Veeam Backup for Microsoft Office 365

Version 5.0

User Guide

December, 2020

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

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

Customer Support

Should you have a technical concern, suggestion or question, visit the Veeam Customer Support Portal 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
- Veeam R&D Forums at forums.veeam.com

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 organizations, including Microsoft Exchange, Microsoft SharePoint, Microsoft OneDrive for Business and Microsoft Teams data, as well as data of on-premises Microsoft Exchange and on-premises Microsoft SharePoint organizations.

About This Document

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

The document applies to Veeam Backup for Microsoft Office 365 version 5.0 until it is replaced with a newer version of the product.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.

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	Comments
Microsoft SharePoint Server 2019, 2016	For more information about hardware and software requirements for Microsoft SharePoint Server 2019/2016, see: • 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	The following hardware is required: • *CPU*: any modern multi-core x64 processor, 4 cores minimum. • *Memory*: 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. • *Disk Space*: 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	Only 64-bit version of the following operating systems are supported: • 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

Specification	Requirement
Software	The following software is required: • Microsoft .NET Framework 4.7.2 or higher. • Windows C Runtime and Update (UCRT) in Windows. For more information, see this Microsoft article. • To use PowerShell cmdlets for backup and/or restore, Windows PowerShell 2.0 or higher is required. When using Windows 2012 or 2012 R2, 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), Veeam Explorer for Microsoft Teams 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 5.0 or the *Veeam Backup for Microsoft Office 365 Console* component. You can also use a machine with Veeam Backup & Replication 10 or later that is deployed either along with any of these components, or as an independent solution.

Backup Proxy Server

The following table lists system requirements for machines that you plan to use as backup proxy servers.

Specification	Requirement
Hardware	The following hardware is required: • *CPU*: any modern x64 processor, 4 cores minimum. • *Memory*: 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. • *Disk space*: 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.

Specification	Requirement
OS	Only 64-bit version of the following operating systems are supported: • 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 Proxy servers can be deployed to the following core editions: • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 LTSC, 1709 • Microsoft Windows Server 2012 R2
Other	The following components are required: • Microsoft .NET Framework 4.7.2 or higher. • Windows C Runtime and Update (UCRT) in Windows. For more information, see this Microsoft article. For a machine used as a workgroup backup proxy, the following settings are required: • The *Remote Registry* service must run on the target machine. The service startup type must be set to *Automatic*. • Windows Firewall must be turned off on the target machine.

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	443	Required to connect to Microsoft Exchange Online organizations.
	Microsoft SharePoint Online	TCP	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 or 443	Required to connect to on-premises Microsoft Exchange organizations.
	Backup Proxy Server	TCP	9193 (used by default)	Required to manage inbound/outbound traffic when interacting with the Veeam Backup for Microsoft Office 365 server. Make sure to open this port on a backup proxy server.
		TCP	445	This port is used to: • Install and manage the *Veeam.Archiver.Proxy* service on a target proxy machine. • Perform RPC requests.

From	To	Protocol	Port	Description
	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: *https://vbo.butler.veeam.com/json-rpc.php*
	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	Required to manage inbound/outbound traffic when interacting with the following components: • RESTful API • PowerShell • Veeam.Archiver.Shell (UI) • (optionally) A remote management server (if any) Make sure to open this port on a Veeam Backup for Microsoft Office 365 server.
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	Required to manage inbound/outbound traffic when interacting with: • Veeam Explorer for Microsoft Exchange • Veeam Explorer for Microsoft SharePoint Make sure to open this port on a Veeam Backup for Microsoft Office 365 server.

From	To	Protocol	Port	Description
Backup Proxy Server	**Veeam Backup for Microsoft Office 365 Server**	TCP	9191	Required to manage inbound/outbound traffic when interacting with backup proxy servers. Make sure to open this port on a Veeam Backup for Microsoft Office 365 server. You can also change this port, as described in Editing Backup Proxy Server.
	Microsoft Exchange Online	TCP	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 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. The table lists roles required by Veeam Backup for Microsoft Office 365 when you add organizations using modern authentication with legacy protocols allowed or basic authentication.

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 *ApplicationImpersonation* 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 *Default* user.

Granting ApplicationImpersonation Role in PowerShell

For On-Premises Microsoft Exchange Organizations

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

1. Connect to the Exchange server, 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
```

Microsoft SharePoint and OneDrive for Business

This section lists required permissions to work with Microsoft SharePoint and OneDrive for Business organizations. The section lists permissions required by Veeam Backup for Microsoft Office 365 when you add organizations using modern authentication with legacy protocols allowed or basic authentication.

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 *Farm Administrator* 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 Teams

To back up Microsoft Teams data, Veeam Backup for Microsoft Office 365 requires access to the Exchange mailbox of the group associated with a team and to the SharePoint site of this group. Thus, the account that you use to add an organization must have permissions required for backup of Exchange Online and SharePoint Online data. For more information, see Microsoft Exchange Organizations and Microsoft SharePoint and OneDrive for Business.

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

- The account must have a Microsoft Office 365 license that permits access to Microsoft Teams API. The minimum sufficient license is Microsoft Teams Exploratory experience.
- The account must have the *Team Service Administrator* role assigned.

> **NOTE:**
>
> In case you add an organization in Veeam Backup for Microsoft Office 365 using the modern authentication method with legacy protocols allowed, and specify different accounts to connect to Microsoft Exchange and Microsoft SharePoint, the required license and role must be assigned to the account used to connect to Microsoft SharePoint.

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.

Requirements for Modern App-Only Authentication

The following table lists permissions for Azure AD applications that are granted automatically by Veeam Backup for Microsoft Office 365 when you add organizations using the modern app-only authentication method.

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

API	Permission name	Type	Usage	Description
Microsoft Graph	Directory.Read.All	Application	Backup	Querying Azure AD for organization properties, the list of users and groups and their properties.
		Delegated[1]	Restore	Querying Azure AD for organization properties, the list of users and groups and their properties.
	Group.Read.All	Application	Backup	Querying Azure AD for the list of groups and group sites.
	Group.ReadWrite.All	Application[2]	Restore	Recreating in Azure AD an associated group in case of a deleted team site restore. This permission is only required for restore of SharePoint site data with Azure AD applications using a certificate. The operation is available through RESTful API and PowerShell.
	offline_access	Delegated[1]	Restore	Obtaining a refresh token from Azure AD.
	Sites.ReadWrite.All	Application	Backup	Querying Azure AD for the list of sites and getting download URLs for files and their versions.
Exchange	EWS.AccessAsUser.All	Delegated[1]	Restore	Accessing mailboxes as the signed-in user (impersonation) through EWS for the purpose of restore.

API	Permission name	Type	Usage	Description
	full_access_as_app	Application	Backup	Reading mailboxes content for the purpose of backup.
	full_access_as_user	Delegated[1]	Restore	Reading the current state and restoring mailboxes content. This permission is only required when you add an organization in the *Germany* region.
SharePoint	AllSitesFullControl	Delegated[1]	Restore	Reading the current state and restoring SharePoint sites and OneDrive accounts content.
	Sites.FullControl.All	Application	Backup	Reading sites and OneDrive accounts content for the purpose of backup.
		Application[2]	Restore	Reading the current state and restoring SharePoint sites and OneDrive accounts content.
	User.Read.All	Application	Backup	Reading OneDrive accounts for the purpose of backup (getting site IDs).
		Application[2]	Restore	Resolving OneDrive accounts for the purpose of restore (getting site IDs).
	User.ReadWrite.All	Delegated[1]	Restore	Resolving OneDrive accounts for the purpose of restore (getting site IDs).
Teams	TeamSettings.ReadWrite.All	Application	Backup	Resolving Microsoft Teams settings for the purpose of backup.
		Application[2]	Restore	Resolving Microsoft Teams settings for the purpose of restore.

[1] Permissions of the *Delegated* type are used for data restore using the device code flow.

[2] Permissions of the *Application* type are used for data restore using an application certificate.

The following table lists required permissions for Azure AD applications that you add as backup applications.

API	Permission name	Type	Usage	Description
Microsoft Graph	Sites.ReadWrite.All	Application	Backup	Getting download URLs for files and their versions.
SharePoint	Sites.FullControl.All			Reading site and OneDrive account content for the purpose of backup.
	User.Read.All			Reading OneDrive accounts for the purpose of backup (getting site IDs).

Required Azure AD Application Settings

For data restore using an Azure AD application, the following settings must be specified for the application in Microsoft Azure:

1. In the Azure AD application settings, the **Treat application as a public client** option must be set to **Yes**. For more information on application settings, see Microsoft Docs.

   Note that this option is not available in Microsoft Azure for the *Germany* region. In this region, you must register Azure AD applications used for backup and restore as applications of the *Public client/Native* type.

2. In the Azure AD application settings, a redirect URI must be specified for the application. For more information, see Microsoft Docs.

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

Required User Account Roles for Azure AD Applications

The account that the Azure AD application will use to log in to Microsoft Office 365 must be assigned the following roles:

- *Global Administrator* or *Exchange Administrator* — required for data restore with Veeam Explorer for Microsoft Exchange.
- *Global Administrator* or *SharePoint Administrator* — required for data restore with Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft OneDrive for Business.
- *Global Administrator* or *Teams Service Administrator* — required for data restore with Veeam Explorer for Microsoft Teams.
- *Global Administrator* — required for establishing a connection to a service provider in the Office 365 Backup as a Service scenario.

Requirements for Modern Authentication with Legacy Protocols Allowed

The following table lists required permissions that must be granted to Azure AD applications for backup operations for organizations with modern authentication and legacy protocols allowed.

API	Permission name	Type	Usage	Description
Microsoft Graph	Directory.Read.All	Application	Backup	Querying Azure AD for organization properties, the list of users and groups and their properties.
	Group.Read.All			Querying Azure AD for the list of groups and group sites.
Exchange	full_access_as_app			Reading mailbox content for the purpose of backup.
SharePoint	Sites.FullControl.All			Reading site and OneDrive account content for the purpose of backup.
	User.Read.All			Reading OneDrive accounts for the purpose of backup (getting site IDs).

Considerations and Limitations

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

- Infrastructure
- Backup Repositories
- Object Storage Repositories
- Backup
- Restore

> **NOTE:**
>
> For the complete list of known issues and limitations in Veeam Backup for Microsoft Office 365 5.0, see Release Notes.

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).
- [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 user 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.

- To back up user 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 does not back up the following Microsoft Teams objects:
  - Private channels
  - One-on-one chats
  - Audio and video calls
  - Video recordings
  - Contacts
  - Calendar: information about meetings and meeting chats
  - Code snippets in posts
  - Banner notifications in posts
  - Data of applications added as channel tabs that does not reside in the SharePoint document library of the channel.
- As part of Microsoft Teams data backup, Veeam Backup for Microsoft Office 365 backs up only the following types of channel tabs: Website, Planner, Word, Excel, PowerPoint, Visio, PDF, Document Library, OneNote, SharePoint, Stream, Forms, Power BI, Flow and Azure DevOps.

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.
- Bulk restore (restore of multiple objects) is not supported for public folder mailboxes. Use the regular per-object restore instead.
- Cross-tenant restore to Microsoft 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.
- Restore of OneNote notebooks from backups of Microsoft SharePoint and Microsoft Teams data for organizations with enabled security defaults using multi-factor authentication is not supported.

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 whose data you back up; each protected 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.

- **Microsoft OneDrive for Business account**

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

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

  Additionally, each user in your Office 365 subscription (or on-premises deployment) that has been granted access to team, communication, collaboration and other non-personal SharePoint sites that you plan to back up must be licensed. If you have a hybrid SharePoint deployment (on-premises Microsoft SharePoint and SharePoint Online), and the same user has access to both, then only one Veeam license is required.

- **Microsoft Teams teams**

  Each user in your Office 365 subscription that has been granted access to Microsoft Teams objects that you plan to back up must be licensed.

A license is consumed by objects (mailboxes, OneDrive for Business accounts, SharePoint personal sites) for which at least one restore point has been created within the last 31 days. If an object was not backed up for 31 days, its license is automatically revoked.

A license is not required for:

- **Shared, resource and group mailboxes**

  Shared and resource mailboxes do not consume units in the Veeam Backup for Microsoft Office 365 license only if Microsoft Office 365 licenses are not assigned to these users.

- **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.

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.

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, the product will operate in the *Community Edition* mode that allows you to process up to 10 user accounts, up to 1 TB of Microsoft SharePoint data and up to 10 teams in all organizations. *Community Edition* mode is not limited in time and does not have limitations in terms of program functionality.

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. To do this, 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.

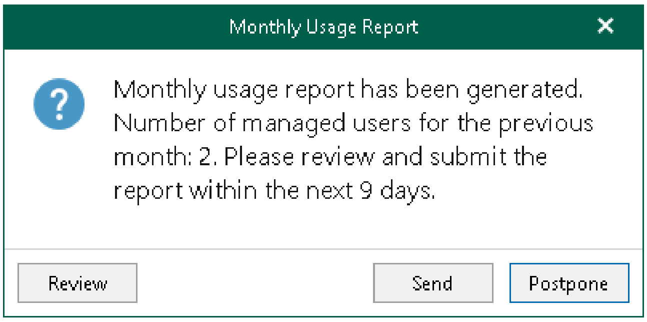
The grace period in this case is 2 months. After this period, processing of excessive user accounts (in FIFO queue) will be stopped; no more extra accounts will be queued for processing.

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.



Monthly usage report has been generated. Number of managed users for the previous month: 2. Please review and submit the report within the next 9 days.

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

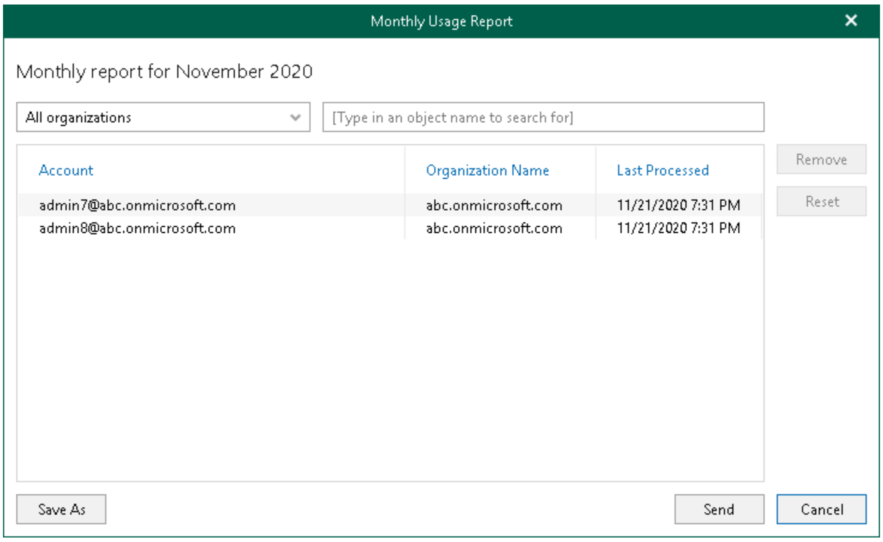
To review details of a report, in the **Monthly Usage Report** window, click **Review**.

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

In the **Monthly Usage Report** window, you can do the following 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 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 report for November 2020

Account	Organization Name	Last Processed
admin7@abc.onmicrosoft.com	abc.onmicrosoft.com	11/21/2020 7:31 PM
admin8@abc.onmicrosoft.com	abc.onmicrosoft.com	11/21/2020 7:31 PM

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 and Veeam Explorers.
- To use the solution in hybrid Exchange deployment or on-premises organizations with SPN and Kerberos authentication, make sure to install Veeam Backup for Microsoft 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 Veeam Explorer for Microsoft Exchange.
- `VeeamExplorerForSharePoint.msi` — installs Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft OneDrive for Business.

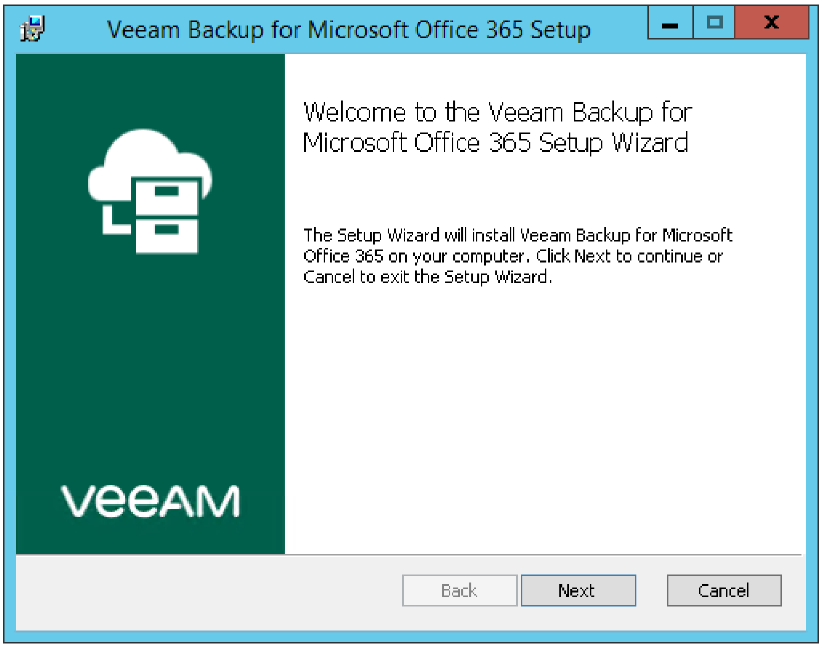
  For more information, see Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft OneDrive for Business.
- `VeeamExplorerForTeams.msi` — installs Veeam Explorer for Microsoft Teams.

  For more information, see Veeam Explorer for Microsoft Teams.

Installing Veeam Backup for Microsoft Office 365

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

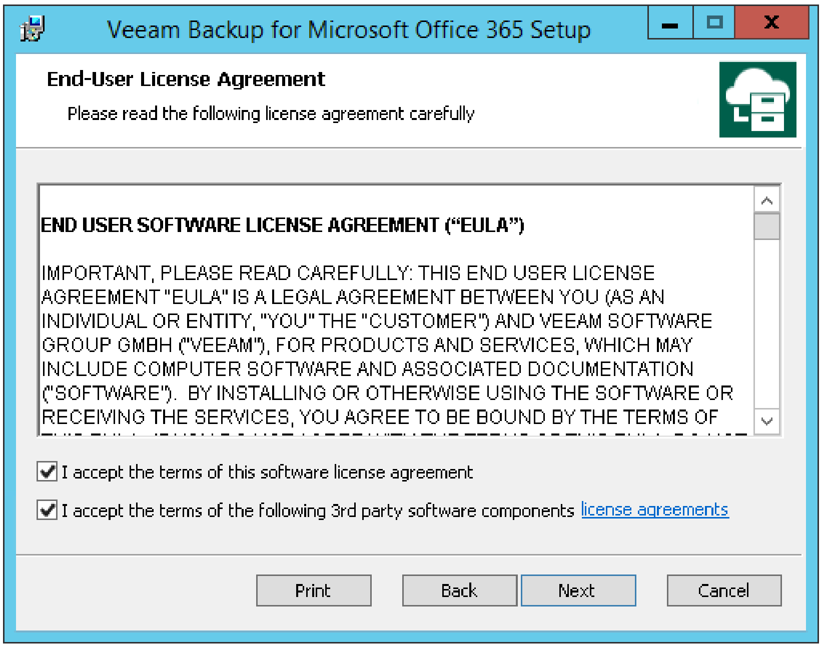
1. Run the `Veeam.Backup365.msi` file from the *Veeam Backup for Microsoft Office 365* distribution package.



Welcome to the Veeam Backup for Microsoft Office 365 Setup Wizard

The Setup Wizard will install Veeam Backup for Microsoft Office 365 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

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



End-User License Agreement

Please read the following license agreement carefully

END USER SOFTWARE LICENSE AGREEMENT (“EULA”)

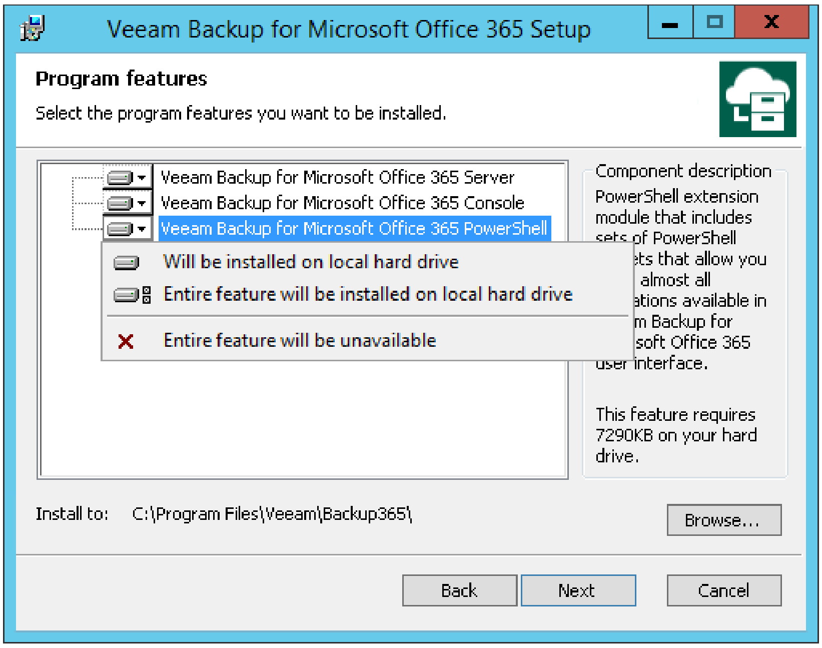
IMPORTANT, PLEASE READ CAREFULLY: THIS END USER LICENSE AGREEMENT "EULA" IS A LEGAL AGREEMENT BETWEEN YOU (AS AN INDIVIDUAL OR ENTITY, "YOU" THE "CUSTOMER") AND VEEAM SOFTWARE GROUP GMBH ("VEEAM"), FOR PRODUCTS AND SERVICES, WHICH MAY INCLUDE COMPUTER SOFTWARE AND ASSOCIATED DOCUMENTATION ("SOFTWARE"). BY INSTALLING OR OTHERWISE USING THE SOFTWARE OR RECEIVING THE SERVICES, YOU AGREE TO BE BOUND BY THE TERMS OF

☑ I accept the terms of this software license agreement

☑ I accept the terms of the following 3rd party software components license agreements

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.



Veeam Backup for Microsoft Office 365 Setup

Program features

Select the program features you want to be installed.

Veeam Backup for Microsoft Office 365 Server
Veeam Backup for Microsoft Office 365 Console
Veeam Backup for Microsoft Office 365 PowerShell
Will be installed on local hard drive
Entire feature will be installed on local hard drive
Entire feature will be unavailable

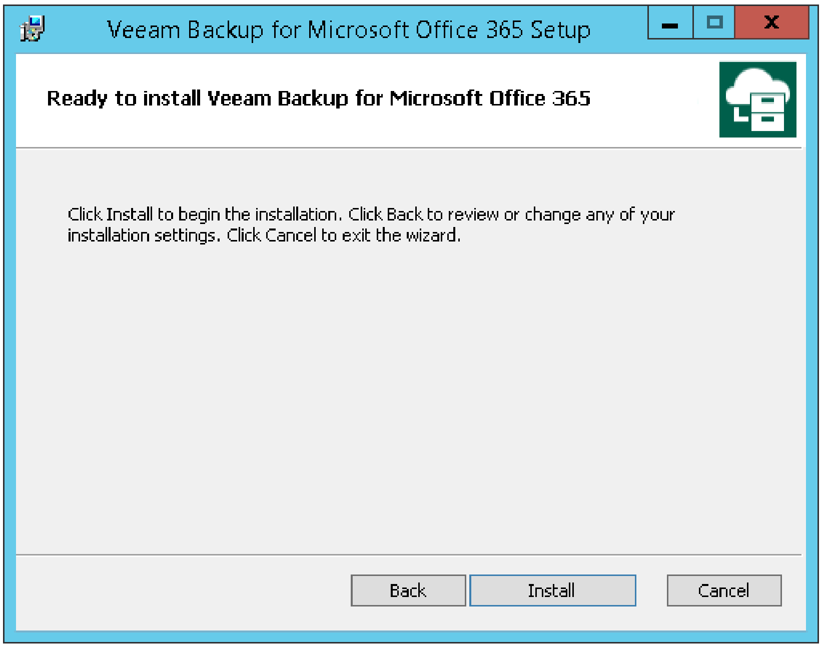
Component description

PowerShell extension module that includes sets of PowerShell ...ts that allow you ... almost all ...ations available in ...m Backup for ...soft Office 365 user interface.

This feature requires 7290KB on your hard drive.

Install to: C:\Program Files\Veeam\Backup365\

4. Click **Install**.



Veeam Backup for Microsoft Office 365 Setup

Ready to install Veeam Backup for Microsoft Office 365

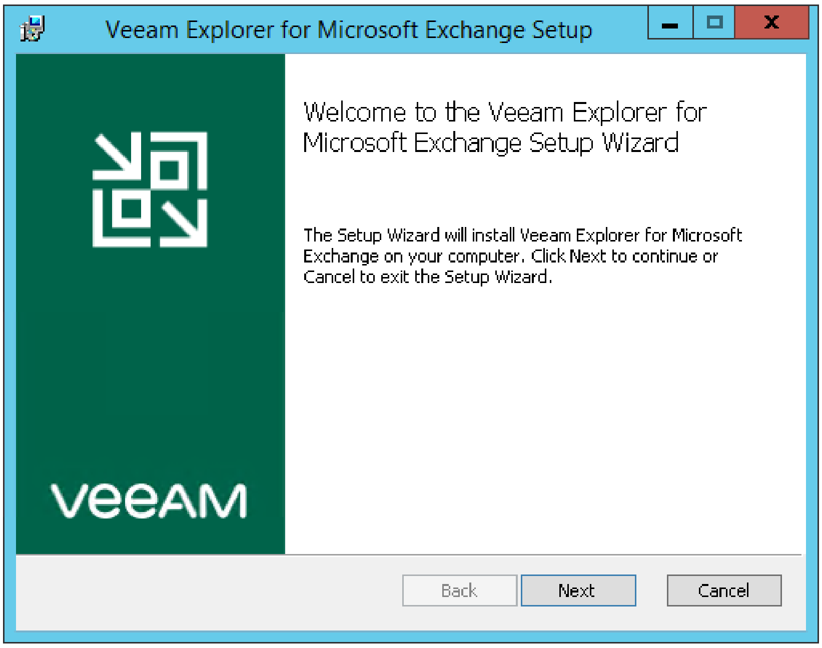
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

5. Click **Finish**.

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.

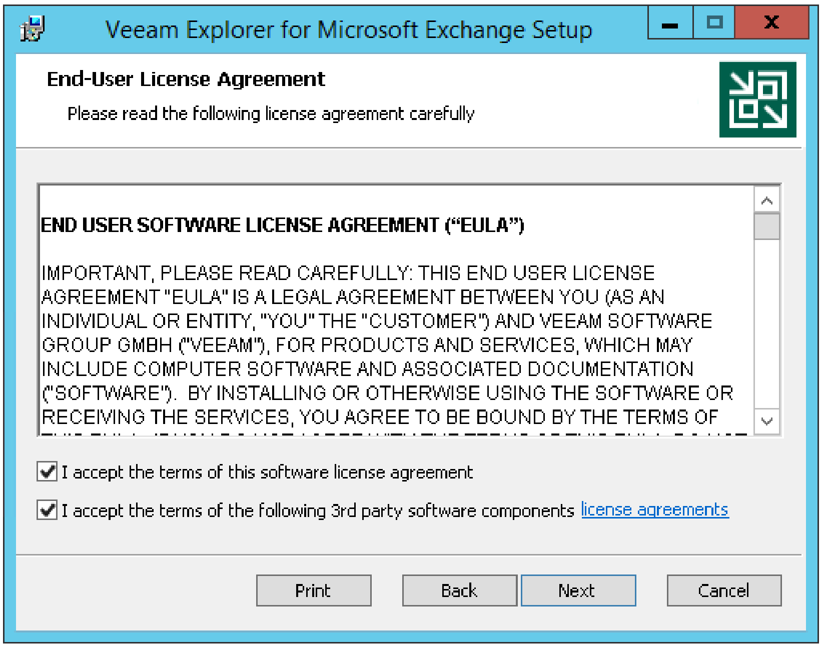


Veeam Explorer for Microsoft Exchange Setup

Welcome to the Veeam Explorer for Microsoft Exchange Setup Wizard

The Setup Wizard will install Veeam Explorer for Microsoft Exchange on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

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



Veeam Explorer for Microsoft Exchange Setup

End-User License Agreement

Please read the following license agreement carefully

END USER SOFTWARE LICENSE AGREEMENT (“EULA”)

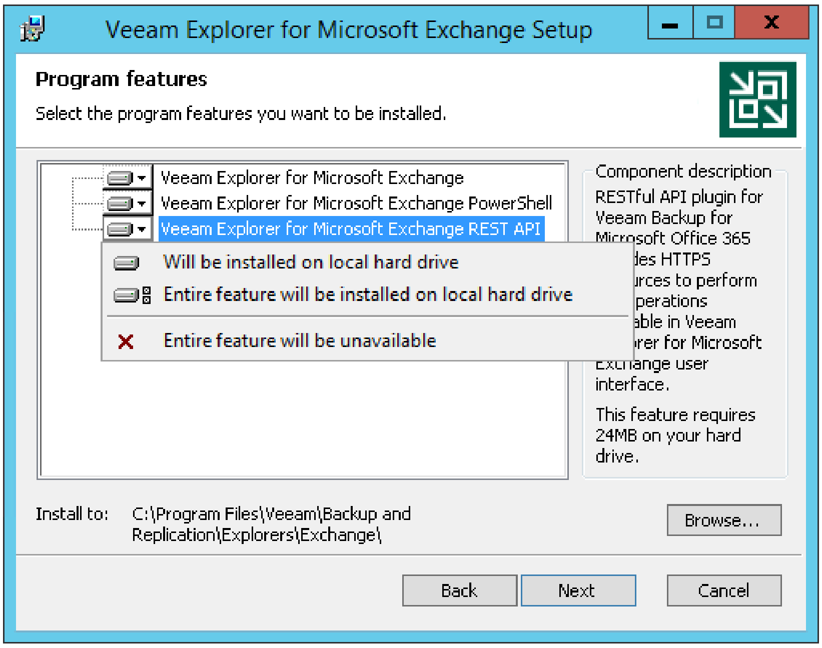
IMPORTANT, PLEASE READ CAREFULLY: THIS END USER LICENSE AGREEMENT "EULA" IS A LEGAL AGREEMENT BETWEEN YOU (AS AN INDIVIDUAL OR ENTITY, "YOU" THE "CUSTOMER") AND VEEAM SOFTWARE GROUP GMBH ("VEEAM"), FOR PRODUCTS AND SERVICES, WHICH MAY INCLUDE COMPUTER SOFTWARE AND ASSOCIATED DOCUMENTATION ("SOFTWARE"). BY INSTALLING OR OTHERWISE USING THE SOFTWARE OR RECEIVING THE SERVICES, YOU AGREE TO BE BOUND BY THE TERMS OF

☑ I accept the terms of this software license agreement

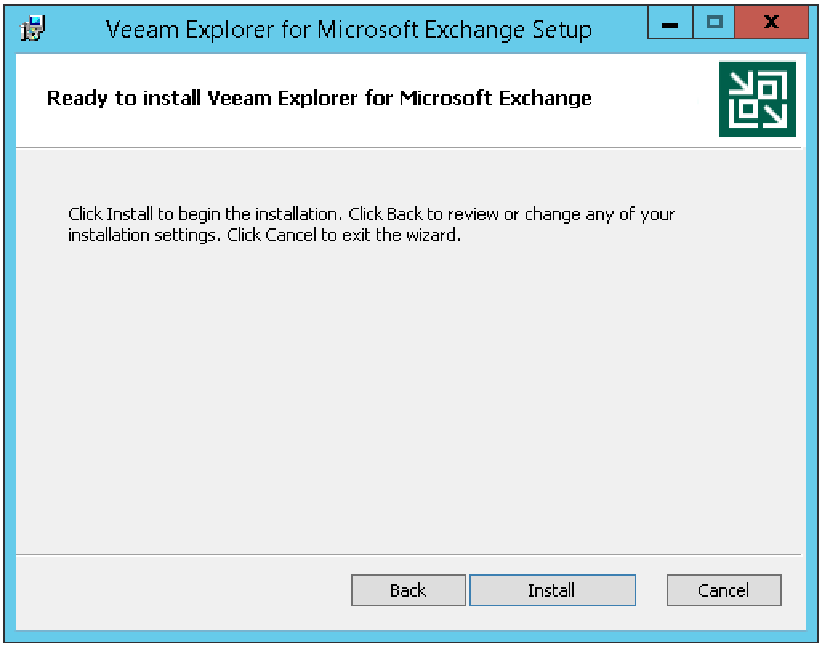
☑ I accept the terms of the following 3rd party software components license agreements

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.


Veeam Explorer for Microsoft Exchange Setup
Program features
Select the program features you want to be installed.
Veeam Explorer for Microsoft Exchange
Veeam Explorer for Microsoft Exchange PowerShell
Veeam Explorer for Microsoft Exchange REST API
Will be installed on local hard drive
Entire feature will be installed on local hard drive
Entire feature will be unavailable
Component description
RESTful API plugin for Veeam Backup for Microsoft Office 365 ...des HTTPS ...rces to perform ...perations ...able in Veeam ...rer for Microsoft Exchange user interface.
This feature requires 24MB on your hard drive.
Install to:
C:\Program Files\Veeam\Backup and Replication\Explorers\Exchange\
Browse...
Back
Next
Cancel

4. Click **Install**.


Veeam Explorer for Microsoft Exchange Setup
Ready to install Veeam Explorer for Microsoft Exchange
Back
Install
Cancel

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

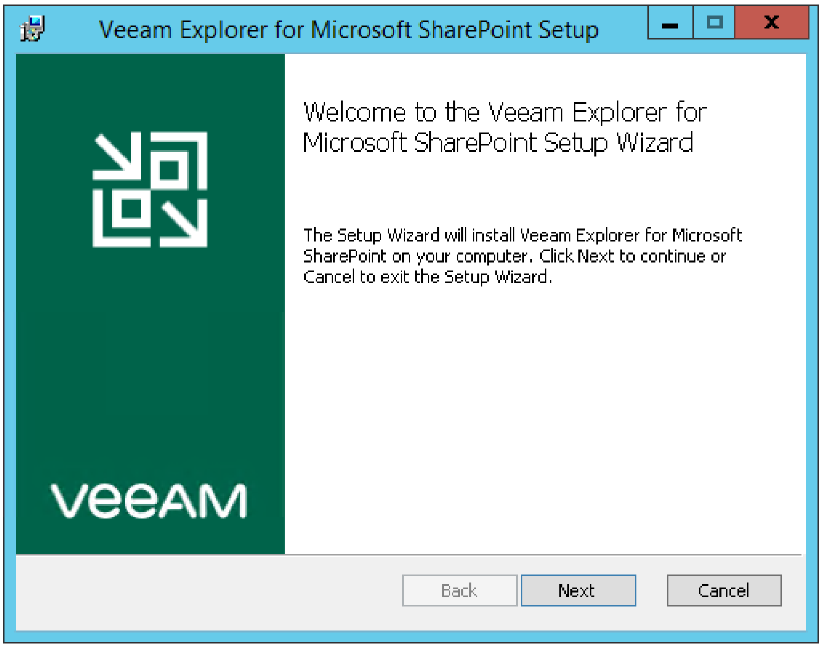
5. Click **Finish**.

Installing Veeam Explorer for Microsoft SharePoint

Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft OneDrive for Business are distributed in one package. When you install Veeam Explorer for Microsoft SharePoint, both Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft OneDrive for Business are installed on the machine.

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.

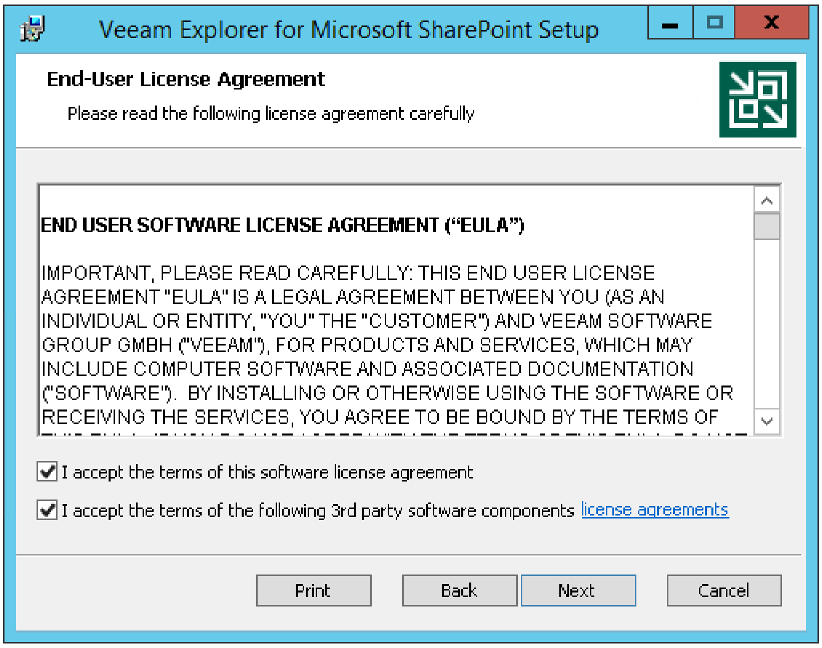


Veeam Explorer for Microsoft SharePoint Setup

Welcome to the Veeam Explorer for Microsoft SharePoint Setup Wizard

The Setup Wizard will install Veeam Explorer for Microsoft SharePoint on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

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



Veeam Explorer for Microsoft SharePoint Setup

End-User License Agreement

Please read the following license agreement carefully

END USER SOFTWARE LICENSE AGREEMENT (“EULA”)

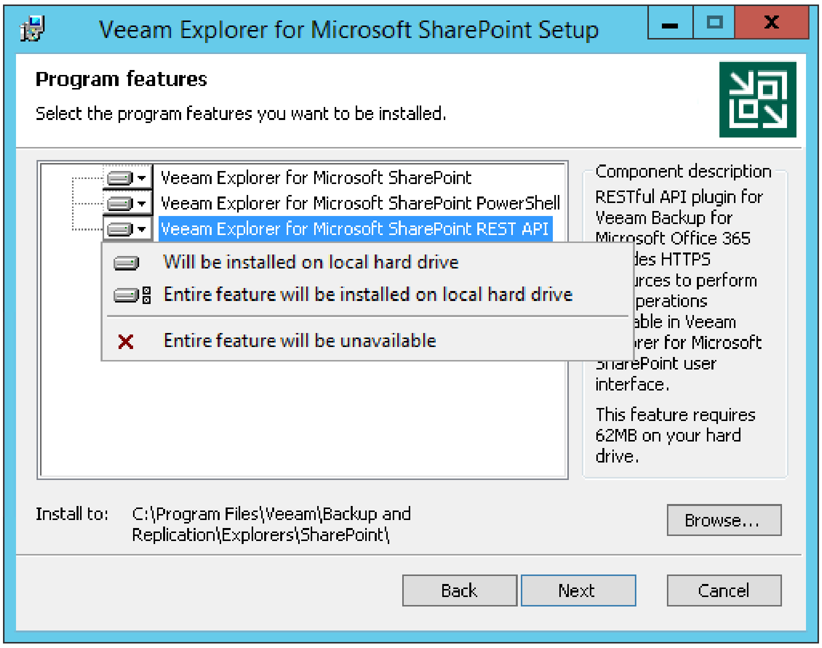
IMPORTANT, PLEASE READ CAREFULLY: THIS END USER LICENSE AGREEMENT "EULA" IS A LEGAL AGREEMENT BETWEEN YOU (AS AN INDIVIDUAL OR ENTITY, "YOU" THE "CUSTOMER") AND VEEAM SOFTWARE GROUP GMBH ("VEEAM"), FOR PRODUCTS AND SERVICES, WHICH MAY INCLUDE COMPUTER SOFTWARE AND ASSOCIATED DOCUMENTATION ("SOFTWARE"). BY INSTALLING OR OTHERWISE USING THE SOFTWARE OR RECEIVING THE SERVICES, YOU AGREE TO BE BOUND BY THE TERMS OF

☑ I accept the terms of this software license agreement

☑ I accept the terms of the following 3rd party software components license agreements

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.



Veeam Explorer for Microsoft SharePoint Setup

Program features

Select the program features you want to be installed.

- Veeam Explorer for Microsoft SharePoint
- Veeam Explorer for Microsoft SharePoint PowerShell
- Veeam Explorer for Microsoft SharePoint REST API

Will be installed on local hard drive
Entire feature will be installed on local hard drive
Entire feature will be unavailable

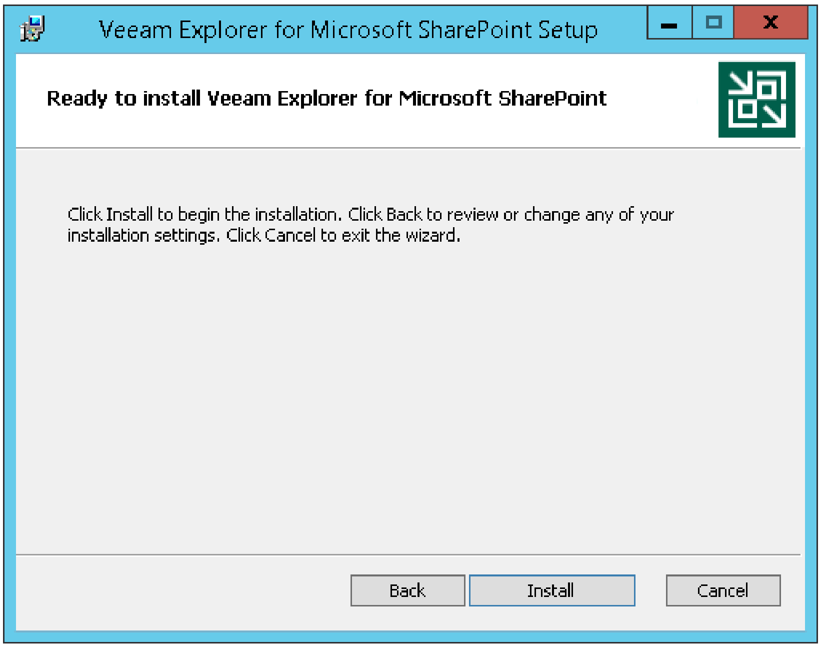
Component description

RESTful API plugin for Veeam Backup for Microsoft Office 365 ...des HTTPS ...rces to perform ...perations ...able in Veeam ...rer for Microsoft SharePoint user interface.

This feature requires 62MB on your hard drive.

Install to: C:\Program Files\Veeam\Backup and Replication\Explorers\SharePoint\

4. Click **Install**.



Veeam Explorer for Microsoft SharePoint Setup

Ready to install Veeam Explorer for Microsoft SharePoint

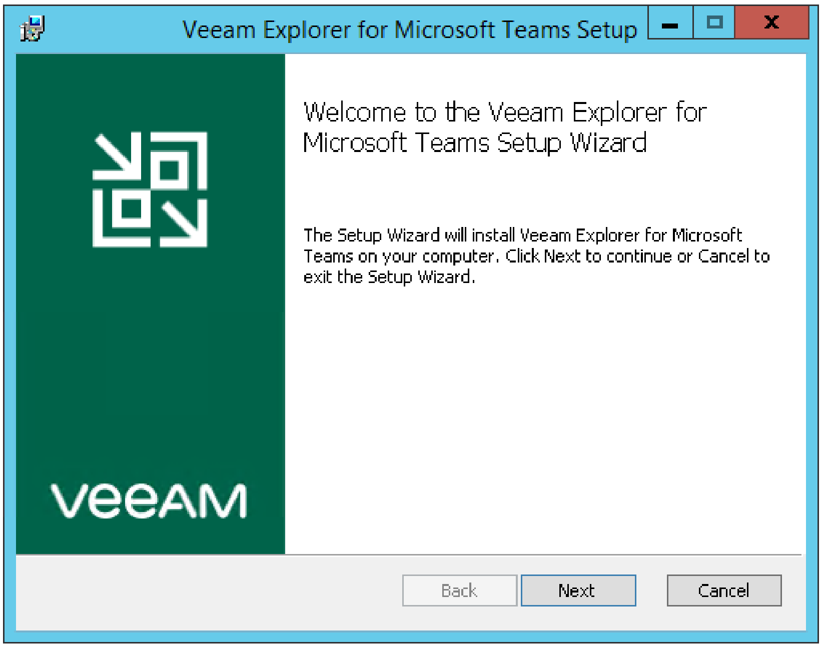
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

5. Click **Finish**.

Installing Veeam Explorer for Microsoft Teams

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

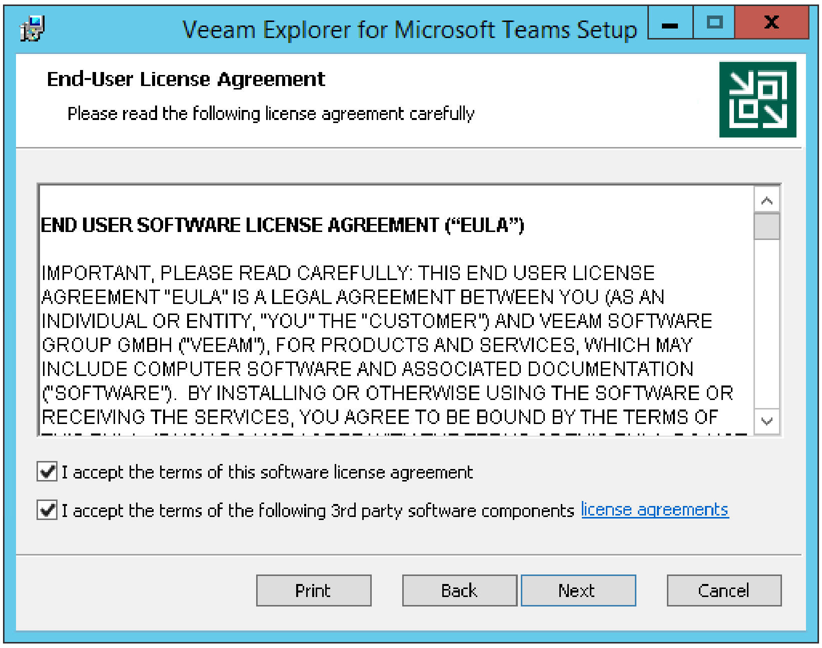
1. Run the `VeeamExplorerForTeams.msi` file from the *Veeam Backup for Microsoft Office 365* distribution package.



Welcome to the Veeam Explorer for Microsoft Teams Setup Wizard

The Setup Wizard will install Veeam Explorer for Microsoft Teams on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

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



End-User License Agreement

Please read the following license agreement carefully

END USER SOFTWARE LICENSE AGREEMENT (“EULA”)

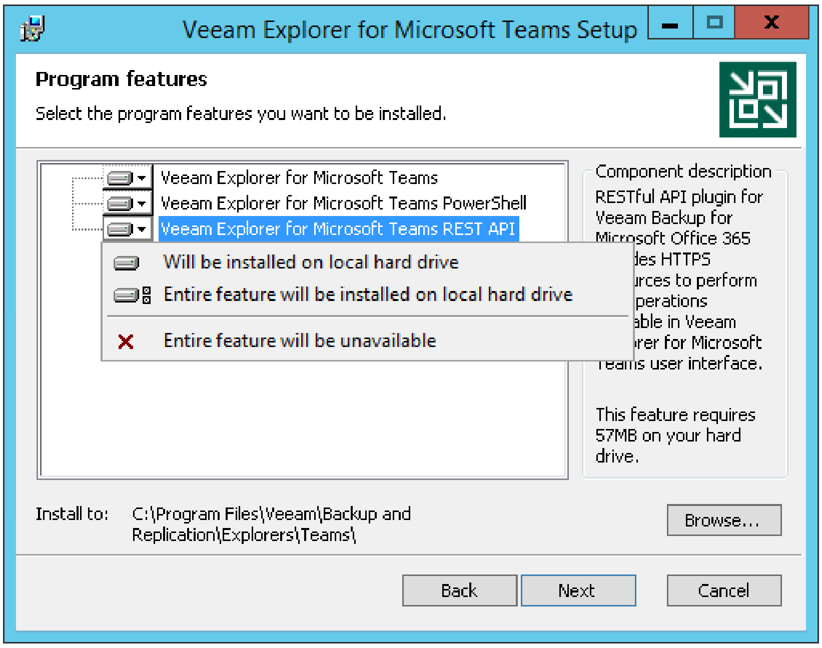
IMPORTANT, PLEASE READ CAREFULLY: THIS END USER LICENSE AGREEMENT "EULA" IS A LEGAL AGREEMENT BETWEEN YOU (AS AN INDIVIDUAL OR ENTITY, "YOU" THE "CUSTOMER") AND VEEAM SOFTWARE GROUP GMBH ("VEEAM"), FOR PRODUCTS AND SERVICES, WHICH MAY INCLUDE COMPUTER SOFTWARE AND ASSOCIATED DOCUMENTATION ("SOFTWARE"). BY INSTALLING OR OTHERWISE USING THE SOFTWARE OR RECEIVING THE SERVICES, YOU AGREE TO BE BOUND BY THE TERMS OF

☑ I accept the terms of this software license agreement

☑ I accept the terms of the following 3rd party software components license agreements

3. Select system components to install.

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



Veeam Explorer for Microsoft Teams Setup

Program features

Select the program features you want to be installed.

- Veeam Explorer for Microsoft Teams
- Veeam Explorer for Microsoft Teams PowerShell
- Veeam Explorer for Microsoft Teams REST API

Will be installed on local hard drive
Entire feature will be installed on local hard drive
Entire feature will be unavailable

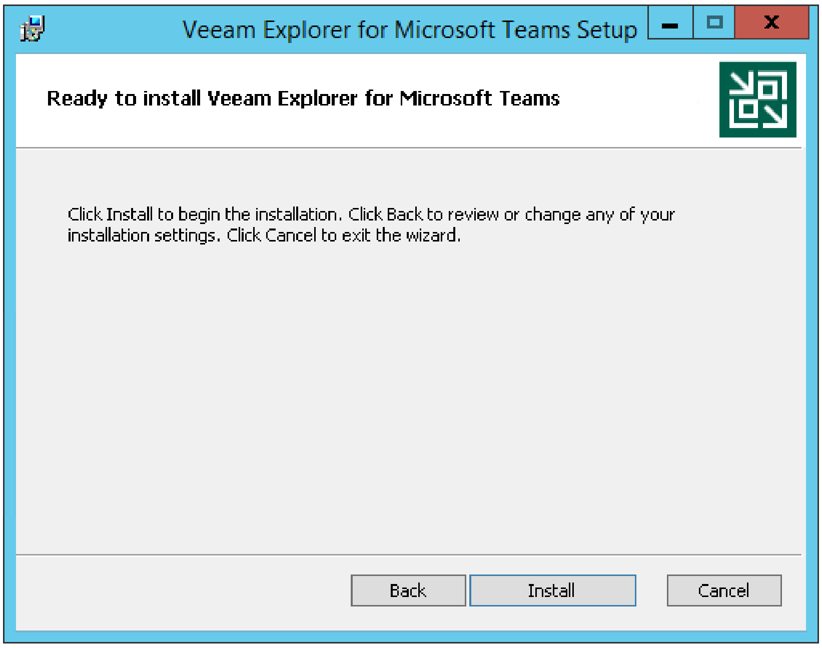
Component description

RESTful API plugin for Veeam Backup for Microsoft Office 365 ...des HTTPS ...rces to perform ...perations ...able in Veeam ...rer for Microsoft Teams user interface.

This feature requires 57MB on your hard drive.

Install to: C:\Program Files\Veeam\Backup and Replication\Explorers\Teams\

4. Click **Install**.



Veeam Explorer for Microsoft Teams Setup

Ready to install Veeam Explorer for Microsoft Teams

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

5. Click **Finish**.

Installing in Unattended Mode

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

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

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

The following table lists components and feature names for *Veeam Backup for Microsoft 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
REST API	REST_EXCHANGEEXPLORER

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

> **NOTE:**
>
> Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft OneDrive for Business are distributed in a single package.

Component	Feature name
UI	BR_SHAREPOINTEXPLORER
PowerShell	PS_SHAREPOINTEXPLORER

Component	Feature name
REST API	REST_SHAREPOINTEXPLORER

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

Component	Feature name
UI	BR_TEAMSEXPLORER
PowerShell	PS_TEAMSEXPLORER
REST API	REST_TEAMSEXPLORER

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*, *PowerShell* and *REST API* components.

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

To install the *Veeam Explorer for Microsoft SharePoint*, *UI*, *PowerShell* and *REST API* components.

```
msiexec /i VeeamExplorerForSharePoint.msi /qn ADDLOCAL=BR_SHAREPOINTEXPLORER,PS_SHAREPOINTEXPLORER,REST_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.

To install the *Veeam Explorer for Microsoft Teams*, *UI*, *PowerShell* and *REST API* components.

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

Deploying to Azure and AWS

Veeam Backup for Microsoft Office 365 can be deployed to Microsoft 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.

   For more information on how to deploy a backup proxy server to AWS, see this Veeam KB article.

3. Configure backup repositories, as described in Configuring Backup Repositories.

4. Install Veeam Explorer for Microsoft Exchange, Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft Teams, as described in Installing Veeam Explorer for Microsoft Exchange, Installing Veeam Explorer for Microsoft SharePoint and Installing Veeam Explorer for Microsoft Teams.

After deployment is complete, you can:

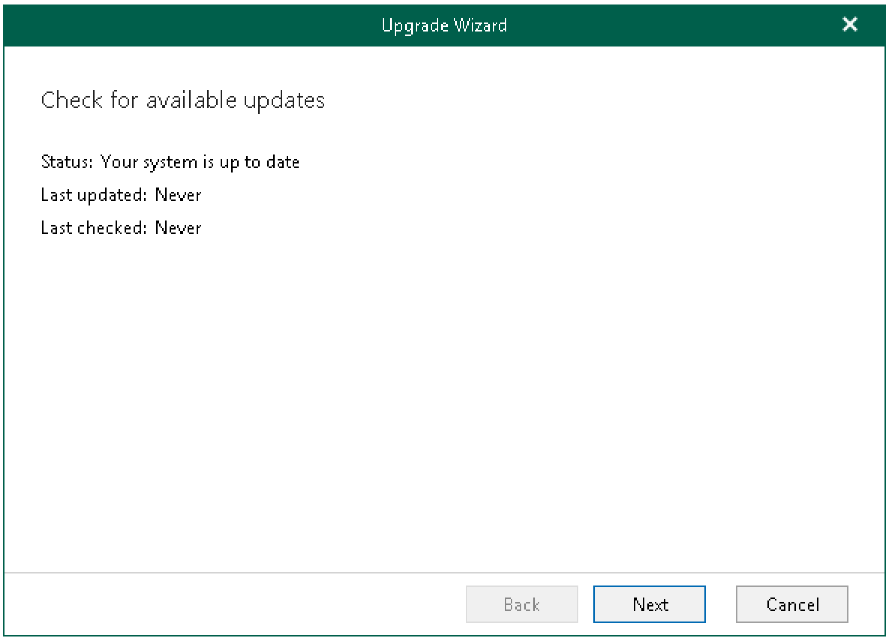
- Add Microsoft Office 365 and on-premises Microsoft organizations to the program scope, as described in Microsoft Organizations Management.
- Create new backups, as described in Data Backup.
- View and restore your data, as described in Data Restore.

Checking for Updates

To perform 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.



Check for available updates

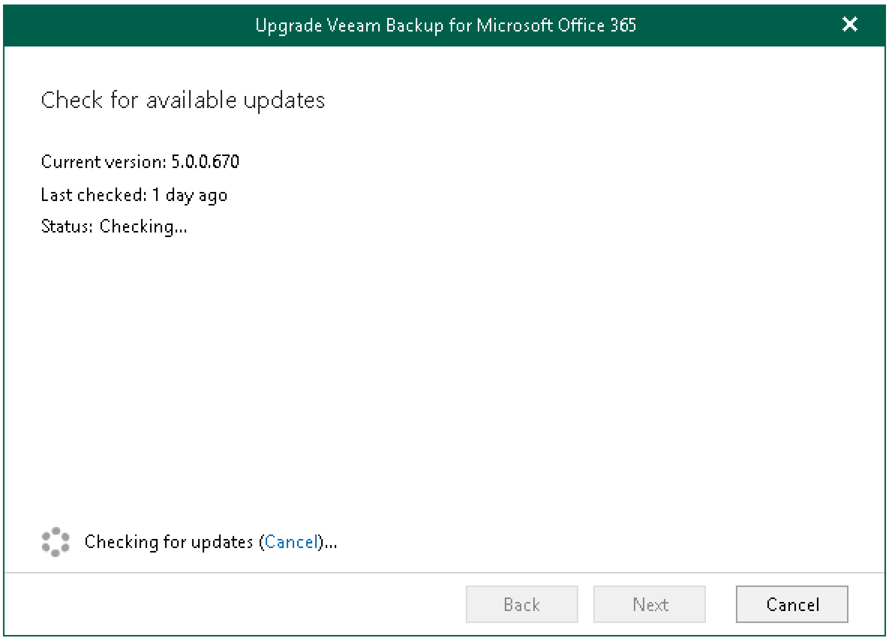
Status: Your system is up to date

Last updated: Never

Last checked: Never

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

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



Check for available updates

Current version: 5.0.0.670

Last checked: 1 day ago

Status: Checking...

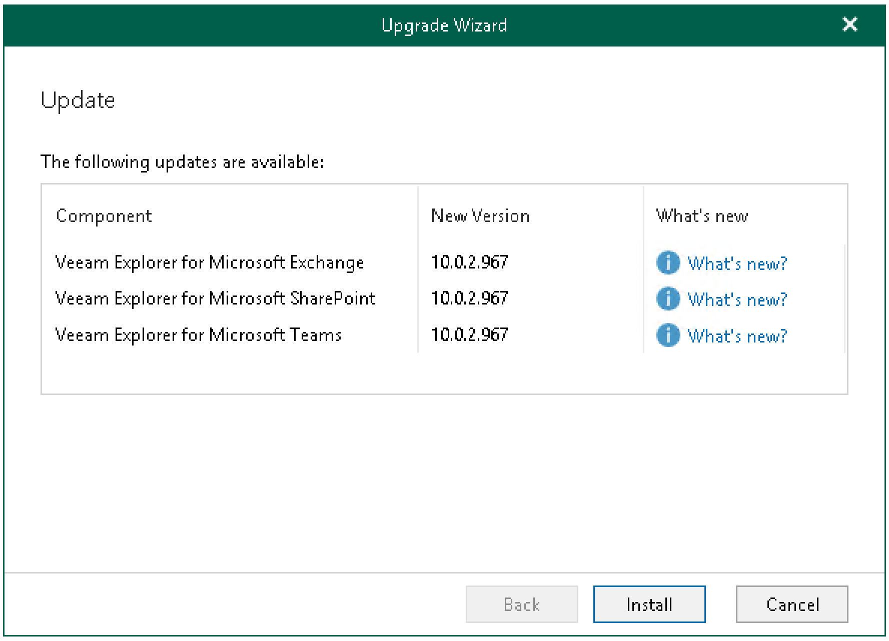
Checking for updates (Cancel)...

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, Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft Teams.



The following updates are available:

Component	New Version	What's new
Veeam Explorer for Microsoft Exchange	10.0.2.967	What's new?
Veeam Explorer for Microsoft SharePoint	10.0.2.967	What's new?
Veeam Explorer for Microsoft Teams	10.0.2.967	What's new?

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, up to 1 TB of Microsoft SharePoint data and up to 10 teams in all organizations. *Community Edition* mode is not limited in time and does not have limitations in terms of 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, more than 1 TB of Microsoft SharePoint data or more than 10 teams. For more information about available license types in Veeam Backup for Microsoft 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** window, click **Install** and specify the path to the *.lic* file.

Updating License

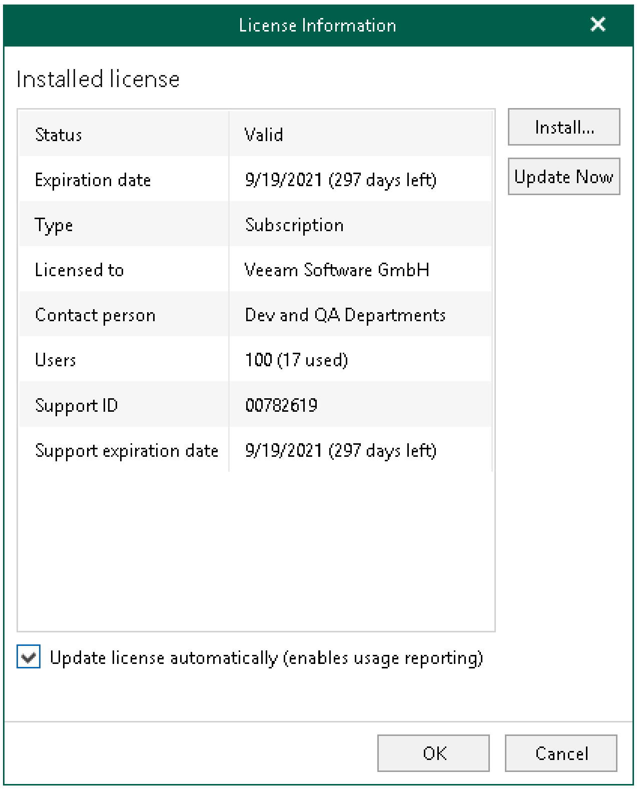
You can update an existing license, for example, if you want to extend the number of supported user accounts that you need to back up.

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.



Status	Valid
Expiration date	9/19/2021 (297 days left)
Type	Subscription
Licensed to	Veeam Software GmbH
Contact person	Dev and QA Departments
Users	100 (17 used)
Support ID	00782619
Support expiration date	9/19/2021 (297 days left)

☑ Update license automatically (enables usage reporting)

Upgrading to Veeam Backup for Microsoft Office 365 5.0

Veeam Backup for Microsoft Office 365 supports upgrade to version 5.0 from following versions of the product:

- 3.0 (build 3.0.0.422)
- 4.0 (build 4.0.0.1345)
- 4a (builds 4.0.0.1553, 4.0.0.1580)
- 4b (builds 4.0.0.2516, 4.0.0.2549)
- 4c (builds 4.0.1.519, 4.0.1.531, 4.0.1.545)

Consider the following:

- All modifications made to the `Config.xml` file manually will be lost.
- 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 5.0, 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
- Installing Veeam Explorer for Microsoft Teams

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

- *Backup repositories*

  For information on how to upgrade backup repositories, see Upgrading Backup Repositories.

- *Backup jobs*

  For information on how to upgrade backup jobs, see Upgrading Backup Job.

