menu or right-click a SQL database and select **Custom list templates settings**.



3. Choose how you want your templates to be applied:

- a) Select **Use global custom list settings** to apply global list templates to the select database.
- b) Select **Use the following custom list settings** to apply the templates to the selected database only.

When using the latter option, specify the path to the Microsoft SharePoint templates, select the language and click **OK**. The language set in the drop-down list depends on the installed language packages on a SharePoint server.



SMTP Settings

To send Microsoft SharePoint items as attachments, you must configure SMTP server settings.

To configure SMTP settings, do the following:

1. Go to the main menu and click **General Options**.
2. On the **SMTP Settings** tab, select the **Configure SMTP settings** check box and specify the following:
 - DNS name or IP address of the mail server.
 - SMTP communication port.
 - The sender email address. This address will appear in the **From** field when sending SharePoint items.
 - Select **Use authentication** check box If your SMTP server requires SMTP authentication for outgoing mail and provide valid credentials.
 - Select **Enable SSL security** check box to enable SSL data encryption.
3. Click **Send** to send a test email message.
4. Click **Apply**.

The screenshot shows a dialog box titled "OPTIONS" with a close button (X) in the top right corner. It has four tabs: "Staging Server", "Custom Lists", "SMTP Settings" (which is selected), and "Advanced". Under the "SMTP Settings" tab, there is a section with a checked checkbox labeled "Configure SMTP settings". Below this, there are several fields: "Server:" with the value "smtp.office365.com", "Port:" with a spinner set to "25", "From:" with the value "Administrator@abc.com", a checked checkbox labeled "Use authentication", "User:" with the value "Administrator", "Password:" with masked characters "••••••••••", and a checked checkbox labeled "Enable SSL security". At the bottom of this section, there is a label "Send test e-mail to:" followed by an "E-mail:" field with the value "Administrator@abc.com" and a "Send" button. At the very bottom of the dialog box, there are three buttons: "OK", "Cancel", and "Apply".

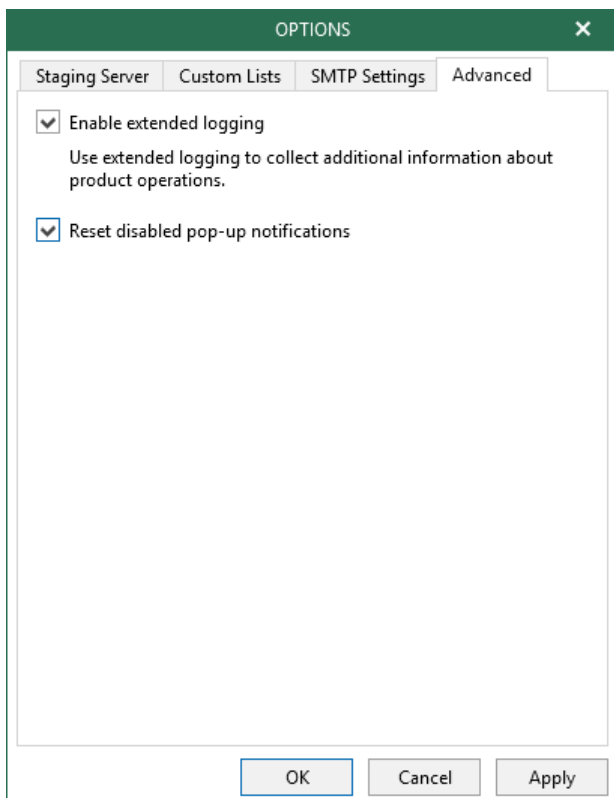
Advanced Settings

This section explains how to configure advanced settings of the application.

To configure advanced settings, do the following:

1. Go to the main menu and click **General Options**.
 2. Got to the **Advanced** tab and select the following:
 - Select the **Enable Extended logging** check box to enable extended logging mode to collect logs that contain more details on specific operations.
- After enabling extended logging mode, you can go back to the application and perform required actions, then collect logs.
- Select the **Reset disabled pop-up notifications** check box to enable notifications when loading backups from object storage repositories.

Applicable to backups created in Veeam Backup for Microsoft Office 365.



Standalone Databases

This section explains how to add standalone databases to the Veeam Explorer for Microsoft SharePoint scope and how to connect to a Veeam Backup for Microsoft Office 365 server and service provider server to view backups located on these servers.

Adding Microsoft SharePoint Databases

Continue with this section to learn more about the addition of Microsoft SharePoint databases to the application scope manually.

When you add standalone Microsoft SharePoint databases to the application scope, Veeam attaches such a database to the staging SQL server, creating a temporary Microsoft SharePoint content database from which you can recover your items.

To manually add new Microsoft SharePoint databases to the application scope, do the following:

1. Click **Add Database > Microsoft SharePoint Databases** on the toolbar or right-click the root **Database** node and select **Add database**.
2. Specify the location of the Microsoft SharePoint primary content database file (.mdf). The secondary database and the transaction log file (.ldf) will be added as well.

To add remote BLOB stores, click **Add** next to the **Remote BLOB Stores** section.

3. Click **OK**.

ADD DATABASE

Specify content database files location

Primary database file:

C:\sharepoint\newBase2.mdf Browse...

Secondary database and log files:

FILE	STATUS	
C:\sharepoint\newBase2_log.LDF	OK	Browse...

Remote BLOB Stores:

FOLDER	STATUS	
--------	--------	--

Add...

OK Cancel

Adding Veeam Backup for Microsoft Office 365 Databases

To manually add databases that store Microsoft Office 365 organization data, do the following:

1. Click **Add Database > Veeam Backup for Microsoft Office 365 Databases** or right-click the root **Database** node and select **Veeam Backup for Microsoft Office 365 databases**.
2. Specify the database file location and log directory.
3. Click **Open**.

NOTE:

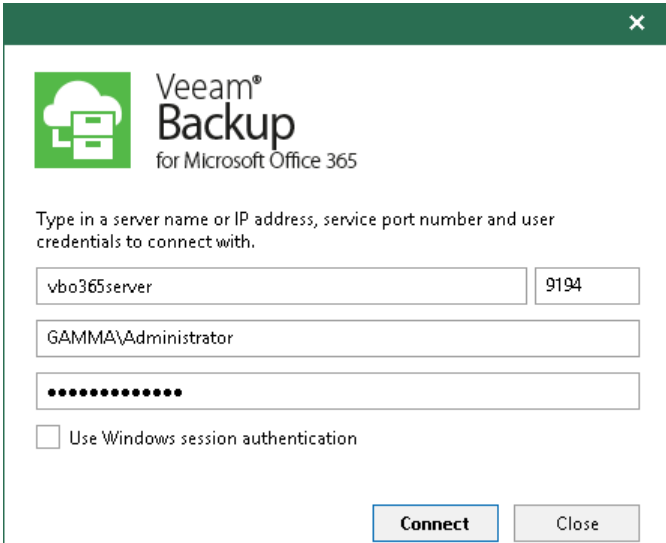
Make sure you have disabled the **Veeam Backup Proxy for Microsoft Office 365** service when adding local databases. You can stop this service by using the `services.msc` console. If you try to add a database having this service still in progress, you will receive an error message and will not be able to access the database due to database lock.

Adding Veeam Backup for Microsoft Office 365 Server

You can use the built-in Veeam Explorer abilities to connect to another Veeam Backup for Microsoft Office 365 server and add its databases to the Veeam Explorer for Microsoft SharePoint scope.

To connect to another Veeam Backup for Microsoft Office 365 server remotely, do the following:

1. Click **Add Database > Veeam Backup for Microsoft Office 365 Server** on the ribbon menu or use the corresponding context menu command.
2. Specify connection settings under which to connect to the Veeam Backup for Microsoft Office 365 server and click **Connect**.

A screenshot of the Veeam Backup for Microsoft Office 365 connection dialog box. The dialog has a green header bar with a close button (X). Below the header is the Veeam logo and the text "Veeam® Backup for Microsoft Office 365". A prompt reads: "Type in a server name or IP address, service port number and user credentials to connect with." There are three input fields: the first contains "vbo365server", the second contains "9194", and the third contains "GAMMA\Administrator". Below these fields is a checkbox labeled "Use Windows session authentication" which is currently unchecked. At the bottom right are two buttons: "Connect" and "Close".

Veeam®
Backup
for Microsoft Office 365

Type in a server name or IP address, service port number and user credentials to connect with.

vbo365server 9194

GAMMA\Administrator

.....

☐ Use Windows session authentication

Connect Close

Adding Veeam Backup for Microsoft Office 365 Service Provider

In Veeam Explorer for Microsoft SharePoint, you can connect to a service provider server to add its backups to the application scope and perform a restore directly from such backups.


NOTE:

Make sure that both Veeam Explorer for Microsoft SharePoint and Veeam Backup & Replication are installed on the same server and at least one service provider is added to Veeam Backup & Replication.

To add Veeam Backup for Microsoft Office 365 service providers, do the following:

1. On the toolbar, click **Add Store > Veeam Backup for Microsoft Office 365 Service Provider** or use the corresponding context menu command.
2. From the **Select service provider and authentication method** drop-down list, select a service provider that you want to add and choose an authentication method that can be either *Modern authentication* or *Basic authentication*.
4. [For *Modern authentication*] Select a region to which an Office 365 organization of the selected service provider belongs.
5. [For *Modern authentication*] Copy the device code and use it to sign in to Microsoft Azure Active Directory.

For *Basic authentication*, you must enter a user name and password to connect to the service provider server.
6. Select a point-in-time state as of which you want to load Office 365 backups.
To select a state, use the calendar control.
7. Select the **Show items that have been deleted by user** check box to see all the items that were removed.
8. Select the **Show all versions of items that have been modified by user** check box if you want to load modified versions.
9. Click **Connect**.



Veeam Backup

for Microsoft Office 365

Select service provider and authentication method:

office.tech.local (Tenant1)

Modern authentication

Select Office 365 organization region and sign in to Azure AD:

Default

To sign in, authenticate with the below code at:
<https://microsoft.com/devicelogin>

CGJF25HY5

Copy code

i Waiting for user logon...

Specify point in time you want to open:

☒ Use the latest available state

☐ Use the following point in time:

Wednesday, May 27, 2020 4:57:23 AM

☒ Show items that have been deleted by user

☒ Show all versions of items that have been modified by user

☐ Hide

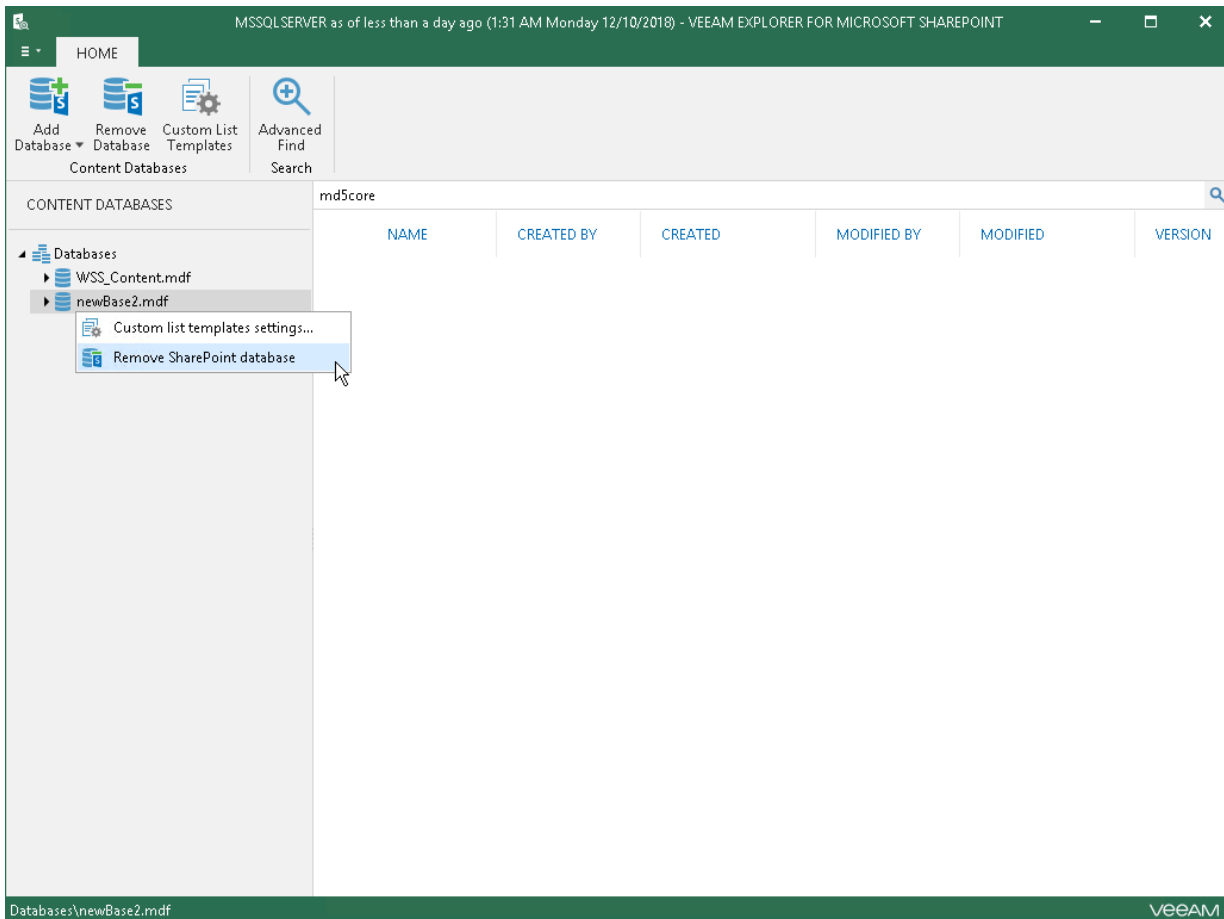
Connect

Close

Removing Databases

Veeam Explorer for Microsoft SharePoint allows you to remove Microsoft SharePoint databases from the application scope when you no longer need it.

To remove a database from the application scope, right-click a database in the navigation pane and select **Remove SharePoint database**.



Restore

This section explains how to restore data to [Microsoft Office 365](#) and [on-premises Microsoft](#) organizations.

IMPORTANT!

This section explains how to perform a restore in Veeam Explorer for Microsoft SharePoint that comes as part of Veeam Backup for Microsoft Office 365 version 4c. For more information on how to restore data in Veeam Explorer for Microsoft SharePoint that comes with Veeam Backup for Microsoft Office 365 version 4, see [this section](#) of the Veeam Explorers User Guide.

Restoring Sites

To restore Microsoft SharePoint sites, do the following:

1. [Launch the Restore wizard.](#)
2. [Select an authentication method.](#)
3. [Log on to Office 365.](#)
4. [Specify a target site.](#)
5. [Specify restore options.](#)

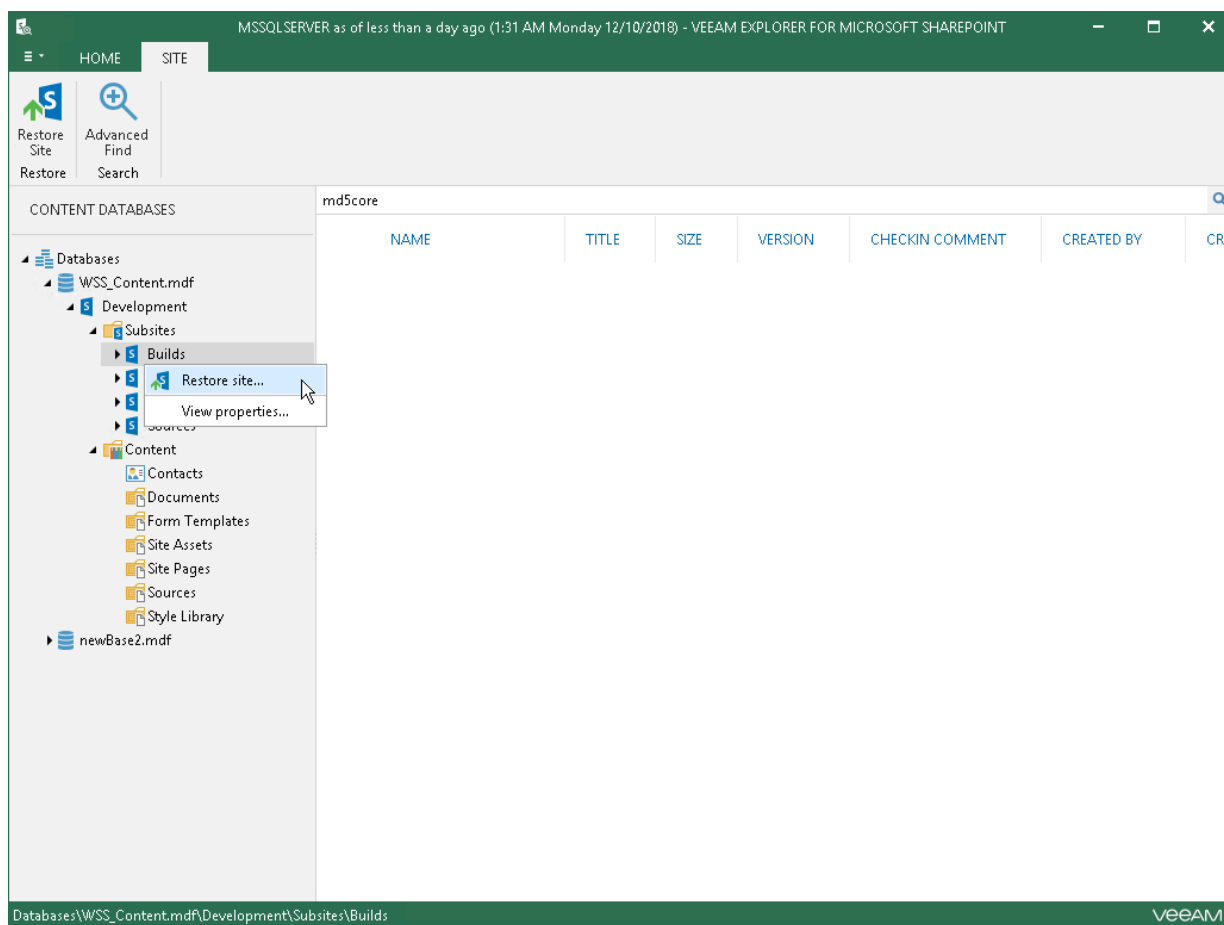
Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. In the navigation pane, select a site.
2. On the **Site** tab, select **Restore Site** or right-click a site and select **Restore Site**.

NOTE:

Sites can only be restored to the existing site collection. Creating a new collection is not supported.



Step 2. Select Authentication Method

At this step of the wizard, choose whether you want to use modern or basic authentication, or authenticate on an on-premises Microsoft SharePoint server.