- *Backup proxy servers*

  For information on how to upgrade backup proxy servers, see Upgrading Backup Proxy Servers

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

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, Veeam Explorer for Microsoft OneDrive for Business and Veeam Explorer for Microsoft Teams.
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. From the **Start** menu, select **Control Panel** > **Programs and Features**.
4. In the programs list, right-click **Veeam Backup for Microsoft Office 365** and select **Uninstall**.
5. Right-click **Veeam Backup & Replication** and select **Uninstall** to uninstall Veeam Explorers.

Launching Veeam Backup for Microsoft Office 365

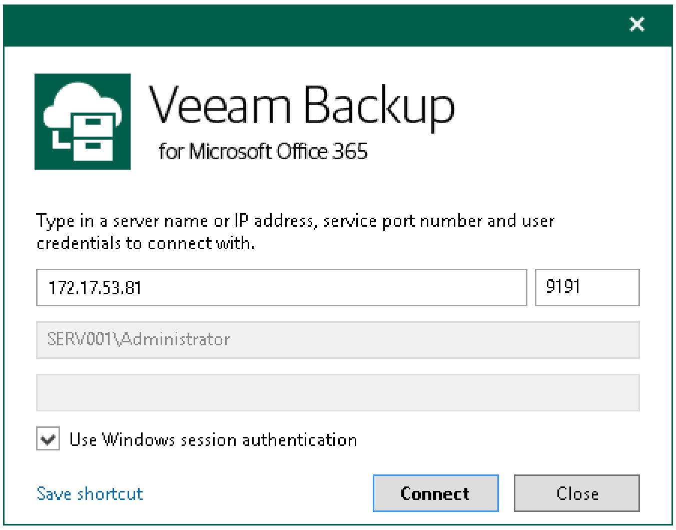
To launch Veeam Backup for Microsoft Office 365, go to **Start**, select **Veeam Backup for Microsoft Office 365** and specify the following:

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.



Type in a server name or IP address, service port number and user credentials to connect with.

172.17.53.81 | 9191

SERV001\Administrator

☑ Use Windows session authentication

Launching with Command Line

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

- */local=true*

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

  For example:

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

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

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

  For example:

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

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

  To connect to Veeam Backup for Microsoft 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.

  For 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
- Main Application Window

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.

- **Manage Cloud Credentials**. Allows you to manage cloud passwords.

  For more information, see Managing Cloud Credentials.

- **Manage Passwords**. Allows you to manage encryption passwords.

  For more information, see Managing Encryption Passwords.

- **General Options**. Allows you to configure general application 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.

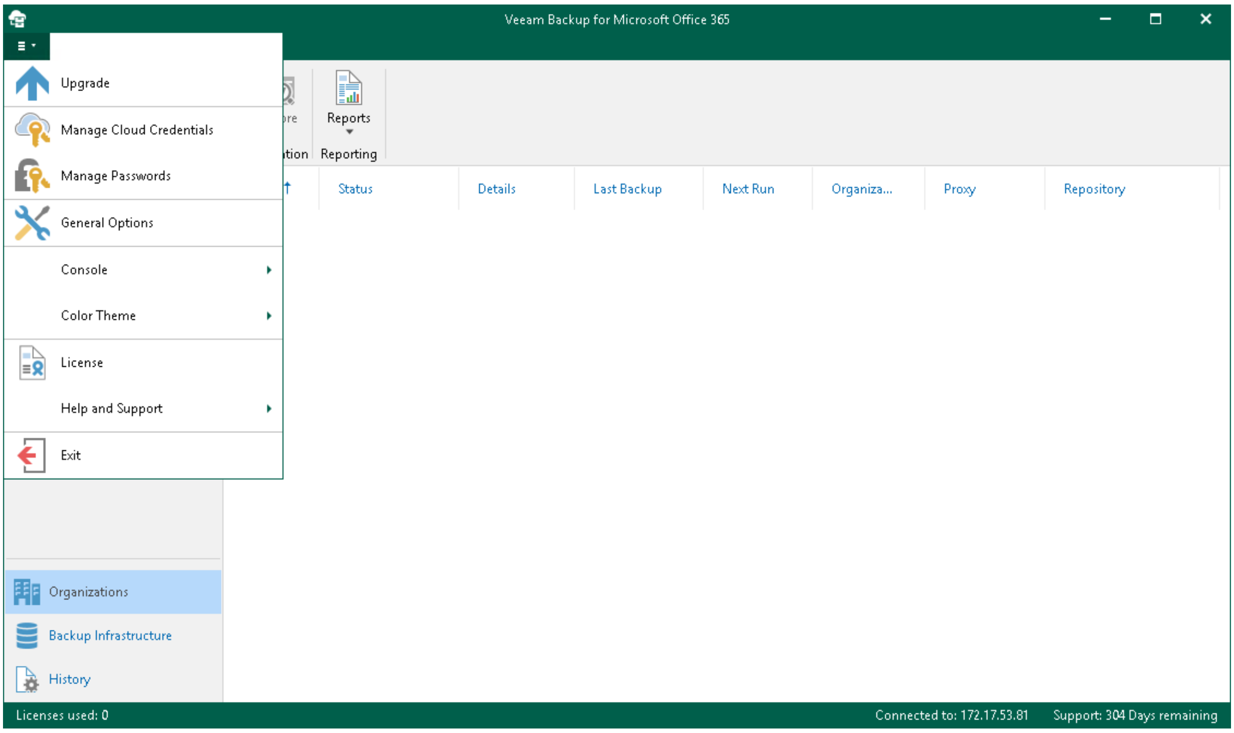
- **Color Theme**. Contains four different color schemes that you can select for your application console.

- **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.



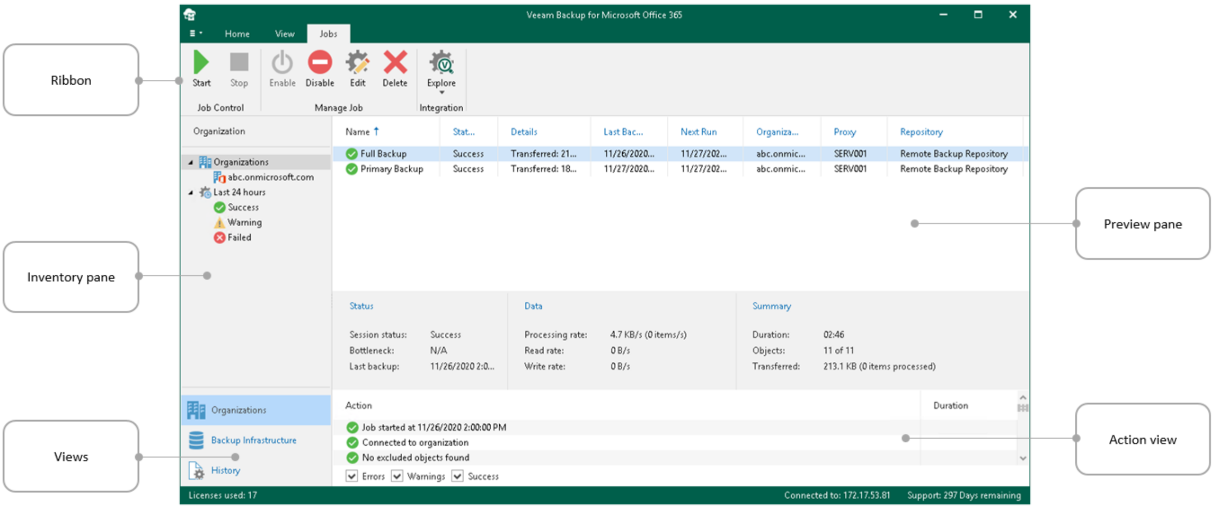
Main Application Window

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.
    - The **Backup Repository** tab contains commands specific for backup repositories.
    - The **Object Storage Repository** tab contains commands specific for object storage 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.



Name ↑	Stat...	Details	Last Bac...	Next Run	Organiza...	Proxy	Repository
Full Backup	Success	Transferred: 21...	11/26/2020...	11/27/202...	abc.onmic...	SERV001	Remote Backup Repository
Primary Backup	Success	Transferred: 18...	11/27/2020...	11/27/202...	abc.onmic...	SERV001	Remote Backup Repository

Status

Session status: Success
Bottleneck: N/A
Last backup: 11/26/2020 2:0...

Data

Processing rate: 4.7 KB/s (0 items/s)
Read rate: 0 B/s
Write rate: 0 B/s

Summary

Duration: 02:46
Objects: 11 of 11
Transferred: 213.1 KB (0 items processed)

Action	Duration
Job started at 11/26/2020 2:00:00 PM	
Connected to organization	
No excluded objects found	

☑ Errors ☑ Warnings ☑ Success

Licenses used: 17   Connected to: 172.17.53.81   Support: 297 Days remaining

TIP:

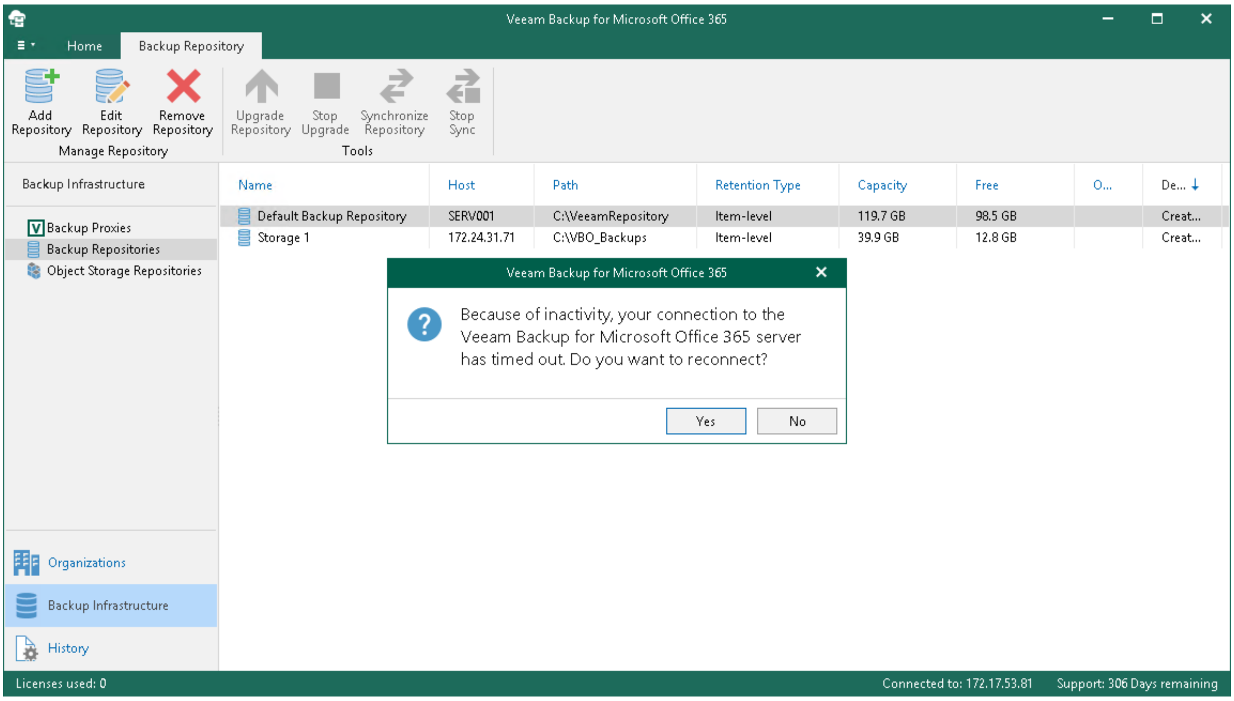
To open online help, press **[F1]** in any Veeam Backup for Microsoft Office 365 wizard or window.

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. Veeam Backup for Microsoft Office 365 prompts you whether to re-establish a connection and continue using the product, or exit the console.

Consider the following:

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



Name	Host	Path	Retention Type	Capacity	Free	O...	De...
Default Backup Repository	SERV001	C:\VeeamRepository	Item-level	119.7 GB	98.5 GB		Creat...
Storage 1	172.24.31.71	C:\VBO_Backups	Item-level	39.9 GB	12.8 GB		Creat...

Veeam Backup for Microsoft Office 365

Because of inactivity, your connection to the Veeam Backup for Microsoft Office 365 server has timed out. Do you want to reconnect?

Yes No

Licenses used: 0 Connected to: 172.17.53.81 Support: 306 Days remaining

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.

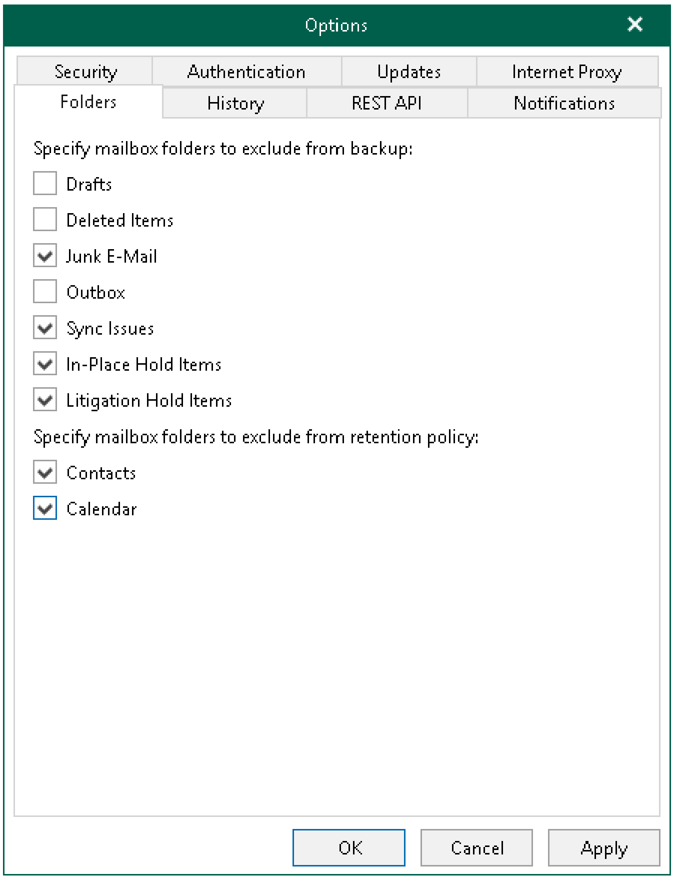
To configure exclusions, do the following:

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 check boxes next to folders that you want to exclude from a backup.
4. Click **OK**.

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

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

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



Specify mailbox folders to exclude from backup:

☐ Drafts
☐ Deleted Items
☑ Junk E-Mail
☐ Outbox
☑ Sync Issues
☑ In-Place Hold Items
☑ Litigation Hold Items

Specify mailbox folders to exclude from retention policy:

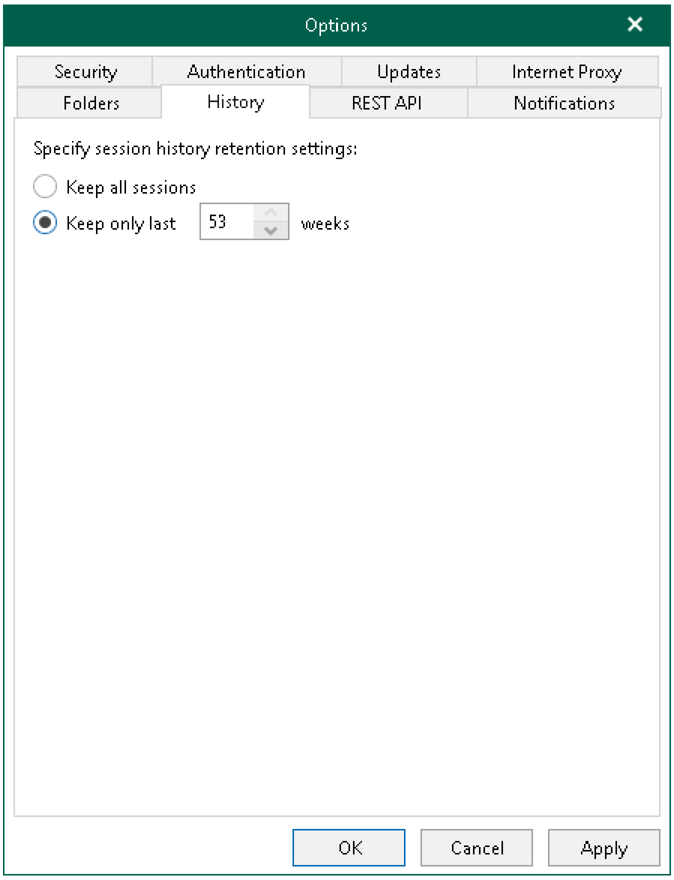
☑ Contacts
☑ Calendar

Session History

Veeam Backup for Microsoft Office 365 saves information about backup and restore sessions to the configuration database. You can review this information, as described in Backup and Restore Statistics.

To specify a period during which to keep information about backup and restore sessions, do the following:

1. In the main menu, click **General Options**.
2. Open the **History** tab.
3. Specify for how long Veeam Backup for Microsoft Office 365 will keep history for backup and restore sessions. You can select one of the following options:
   - **Keep all sessions**
   - **Keep only last <N> weeks**. If you select this option, you can specify a number of weeks during which Veeam Backup for Microsoft Office 365 will keep history for backup and restore sessions.
4. Click **OK**.



Specify session history retention settings:

○ Keep all sessions

● Keep only last 53 weeks

RESTful API Settings

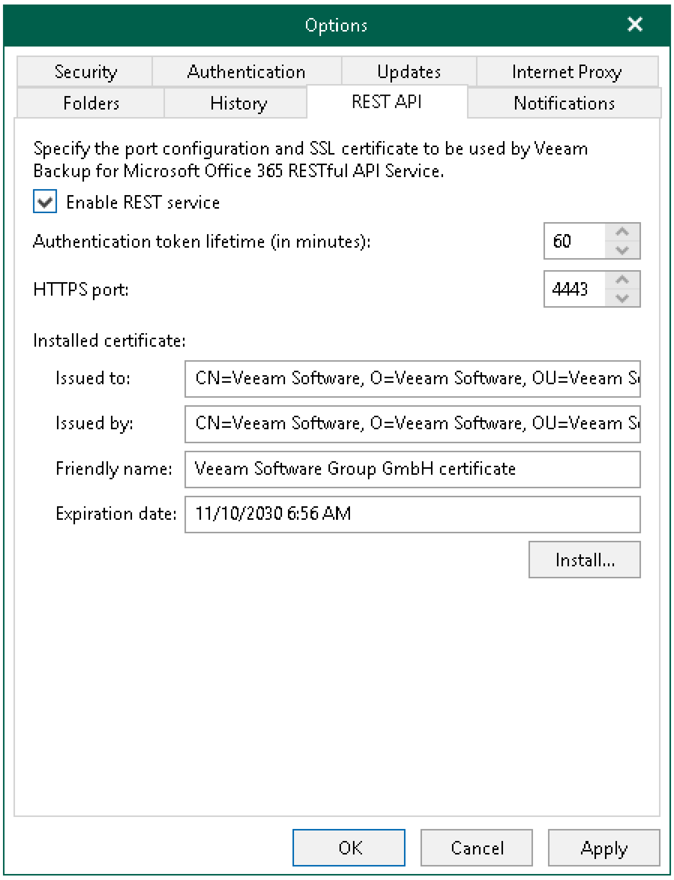
You can use the RESTful API to communicate with Veeam Backup for Microsoft Office 365.

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** field, specify the lifetime value for an authentication token (in minutes).

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

   You can generate a new certificate or select an existing certificate using the **Select Certificate** wizard, as described in SSL Certificates.
7. Click **OK**.



Specify the port configuration and SSL certificate to be used by Veeam Backup for Microsoft Office 365 RESTful API Service.

☑ Enable REST service

Authentication token lifetime (in minutes): 60

HTTPS port: 4443

Installed certificate:

Issued to: CN=Veeam Software, O=Veeam Software, OU=Veeam S

Issued by: CN=Veeam Software, O=Veeam Software, OU=Veeam S

Friendly name: Veeam Software Group GmbH certificate

Expiration date: 11/10/2030 6:56 AM

Notification Settings

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

> **NOTE:**
>
> Notifications about the backup job results are sent by a backup proxy server specified in the properties of the backup job. For more information, see Specify Backup Proxy and Repository.

To configure email notifications, do the following:

1. In the main menu, click **General Options**.
2. Open the **Notifications** tab.
3. Select the **Enable e-mail notifications** check box.
4. Specify the address of a server that 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.

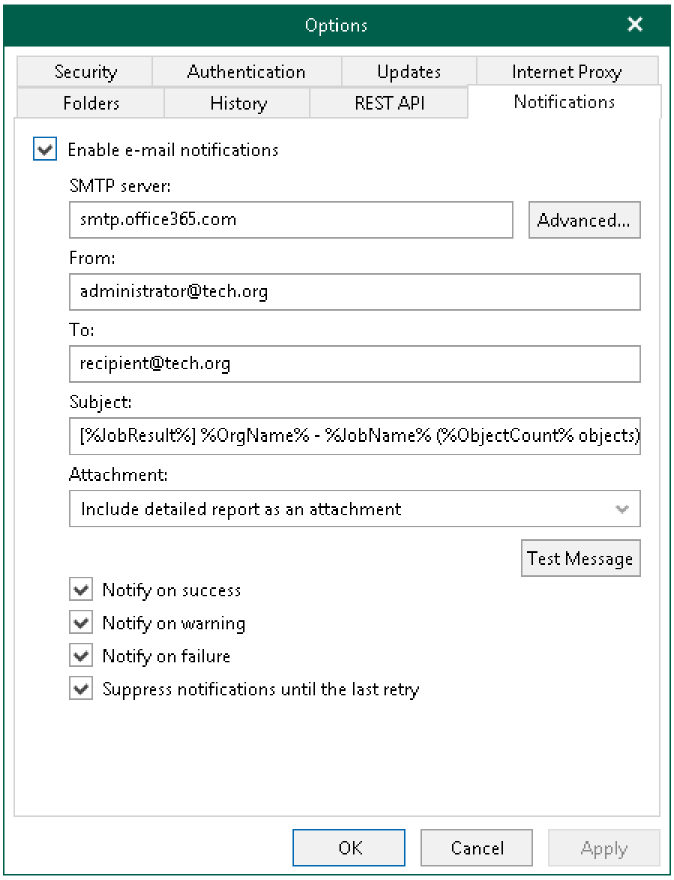
      By default, Veeam Backup for Microsoft Office 365 establishes a connection to the *smtp.office365.com* server over port *587*. For more information, see Microsoft Docs.
    - Select the **Connect Using SSL** check box to establish a secure connection.
    - Select the **The SMTP server requires authentication** 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 of 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. From the **Attachment** drop-down list, select whether to include a detailed report as an attachment to the email notification. This setting applies to notifications about backup jobs that process more than 1000 objects.
    - Select **Include detailed report as an attachment** if you want to include a detailed report as an email attachment. If you select this option, Veeam Backup for Microsoft Office 365 will provide a summary about the backup job results in the notification body and a detailed report for each object processed by the job in the email attachment.

- Select **Do not include detailed report** if you do not want to include a detailed report as an email attachment. If you select this option, email notifications will only contain a summary about the job results in the notification body.

This setting does not apply to backup jobs that process up to 1000 objects. For such backup jobs, Veeam Backup for Microsoft Office 365 always provides both a summary and a detailed report in the notification body.

10. By default, system notifications are sent every time a backup job session is completed with any of the following states: *Success*, *Warning* and *Failure*. To turn off unwanted notifications, clear check boxes next to the events for which you do not want to receive notifications:
    - **Notify on success**
    - **Notify on warning**
    - **Notify on failure**
11. [Optional] If a backup job is configured to perform retry attempts, select the **Suppress notifications until the last retry** check box to send email notifications only after the last attempt.
12. Click **Test Message** to send a test message.
13. Click **OK**.



☑ Enable e-mail notifications

SMTP server: smtp.office365.com

From: administrator@tech.org

To: recipient@tech.org

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

Attachment: Include detailed report as an attachment

☑ Notify on success

☑ Notify on warning

☑ Notify on failure

☑ Suppress notifications until the last retry

Security Settings

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

To configure security settings, do the following:

1. In the main menu, click **General Options**.

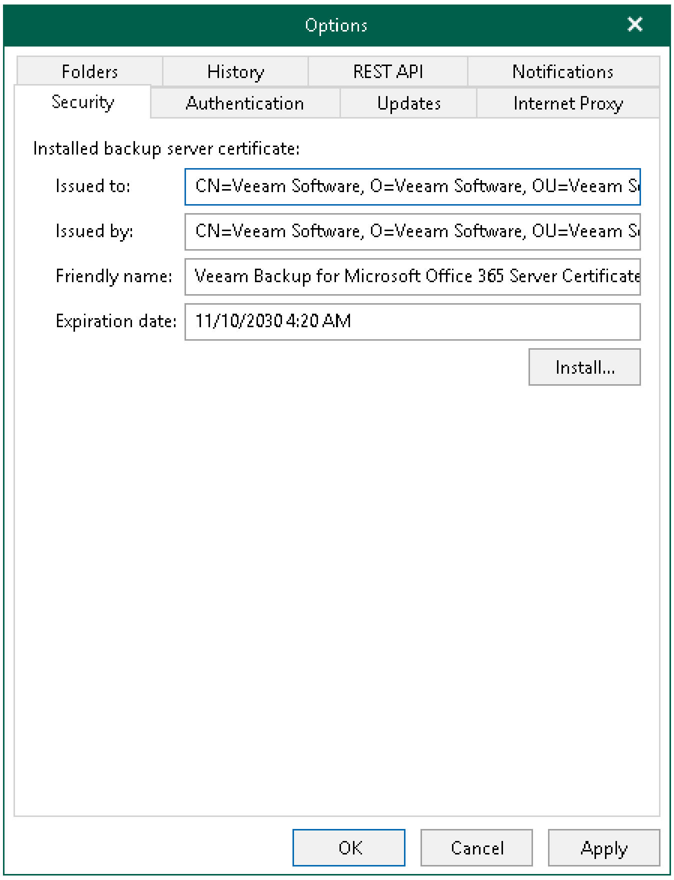
2. Open the **Security** tab.

3. In the **Installed backup server certificate** field, review information about the certificate that is used to establish a connection with a backup proxy server deployed in a workgroup.

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

4. Click **OK**.

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



Installed backup server certificate:

Issued to: CN=Veeam Software, O=Veeam Software, OU=Veeam S

Issued by: CN=Veeam Software, O=Veeam Software, OU=Veeam S

Friendly name: Veeam Backup for Microsoft Office 365 Server Certificate

Expiration date: 11/10/2030 4:20 AM

Tenant Authentication Settings

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

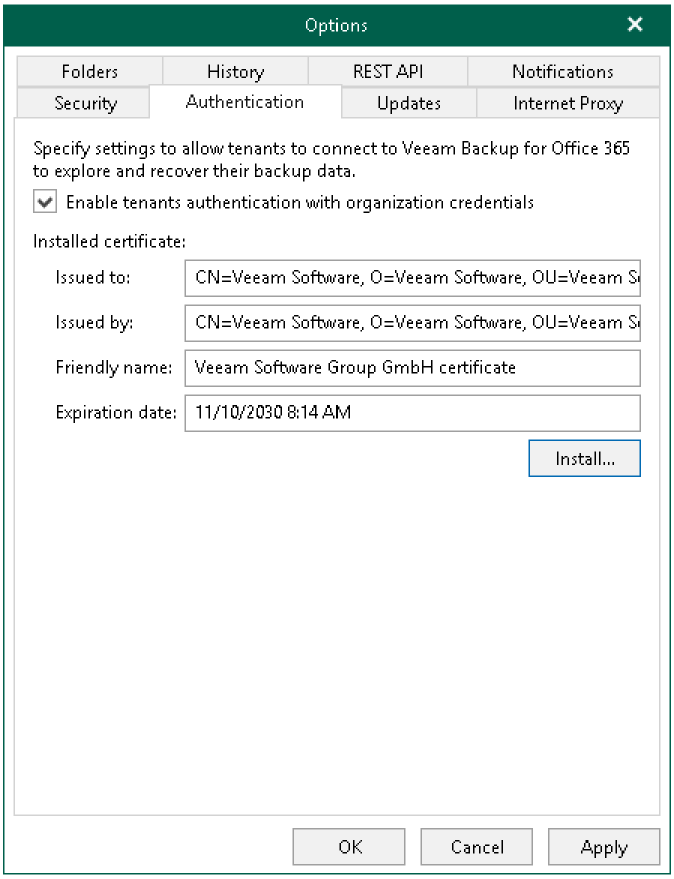
To enable tenant authentication, do the following:

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

   You can generate a new certificate or select an existing certificate using the **Select Certificate** wizard, as described in SSL Certificates.
5. Click **OK**.

TIP:

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



Specify settings to allow tenants to connect to Veeam Backup for Office 365 to explore and recover their backup data.

☑ Enable tenants authentication with organization credentials

Installed certificate:

Issued to: CN=Veeam Software, O=Veeam Software, OU=Veeam S

Issued by: CN=Veeam Software, O=Veeam Software, OU=Veeam S

Friendly name: Veeam Software Group GmbH certificate

Expiration date: 11/10/2030 8:14 AM

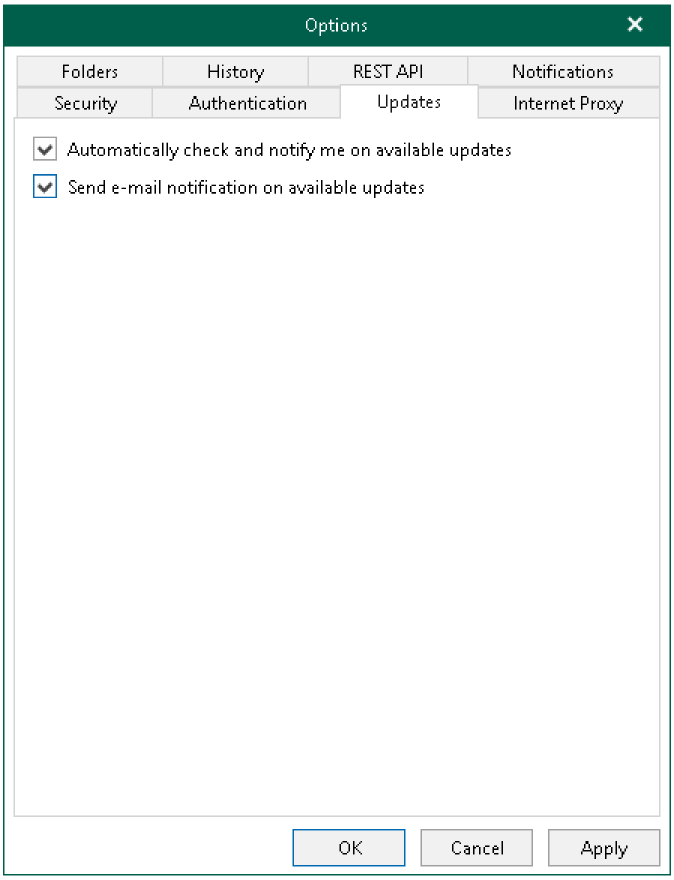
Update Notification Settings

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**. If you select this check box, Veeam Backup for Microsoft Office 365 will notify you about available updates with a dialog message in the user interface.
   - **Send e-mail notification on available updates**. If you select this check box, Veeam Backup for Microsoft Office 365 will notify you about available updates with an email message. Veeam Backup for Microsoft Office 365 will use the recipient address and SMTP server settings specified in the email notification settings. For more information, see Notification Settings.
4. Click **OK**.

> **TIP:**
>
> For information on how to manually check for a new version, see Checking for Updates.



☑ Automatically check and notify me on available updates

☑ Send e-mail notification on available updates

Global Internet Proxy Server Settings

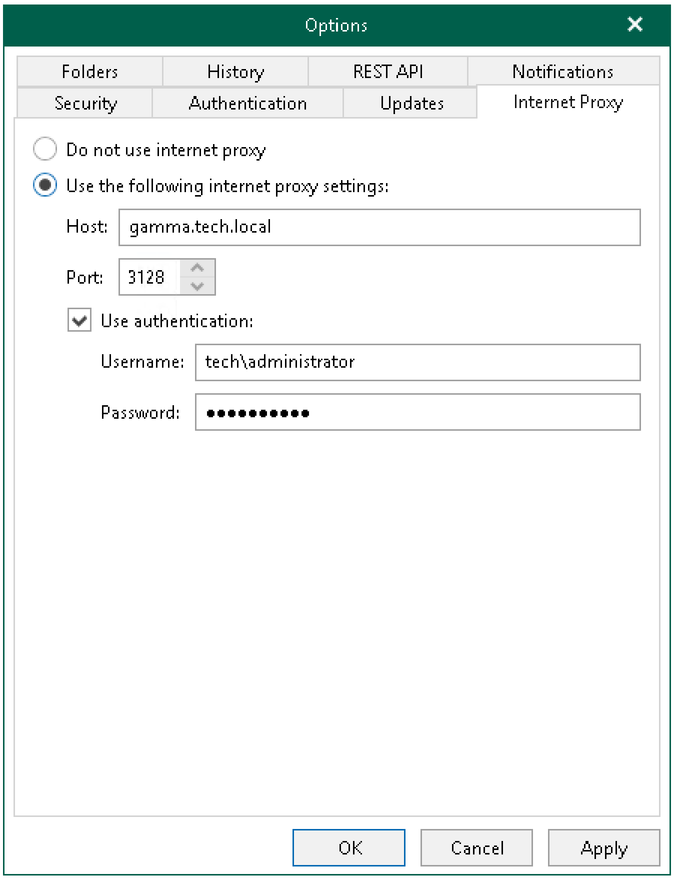
If a server on which Veeam Backup for Microsoft Office 365 is deployed does not have a direct access to the internet, you can assign an internet proxy server to be used as a gateway.

To set an internet proxy server, do the following:

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

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

> **TIP:**
>
> 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.



○ Do not use internet proxy

● Use the following internet proxy settings:

Host: gamma.tech.local

Port: 3128

☑ Use authentication:

Username: tech\administrator

Password: ●●●●●●●●●●●

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 communication with a backup proxy server in a workgroup.

  For more information, see Security Settings.

- To enable user authentication with organization credentials for tenants.

  For more information, see Tenant Authentication Settings.

- To add Microsoft Office 365 organizations.

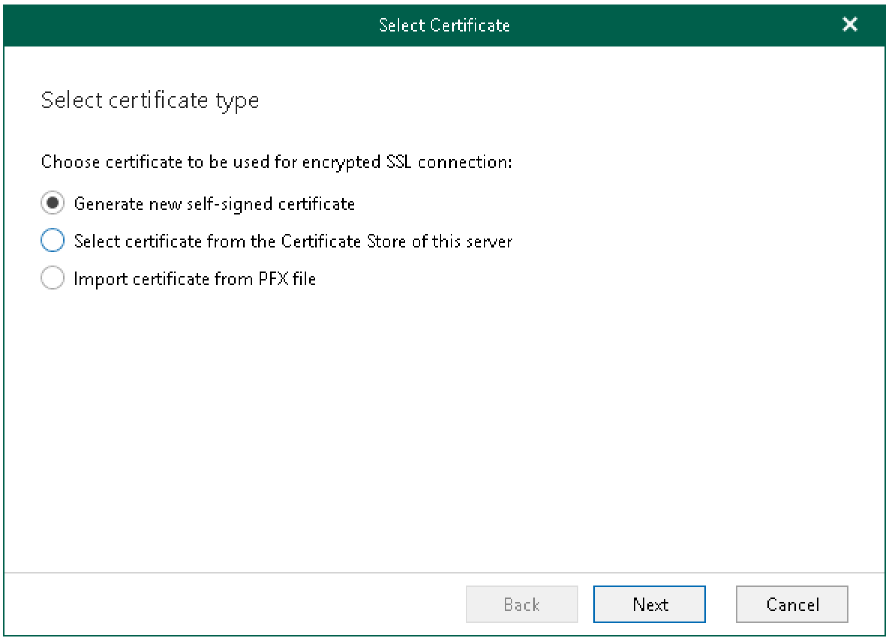
  For more information, see Microsoft Office 365 Organizations.

- 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 PFX file


Select Certificate

Select certificate type

Choose certificate to be used for encrypted SSL connection:

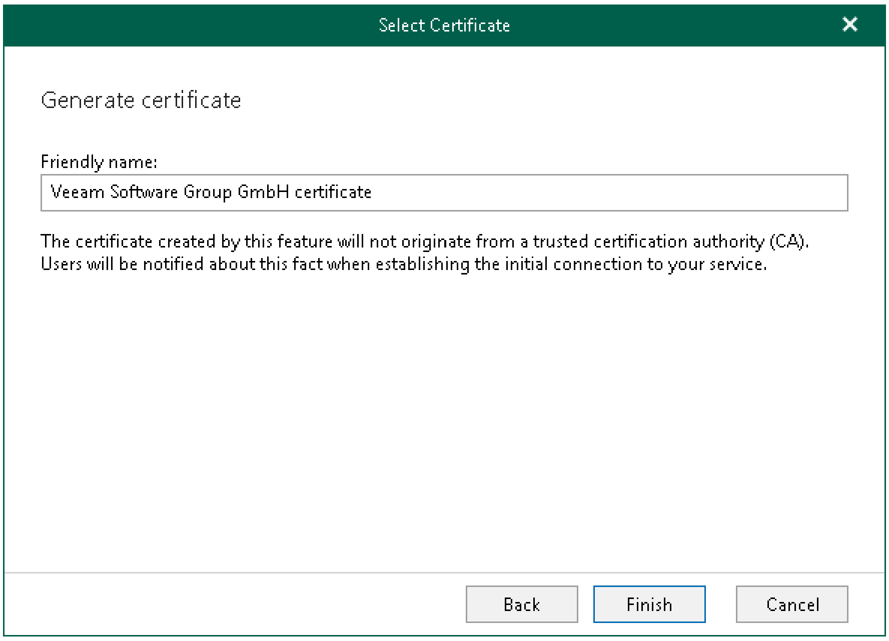
● Generate new self-signed certificate

○ Select certificate from the Certificate Store of this server

○ Import certificate from PFX file

Generating New Certificate

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

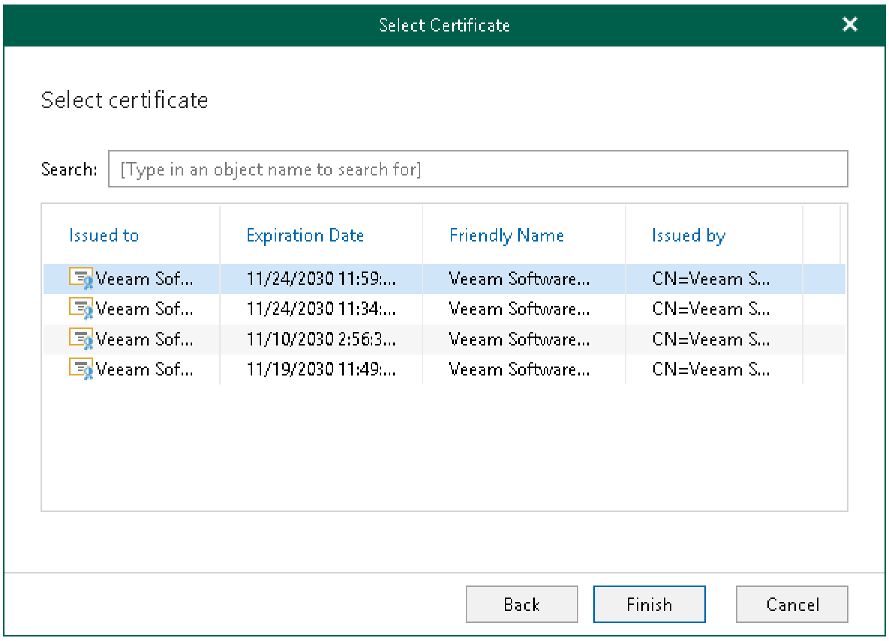


Friendly name: Veeam Software Group GmbH certificate

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.

Selecting Certificate

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

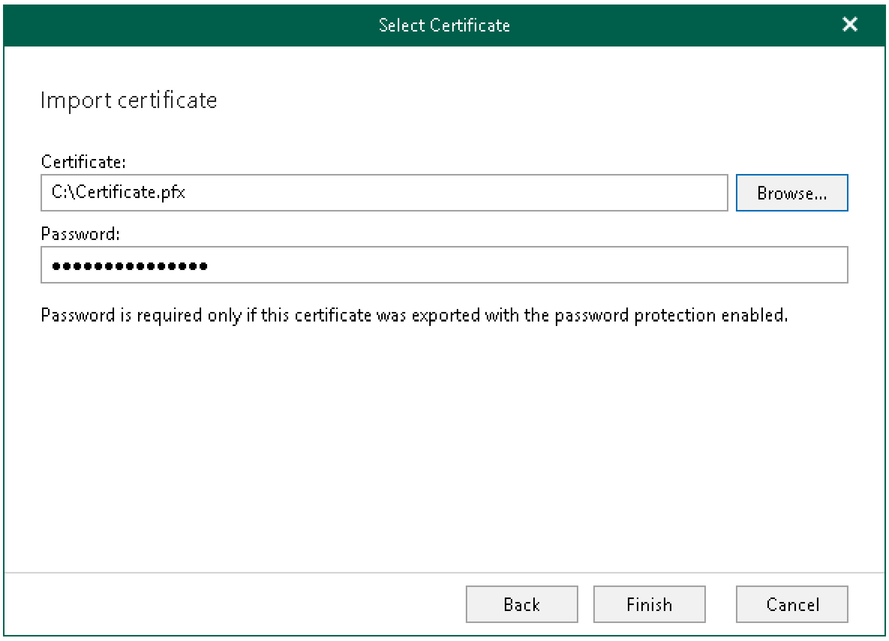


Search: [Type in an object name to search for]

Issued to	Expiration Date	Friendly Name	Issued by
Veeam Sof...	11/24/2030 11:59:...	Veeam Software...	CN=Veeam S...
Veeam Sof...	11/24/2030 11:34:...	Veeam Software...	CN=Veeam S...
Veeam Sof...	11/10/2030 2:56:3...	Veeam Software...	CN=Veeam S...
Veeam Sof...	11/19/2030 11:49:...	Veeam Software...	CN=Veeam S...

Importing Certificate

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



Certificate: C:\Certificate.pfx

Password: ●●●●●●●●●●●●●●●

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

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 architecture component used to leverage network traffic when backing up or restoring data.

Consider the following:

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

- Veeam Backup for Microsoft Office 365 lets you deploy the following types of backup proxy servers:

  - Domain backup proxy
  - Workgroup backup proxy

  For more information, see Backup Proxy Deployment Scenarios.

- Each backup proxy server can process one or several organizations.

- An organization can be processed by one or several backup proxies.

- A backup proxy server is responsible for sending email notifications about backup job completion results.

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

Backup Proxy Deployment Scenarios

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

- *Scenario 1. Domain backup proxy*

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

- *Scenario 2. Workgroup backup proxy*

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

Adding Backup Proxy Servers

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

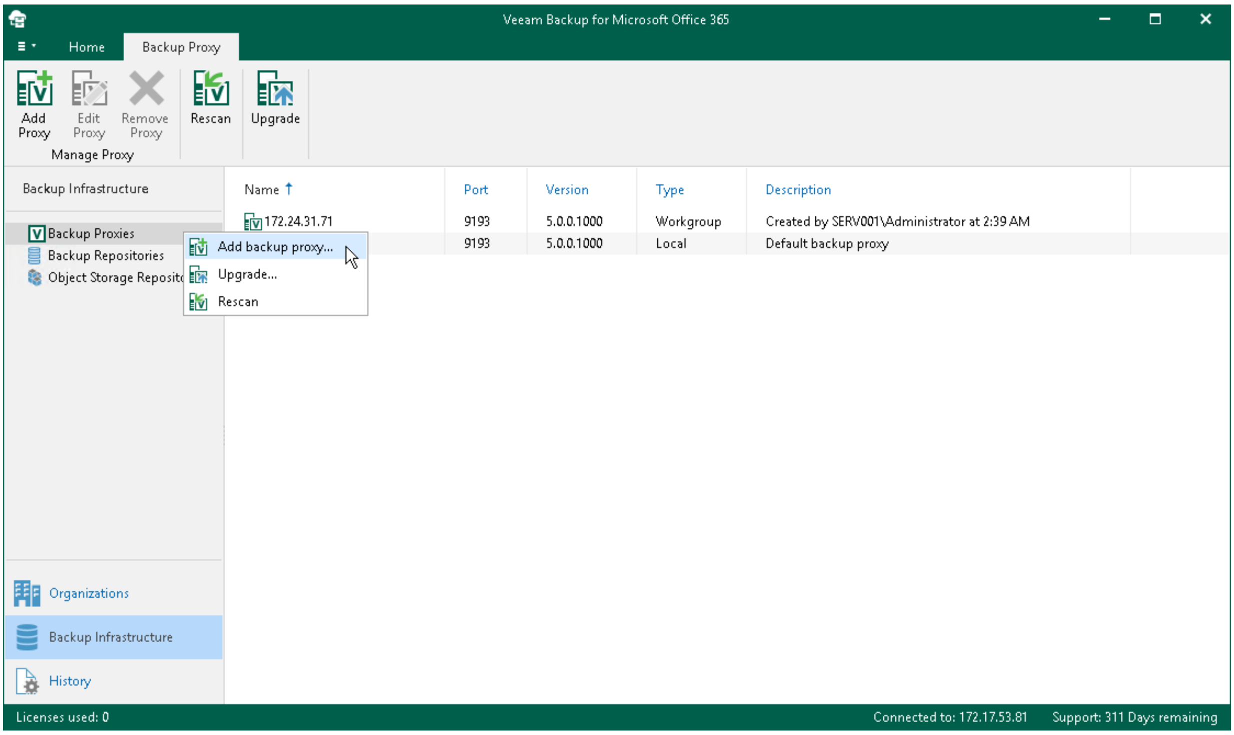
1. Launch the New Backup Proxy wizard.
2. Specify a backup proxy server address.
3. Specify credentials.

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** on the ribbon.

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



Name ↑	Port	Version	Type	Description
172.24.31.71	9193	5.0.0.1000	Workgroup	Created by SERV001\Administrator at 2:39 AM
	9193	5.0.0.1000	Local	Default 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, specify a computer that you want to use as a backup proxy server:

   - For a domain backup proxy, enter a DNS name or IP address of the computer that you want to use as a backup proxy server.

   - For a workgroup backup proxy, enter an 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.

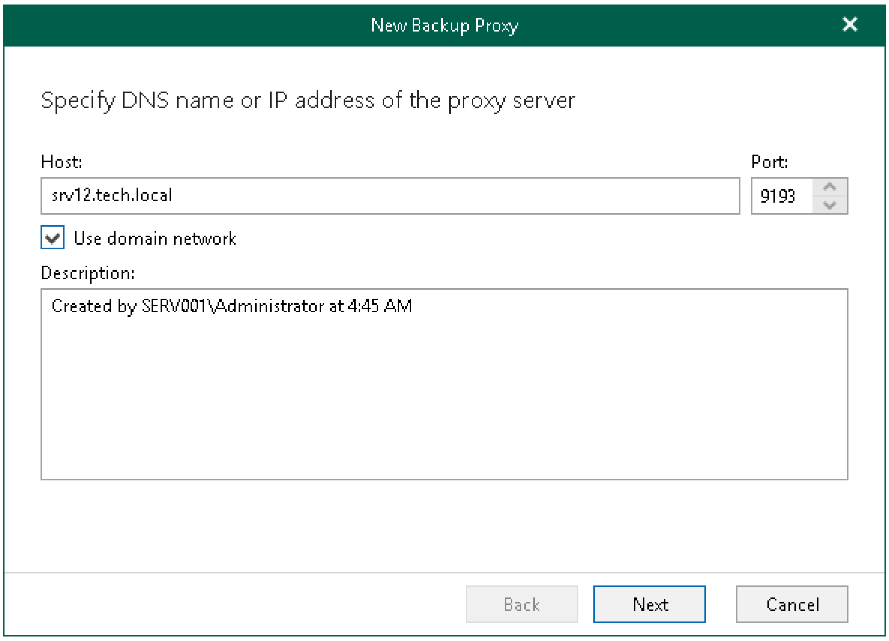
   Make sure that the default admin share ADMIN$ (*C:\Windows*) is enabled on the specified computer.

2. In the **Port** field, enter a port number to access the specified computer.

3. If you want to add a domain backup proxy server, select the **Use domain network** check box. Otherwise, Veeam Backup for Microsoft Office 365 will add a workgroup backup proxy server. For more information, see Backup Proxy Deployment Scenarios.

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

4. [Optional] In the **Description** field, enter a description for the backup proxy server.


New Backup Proxy

Specify DNS name or IP address of the proxy server

Host: srv12.tech.local

Port: 9193

☑ Use domain network

Description: Created by SERV001\Administrator at 4:45 AM

Step 3. Specify Credentials

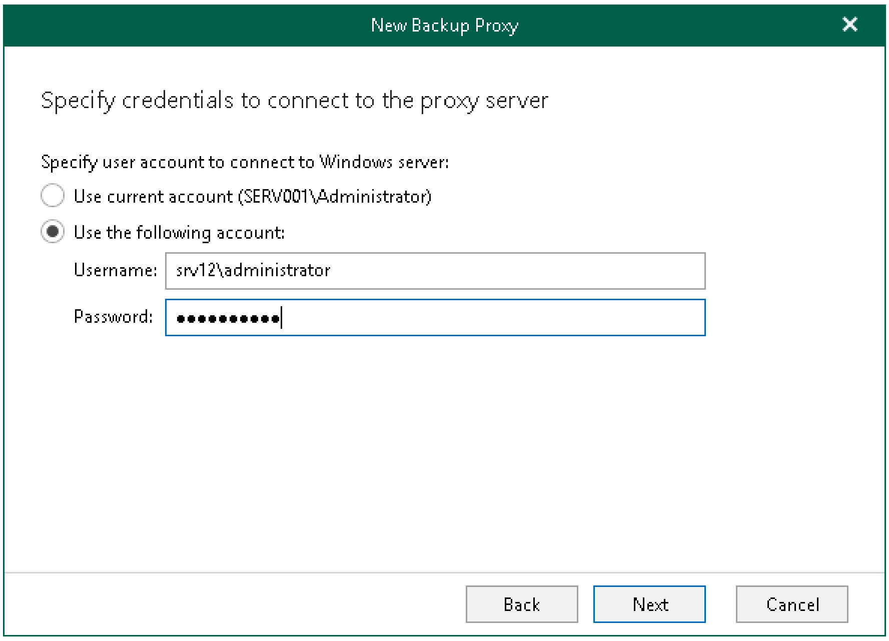
At this step of the wizard, enter user credentials to connect to the specified computer.

The account must be a member of the *Local Administrator* group.

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

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

Once a new proxy is added, you will be prompted to create a new backup repository on this proxy. You can dismiss this step and create a backup repository later, 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 (SERV001\Administrator)

● Use the following account:

Username: srv12\administrator

Password: ••••••••••

Editing Backup Proxy Server Settings

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

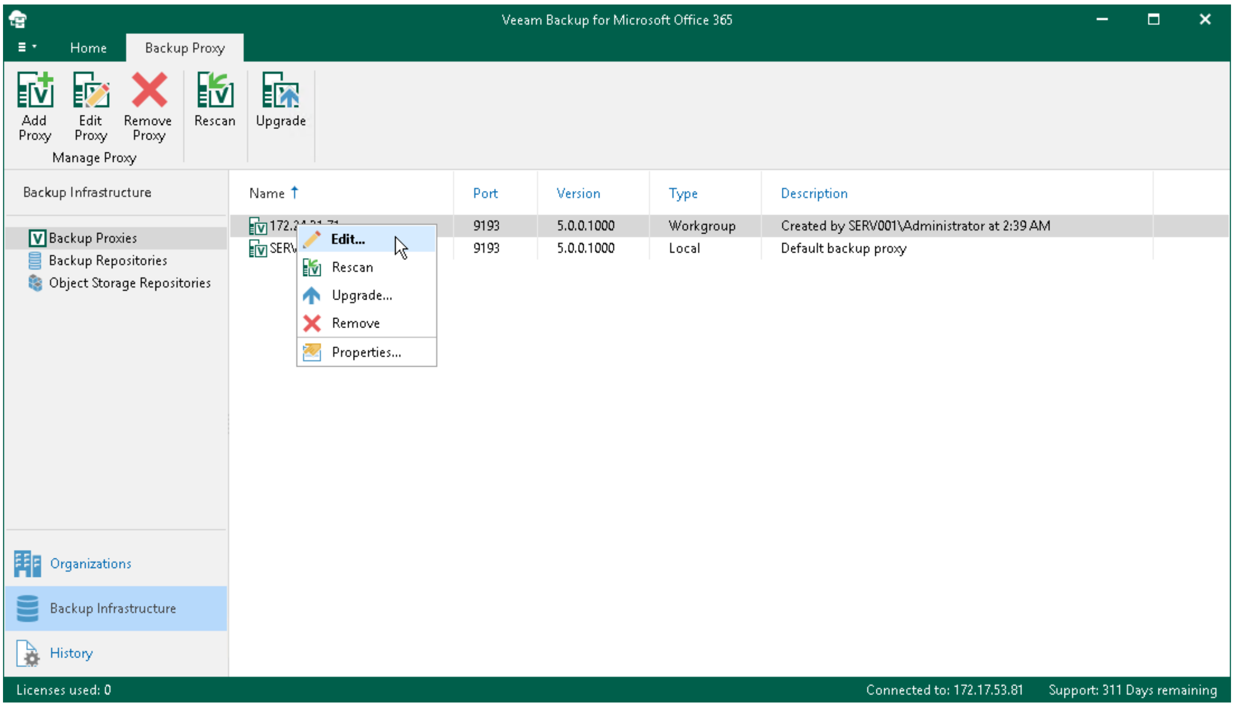
To edit backup proxy server settings, do the following:

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.
- You cannot change the type of a backup proxy server from the domain backup proxy to the workgroup backup proxy and vice versa.



Name	Port	Version	Type	Description
172.2	9193	5.0.0.1000	Workgroup	Created by SERV001\Administrator at 2:39 AM
SERV	9193	5.0.0.1000	Local	Default backup proxy

Rescanning Backup Proxy Servers

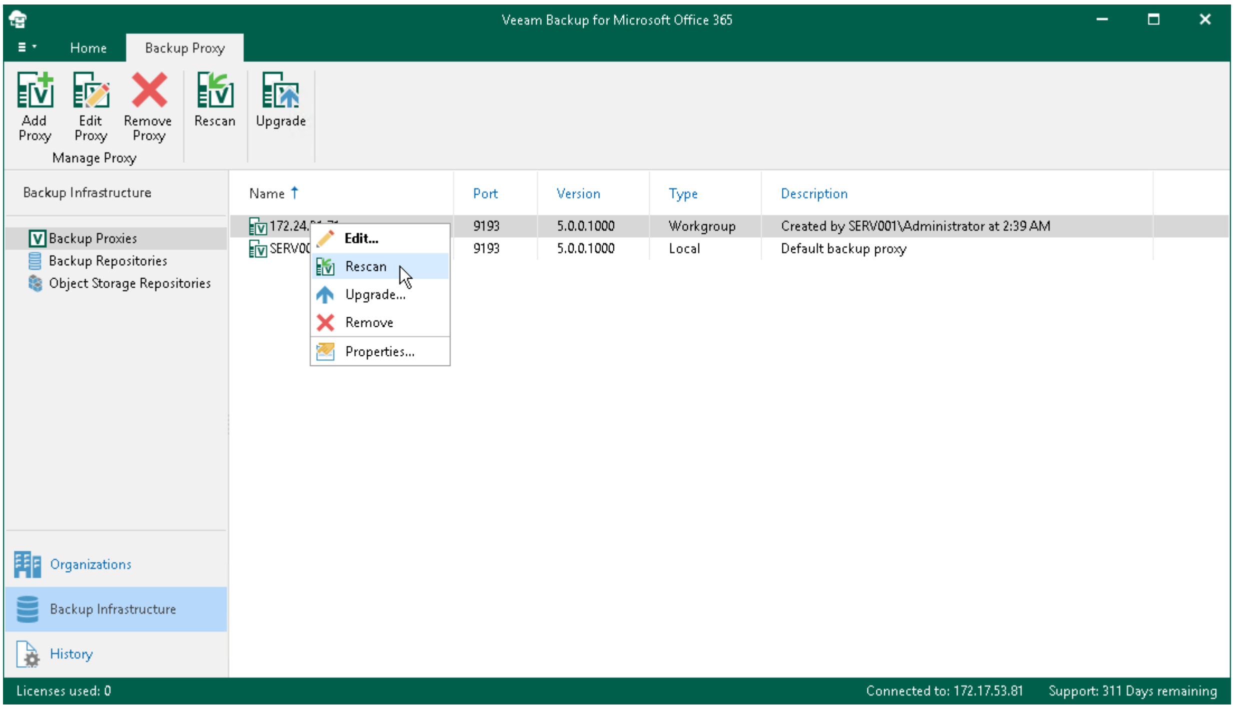
Rescan is required if some of your backup proxy servers are unavailable.

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**.



Name	Port	Version	Type	Description
172.24.	9193	5.0.0.1000	Workgroup	Created by SERV001\Administrator at 2:39 AM
SERV00	9193	5.0.0.1000	Local	Default backup proxy

Licenses used: 0

Connected to: 172.17.53.81

Support: 311 Days remaining

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.

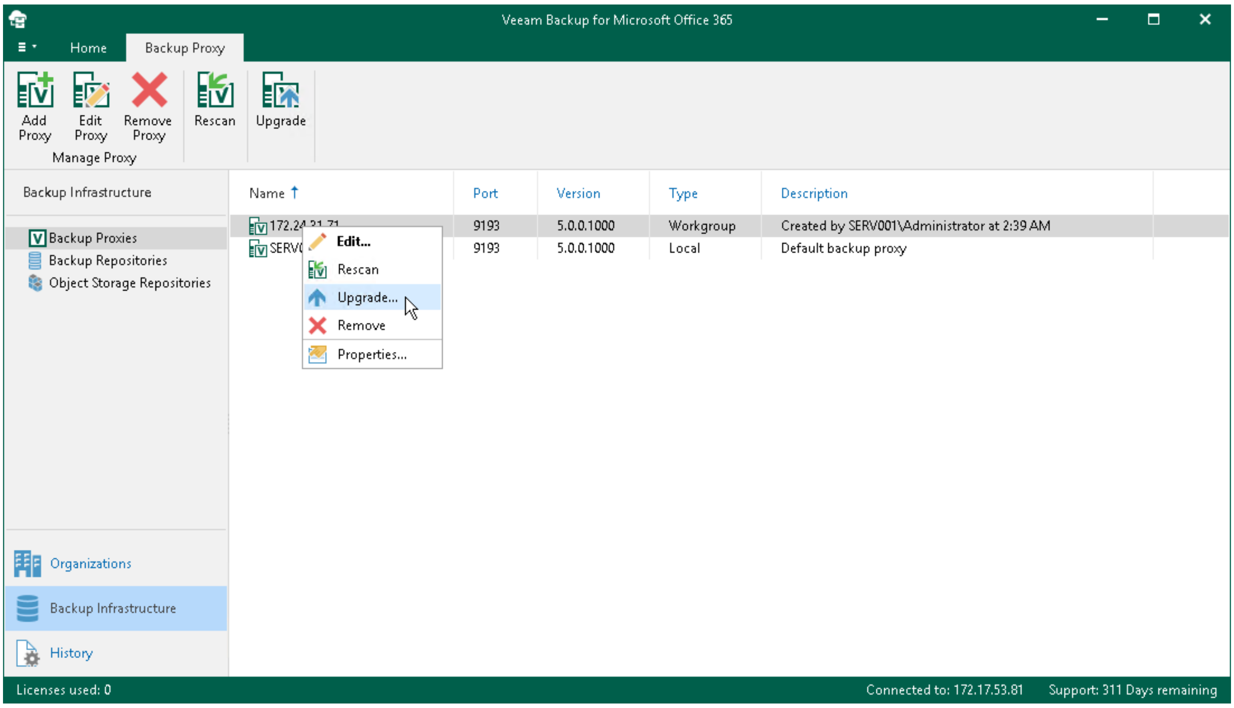
Step 1. Launch New Proxy Upgrade Wizard

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** on the ribbon.

   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**.



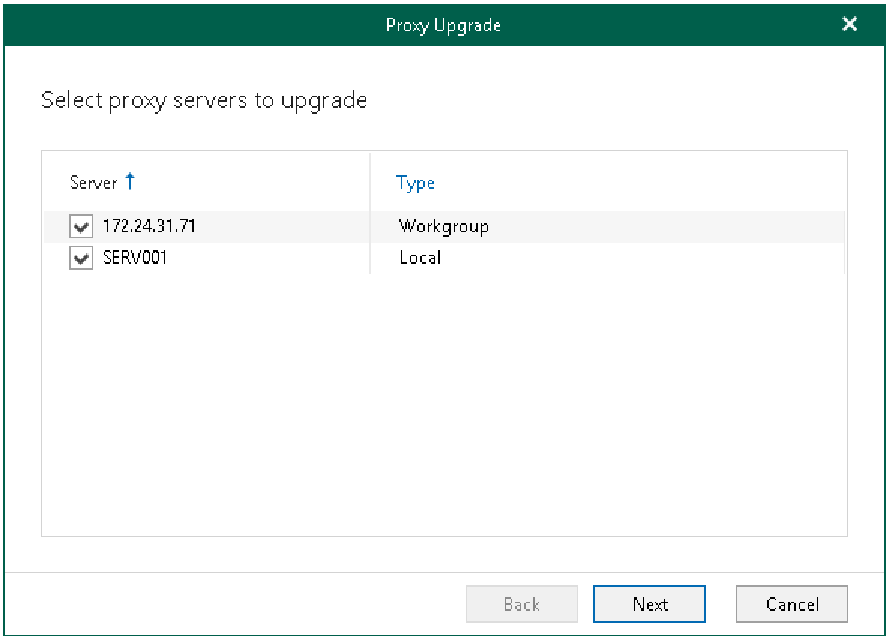
Name	Port	Version	Type	Description
172.24.31.71	9193	5.0.0.1000	Workgroup	Created by SERV001\Administrator at 2:39 AM
SERV[illegible]	9193	5.0.0.1000	Local	Default backup proxy

Licenses used: 0   Connected to: 172.17.53.81   Support: 311 Days remaining

Step 2. Select Backup Proxy Server to Upgrade

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

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



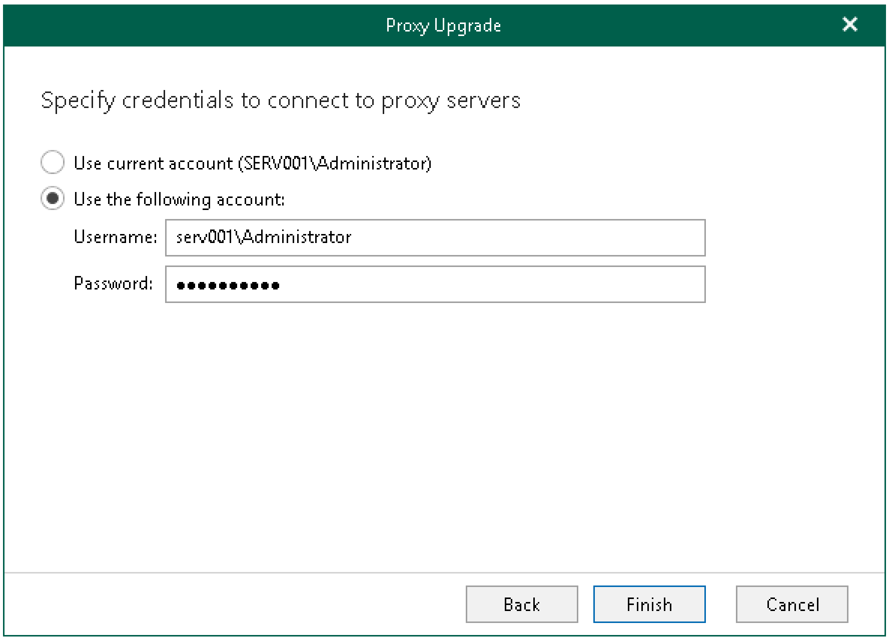
Select proxy servers to upgrade

Server ↑	Type
☑ 172.24.31.71	Workgroup
☑ SERV001	Local

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.