Modern Authentication

To use modern authentication, do the following:

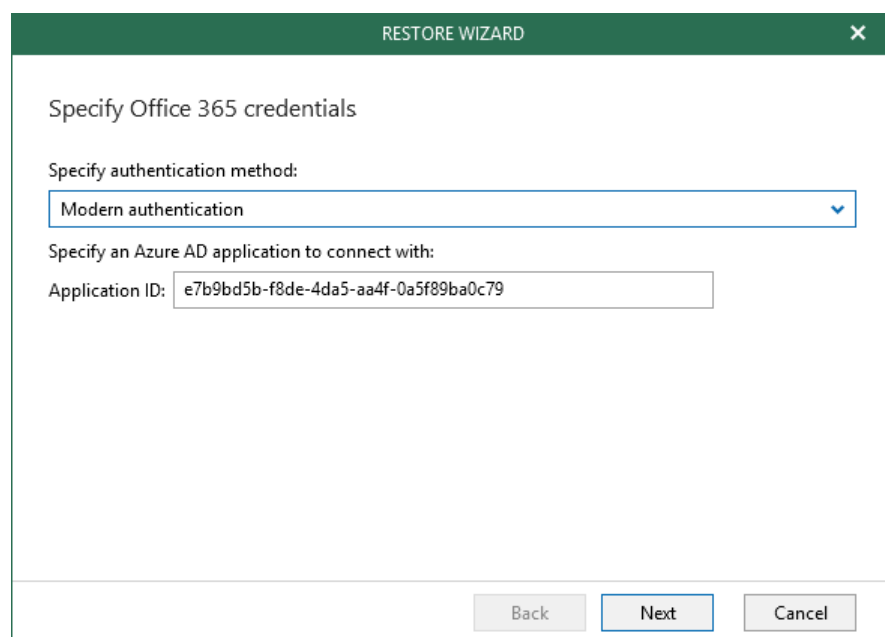
1. From the **Specify authentication method** drop-down list, select *Modern authentication*.

This will allow Veeam Backup for Microsoft Office 365 to use an Azure AD application for a restore. Such an application is used to restore the specified mailbox back to Office 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults.

For more information, see [Microsoft Office 365 Organizations](#).

2. In the **Application ID** field, enter an identification number of the Azure AD application that you want to use for a restore.

By default, Veeam Explorer for Microsoft Exchange populates this field with the identification number of the application that was used during a backup session. If you want to use another application, make sure to grant this application required permissions, as described in [Azure AD Applications](#).



RESTORE WIZARD

Specify Office 365 credentials

Specify authentication method:

Modern authentication

Specify an Azure AD application to connect with:

Application ID: e7b9bd5b-f8de-4da5-aa4f-0a5f89ba0c79

Back Next Cancel

Basic Authentication

To use basic authentication, do the following:

1. From the **Specify authentication method** drop-down list, select *Basic Authentication*.
2. Enter credentials to connect to the SharePoint organization.

RESTORE WIZARD

Specify Office 365 credentials

Specify authentication method:

Basic authentication

Specify user account to connect with:

Username: administrator@abc.onmicrosoft.com

Password:

To connect with an account enabled for multi-factor authentication (MFA), use an app password instead of a user password.

Back Next Cancel

On-Premises Organizations

To authenticate on an on-premises Microsoft SharePoint server, provide a user name and password.

RESTORE WIZARD

Specify target Microsoft SharePoint Server credentials

☐ Use current account (TECH\Administrator)

☒ Use the following account:

Username: tech\administrator

Password:

Back Next Cancel

Step 3. Log on to Office 365

[This step is only available if you have selected the *Modern Authentication* option at the [previous step](#).]

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

To sign in to the Microsoft Office 265 organization, do the following:

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

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

2. Click the link to the Microsoft portal.
3. On the **Microsoft Azure device logon** page, paste the code that you have copied and sign in to Azure. Make sure to log in with the user account that has the *SharePoint Administrator* role.
4. Return to the **Restore Wizard** window and click **Next**.

The screenshot shows the 'RESTORE WIZARD' window with a green title bar. The main content area is titled 'Logon to Office 365'. It contains the following text: 'Provided account must have permissions to authenticate to the Office 365 organization. To sign in, use a web browser and authenticate by entering a code below to the page: <https://microsoft.com/devicelogin>'. Below this text is a text input field containing the code 'CLFZXJFNE' and a 'Copy code' button. At the bottom left, there is an information icon and the text 'Waiting for user logon...'. At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

Step 4. Specify Target Site

At this step of the wizard, specify the target site alias that you want to use for a restore.

The screenshot shows the 'RESTORE WIZARD' window with a green title bar. The main content area is titled 'Specify target site'. It contains the following text: 'Specify the site alias to restore:'. Below this text are two radio button options: 'Restore to the original site (music)' and 'Restore to the following site alias:'. The second option is selected. Below the selected option is a text input field containing the alias 'music_restored'. At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

Step 5. Specify Restore Options

At this step of the wizard, specify restore options and click **Restore**.

You can specify the following restore options:

1. **Changed items.** Allows you to recover data that has been modified in your production environment.
2. **Missed items.** Allows you to recover missed items.
3. **Restore permissions.** Allows you to recover permissions. If not selected, the permissions for the recovered document library or list will be set as follows:
 - If the library (or list) does not exist on target, it will be created inheriting permissions from the parent object.
 - If the library (or list) already exists on target, permissions will be preserved.
4. **Restore list view.** Allows you to recover your list views.
5. **Restore subsites.** Allows you to restore your subsites.
6. **History restore options.** Allows you to select a version:
 - **Overwrite.** To overwrite data in the production environment by recovering only the latest version of the document from the backup.
 - **Merge.** To merge an existing version of the document with that of a backup version.

If not selected, all the versions in the production environment will be replaced with the corresponding data from the backup file.

NOTE:

The **Send a notification by e-mail to the users with permission to the file** check box is only available when restoring data from backups created in Veeam Backup for Microsoft Office 365 for Microsoft Online organizations.

RESTORE WIZARD

Specify the restore options

Restore the following items:

- ☒ Changed items
- ☒ Missing items

Additional options:

- ☒ Restore permissions
- ☒ Send a notification by e-mail to the users with permissions to the file
- ☒ Restore list views
- ☒ Restore subsites

History restore options:

- ☒ Restore only latest version
- ☒ Overwrite
- ☐ Merge

Back Restore Cancel

Restoring Document Libraries and Lists

To restore Microsoft SharePoint document libraries and lists, do the following:

1. [Launch the restore wizard.](#)
2. [Select an authentication method.](#)
3. [Log on to Office 365.](#)
4. [Specify a target list.](#)
5. [Specify restore options.](#)

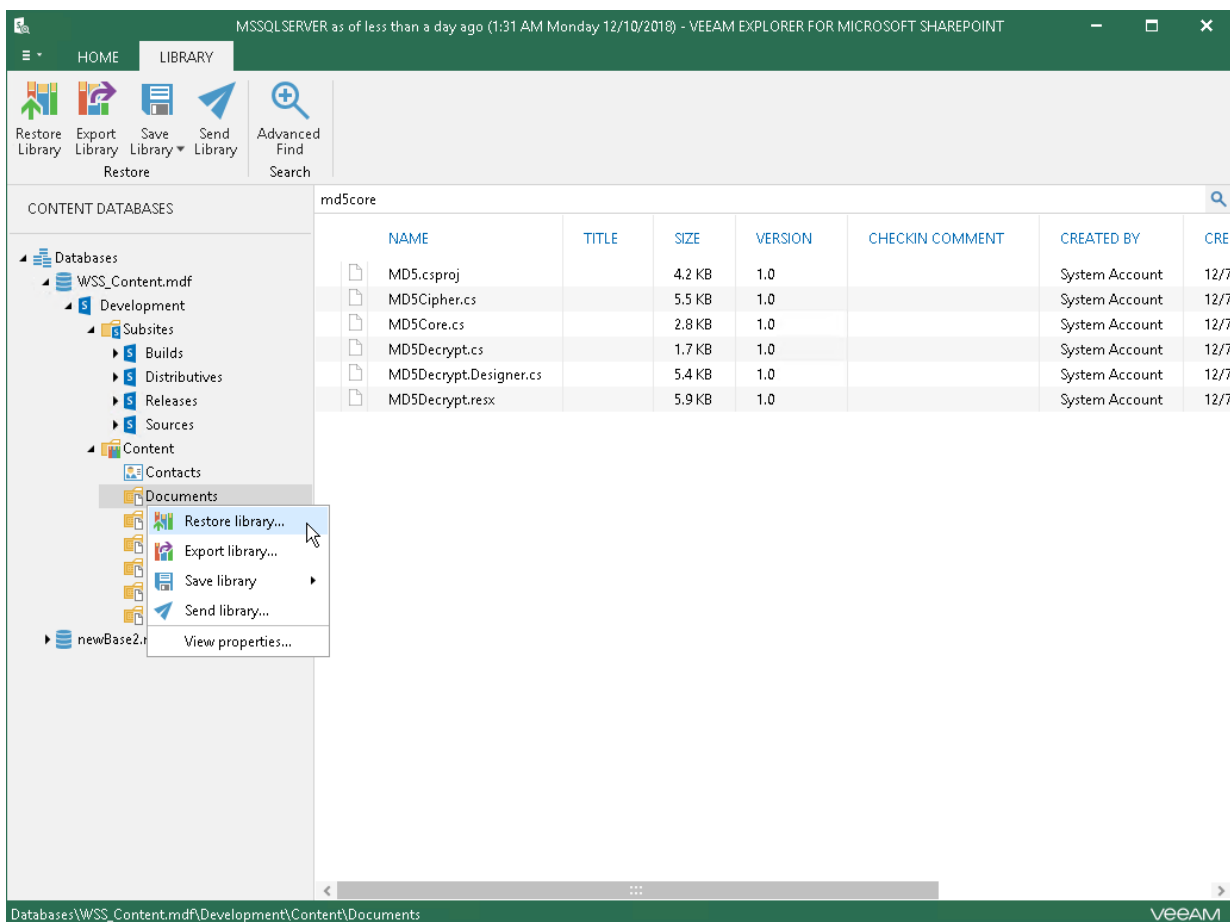
Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. In the navigation pane, select a library or list.
2. On the **Library** tab, select **Restore Library/Restore List** or right-click a library or list and select **Restore Library/Restore List**.

NOTE:

Document libraries and lists can only be restored back to the source site from which they were backed up.



Step 2. Select Authentication Method

At this step of the wizard, choose whether you want to use modern or basic authentication, or authenticate on an on-premises Microsoft SharePoint server.

Modern Authentication

To use modern authentication, do the following:

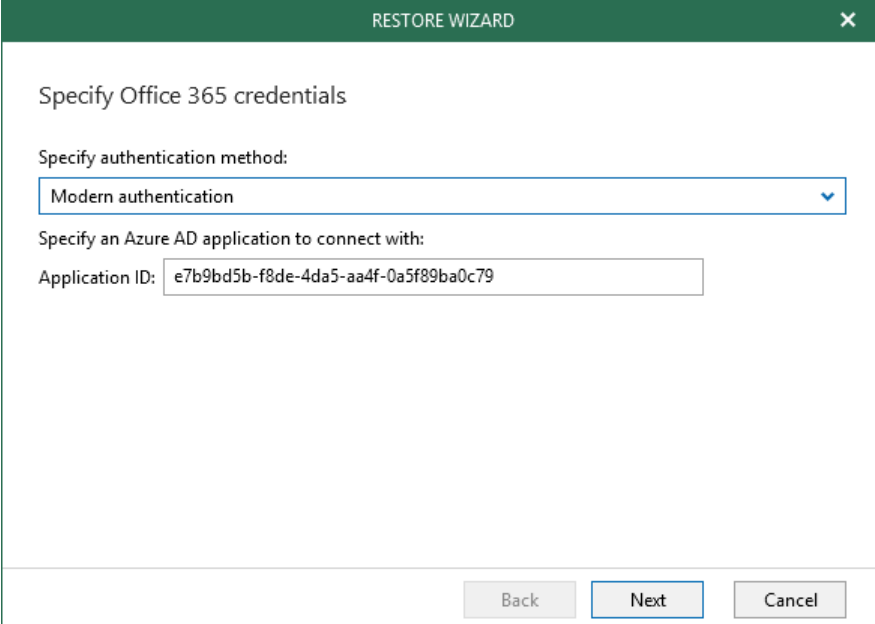
1. From the **Specify authentication method** drop-down list, select *Modern authentication*.

This will allow Veeam Backup for Microsoft Office 365 to use an Azure AD application for a restore. Such an application is used to restore the specified mailbox back to Office 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults.

For more information, see [Microsoft Office 365 Organizations](#).

2. In the **Application ID** field, enter an identification number of the Azure AD application that you want to use for a restore.

By default, Veeam Explorer for Microsoft Exchange populates this field with the identification number of the application that was used during a backup session. If you want to use another application, make sure to grant this application required permissions, as described in [Azure AD Applications](#).



RESTORE WIZARD

Specify Office 365 credentials

Specify authentication method:

Modern authentication

Specify an Azure AD application to connect with:

Application ID: e7b9bd5b-f8de-4da5-aa4f-0a5f89ba0c79

Back Next Cancel

Basic Authentication

To use basic authentication, do the following:

1. From the **Specify authentication method** drop-down list, select *Basic Authentication*.
2. Enter credentials to connect to the SharePoint organization.

RESTORE WIZARD

Specify Office 365 credentials

Specify authentication method:

Basic authentication

Specify user account to connect with:

Username: administrator@abc.onmicrosoft.com

Password: ●●●●●●●●

i To connect with an account enabled for multi-factor authentication (MFA), use an app password instead of a user password.

Back Next Cancel

On-Premises Organizations

To authenticate on an on-premises Microsoft SharePoint server, provide a user name and password.

RESTORE WIZARD

Specify target Microsoft SharePoint Server credentials

☐ Use current account (TECH\Administrator)

☒ Use the following account:

Username: tech\administrator

Password: ●●●●●●●●

Back Next Cancel

Step 3. Log on to Office 365

[This step is only available if you have selected the *Modern Authentication* option at the [previous step](#).]

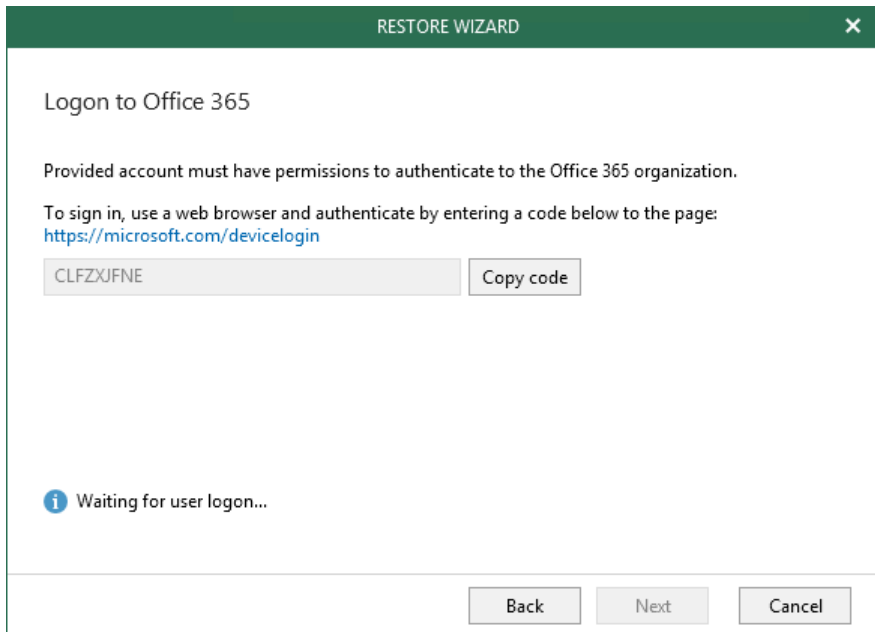
At this step of the wizard, sign in to your Microsoft Office 365 organization.

To sign in to the Microsoft Office 265 organization, do the following:

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

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

2. Click the link to the Microsoft portal.
3. On the **Microsoft Azure device logon** page, paste the code that you have copied and sign in to Azure. Make sure to log in with the user account that has the *SharePoint Administrator* role.
4. Return to the **Restore Wizard** window and click **Next**.



Step 4. Specify Target List

At this step of the wizard, select whether to restore data to the original list or specify a custom one.

You can select the following options:

- **Restore to the original list.** To restore data back to the original location.
- **Restore to the following list.** To restore data to a custom list.

If the specified list does not exist, it will be created automatically.

The screenshot shows a window titled "RESTORE WIZARD" with a close button (X) in the top right corner. The main heading is "Specify target list". Below it, the text "Specify the list to restore items to:" is followed by two radio button options. The first option is "Restore to the original list (Documents)" and is unselected. The second option is "Restore to the following list:" and is selected. Below the second option is a text input field containing the text "my_new_list". At the bottom of the window, there are three buttons: "Back", "Next", and "Cancel". The "Next" button is highlighted with a blue border.

Step 5. Specify Restore Options

At this step of the wizard, specify restore options and click **Restore**.

You can specify the following restore options:

1. **Changed items.** Allows you to recover data that has been modified in your production environment.
2. **Missed items.** Allows you to recover missed items.
3. **Restore permissions.** Allows you to recover permissions. If not selected, the permissions for the recovered document library or list will be set as follows:
 - If the library (or list) does not exist on target, it will be created inheriting permissions from the parent object.
 - If the library (or list) already exists on target, permissions will be preserved.
4. **Restore list view.** Allows you to recover your list views.
5. **History restore options.** Allows you to select a version:
 - **Overwrite.** To overwrite data in the production environment by recovering only the latest version of the document from the backup.
 - **Merge.** To merge an existing version of the document with that of a backup version.

If not selected, all the versions in the production environment will be replaced with the corresponding data from the backup file.

NOTE:

The **Send a notification by e-mail to the users with permission to the file** check box is only available when restoring data from backups created in Veeam Backup for Microsoft Office 365 for Microsoft Online organizations.