Specify credentials to connect to proxy servers

○ Use current account (SERV001\Administrator)

● Use the following account:

Username: serv001\Administrator

Password: ●●●●●●●●●●●

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.

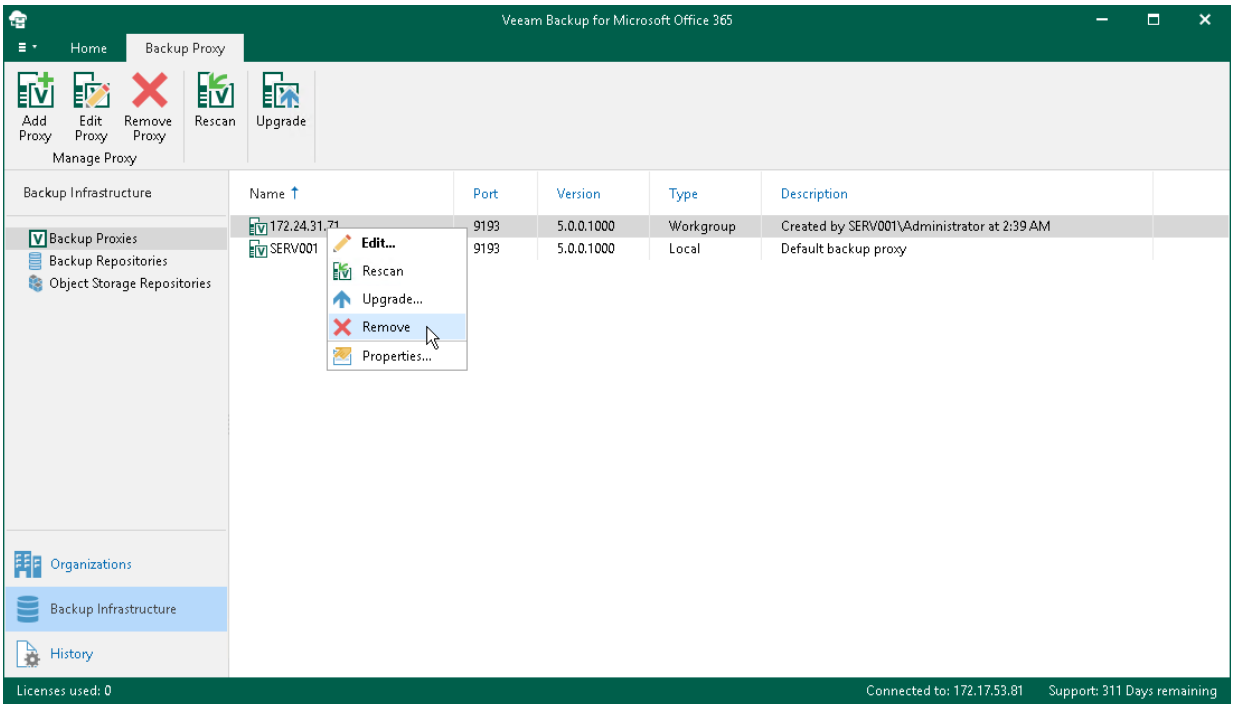
Consider the following:

- 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**.



Name	Port	Version	Type	Description
172.24.31.71	9193	5.0.0.1000	Workgroup	Created by SERV001\Administrator at 2:39 AM
SERV001	9193	5.0.0.1000	Local	Default backup proxy

Licenses used: 0

Connected to: 172.17.53.81 Support: 311 Days remaining

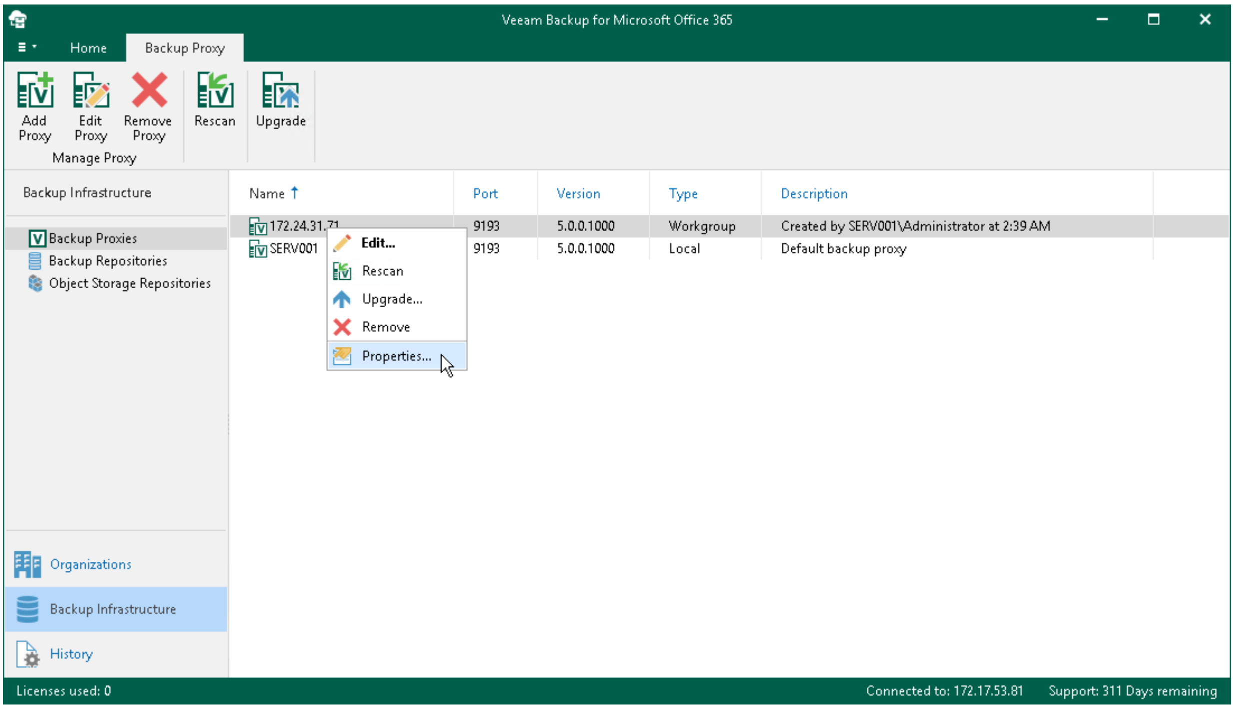
Modifying Backup Proxy Server Properties

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.



Name	Port	Version	Type	Description
172.24.31.71	9193	5.0.0.1000	Workgroup	Created by SERV001\Administrator at 2:39 AM
SERV001	9193	5.0.0.1000	Local	Default backup proxy

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:

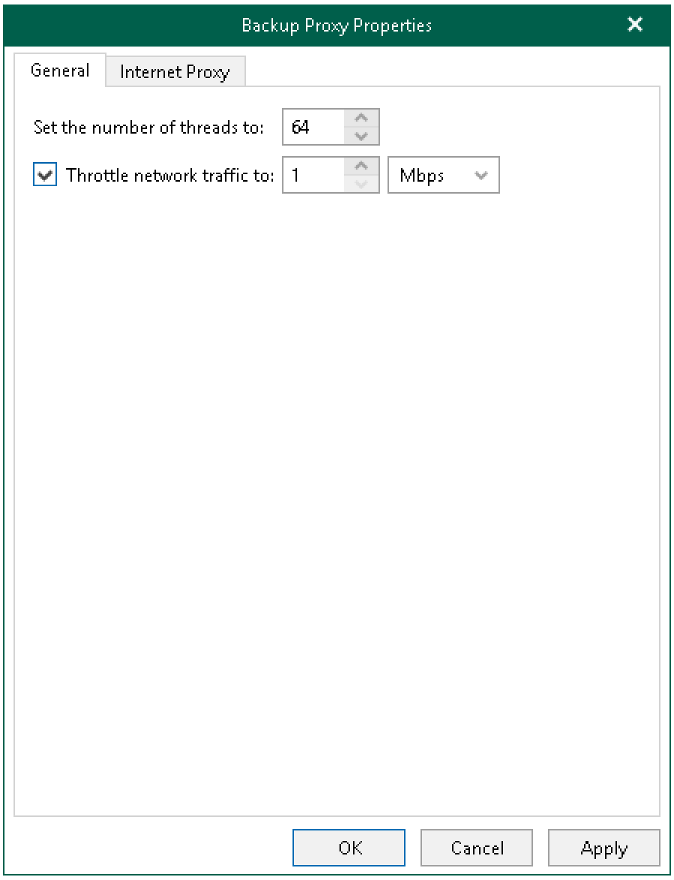
   ○ In the **Set the number of threads to** field, specify the allowed number of threads.

   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.



Set the number of threads to: 64

☑ Throttle network traffic to: 1 Mbps

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.

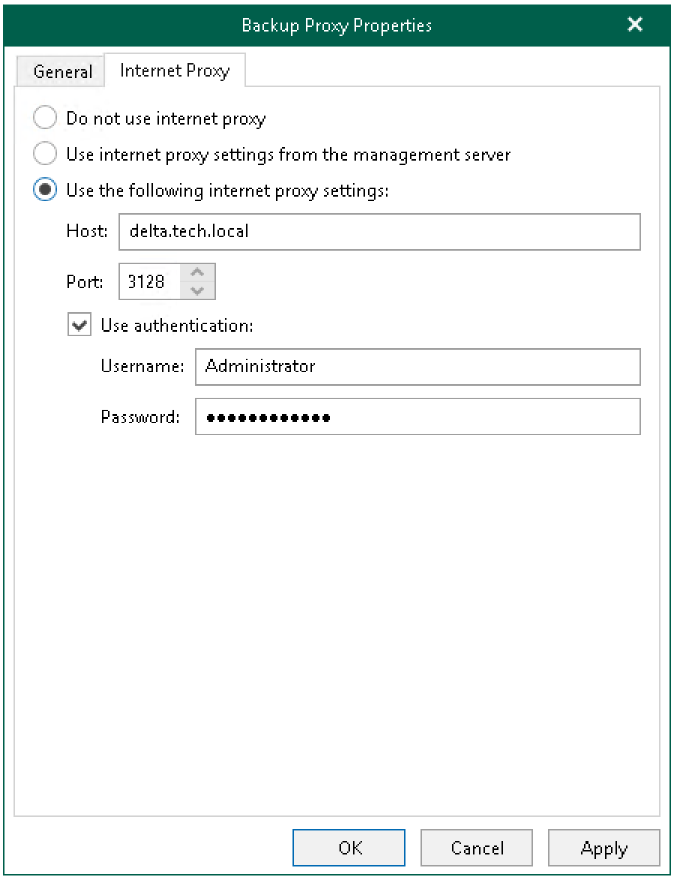
To set up an internet proxy server for a backup proxy, do the following:

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** files, 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.



○ 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: ●●●●●●●●●●●●●

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:

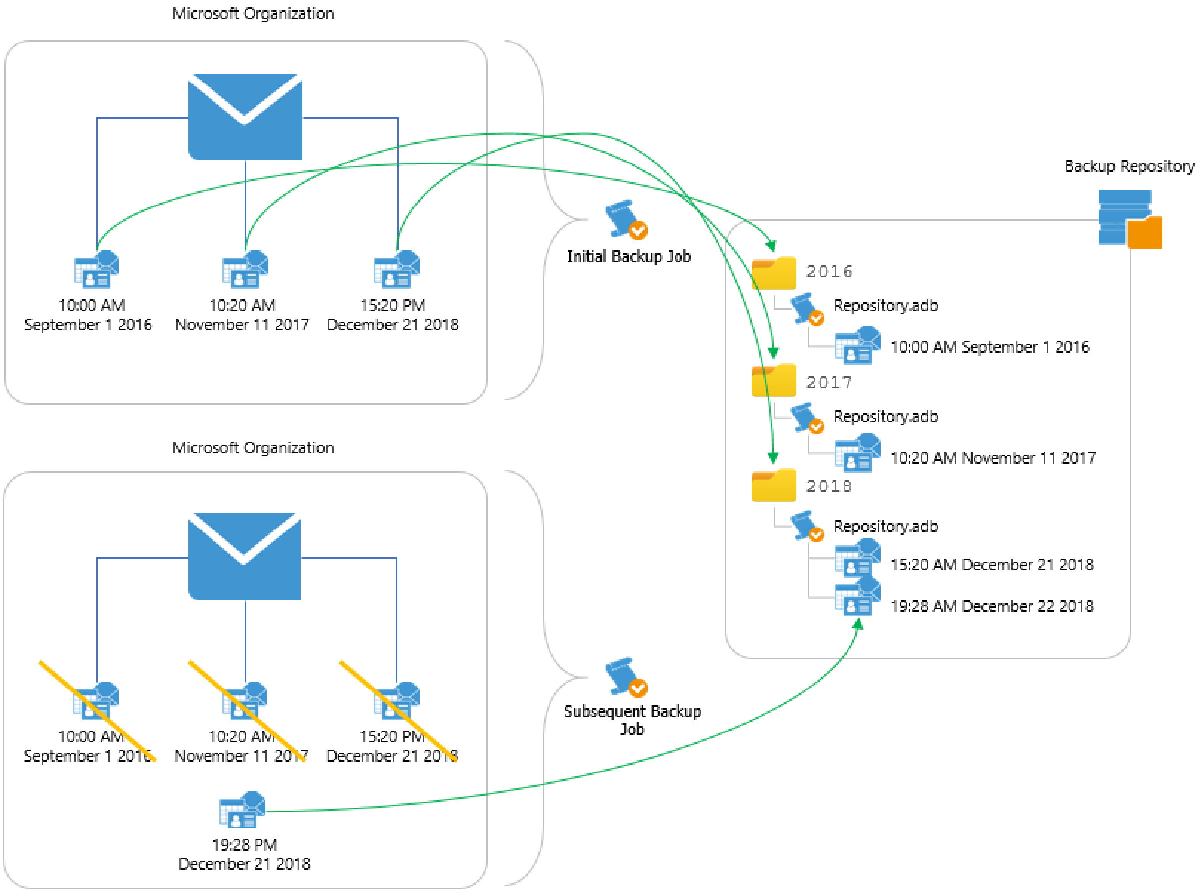
1. During the initial backup job session, Veeam Backup for Microsoft Office 365 will collect all data from the Microsoft organization and save the data to folders in the backup repository.

   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 items, Microsoft OneDrive for Business items and Microsoft Teams items.


Microsoft Organization
10:00 AM September 1 2016
10:20 AM November 11 2017
15:20 PM December 21 2018
Initial Backup Job
Backup Repository
2016
Repository.adb
10:00 AM September 1 2016
2017
Repository.adb
10:20 AM November 11 2017
2018
Repository.adb
15:20 AM December 21 2018
19:28 AM December 22 2018
Microsoft Organization
10:00 AM September 1 2016
10:20 AM November 11 2017
15:20 PM December 21 2018
19:28 PM December 21 2018
Subsequent Backup Job

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

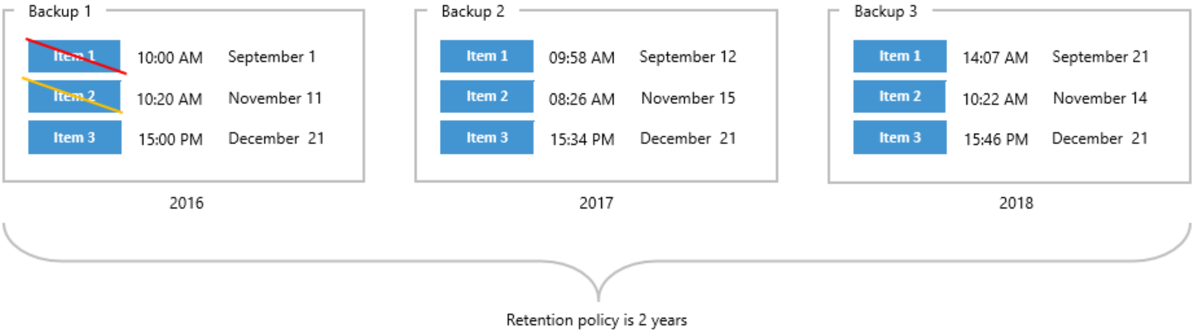
Data removal from backup repositories with the *Item-Level Retention* type occurs every time the creation time or last modification time of an item in a backup file goes beyond the retention coverage.

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. After that, Veeam Backup for Microsoft Office 365 completely removes such a repository from the hard drive.



Snapshot-Based Retention

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.

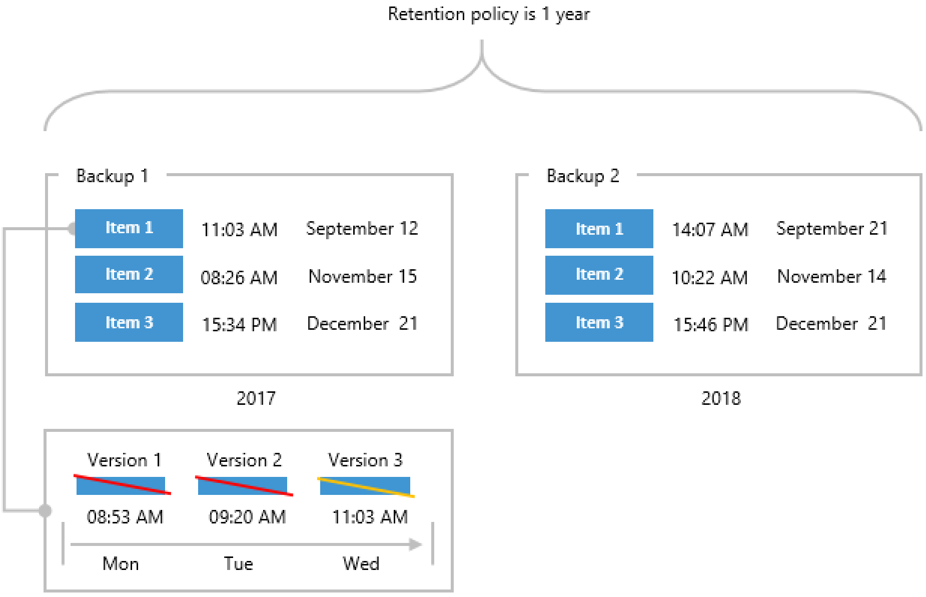
A different version means that the user could have changed any attribute in the production environment; for instance, he could have assigned a new category to an email in the mailbox. Such an action leads to a new version of an item to be created during the subsequent backup job session.

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.

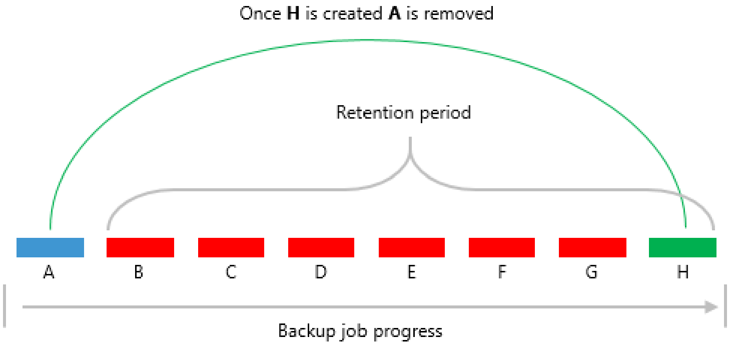
Such an approach repeats itself until no other items (or versions of items) left in a repository. After that, Veeam Backup for Microsoft Office 365 completely removes such a repository from the hard drive.



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* though *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*.

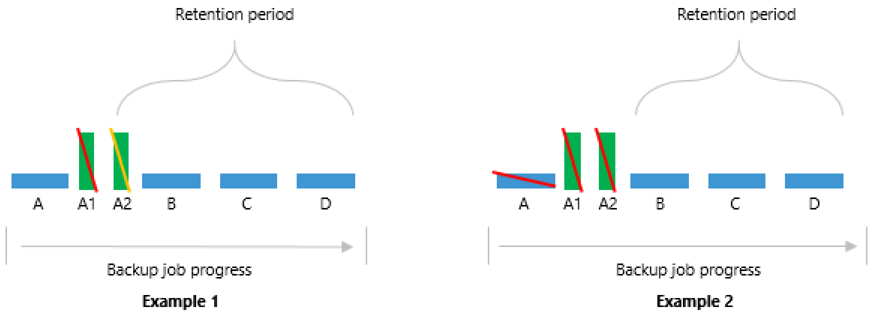


Removing Restore Points

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*).

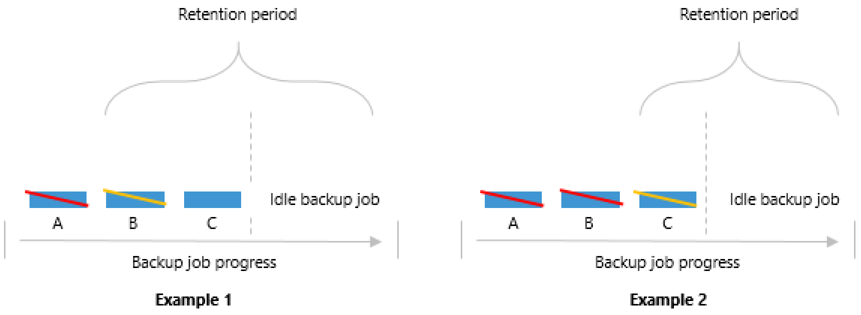


Backup Job Idleness

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, Microsoft OneDrive for Business and Microsoft Teams.



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.

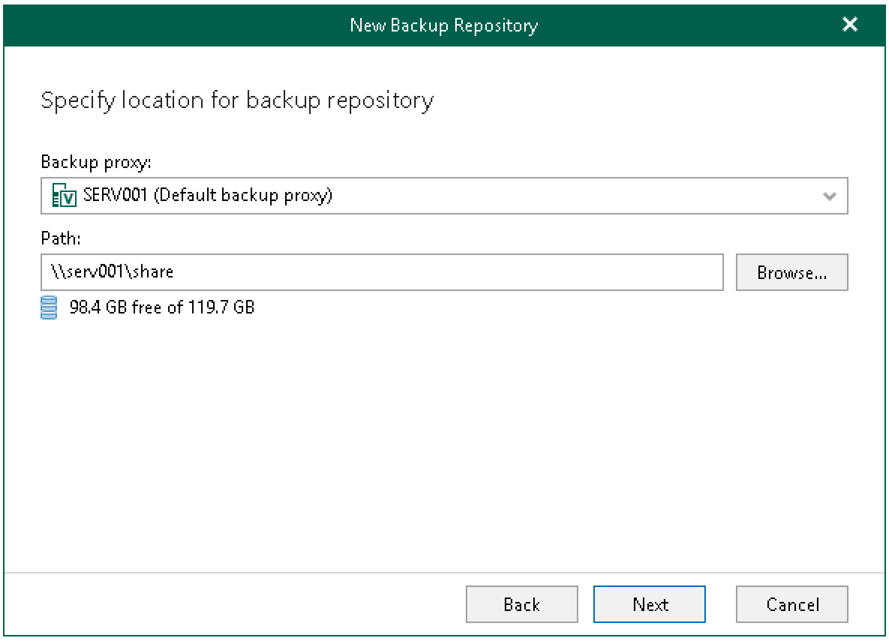
To access and use a shared folder, do the following:

- Configure NTFS permissions.
- Configure share permissions.

For more information, see this Veeam 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: SERV001 (Default backup proxy)

Path: \\serv001\share

98.4 GB free of 119.7 GB

Adding Backup Repositories

To add a new backup repository, do the following:

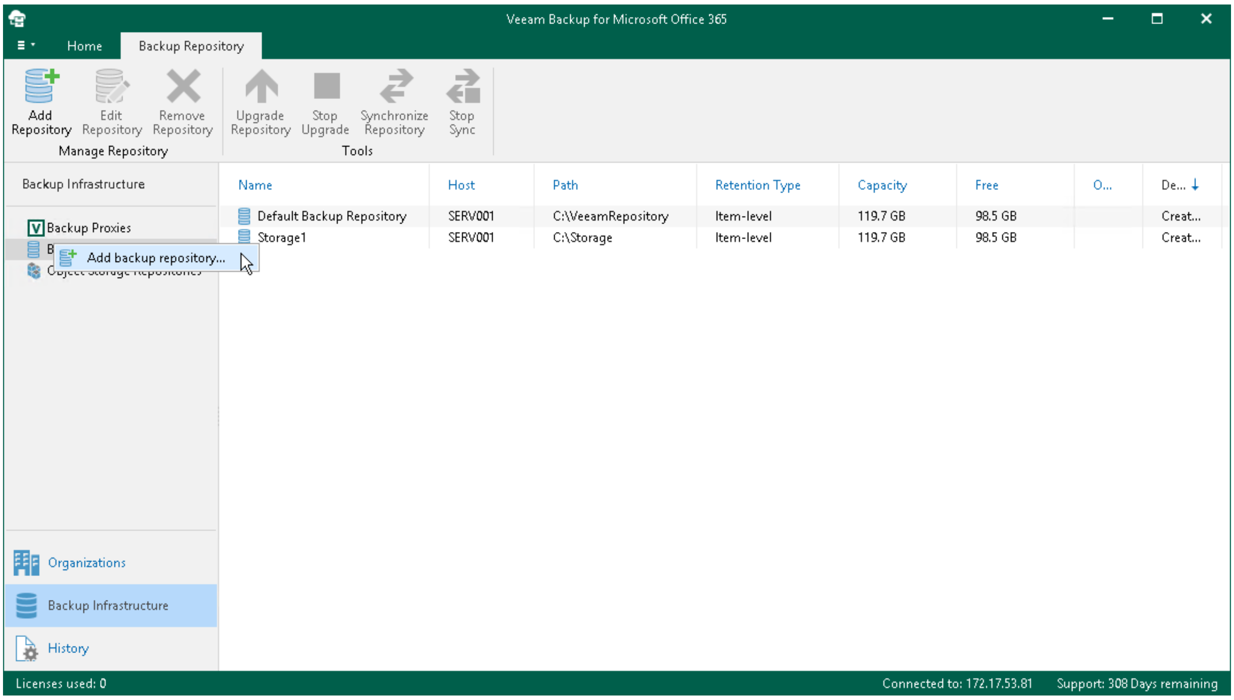
1. Launch the New Backup Repository wizard.
2. Specify a backup repository name.
3. Specify a backup proxy server.
4. Specify an object storage repository.
5. Specify retention policy settings.

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** on the ribbon.

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

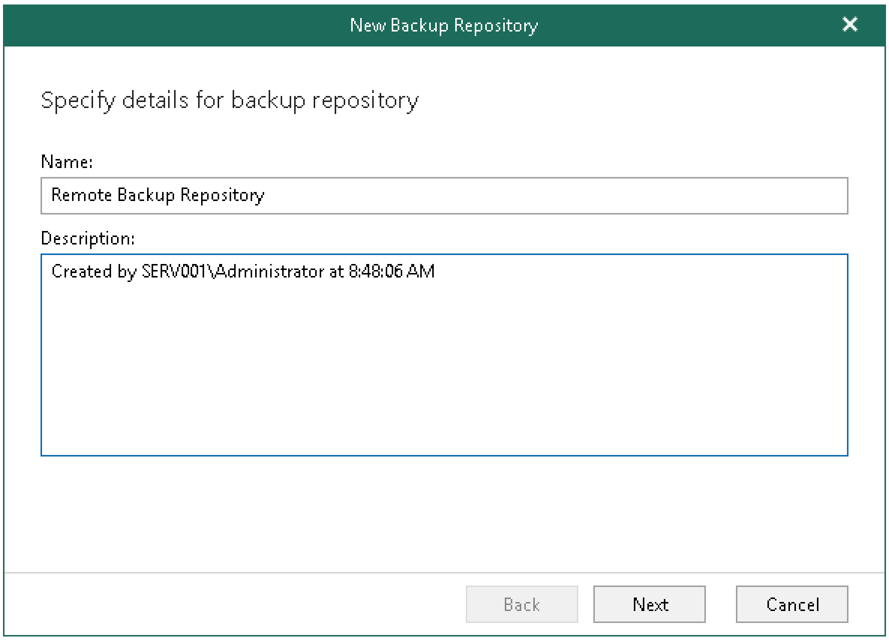


Name	Host	Path	Retention Type	Capacity	Free	O...	De...
Default Backup Repository	SERV001	C:\VeeamRepository	Item-level	119.7 GB	98.5 GB		Creat...
Storage1	SERV001	C:\Storage	Item-level	119.7 GB	98.5 GB		Creat...

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).



Specify details for backup repository

Name: Remote Backup Repository

Description: Created by SERV001\Administrator at 8:48:06 AM

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.

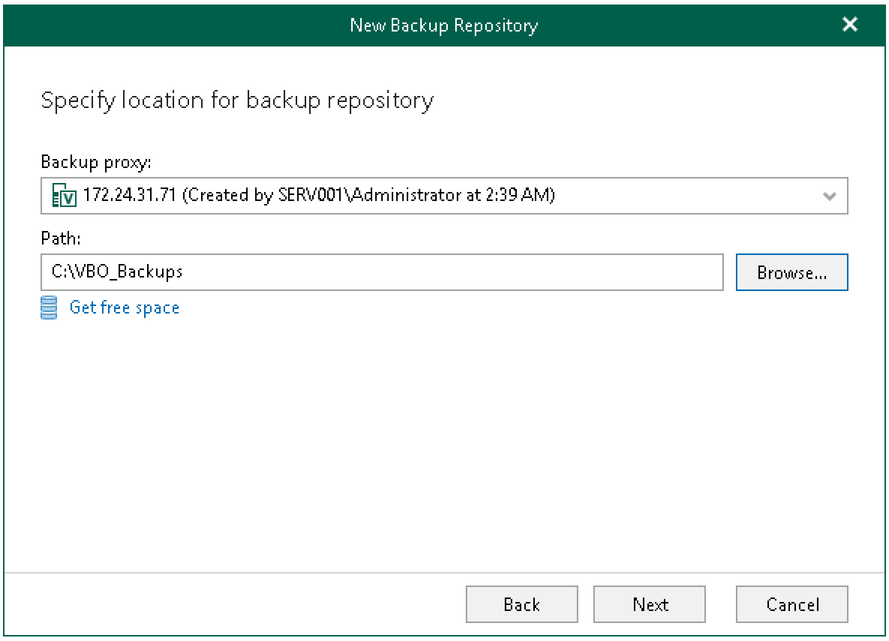
To specify a backup proxy server and directory for storing backups, do the following:

1. From 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 at the next step.

   When specifying a directory that already contains cache, at the next step, make sure to select the same exact object storage 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).



Backup proxy: 172.24.31.71 (Created by SERV001\Administrator at 2:39 AM)

Path: C:\VBO_Backups

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. From the drop-down list, select an object storage repository to which you want to offload your data.

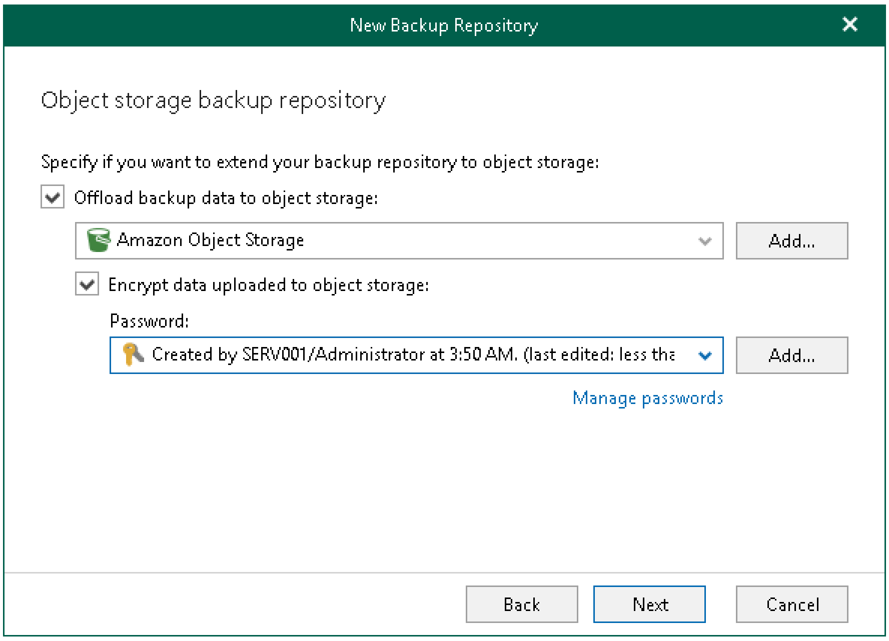
   Make sure that an object storage repository has been added to your environment in advance. Otherwise, click **Add** and follow the steps of the wizard, as described in Adding Object Storage Repositories.
3. To offload data encrypted, select **Encrypt data uploaded to object storage** and provide a password.

   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.



New Backup Repository

Object storage backup repository

Specify if you want to extend your backup repository to object storage:

☑ Offload backup data to object storage:

Amazon Object Storage

☑ Encrypt data uploaded to object storage:

Password:

Created by SERV001/Administrator at 3:50 AM. (last edited: less tha

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**

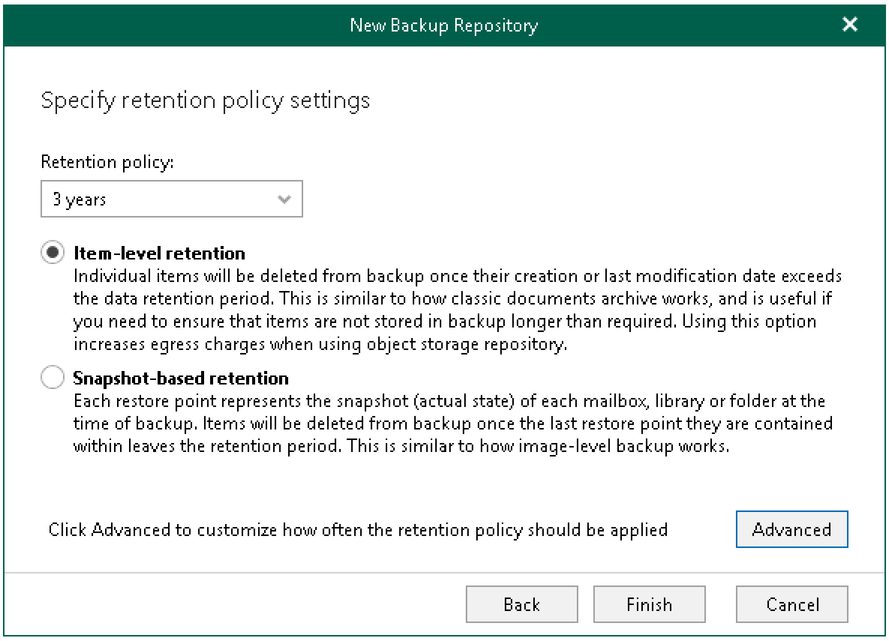
     Select this option if you want a retention policy to be applied on a daily basis and choose the time and day.
   - **Monthly at**

     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.



New Backup Repository

Specify retention policy settings

Retention policy:

3 years

● **Item-level retention**
Individual items will be deleted from backup once their creation or last modification date exceeds the data retention period. This is similar to how classic documents archive works, and is useful if you need to ensure that items are not stored in backup longer than required. Using this option increases egress charges when using object storage repository.

○ **Snapshot-based retention**
Each restore point represents the snapshot (actual state) of each mailbox, library or folder at the time of backup. Items will be deleted from backup once the last restore point they are contained within leaves the retention period. This is similar to how image-level backup works.

Click Advanced to customize how often the retention policy should be applied

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.

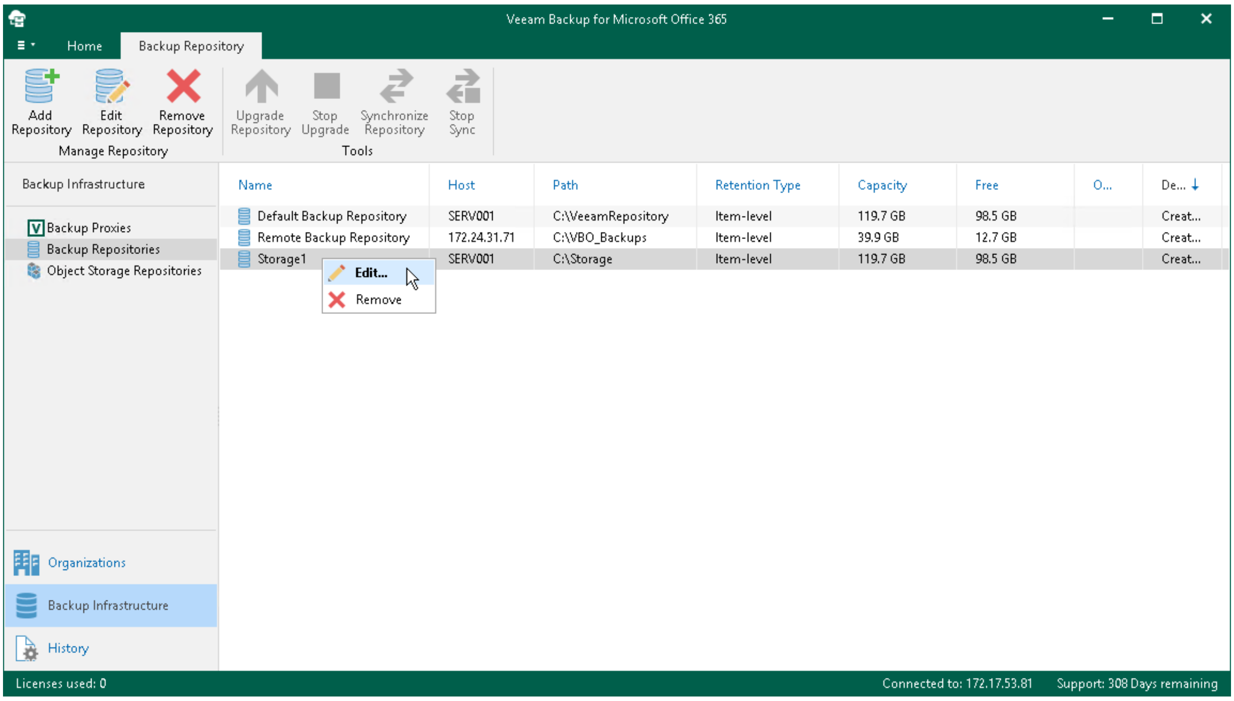
  For more information about retention policies, see Retention Policy.
- The **Edit** command is unavailable if a backup repository is out of date.

  For 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.



Name	Host	Path	Retention Type	Capacity	Free	O...	De...
Default Backup Repository	SERV001	C:\VeeamRepository	Item-level	119.7 GB	98.5 GB		Creat...
Remote Backup Repository	172.24.31.71	C:\VBO_Backups	Item-level	39.9 GB	12.7 GB		Creat...
Storage1	SERV001	C:\Storage	Item-level	119.7 GB	98.5 GB		Creat...

Licenses used: 0

Connected to: 172.17.53.81 Support: 308 Days remaining

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:

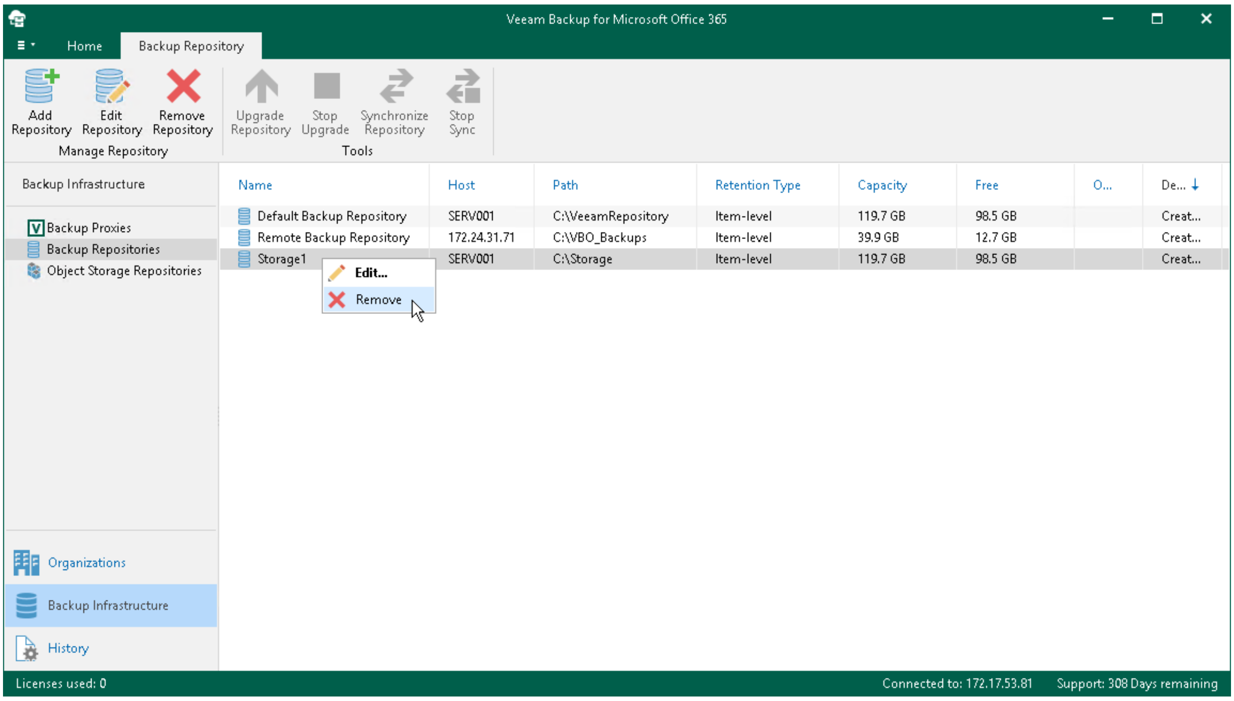
- When removing a backup repository, backup files that reside in such a repository will not be removed.
- The last remaining backup repository cannot be removed.
- When removing an extended backup repository that was synchronized, as described in Synchronizing Repositories, the backup data located in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

  To remove such a repository, remove (or re-map) all backup jobs that are mapped to this repository and then remove a repository. For more information on how to remove a backup job, see Removing Backup Job.

To remove a backup repository, do the following:

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**.



Name	Host	Path	Retention Type	Capacity	Free	O...	De...
Default Backup Repository	SERV001	C:\VeeamRepository	Item-level	119.7 GB	98.5 GB		Creat...
Remote Backup Repository	172.24.31.71	C:\VBO_Backups	Item-level	39.9 GB	12.7 GB		Creat...
Storage1	SERV001	C:\Storage	Item-level	119.7 GB	98.5 GB		Creat...

Upgrading Backup Repositories

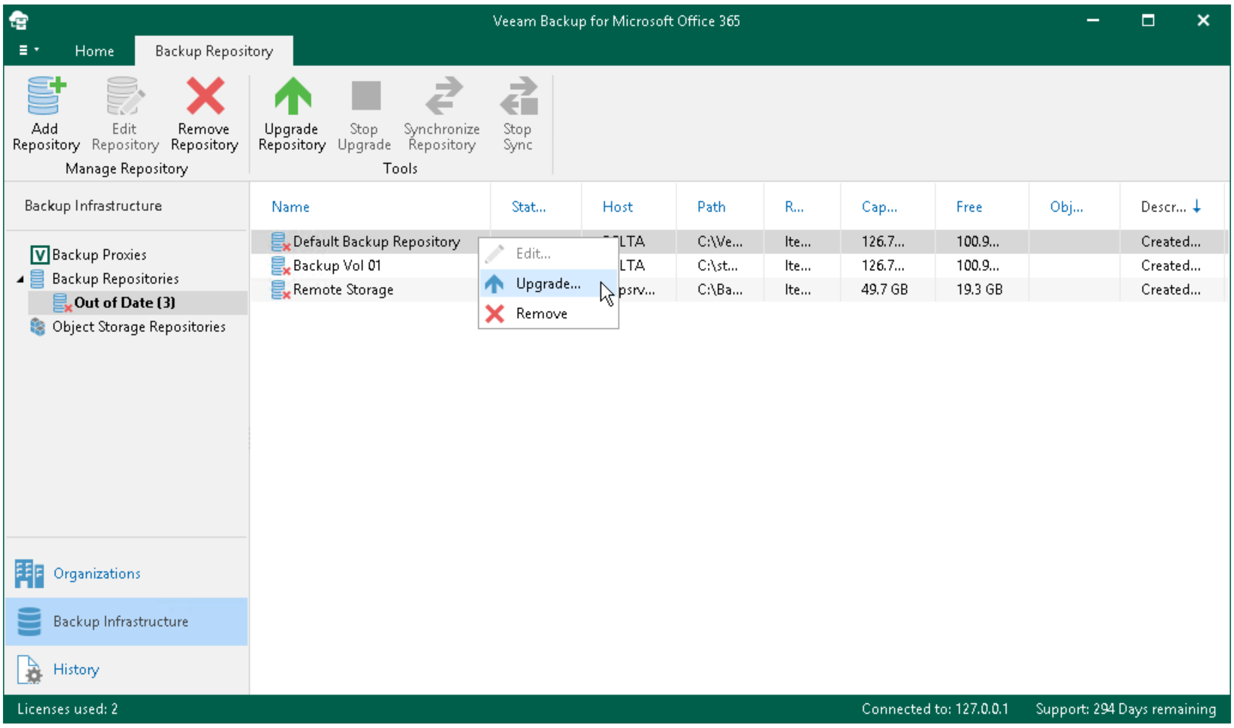
When you upgrade Veeam Backup for Microsoft Office 365 to a newer version, all backup repositories configured in your environment are marked as *Out of Date* and have to be upgraded manually.

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.



Name	Stat...	Host	Path	R...	Cap...	Free	Obj...	Descr... ↓
Default Backup Repository		LTA	C:\Ve...	Ite...	126.7...	100.9...		Created...
Backup Vol 01		LTA	C:\st...	Ite...	126.7...	100.9...		Created...
Remote Storage		psrv...	C:\Ba...	Ite...	49.7 GB	19.3 GB		Created...

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.

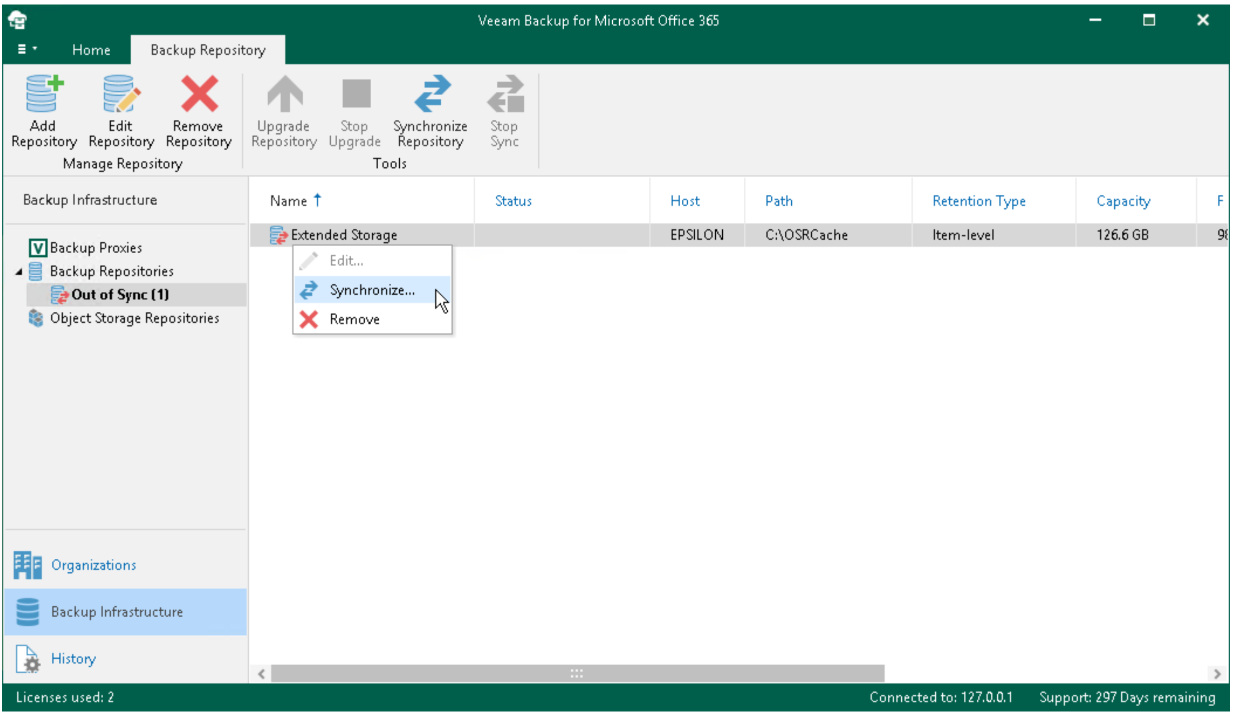
To synchronize cache between object storage and extended backup repositories, do the following:

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.



Name	Status	Host	Path	Retention Type	Capacity	F
Extended Storage		EPSILON	C:\OSRCache	Item-level	126.6 GB	9

Licenses used: 2

Connected to: 127.0.0.1

Support: 297 Days remaining

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.

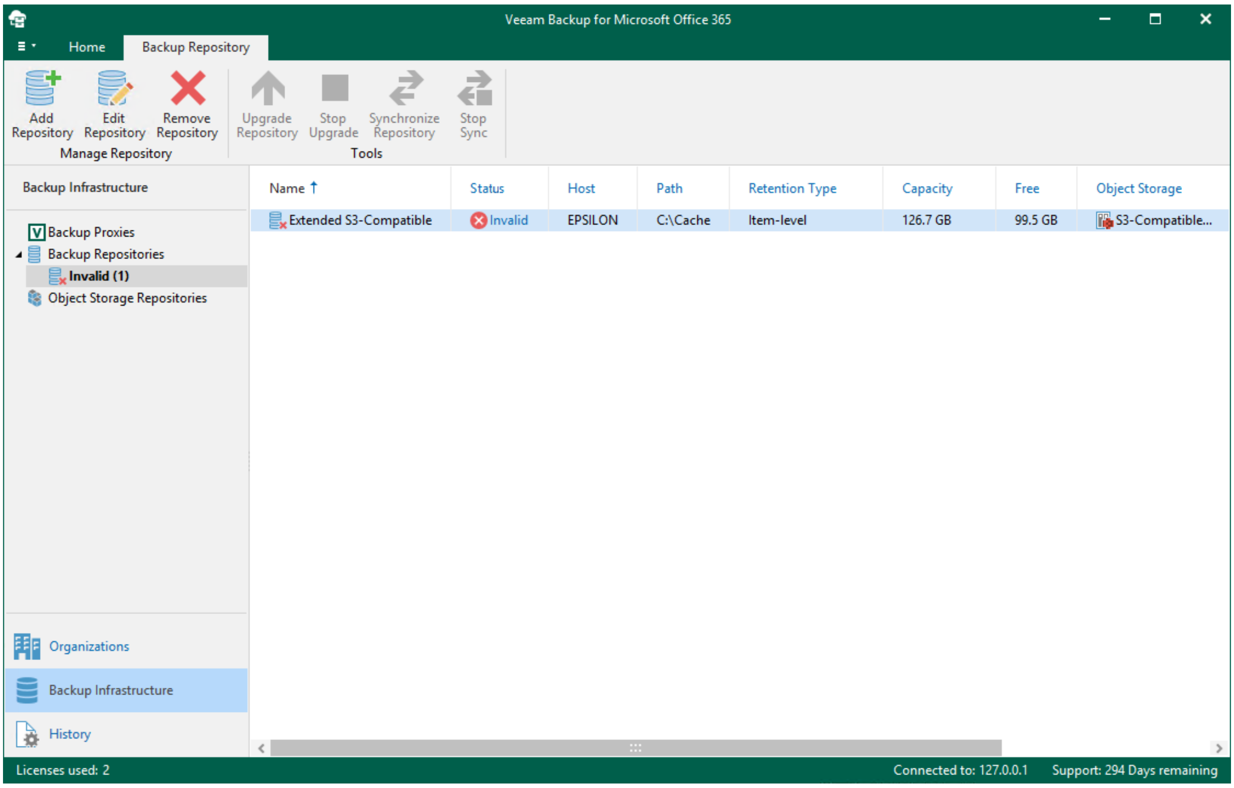
- A trusted certificate for S3 Compatible object storage has been changed.

- 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.



Name ↑	Status	Host	Path	Retention Type	Capacity	Free	Object Storage
Extended S3-Compatible	Invalid	EPSILON	C:\Cache	Item-level	126.7 GB	99.5 GB	S3-Compatible...

Licenses used: 2

Connected to: 127.0.0.1

Support: 294 Days remaining

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 Microsoft Azure Blob storage, see this Microsoft article.

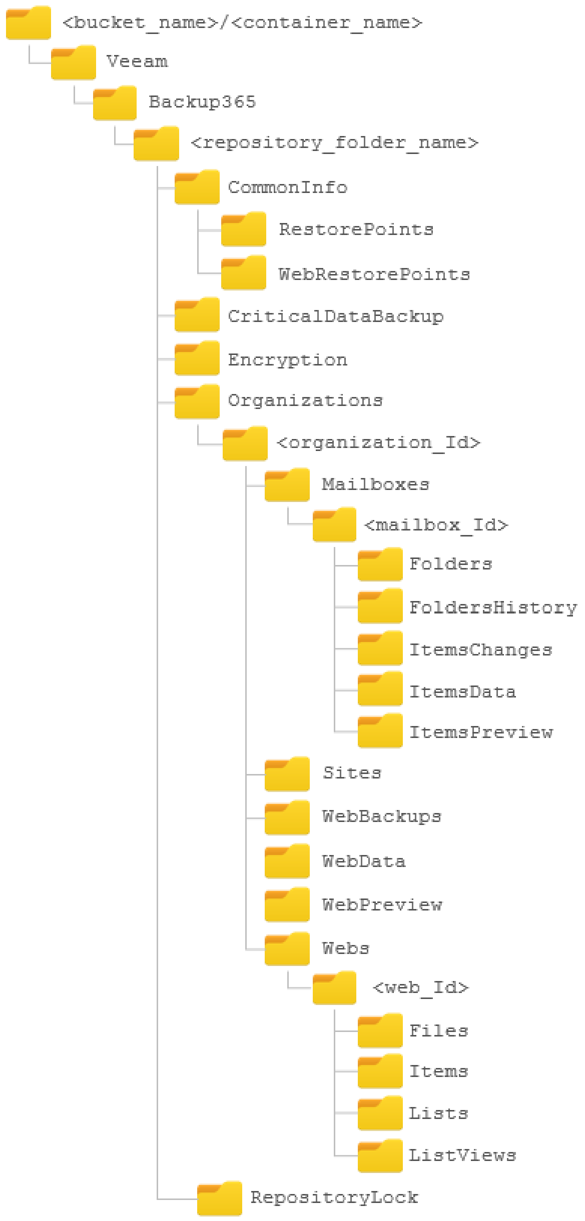
- IBM Cloud Object Storage

  For more information about IBM Cloud Object Storage, see this IBM article.

To back up data to object storage, you can 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.



```
<bucket_name>/<container_name>
  Veeam
    Backup365
      <repository_folder_name>
        CommonInfo
          RestorePoints
          WebRestorePoints
        CriticalDataBackup
        Encryption
        Organizations
          <organization_Id>
            Mailboxes
              <mailbox_Id>
                Folders
                FoldersHistory
                ItemsChanges
                ItemsData
                ItemsPreview
            Sites
            WebBackups
            WebData
            WebPreview
            Webs
              <web_Id>
                Files
                Items
                Lists
                ListViews
        RepositoryLock
```

Directory	Description
<bucket_name/container_name>	A bucket or container name. Buckets and containers must be created in advance using the cloud provider tools. Veeam Backup for Microsoft Office 365 does not support creating new buckets or containers.
<bucket_name/container_name>/Veeam/Backup365/	A set of mandatory folders created by Veeam Backup for Microsoft Office 365.

Directory	Description
<repository_folder_name>	A repository folder that you create when adding a new object storage repository. For more information on how to add a new object storage repository, see Adding Object Storage Repositories.
<repository_folder_name>/CommonInfo	Contains the following directories and blob files: • *[Directory] RestorePoints*. Contains information about available restore points for Microsoft Exchange. • *[Directory] WebRestorePoints*. 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. • *[Blob file] Organizations*. Contains a list of backed-up organizations. • *[Blob file] RepositoryConfig*. Contains extended backup repository configuration such as the retention type and other auxiliary information.
<repository_folder_name>/CriticalDataBackup	Contains identical copies of the following blob files: • *[Blob file] Organizations*. Contains a list of backed-up organizations. • *[Blob file] RepositoryConfig*. Contains extended backup repository configuration such as the retention type and other auxiliary information. • *[Blob file] BackupKeys*. Contains information about the encryption keys that you might have set during extension of a backup repository with object storage.
<repository_folder_name>/Encryption	Contains a *BackupKeys* blob file that holds information about the encryption keys that you might have set during extension of a backup repository with object storage. For more information on how to extend a backup repository with object storage, see Specify Object Storage Repository.

Directory	Description
<repository_folder_name>/Organizations	The root folder that contains backed-up Microsoft organizations. Each organization is kept in its own folder with a unique identification number.
Organizations/<organization_Id>	The *<organization_Id>* directory contains the following blob files: • *AccountMailbox*. Contains information required to load the backup contents into the Veeam Explorer for Microsoft Exchange scope. • AccountWeb. Contains information required to load the backup contents into the Veeam Explorer for Microsoft SharePoint scope.
<organization_Id>/Mailboxes/<mailbox_Id>	The *Mailboxes* directory contains backed-up Exchange mailboxes. Each mailbox is saved under a unique identification number to the <mailbox_Id> directory. The *<mailbox_Id>* directory contains the following directories: • *Folders.* Contains backed-up Exchange folders such as *Inbox*, *Drafts*, *Sent Items*, and so on. • *FoldersHistory*. 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 *FoldersHistory* directory. • *ItemsChanges.* Contains incremental backup data. • *ItemsData.* Contains blob data of the backed-up Exchange messages. For example, attachments are saved to this folder. • *ItemsPreview.* 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.

Directory	Description
<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: • *Files.* Contains files of your SharePoint site. • *Items.* Contains items such as those located under the *Subsites* and *Content* folders for SharePoint, and users folders for OneDrive. • *Lists.* Contains SharePoint lists. • *ListViews.* 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 Object 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:

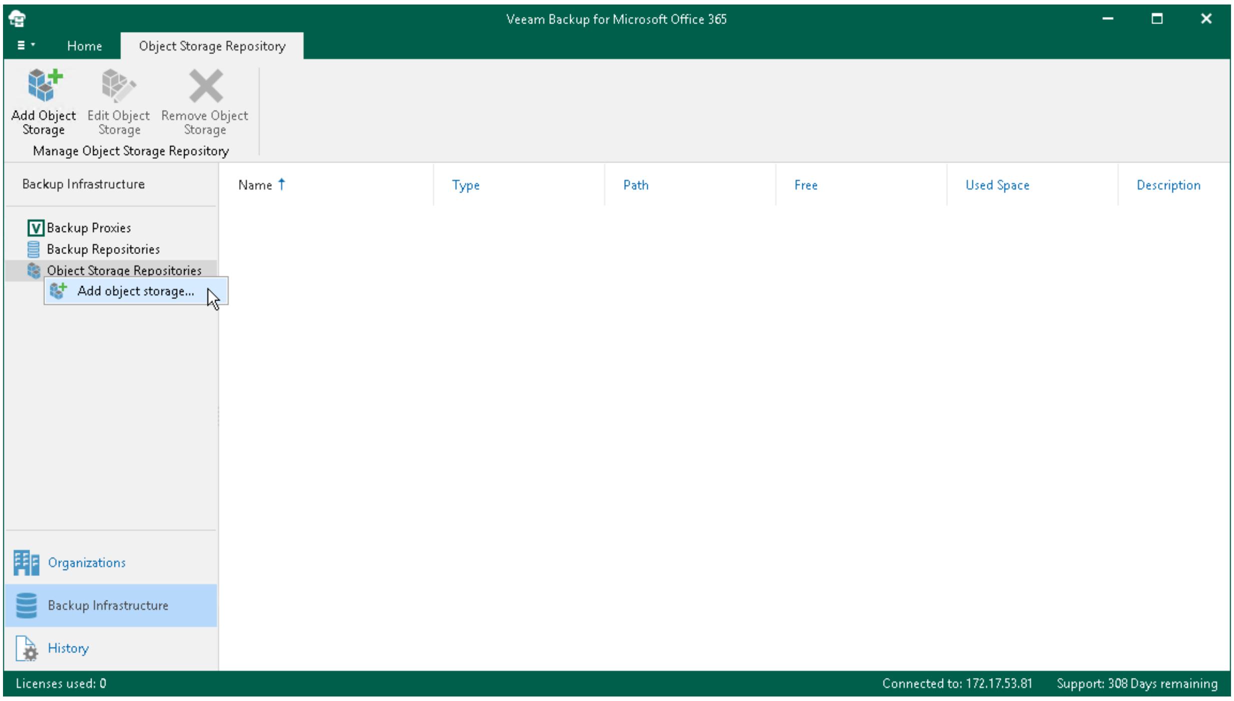
1. Launch the New Object Storage Repository wizard.
2. Specify an object storage repository name.
3. Select an object storage type.
4. Specify an object storage service point and account.
5. Specify an object storage bucket.

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** on the ribbon.

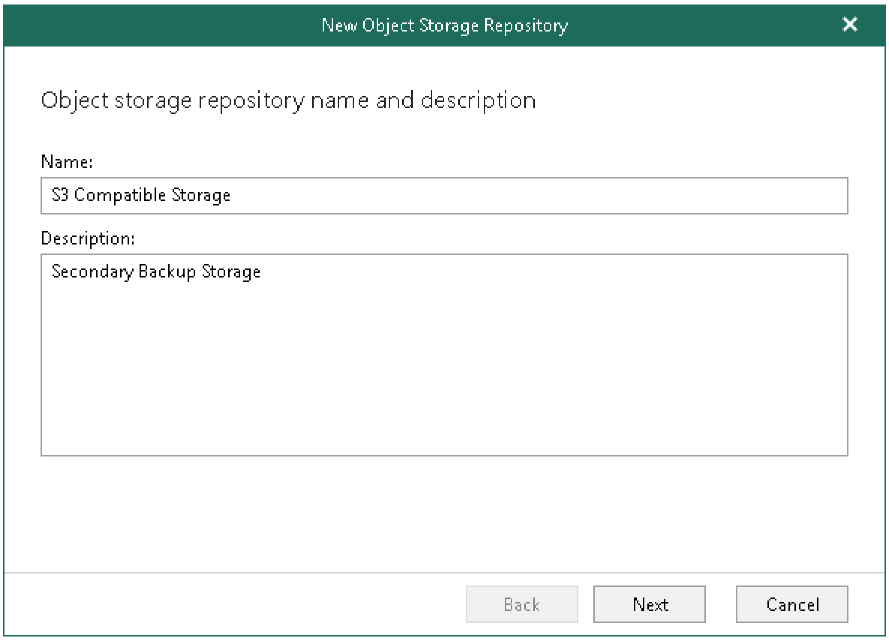
   Alternatively, in the inventory pane, right-click the **Object Storage Repositories** node and select **Add object storage**.



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).

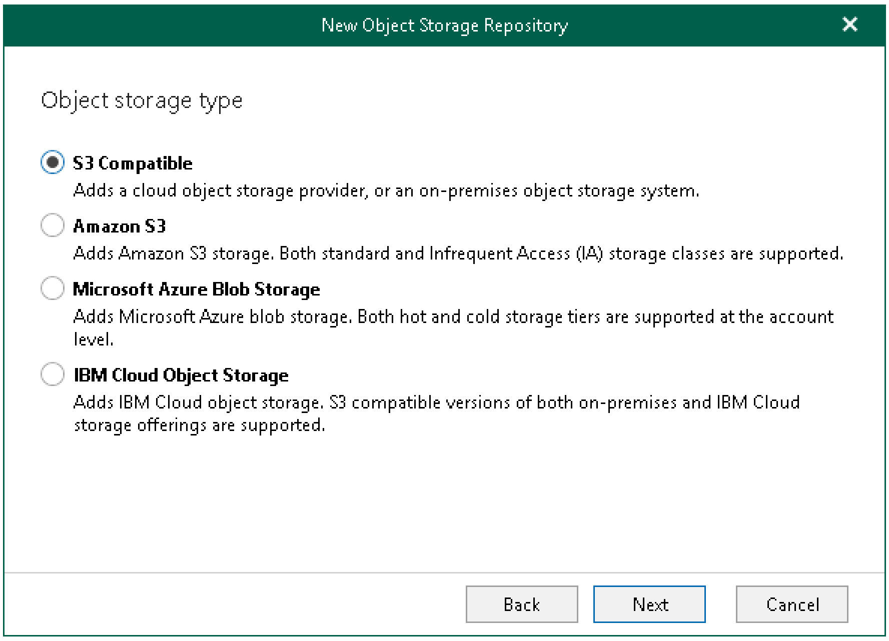

New Object Storage Repository
Object storage repository name and description
Back
Next
Cancel

Name: S3 Compatible Storage

Description: Secondary Backup Storage

Step 3. Select Object Storage Type

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



Object storage type

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

○ **Amazon S3**
Adds Amazon S3 storage. 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.

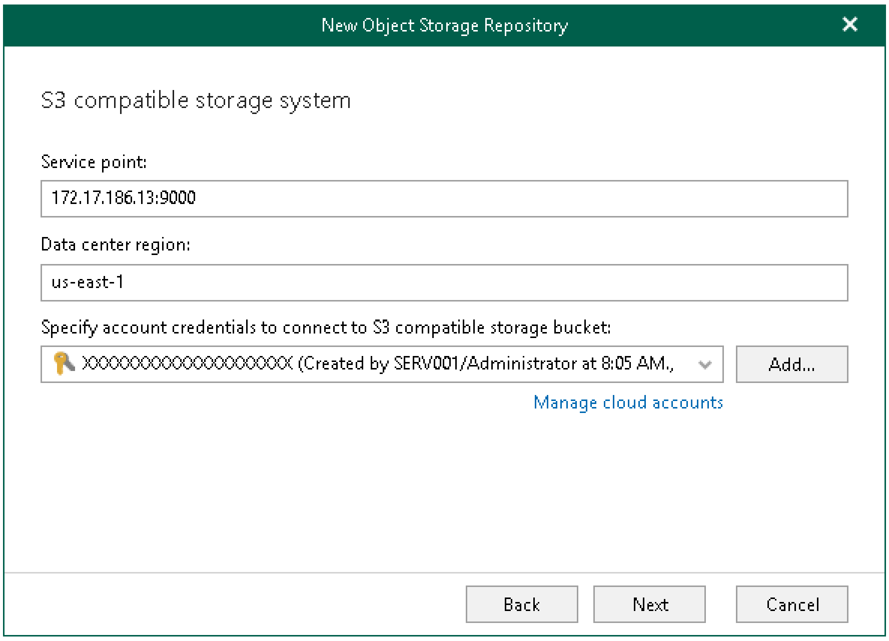
○ **IBM Cloud Object Storage**
Adds IBM Cloud object storage. S3 compatible versions of both on-premises and IBM Cloud storage offerings are supported.

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. From the **Specify account credentials to connect to S3 compatible storage bucket** drop-down list, select user credentials to access your S3 Compatible object storage.

   If you already have a credentials record that was configured beforehand, select such a record in the drop-down list. Otherwise, click **Add** and provide your access and secret keys, as described in Adding S3 Compatible and IBM Storage Access Key. You can also click **Manage cloud accounts** to manage existing credentials records.



New Object Storage Repository

S3 compatible storage system

Service point: 172.17.186.13:9000

Data center region: us-east-1

Specify account credentials to connect to S3 compatible storage bucket: XXXXXXXXXXXXXXXXXXXX (Created by SERV001/Administrator at 8:05 AM.,

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. From the **Bucket** drop-down list, select a bucket.

   Make sure that the bucket you want to use to store your data was created in advance; Veeam Backup for Microsoft Office 365 does not support creating new buckets.

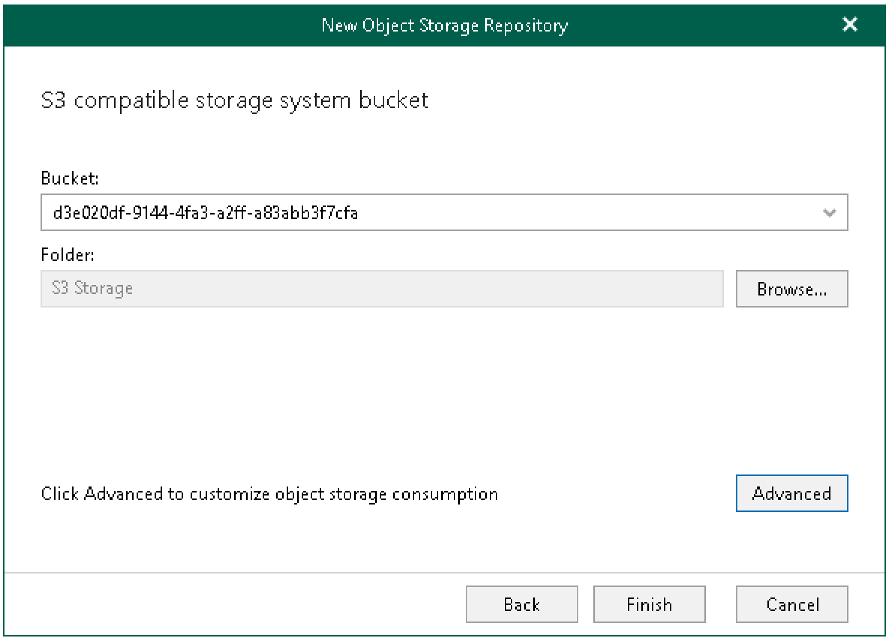
2. In the **Folder** field, select a folder to which you want to map your object storage repository, and which will be used to store backups.

   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: d3e020df-9144-4fa3-a2ff-a83abb3f7cfa

Folder: S3 Storage

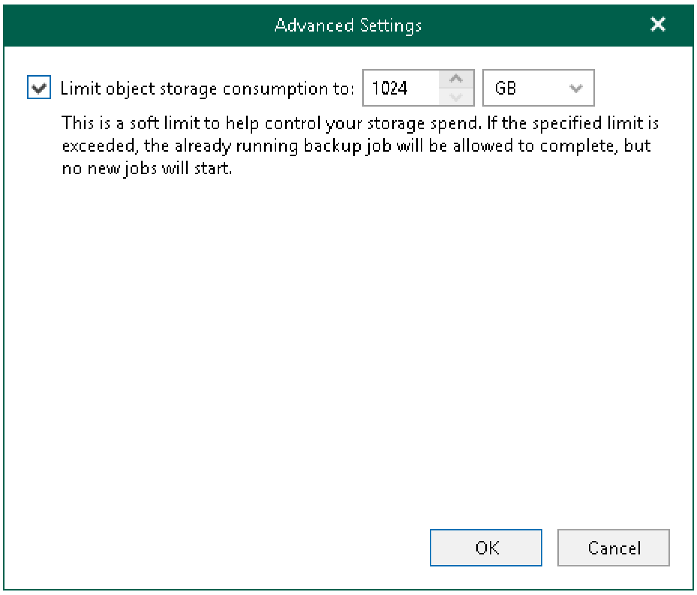
Click Advanced to customize object storage consumption

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**.



☑ 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.

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:

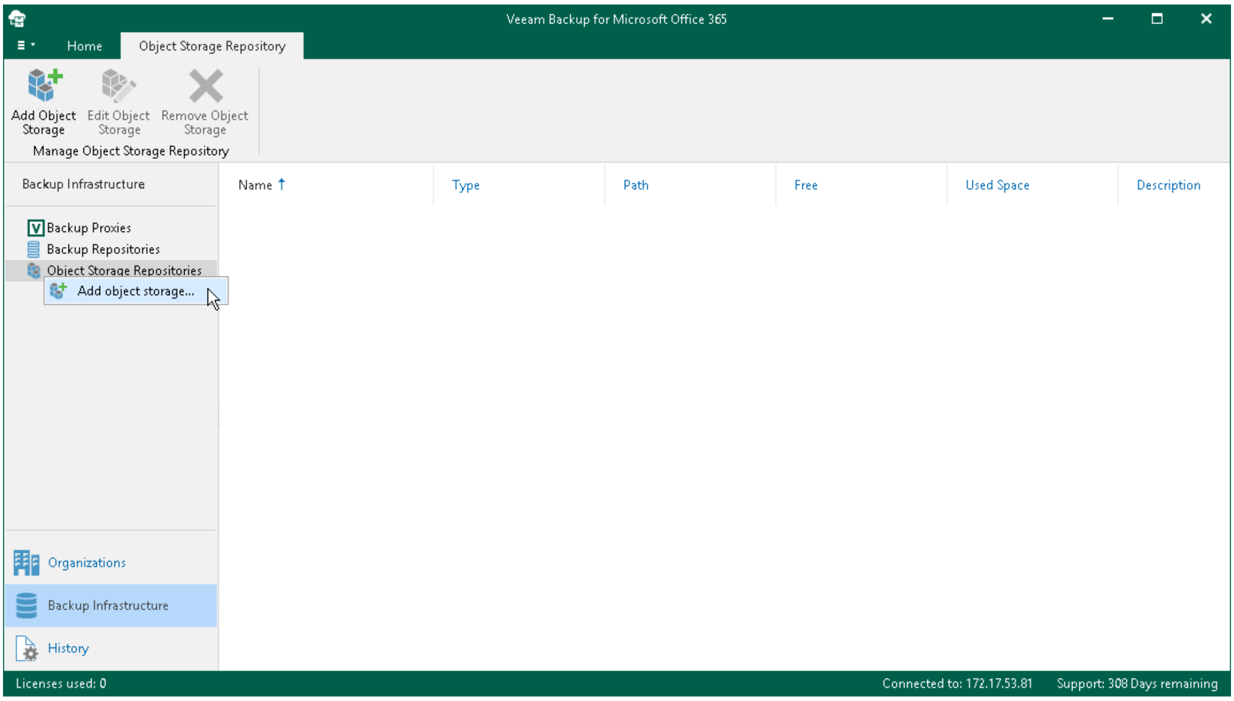
1. Launch the New Object Storage Repository wizard.
2. Specify an object storage repository name.
3. Select an object storage type.
4. Specify an object storage account.
5. Specify object storage settings.

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** on the ribbon.

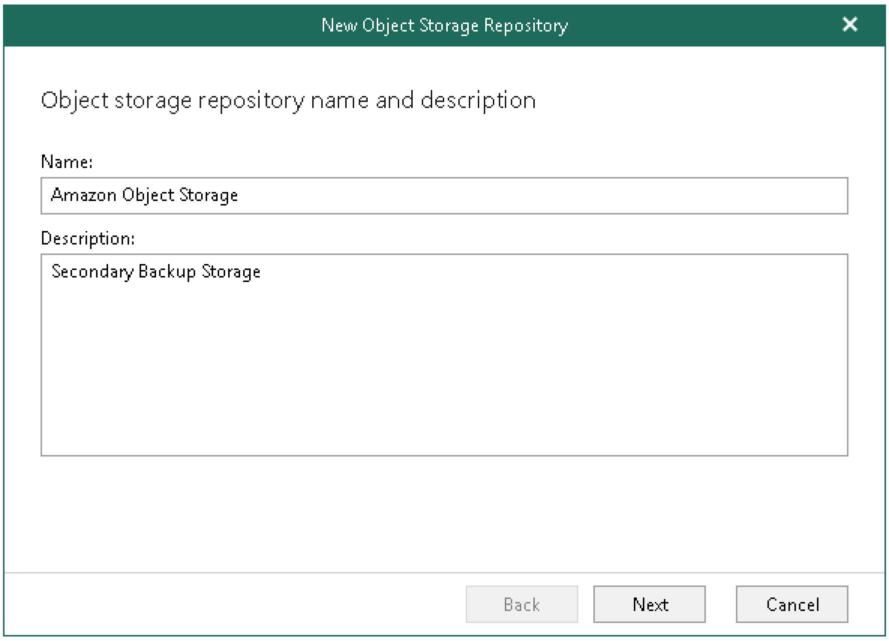
   Alternatively, in the inventory pane, right-click the **Object Storage Repositories** node and select **Add object storage**.



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

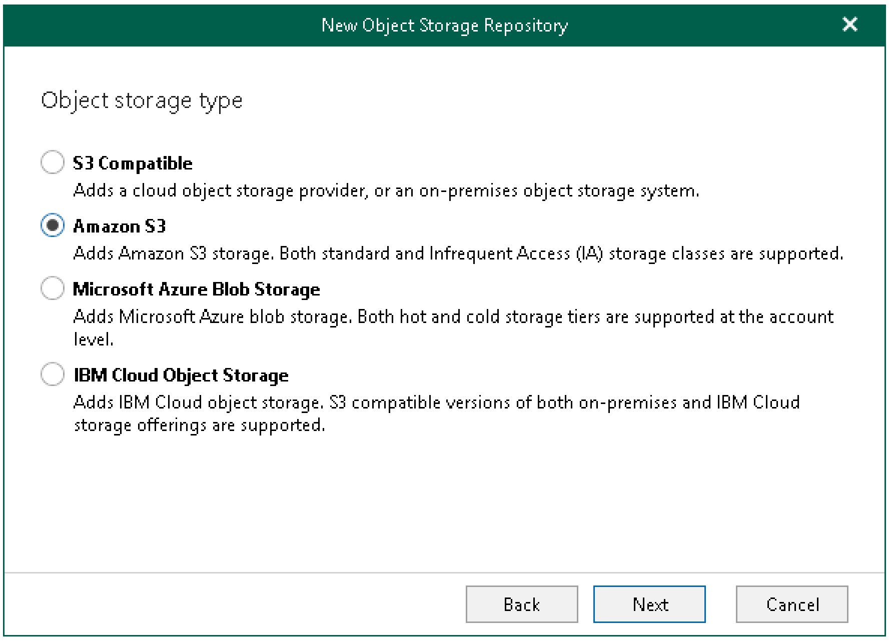
Object storage repository name and description

Name: Amazon Object Storage

Description: Secondary Backup Storage

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.

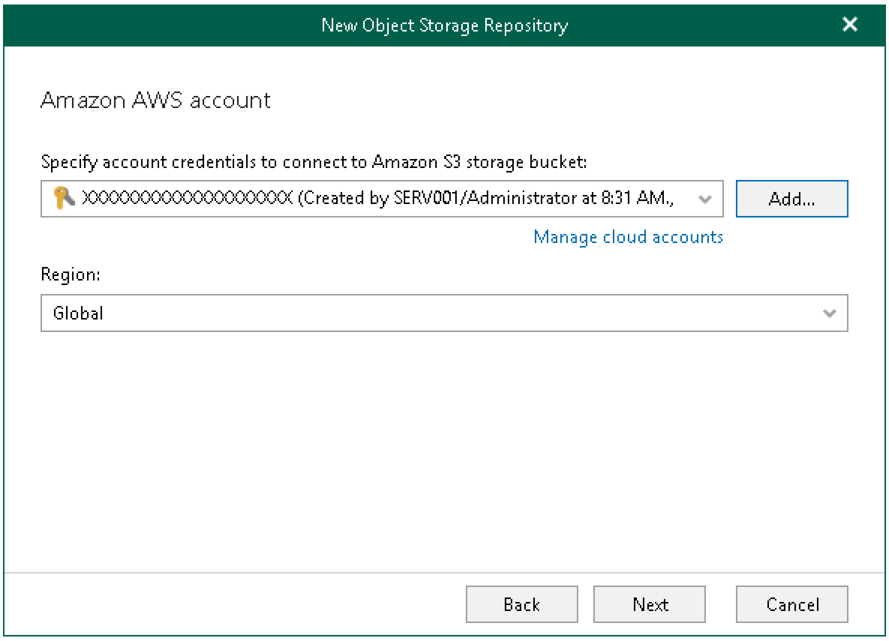
Step 4. Specify Object Storage Account

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

1. From the **Specify account credentials to connect to Amazon S3 storage bucket** drop-down list, select user credentials to access your Amazon S3 object storage.

   If you already have a credentials record that was configured beforehand, select such a record in the drop-down list. Otherwise, click **Add** and provide your access and secret keys, as described in Adding Amazon AWS Access Key. You can also click **Manage cloud accounts** to manage existing credentials records.

2. From the **Region** drop-down list, select a data center region.



New Object Storage Repository

Amazon AWS account

Specify account credentials to connect to Amazon S3 storage bucket: XXXXXXXXXXXXXXXXXXXX (Created by SERV001/Administrator at 8:31 AM.,

Region: Global

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.

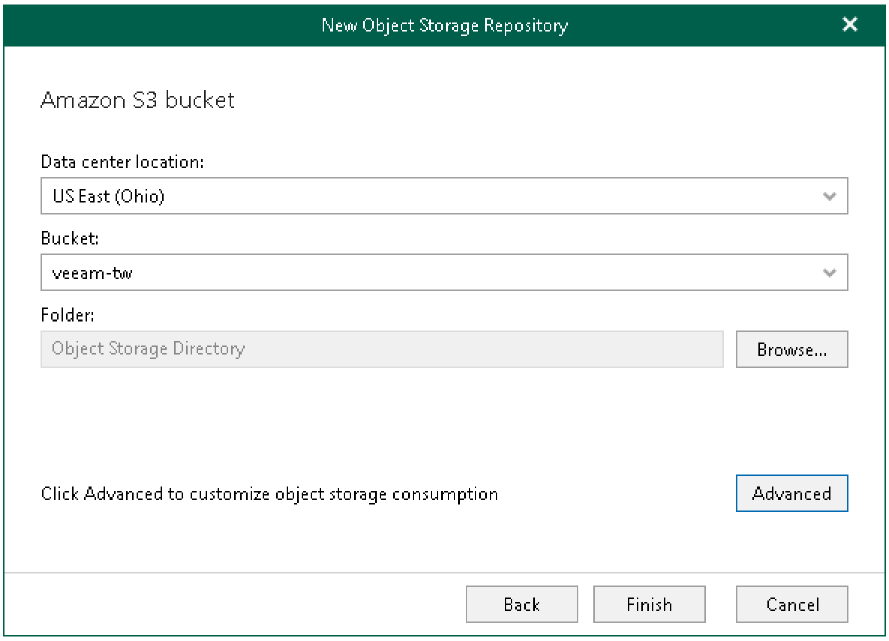
1. From the **Data center location** drop-down list, select a region that contains available buckets.
2. From the **Bucket** drop-down list, select a bucket.

   Make sure that the bucket you want to use to store your data was created in advance; Veeam Backup for Microsoft 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.
4. 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-tw

Folder: Object Storage Directory

Browse...
Click Advanced to customize object storage consumption
Advanced
Back
Finish
Cancel

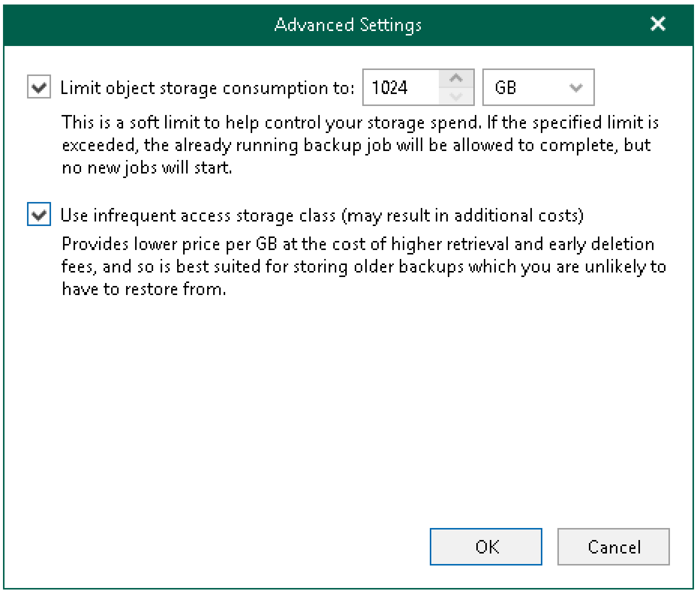
5. In the **Advanced Settings** window, do the following:

   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. 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.

   d. 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.

Adding Microsoft Azure Blob Object Storage Repositories

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

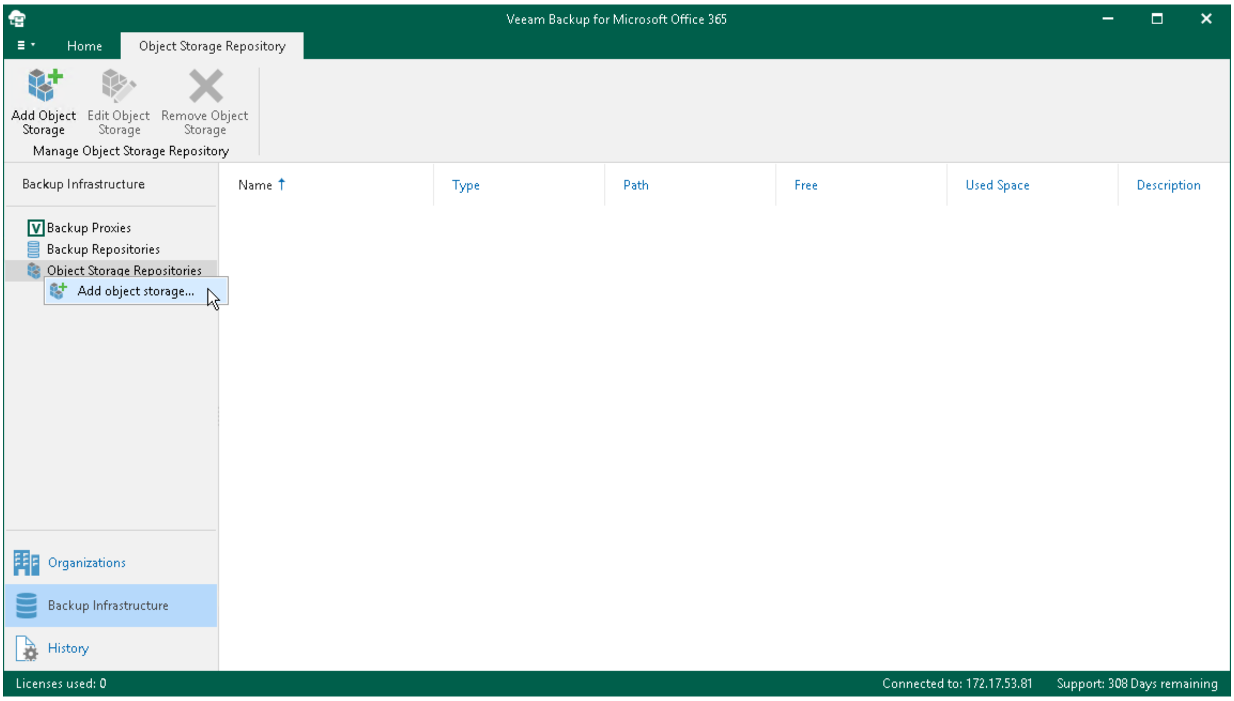
1. Launch the New Object Storage Repository wizard.
2. Specify an object storage repository name.
3. Select an object storage type.
4. Specify an object storage account.
5. Specify object storage settings.

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** on the ribbon.

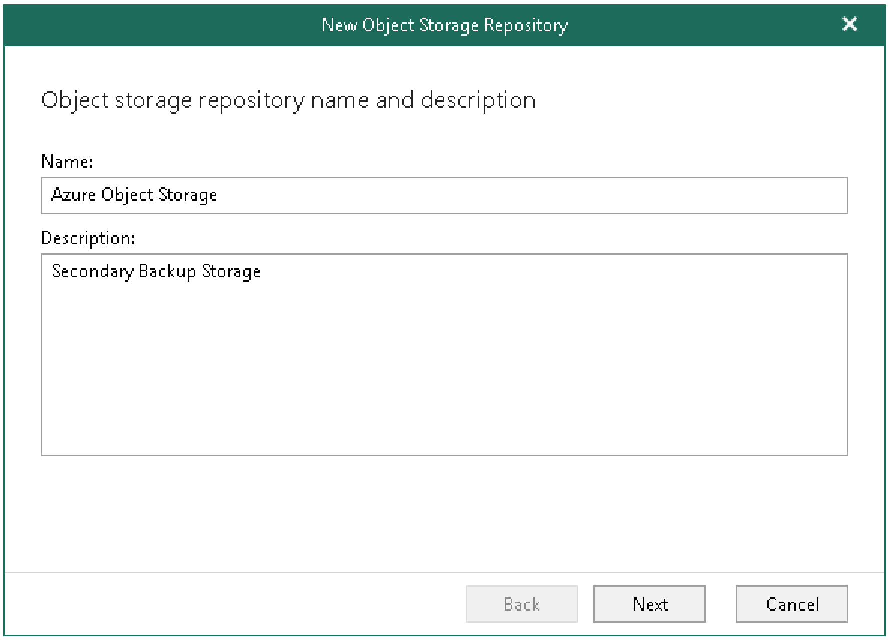
   Alternatively, in the inventory pane, right-click the **Object Storage Repositories** node and select **Add object storage**.



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).

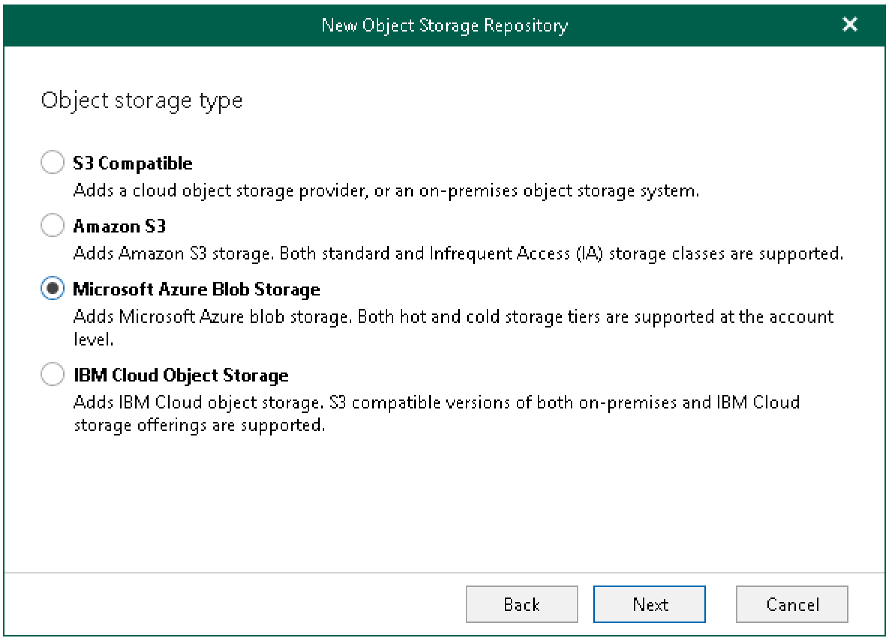

New Object Storage Repository
Object storage repository name and description

Name: Azure Object Storage

Description: Secondary Backup Storage

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.

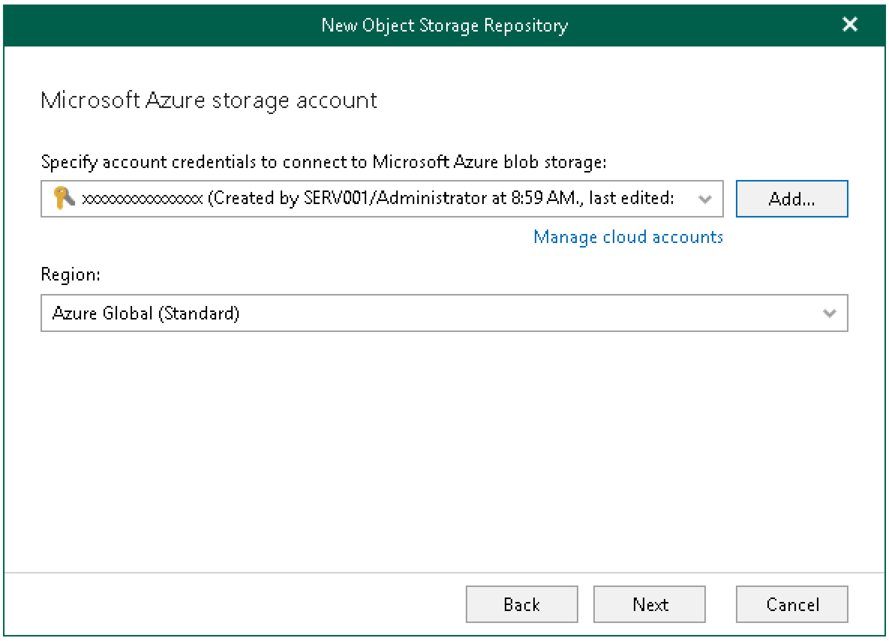
Step 4. Specify Object Storage Account

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

1. From the **Specify account credentials to connect to Microsoft Azure blob storage** drop-down list, select user credentials to access your Azure Blob storage.

   If you already have a credentials record that was configured beforehand, select such a record 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. From the **Region** drop-down list, select a region.



New Object Storage Repository

Microsoft Azure storage account

Specify account credentials to connect to Microsoft Azure blob storage: xxxxxxxxxxxxxxx (Created by SERV001/Administrator at 8:59 AM., last edited:

Region: Azure Global (Standard)

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. From the **Container** drop-down list, select an Azure container.

   Make sure that the container you want to use to store your data was created in advance; Veeam Backup for Microsoft Office 365 does not support creating new containers.

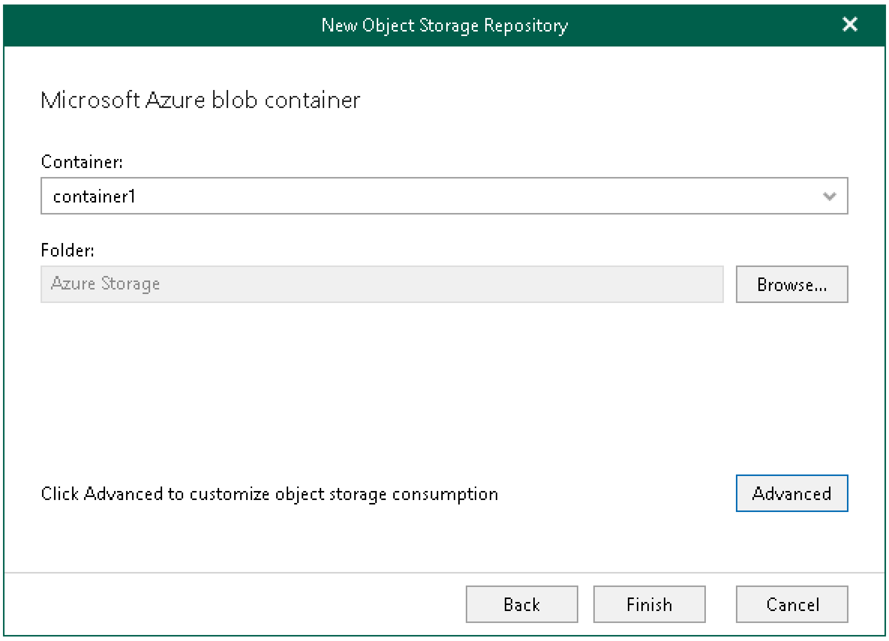
2. In the **Folder** field, select a cloud folder to which you want to map your object storage repository, and which will be used to store offloaded data.

   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

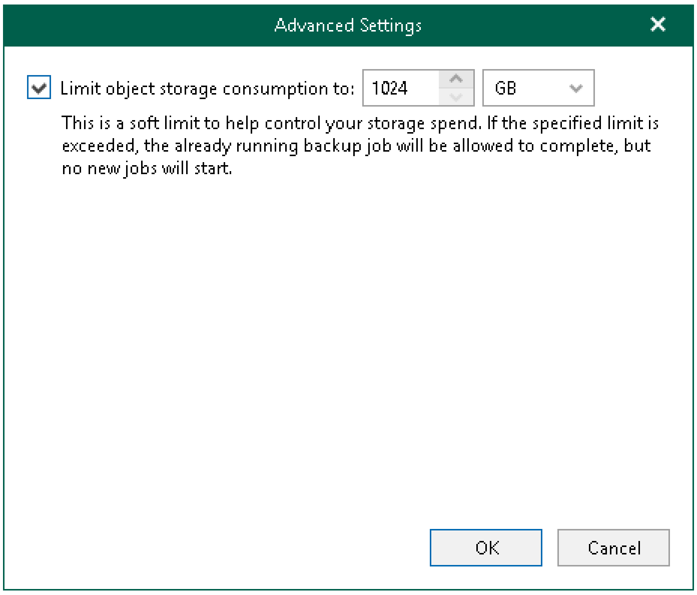
Click Advanced to customize object storage consumption

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**.



☑ 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.

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:

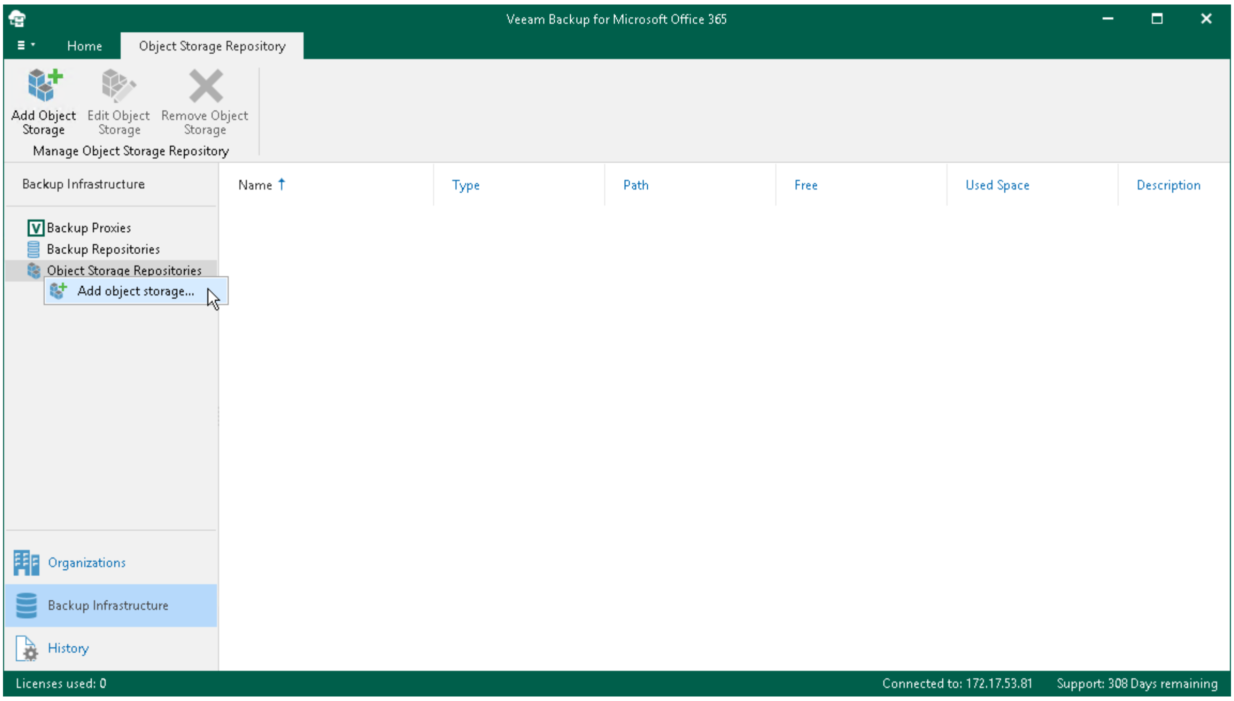
1. Launch the New Object Storage Repository wizard.
2. Specify an object storage repository name.
3. Select an object storage type.
4. Specify an object storage service point and account.
5. Specify object storage bucket.

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** on the ribbon.

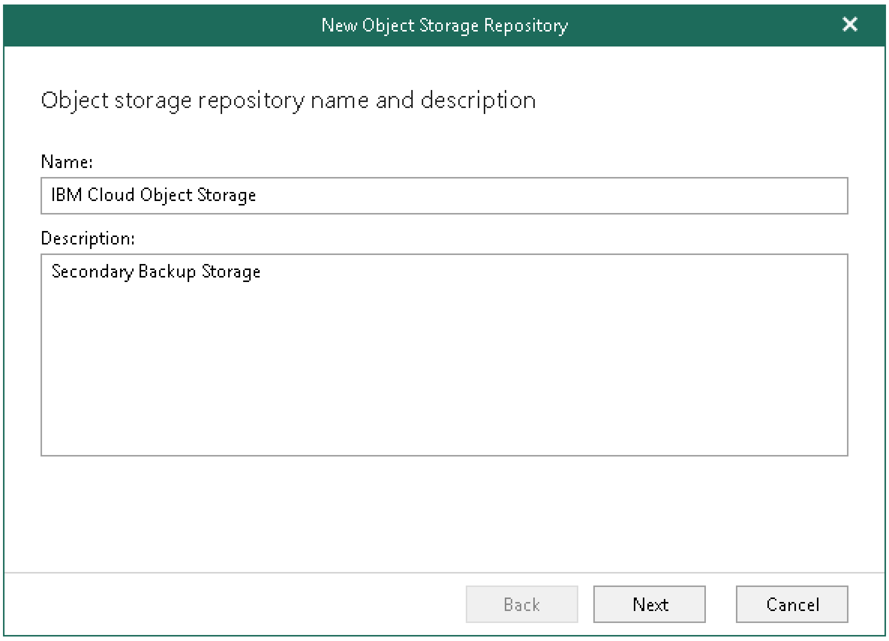
   Alternatively, in the inventory pane, right-click the **Object Storage Repositories** node and select **Add object storage**.



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).

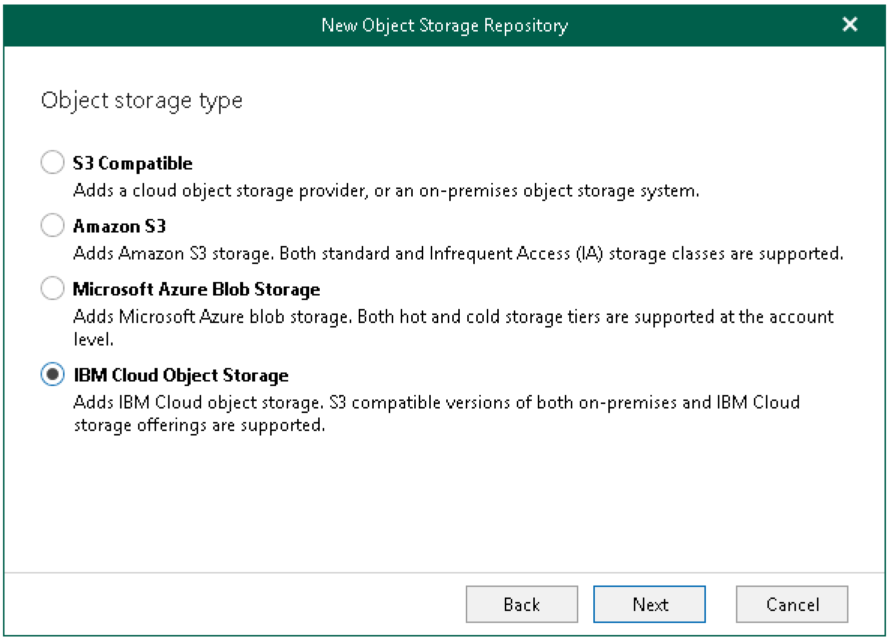

New Object Storage Repository
Object storage repository name and description

Name: IBM Cloud Object Storage

Description: Secondary Backup Storage

Step 3. Select Object Storage Type

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



Object storage type

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

○ **Amazon S3**
Adds Amazon S3 storage. 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.

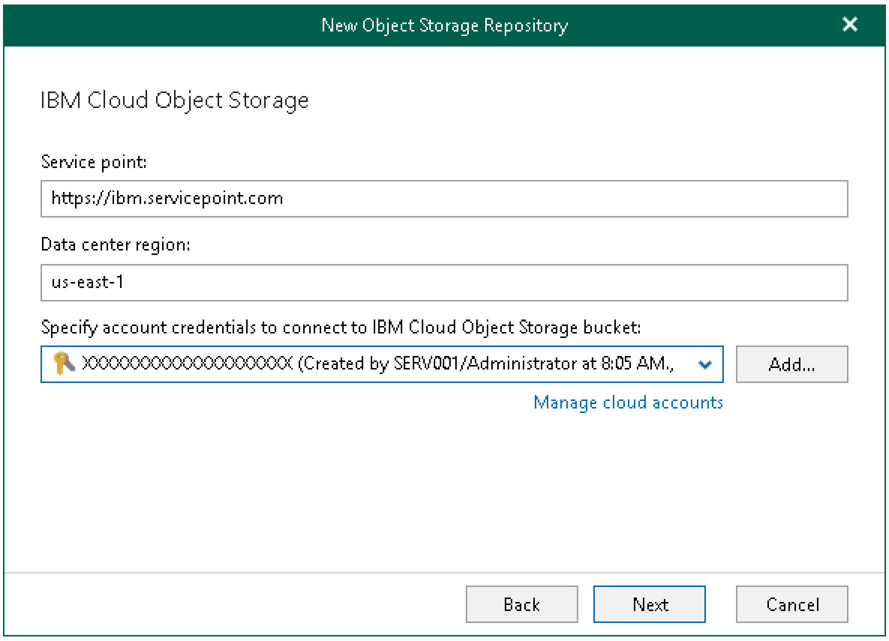
● **IBM Cloud Object Storage**
Adds IBM Cloud object storage. S3 compatible versions of both on-premises and IBM Cloud storage offerings are supported.

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.

1. In the **Service point** field, specify an endpoint address of your IBM Cloud object storage.
2. In the **Data center region** field, specify a region.
3. From the **Specify account credentials to connect to IBM Cloud Object Storage bucket** drop-down list, select user credentials to access your IBM Cloud object storage.

   If you already have a credentials record that was configured beforehand, select such a record in the drop-down list. Otherwise, click **Add** and provide your access and secret keys, as described in Adding S3 Compatible and IBM Storage Access Key. You can also click **Manage cloud accounts** to manage existing credentials records.


New Object Storage Repository

IBM Cloud Object Storage

Service point: https://ibm.servicepoint.com

Data center region: us-east-1

Specify account credentials to connect to IBM Cloud Object Storage bucket: XXXXXXXXXXXXXXXXXXXX (Created by SERV001/Administrator at 8:05 AM.,

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. From the **Bucket** drop-down list, select a bucket.

   Make sure that the bucket you want to use to store your data was created in advance; Veeam Backup for Microsoft Office 365 does not support creating new buckets.

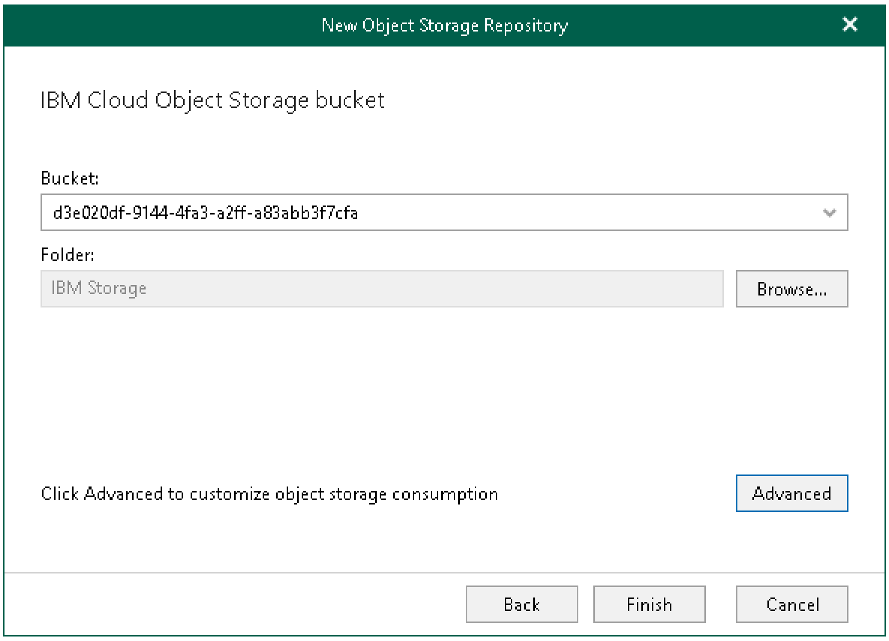
2. In the **Folder** field, select a folder to which you want to map your object storage repository, and which will be used to store backups.

   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: d3e020df-9144-4fa3-a2ff-a83abb3f7cfa

Folder: IBM Storage

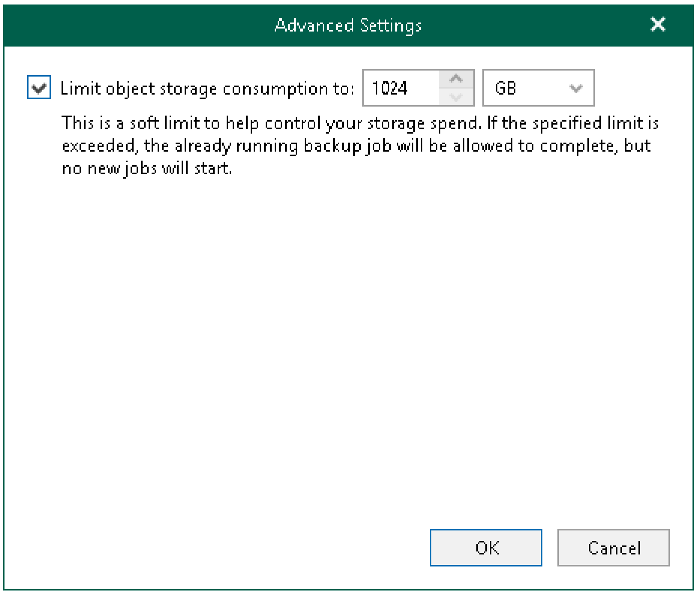
Click Advanced to customize object storage consumption

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**.



☑ 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.

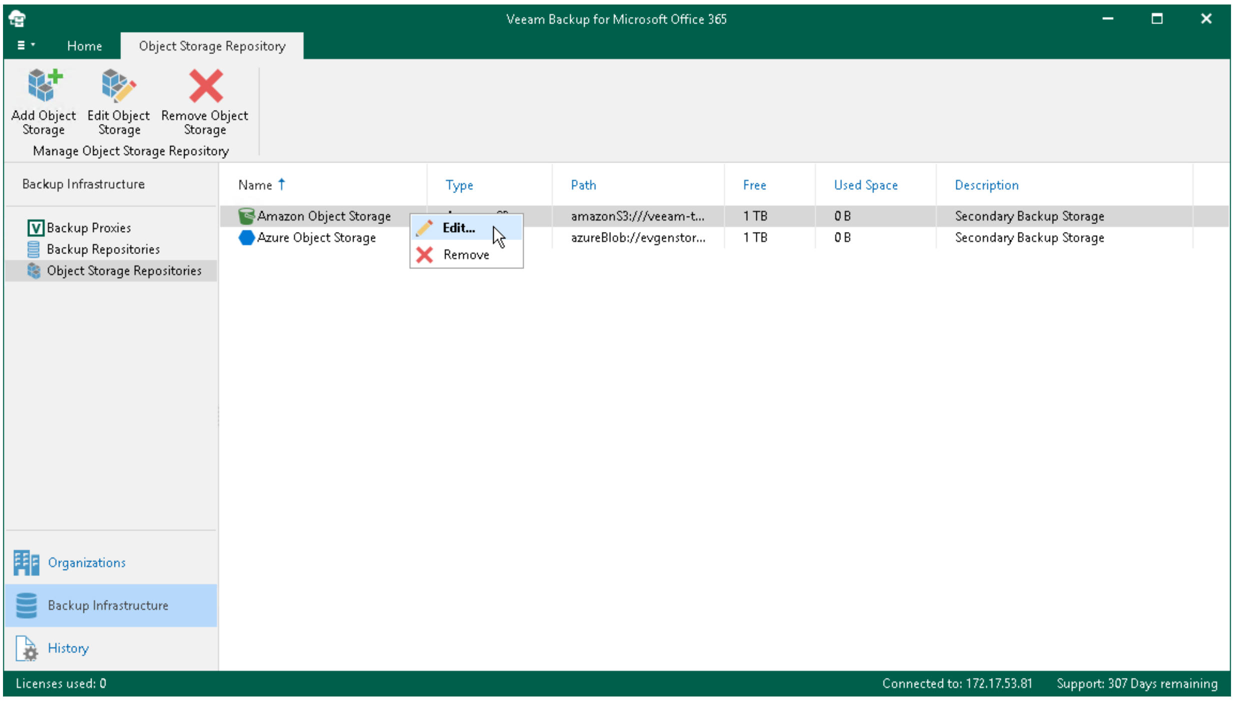
Editing Object Storage Settings

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.



Name	Type	Path	Free	Used Space	Description
Amazon Object Storage		amazonS3:///veeam-t...	1 TB	0 B	Secondary Backup Storage
Azure Object Storage		azureBlob://evgenstor...	1 TB	0 B	Secondary Backup Storage

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.

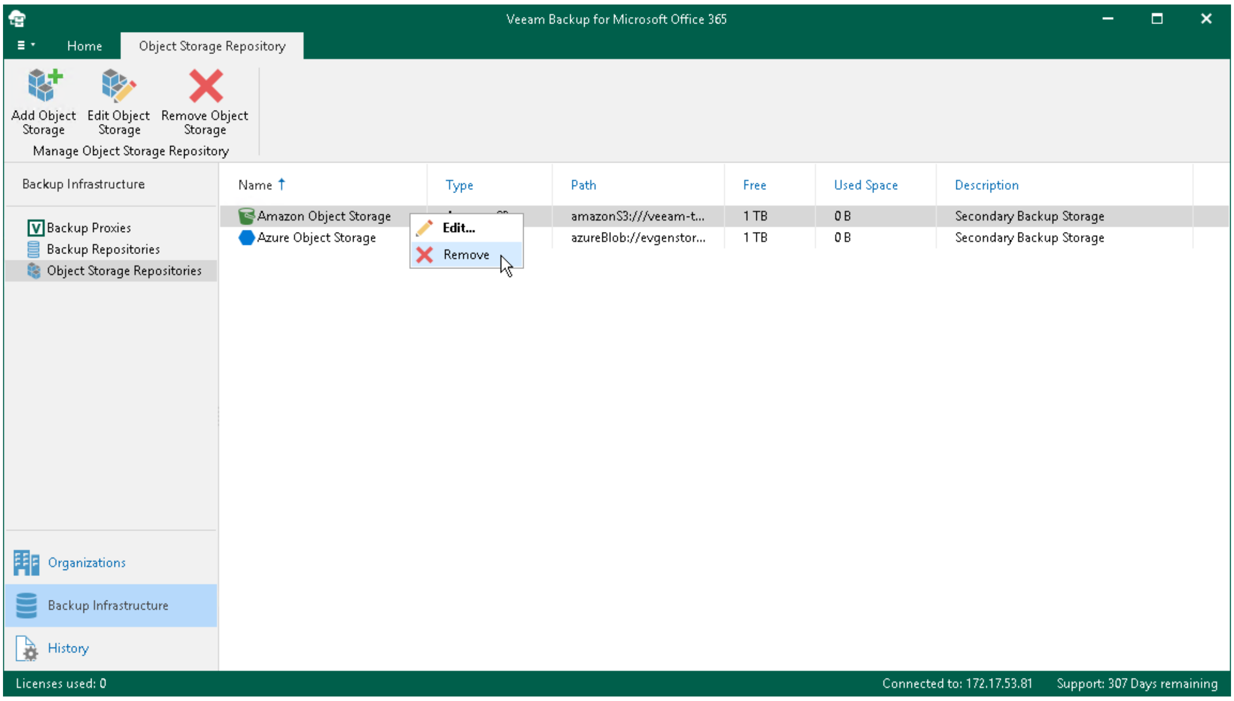
  To remove such object storage, remove an extended backup repository and then remove object storage. For more information on how to remove a backup repository, see Removing Backup Repositories.

- 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**.



Name	Type	Path	Free	Used Space	Description
Amazon Object Storage		amazonS3:///veeam-t...	1 TB	0 B	Secondary Backup Storage
Azure Object Storage		azureBlob://evgenstor...	1 TB	0 B	Secondary Backup Storage

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:

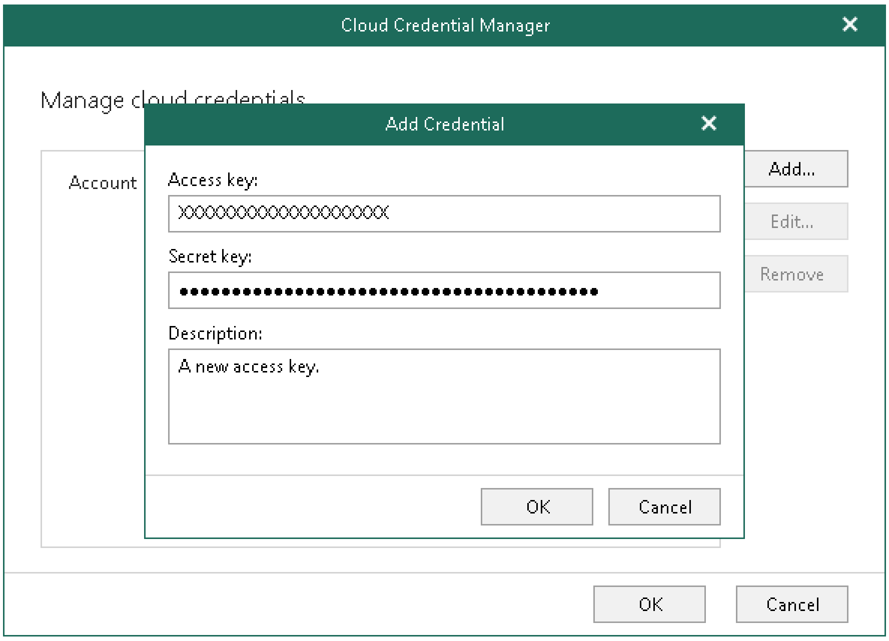
- S3 Compatible and IBM storage
- Amazon AWS object storage
- Microsoft Azure Storage

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**.



Access key: XXXXXXXXXXXXXXXXXXXX

Secret key: ••

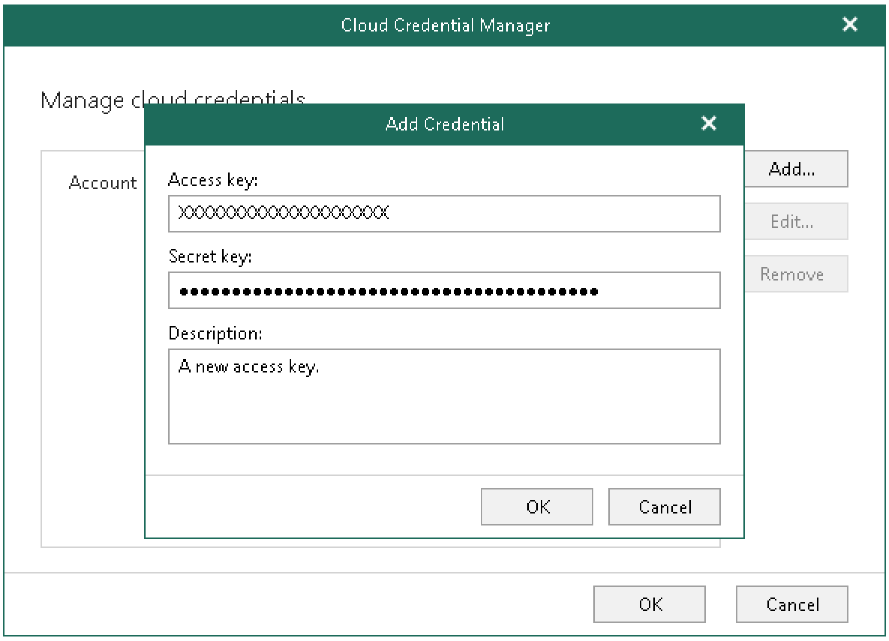
Description: A new access key.

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**.



Access key: XXXXXXXXXXXXXXXXXXXX

Secret key: ••

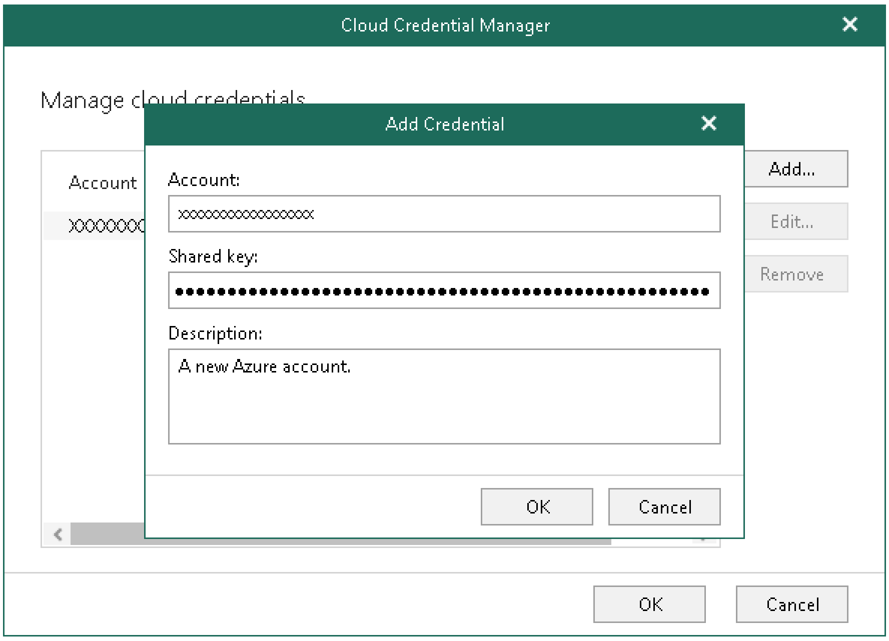
Description: A new access key.

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**.



Account: xxxxxxxxxxxxxxxxxx

Shared key: ••

Description: A new Azure account.

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.

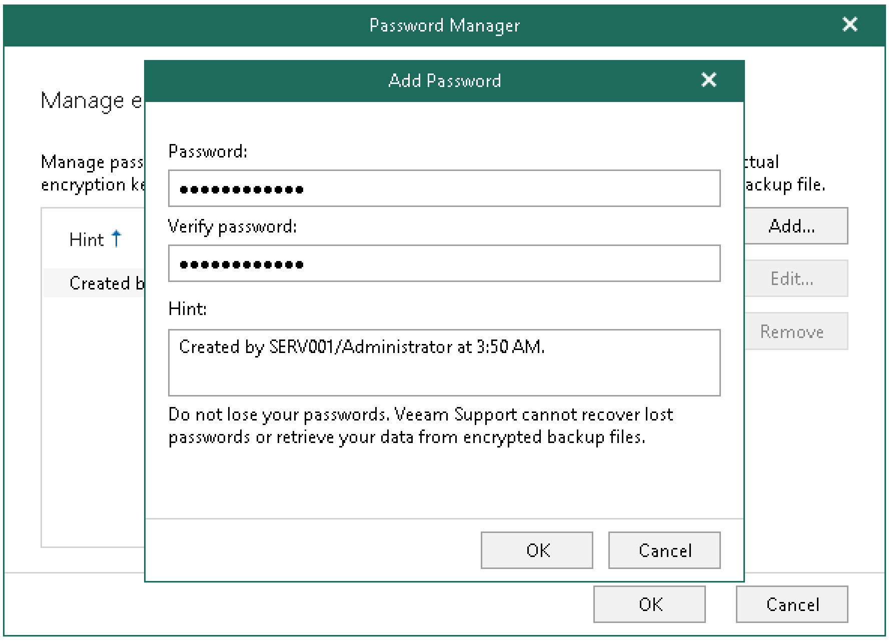
Managing Encryption Passwords

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.



Created by SERV001/Administrator at 3:50 AM.

Do not lose your passwords. Veeam Support cannot recover lost passwords or retrieve your data from encrypted backup files.