RESTORE WIZARD

Specify the restore options

Restore the following items:

☒ Changed items

☒ Missing items

History restore options:

☒ Restore only latest version

☒ Overwrite

☐ Merge

Additional options:

☒ Restore permissions

☒ Send a notification by e-mail to the users with permissions to the file

☒ Restore list views

Back

Restore

Cancel

Restoring Documents and List Items

To restore Microsoft SharePoint documents and list items, do the following:

1. [Launch the Restore wizard.](#)
2. [Select an authentication method.](#)
3. [Log on to Office 365.](#)
4. [Specify a target list.](#)
5. [Specify restore options.](#)

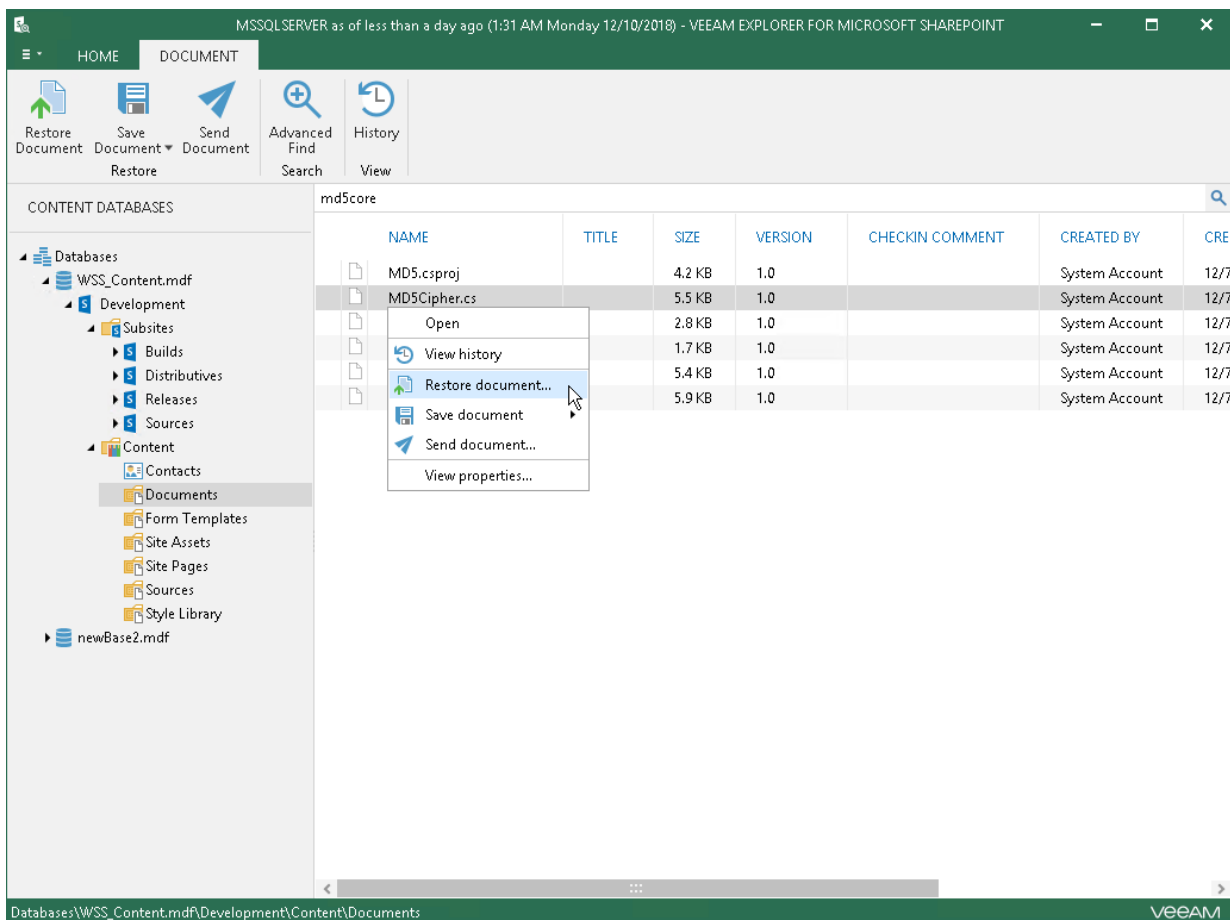
Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. In the navigation pane, select a document or list item.
2. On the **Document** tab, select **Restore Document/Restore Item** or right-click an object and select **Restore Document/Restore Item**.

NOTE:

When restoring backups created with Veeam Backup for Microsoft Office 365, document libraries and lists can only be restored back to the source site from which they were backed-up.



Step 2. Select Authentication Method

At this step of the wizard, choose whether you want to use modern or basic authentication, or authenticate on an on-premises Microsoft SharePoint server.

Modern Authentication

To use modern authentication, do the following:

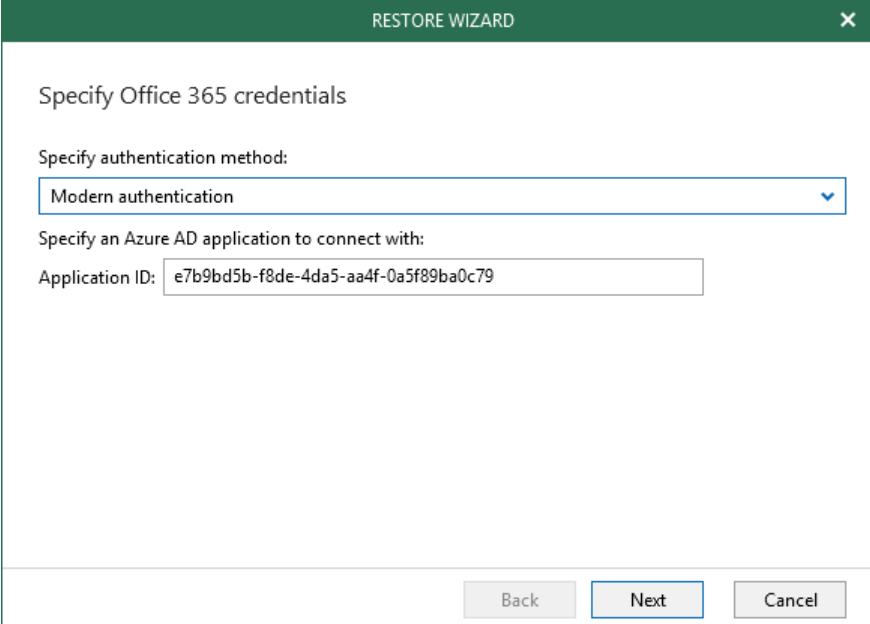
1. From the **Specify authentication method** drop-down list, select *Modern authentication*.

This will allow Veeam Backup for Microsoft Office 365 to use an Azure AD application for a restore. Such an application is used to restore the specified mailbox back to Office 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults.

For more information, see [Microsoft Office 365 Organizations](#).

2. In the **Application ID** field, enter an identification number of the Azure AD application that you want to use for a restore.

By default, Veeam Explorer for Microsoft Exchange populates this field with the identification number of the application that was used during a backup session. If you want to use another application, make sure to grant this application required permissions, as described in [Azure AD Applications](#).



RESTORE WIZARD

Specify Office 365 credentials

Specify authentication method:

Modern authentication

Specify an Azure AD application to connect with:

Application ID: e7b9bd5b-f8de-4da5-aa4f-0a5f89ba0c79

Back Next Cancel

Basic Authentication

To use basic authentication, do the following:

1. From the **Specify authentication method** drop-down list, select *Basic Authentication*.
2. Enter credentials to connect to the SharePoint organization.

RESTORE WIZARD

Specify Office 365 credentials

Specify authentication method:

Basic authentication

Specify user account to connect with:

Username: administrator@abc.onmicrosoft.com

Password:

To connect with an account enabled for multi-factor authentication (MFA), use an app password instead of a user password.

Back Next Cancel

On-Premises Organizations

To authenticate on an on-premises Microsoft SharePoint server, provide a user name and password.

RESTORE WIZARD

Specify target Microsoft SharePoint Server credentials

☐ Use current account (TECH\Administrator)

☒ Use the following account:

Username: tech\administrator

Password:

Back Next Cancel

Step 3. Log on to Office 365

[This step is only available if you have selected the *Modern Authentication* option at the [previous step](#).]

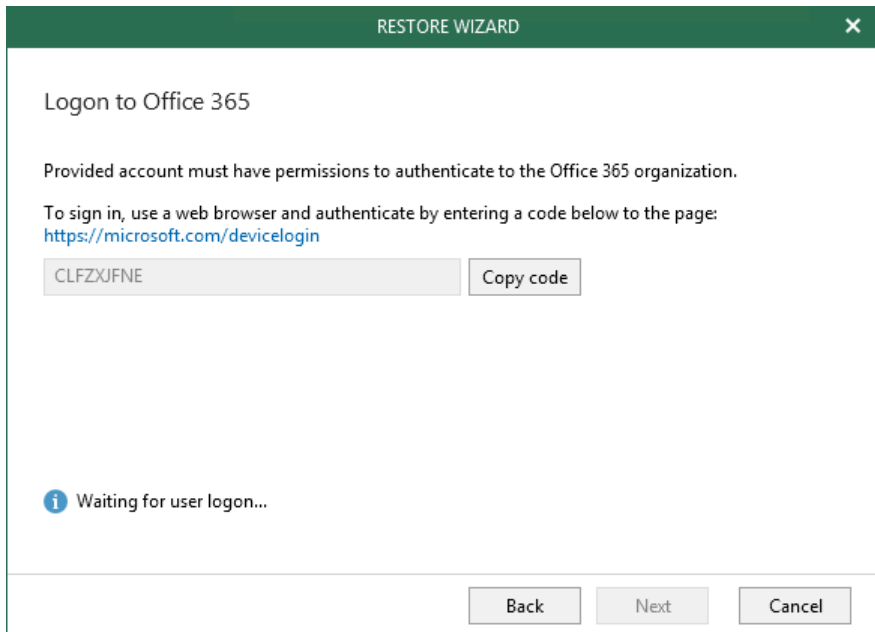
At this step of the wizard, sign in to your Microsoft Office 365 organization.

To sign in to the Microsoft Office 265 organization, do the following:

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

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

2. Click the link to the Microsoft portal.
3. On the **Microsoft Azure device logon** page, paste the code that you have copied and sign in to Azure. Make sure to log in with the user account that has the *SharePoint Administrator* role.
4. Return to the **Restore Wizard** window and click **Next**.



RESTORE WIZARD

Logon to Office 365

Provided account must have permissions to authenticate to the Office 365 organization.

To sign in, use a web browser and authenticate by entering a code below to the page:
<https://microsoft.com/devicelogin>

CLFZXJFNE Copy code

i Waiting for user logon...

Back Next Cancel

Step 4. Specify Target List

At this step of the wizard, select whether to restore data to the original list or specify a custom one.

You can select the following options:

- **Restore to the original list.** To restore data back to the original location.
- **Restore to the following list.** To restore data to a custom list.
Make sure to specify an existing list.

RESTORE WIZARD

Specify target list

Specify the list to restore items to:

☐ Restore to the original list (Documents)

☒ Restore to the following list:

my_new_list

Back Next Cancel

Step 5. Specify Restore Options

At this step of the wizard, specify restore options and click **Restore**.

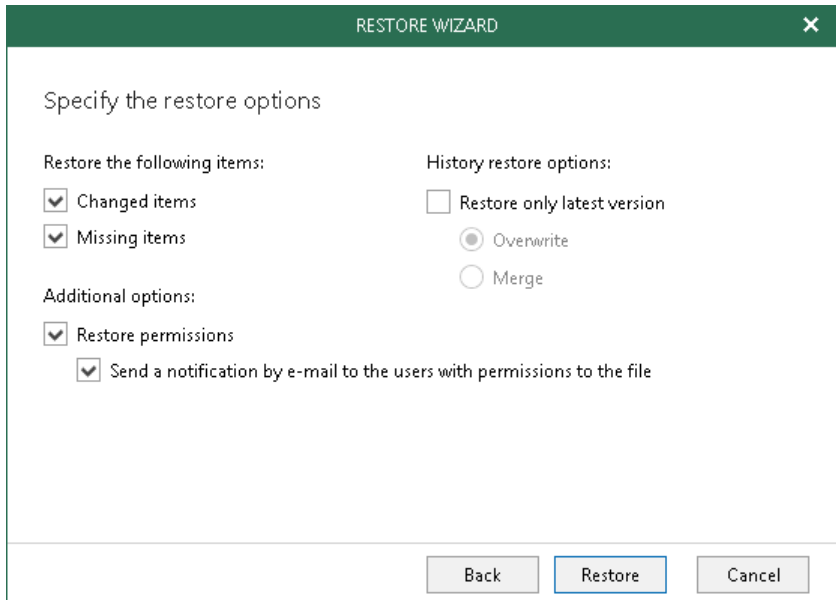
The restore options are as follows:

1. **Changed items.** Allows you to recover data that has been modified in your production environment.
2. **Missed items.** Allows you to recover missed items.
3. **Restore permissions.** Allows you to recover permissions. If not selected, permissions for the recovered document library or list will be set as follows:
 - If the library (or list) does not exist on target, it will be created inheriting permissions from the parent object.
 - If the library (or list) already exists on target, permissions will be preserved.
4. **History restore options.** Allows you to select a version:
 - **Overwrite.** To overwrite data in the production environment by recovering only the latest version of the document from the backup.
 - **Merge.** To merge an existing version of the document with that of a backup version.

If not selected, all the versions in the production environment will be replaced with the corresponding data from the backup file.

NOTE:

The **Send a notification by e-mail to the users with permission to the file** check box is only available when restoring data from backups created in Veeam Backup for Microsoft Office 365 for Microsoft Online organizations.



The screenshot shows the 'RESTORE WIZARD' dialog box with a dark green title bar. The main area is titled 'Specify the restore options'. It contains three sections of checkboxes: 'Restore the following items:' with 'Changed items' and 'Missing items' checked; 'History restore options:' with 'Restore only latest version' unchecked and radio buttons for 'Overwrite' (selected) and 'Merge'; and 'Additional options:' with 'Restore permissions' checked and a sub-checked option 'Send a notification by e-mail to the users with permissions to the file'. At the bottom are 'Back', 'Restore' (highlighted with a blue border), and 'Cancel' buttons.

RESTORE WIZARD

Specify the restore options

Restore the following items:

- ☒ Changed items
- ☒ Missing items

History restore options:

- ☐ Restore only latest version
- ☒ Overwrite
- ☐ Merge

Additional options:

- ☒ Restore permissions
 - ☒ Send a notification by e-mail to the users with permissions to the file

Back Restore Cancel

Export

This section explains how to export and import Microsoft SharePoint data.

Consider the following:

- Export is unavailable for backups created in Veeam Backup for Microsoft Office 365.
- Make sure to read [Unsupported SharePoint Lists](#) before exporting Microsoft SharePoint lists.

Exporting Microsoft SharePoint Data

Veeam Explorer for Microsoft SharePoint allows you to export SharePoint document libraries and lists.

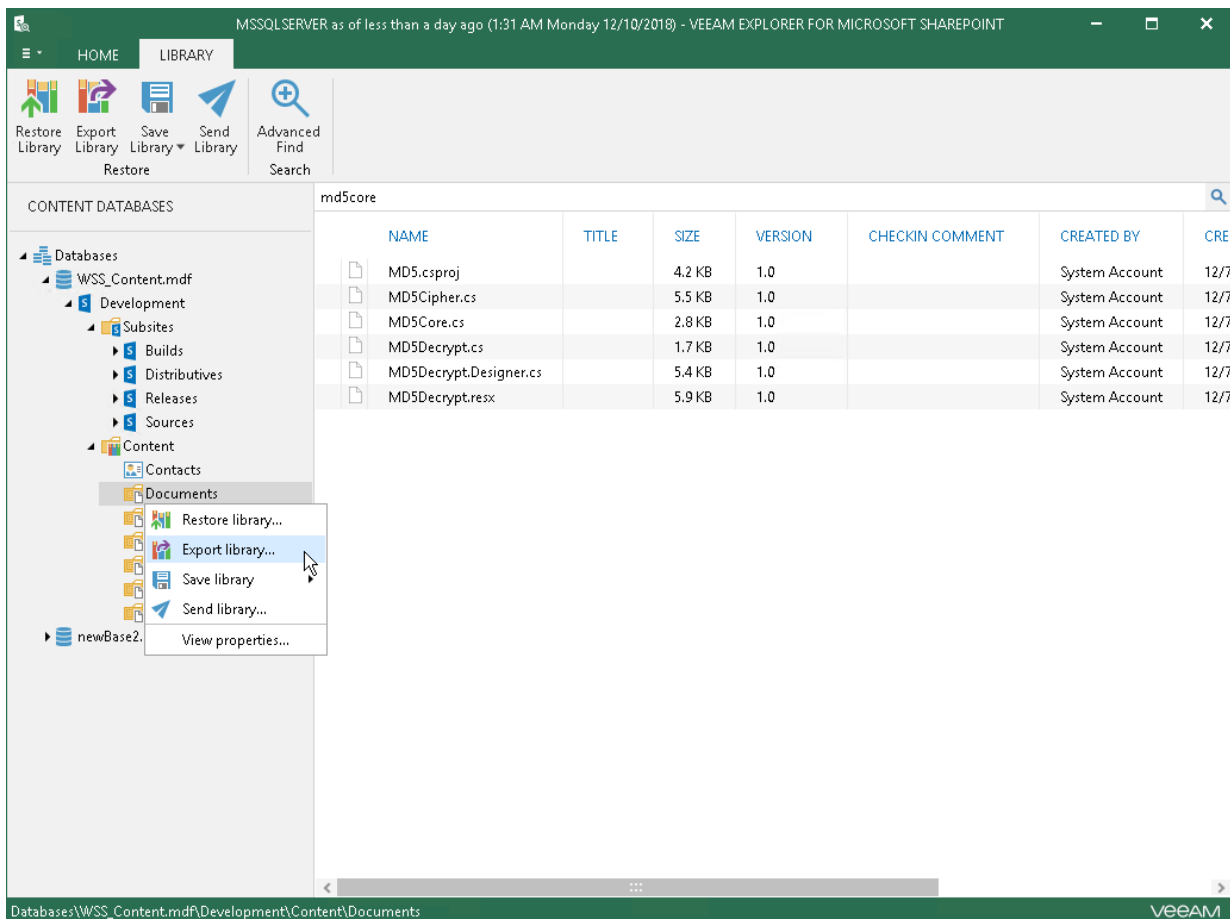
The exported content will be saved as a set of XML files and can be imported to another SharePoint database using PowerShell cmdlets, as described in [Importing Microsoft SharePoint Data](#).

To export SharePoint data, do the following:

1. In the navigation pane, select a library or list.
2. On the **Library** tab, select **Export Library/Export List** or right-click an object and select **Export Library/Export List**.
3. Specify the output directory and click **OK**.

NOTE:

Export of items is not supported in the current version.



Importing Microsoft SharePoint Data

To import document library or list, use either of the following PowerShell cmdlets:

- For PowerShell snap-in, use the following command.

```
Add-PsSnapin Microsoft.SharePoint.PowerShell  
  
Import-SPWeb -Identity "http://<web_server_name>/sites/<destination_site>" -Path  
"C:\<export_folder>" -NoFileCompression -IncludeUserSecurity
```

- For SharePoint Management Shell, use the following command.

```
Import-SPWeb -Identity "http://<web_server_name>/sites/<destination_site>" -Path  
"C:\<export_folder>" -NoFileCompression -IncludeUserSecurity
```

where:

- *<web_server_name>* – destination web server;
- *<destination_site>* – destination web site;
- *<export_folder>* – source folder containing exported library/list content.