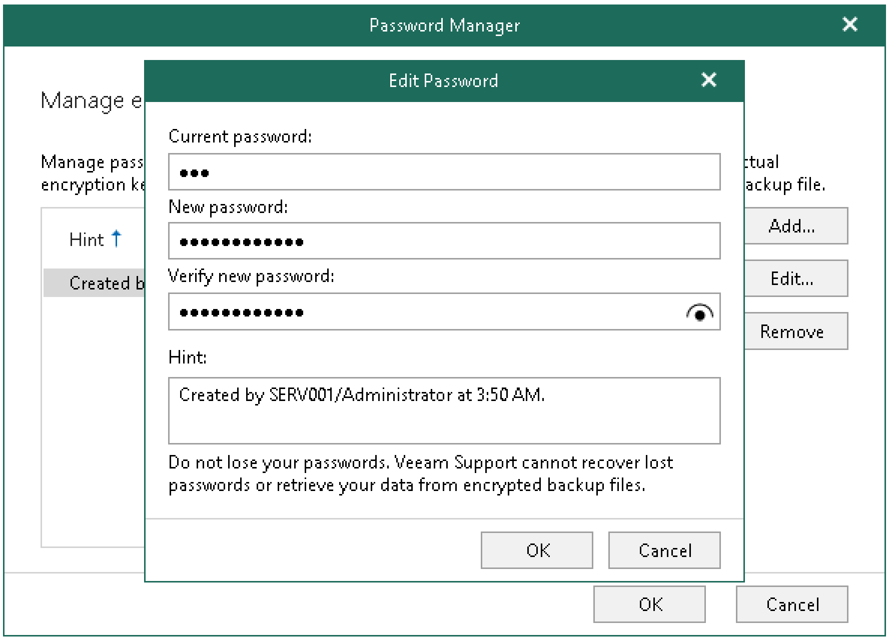
Editing and Removing Password Records

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 **Password Manager** 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.



Current password: ●●●

New password: ●●●●●●●●●●●●

Verify new password: ●●●●●●●●●●●●

Hint: Created by SERV001/Administrator at 3:50 AM.

Do not lose your passwords. Veeam Support cannot recover lost passwords or retrieve your data from encrypted backup files.

Removing Records

To remove a password, do the following:

1. In the main menu, click **Manage Passwords.**
2. In the **Password Manager** 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 app-only 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 with the modern app-only authentication method.

- Modern authentication with legacy protocols allowed

  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 Modern App-Only Authentication

When you add an organization using the modern app-only authentication method, you are required to provide Azure AD application settings. Veeam Backup for Microsoft 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 app-only authentication, you cannot use a user account; only communications via an Azure AD application is possible.

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

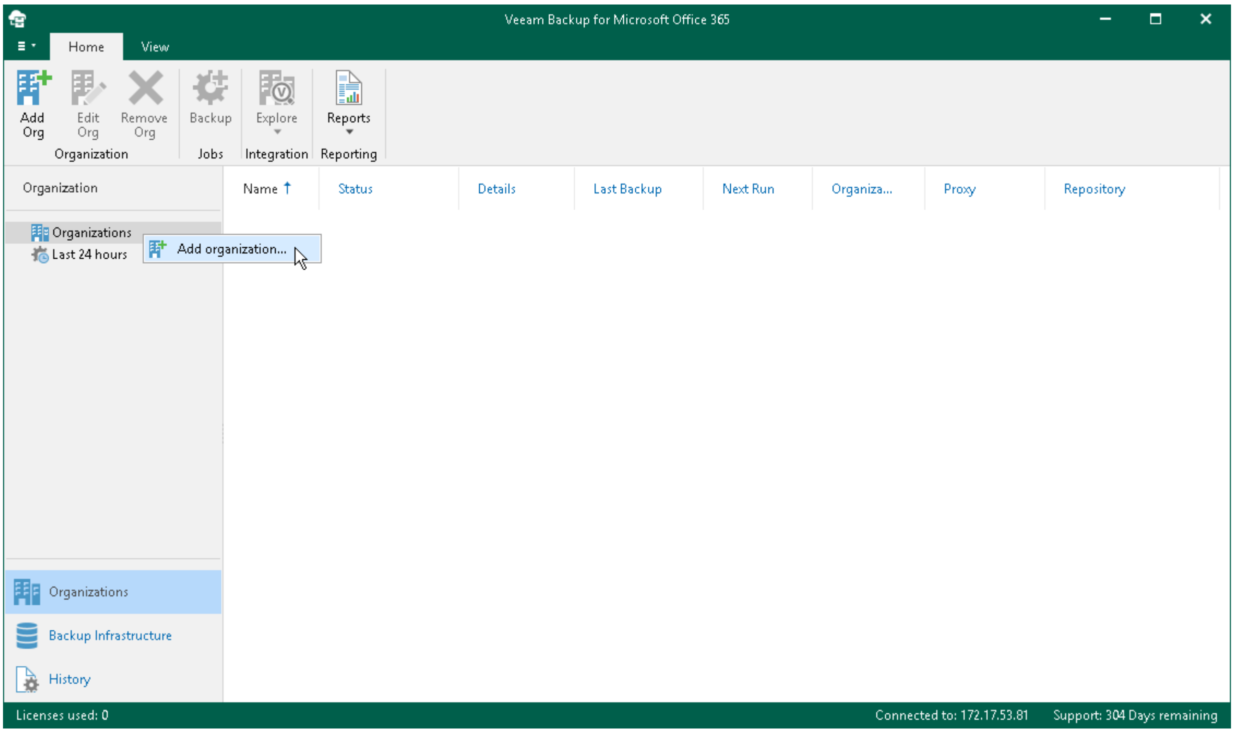
1. Launch the Add Organization wizard.
2. Select an organization deployment type.
3. Specify connection settings.
4. Choose an Azure AD application.
5. Register an Azure AD application.
6. Log in to Office 365.
7. Finish the wizard.

Step 1. Launch Add Organization Wizard

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

1. Open the **Organizations** view.
2. 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:

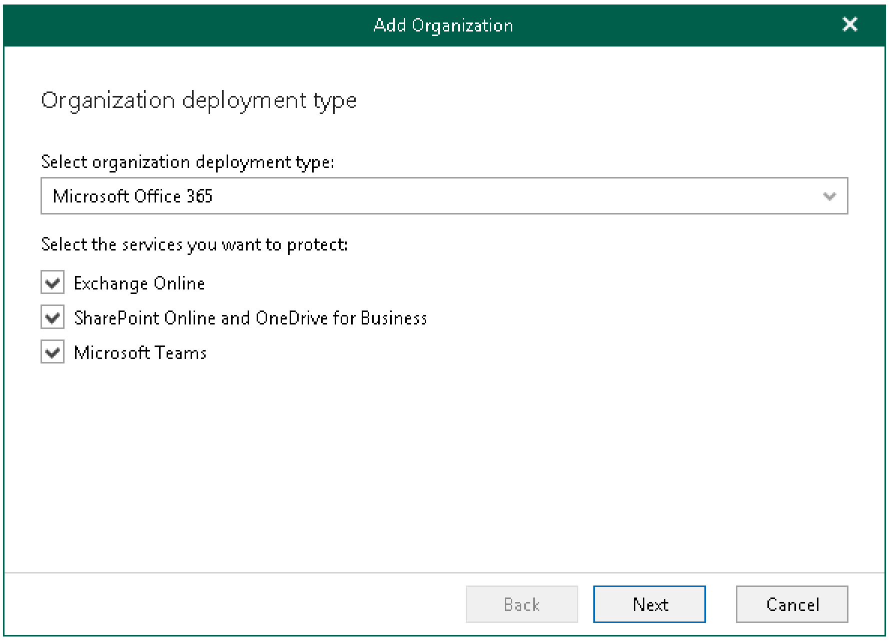
1. From the **Select organization deployment type** drop-down list, select **Microsoft Office 365**.
2. Select services that you want to protect:
   - **Exchange Online**

     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.
   - **Microsoft Teams**

     Select this check box if you want to back up Microsoft Teams data.

     You can select this check box only if both **Exchange Online** and **SharePoint Online and OneDrive for Business** check boxes are selected.



Add Organization

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

☑ Microsoft Teams

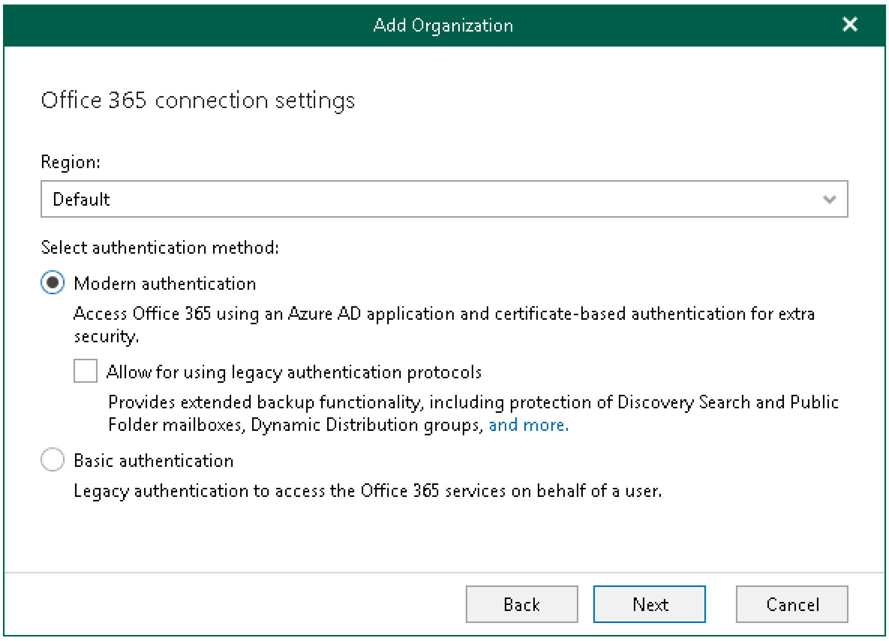
Step 3. Specify Connection Settings

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

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

1. From the **Region** drop-down list, select a Microsoft Azure region your Office 365 organization belongs to.
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 cleared. This check box allows you to add an Office 365 organization with disabled security defaults, as described in Adding Organizations with Modern Authentication 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.

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 Azure AD application.

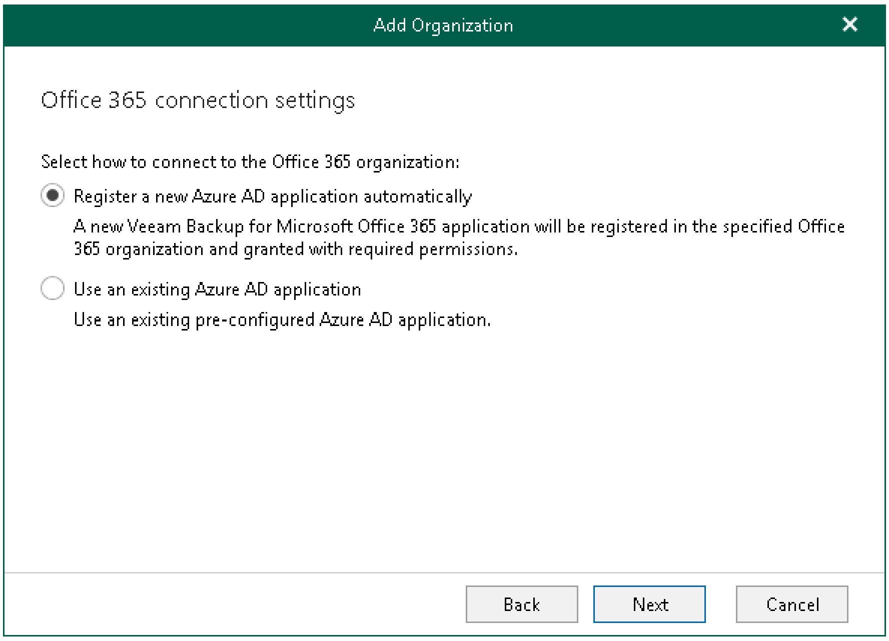
You can select either of the following options:

- **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 Azure 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 Azure AD application, as described in Using Existing Application.



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.

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.

- 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 Azure 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 Azure AD application, Veeam Backup for Microsoft Office 365 automatically grants required permissions to this application.

To register a new application, do the following:

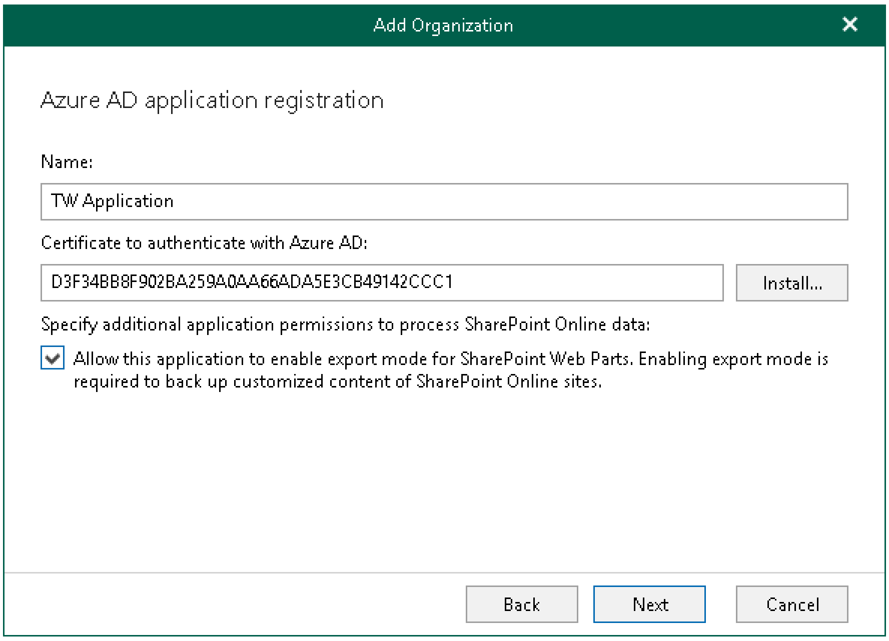
1. In the **Name** field, enter a name that you want to use to register a new Azure AD application in your Microsoft Azure Active Directory.
2. Click **Install** to choose an SSL certificate that you want to use for data exchange between Veeam Backup for Microsoft Office 365 and an Azure AD application.
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 enable 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.



Name: TW Application

Certificate to authenticate with Azure AD: D3F34BB8F902BA259A0AA66ADA5E3CB49142CCC1

Specify additional application permissions to process SharePoint Online data:

☑ Allow this application to enable export mode for SharePoint Web Parts. Enabling export mode is required to back up customized content of SharePoint Online sites.

Using Existing Azure AD Application

You can specify an existing Azure 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 Azure 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 Azure 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 Azure AD application.

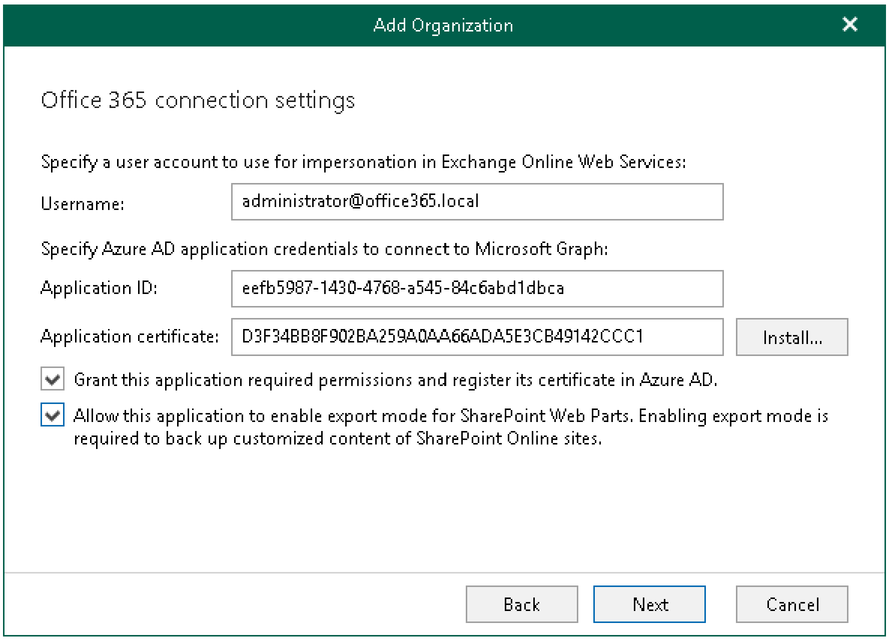
   Veeam Backup for Microsoft Office 365 will also register the specified certificate in your Microsoft Azure Active Directory.

   Mind that if this check box is not selected, Veeam Backup for Microsoft Office 365 skips the Log in to Office 365 step and proceeds to Finish Wizard.

8. Select the **Allow this application to enable 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.



Office 365 connection settings

Specify a user account to use for impersonation in Exchange Online Web Services:

Username: administrator@office365.local

Specify Azure AD application credentials to connect to Microsoft Graph:

Application ID: eefb5987-1430-4768-a545-84c6abd1dbca

Application certificate: D3F34BB8F902BA259A0AA66ADA5E3CB49142CCC1

☑ Grant this application required permissions and register its certificate in Azure AD.

☑ Allow this application to enable export mode for SharePoint Web Parts. Enabling export mode is required to back up customized content of SharePoint Online sites.

Step 6. Log In to Office 365

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

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

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

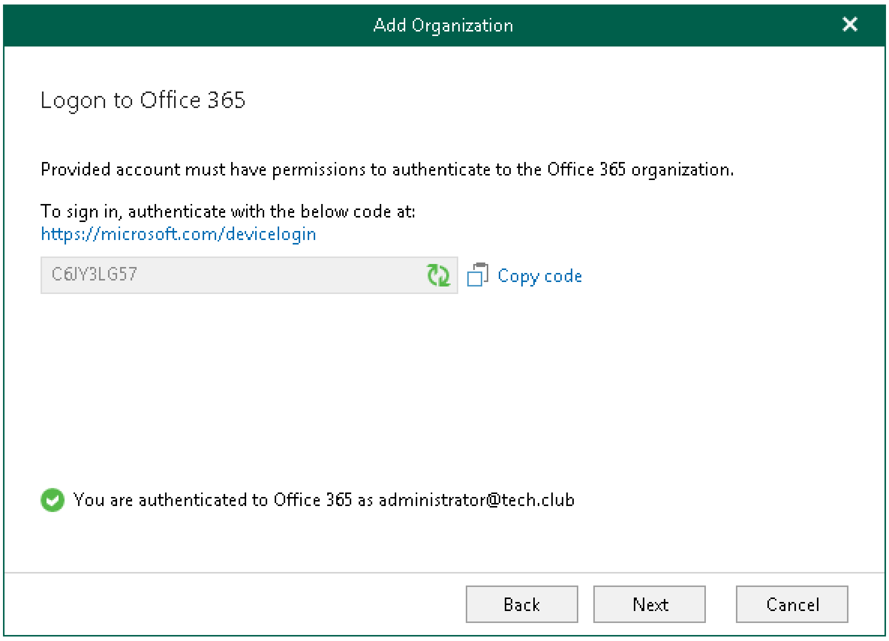
   Mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.

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 sign in with the user account that has the *Global Administrator* role. For more information about this role, see this Microsoft article.

4. Return to the **Add Organization** window and click **Next**.



Logon to Office 365

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

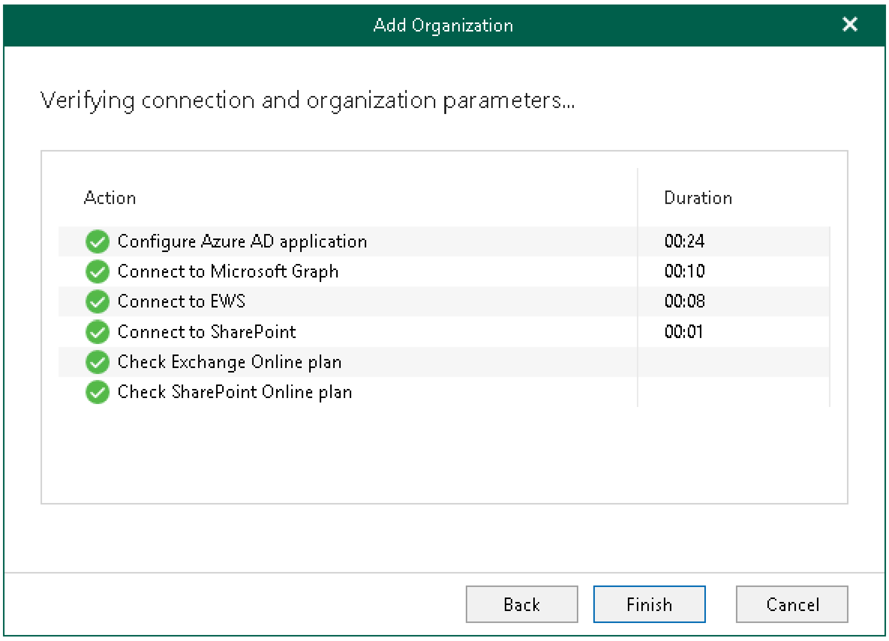
To sign in, authenticate with the below code at:
https://microsoft.com/devicelogin

C6JY3LG57

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

Step 7. Finish Working with Wizard

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



Verifying connection and organization parameters...

Action	Duration
✓ Configure Azure AD application	00:24
✓ Connect to Microsoft Graph	00:10
✓ Connect to EWS	00:08
✓ Connect to SharePoint	00:01
✓ Check Exchange Online plan	
✓ Check SharePoint Online plan	

Adding Organizations with Modern Authentication and Legacy Protocols

When you add an organization using the modern authentication method with legacy protocols allowed, 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, OneDrive for Business and Microsoft Teams 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.

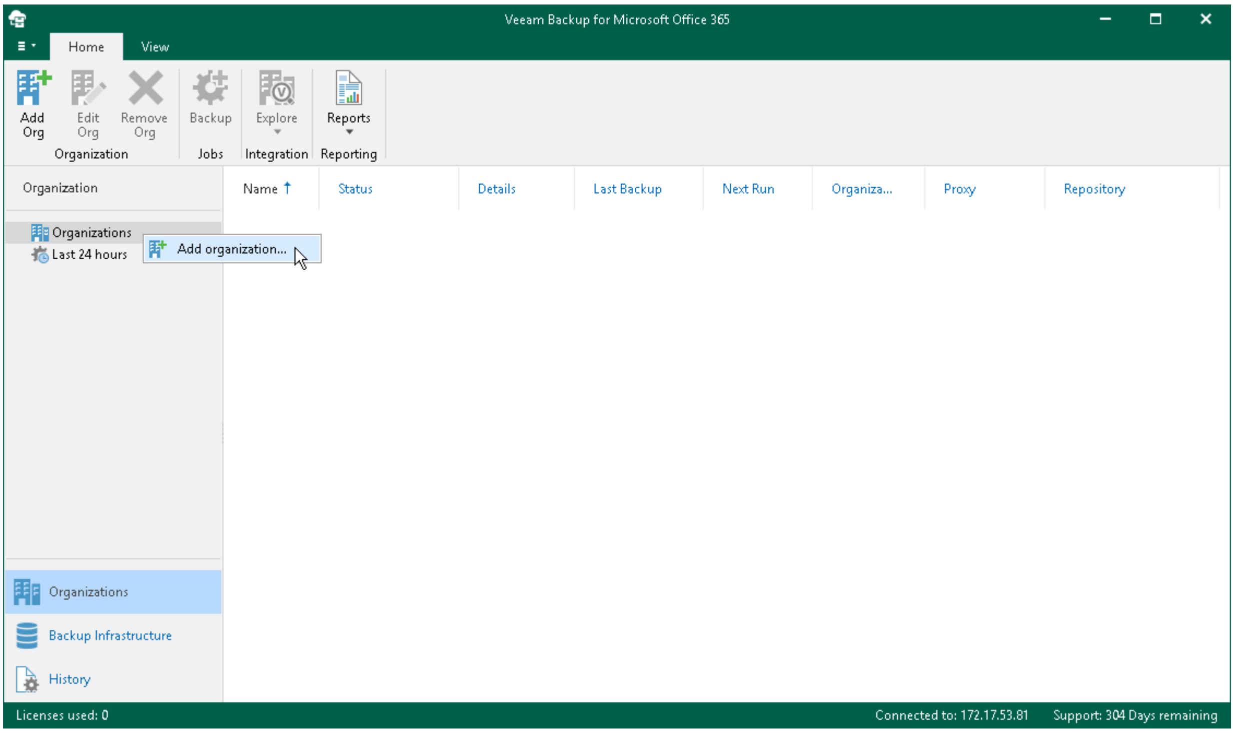
Make sure to grant your Azure AD application required permissions.

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:

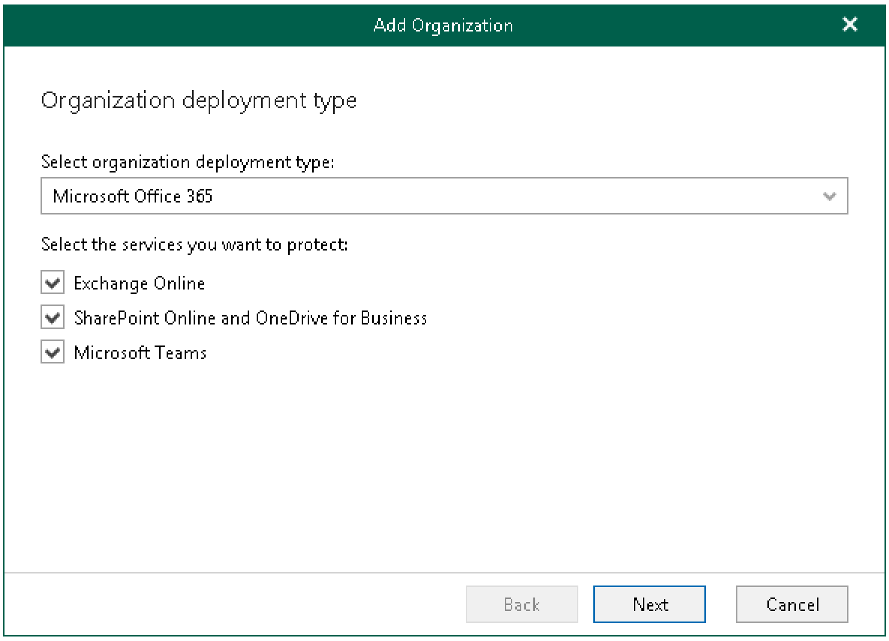
1. From the **Select organization deployment type** drop-down list, select **Microsoft Office 365**.
2. Select services that you want to protect:
   - **Exchange Online**

     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.
   - **Microsoft Teams**

     Select this check box if you want to back up Microsoft Teams data.

     You can select this check box only if both **Exchange Online** and **SharePoint Online and OneDrive for Business** check boxes are selected.



Select organization deployment type: Microsoft Office 365

Select the services you want to protect:

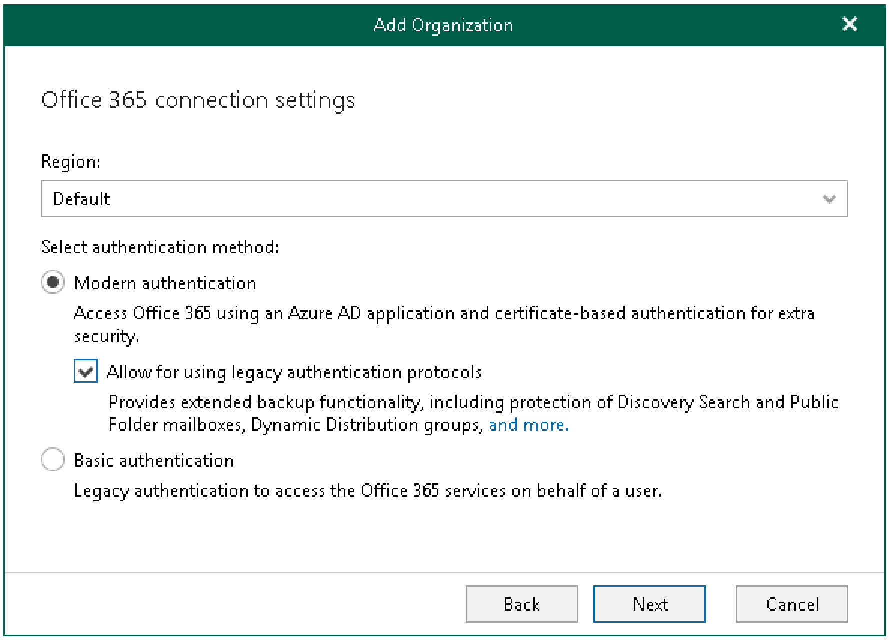
☑ Exchange Online
☑ SharePoint Online and OneDrive for Business
☑ Microsoft Teams

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

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 Azure 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 Azure 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.

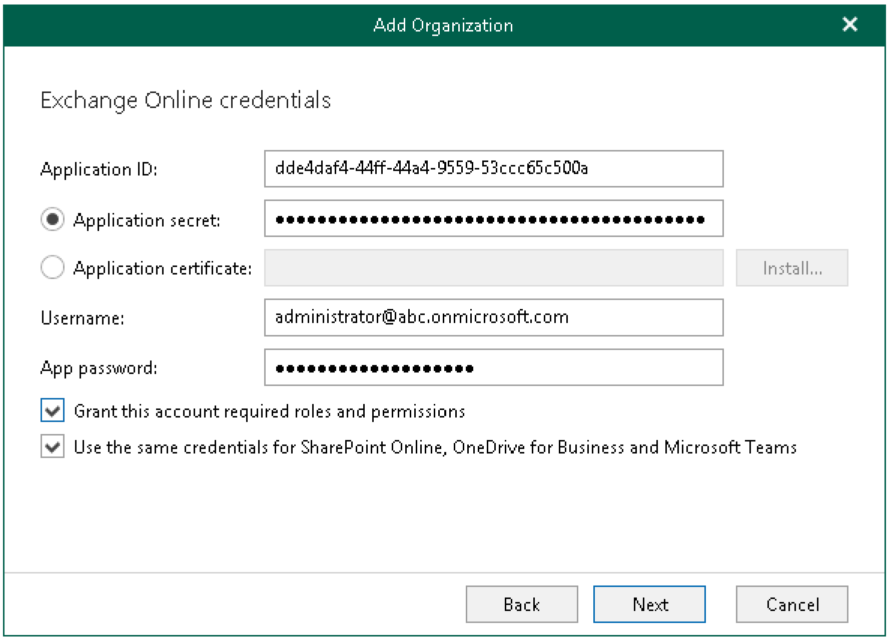
   The user account must be provided in either of the following formats: *user@domain*.com or *user@domain.onmicrosoft.com*. If you are using an ADFS account, you can only use a non-MFA enabled ADFS account.

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, OneDrive for Business and Microsoft Teams** check box if you want to use the same credentials to access your Microsoft SharePoint Online, OneDrive for Business and Microsoft Teams organizations. This check box is only available if these organization types have been selected at the Select Organization Deployment Type step.

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



Add Organization

Exchange Online credentials

Application ID: dde4daf4-44ff-44a4-9559-53ccc65c500a

● Application secret: ••

○ Application certificate:

Username: administrator@abc.onmicrosoft.com

App password: ••••••••••••••••••••

☑ Grant this account required roles and permissions

☑ Use the same credentials for SharePoint Online, OneDrive for Business and Microsoft Teams

Step 5. Specify SharePoint Online, OneDrive for Business and Microsoft Teams Credentials

This step is only available if you did not select the **Use the same credentials for SharePoint Online, OneDrive for Business and Microsoft Teams** check box at the Specify Azure AD Application Credentials step of the wizard.

At this step of the wizard, enter credentials to connect to the Microsoft SharePoint Online organization. Keep in mind that if you plan to back up Microsoft Teams data, Veeam Backup for Microsoft Office 365 will also use these credentials to connect to Microsoft Teams.

To enter credentials, do the following:

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

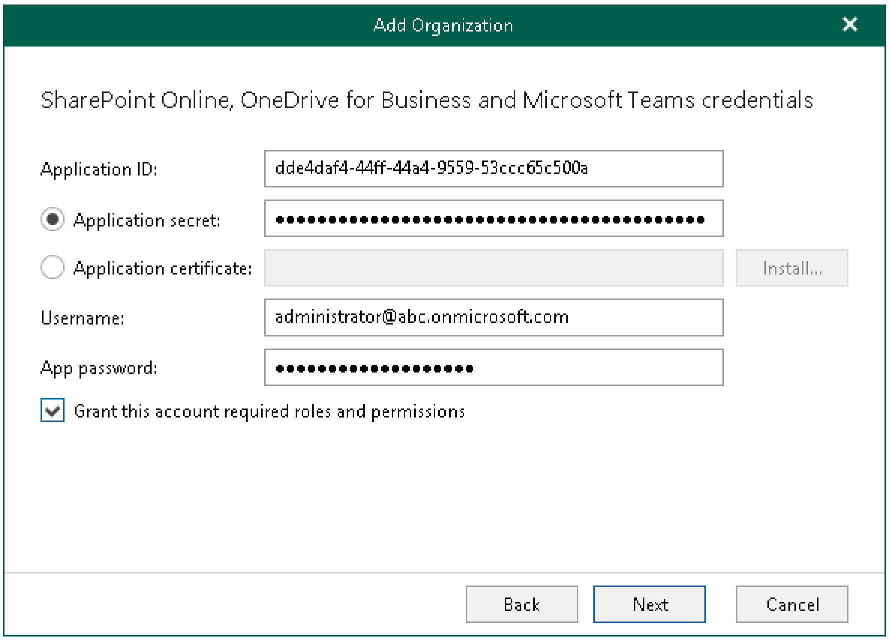
   b. To use a certificate, switch to the **Application certificate** option and click **Install**. For more information, see SSL Certificates.

      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 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.



SharePoint Online, OneDrive for Business and Microsoft Teams credentials

Application ID: dde4daf4-44ff-44a4-9559-53ccc65c500a

● Application secret: ••

○ Application certificate:

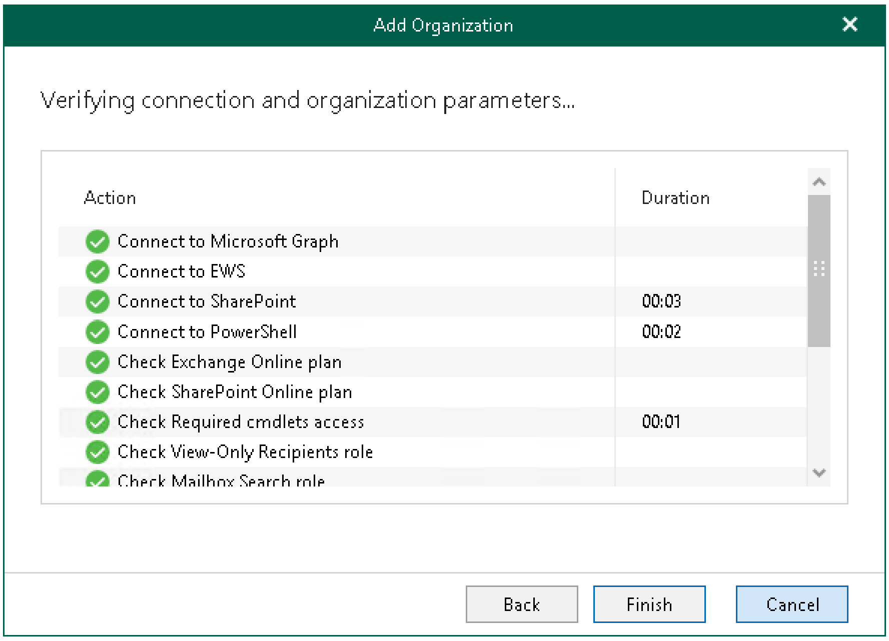
Username: administrator@abc.onmicrosoft.com

App password: •••••••••••••••••••

☑ Grant this account required roles and permissions

Step 6. Finish Working with Wizard

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



Verifying connection and organization parameters...

Action	Duration
✓ Connect to Microsoft Graph	
✓ Connect to EWS	
✓ Connect to SharePoint	00:03
✓ Connect to PowerShell	00:02
✓ Check Exchange Online plan	
✓ Check SharePoint Online plan	
✓ Check Required cmdlets access	00:01
✓ Check View-Only Recipients role	
✓ Check Mailbox Search role	

Adding Organizations with Basic Authentication

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

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

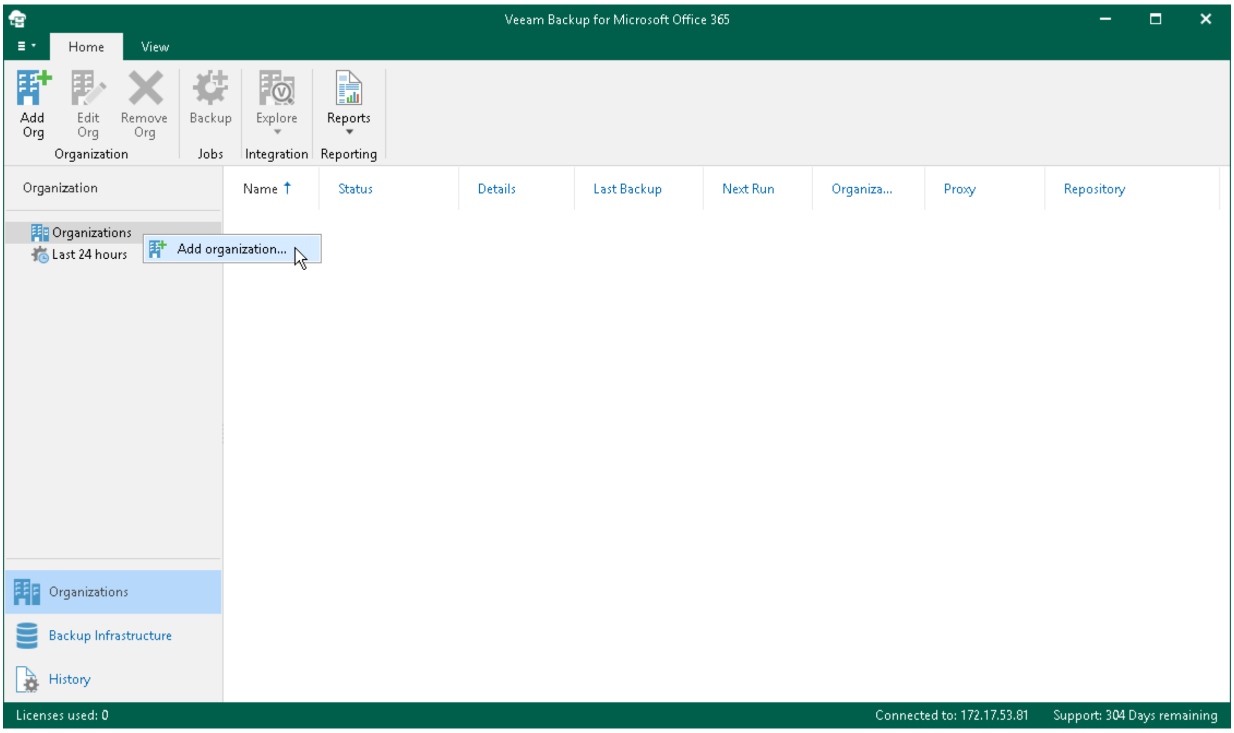
1. Launch the Add Organization wizard.
2. Select an organization deployment type.
3. Specify connection settings.
4. Specify Exchange Online credentials.
5. Specify SharePoint Online, OneDrive for Business and Microsoft Teams credentials.
6. Finish the wizard.

Step 1. Launch Add Organization Wizard

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

1. Open the **Organizations** view.
2. 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:

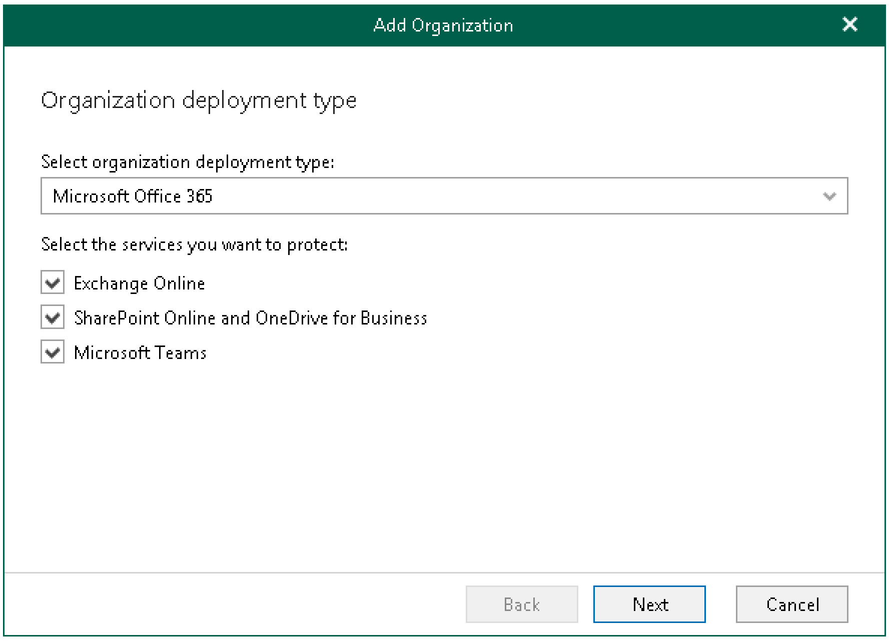
1. From the **Select organization deployment type** drop-down list, select **Microsoft Office 365**.
2. Select services that you want to protect:
   - **Exchange Online**

     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.
   - **Microsoft Teams**

     Select this check box if you want to back up Microsoft Teams data.

     You can select this check box only if both **Exchange Online** and **SharePoint Online and OneDrive for Business** check boxes are selected.



Add Organization

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
☑ Microsoft Teams

Step 3. Specify Connection Settings

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

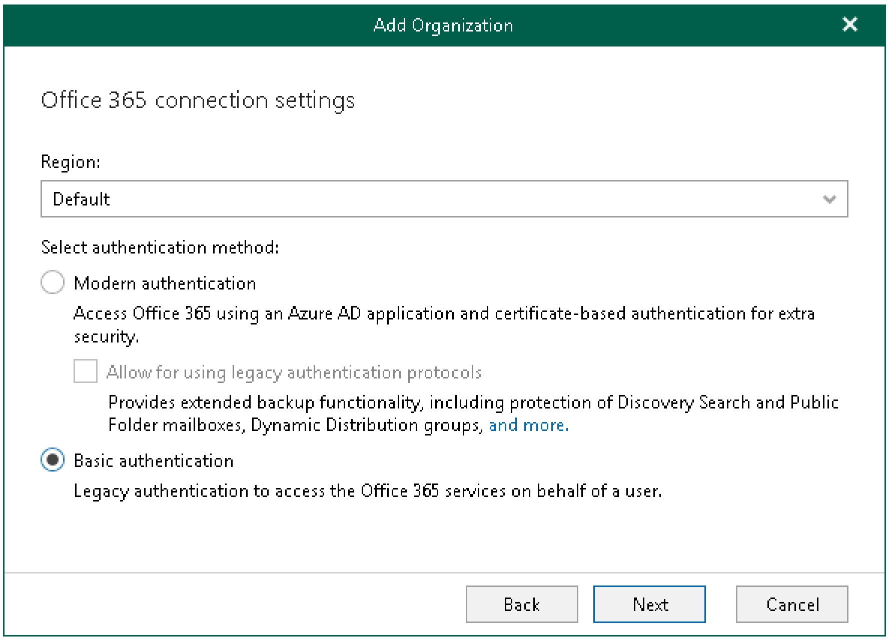
To select a region and authentication method, do the following:

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

   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



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.

Step 4. Specify Exchange Online Credentials

At this step of the wizard, enter credentials to connect to the Microsoft Exchange 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.

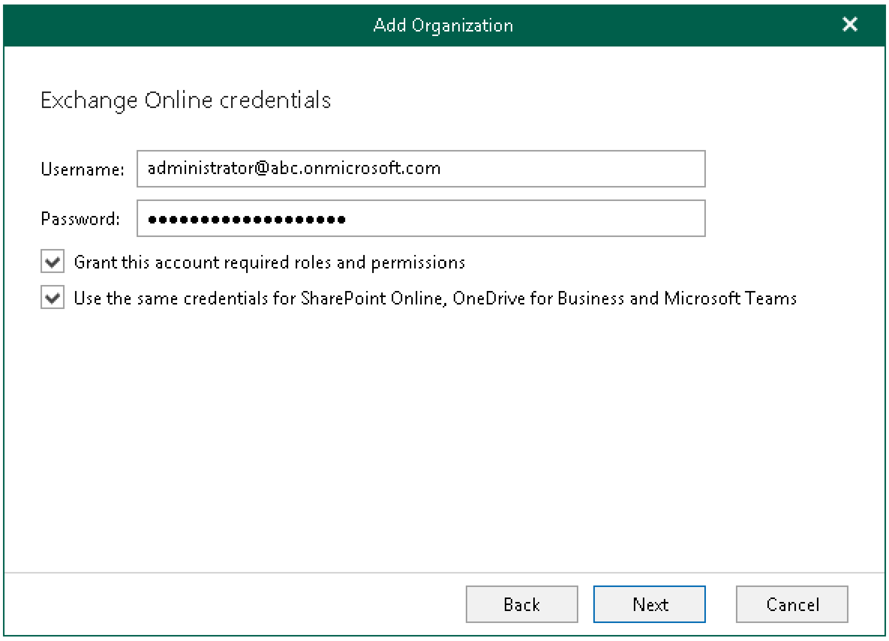
   The user account must be provided in either of the following formats: *user@domain*.com or *user@domain.onmicrosoft.com*. If you are using an ADFS account, you can only use a non-MFA enabled ADFS account.

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, OneDrive for Busines and Microsoft Teams** check box if you want to use the same credentials to access your Microsoft SharePoint Online, OneDrive for Business and Microsoft Teams organizations. This check box is only available if these organization types have been selected at the Select Organization Deployment Type step.

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



Exchange Online credentials

Username: administrator@abc.onmicrosoft.com

Password: ●●●●●●●●●●●●●●●●●●●

☑ Grant this account required roles and permissions

☑ Use the same credentials for SharePoint Online, OneDrive for Business and Microsoft Teams

Step 5. Specify SharePoint Online, OneDrive for Business and Microsoft Teams Credentials

This step is only available if you did not select the **Use the same credentials for SharePoint Online, OneDrive for Business and Microsoft Teams** check box at the Specify Exchange Online Credentials step of the wizard.

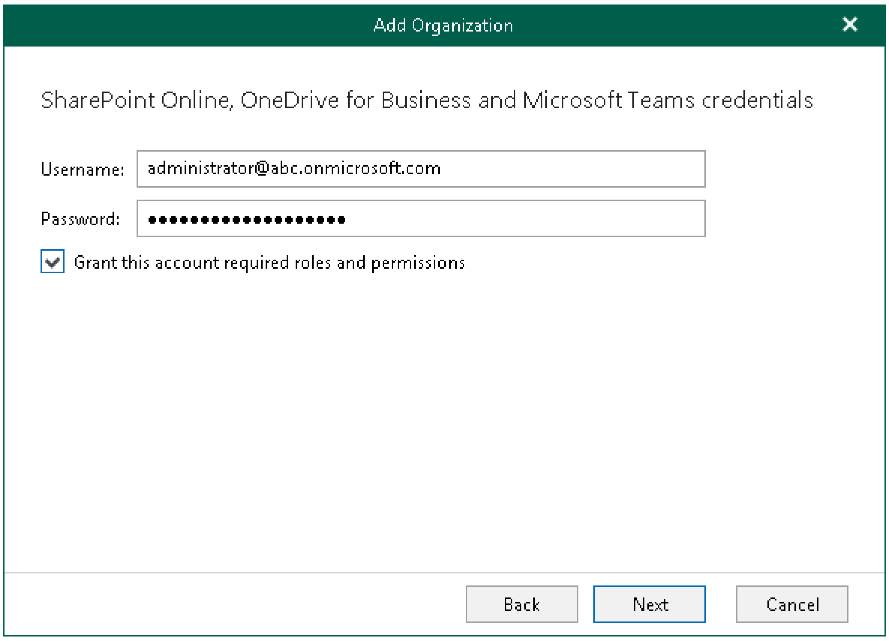
At this step of the wizard, enter credentials to connect to the Microsoft SharePoint Online organization. Keep in mind that if you plan to back up Microsoft Teams data, Veeam Backup for Microsoft Office 365 will also use these credentials to connect to Microsoft Teams.

To enter credentials, do the following:

1. In the **Username** and **Password** fields, specify 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, OneDrive for Business and Microsoft Teams credentials

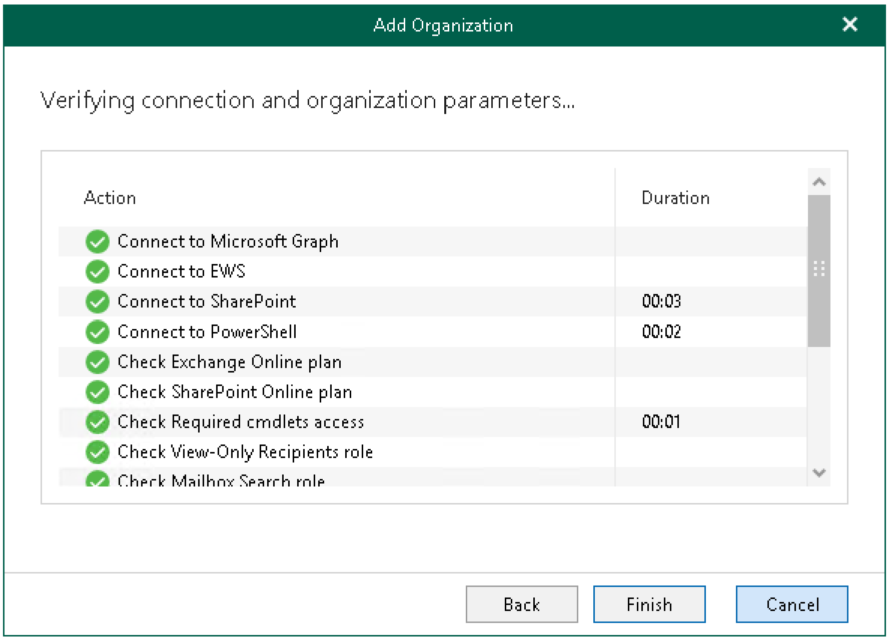
Username: administrator@abc.onmicrosoft.com

Password: ●●●●●●●●●●●●●●●●●●●

☑ Grant this account required roles and permissions

Step 6. Finish Working with Wizard

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



Verifying connection and organization parameters...

Action	Duration
✓ Connect to Microsoft Graph	
✓ Connect to EWS	
✓ Connect to SharePoint	00:03
✓ Connect to PowerShell	00:02
✓ Check Exchange Online plan	
✓ Check SharePoint Online plan	
✓ Check Required cmdlets access	00:01
✓ Check View-Only Recipients role	
✓ Check Mailbox Search role	

On-Premises Microsoft Organizations

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

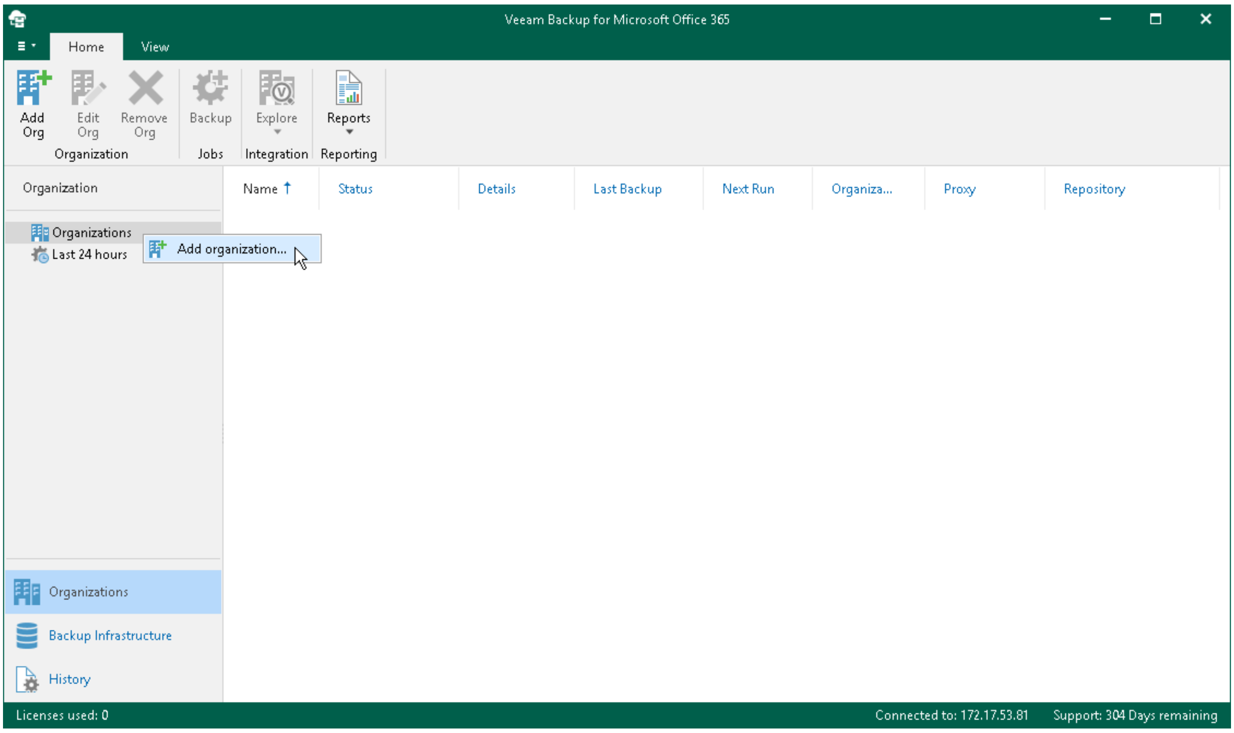
1. Launch the Add Organization wizard.
2. Select an organization deployment type.
3. Specify Microsoft Exchange connection settings.
4. Specify Microsoft SharePoint connection settings.
5. Finish the Wizard.

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**.



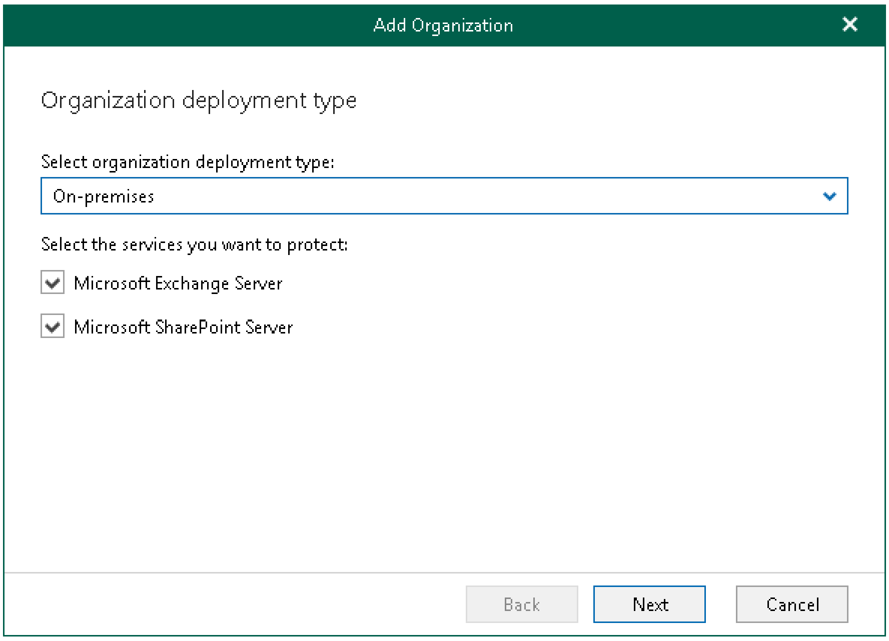
Step 2. Select Organization Deployment Type

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

1. From the **Select organization deployment type** drop-down list, select **On-premises**.
2. Select services that you want to protect:
   - **Microsoft Exchange Server**

     Select this check box if you want to back up Microsoft Exchange data.
   - **Microsoft SharePoint Server**

     Select this check box if you want to back up Microsoft SharePoint data.



Add Organization

Organization deployment type

Select organization deployment type: On-premises

Select the services you want to protect:

☑ Microsoft Exchange Server

☑ Microsoft SharePoint Server

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 advanced settings.

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

1. In the **Server name** field, specify a Microsoft Exchange server to which you want to connect.

   You can use a DNS name of a server, NetBIOS name or its IP address. Make sure that the server has the *Mailbox Server* role.

2. In the **Username** and **Password** fields, specify authentication credentials to connect to the Microsoft Exchange server using either of the following formats: *domain\account* or *account@domain*.

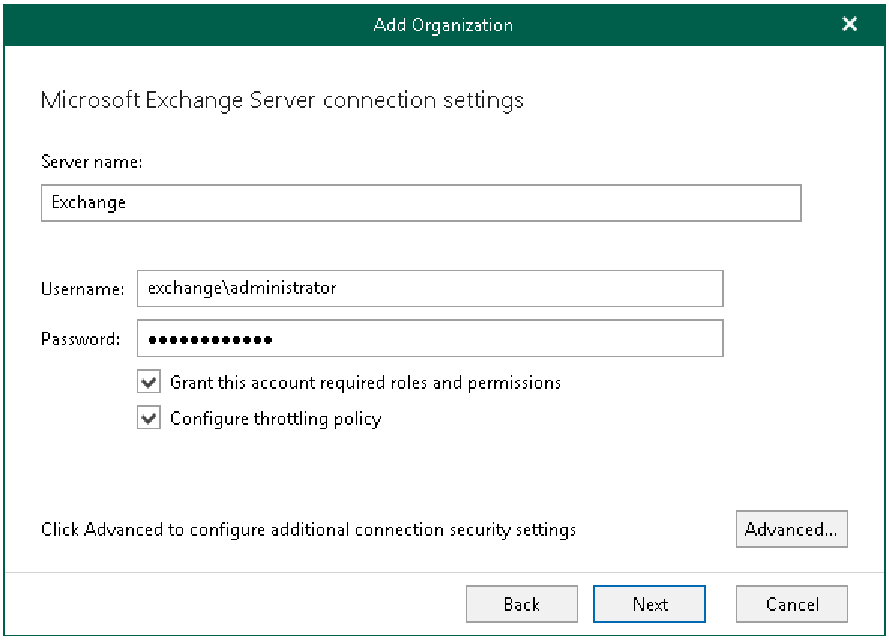
   For more information, see Required Permissions.

   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*.



Server name: Exchange

Username: exchange\administrator

Password: •••••••••••••

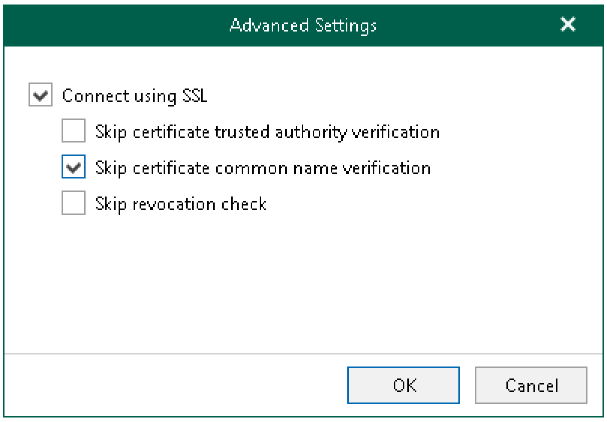
☑ Grant this account required roles and permissions

☑ Configure throttling policy

Click Advanced to configure additional connection security settings

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**



☑ Connect using SSL

□ Skip certificate trusted authority verification

☑ Skip certificate common name verification

□ Skip revocation check

Step 4. Specify Microsoft SharePoint Connection Settings

At this step of the wizard, specify a Microsoft SharePoint server to which you want to connect, provide user credentials, assign appropriate permissions and configure advanced settings.

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

1. In the **Server name and port** field, specify a Microsoft SharePoint server name and the WinRM port.

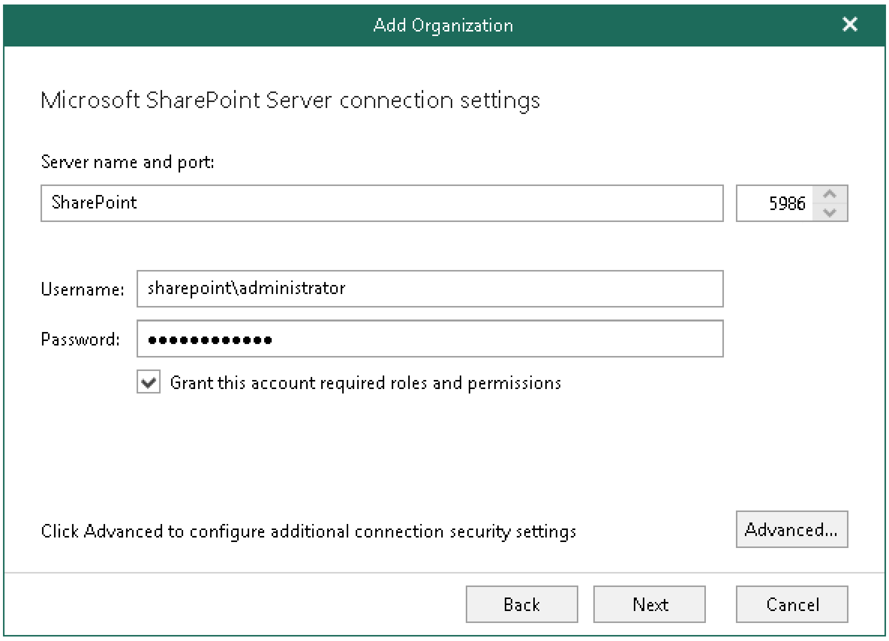
   For the server name, you can use a DNS name of a server, NetBIOS name or its IP address.

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.



Add Organization

Microsoft SharePoint Server connection settings

Server name and port: SharePoint 5986

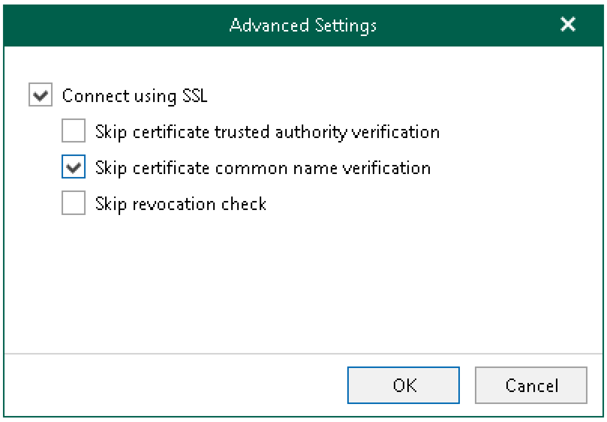
Username: sharepoint\administrator

Password: ••••••••••••

☑ Grant this account required roles and permissions

Click Advanced to configure additional connection security settings

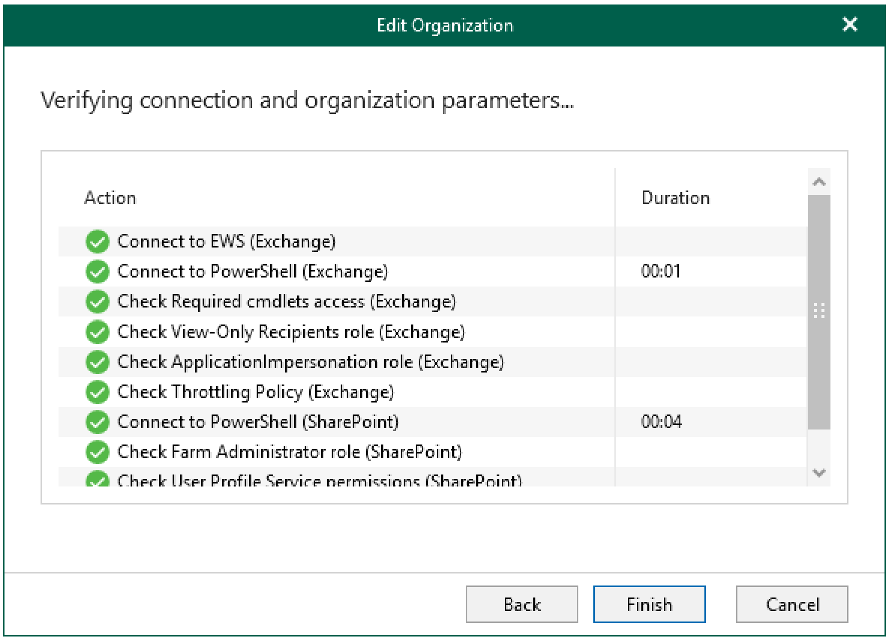
4. Click **Advanced** if you want to skip one or more SSL verifications and select any of the following check boxes:
   - **Skip certificate trusted authority verification**
   - **Skip certificate common name verification**
   - **Skip revocation check**



☑ Connect using SSL
- ☐ Skip certificate trusted authority verification
- ☑ Skip certificate common name verification
- ☐ Skip revocation check

Step 5. Finish Working with Wizard

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



Verifying connection and organization parameters...

Action	Duration
✓ Connect to EWS (Exchange)	
✓ Connect to PowerShell (Exchange)	00:01
✓ Check Required cmdlets access (Exchange)	
✓ Check View-Only Recipients role (Exchange)	
✓ Check ApplicationImpersonation role (Exchange)	
✓ Check Throttling Policy (Exchange)	
✓ Connect to PowerShell (SharePoint)	00:04
✓ Check Farm Administrator role (SharePoint)	
✓ Check User Profile Service permissions (SharePoint)	

Hybrid Organizations

This section explains how to create hybrid configurations consisting of Microsoft Office 365 organizations and on-premises Microsoft Exchange/SharePoint organizations.

You can add hybrid organizations as per the following scenarios:

- Microsoft Exchange Online + on-premises Microsoft Exchange.
- Microsoft Exchange Online + on-premises Microsoft Exchange + Microsoft SharePoint Online and OneDrive for Business.
- Microsoft Exchange Online + on-premises Microsoft Exchange + Microsoft SharePoint Online and OneDrive for Business + Microsoft Teams.
- Microsoft Exchange Online + on-premises Microsoft Exchange + Microsoft SharePoint Online and OneDrive for Business + on-premises Microsoft SharePoint.
- Microsoft Exchange Online + on-premises Microsoft Exchange + Microsoft SharePoint Online and OneDrive for Business + on-premises Microsoft SharePoint + Microsoft Teams.
- Microsoft SharePoint Online and OneDrive for Business + on-premises Microsoft SharePoint.
- Microsoft Exchange Online + Microsoft SharePoint Online and OneDrive for Business + on-premises Microsoft SharePoint.
- Microsoft Exchange Online + Microsoft SharePoint Online and OneDrive for Business + on-premises Microsoft SharePoint + Microsoft Teams.

To specify services that you want to add to a hybrid organization, select 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.
- **Microsoft Teams**

  To back up Microsoft Teams data.

  You can select this check box only if both **Exchange Online** and **SharePoint Online and OneDrive for Business** check boxes are selected.

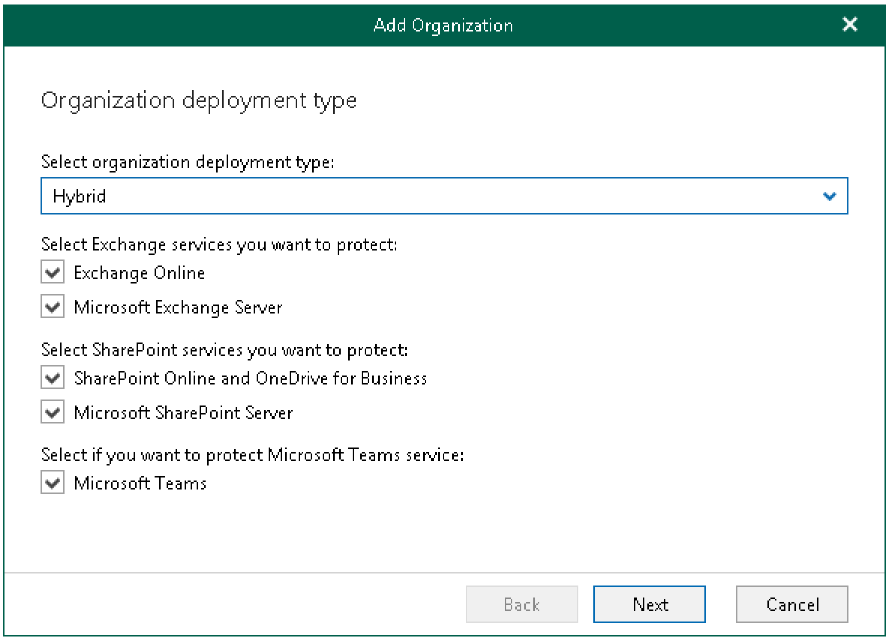
Depending on the types of services that you have selected, do the following:

- Specify connection settings for the Microsoft Office 365 organization, as described in Microsoft Office 365 Organizations.
- Specify connection settings for the on-premises Microsoft Exchange and/or Microsoft SharePoint organization, as described in On-Premises Microsoft 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.



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

Select if you want to protect Microsoft Teams service:

☑ Microsoft Teams

Backup Accounts

If you add Microsoft Office 365 organization using either basic authentication or modern authentication with legacy protocols allowed, you can configure auxiliary backup accounts to minimize throttling when backing up Microsoft SharePoint and OneDrive for Business data.

> **NOTE:**
>
> For Microsoft Office 365 organizations added using modern app-only authentication, you use backup applications instead. For more information, see Backup Applications.

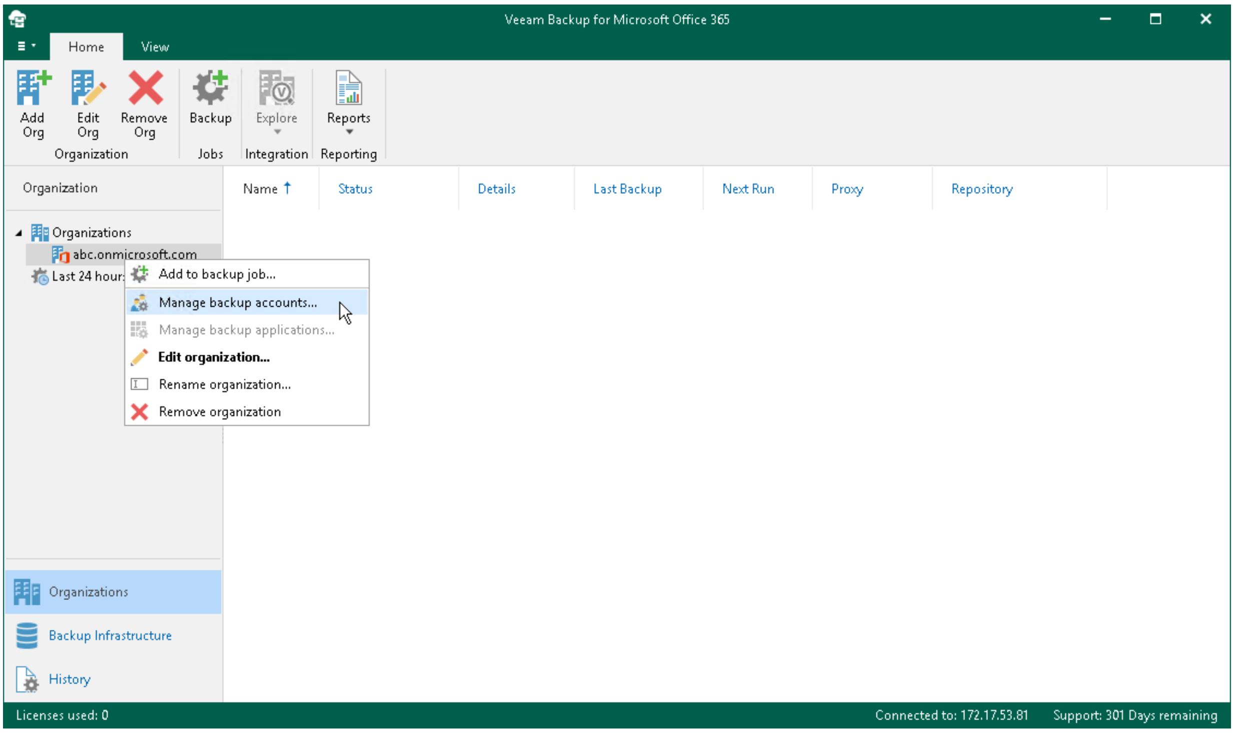
Adding Accounts

For Microsoft Office 365 organizations added using either basic authentication or modern authentication with legacy protocols allowed, you can configure auxiliary backup accounts.

To add auxiliary backup accounts to the backup configuration, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, right-click an organization and select **Manage backup accounts**.

   Mind that the **Manage backup accounts** option is unavailable for organizations with modern app-only authentication. For organizations added using modern app-only authentication, you use the **Manage backup applications** option, as described in Adding Applications.

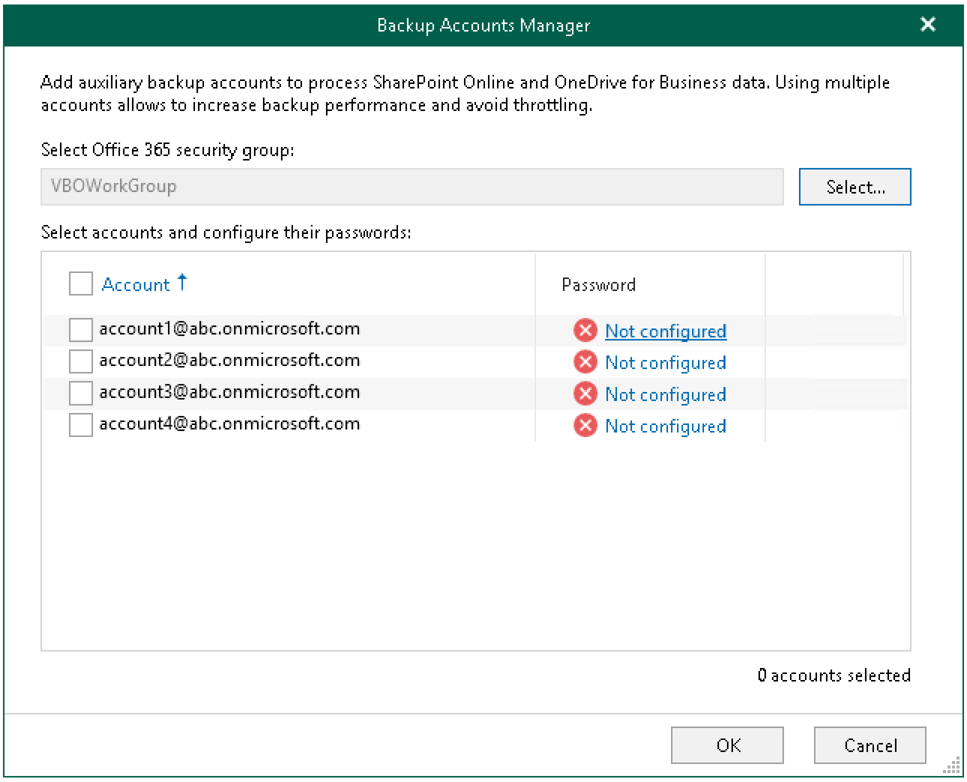
3. In the **Backup Accounts Manager** window, click **Select**.
4. In the **Select Security Group** window, select a security group with accounts that you want to use as auxiliary backup accounts and click **Add**.

   Consider the following:

   - The entire security group will be granted the *Site Collection Administrator* role. If a user ceases to be a member of the selected group, the role is automatically revoked for this user.
   - 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 does not use an account under which you add your Office 365 organization.

5. In the **Select accounts and configure their passwords** list, select check boxes next to accounts that you want to add as backup applications.

6. In the **Password** column, click **Not configured**.



Backup Accounts Manager

Add auxiliary backup accounts to process SharePoint Online and OneDrive for Business data. Using multiple accounts allows to increase backup performance and avoid throttling.

Select Office 365 security group:

VBOWorkGroup

Select Office 365 security group: VBOWorkGroup [Select...]

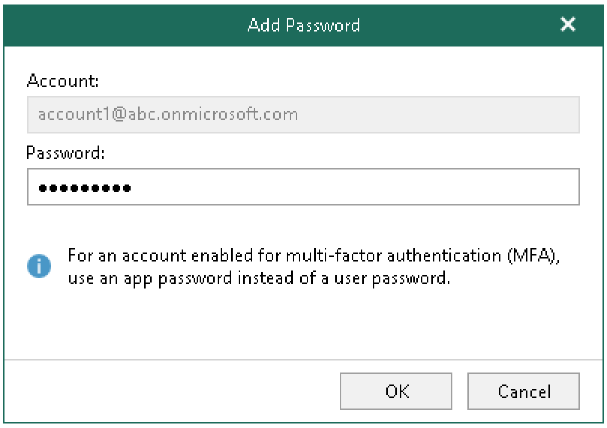
Select accounts and configure their passwords:

□ Account ↑	Password
□ account1@abc.onmicrosoft.com	☒ Not configured
□ account2@abc.onmicrosoft.com	☒ Not configured
□ account3@abc.onmicrosoft.com	☒ Not configured
□ account4@abc.onmicrosoft.com	☒ Not configured

0 accounts selected

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

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



Add Password

Account: account1@abc.onmicrosoft.com

Password: ●●●●●●●●●

For an account enabled for multi-factor authentication (MFA), use an app password instead of a user password.

Changing Password and Removing Accounts

You can change the password of each configured backup account or you can remove an account from the backup configuration if you no longer want to use it.

Changing Password

To change the password of a backup account, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, right-click an organization and select **Manage backup accounts**.
3. In the **Backup Accounts Manager** window, in the **Password** column, click **Configured** next to the backup account whose password you want to change.
4. In the **Edit Password** window, modify the password 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** window, in the **Account** column, clear check boxes next to accounts that you no longer want to use and click **OK.**

Backup Applications

You can configure Microsoft Azure AD applications for Microsoft Office 365 organizations added using modern app-only authentication to minimize throttling when backing up Microsoft SharePoint Online and Microsoft OneDrive for Business data. You can add existing applications to the backup configuration or create new applications in your Microsoft 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 Azure AD application secret.

> **NOTE:**
>
> For Microsoft Office 365 organizations added using either basic authentication or modern authentication with legacy protocols allowed, you use backup accounts instead. For more information, see Backup Accounts.

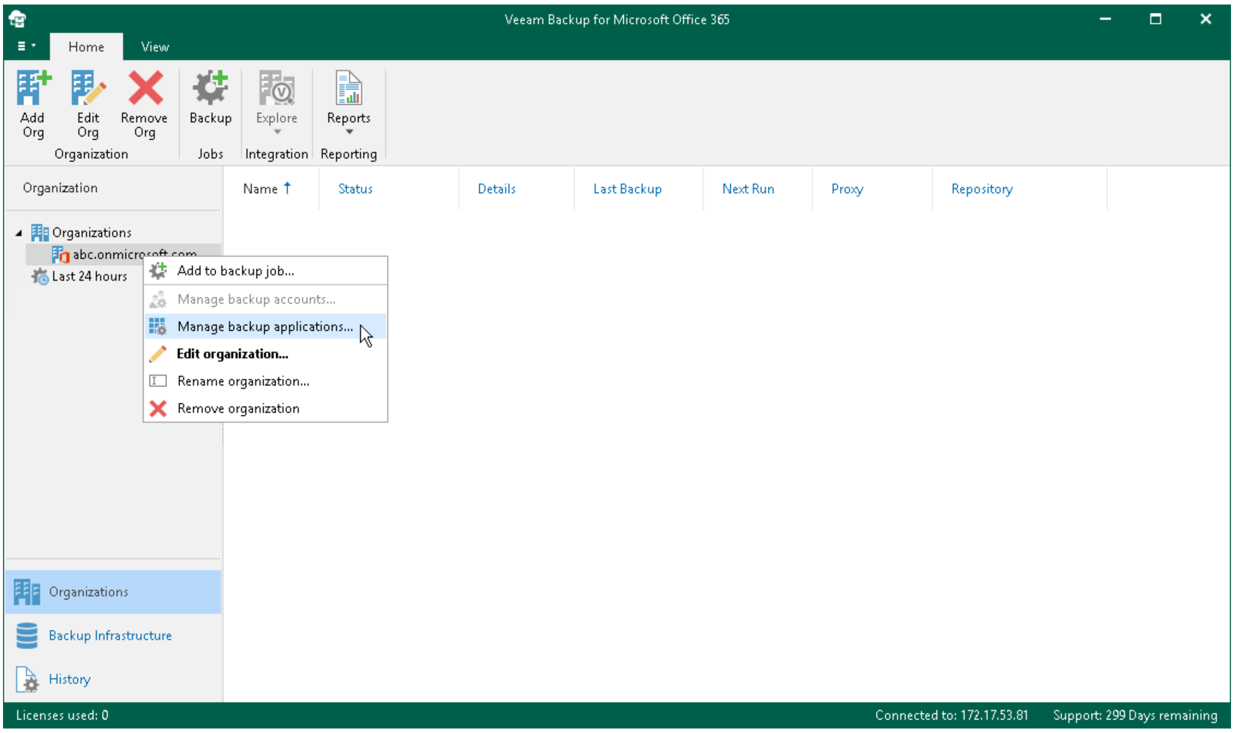
Adding Applications

When you add Azure 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 Online and Microsoft OneDrive for Business data. For more information about Azure AD applications, see this Microsoft article.

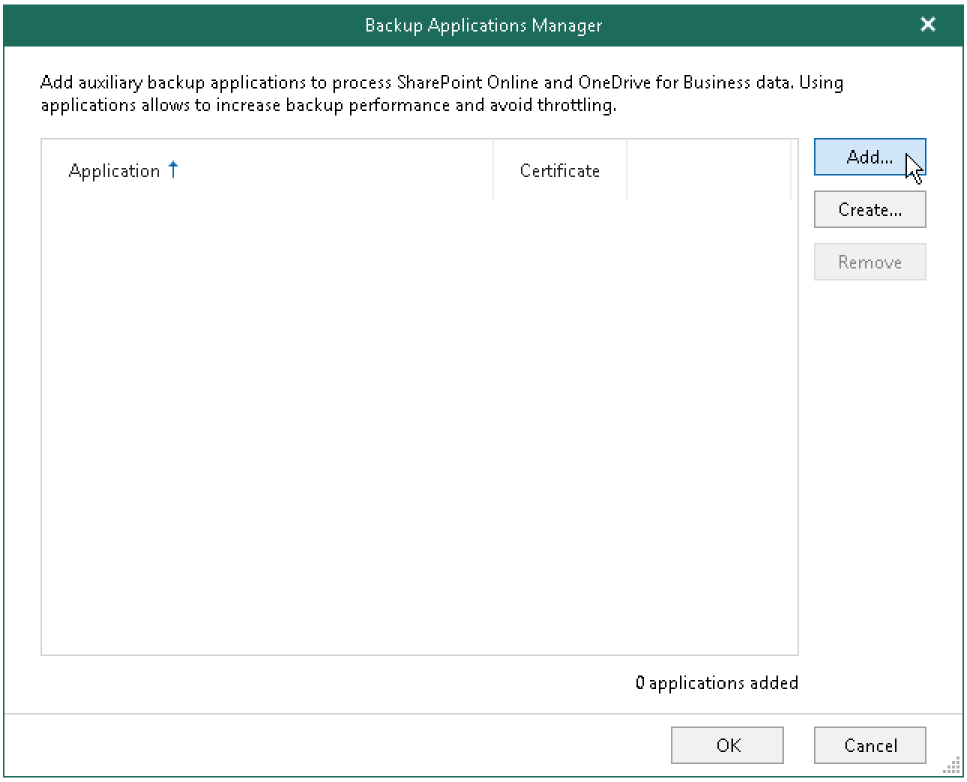
To add Azure AD applications to the backup configuration, do the following:

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

   Mind that the **Manage backup applications** option is available only for organizations added using modern app-only authentication. For organizations added using either basic authentication or modern authentication with legacy protocols allowed, you use the **Manage backup accounts** option, as described in Adding Accounts.



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



Backup Applications Manager

Add auxiliary backup applications to process SharePoint Online and OneDrive for Business data. Using applications allows to increase backup performance and avoid throttling.

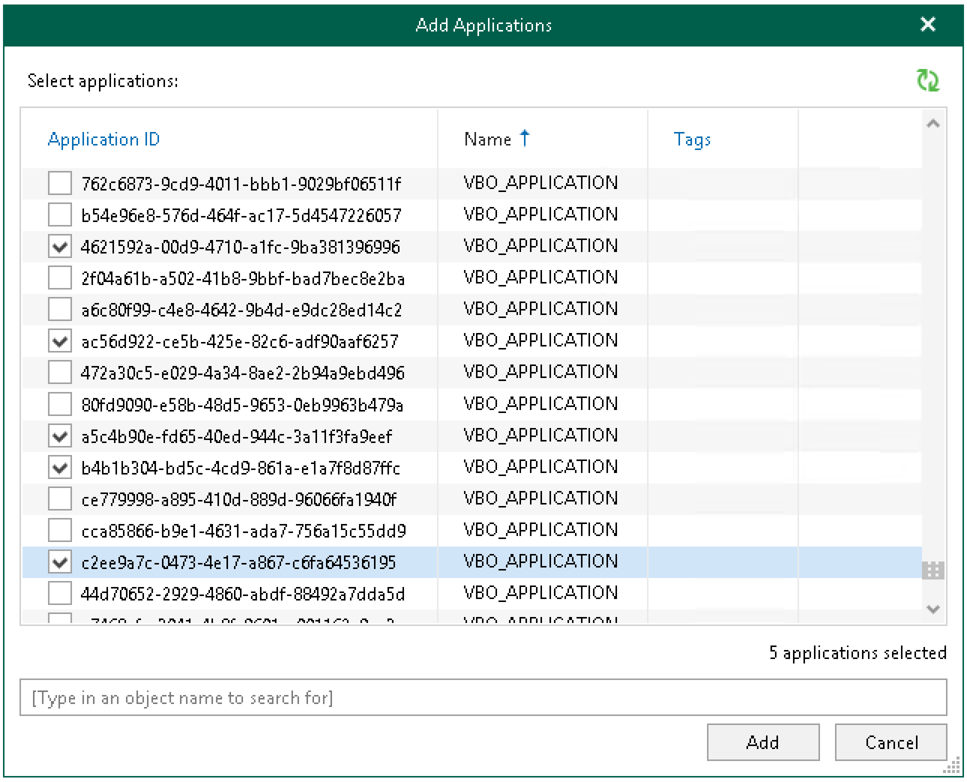
Application	Certificate

0 applications added

4. In the **Add Applications** window, select Azure 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 Azure AD application that you use when adding your Microsoft Office 365 organization; such applications are never used to reduce throttling.



Add Applications

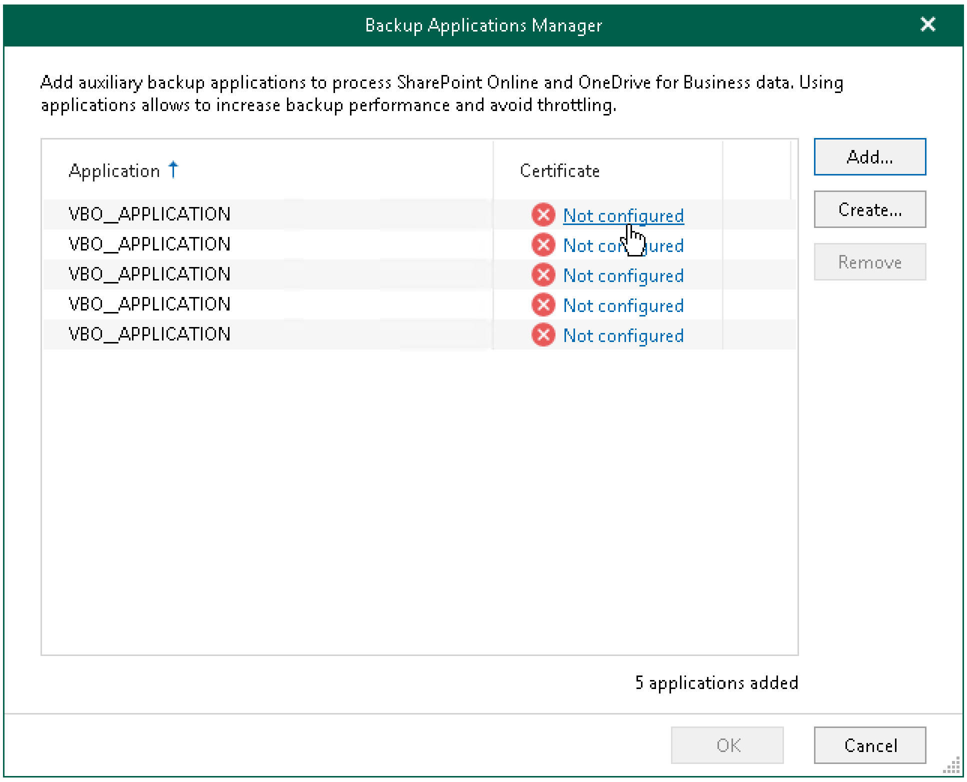
Select applications:

Application ID	Name	Tags
□ 762c6873-9cd9-4011-bbb1-9029bf06511f	VBO_APPLICATION	
□ b54e96e8-576d-464f-ac17-5d4547226057	VBO_APPLICATION	
☑ 4621592a-00d9-4710-a1fc-9ba381396996	VBO_APPLICATION	
□ 2f04a61b-a502-41b8-9bbf-bad7bec8e2ba	VBO_APPLICATION	
□ a6c80f99-c4e8-4642-9b4d-e9dc28ed14c2	VBO_APPLICATION	
☑ ac56d922-ce5b-425e-82c6-adf90aaf6257	VBO_APPLICATION	
□ 472a30c5-e029-4a34-8ae2-2b94a9ebd496	VBO_APPLICATION	
□ 80fd9090-e58b-48d5-9653-0eb9963b479a	VBO_APPLICATION	
☑ a5c4b90e-fd65-40ed-944c-3a11f3fa9eef	VBO_APPLICATION	
☑ b4b1b304-bd5c-4cd9-861a-e1a7f8d87ffc	VBO_APPLICATION	
□ ce779998-a895-410d-889d-96066fa1940f	VBO_APPLICATION	
□ cca85866-b9e1-4631-ada7-756a15c55dd9	VBO_APPLICATION	
☑ c2ee9a7c-0473-4e17-a867-c6fa64536195	VBO_APPLICATION	
□ 44d70652-2929-4860-abdf-88492a7dda5d	VBO_APPLICATION	

5 applications selected

[Type in an object name to search for]

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 Azure AD application.



Add auxiliary backup applications to process SharePoint Online and OneDrive for Business data. Using applications allows to increase backup performance and avoid throttling.

Application	Certificate
VBO_APPLICATION	Not configured
VBO_APPLICATION	Not configured
VBO_APPLICATION	Not configured
VBO_APPLICATION	Not configured
VBO_APPLICATION	Not configured

5 applications added

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.

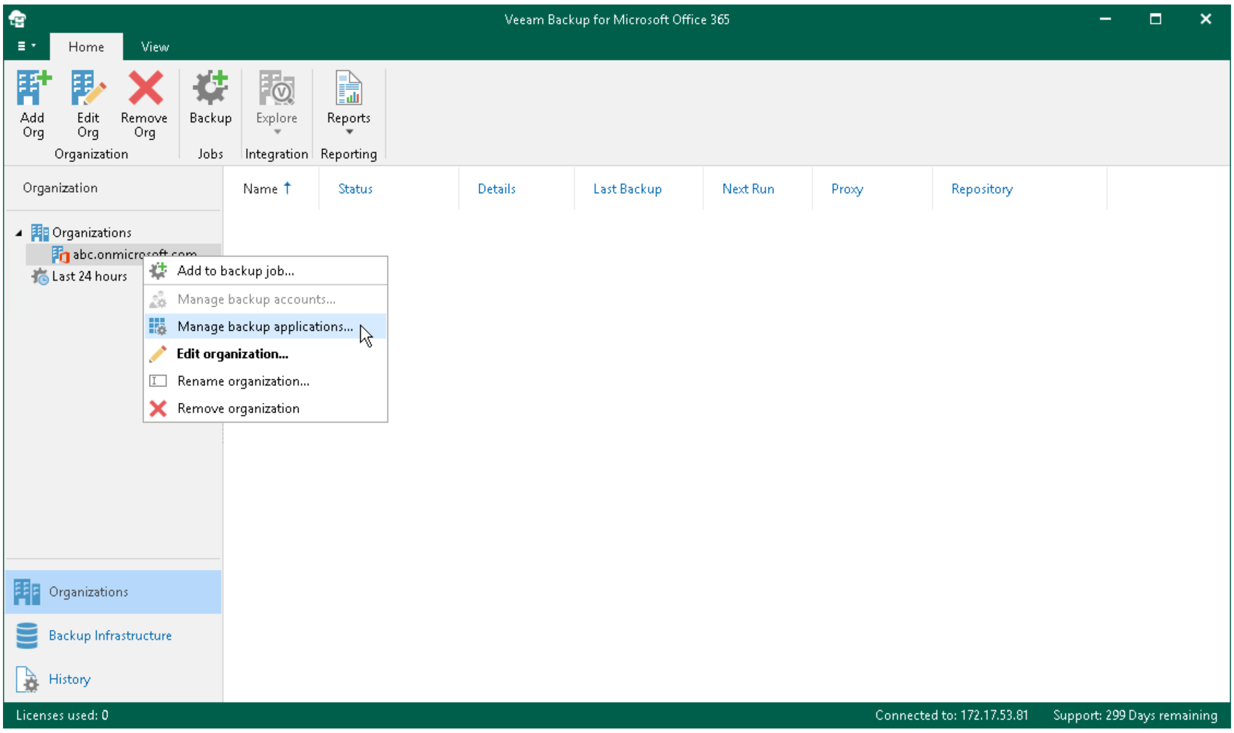
Creating Applications

When you create a new Azure 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 Azure AD applications, see this Microsoft article.

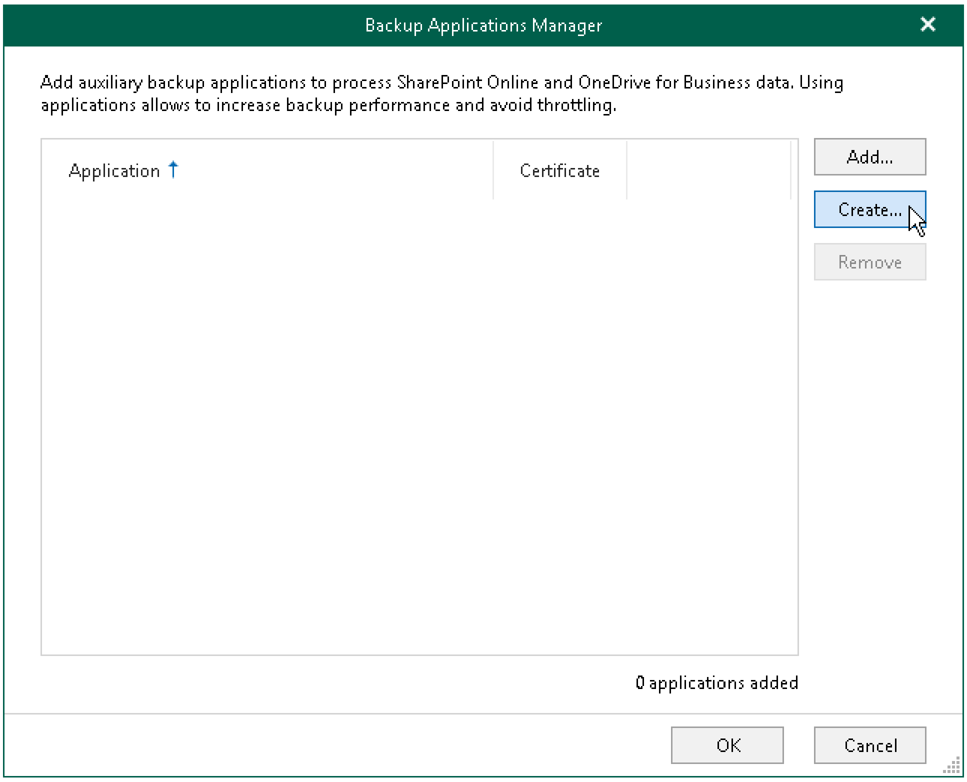
To create Azure AD applications and add them to the backup configuration, do the following:

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

   Mind that the **Manage backup applications** option is available only for organizations added using modern app-only authentication. For organizations added using either basic authentication or modern authentication with legacy protocols allowed, you can use the **Manage backup accounts** option, as described in Adding Accounts.



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

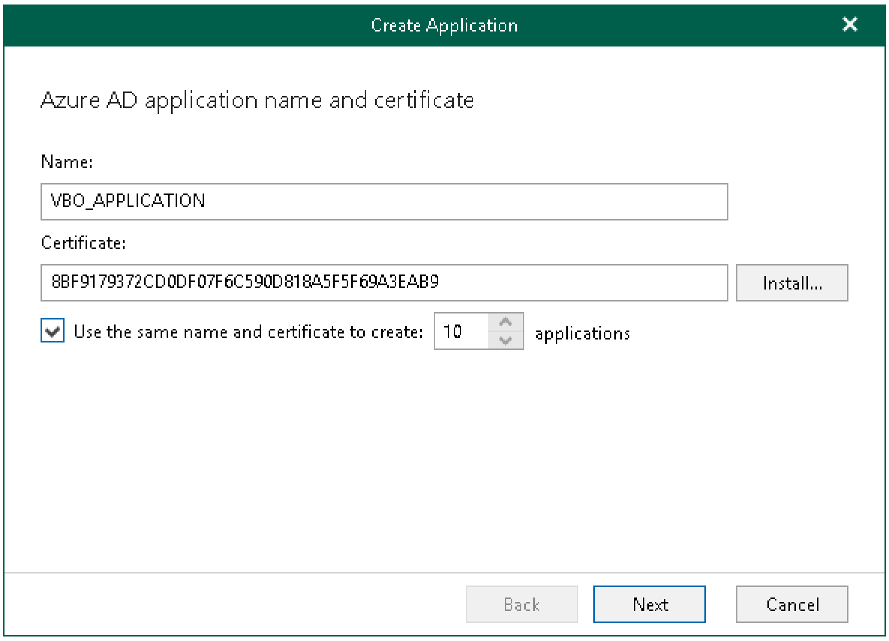


Backup Applications Manager
Add auxiliary backup applications to process SharePoint Online and OneDrive for Business data. Using applications allows to increase backup performance and avoid throttling.
Application
Certificate
Add...
Create...
Remove
0 applications added
OK
Cancel

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 Azure 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 Azure AD application, select the **Use the same name and certificate to create N applications** check box and specify how many applications Veeam Backup for Microsoft 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.



Azure AD application name and certificate

Name: VBO_APPLICATION

Certificate: 8BF9179372CD0DF07F6C590D818A5F5F69A3EAB9

☑ Use the same name and certificate to create: 10 applications

5. In the **Create Application** window, click **Copy code** to copy an authentication code.Mind that a code is valid for 15 minutes.

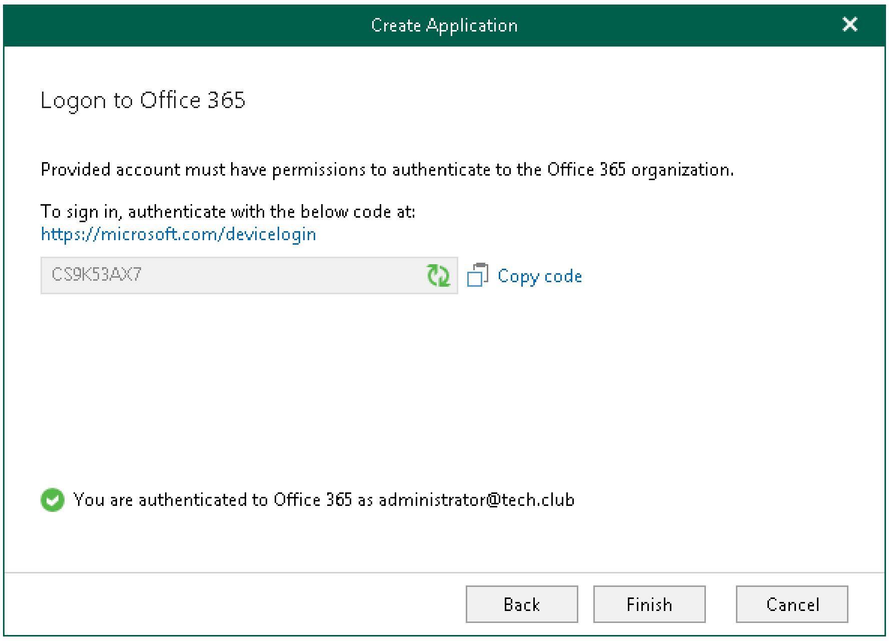
   You can click **Refresh** to request a new code from Microsoft.

6. Click the link to the Microsoft portal.

7. On the **Microsoft Azure device logon** page, paste the code that you have copied and sign in to Azure.

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

8. Return to the **Create Application** window and click **Finish**.



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

CS9K53AX7

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

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** window, in the **Certificate** column, click **Configured** next to the application whose certificate you want to update.
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 **Backup Applications Manager** window, select an application in the list and click **Remove**.

   You can select multiple applications using the **[CTRL]** key.

Editing Organization Parameters

You can edit the following organization parameters:

- Organization deployment type.

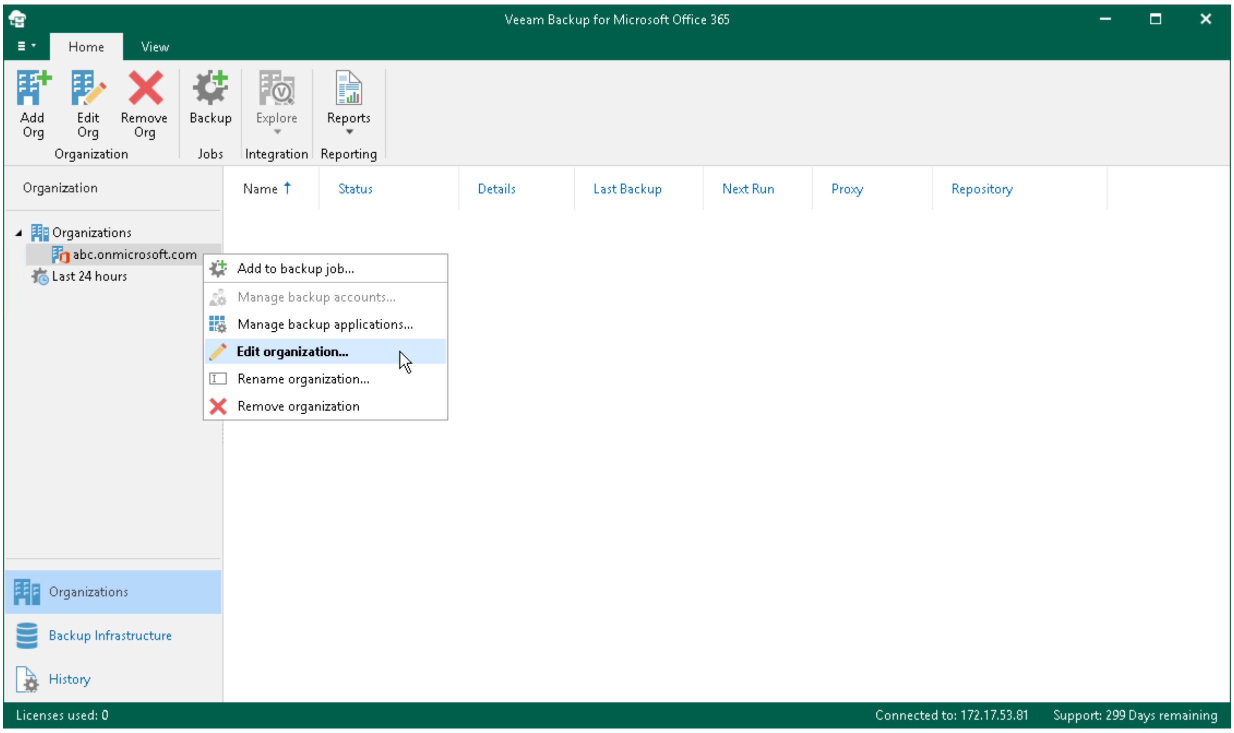
  Consider that you cannot change the *Microsoft Office 365* organization deployment type to the *On-premises* type.

- 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**.

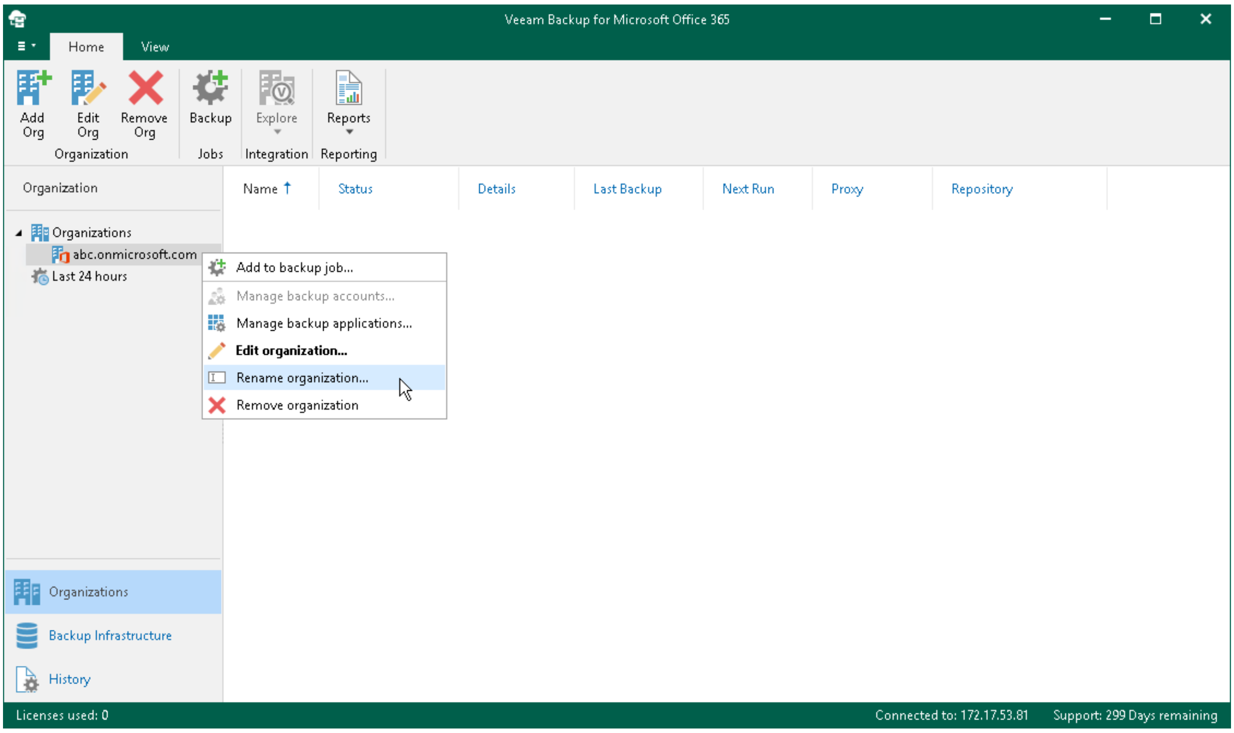


Renaming Organizations

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:

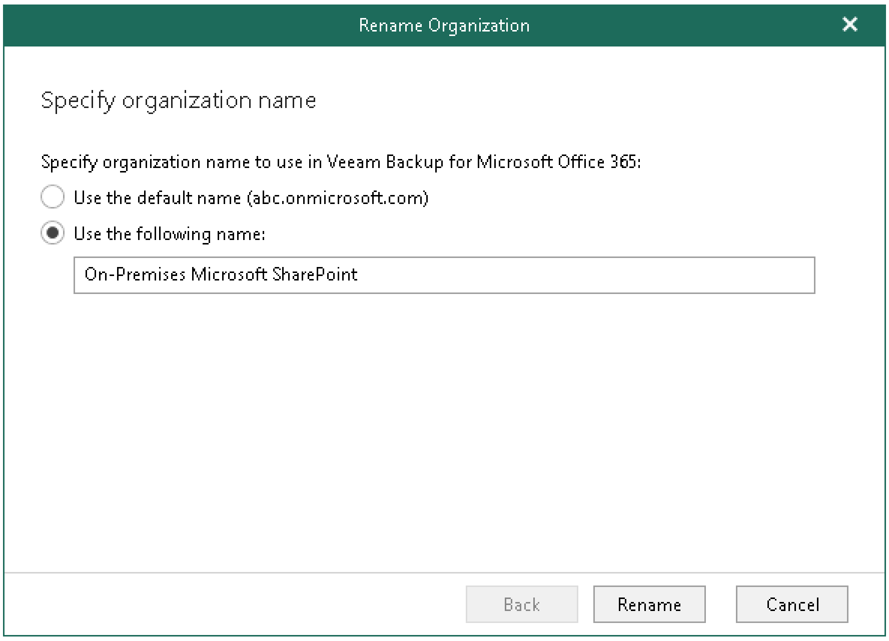
1. Open the **Organizations** view.
2. In the inventory pane, right-click an organization and select **Rename organization**.



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 (abc.onmicrosoft.com)

● Use the following name:

On-Premises Microsoft SharePoint

Removing Organizations

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

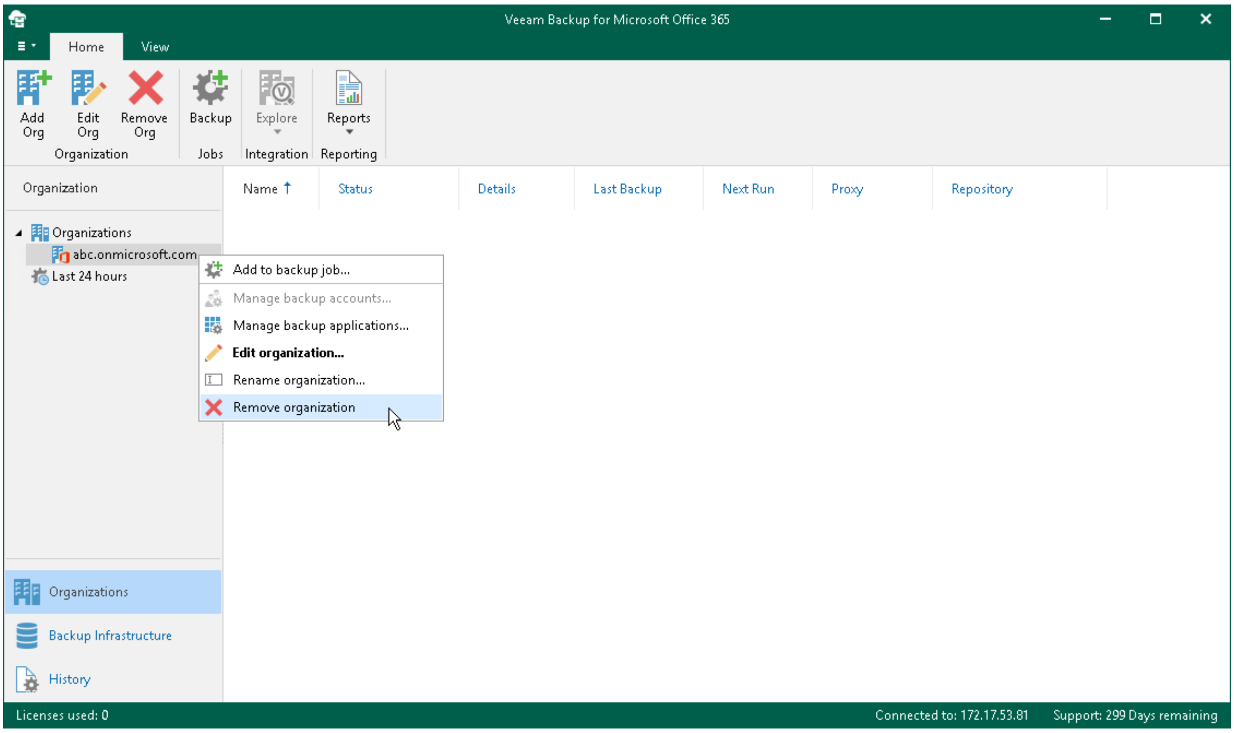
Consider the following:

- 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 inventory 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 Microsoft 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, teams 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 for backup and restore:

- 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.

- Teams

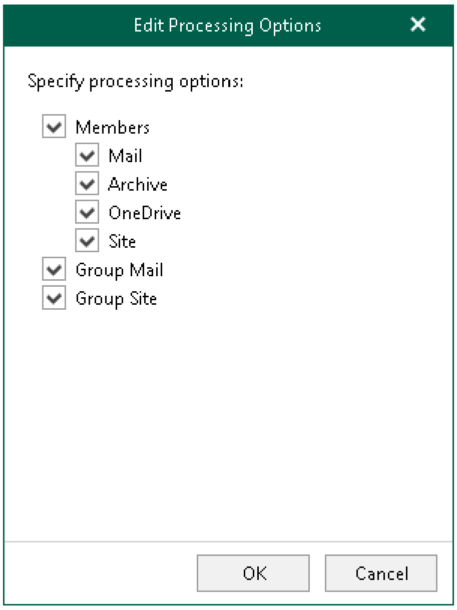
  Consists of Microsoft Teams teams.

- Organizations

  Consists of organization objects and their processing options.

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

Processing and exclusion options can be selected at the Select Objects to Back Up and Select Objects to Exclude steps of the **New Backup Job** wizard.



Specify processing options:

☑ Members
  ☑ Mail
  ☑ Archive
  ☑ OneDrive
  ☑ Site
☑ Group Mail
☑ Group Site

Groups

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

Group Type	Options for Microsoft Office 365 Organizations	Options for On-premises Microsoft Exchange Organizations
O365 group (available only in Office 365 organizations)	When configuring Microsoft Office 365 organizations, the following set of processing/exclusion options is available: • *Members* with *Mail*, *Archive*, *OneDrive* and *Site* • *Group Mail* • *Group Site*	N/A
Security Group	*Members* with *Mail*, *Archive*, *OneDrive* and *Site*	*Members* with *Mail* and *Archive* 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	Options for Microsoft Office 365 Organizations	Options for On-premises Microsoft Exchange Organizations	Options for On-premises Microsoft SharePoint Organizations
User	*Mail*, *Archive*, *OneDrive* and *Site*	*Mail* and *Archive*	*OneDrive* and *Site*
Shared mailbox (available only in Office 365 and Exchange organizations)			N/A

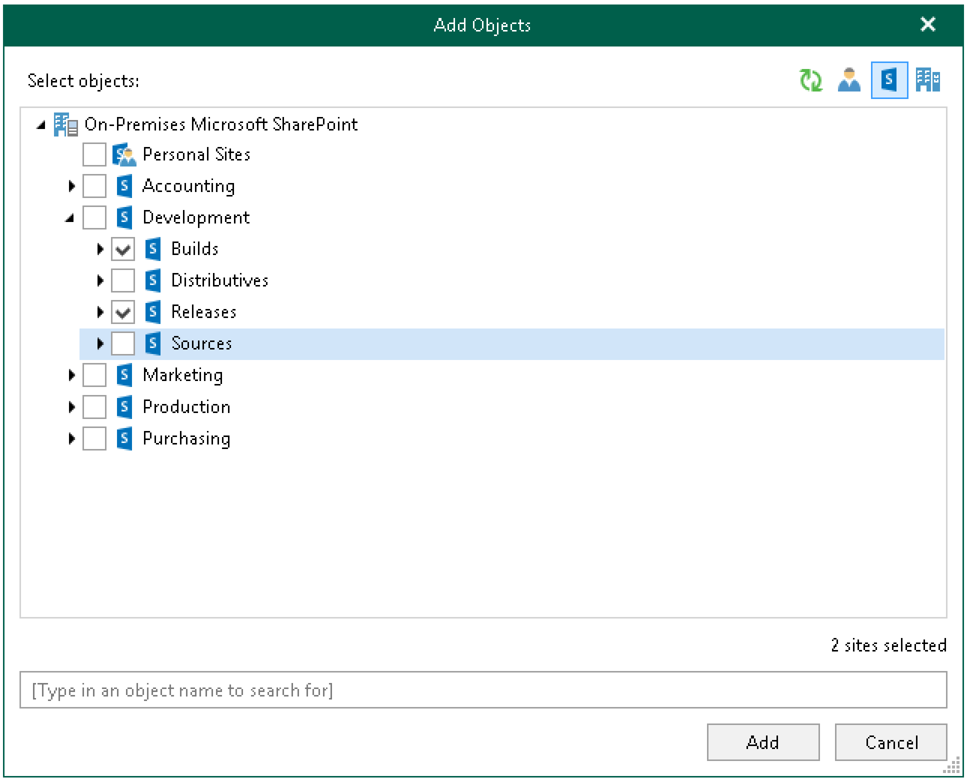
User Type	Options for Microsoft Office 365 Organizations	Options for On-premises Microsoft Exchange Organizations	Options for On-premises Microsoft SharePoint Organizations
Public mailbox (available only in Office 365 and Exchange organizations)			

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 SharePoint 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.



- On-Premises Microsoft SharePoint
  - ☐ Personal Sites
  - ☐ Accounting
  - ☐ Development
    - ☑ Builds
    - ☐ Distributives
    - ☑ Releases
    - ☐ Sources
  - ☐ Marketing
  - ☐ Production
  - ☐ Purchasing

2 sites selected

[Type in an object name to search for]

Teams

Consider the following:

- Objects of this type do not have any processing/exclusion options.
- Objects of this type are available in Microsoft Office 365 organizations only.

- When you add an object of this type to a backup job, Veeam Backup for Microsoft Office 365 backs up the following objects:
  - Team Chat folder of the group mailbox that belongs to the Office 365 group associated with the backed-up team.
  - Document library of the SharePoint team site.
  - Team metadata: settings of the team, information about team members, channels, tabs, applications, and so on.

Organizations

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

Microsoft Office 365 Organizations	Options for On-premises Microsoft Exchange Organizations	Options for On-premises Microsoft SharePoint Organizations
Mail, *Archive*, *OneDrive*, *Sites* and *Teams*	*Mail* and *Archive*	*OneDrive* and *Sites*

Creating Backup Job

To create a backup job, do the following:

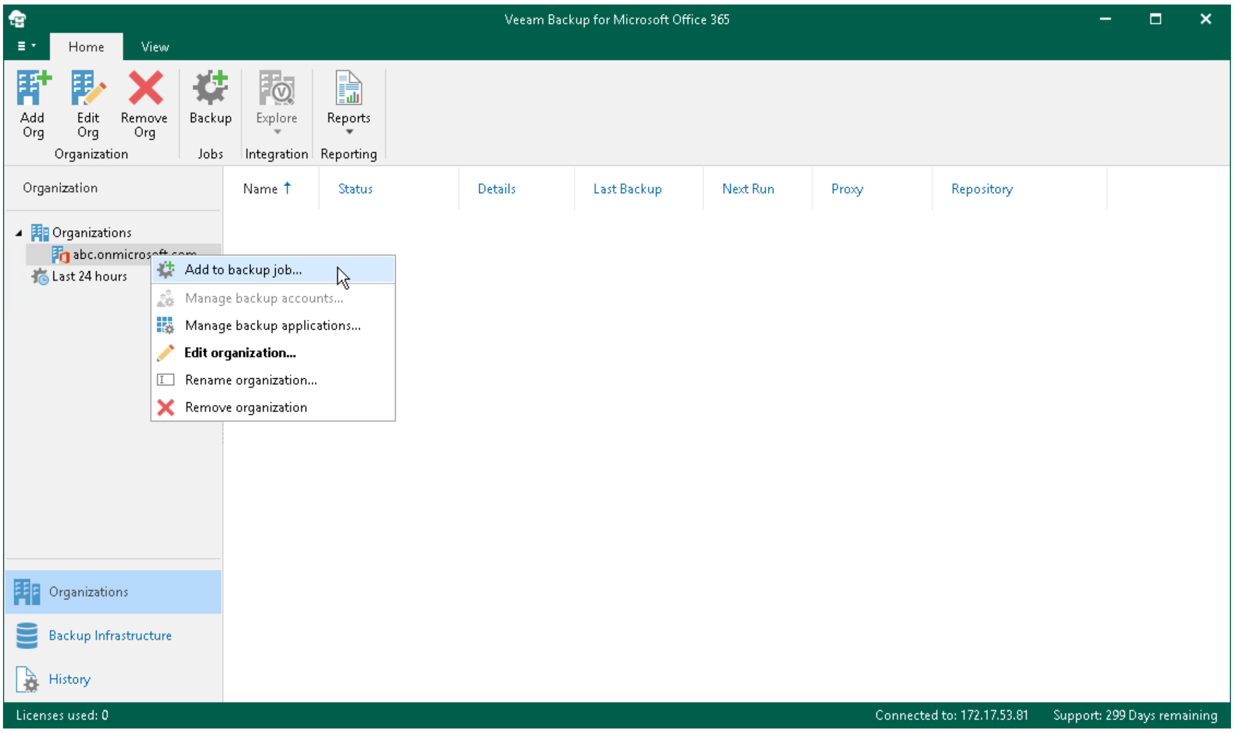
1. Launch the New Backup Job wizard.
2. Specify a backup job name.
3. Select objects to back up.
4. Select objects to exclude.
5. Specify a backup proxy and repository.
6. Specify scheduling options.

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.

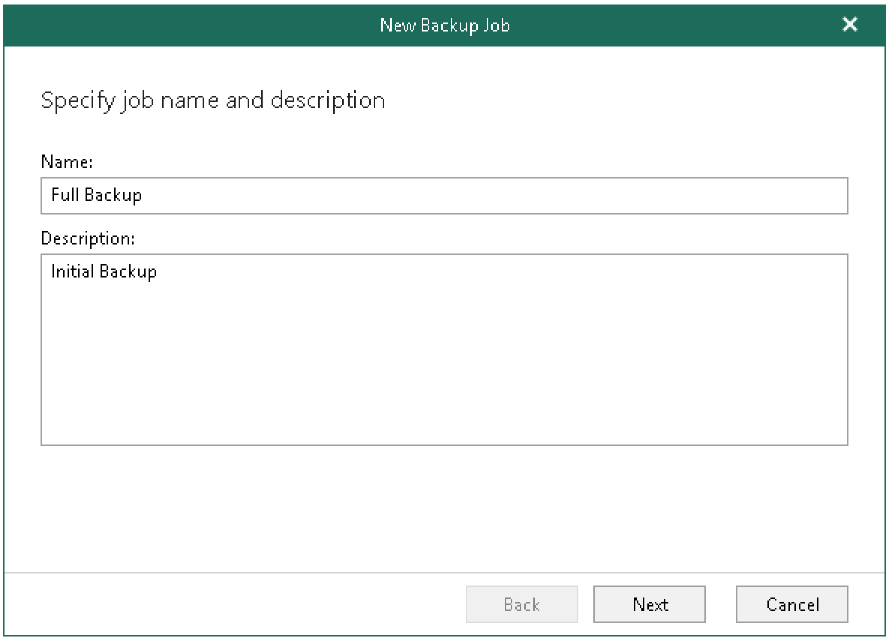
   Alternatively, in the inventory pane, right-click an organization and select **Add to backup job**.



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

Step 3. Select Objects to Back Up

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

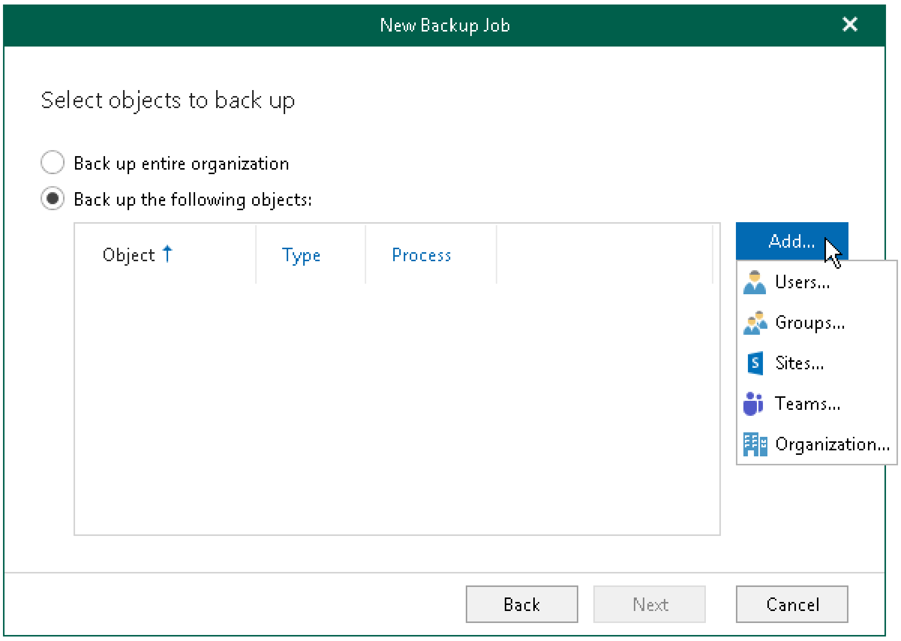
In Veeam Backup for Microsoft Office 365, you can select to back up an entire organization or specify users, groups, sites, teams and organizations.

Consider 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, processing options are applied to all users, groups and sites in the selected organization.

To specify objects to back up, do the following:

1. Select the **Back up the following objects** option.
2. Click **Add** and select one of the following options: *Users*, *Groups*, *Sites*, *Teams* or *Organization*.