To get extended help on the **Import-SPWeb** command, use the following command.

```
Get-Help Import-SPWeb -full
```

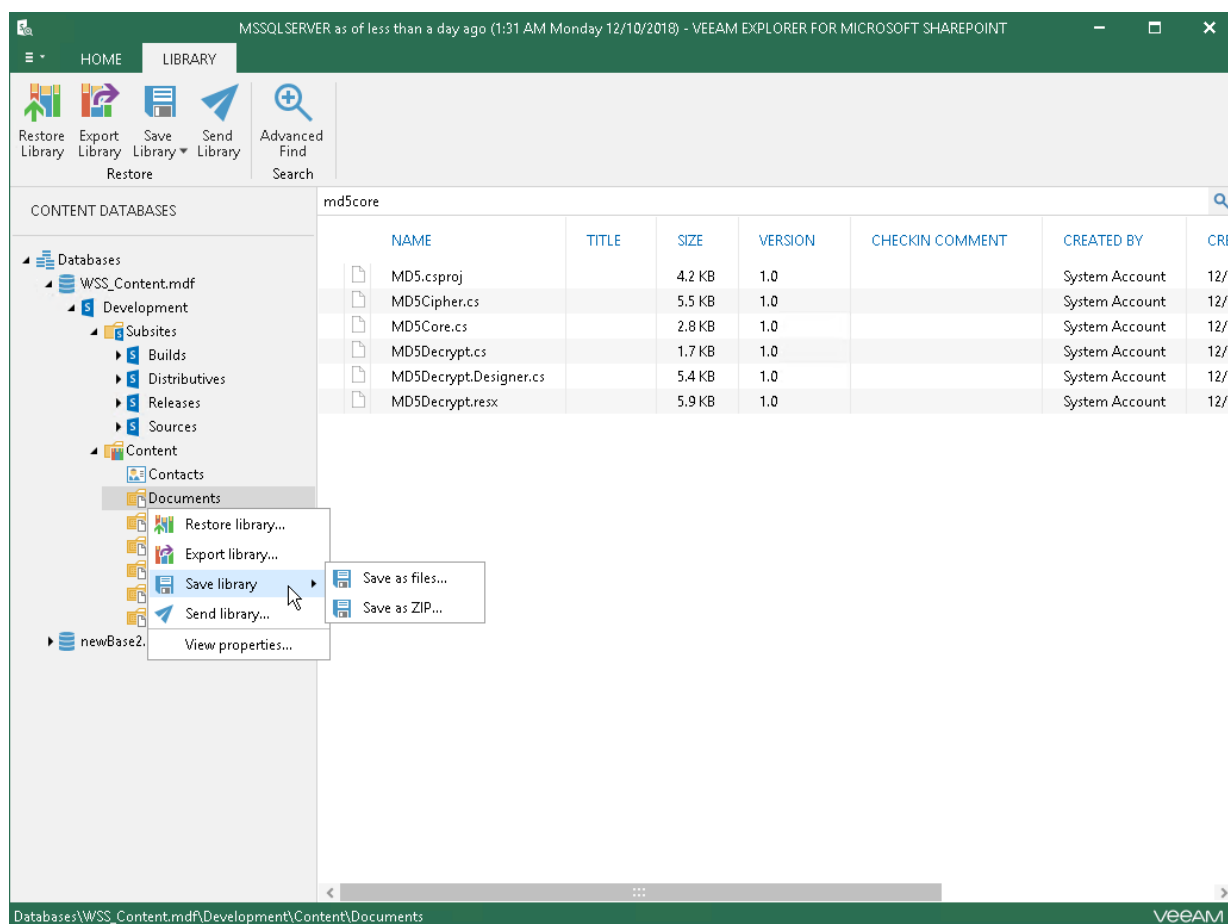

Saving Microsoft SharePoint Documents and Libraries

Veeam Explorer for Microsoft SharePoint allows you to save your libraries and library documents to a specified location.

To save a Microsoft SharePoint library or library documents, do the following:

1. In the navigation pane, select a library.
2. On the **Library** tab, select **Save Library > Save files** or **Save Library > Save as ZIP** or right-click an object and select **Save Library > Save files** or **Save Library > Save as ZIP**.

To save documents from a library, select a document in the preview pane and click **Save Document > Save files** or **Save Document > Save as ZIP**.



Sending Microsoft SharePoint Documents and Libraries

Veeam Explorer for Microsoft SharePoint allows you to send libraries or library documents to the specified recipients via email.

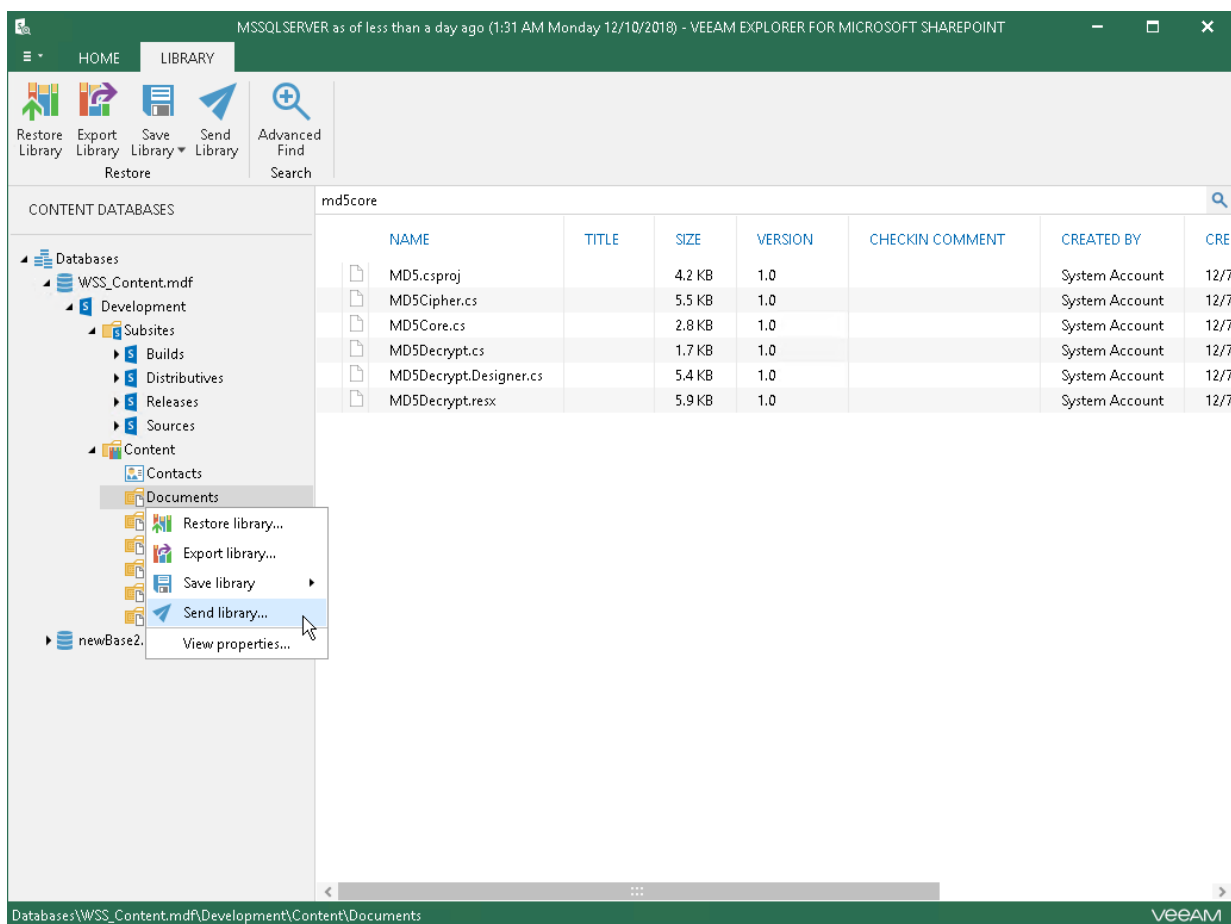
TIP:

Before sending documents, make sure to configure SMTP settings, as described in [Configuring SMTP Settings](#). The amount of data you can send at a time depends on your SMTP server configuration.

To send Microsoft SharePoint library or library documents, do the following:

1. In the navigation pane, select a library to send.
2. On the **Library** tab, select **Send Library** or right-click an object and select **Send Library**.


To send documents from a library, select a document in the preview pane and click **Send Document**.



3. Provide a recipient address.

The **From** field is filled automatically based on the address you have provided when configuring SMTP settings. To edit the message body, click **More Details**.

SEND ITEMS

Send


From:


administrator@tech.local


To:


Subject:


SharePoint Documents Recovery


 MD5Core.cs 2.8 KB

 MD5Decrypt.cs 1.7 KB

 MD5Decrypt.resx 5.9 KB

 MD5.csproj 4.2 KB

 MD5Cipher.cs 5.5 KB

 MD5Decrypt.Designer.cs 5.4 KB

^ Fewer details

by Veeam Explorer for Microsoft SharePoint.

Appendix A: Unsupported SharePoint Lists

The following table contains unsupported Microsoft SharePoint lists.

ID	List Name	Version
101	SearchConfigListTemplate	2013/2016/2019
110	datasrcs	2010/2013/2016/2019
111	webtemp	2010/2013/2016/2019
112	users	2010/2013/2016/2019
113	wplib	2010/2013/2016/2019
114	listtemp	2010/2013/2016/2019
116	mplib	2010
117	nocodewf	2010/2013/2016/2019
118	workflowProcess	2010/2013/2016/2019
121	solutions	2010/2013/2016/2019
122	nocodepublicwf	2010/2013/2016/2019
123	themes	2010/2013/2016/2019
124	designs	2013/2016/2019
125	appdata	2013/2016/2019
126	appfiles	2019
160	accessrequests	2013/2016/2019
175	MaintenanceLogs	2013/2016/2019
200	meetings	2010/2013/2016/2019
212	wkspglib	2010/2013/2016/2019
331	ComponentManifests	2019
334	ClientSideAssets	2019

335	SiteCollectionAppCatalogs	2019
336	WebApiPermissionRequests	2019
401	fcgroups	2010/2013/2016/2019
401	MonitoredAppsList	2013/2016/2019
420	timecard	2013/2016/2019
425	whatsnew	2010/2013/2016/2019
530	ContentFollowingList	2013/2016/2019
544	MicroBlogList	2013/2016/2019
550	SocialDataStoreList	2013/2016/2019
563	AnnouncementTilesList	2016/2019
600	extlist	2010/2013/2016/2019
880	members	2013/2016/2019
925	abusereports	2013/2016/2019
1221	healthreports	2010/2013/2016/2019
1305	EDiscoverySources	2016/2019
1306	EDiscoverySourceInstances	2013/2016/2019
1309	DlpEDiscoveryQueries	2016/2019
1310	PreservationListTemplate	2013/2016/2019
2000	PNSubscribers	2013/2016/2019
2001	ExternalSubscriptions	2013/2016/2019
3100	AccSrvAddApp	2013/2016/2019
3300	SharingLinks	2016/2019
3400	HashtagStore	2019
3401	BlockedHashtags	2019
3412	HubSites	2019

3415	WebTemplateExtensions	2019
3500	IRCollection	2019
3501	IRReference	2019
3502	IRReferenceCollection	2019
4501	wfsvc	2013/2016/2019
10000	Academic Library	N/A
10001	eduentity"	2013/2016/2019
10007	EduWorkItem	2013/2016/2019
10008	EduQuiz	2013/2016/2019
10051	eduentity	2013/2016/2019
10060	eduusersetting	2013/2016/2019
10061	eduexternalsyncsetting	2013/2016/2019
10099	AcquisitionHistoryList	2013/2016/2019
10101	edudocument	2013/2016/2019
10102	IWConvertedForms	2010/2013/2016/2019
10401	eduannouncement	2013/2016/2019
10631	educalendar	2013/2016/2019

Veeam Explorer for Microsoft OneDrive for Business

Veeam Explorer for Microsoft OneDrive for Business allows you to restore Microsoft OneDrive data from backups created in Veeam Backup for Microsoft Office 365.

You can also save data from backups to a local computer and send data from backups via email.

Planning and Preparation

Veeam Explorer for Microsoft OneDrive for Business comes as part of the Veeam Explorer for Microsoft SharePoint installation package and has the same [system requirements](#).

Consider that when Veeam Explorer for Microsoft SharePoint is installed on a server on which both Veeam Backup & Replication and Veeam Backup for Microsoft Office 365 are installed, the notification settings will be inherited from the Veeam Backup and Replication Global Notification settings.

Launching Application and Exploring Backups

To open Veeam Explorer for Microsoft OneDrive for Business and load backups, you can use any of the following methods:

- The **Explore** option. For more information, see [Data Restore](#).

When loading backups located in object storage repositories, Veeam Explorer for Microsoft OneDrive for Business will notify you about the location of these backups. You can select the **Don't show this message again** check box to unsubscribe from such notifications. To enable notifications, select the **Reset disabled pop-up notifications** check box, as described in [Configuring Advanced Settings](#).

- Go to **Start** and click **Veeam Explorer for Microsoft OneDrive for Business**.

When you open Veeam Explorer for Microsoft OneDrive for Business from the **Start** menu, all backed-up databases will be loaded automatically.

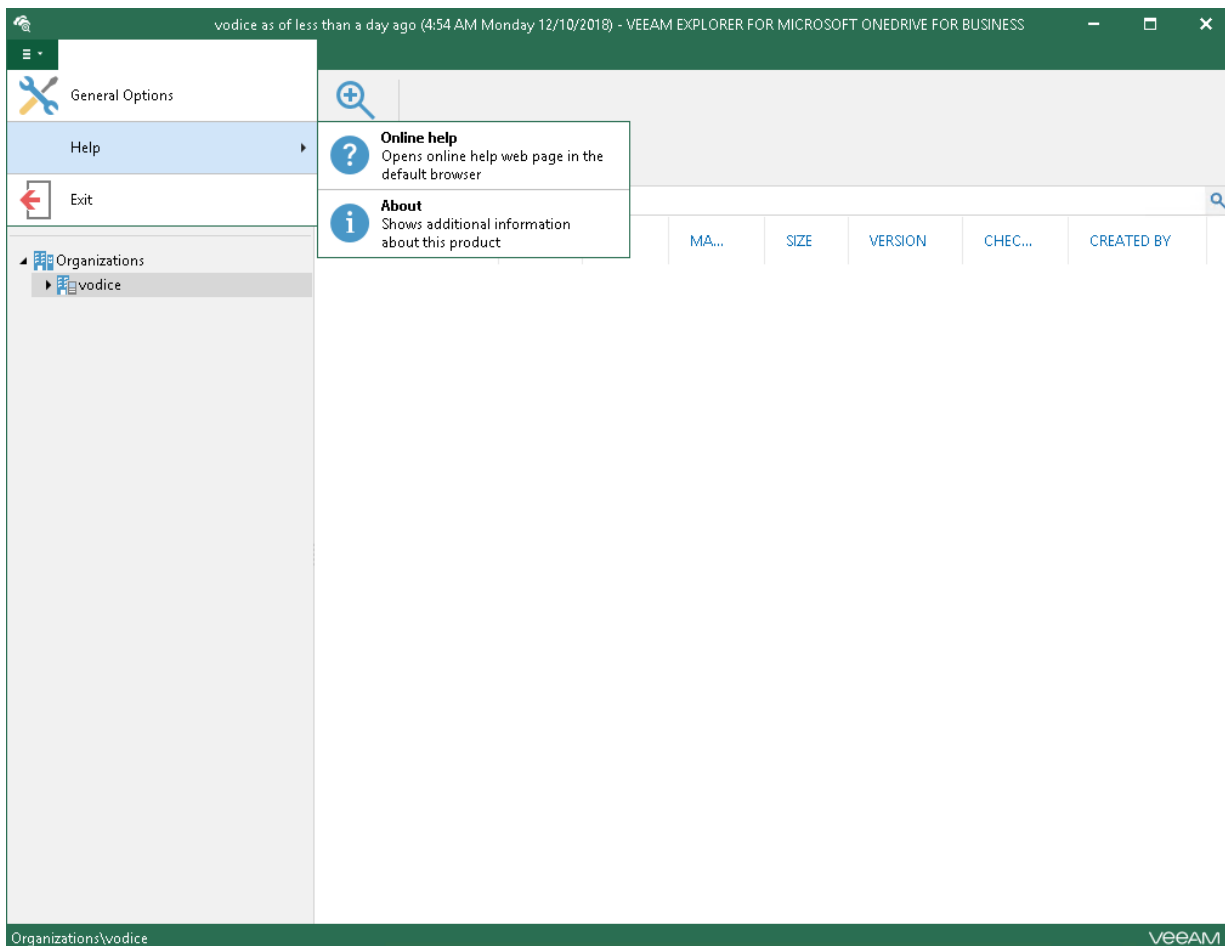
Understanding User Interface

Veeam Explorer for Microsoft OneDrive for Business provides you with the convenient user interface that allows you to perform required operations in a user-friendly manner.

Main Menu

The main menu comprises the following features:

- **General Options.** Allows you to configure program options. See [Performing Initial Configuration Settings](#).
- **Help.**
 - **Online help.** Opens the online web help page.
 - **About.** Shows current product information.
- **Exit.** Closes the program.

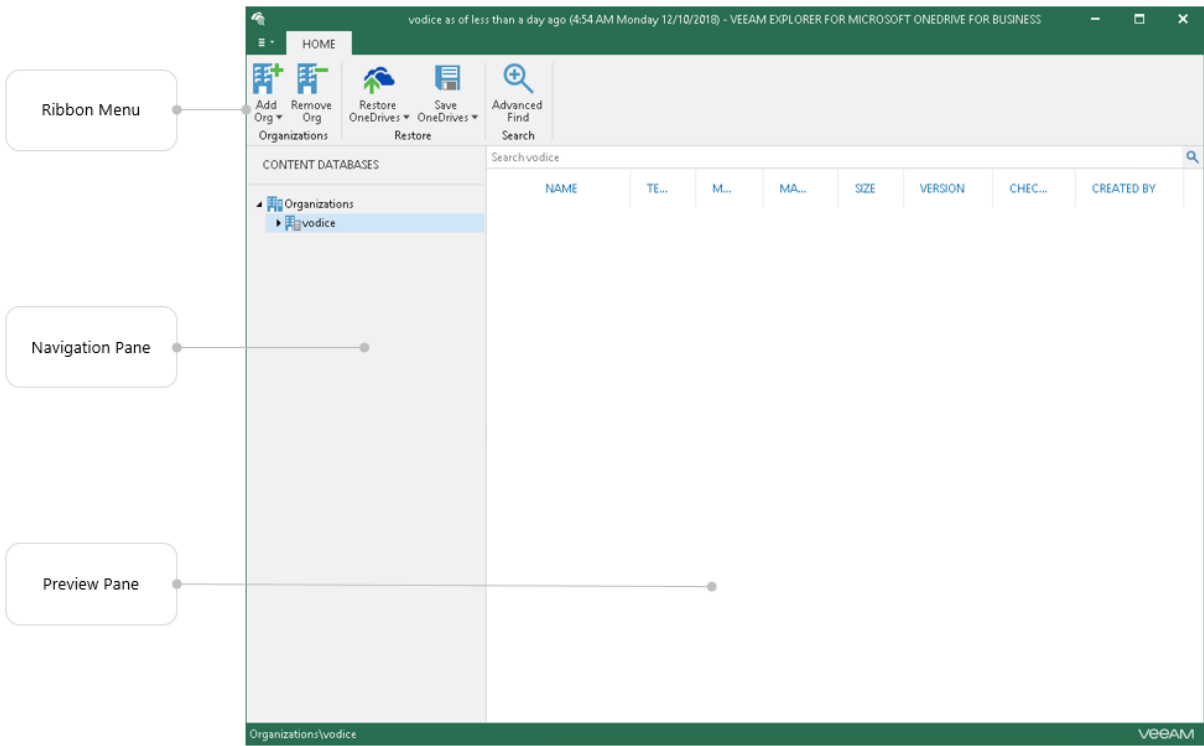


Main Application Window

The main application window might be divided into three categories:

1. The ribbon menu, which contains general program commands organized into logical groups.
2. The navigation area, which allows you to browse through the hierarchy of your backup files.

3. The preview pane, which shows you the details about objects you have selected in the navigation area.



Browsing, Searching and Viewing Items

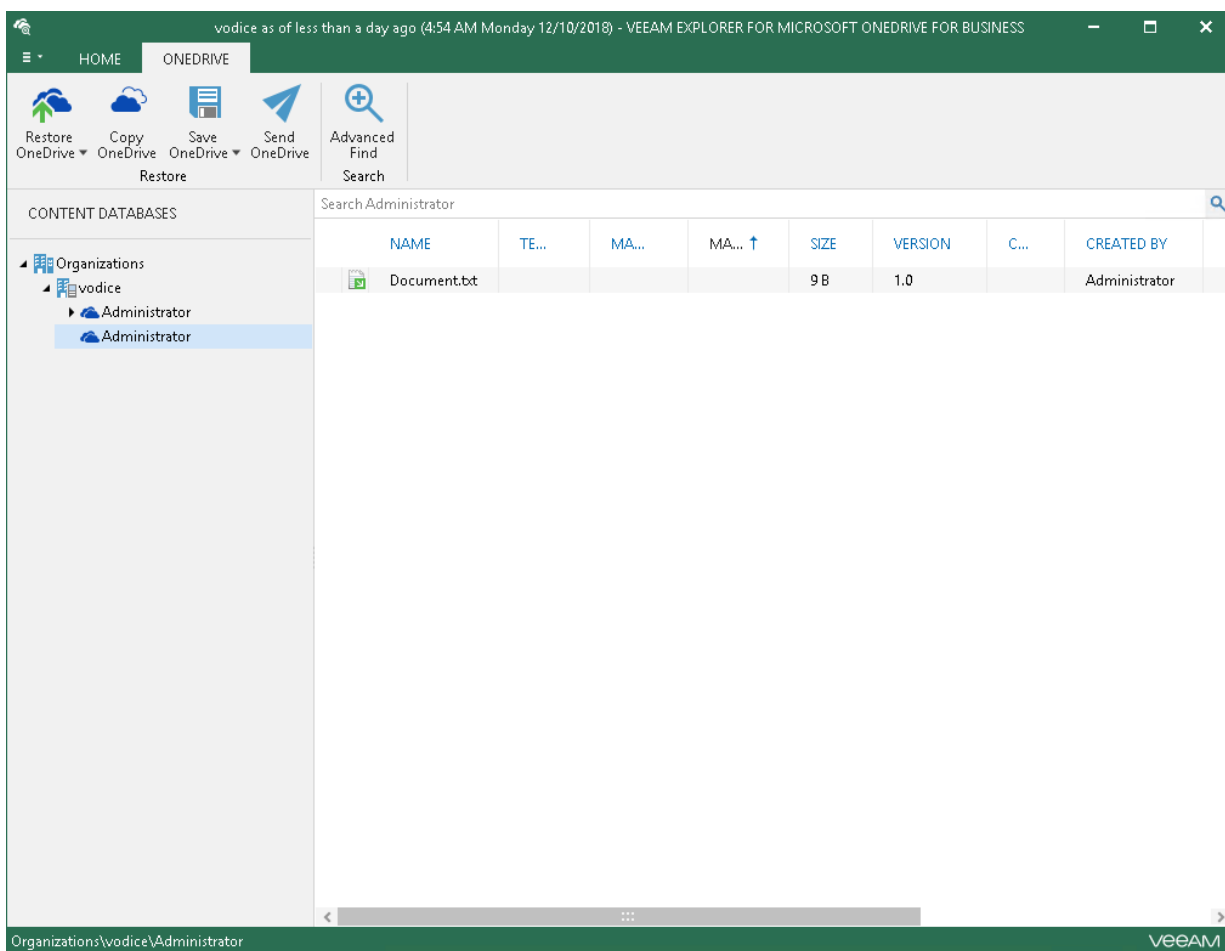
Continue with this section to learn more about:

- [Browsing backup content](#)
- [Viewing objects properties and open files](#)
- [Searching for objects in a backup file](#)
- [Using the advance search capabilities](#)

Browsing

To view the contents of a backup file, you use the navigation pane which shows you the database structure containing your OneDrive documents.

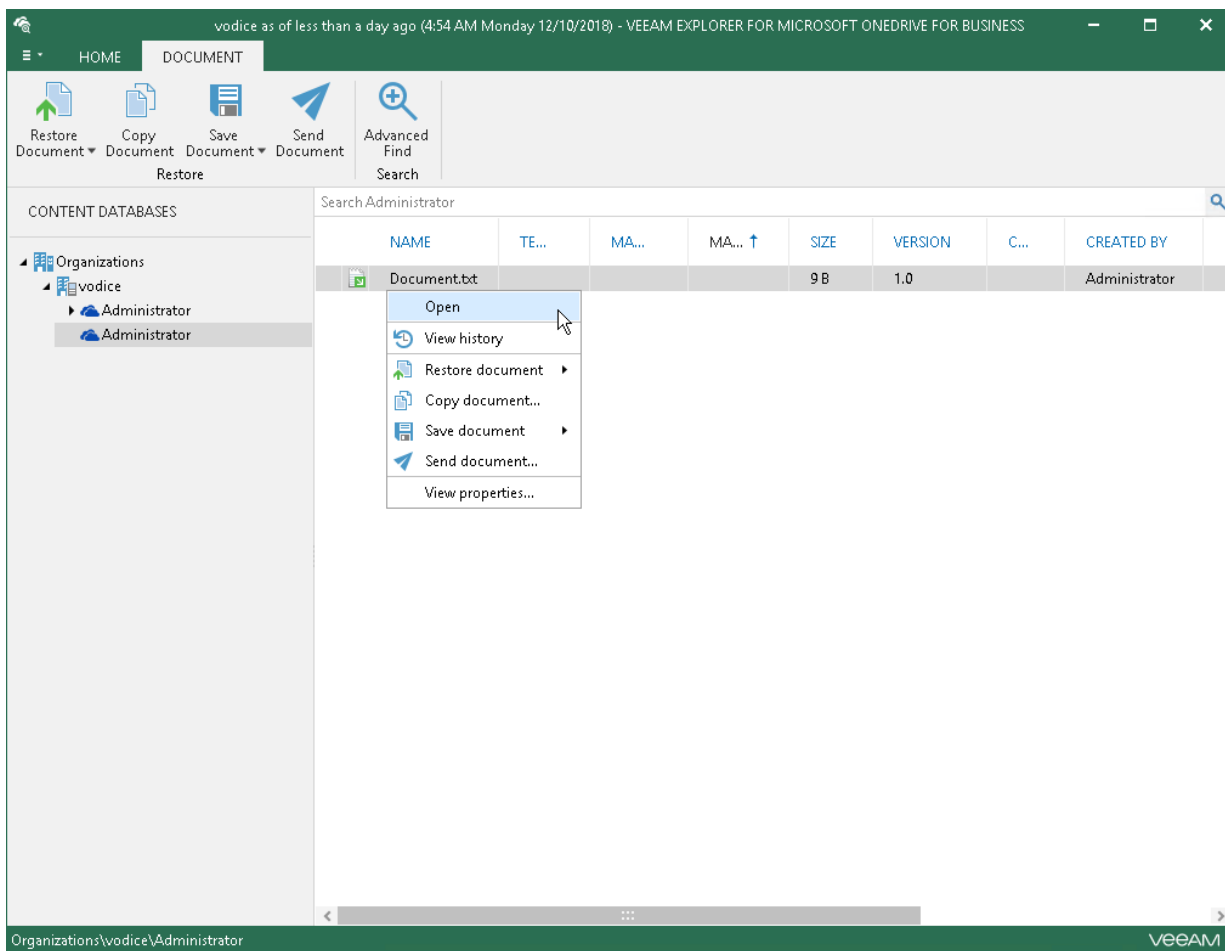
After you select an object in the navigation pane, you can see its content in the preview pane.



Viewing Properties and Opening Files

To view object properties, right-click an object in the preview pane and select **View Properties**.

To open a document using an associated application, right-click a document in the preview pane and select **Open**.



Searching

The search mechanism allows you to find items matching specified search criteria.

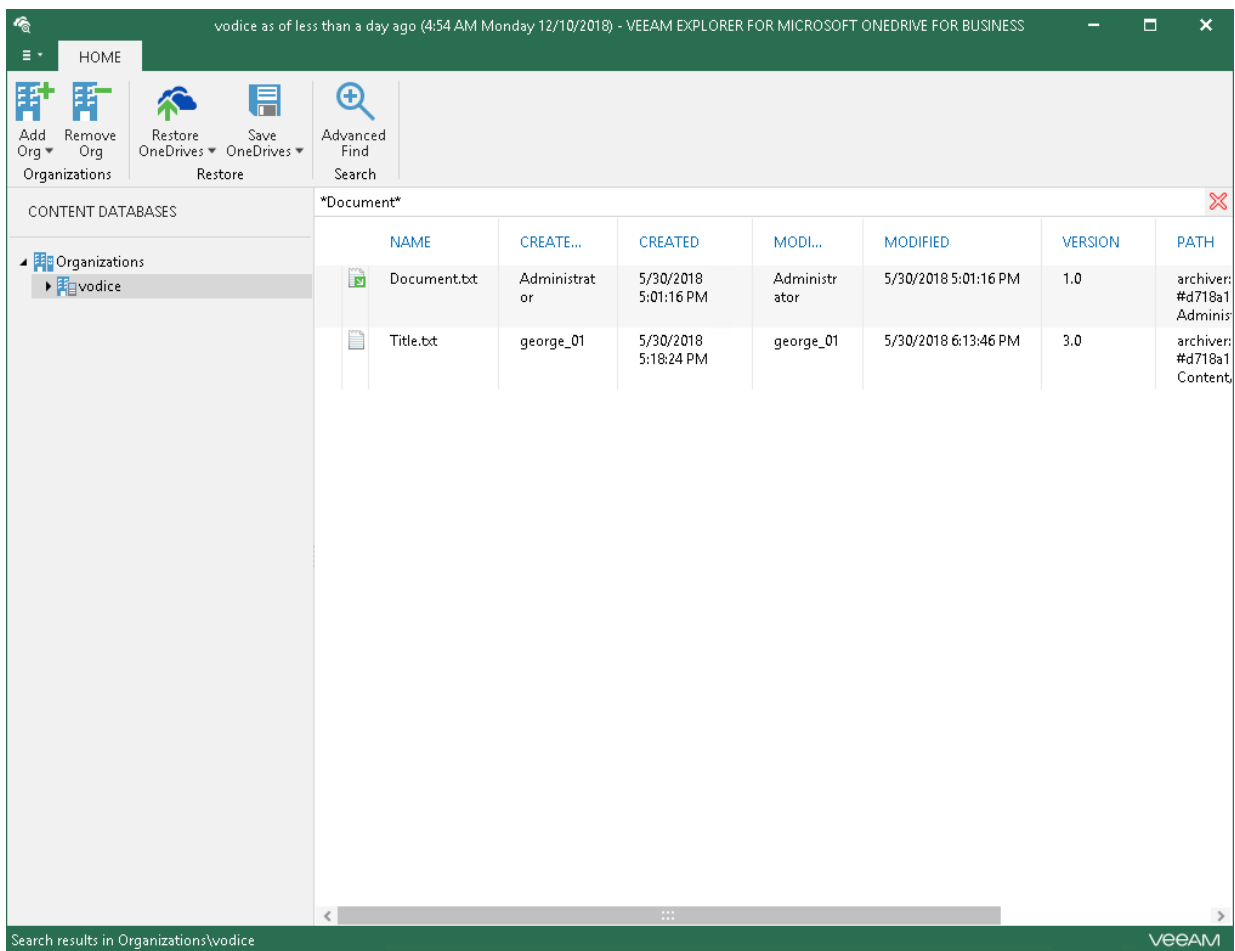
To search for required items, do the following:

1. In the navigation pane, select an object in which you want to find your data.
2. Enter a search query to the search field at the top of the preview pane.

NOTE:

To find the exact phrase, use double quotes. For example, *"Attachments"*.

You can narrow your search results by specifying various search criteria using the *criteria:value* format. You can also use logical upper-cased operators such as *AND*, *OR* and *NOT* along with wildcard characters such as *** and *?*.



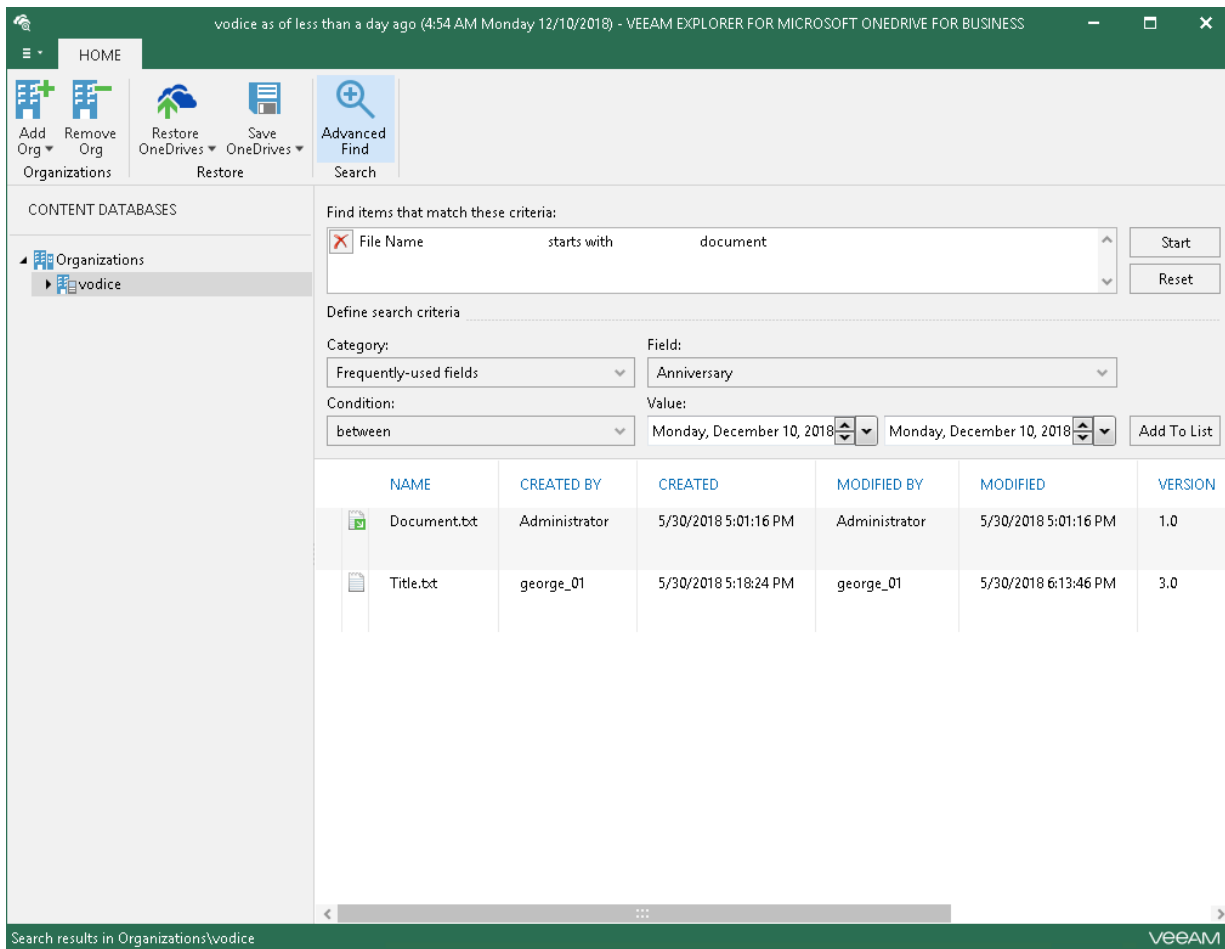
Using Advanced Find Capabilities

The **Advanced Find** mechanism allows you to define your search criteria more precisely.

For example, to find an object that starts with the word *Attachme*, do the following:

1. In the preview pane, select a content node and click **Advanced Find**.
2. In the **Define search criteria** section, select **Category > Document fields**.
3. In the **Field** list, select **File Name**.
4. In the **Condition** list, select **Starts With**.
5. In the **Value** field, specify a file name.
6. Click **Start**.

To remove a filter, click the cross mark next to it. To remove all configured filters, click **Reset**.



General Application Settings

Continue with this section to learn more about configuring general application settings and components.

SMTP Settings

To send Microsoft OneDrive items as attachments, you must configure SMTP server settings.

To configure SMTP settings, do the following:

1. Go to the main menu and click **General Options**.
2. On the **SMTP Settings** tab, select the **Configure SMTP settings** check box and specify the following:
 - DNS name or IP address of the mail server.
 - SMTP communication port.
 - The sender email address. This address will appear in the **From** field when sending OneDrive items. See [Sending Microsoft OneDrive Documents](#).
 - Select **Use authentication** check box If your SMTP server requires SMTP authentication for outgoing mail and provide valid credentials.
 - Select **Enable SSL security** check box to enable SSL data encryption.
3. Click **Send** to send a test email message.
4. Click **Apply**.