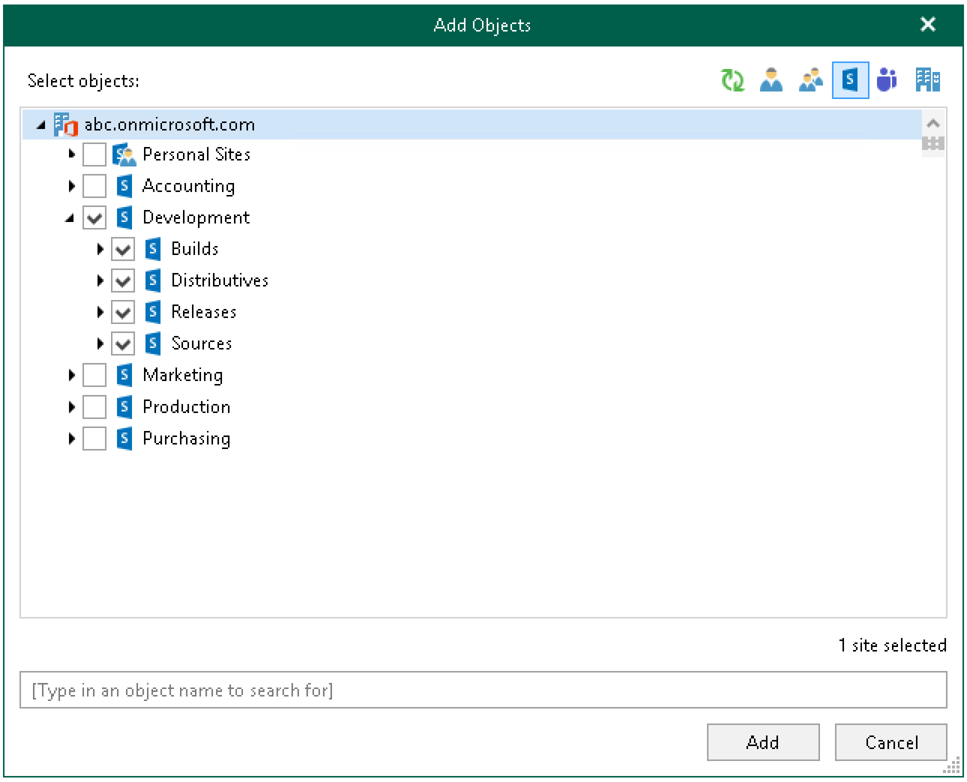
3. In the **Add Objects** window, select users, groups, sites, teams and organizations that you want to back up.

   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.

> **NOTE:**
>
> If you select a group, site or team as an individual object for backup (and not as a part of a user account, group or organization), this object does not consume a unit in the license.

4. Click **Add**.



Add Objects

Select objects:

- abc.onmicrosoft.com
  - □ Personal Sites
  - □ Accounting
  - ☑ Development
    - ☑ Builds
    - ☑ Distributives
    - ☑ Releases
    - ☑ Sources
  - □ Marketing
  - □ Production
  - □ Purchasing

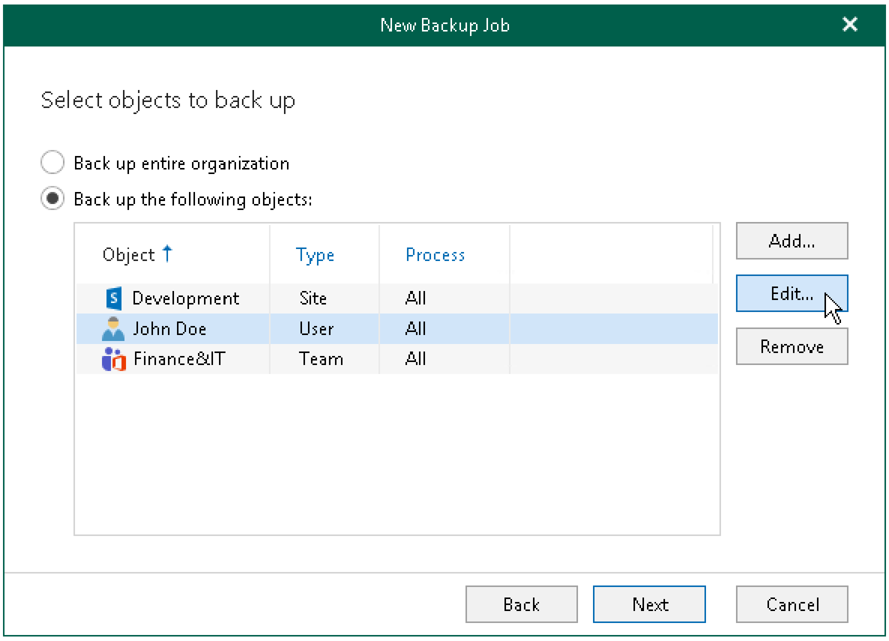
1 site selected

[Type in an object name to search for]

5. If you want to specify processing options, do the following:

   a. In the list of objects to back up, select the necessary object and click **Edit**.

      Mind that you cannot edit processing options for the *Sites*, *Teams* and *Public Mailbox* objects.



New Backup Job

Select objects to back up

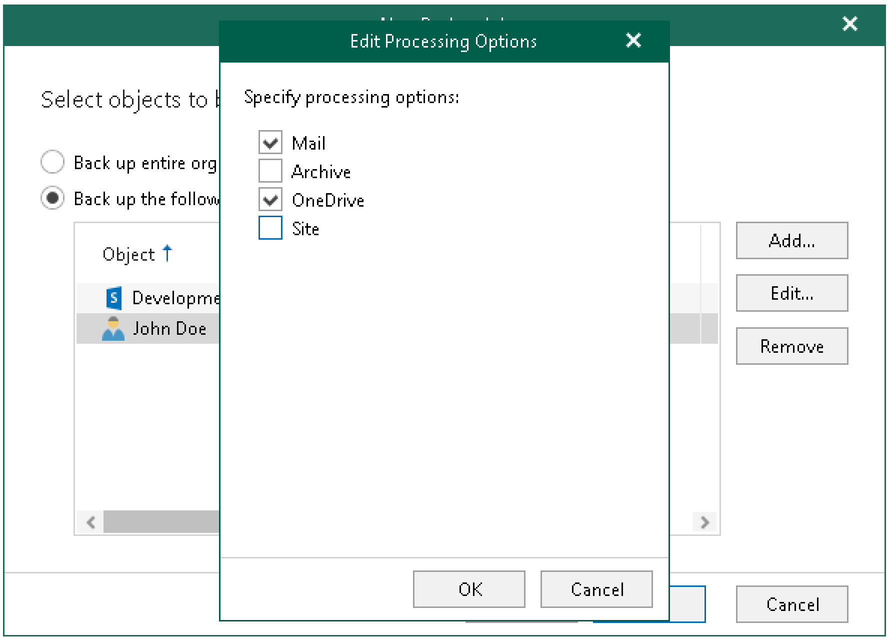
○ Back up entire organization

● Back up the following objects:

Object ↑	Type	Process
Development	Site	All
John Doe	User	All
Finance&IT	Team	All

b. In the **Edit Processing Options** window, select processing options and click **OK**.

For more information about available object types and their processing options, see Organization Object Types.



Edit Processing Options

Specify processing options:

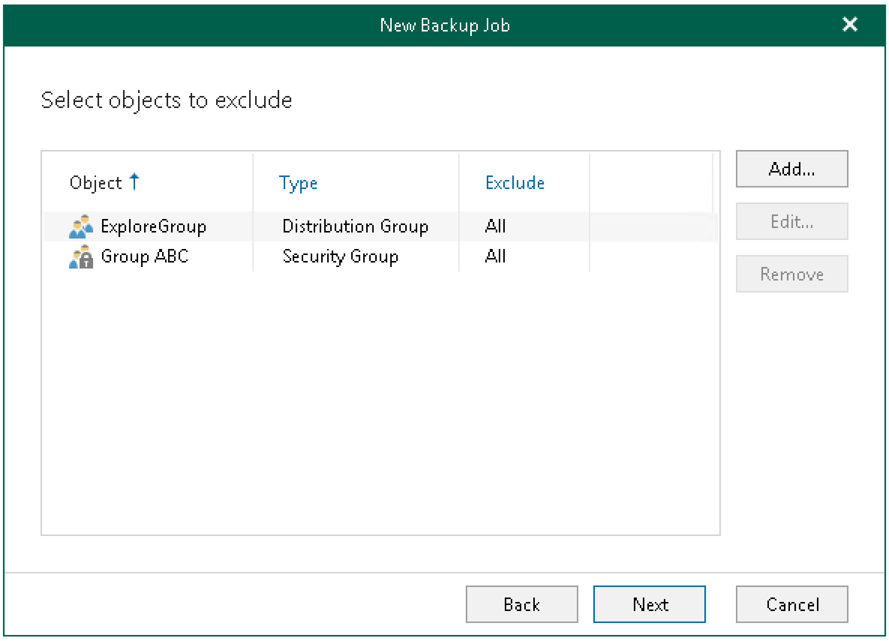
☑ Mail
□ Archive
☑ OneDrive
□ Site

Step 4. Select Objects to Exclude

At this step of the wizard, select objects that you do not want to back up.

To exclude an object, click **Add** and select users, groups, sites and teams that you do not want to back up.

> **NOTE:**
>
> 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*.



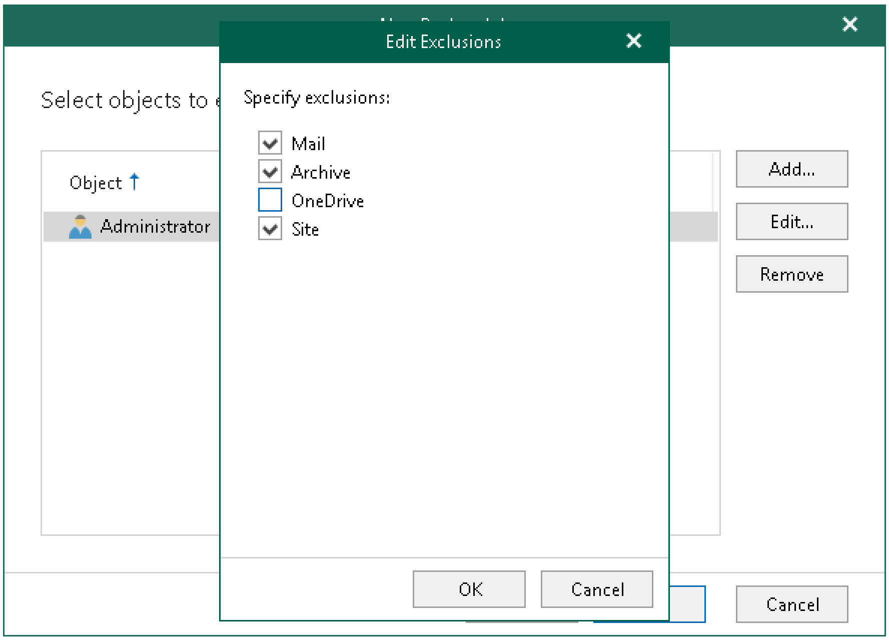
Object	Type	Exclude
ExploreGroup	Distribution Group	All
Group ABC	Security Group	All

If you want to specify exclusion options, select an object in the list, click **Edit** and in the **Edit Exclusions** 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*, *Teams* and *Public Mailbox* object types.

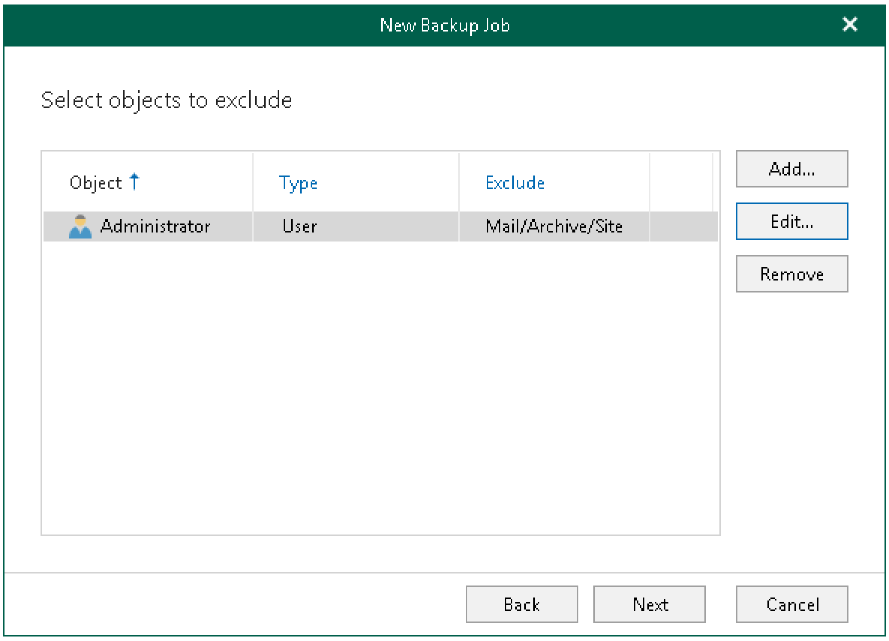
The following is an example where the *Mail*, *Archive* and *Site* objects are excluded from the backup for the *Administrator* user. Veeam Backup for Microsoft Office 365 will only back up OneDrive data for this user.



Specify exclusions:

☑ Mail
☑ Archive
☐ OneDrive
☑ Site

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



Object	Type	Exclude
Administrator	User	Mail/Archive/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.

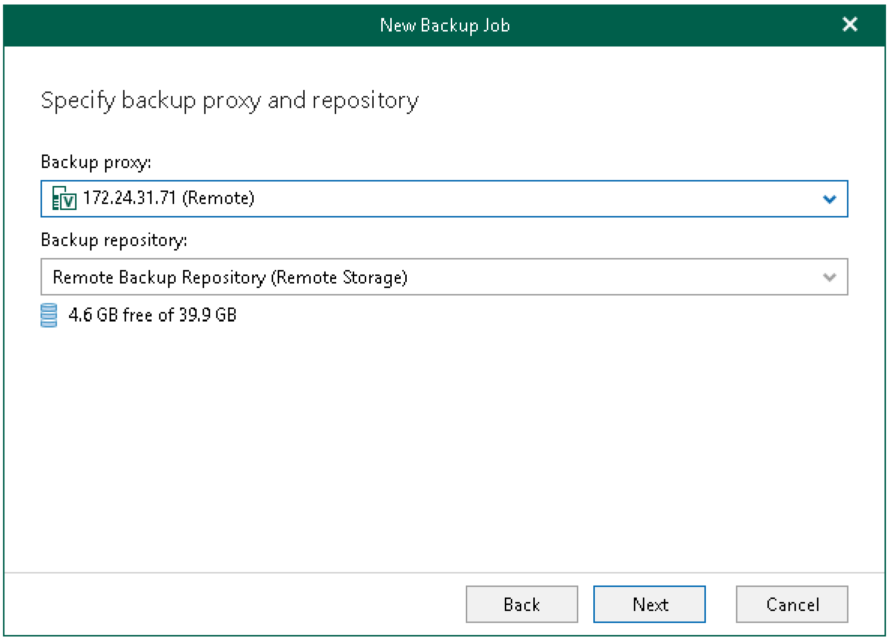
To specify a backup proxy server and backup repository, do the following:

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

2. From the **Backup repository** drop-down list, select a backup repository to which you want to save your data.

   You can select a 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.



New Backup Job

Specify backup proxy and repository

Backup proxy: 172.24.31.71 (Remote)

Backup repository: Remote Backup Repository (Remote Storage)

4.6 GB free of 39.9 GB

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 one of the following options:

   - **Daily at this time**. Select this option if you want to run the job daily at the specified hours.

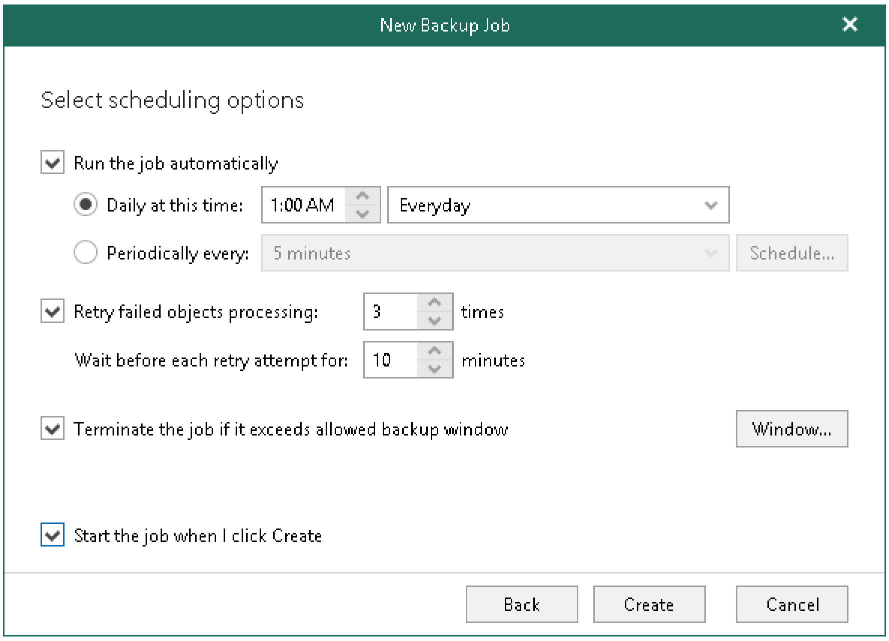
   - **Periodically every**. Select this option if you want to run the job every *N* minutes.

2. Select the **Retry failed objects processing** check box and specify the maximum number of retry attempts. You can also set an interval between subsequent retries.

3. Select the **Terminate the job if it exceeds allowed backup window** check box, click **Window** and specify allowed and prohibited hours for the backup job. For more information, see Selecting Time Periods.

4. 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.



New Backup Job

Select scheduling options

☑ Run the job automatically

● Daily at this time: 1:00 AM Everyday

○ Periodically every: 5 minutes

☑ Retry failed objects processing: 3 times

Wait before each retry attempt for: 10 minutes

☑ Terminate the job if it exceeds allowed backup window

☑ Start the job when I click Create

Selecting Time Periods

When you click **Window**, the **Time Periods** dialog appears in which you can:

- Set the **Permitted** execution time frame for the backup 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.

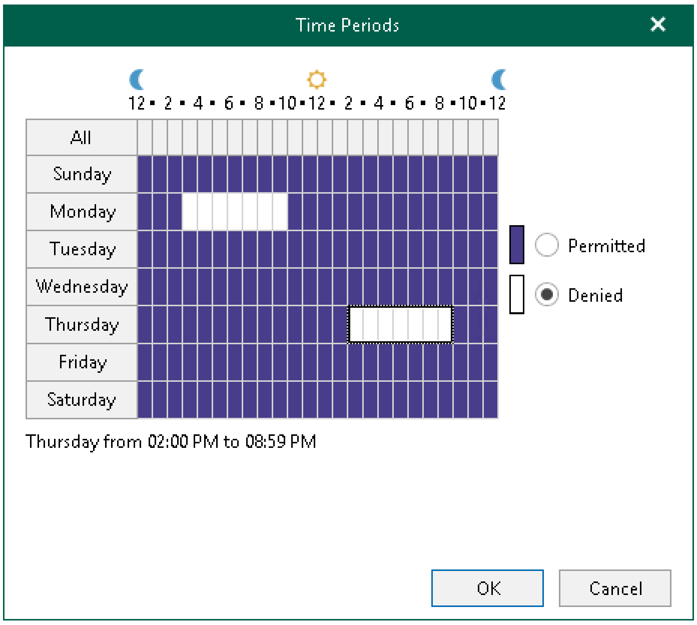
   In addition, you can:

   - 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.
   - 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.



Thursday from 02:00 PM to 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.

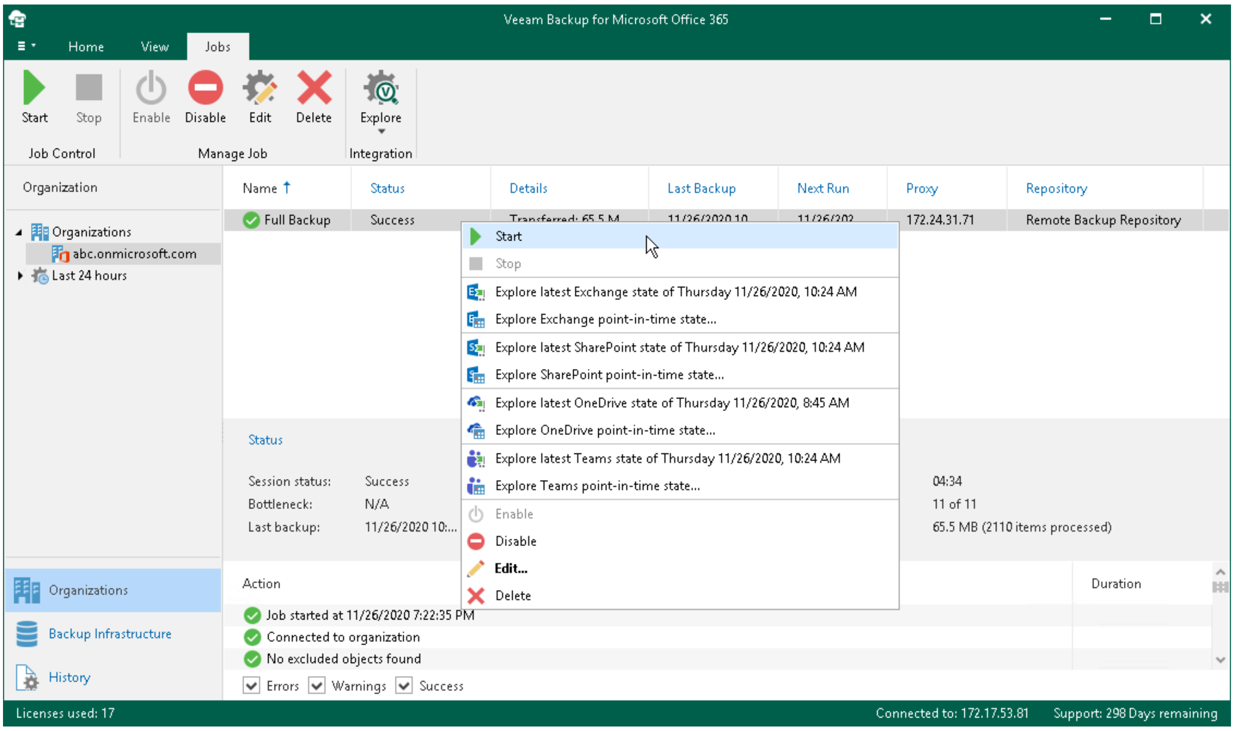
Starting Backup Job

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**.


Veeam Backup for Microsoft Office 365
Home
View
Jobs
Start
Stop
Enable
Disable
Edit
Delete
Explore
Job Control
Manage Job
Integration
Organization
Organizations
abc.onmicrosoft.com
Last 24 hours
Start
Stop
Explore latest Exchange state of Thursday 11/26/2020, 10:24 AM
Explore Exchange point-in-time state...
Explore latest SharePoint state of Thursday 11/26/2020, 10:24 AM
Explore SharePoint point-in-time state...
Explore latest OneDrive state of Thursday 11/26/2020, 8:45 AM
Explore OneDrive point-in-time state...
Explore latest Teams state of Thursday 11/26/2020, 10:24 AM
Explore Teams point-in-time state...
Enable
Disable
Edit...
Delete
Organizations
Backup Infrastructure
History
☑ Errors ☑ Warnings ☑ Success

Name	Status	Details	Last Backup	Next Run	Proxy	Repository
Full Backup	Success	Transferred: 65.5 M	11/26/2020 10	11/26/202	172.24.31.71	Remote Backup Repository

Status

Session status: Success
Bottleneck: N/A
Last backup: 11/26/2020 10:...

04:34
11 of 11
65.5 MB (2110 items processed)

Action	Duration
Job started at 11/26/2020 7:22:35 PM	
Connected to organization	
No excluded objects found	

Licenses used: 17
Connected to: 172.17.53.81
Support: 298 Days remaining

Stopping Backup Job

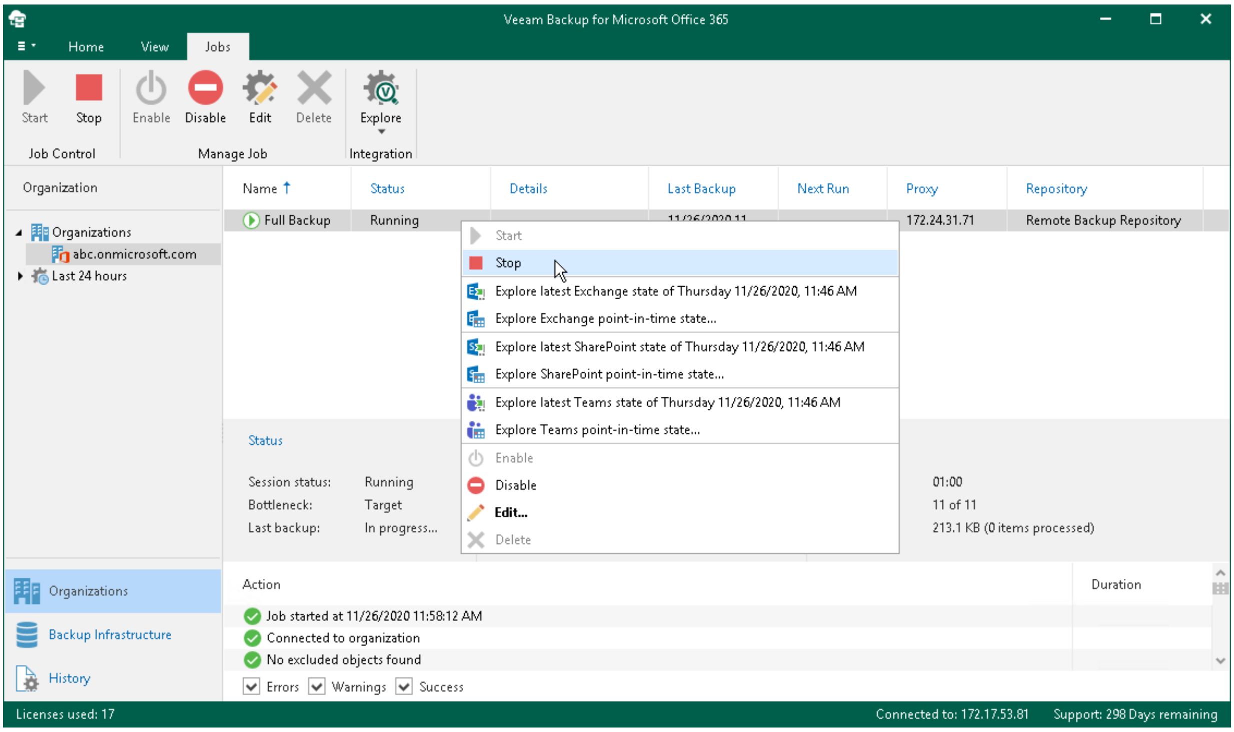
When Veeam Backup for Microsoft Office 365 stops a backup job, it freezes the current backup state preserving what has already been backed up so that you can continue where you left off. To continue, use the **Start** command, as described in Starting Backup Job.

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**.


Veeam Backup for Microsoft Office 365
Home
View
Jobs
Start
Stop
Enable
Disable
Edit
Delete
Explore
Job Control
Manage Job
Integration
Organization
Organizations
abc.onmicrosoft.com
Last 24 hours
Start
Stop
Explore latest Exchange state of Thursday 11/26/2020, 11:46 AM
Explore Exchange point-in-time state...
Explore latest SharePoint state of Thursday 11/26/2020, 11:46 AM
Explore SharePoint point-in-time state...
Explore latest Teams state of Thursday 11/26/2020, 11:46 AM
Explore Teams point-in-time state...
Enable
Disable
Edit...
Delete
Organizations
Backup Infrastructure
History

Name	Status	Details	Last Backup	Next Run	Proxy	Repository
Full Backup	Running		11/26/2020 11...		172.24.31.71	Remote Backup Repository

Status

Session status: Running
Bottleneck: Target
Last backup: In progress...

01:00
11 of 11
213.1 KB (0 items processed)

Action	Duration
✓ Job started at 11/26/2020 11:58:12 AM	
✓ Connected to organization	
✓ No excluded objects found	

☑ Errors ☑ Warnings ☑ Success

Licenses used: 17 Connected to: 172.17.53.81 Support: 298 Days remaining

Enabling or Disabling Backup Job

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

Consider the following:

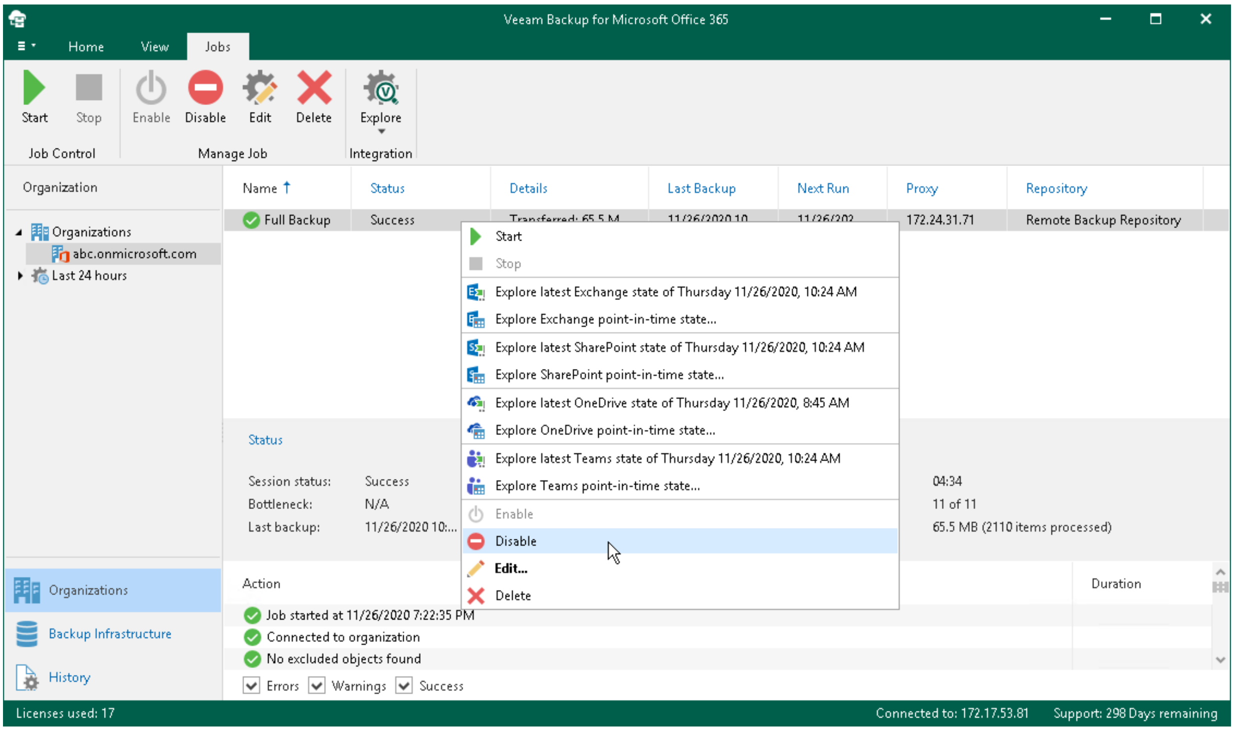
- If a backup job is enabled, it can be executed on schedule.
- If a backup job is disabled, it cannot be executed on schedule but can be executed manually, using the **Start** command.

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** or **Disable** on the ribbon.

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


Veeam Backup for Microsoft Office 365
Home
View
Jobs
Start
Stop
Enable
Disable
Edit
Delete
Explore
Job Control
Manage Job
Integration
Organization
Organizations
abc.onmicrosoft.com
Last 24 hours
Name
Status
Details
Last Backup
Next Run
Proxy
Repository
Start
Stop
Explore latest Exchange state of Thursday 11/26/2020, 10:24 AM
Explore Exchange point-in-time state...
Explore latest SharePoint state of Thursday 11/26/2020, 10:24 AM
Explore SharePoint point-in-time state...
Explore latest OneDrive state of Thursday 11/26/2020, 8:45 AM
Explore OneDrive point-in-time state...
Explore latest Teams state of Thursday 11/26/2020, 10:24 AM
Explore Teams point-in-time state...
Enable
Disable
Edit...
Delete
Organizations
Backup Infrastructure
History
Action
Duration

Name	Status	Details	Last Backup	Next Run	Proxy	Repository
Full Backup	Success	Transferred: 65.5 M	11/26/2020 10	11/26/202	172.24.31.71	Remote Backup Repository

Status

Session status: Success
Bottleneck: N/A
Last backup: 11/26/2020 10:...

04:34
11 of 11
65.5 MB (2110 items processed)

Job started at 11/26/2020 7:22:35 PM
Connected to organization
No excluded objects found

☑ Errors ☑ Warnings ☑ Success

Licenses used: 17
Connected to: 172.17.53.81
Support: 298 Days remaining

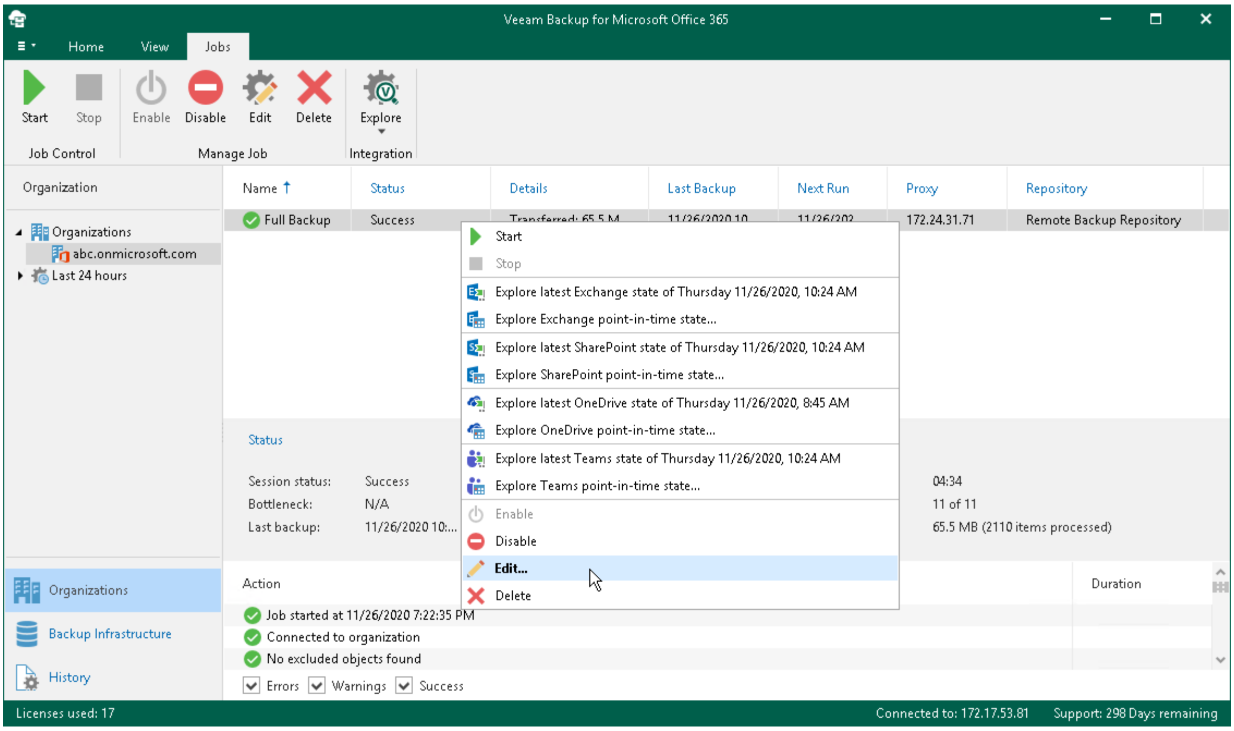
Editing Backup Job Settings

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.


Veeam Backup for Microsoft Office 365
Home
View
Jobs
Start
Stop
Enable
Disable
Edit
Delete
Explore
Job Control
Manage Job
Integration
Organization
Organizations
abc.onmicrosoft.com
Last 24 hours
Start
Stop
Explore latest Exchange state of Thursday 11/26/2020, 10:24 AM
Explore Exchange point-in-time state...
Explore latest SharePoint state of Thursday 11/26/2020, 10:24 AM
Explore SharePoint point-in-time state...
Explore latest OneDrive state of Thursday 11/26/2020, 8:45 AM
Explore OneDrive point-in-time state...
Explore latest Teams state of Thursday 11/26/2020, 10:24 AM
Explore Teams point-in-time state...
Enable
Disable
Edit...
Delete
Organizations
Backup Infrastructure
History
☑ Errors
☑ Warnings
☑ Success

Name	Status	Details	Last Backup	Next Run	Proxy	Repository
Full Backup	Success	Transferred: 65.5 M...	11/26/2020 10...	11/26/202...	172.24.31.71	Remote Backup Repository

Status

Session status: Success
Bottleneck: N/A
Last backup: 11/26/2020 10:...

04:34
11 of 11
65.5 MB (2110 items processed)

Action	Duration
Job started at 11/26/2020 7:22:35 PM	
Connected to organization	
No excluded objects found	

Licenses used: 17
Connected to: 172.17.53.81
Support: 298 Days remaining

Removing Backup Job

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

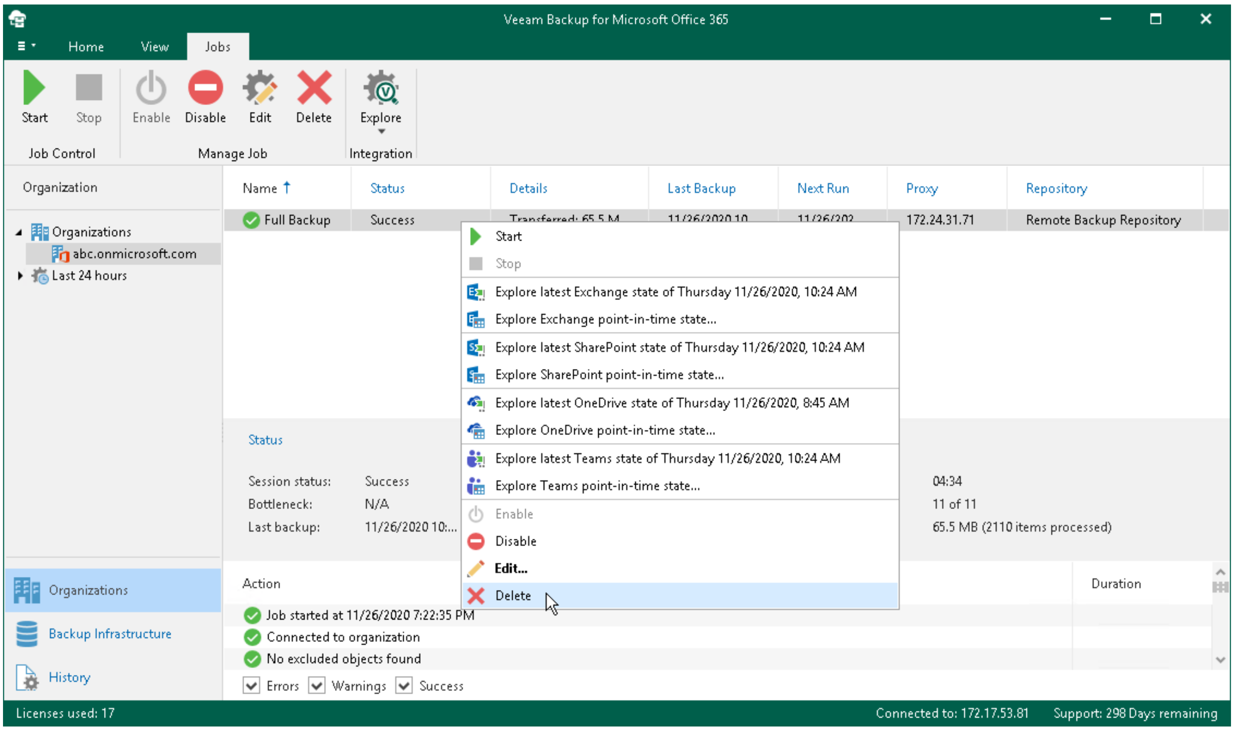
> **NOTE:**
>
> When you remove a backup job from configuration, the backup data is not be deleted from the backup location.

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 **Delete** on the ribbon.

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


Veeam Backup for Microsoft Office 365
Home
View
Jobs
Start
Stop
Enable
Disable
Edit
Delete
Explore
Job Control
Manage Job
Integration
Organization
Organizations
abc.onmicrosoft.com
Last 24 hours
Start
Stop
Explore latest Exchange state of Thursday 11/26/2020, 10:24 AM
Explore Exchange point-in-time state...
Explore latest SharePoint state of Thursday 11/26/2020, 10:24 AM
Explore SharePoint point-in-time state...
Explore latest OneDrive state of Thursday 11/26/2020, 8:45 AM
Explore OneDrive point-in-time state...
Explore latest Teams state of Thursday 11/26/2020, 10:24 AM
Explore Teams point-in-time state...
Enable
Disable
Edit...
Delete
Organizations
Backup Infrastructure
History

Name	Status	Details	Last Backup	Next Run	Proxy	Repository
Full Backup	Success	Transferred: 65.5 M	11/26/2020 10	11/26/202	172.24.31.71	Remote Backup Repository

Status

Session status: Success
Bottleneck: N/A
Last backup: 11/26/2020 10:...

04:34
11 of 11
65.5 MB (2110 items processed)

Action	Duration
Job started at 11/26/2020 7:22:35 PM	
Connected to organization	
No excluded objects found	

☑ Errors ☑ Warnings ☑ Success

Licenses used: 17 Connected to: 172.17.53.81 Support: 298 Days remaining

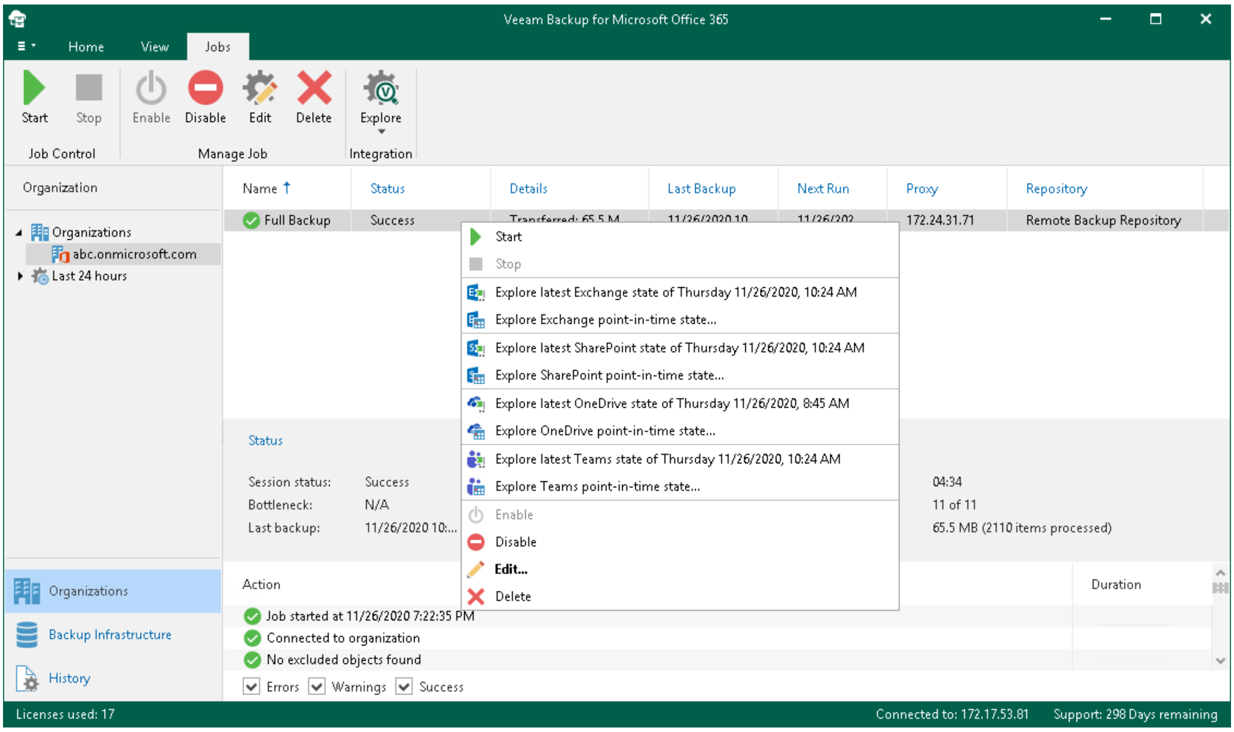
Exploring Backup Job

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.


Veeam Backup for Microsoft Office 365
Home
View
Jobs
Start
Stop
Enable
Disable
Edit
Delete
Explore
Job Control
Manage Job
Integration
Organization
Organizations
abc.onmicrosoft.com
Last 24 hours
Organizations
Backup Infrastructure
History
Start
Stop
Explore latest Exchange state of Thursday 11/26/2020, 10:24 AM
Explore Exchange point-in-time state...
Explore latest SharePoint state of Thursday 11/26/2020, 10:24 AM
Explore SharePoint point-in-time state...
Explore latest OneDrive state of Thursday 11/26/2020, 8:45 AM
Explore OneDrive point-in-time state...
Explore latest Teams state of Thursday 11/26/2020, 10:24 AM
Explore Teams point-in-time state...
Enable
Disable
Edit...
Delete
Licenses used: 17
Connected to: 172.17.53.81
Support: 298 Days remaining

Name ↑	Status	Details	Last Backup	Next Run	Proxy	Repository
Full Backup	Success	Transferred: 65.5 M	11/26/2020 10	11/26/202	172.24.31.71	Remote Backup Repository

Status

Session status: Success
Bottleneck: N/A
Last backup: 11/26/2020 10:...

04:34
11 of 11
65.5 MB (2110 items processed)

Action	Duration
Job started at 11/26/2020 7:22:35 PM	
Connected to organization	
No excluded objects found	

☑ Errors ☑ Warnings ☑ Success

Upgrading Backup Job

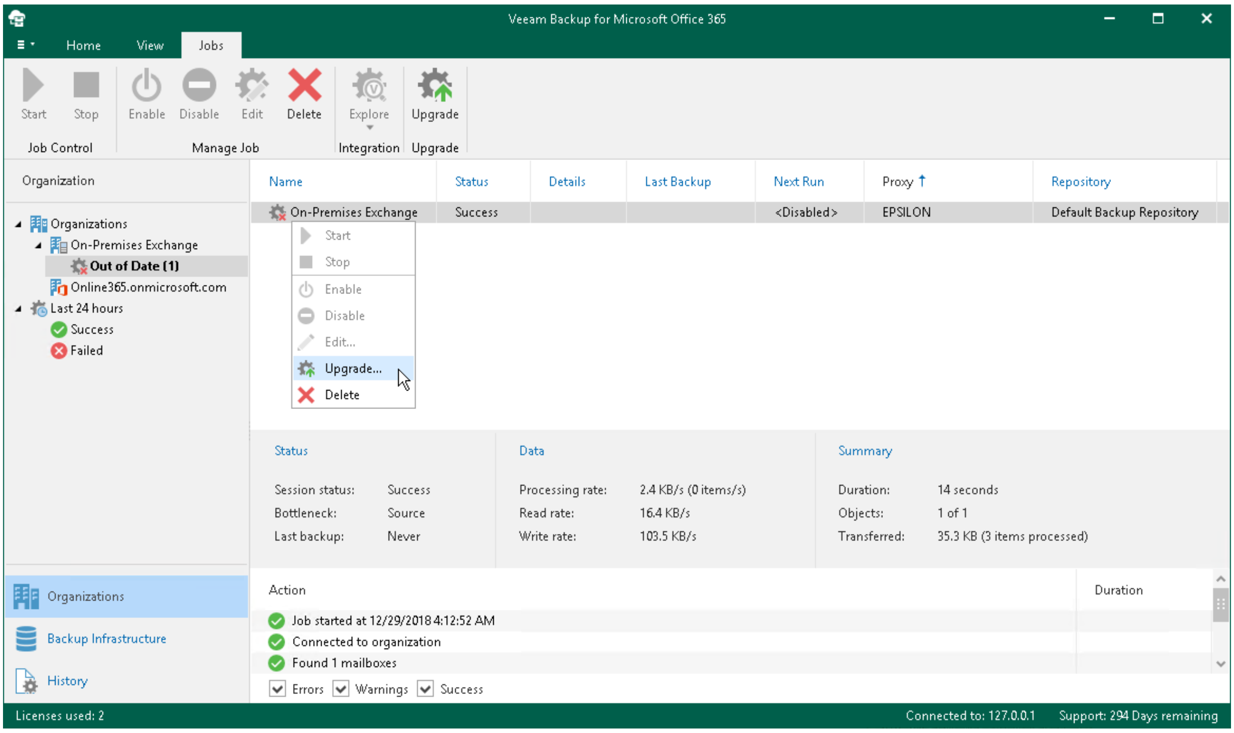
After you install Veeam Backup for Microsoft Office 365 version 5.0, the existing backup jobs that were created with an earlier version of the product must be upgraded manually. This applies to the following types of jobs:

- All backup jobs created with Veeam Backup for Microsoft Office 365 version 3.0.
- Backup jobs created with Veeam Backup for Microsoft Office 365 versions 4.0, 4a and 4b that contain Office 365 group objects.

To upgrade backup jobs, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select an organization and then 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**.



Name	Status	Details	Last Backup	Next Run	Proxy	Repository
On-Premises Exchange	Success			<Disabled>	EPSILON	Default Backup Repository

Status

Session status: Success
Bottleneck: Source
Last backup: Never

Data

Processing rate: 2.4 KB/s (0 items/s)
Read rate: 16.4 KB/s
Write rate: 103.5 KB/s

Summary

Duration: 14 seconds
Objects: 1 of 1
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	

Licenses used: 2
Connected to: 127.0.0.1
Support: 294 Days remaining

Data Restore

To restore Microsoft Office 365 data, you can use Veeam Explorers:

- 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.

- Veeam Explorer for Microsoft Teams

  To explore and recover Microsoft Teams teams, channels, tabs, posts and files.

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.

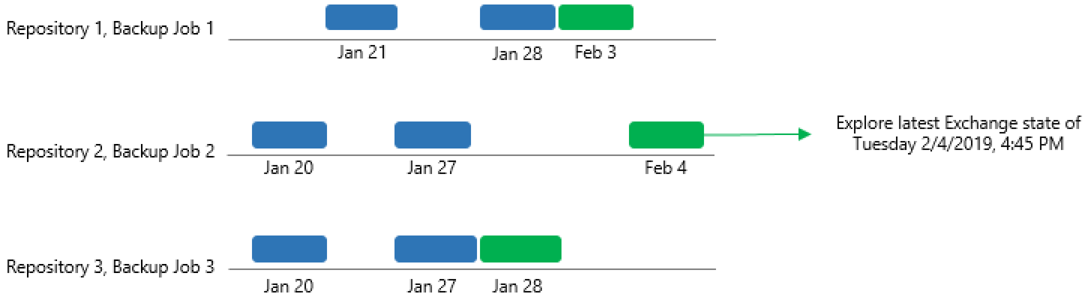
- Exploring All Organizations

  To open backups of all organizations.

Exploring Backup Jobs

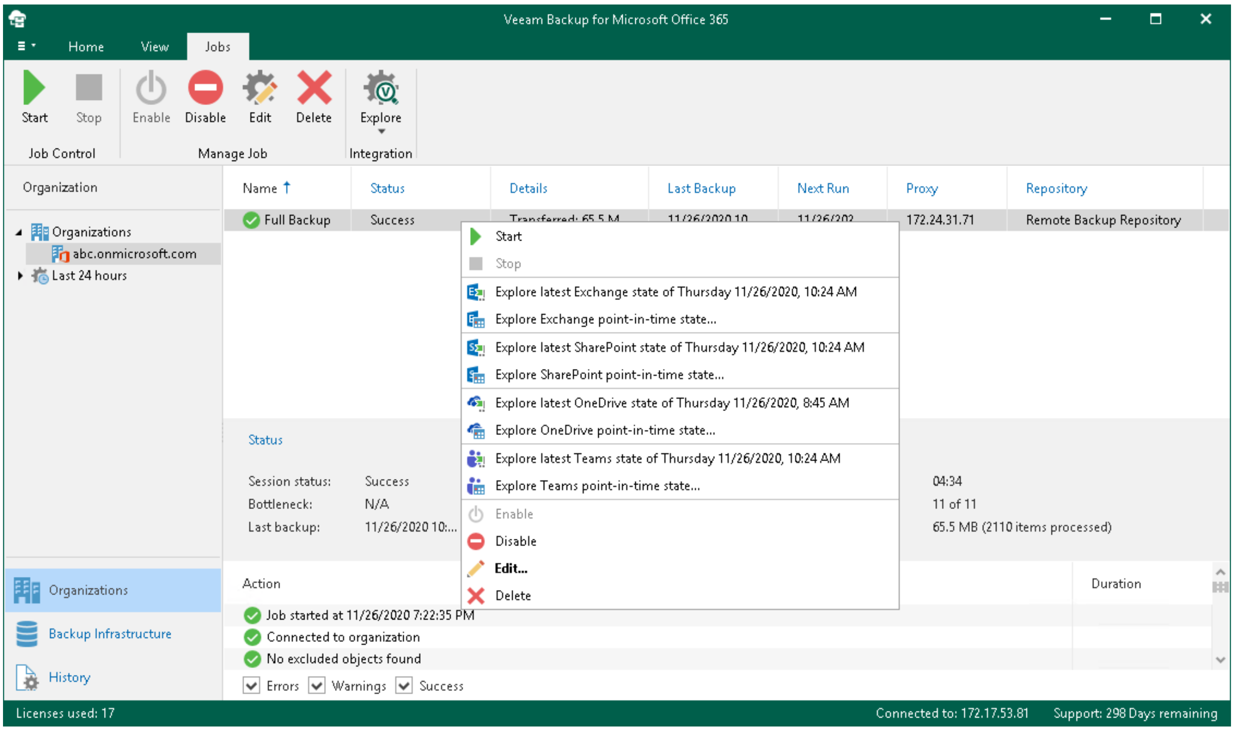
When exploring backup jobs, Veeam Backup for Microsoft Office 365 loads the latest restore point that was created by the selected job.

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 restore point (created on February 4) into the Veeam Explorer scope.


Repository 1, Backup Job 1
Jan 21
Jan 28
Feb 3
Repository 2, Backup Job 2
Jan 20
Jan 27
Feb 4
Explore latest Exchange state of
Tuesday 2/4/2019, 4:45 PM
Repository 3, Backup Job 3
Jan 20
Jan 27
Jan 28

To open backups created by the selected backup job, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select an organization.
3. In the preview pane, select a backup job that contains backups that you want to open.
4. On the **Jobs** tab, click **Explore** 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 <product> point-in-time state**. To select a point-in-time state. For more information, see Exploring Point-In-Time.


Veeam Backup for Microsoft Office 365
Home
View
Jobs
Start
Stop
Enable
Disable
Edit
Delete
Explore
Job Control
Manage Job
Integration
Organization
Organizations
abc.onmicrosoft.com
Last 24 hours
Name
Status
Details
Last Backup
Next Run
Proxy
Repository
Start
Stop
Explore latest Exchange state of Thursday 11/26/2020, 10:24 AM
Explore Exchange point-in-time state...
Explore latest SharePoint state of Thursday 11/26/2020, 10:24 AM
Explore SharePoint point-in-time state...
Explore latest OneDrive state of Thursday 11/26/2020, 8:45 AM
Explore OneDrive point-in-time state...
Explore latest Teams state of Thursday 11/26/2020, 10:24 AM
Explore Teams point-in-time state...
Enable
Disable
Edit...
Delete
Organizations
Backup Infrastructure
History
Action
Duration
☑ Errors ☑ Warnings ☑ Success

Name	Status	Details	Last Backup	Next Run	Proxy	Repository
Full Backup	Success	Transferred: 65.5 M...	11/26/2020 10...	11/26/202...	172.24.31.71	Remote Backup Repository

Status

Session status: Success
Bottleneck: N/A
Last backup: 11/26/2020 10:...

04:34
11 of 11
65.5 MB (2110 items processed)

Job started at 11/26/2020 7:22:35 PM
Connected to organization
No excluded objects found

Licenses used: 17
Connected to: 172.17.53.81
Support: 298 Days remaining

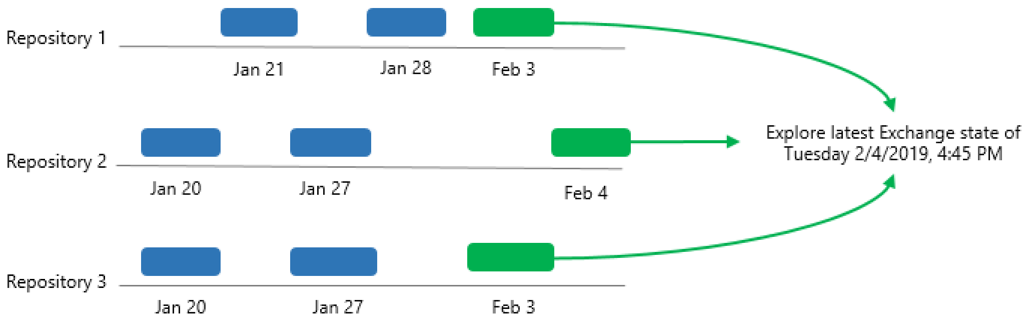
Exploring Single Organization

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:

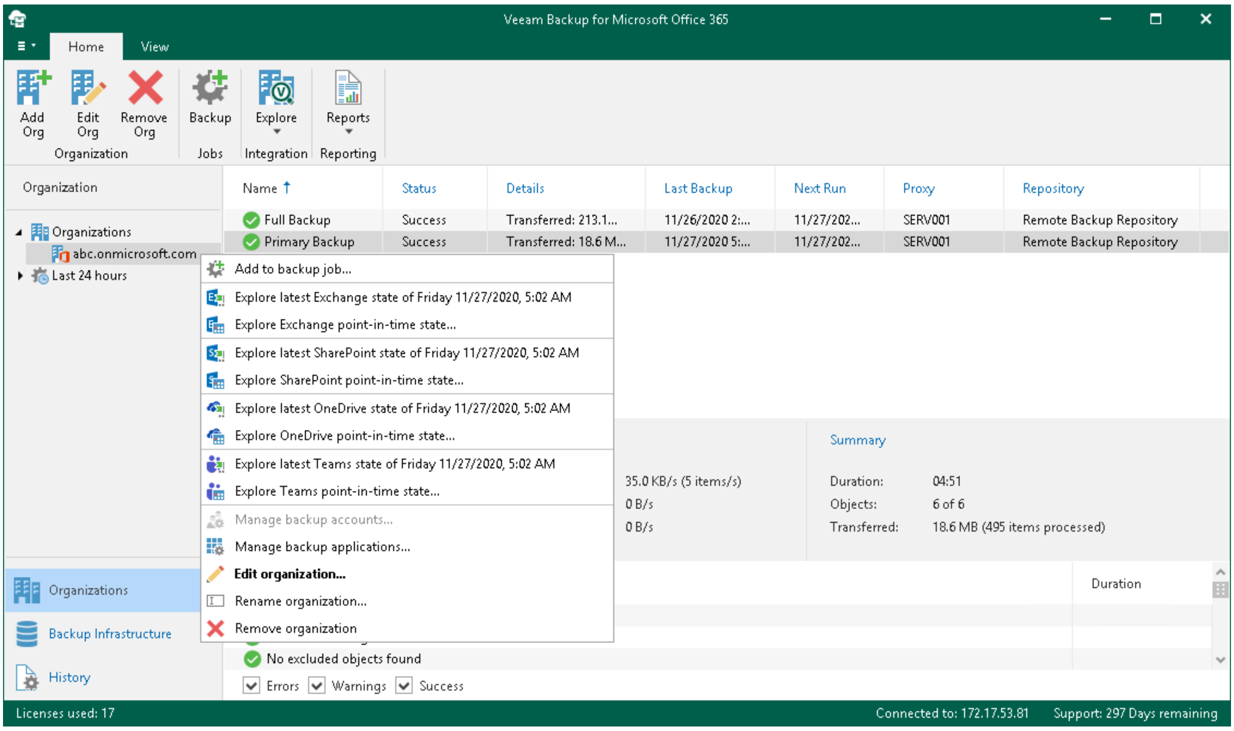
- For *Repository 1*, only the restore point created on February 3.
- For *Repository 2*, only the restore point created on February 4.
- For *Repository 3*, only the restore point created on February 3.

> **NOTE:**
>
> If you remove a backup job from the Veeam Backup for Microsoft Office 365 configuration, the backup data created by this job remains 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 <product> point-in-time state.** To select a point-in-time state. For more information, see Exploring Point-in-Time.


Veeam Backup for Microsoft Office 365
Home
View
Add Org
Edit Org
Remove Org
Organization
Backup
Jobs
Explore
Integration
Reports
Reporting
Organization
Organizations
abc.onmicrosoft.com
Last 24 hours
Organizations
Backup Infrastructure
History
Add to backup job...
Explore latest Exchange state of Friday 11/27/2020, 5:02 AM
Explore Exchange point-in-time state...
Explore latest SharePoint state of Friday 11/27/2020, 5:02 AM
Explore SharePoint point-in-time state...
Explore latest OneDrive state of Friday 11/27/2020, 5:02 AM
Explore OneDrive point-in-time state...
Explore latest Teams state of Friday 11/27/2020, 5:02 AM
Explore Teams point-in-time state...
Manage backup accounts...
Manage backup applications...
Edit organization...
Rename organization...
Remove organization
Duration
☑ Errors ☑ Warnings ☑ Success

Name	Status	Details	Last Backup	Next Run	Proxy	Repository
Full Backup	Success	Transferred: 213.1...	11/26/2020 2:...	11/27/202...	SERV001	Remote Backup Repository
Primary Backup	Success	Transferred: 18.6 M...	11/27/2020 5:...	11/27/202...	SERV001	Remote Backup Repository

35.0 KB/s (5 items/s)
0 B/s
0 B/s

Summary

Duration: 04:51
Objects: 6 of 6
Transferred: 18.6 MB (495 items processed)

No excluded objects found

Licenses used: 17
Connected to: 172.17.53.81
Support: 297 Days remaining

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*. The organization *A* has three backup jobs and the organization *B*, two backup jobs.