The screenshot shows the 'OPTIONS' dialog box with the 'SMTP Settings' tab selected. The 'Configure SMTP settings' checkbox is checked. The 'Server' field contains 'smtp.office365.com', the 'Port' field contains '25', and the 'From' field contains 'administrator@tech.local'. The 'Use authentication' checkbox is also checked, with the 'User' field containing 'Administrator' and the 'Password' field masked with dots. The 'Enable SSL security' checkbox is checked. At the bottom, there is a 'Send test e-mail' section with an 'E-mail' field containing 'test@tech.local' and a 'Send' button. The dialog box has 'OK', 'Cancel', and 'Apply' buttons at the bottom right.

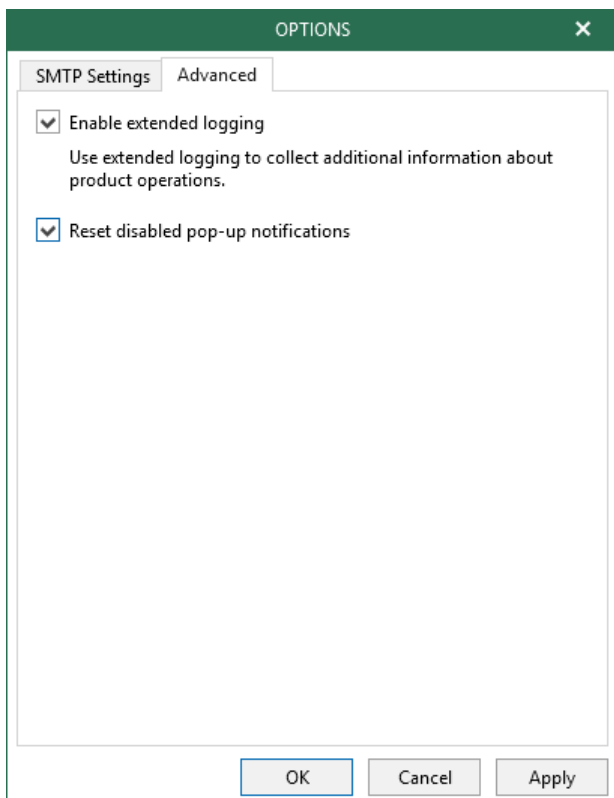
Advanced Settings

This section explains how to configure advanced settings of the application.

To configure advanced settings, do the following:

1. Go to the main menu and click **General Options**.
 2. Got to the **Advanced** tab and select the following:
 - Select the **Enable Extended logging** check box to enable extended logging mode to collect logs that contain more details on specific operations.
- After enabling extended logging mode, you can go back to the application and perform required actions, then collect logs.
- Select the **Reset disabled pop-up notifications** check box to enable notifications when loading backups from object storage repositories.

Applicable to backups created in Veeam Backup for Microsoft Office 365.



Standalone Databases

This section explains how to add standalone databases to the Veeam Explorer for Microsoft OneDrive for Business scope and how to connect to a Veeam Backup for Microsoft Office 365 server and service provider server to view backups located on these servers.

Adding Veeam Backup for Microsoft Office 365 Databases

To manually add databases that store Microsoft Office 365 organization data, do the following:

1. Click **Add Org > Veeam Backup for Microsoft Office 365 Databases** on the ribbon menu or use the corresponding context menu command.
2. Specify the database file location and log directory.
3. Click **Open**.

ADD DATABASE

Specify Veeam Backup for Microsoft Office 365 database (.adb) file location:

Database file:

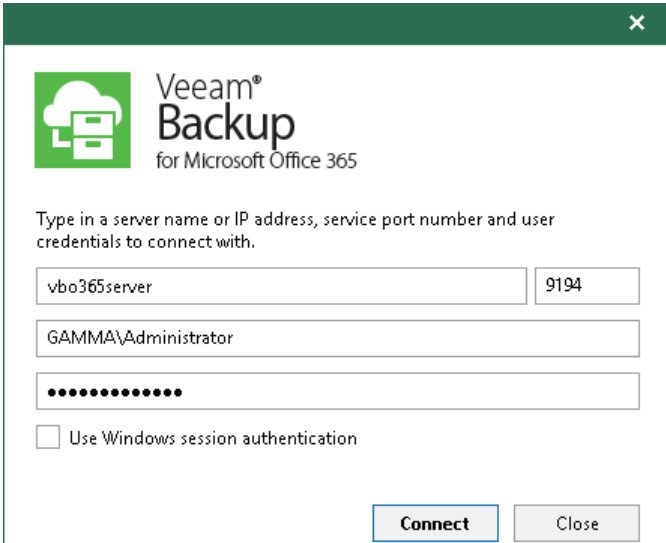
Logs folder:

Adding Veeam Backup for Microsoft Office 365 Server

You can use the built-in Veeam Explorer abilities to connect to another Veeam Backup for Microsoft Office 365 server and add its databases to the Veeam Explorer for Microsoft OneDrive for Business scope.

To connect to another Veeam Backup for Microsoft Office 365 server, do the following:

1. Click **Add Org > Veeam Backup for Microsoft Office 365 Server** on the toolbar or use the corresponding context menu command.
2. Specify connection settings under which to connect to the Veeam Backup for Microsoft Office 365 server and click **Connect**.



The image shows a dialog box titled "Veeam® Backup for Microsoft Office 365". It has a green header bar with a close button (X). The main area is white and contains the Veeam logo (a green square with a white cloud and server icon) and the text "Veeam® Backup for Microsoft Office 365". Below this, there is a prompt: "Type in a server name or IP address, service port number and user credentials to connect with." There are three input fields: the first contains "vbo365server", the second contains "9194", and the third contains "GAMMA\Administrator". Below these fields is a checkbox labeled "Use Windows session authentication" which is currently unchecked. At the bottom right, there are two buttons: "Connect" (highlighted with a blue border) and "Close".

Adding Veeam Backup for Microsoft Office 365 Service Provider

In Veeam Explorer for Microsoft OneDrive for Business, you can connect to a service provider server to add its backups to the application scope and perform a restore directly from such backups.


NOTE:

Make sure that both Veeam Explorer for Microsoft OneDrive for Business and Veeam Backup & Replication are installed on the same server and at least one service provider is added to Veeam Backup & Replication.

To add Veeam Backup for Microsoft Office 365 service providers, do the following:

1. On the toolbar, click **Add Store > Veeam Backup for Microsoft Office 365 Service Provider** or use the corresponding context menu command.
2. From the **Select service provider and authentication method** drop-down list, select a service provider that you want to add and choose an authentication method that can be either *Modern authentication* or *Basic authentication*.
4. [For *Modern authentication*] Select a region to which an Office 365 organization of the selected service provider belongs.
5. [For *Modern authentication*] Copy the device code and use it to sign in to Microsoft Azure Active Directory.

For *Basic authentication*, you must enter a user name and password to connect to the service provider server.
6. Select a point-in-time state as of which you want to load Office 365 backups.
To select a state, use the calendar control.
7. Select the **Show items that have been deleted by user** check box to see all the items that were removed.
8. Select the **Show all versions of items that have been modified by user** check box if you want to load modified versions.
9. Click **Connect**.



Veeam Backup

for Microsoft Office 365

Select service provider and authentication method:

office.tech.local (Tenant1)

Modern authentication

Select Office 365 organization region and sign in to Azure AD:

Default

To sign in, authenticate with the below code at:
<https://microsoft.com/devicelogin>

CGJF25HY5

Copy code

i Waiting for user logon...

Specify point in time you want to open:

☒ Use the latest available state

☐ Use the following point in time:

Wednesday, May 27, 2020 4:57:23 AM

☒ Show items that have been deleted by user

☒ Show all versions of items that have been modified by user

☐ Hide

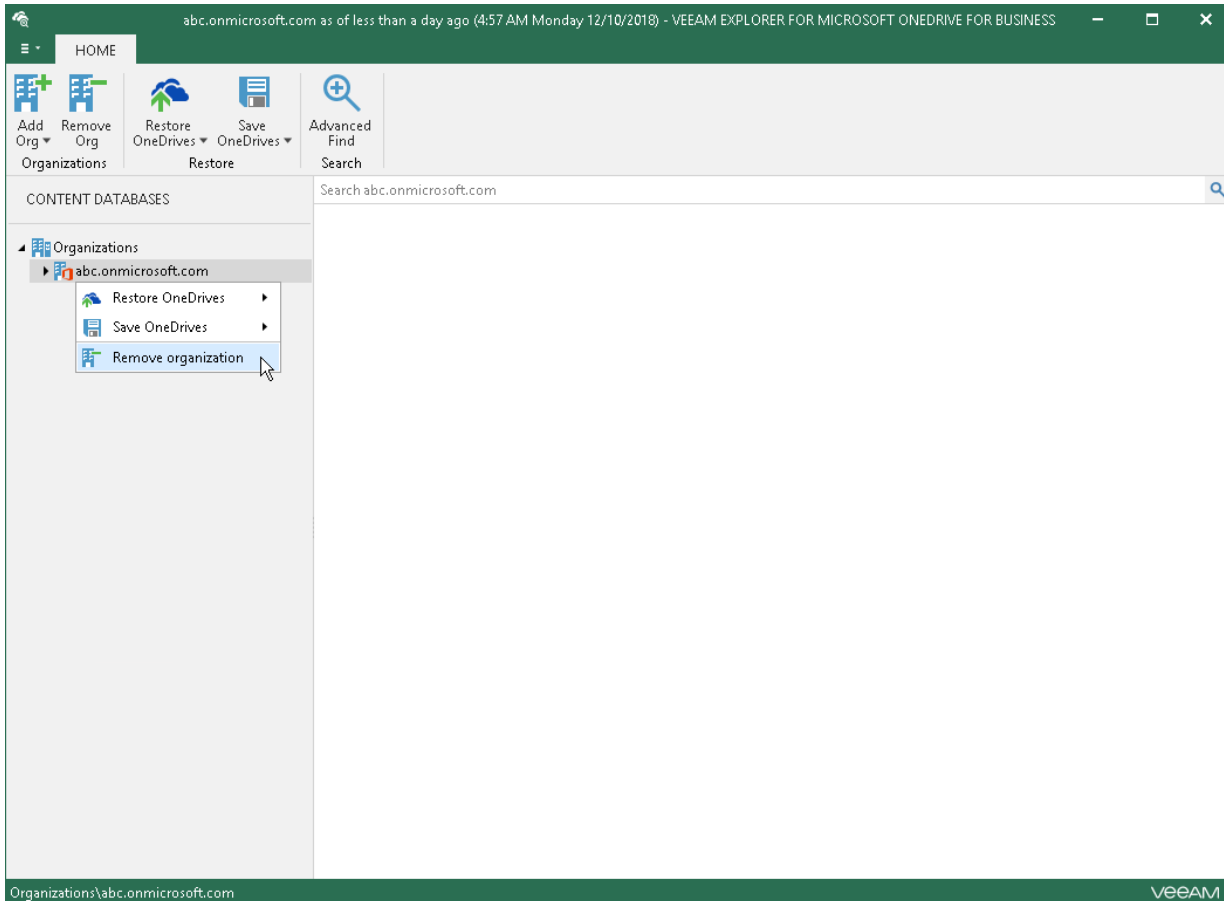
Connect

Close

Removing Standalone Databases

Veeam Explorer for Microsoft OneDrive for Business allows you to remove an organization from the application scope when you no longer need it.

To remove an organization from the application scope, right-click an organization in the navigation pane and select **Remove organization**.



Restore

This section explains how to restore data to [Microsoft Office 365](#) and [on-premises Microsoft](#) organizations.

IMPORTANT!

This section explains how to perform a restore in Veeam Explorer for Microsoft OneDrive for Business that comes as part of Veeam Backup for Microsoft Office 365 version 4c. For more information on how to restore data in Veeam Explorer for Microsoft OneDrive for Business that comes with Veeam Backup for Microsoft Office 365 version 4, see [this section](#) of the Veeam Explorers User Guide.

Restoring Single OneDrive

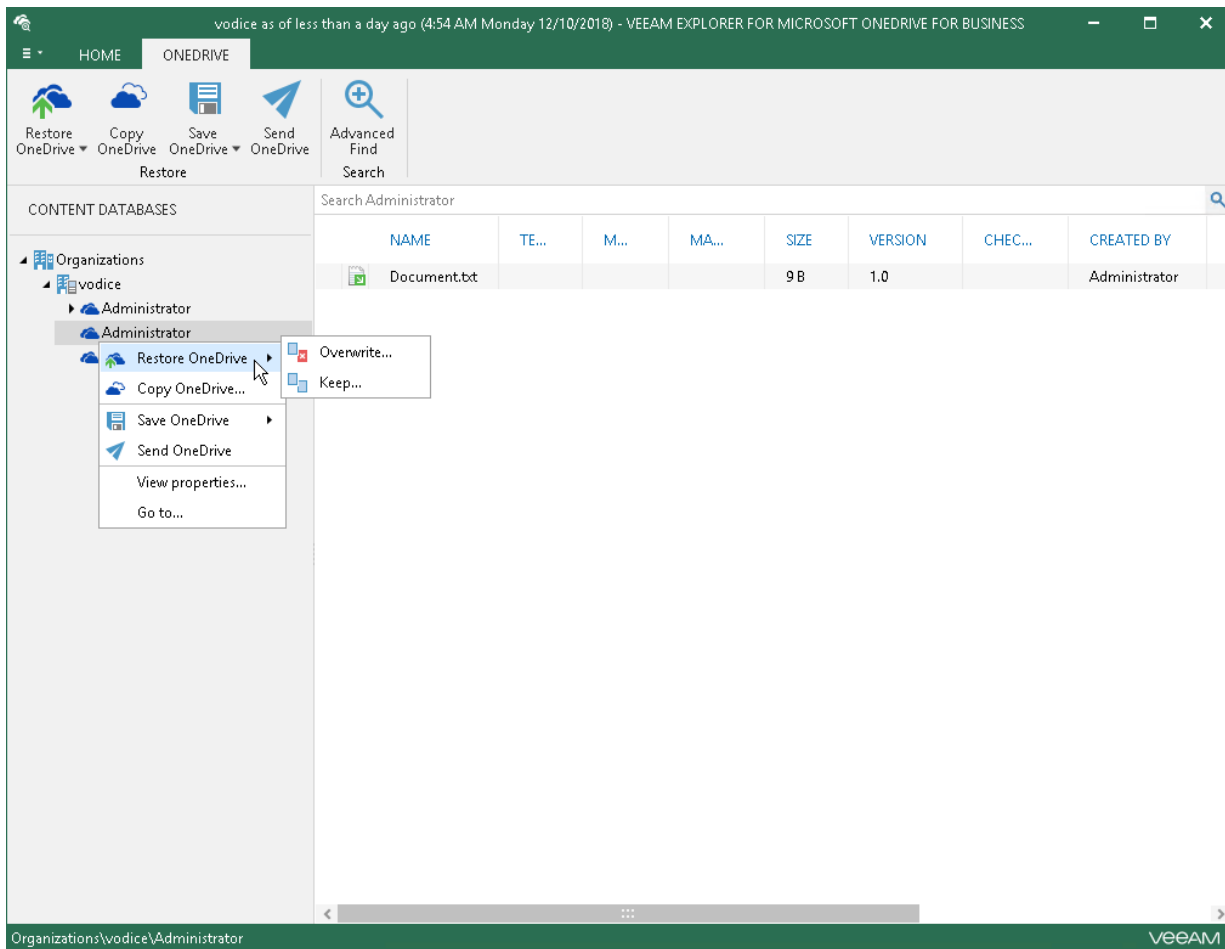
To restore a single OneDrive, do the following:

1. [Launch the Restore wizard.](#)
2. [Select an authentication method.](#)
3. [Log on to Office 365.](#)

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. In the navigation pane, select OneDrive or a folder, or in the preview pane, select a document.
2. On the **OneDrive/Folder/Document** tab, click **Restore OneDrive/Restore Folder/Restore Document** and select:
 - **Overwrite** – to completely overwrite existing OneDrive data.
 - **Keep** – to preserve existing data and recover items with the *RESTORED* prefix (*RESTORED-
<file_name>.ext*).



Step 2. Select Authentication Method

At this step of the wizard, choose whether you want to use modern or basic authentication.

Modern Authentication

To use modern authentication, do the following:

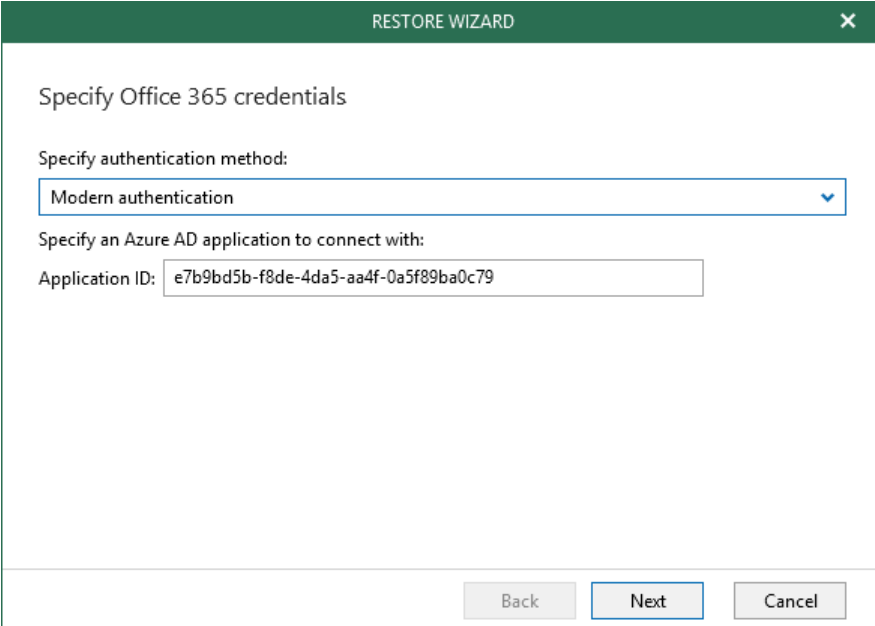
1. From the **Specify authentication method** drop-down list, select *Modern authentication*.

This will allow Veeam Backup for Microsoft Office 365 to use an Azure AD application for a restore. Such an application is used to restore the specified mailbox back to Office 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults.

For more information, see [Microsoft Office 365 Organizations](#).

2. In the **Application ID** field, enter an identification number of the Azure AD application that you want to use for a restore.

By default, Veeam Explorer for Microsoft Exchange populates this field with the identification number of the application that was used during a backup session. If you want to use another application, make sure to grant this application required permissions, as described in [Azure AD Applications](#).



RESTORE WIZARD

Specify Office 365 credentials

Specify authentication method:

Modern authentication

Specify an Azure AD application to connect with:

Application ID: e7b9bd5b-f8de-4da5-aa4f-0a5f89ba0c79

Back Next Cancel

Basic Authentication

To use basic authentication, do the following:

1. From the **Specify authentication method** drop-down list, select *Basic Authentication*.
2. Enter credentials to connect to the SharePoint organization.

RESTORE WIZARD

Specify Office 365 credentials

Specify authentication method:

Basic authentication

Specify user account to connect with:

Username: administrator@abc.onmicrosoft.com

Password: ●●●●●●●●

i To connect with an account enabled for multi-factor authentication (MFA), use an app password instead of a user password.

Back Next Cancel

On-Premises Organizations

To authenticate on an on-premises Microsoft SharePoint server, provide a user name and password.

RESTORE WIZARD

Specify target Microsoft SharePoint Server credentials

☐ Use current account (TECH\Administrator)

☒ Use the following account:

Username: tech\administrator

Password: ●●●●●●●●

Back Next Cancel

Step 3. Log on to Office 365

[This step is only available if you have selected the *Modern Authentication* option at the [previous step](#).]

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

To sign in to the Microsoft Office 265 organization, do the following:

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

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

2. Click the link to the Microsoft portal.
3. On the **Microsoft Azure device logon** page, paste the code that you have copied and sign in to Azure. Make sure to log in with the user account that has the *SharePoint Administrator* role.
4. Return to the **Restore Wizard** window and click **Restore**.



RESTORE WIZARD


Logon to Office 365

Provided account must have permissions to authenticate to the Office 365 organization.

To sign in, authenticate with the below code at:
<https://microsoft.com/devicelogin>

C2H5NTXJ7

  Copy code



You are authenticated to Office 365 as administrator@tech.club

Back

Restore

Cancel

Restoring Multiple OneDrives

To restore multiple OneDrives, do the following:

1. [Launch the Restore wizard.](#)
2. [Select an authentication method.](#)
3. [Log on to Office 365.](#)
4. [Select OneDrives.](#)

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. In the navigation pane, an organization name with OneDrives.
2. On the **Home** tab, click **Restore OneDrives** and select either of the following:
 - **Overwrite** — to completely overwrite existing OneDrives.
 - **Keep** — to preserve existing data and recover items with the *RESTORED* prefix (`RESTORED-<file_name>.ext`).

Step 2. Select Authentication Method

At this step of the wizard, choose whether you want to use modern or basic authentication.

Modern Authentication

To use modern authentication, do the following:

1. From the **Specify authentication method** drop-down list, select *Modern authentication*.

This will allow Veeam Backup for Microsoft Office 365 to use an Azure AD application for a restore. Such an application is used to restore the specified mailbox back to Office 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults.

For more information, see [Microsoft Office 365 Organizations](#).
2. In the **Application ID** field, enter an identification number of the Azure AD application that you want to use for a restore.

By default, Veeam Explorer for Microsoft Exchange populates this field with the identification number of the application that was used during a backup session. If you want to use another application, make sure to grant this application required permissions, as described in [Azure AD Applications](#).

RESTORE WIZARD

Specify Office 365 credentials

Specify authentication method:

Modern authentication

Specify an Azure AD application to connect with:

Application ID: e7b9bd5b-f8de-4da5-aa4f-0a5f89ba0c79

Back Next Cancel

Basic Authentication

To use basic authentication, do the following:

1. From the **Specify authentication method** drop-down list, select *Basic Authentication*.
2. Enter credentials to connect to the SharePoint organization.

RESTORE WIZARD

Specify Office 365 credentials


Specify authentication method:

Basic authentication

Specify user account to connect with:

Username: administrator@abc.onmicrosoft.com

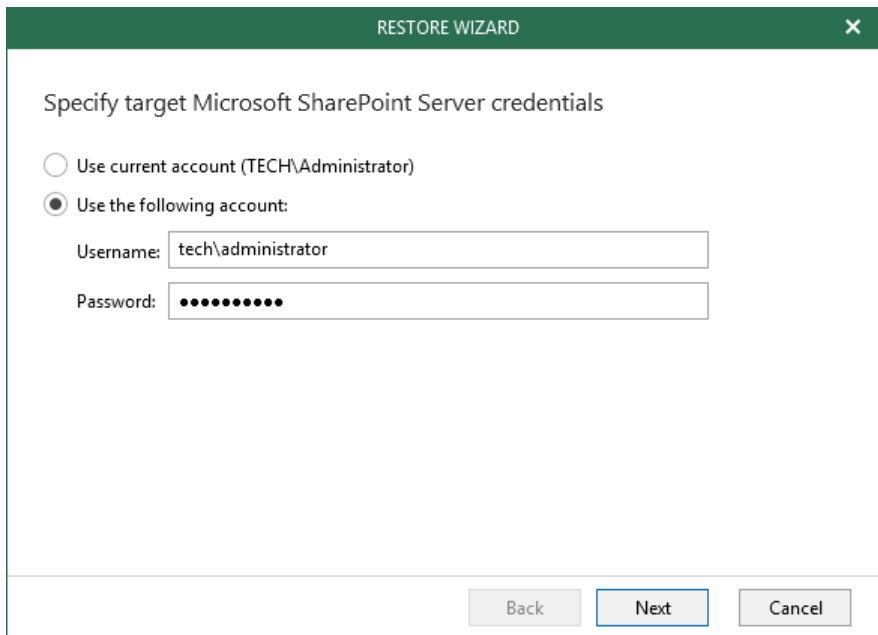
Password:

 To connect with an account enabled for multi-factor authentication (MFA), use an app password instead of a user password.

Back Next Cancel

On-Premises Organizations

To authenticate on an on-premises Microsoft SharePoint server, provide a user name and password.



RESTORE WIZARD

Specify target Microsoft SharePoint Server credentials

☐ Use current account (TECH\Administrator)

☒ Use the following account:

Username:

Password:

Back Next Cancel

Step 3. Log on to Office 365

[This step is only available if you have selected the *Modern Authentication* option at the [previous step](#).]

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

To sign in to the Microsoft Office 265 organization, do the following:

1. Click **Copy Code** to copy an authentication code.
Mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.
2. Click the link to the Microsoft portal.
3. On the **Microsoft Azure device logon** page, paste the code that you have copied and sign in to Azure.
Make sure to log in with the user account that has the *SharePoint Administrator* role.
4. Return to the **Restore Wizard** window and click **Restore**.



RESTORE WIZARD


Logon to Office 365

Provided account must have permissions to authenticate to the Office 365 organization.

To sign in, authenticate with the below code at:
<https://microsoft.com/devicelogin>

C2H5NTXJ7

  Copy code

 You are authenticated to Office 365 as administrator@tech.club

Back

Restore

Cancel



Step 4. Select OneDrives

At this step of the wizard, select OneDrives that you want to restore and click **Restore**.

If you want to check whether users the selected OneDrives belong to exist, click **Resolve selected accounts**.

RESTORE WIZARD

Select OneDrive accounts to restore

<input checked="" type="checkbox"/> ACCOUNT ↑	STATUS
<input checked="" type="checkbox"/> Administrator	 User found
<input checked="" type="checkbox"/> MFA360	 User found

2 accounts selected

[Resolve selected accounts](#)

Back

Restore

Cancel

Copy

This section explains how to copy OneDrive data to a different user.

IMPORTANT!

This section explains how to perform a copy in Veeam Explorer for Microsoft OneDrive for Business that comes as part of Veeam Backup for Microsoft Office 365 version 4c. For more information on how to copy data in Veeam Explorer for Microsoft OneDrive for Business that comes with Veeam Backup for Microsoft Office 365 version 4, see [this section](#) of the Veeam Explorers User Guide.

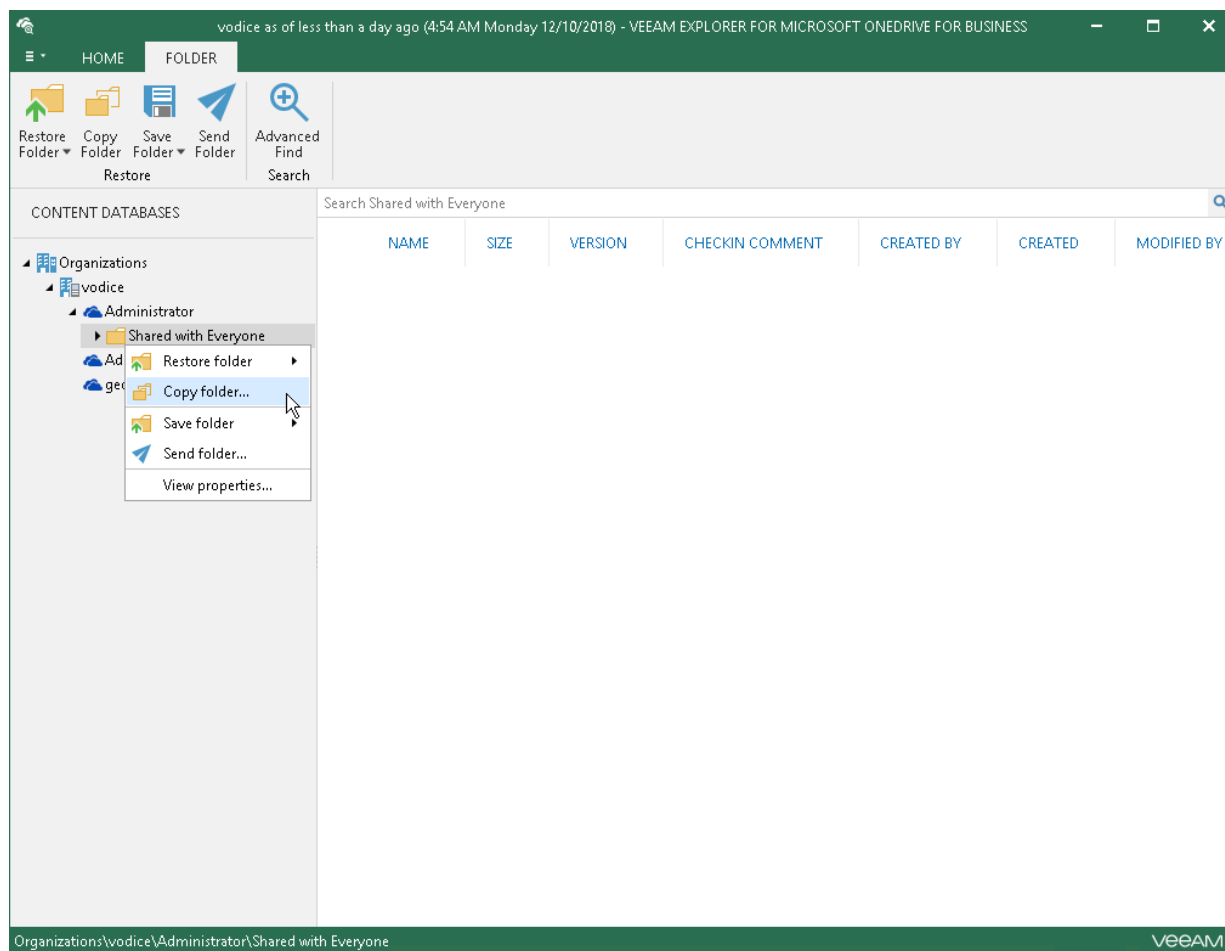
To copy OneDrive data to the same or different user, do the following:

1. [Launch the Restore wizard.](#)
2. [Select an authentication method.](#)
3. [Log on to Office 365.](#)
4. [Specify a target user.](#)
5. [Specify a target folder.](#)
6. [Specify restore options.](#)

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. Select an object.
2. On the **Folder** tab, select **Copy OneDrive/Copy Folder/Copy Document** or right-click an object and select **Copy OneDrive/Copy Folder/Copy Document**.



Step 2. Select Authentication Method

At this step of the wizard, choose whether you want to use modern or basic authentication.

Modern Authentication

To use modern authentication, do the following:

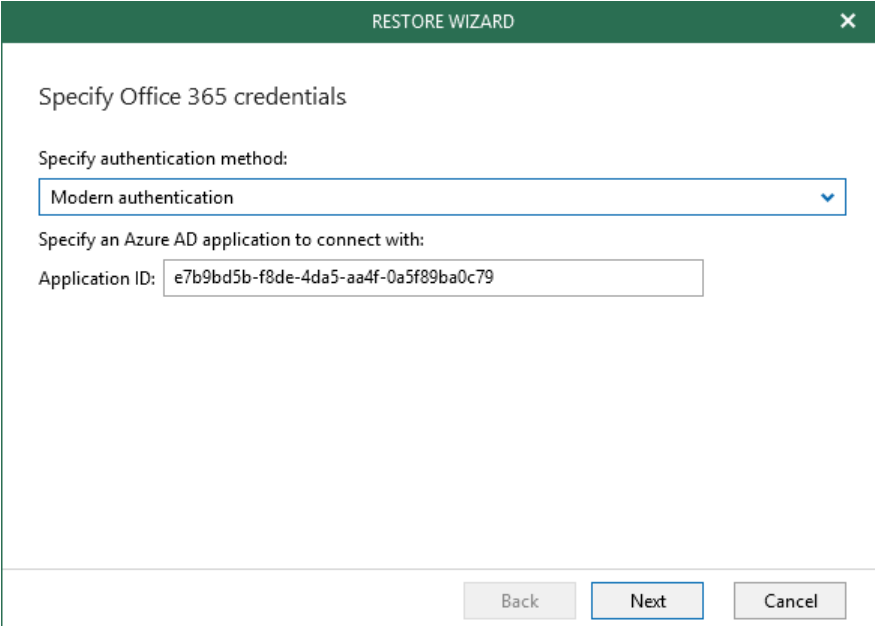
1. From the **Specify authentication method** drop-down list, select *Modern authentication*.

This will allow Veeam Backup for Microsoft Office 365 to use an Azure AD application for a restore. Such an application is used to restore the specified mailbox back to Office 365 organizations with enabled multi-factor authentication (MFA) and enabled or disabled security defaults.

For more information, see [Microsoft Office 365 Organizations](#).

2. In the **Application ID** field, enter an identification number of the Azure AD application that you want to use for a restore.

By default, Veeam Explorer for Microsoft Exchange populates this field with the identification number of the application that was used during a backup session. If you want to use another application, make sure to grant this application required permissions, as described in [Azure AD Applications](#).



RESTORE WIZARD

Specify Office 365 credentials

Specify authentication method:

Modern authentication

Specify an Azure AD application to connect with:

Application ID: e7b9bd5b-f8de-4da5-aa4f-0a5f89ba0c79

Back Next Cancel

Basic Authentication

To use basic authentication, do the following:

1. From the **Specify authentication method** drop-down list, select *Basic Authentication*.
2. Enter credentials to connect to the SharePoint organization.

RESTORE WIZARD

Specify Office 365 credentials

Specify authentication method:
Basic authentication

Specify user account to connect with:
Username: administrator@abc.onmicrosoft.com
Password:

To connect with an account enabled for multi-factor authentication (MFA), use an app password instead of a user password.

Back

Next

Cancel

On-Premises Organizations

To authenticate on an on-premises Microsoft SharePoint server, provide a user name and password.

RESTORE WIZARD

Specify target Microsoft SharePoint Server credentials

☐ Use current account (TECH\Administrator)

☒ Use the following account:
Username: tech\administrator
Password:

Back

Next

Cancel

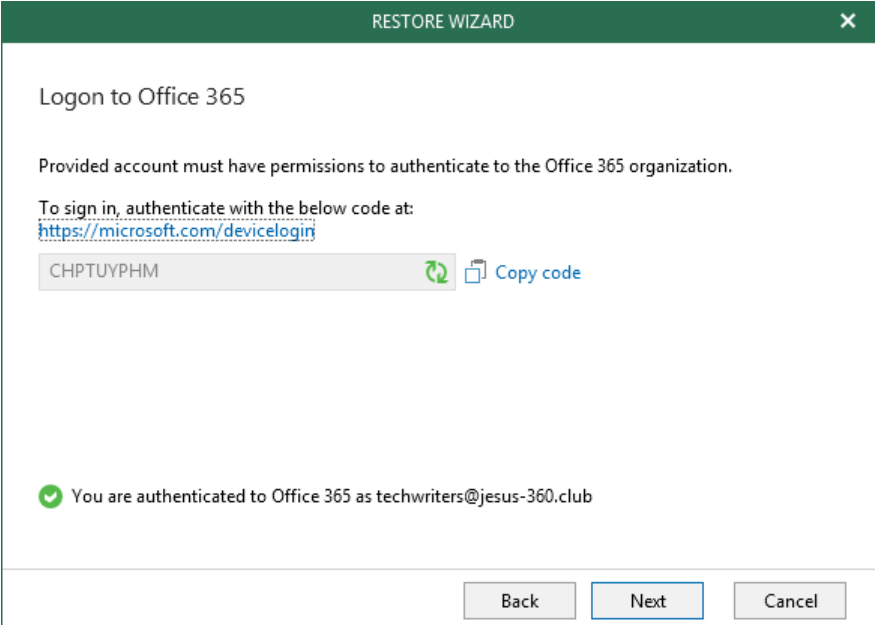
Step 3. Log on to Office 365

[This step is only available if you have selected the *Modern Authentication* option at the [previous step](#).]

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

To sign in to the Microsoft Office 265 organization, do the following:

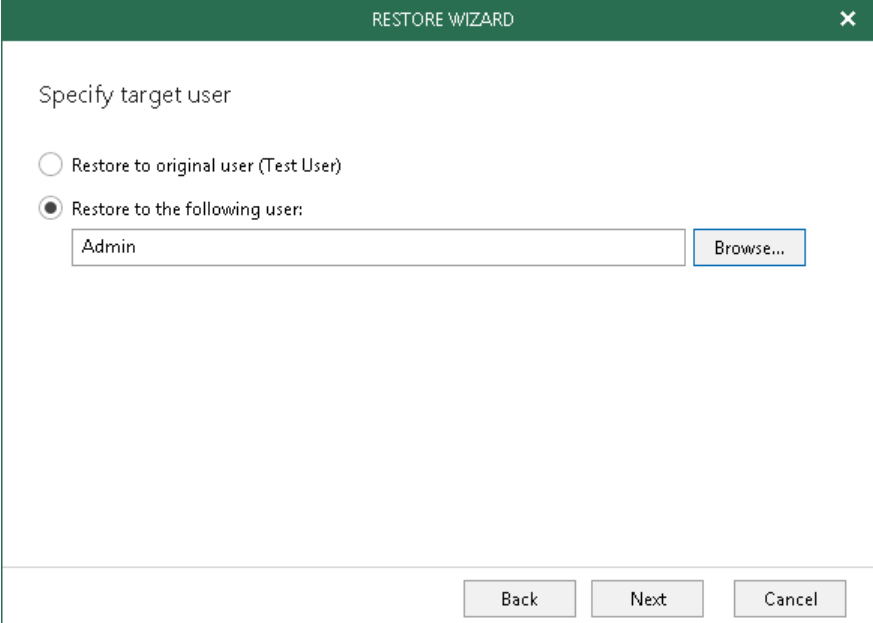
1. Click **Copy Code** to copy an authentication code.
Mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.
2. Click the link to the Microsoft portal.
3. On the **Microsoft Azure device logon** page, paste the code that you have copied and sign in to Azure.
Make sure to log in with the user account that has the *SharePoint Administrator* role.
4. Return to the **Restore Wizard** window and click **Next**.



The screenshot shows a window titled "RESTORE WIZARD" with a close button (X) in the top right corner. The main content area is titled "Logon to Office 365". Below the title, it states: "Provided account must have permissions to authenticate to the Office 365 organization." followed by "To sign in, authenticate with the below code at:" and a blue hyperlink: <https://microsoft.com/devicelogin>. Below the link is a text input field containing the code "CHPTUYPHM". To the right of the input field are two icons: a circular arrow (refresh) and a clipboard icon. Next to the clipboard icon is a blue link that says "Copy code". At the bottom of the main content area, there is a green checkmark icon followed by the text: "You are authenticated to Office 365 as techwriters@jesus-360.club". At the bottom of the window, there are three buttons: "Back", "Next" (which is highlighted with a blue border), and "Cancel".

Step 4. Specify Target User

At this step of the wizard, specify a target user where you want to copy data.



The screenshot shows a window titled "RESTORE WIZARD" with a close button (X) in the top right corner. The main area is titled "Specify target user". There are two radio button options: "Restore to original user (Test User)" and "Restore to the following user:". The second option is selected. Below it is a text input field containing the word "Admin" and a "Browse..." button to its right. At the bottom of the window are three buttons: "Back", "Next", and "Cancel".

RESTORE WIZARD

Specify target user

☐ Restore to original user (Test User)

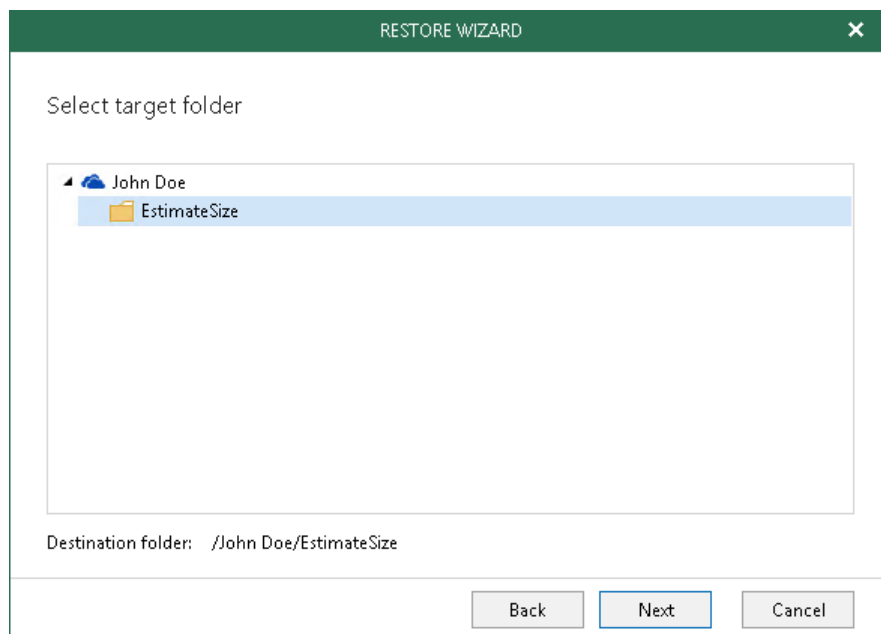
☒ Restore to the following user:

Admin [Browse...](#)

Back Next Cancel

Step 5. Specify Target Folder

At this step of the wizard, specify the target directory to which you want to copy data.



Step 6. Specify Restore Options

At this step of the wizard, specify restore options and click **Restore**.

The restore options are as follows:

- **Changed items.** Allows you to restore data that has been modified in your production environment.
- **Missed items.** Allows you to restore missed items.
- **Restore shared access.** Allows you to restore shared access.
- **History restore options.** Allows you to select a version:
 - **Overwrite.** To overwrite data in the production environment by recovering only the latest version of the document from the backup.
 - **Merge.** To merge an existing version of the document with that of a backup version.

If not selected, all the versions in the production environment will be replaced with the corresponding data from the backup file.

The screenshot shows a dialog box titled "RESTORE WIZARD" with a close button (X) in the top right corner. The main heading inside is "Specify the restore options".

There are three sections of options:

- Restore the following items:**
 - ☒ Changed items
 - ☒ Missing items
- Additional options:**
 - ☒ Restore shared access
 - ☒ Send a notification by e-mail to the users with permissions to the file
- History restore options:**
 - ☒ Restore only latest version
 - ☐ Overwrite
 - ☒ Merge

At the bottom of the dialog box, there are three buttons: "Back", "Restore" (which is highlighted with a blue border), and "Cancel".

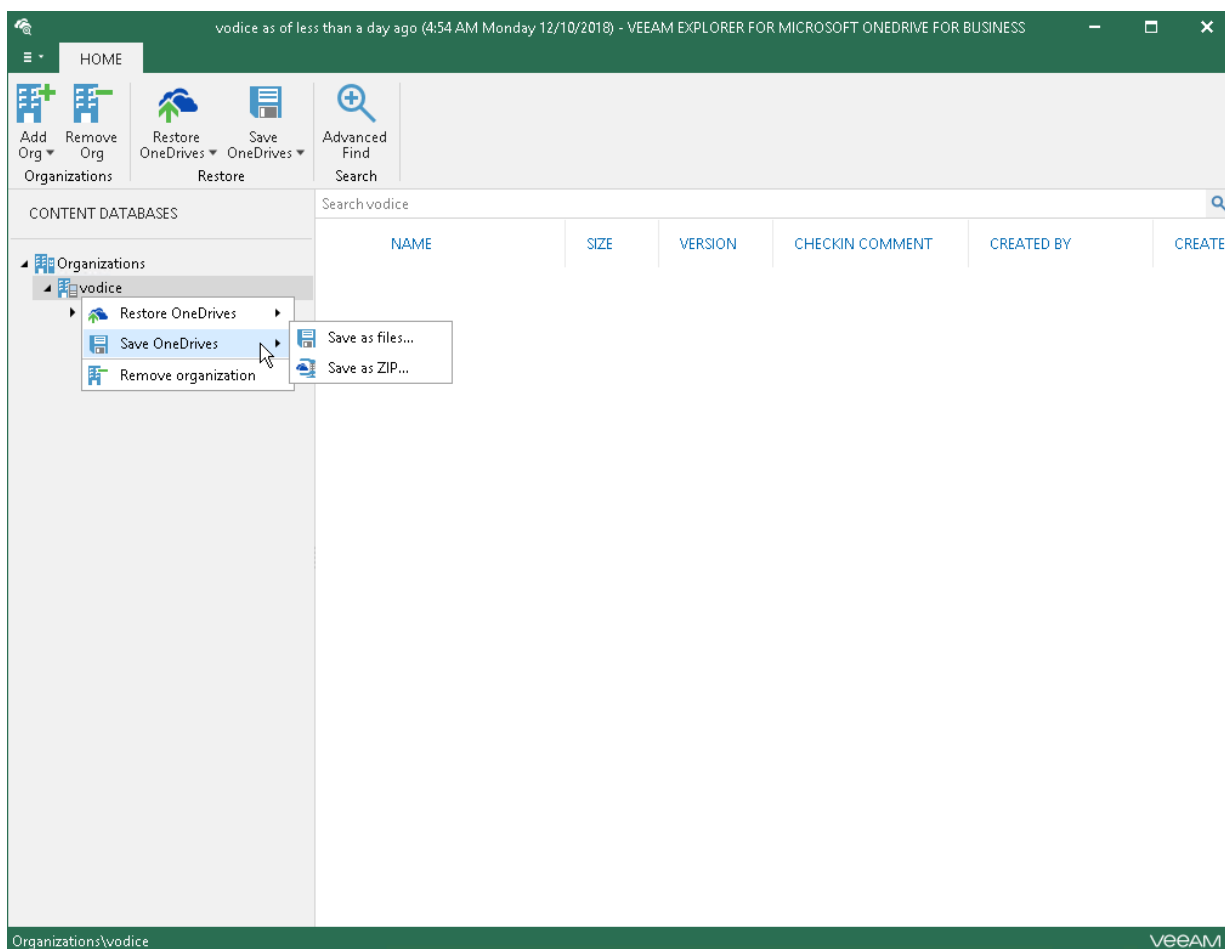
Saving Microsoft OneDrives

Veeam Explorer for Microsoft OneDrive for Business allows you to save OneDrive content to the specified location.

To save data, do the following:

1. Select OneDrive.
2. On the **Home** tab, select **Save OneDrives > Save files/Save OneDrive > Save files** or right-click an object and select **Save OneDrives > Save files/Save OneDrive > Save files**.

Select **Save as ZIP** to save OneDrive documents and/or folders as ZIP.



3. Select OneDrive accounts to save.

SAVE ONEDRIVES WIZARD

Select OneDrive accounts to save

<input type="checkbox"/> ACCOUNT ↑
<input checked="" type="checkbox"/> Arron Brown
<input checked="" type="checkbox"/> Corey Taylor
<input checked="" type="checkbox"/> David Low
<input type="checkbox"/> Don Peters
<input checked="" type="checkbox"/> Fred Eaglesmith
<input type="checkbox"/> Margaret Mitchel
<input checked="" type="checkbox"/> Michael Navarro
<input checked="" type="checkbox"/> Wes Doe

6 accounts selected

Back Next Cancel

4. Specify a directory to save OneDrive data and click **Finish**.

SAVE ONEDRIVES WIZARD

Specify destination path

Specify folder path:

C:\Users\Administrator\Desktop Browse...

Back Save Cancel

Saving Microsoft OneDrive Documents and Folders

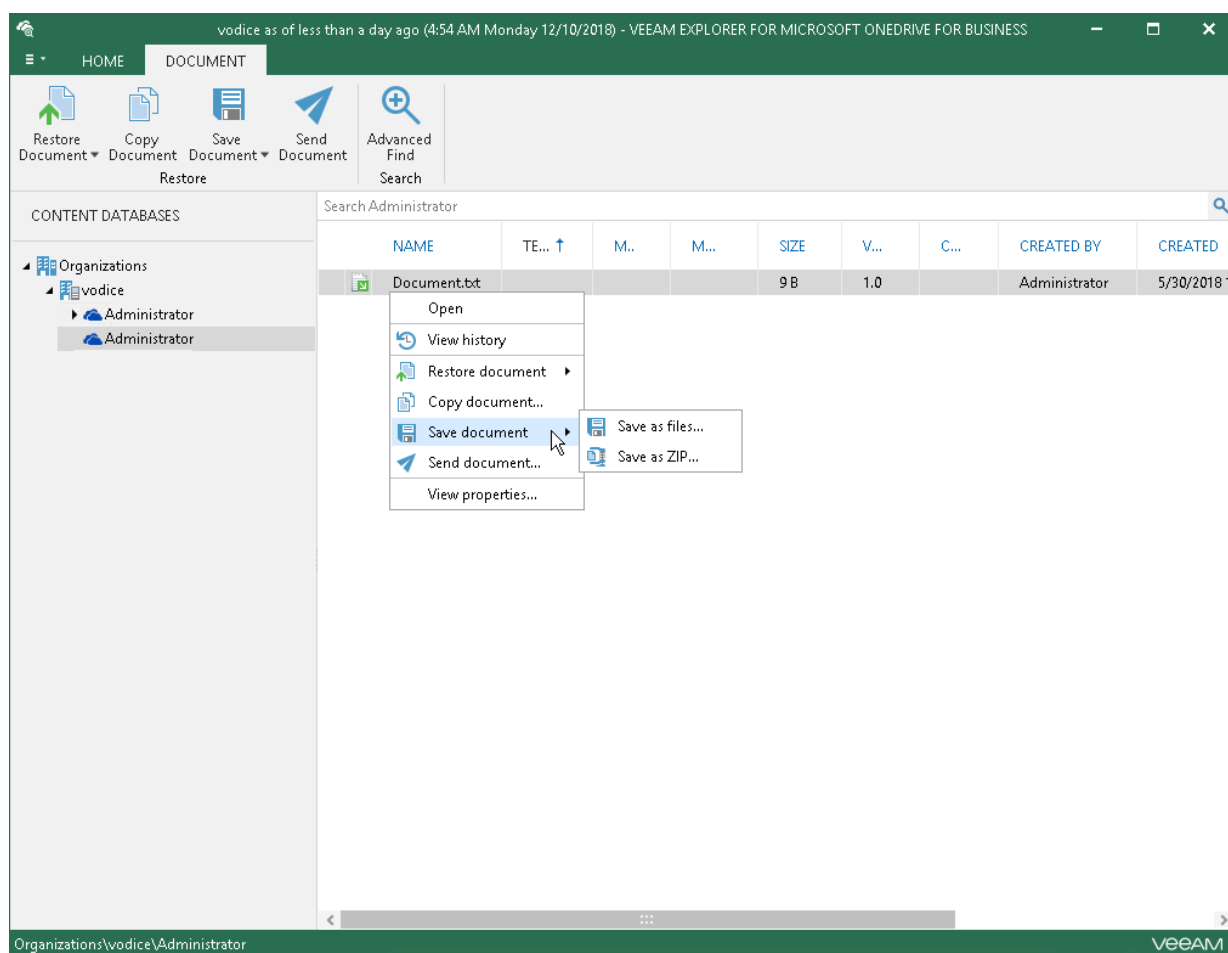
Veeam Explorer for Microsoft OneDrive for Business allows you to save your documents and folders located on users OneDrives to a specified location.

To save a document or folder, do the following:

1. Select a folder or document.
2. On the **Home** tab, select **Save Document > Save files/Save Folder > Save files** or right-click an object and select **Save Document > Save files/Save Folder > Save files**.

Select **Save as ZIP** to save OneDrive documents and/or folders as ZIP.

3. Specify the destination folder and click **Select Folder**.



Sending Microsoft OneDrive Documents

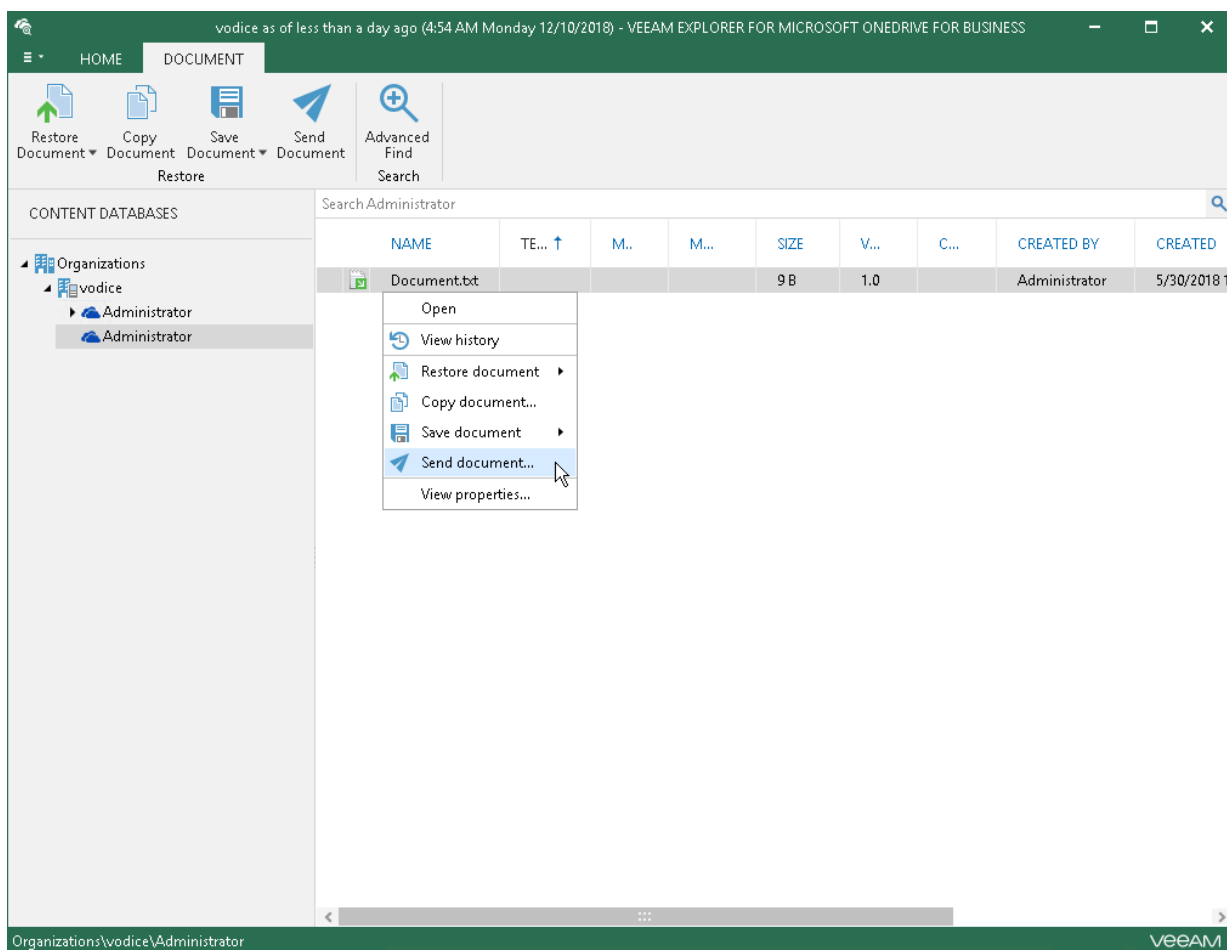
Veeam Explorer for Microsoft OneDrive for Business allows you to send OneDrive documents to specified recipients via email.

TIP:

Before sending documents, make sure to configure SMTP settings, as described in [Configuring SMTP Settings](#). The amount of data you can send at a time depends on your SMTP server configuration.

To send OneDrive documents via email, do the following:

1. Select OneDrive or a document.
2. On the **Document** tab, select **Send OneDrive/Send Document** or right-click an object and select **Send OneDrive/Send Document**.



3. Provide a recipient address.

The **From** field is filled automatically based on the address you have provided when configuring SMTP settings. To edit the message body, click **More Details**.

SEND ITEMS

Send

From:

Administrator@tech.local

To:

recipient@tech.local

Subject:

OneDrive Documents Recovery

Document.txt 9 B

^ Fewer details

by Veeam Explorer for Microsoft OneDrive for Business.