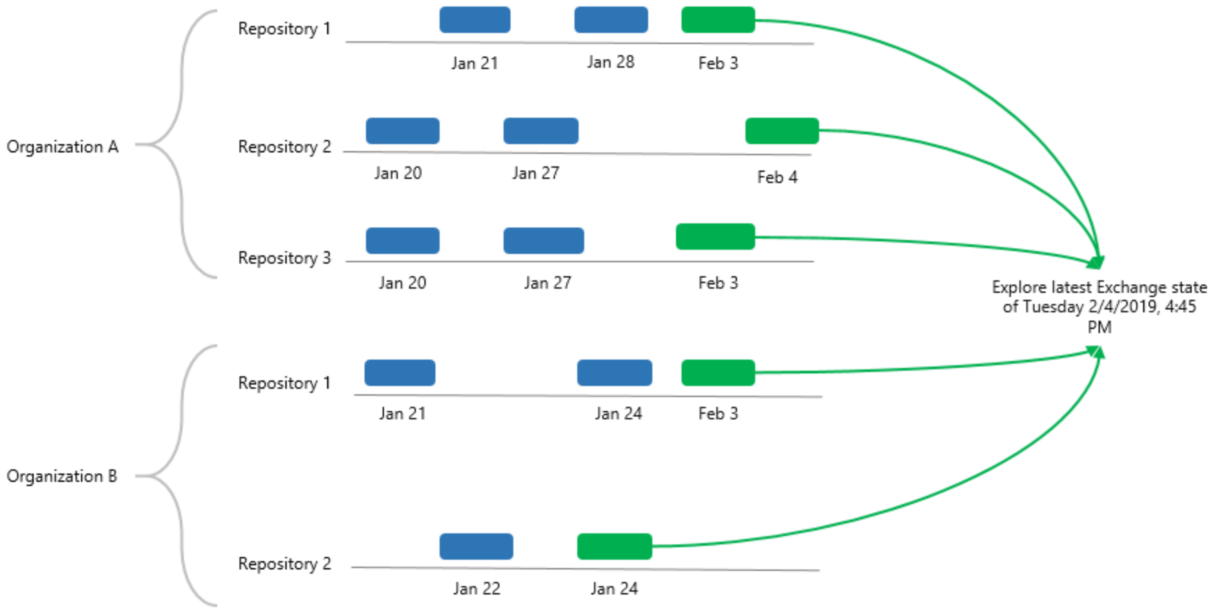
When exploring the organization *A*, the following restore points will be merged and loaded into the Veeam Explorer scope:

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

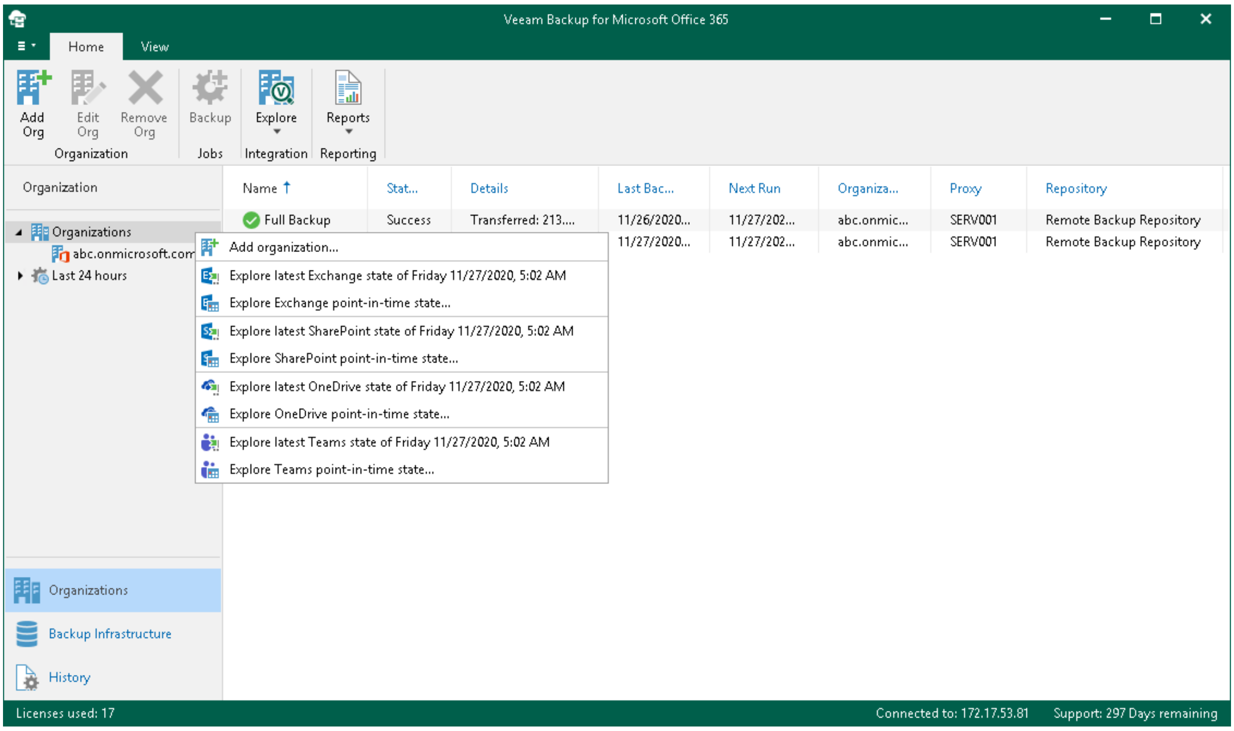
- For *Repository 2*, only the restore point created on February 3.
- For *Repository 2*, only the restore point created on January 24.

> **NOTE:**
>
> If you remove a backup job from the Veeam Backup for Microsoft Office 365 configuration, the backup data created by this job remains 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 <product> point-in-time state**. To select a point-in-time state. For more information, see Exploring Point-in-Time.


Veeam Backup for Microsoft Office 365
Home
View
Add Org
Edit Org
Remove Org
Backup
Explore
Reports
Organization
Jobs
Integration
Reporting
Organization
Organizations
abc.onmicrosoft.com
Last 24 hours
Add organization...
Explore latest Exchange state of Friday 11/27/2020, 5:02 AM
Explore Exchange point-in-time state...
Explore latest SharePoint state of Friday 11/27/2020, 5:02 AM
Explore SharePoint point-in-time state...
Explore latest OneDrive state of Friday 11/27/2020, 5:02 AM
Explore OneDrive point-in-time state...
Explore latest Teams state of Friday 11/27/2020, 5:02 AM
Explore Teams point-in-time state...
Organizations
Backup Infrastructure
History
Licenses used: 17
Connected to: 172.17.53.81
Support: 297 Days remaining

Name ↑	Stat...	Details	Last Bac...	Next Run	Organiza...	Proxy	Repository
Full Backup	Success	Transferred: 213....	11/26/2020...	11/27/202...	abc.onmic...	SERV001	Remote Backup Repository
			11/27/2020...	11/27/202...	abc.onmic...	SERV001	Remote Backup Repository

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.

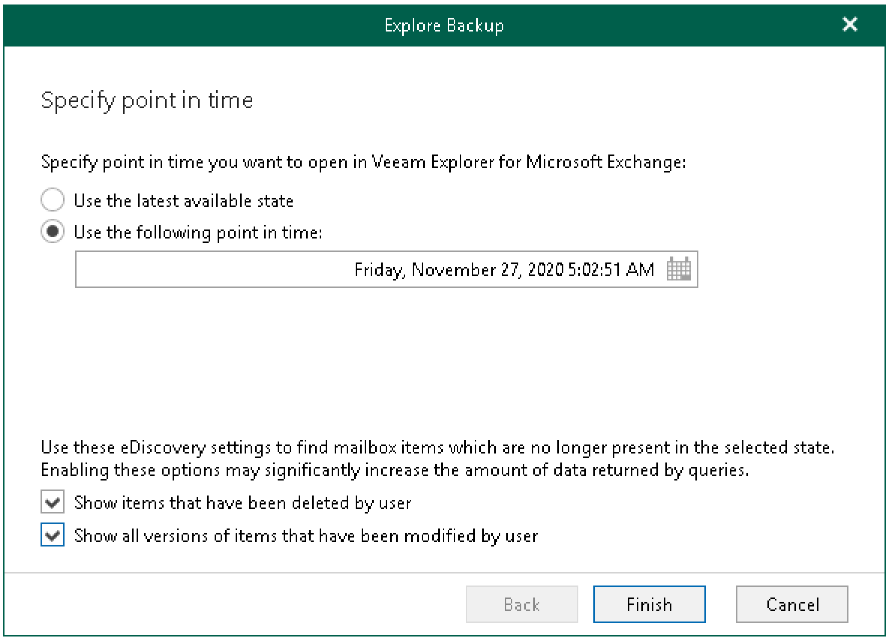
To view historic data, select the following check boxes:

- **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:

Friday, November 27, 2020 5:02:51 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

Backup and Restore Statistics

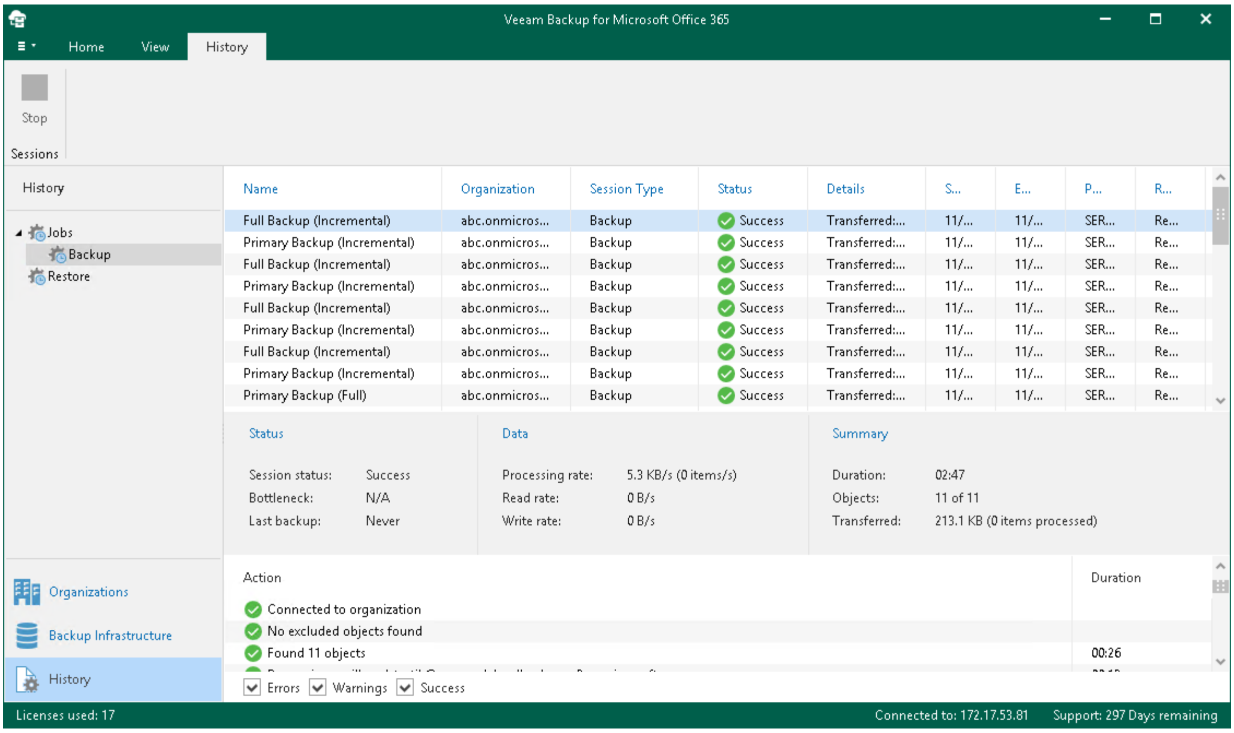
Each backup or restore session saves its results and metrics to the Veeam Backup for Microsoft Office 365 configuration database.

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.



Name	Organization	Session Type	Status	Details	S...	E...	P...	R...
Full Backup (Incremental)	abc.onmicros...	Backup	✓ Success	Transferred:...	11/...	11/...	SER...	Re...
Primary Backup (Incremental)	abc.onmicros...	Backup	✓ Success	Transferred:...	11/...	11/...	SER...	Re...
Full Backup (Incremental)	abc.onmicros...	Backup	✓ Success	Transferred:...	11/...	11/...	SER...	Re...
Primary Backup (Incremental)	abc.onmicros...	Backup	✓ Success	Transferred:...	11/...	11/...	SER...	Re...
Full Backup (Incremental)	abc.onmicros...	Backup	✓ Success	Transferred:...	11/...	11/...	SER...	Re...
Primary Backup (Incremental)	abc.onmicros...	Backup	✓ Success	Transferred:...	11/...	11/...	SER...	Re...
Full Backup (Incremental)	abc.onmicros...	Backup	✓ Success	Transferred:...	11/...	11/...	SER...	Re...
Primary Backup (Incremental)	abc.onmicros...	Backup	✓ Success	Transferred:...	11/...	11/...	SER...	Re...
Primary Backup (Full)	abc.onmicros...	Backup	✓ Success	Transferred:...	11/...	11/...	SER...	Re...

Status

Session status: Success
Bottleneck: N/A
Last backup: Never

Data

Processing rate: 5.3 KB/s (0 items/s)
Read rate: 0 B/s
Write rate: 0 B/s

Summary

Duration: 02:47
Objects: 11 of 11
Transferred: 213.1 KB (0 items processed)

Action	Duration
✓ Connected to organization	
✓ No excluded objects found	
✓ Found 11 objects	00:26

☑ Errors ☑ Warnings ☑ Success

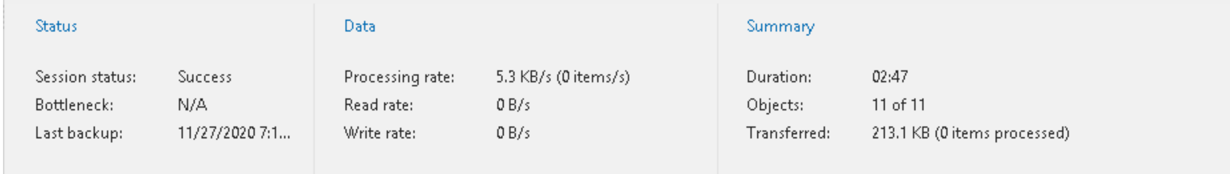
Licenses used: 17 Connected to: 172.17.53.81 Support: 297 Days remaining

Viewing Backup Session Metrics

You can view backup session metrics 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 job in the preview pane.



Status

Session status: Success
Bottleneck: N/A
Last backup: 11/27/2020 7:1...

Data

Processing rate: 5.3 KB/s (0 items/s)
Read rate: 0 B/s
Write rate: 0 B/s

Summary

Duration: 02:47
Objects: 11 of 11
Transferred: 213.1 KB (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**.
    - The **Detecting** state is displayed when a backup job is started and Veeam Backup for Microsoft Office 365 has not calculated the bottleneck value.
    - The **Source** state is displayed when a bottleneck occurs during download.

      For example, if you have a slow connection or problems occur on the internet provider side and your connection speed drops significantly, the bottleneck value will topically be shown as **Source**.
    - The **Target** state is displayed when a bottleneck occurs during writing data to disk.

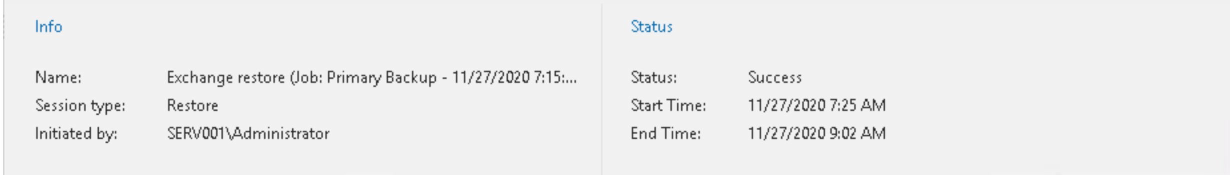
      For example, if you are using a hard drive that is fragmented or an old type of the hard drive, the bottleneck value will typically be shown as **Target**.
    - The **N/A** state is displayed when no bottleneck occurs.
  - **Last Backup**. The date and time of the last backup session.
- The **Data** 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, Microsoft Teams team, mailbox and archive mailbox, including group mailboxes, public folders and discovery search mailboxes.
  - **Transferred**. Shows how many bytes have been downloaded.

Viewing 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

Name: Exchange restore (Job: Primary Backup - 11/27/2020 7:15:...
Session type: Restore
Initiated by: SERV001\Administrator

Status

Status: Success
Start Time: 11/27/2020 7:25 AM
End Time: 11/27/2020 9:02 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.

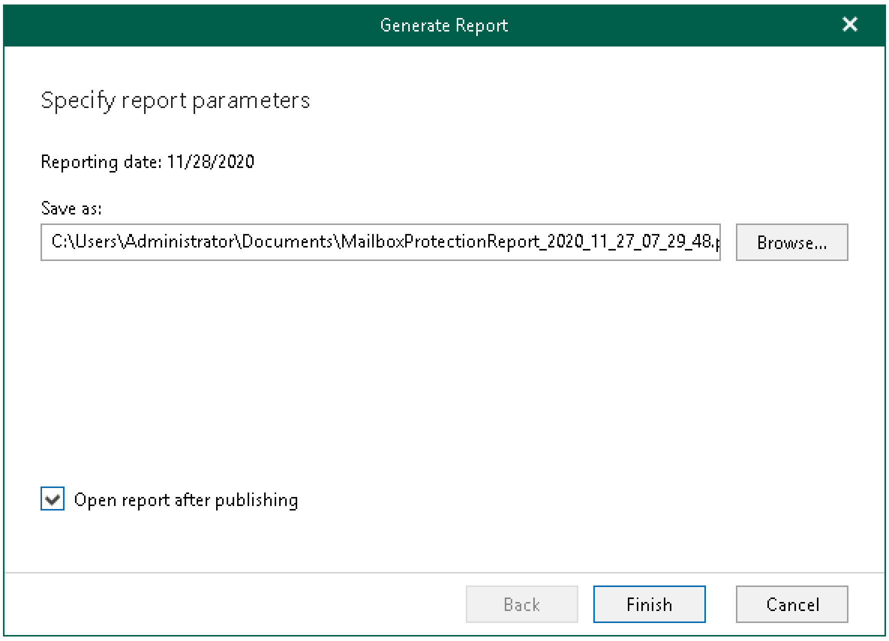
Field	Description
Description	Shows a description of the report.
Reporting Date	Shows the date when the report was created.
License Information	Shows the product name and a license type.
Summary	Shows the total number of protected and unprotected mailboxes per each organization added to the scope: • 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. The following types of mailboxes are included in the report: • *Group mailbox* • *Public mailbox* • *Shared mailbox* • *Resource (Equipment and Room) mailbox* Renamed organizations will be shown with their original names. For more information about renaming organizations, see Renaming Organizations.

To generate a report, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select an organization for which you want to create a report.

   You can also select the root **Organizations** node to generate a report for all organizations added to the scope.
3. 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: 11/28/2020

Save as: C:\Users\Administrator\Documents\MailboxProtectionReport_2020_11_27_07_29_48.p

☑ Open report after publishing

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 backed-up 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 (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: • 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 are not included in the report. No information is available in the following cases:
    - You 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 is not included in the report.
    - You upgraded a previous version of Veeam Backup for Microsoft Office 365 to a newer one, as described in Upgrading to Veeam Backup for Microsoft Office 365 5.0.

      In this case, all backup repositories in your environment are excluded from the report.
- Repositories whose **Daily Change** and **Total Size** values are less than 10 MB are not included in the report.

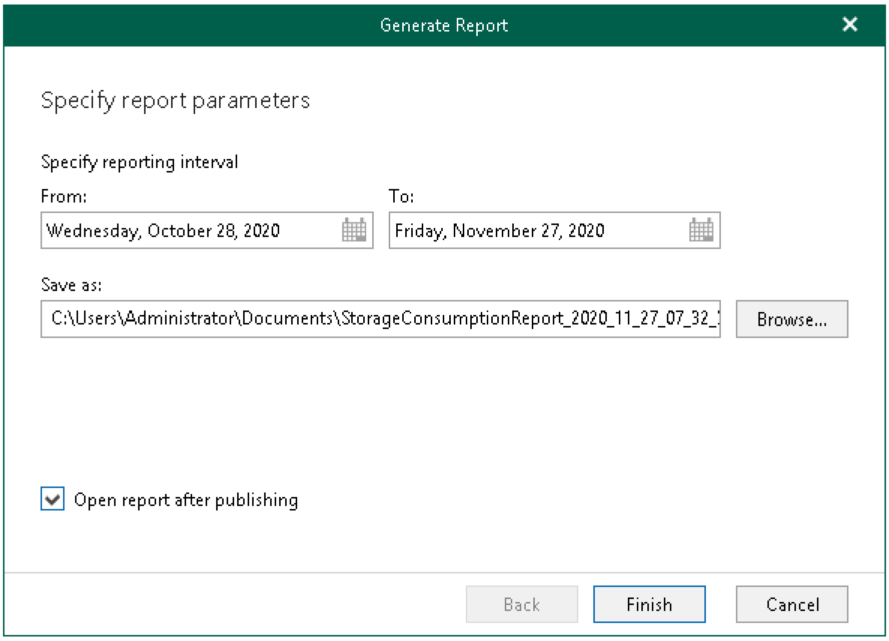
  For example, a report is said to be built starting from *01/11/2020* to *30/11/2020* and the period from *01/11/2020* to *09/11/2020* is empty (both the **Daily Change** and **Total Size** values are less than 10 MB). In this scenario, such a report will only show statistical information starting from *10/11/2020*.

To generate a report, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select an organization for which you want to create a report.

   You can also select the root **Organizations** node to generate a report for all organizations added to the scope.
3. On the **Home** tab, select **Reports** > **Storage Consumption**.
4. Specify a time interval.
5. Click **Browse** to specify a location to save the report.

   Use the **Save as type** drop-down list in the **Save As** dialog to specify the format (*.pdf* or *.csv*) in which to save the report.
6. Select the **Open report after publishing** check box to open the generated report using the default application.
7. Click **Finish**.



Specify report parameters

Specify reporting interval

From: Wednesday, October 28, 2020

To: Friday, November 27, 2020

Save as: C:\Users\Administrator\Documents\StorageConsumptionReport_2020_11_27_07_32_

☑ Open report after publishing

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: • 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 by License Usage	Shows top 5 organizations that consume the license the most.

> **NOTE:**
>
> When using a rental license, *License Overview* report also shows a number of trial licenses per each organization. For more information, see Rental License.

To generate a report, do the following:

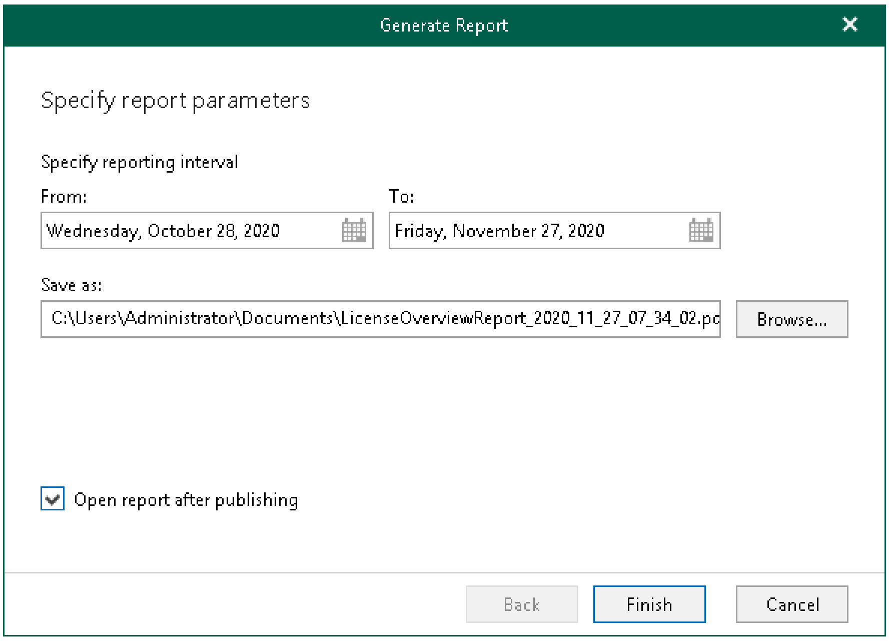
1. Open the **Organizations** view.
2. In the inventory pane, select an organization for which you want to create a report.

   You can also select the root **Organizations** node to generate a report for all organizations added to the scope.
3. On the **Home** tab, select **Reports** > **License Overview**.
4. Specify a time interval.
5. Click **Browse** to specify a location to save the report.

   Use the **Save as type** drop-down list in the **Save As** dialog to specify the format (*.pdf* or *.csv*) in which to save the report.

6. Select the **Open report after publishing** check box to open the generated report using the default application.

7. Click **Finish**.



Generate Report

Specify report parameters

Specify reporting interval

From: Wednesday, October 28, 2020

To: Friday, November 27, 2020

Save as: C:\Users\Administrator\Documents\LicenseOverviewReport_2020_11_27_07_34_02.pd

☑ Open report after publishing

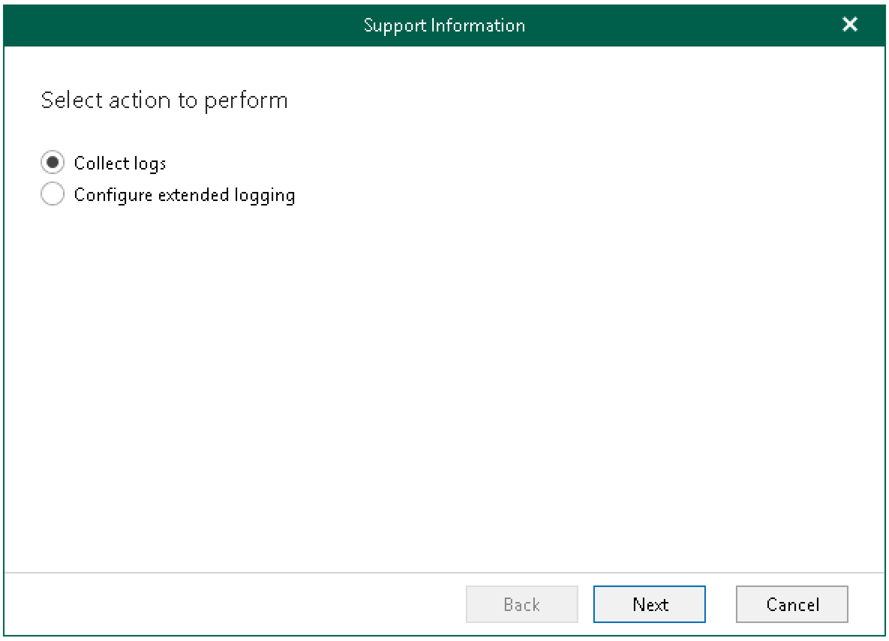
Log Files Export

This section explains how to collect log files that help you troubleshoot unexpected errors when working with Veeam Backup for Microsoft Office 365 and Veeam Explorers.

To collect log files, do the following:

1. In the main menu, click **Help and Support** > **Support information**.
2. Select the **Collect logs** option.

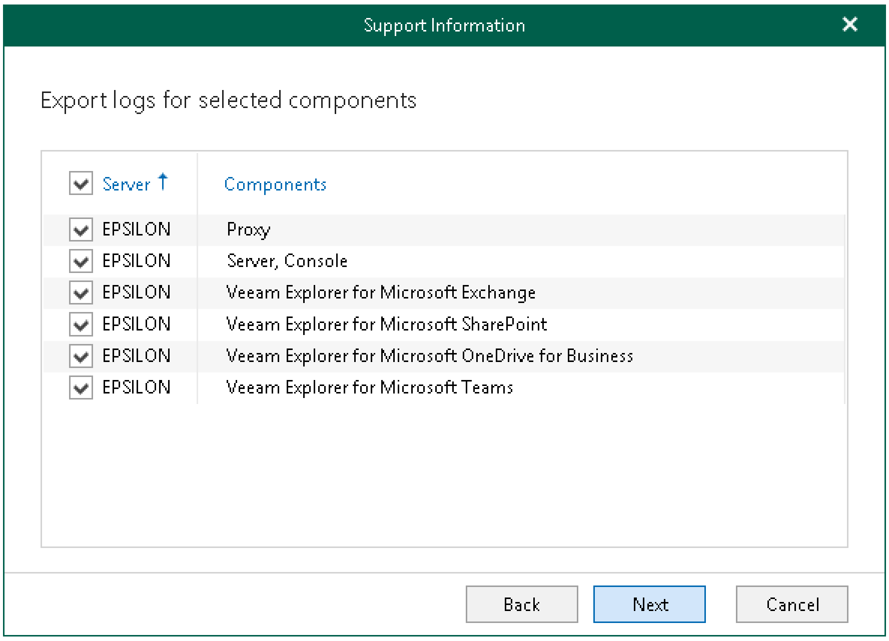
   To enable extended logging mode, select **Configure extended logging** and proceed with the Configuring Extended Logging Mode section.



Select action to perform

● Collect logs
○ Configure extended logging

3. Select Veeam Backup for Microsoft Office 365 infrastructure components for which to obtain log files. If Veeam Explorers are installed on the machine that runs Veeam Backup for Microsoft Office 365, you can select them as well.

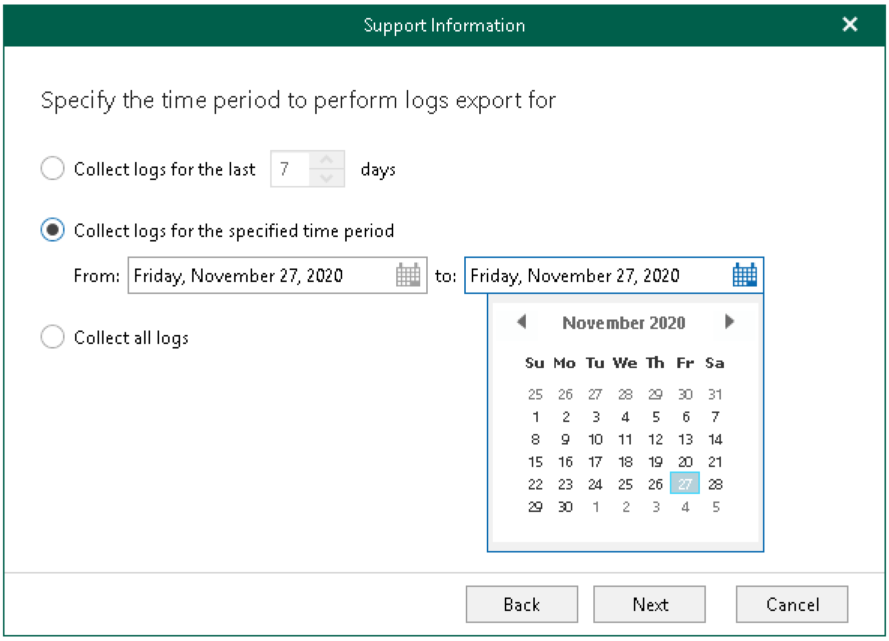


Export logs for selected components

☑ Server ↑	Components
☑ EPSILON	Proxy
☑ EPSILON	Server, Console
☑ EPSILON	Veeam Explorer for Microsoft Exchange
☑ EPSILON	Veeam Explorer for Microsoft SharePoint
☑ EPSILON	Veeam Explorer for Microsoft OneDrive for Business
☑ EPSILON	Veeam Explorer for Microsoft Teams

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

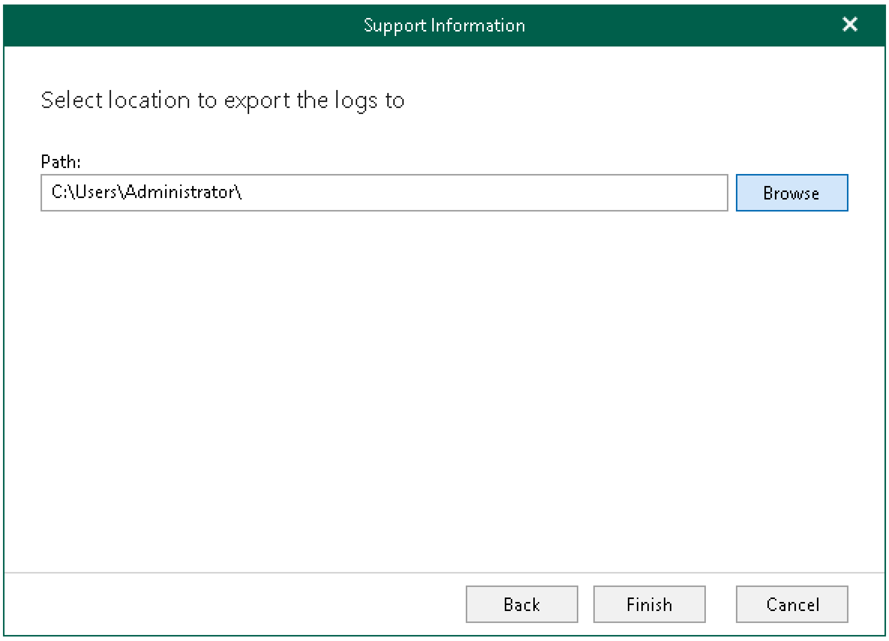
○ Collect logs for the last 7 days

● Collect logs for the specified time period

From: Friday, November 27, 2020 to: Friday, November 27, 2020

○ Collect all logs

5. Specify the path and click **Finish**.



Support Information

Select location to export the logs to

Path: C:\Users\Administrator\

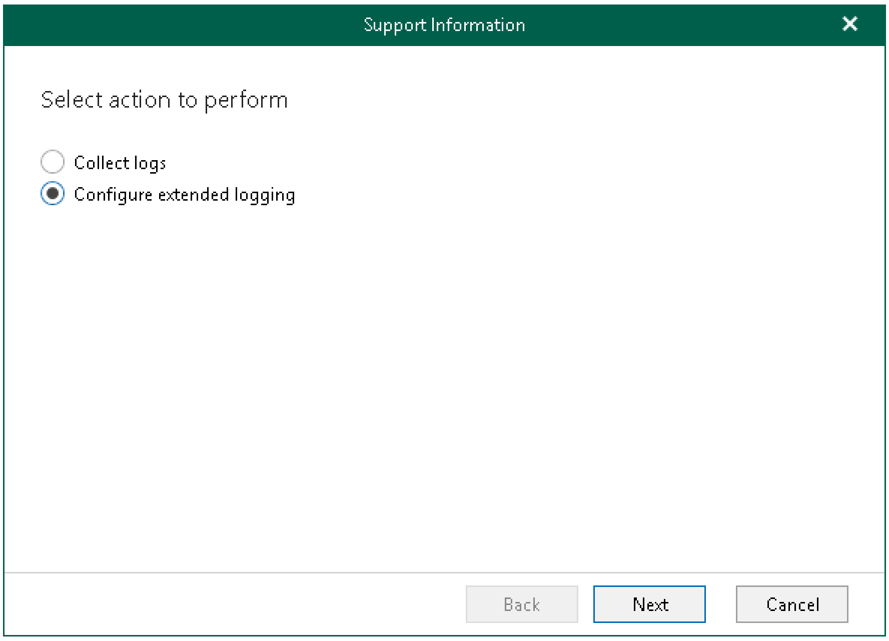
Configuring Extended Logging Mode

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.

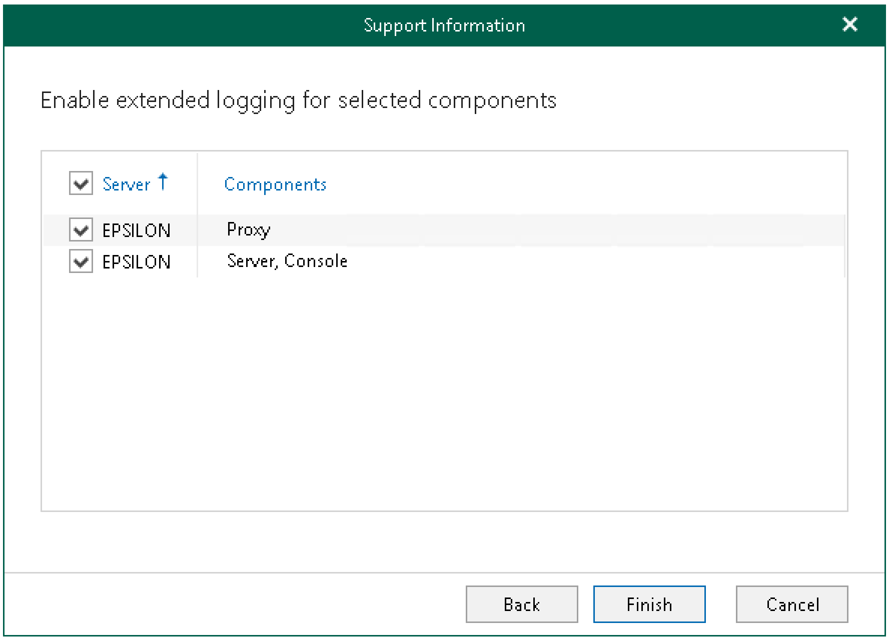


Support Information

Select action to perform

○ Collect logs
● Configure extended logging

3. Select components (local or remote) to which you want to apply the extended logging mode.



Support Information

Enable extended logging for selected components

☑ Server	Components
☑ EPSILON	Proxy
☑ EPSILON	Server, Console

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 for Microsoft Office 365 and Veeam Backup & Replication licenses.

   For more information, see the Licensing and License Types of this guide and the Licensing for Service Providers section of the Veeam Cloud Connect Guide.

3. Configure a TLS certificate, as described in the Managing TLS Certificates section of the Veeam Cloud Connect Guide.

   Without a certificate, you will not be able to add a *Cloud Gateway* component.

4. Configure a cloud gateway, as described in the Adding Cloud Gateways section of the Veeam Cloud Connect Guide.

5. Add new tenants, as described in the Registering Tenant Accounts section of the Veeam Cloud Connect 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, Veeam Explorer for Microsoft OneDrive for Business and Veeam Explorer for Microsoft Teams that come as part of the Veeam Backup for Microsoft Office 365 5.0 distribution package.
- Make sure to install Veeam Backup for Microsoft Office 365 on a server with Veeam Backup & Replication 10 or later.

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.

- Tenant 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.

- Organization Management

  To learn how to add tenant 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 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, Veeam Explorer for Microsoft OneDrive for Business and Veeam Explorer for Microsoft Teams that come as part of the Veeam Backup for Microsoft Office 365 5.0 distribution package.
- By default, tenants cannot 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 Tenant 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 Exploring Backups in Veeam Explorers.

Exploring Backups in Veeam Explorers

To explore backups located on the service provider side, add such backups in Veeam Explorers, 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
- Adding Organization Backups in Veeam Explorer for Microsoft Teams

NOTE:

Consider the following:

- Make sure to have access to the service provider server to be able to explore your backups. Access can be granted, as described in Tenant Authentication Settings.
- [For connection to a service provider using the modern app-only authentication method] The account that you plan to use to log in to Microsoft Office 365 must be assigned the *Global Administrator* role.

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	To restore data to Microsoft Office 365 and on-premises Microsoft Exchange, make sure to configure user accounts as follows: **Restore to Public Folder Using Basic Authentication Method** • The account must own a mailbox on a target Microsoft Exchange server. • The account must be assigned the *Organization Management* role on a target Microsoft Exchange server. See Assigning Organization Management Role. • [For restore of *In-Place Hold Items* to the original location] If the *In-Place Hold Items* folder already exists, make sure the account being used can create, modify and delete items. If the *In-Place Hold Items* folder does not exist, the account being used must be able to create folders under the *All Public Folders* root node. **Restore to Mailbox Using Basic Authentication Method** • If the account owns a mailbox, make sure it has *Full Access.* • If the account does not own a mailbox, then access must be granted through impersonation. See Granting Full Access. **Restore Using Modern App-Only Authentication Method** The account used to log in to Microsoft Office 365 must be assigned the following roles: • *ApplicationImpersonation* role. For more information, see this Microsoft article. • *Global Administrator* or *Exchange Administrator* role Also make sure that the required settings are specified for the Azure AD application used for restore. For more information, see Required Azure AD Application Settings.

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 3 MB 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

- 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 disable these notifications, clear the **Show pop-up notifications on startup** 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.

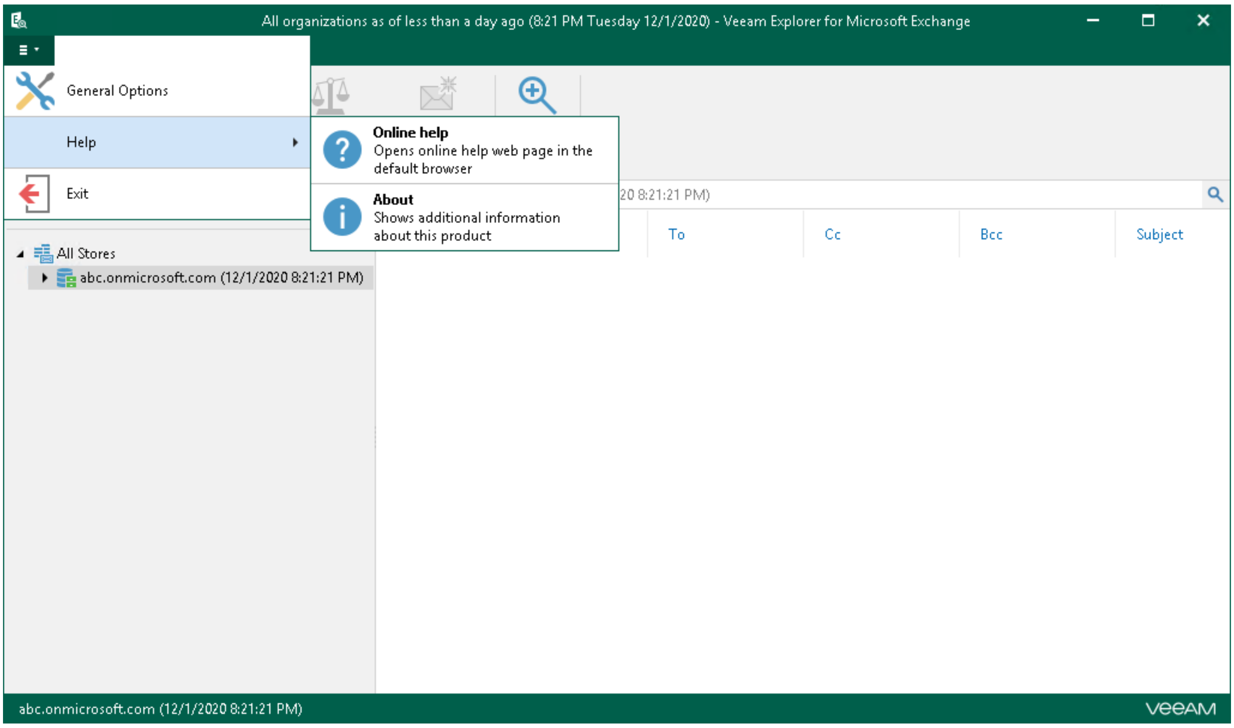
Understanding User Interface

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:

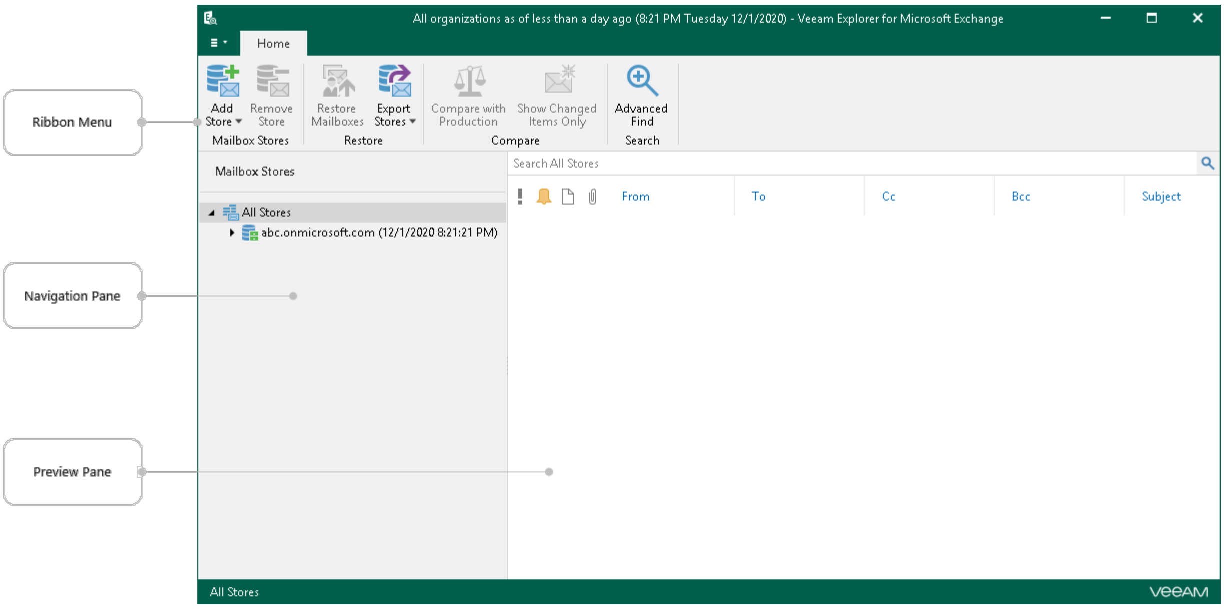
- **General Options**. Allows you to configure program options.
- **Help**.
    - **Online help**. Opens the online web help page.
    - **About**. Shows information about the product.
- **Exit**. Closes the program.


All organizations as of less than a day ago (8:21 PM Tuesday 12/1/2020) - Veeam Explorer for Microsoft Exchange
General Options
Help
Exit
Online help
Opens online help web page in the default browser
About
Shows additional information about this product
20 8:21:21 PM)
To
Cc
Bcc
Subject
All Stores
abc.onmicrosoft.com (12/1/2020 8:21:21 PM)
abc.onmicrosoft.com (12/1/2020 8:21:21 PM)
veeam

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

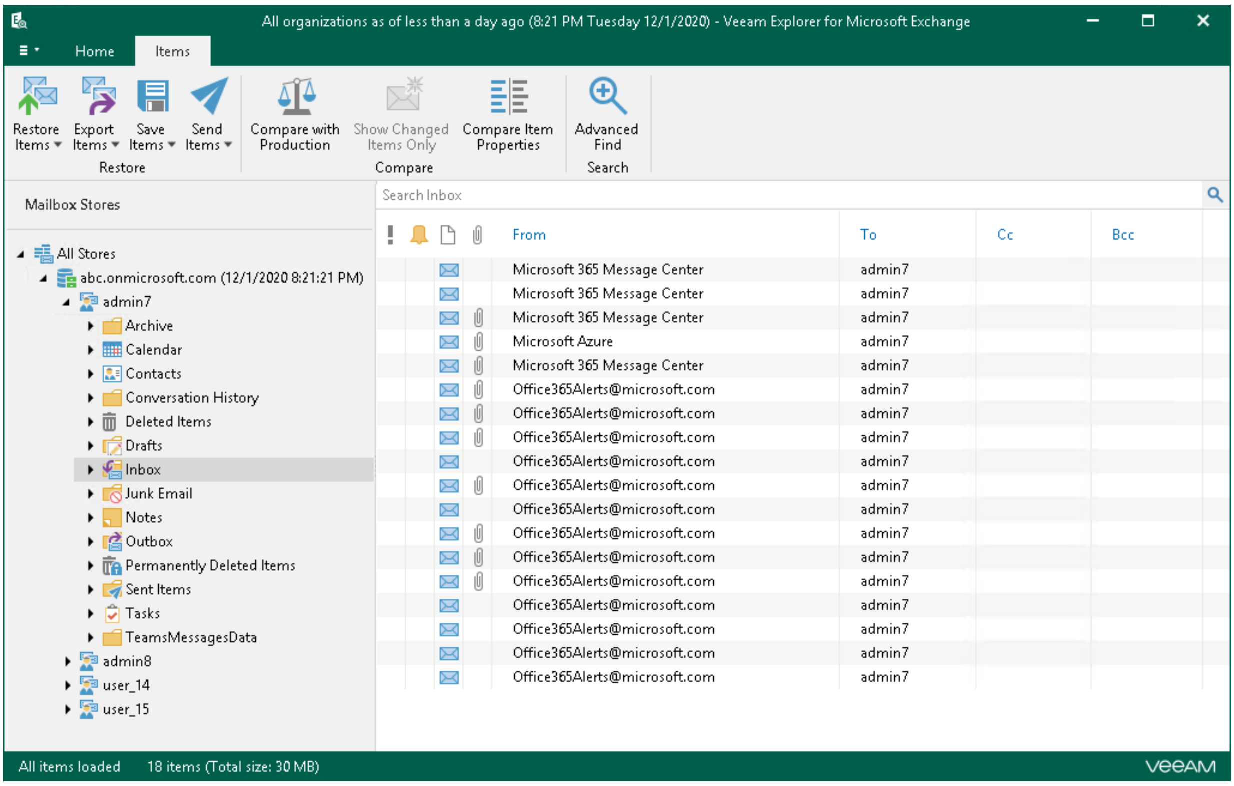
Continue with this section to learn more about:

- 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.

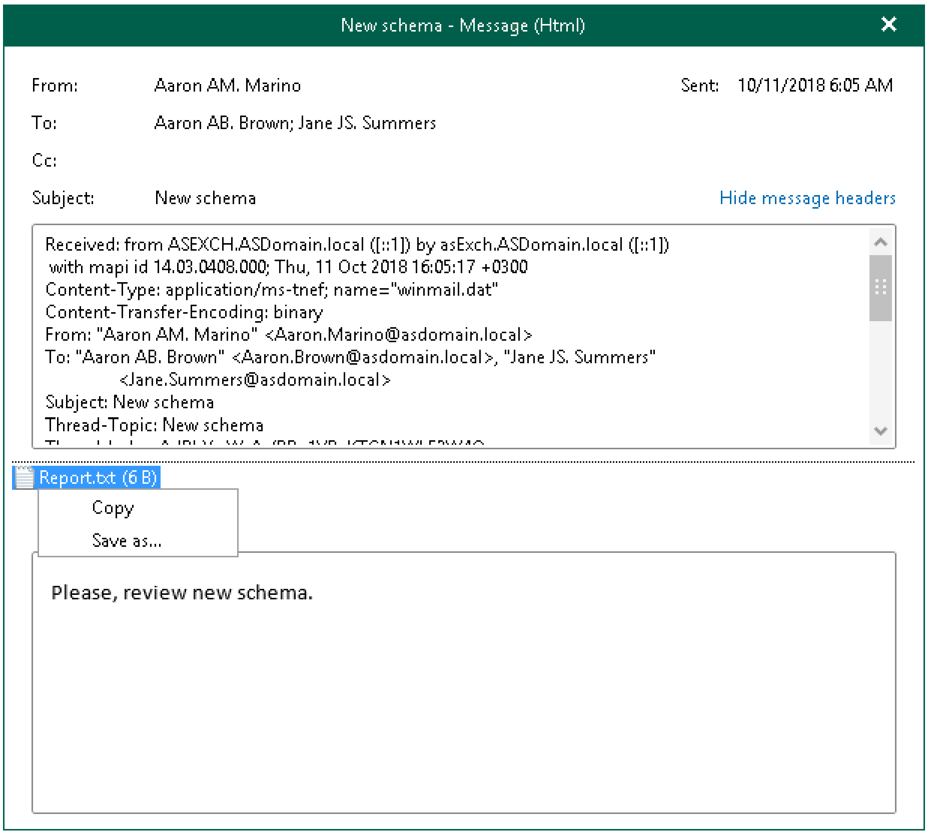


From	To	Cc	Bcc
Microsoft 365 Message Center	admin7		
Microsoft 365 Message Center	admin7		
Microsoft 365 Message Center	admin7		
Microsoft Azure	admin7		
Microsoft 365 Message Center	admin7		
Office365Alerts@microsoft.com	admin7		
Office365Alerts@microsoft.com	admin7		
Office365Alerts@microsoft.com	admin7		
Office365Alerts@microsoft.com	admin7		
Office365Alerts@microsoft.com	admin7		
Office365Alerts@microsoft.com	admin7		
Office365Alerts@microsoft.com	admin7		
Office365Alerts@microsoft.com	admin7		
Office365Alerts@microsoft.com	admin7		
Office365Alerts@microsoft.com	admin7		
Office365Alerts@microsoft.com	admin7		
Office365Alerts@microsoft.com	admin7		
Office365Alerts@microsoft.com	admin7		

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**.



From: Aaron AM. Marino

Sent: 10/11/2018 6:05 AM

To: Aaron AB. Brown; Jane JS. Summers

Cc:

Subject: New schema

```
Received: from ASEXCH.ASDomain.local ([::1]) by asExch.ASDomain.local ([::1])
 with mapi id 14.03.0408.000; Thu, 11 Oct 2018 16:05:17 +0300
Content-Type: application/ms-tnef; name="winmail.dat"
Content-Transfer-Encoding: binary
From: "Aaron AM. Marino" <Aaron.Marino@asdomain.local>
To: "Aaron AB. Brown" <Aaron.Brown@asdomain.local>, "Jane JS. Summers"
        <Jane.Summers@asdomain.local>
Subject: New schema
Thread-Topic: New schema
```

Report.txt (6 B)

Please, review new schema.

Searching

The search mechanism allows you to find items matching specified search criteria.

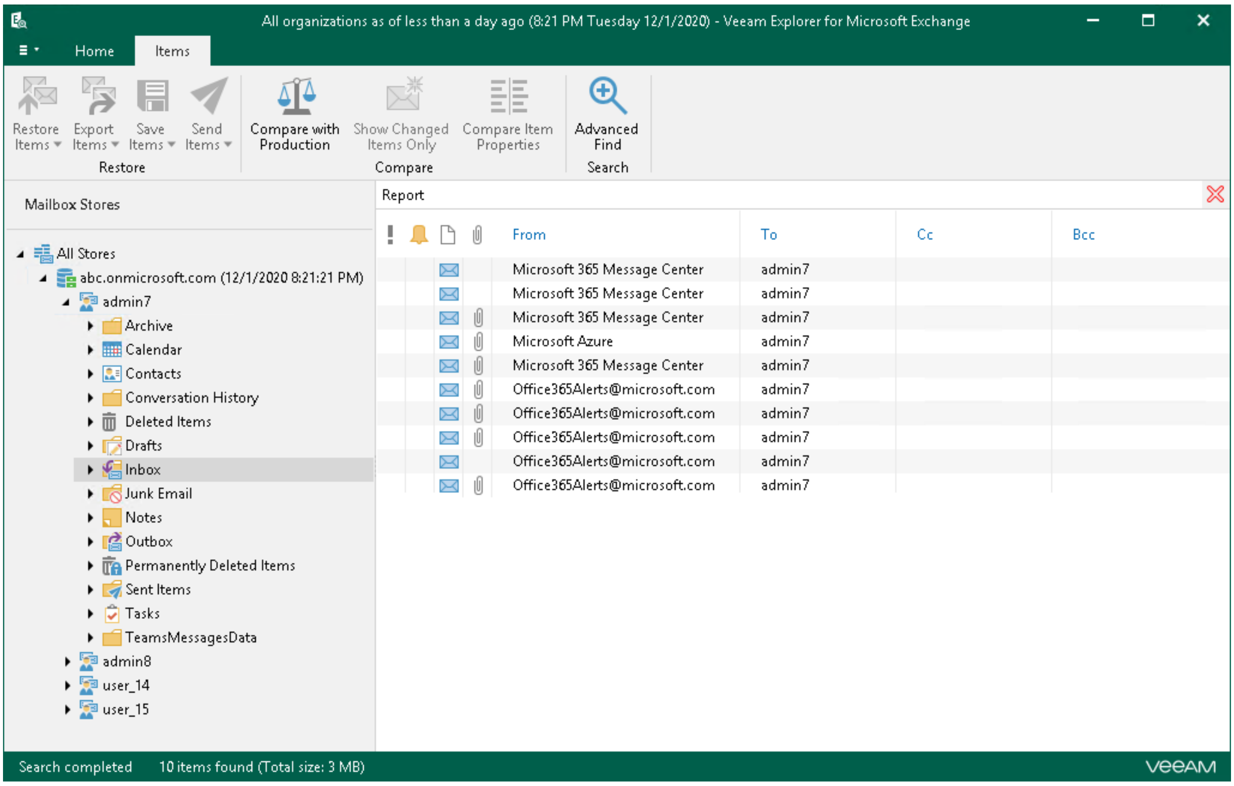
To search for required items, do the following:

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 *?*.



All organizations as of less than a day ago (8:21 PM Tuesday 12/1/2020) - Veeam Explorer for Microsoft Exchange

Report

!	🔔	📄	📎	From	To	Cc	Bcc
		✉		Microsoft 365 Message Center	admin7		
		✉		Microsoft 365 Message Center	admin7		
		✉	📎	Microsoft 365 Message Center	admin7		
		✉	📎	Microsoft Azure	admin7		
		✉	📎	Microsoft 365 Message Center	admin7		
		✉	📎	Office365Alerts@microsoft.com	admin7		
		✉	📎	Office365Alerts@microsoft.com	admin7		
		✉	📎	Office365Alerts@microsoft.com	admin7		
		✉		Office365Alerts@microsoft.com	admin7		
		✉	📎	Office365Alerts@microsoft.com	admin7		

Search completed 10 items found (Total size: 3 MB)

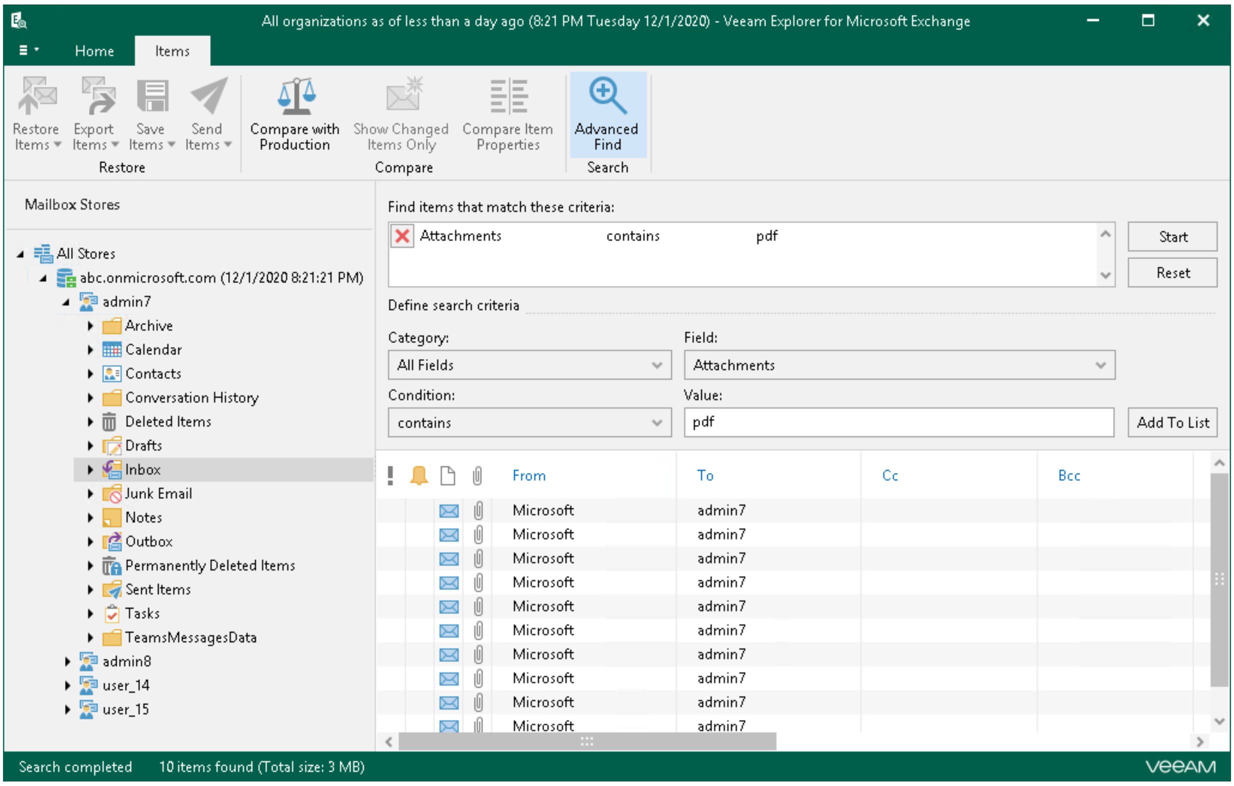
Using Advanced Find Capabilities

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 **Add to List**, then click **Start**.

To remove a filter, click the cross mark on the left. To remove all configured filters, click **Reset**.



All organizations as of less than a day ago (8:21 PM Tuesday 12/1/2020) - Veeam Explorer for Microsoft Exchange

Find items that match these criteria:

☒ Attachments contains pdf

Define search criteria

Category: All Fields

Field: Attachments

Condition: contains

Value: pdf

From	To	Cc	Bcc
Microsoft	admin7		
Microsoft	admin7		
Microsoft	admin7		
Microsoft	admin7		
Microsoft	admin7		
Microsoft	admin7		
Microsoft	admin7		
Microsoft	admin7		
Microsoft	admin7		
Microsoft	admin7		

Search completed 10 items found (Total size: 3 MB)

General Application Settings

Continue with this section to learn more about configuring general application settings and components.

Extensible Storage Engine

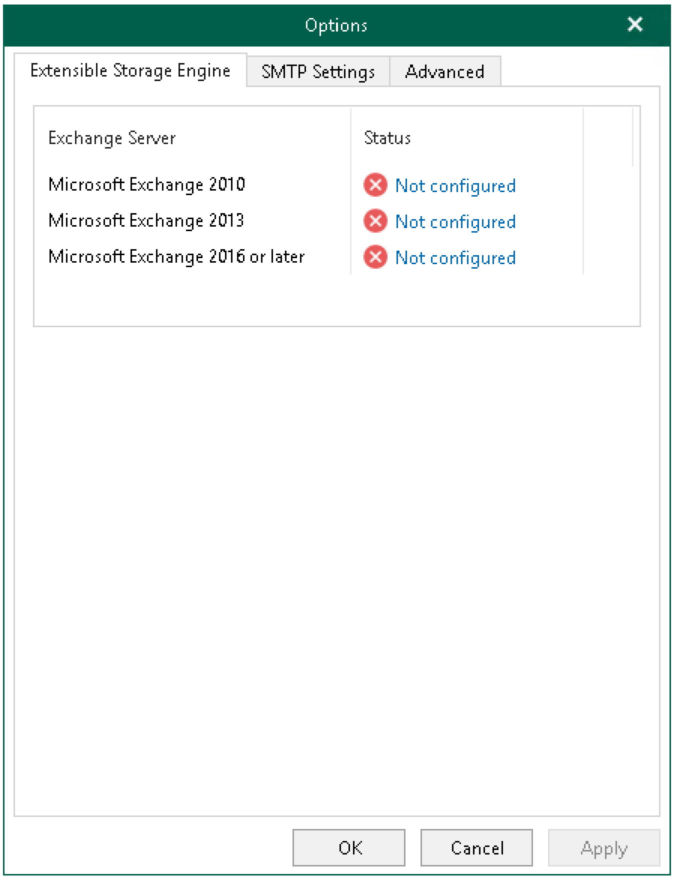
To work with database files, Veeam Explorer for Microsoft Exchange requires a dynamic link library `ese.dll` which is distributed with Microsoft Exchange.

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.



Exchange Server	Status
Microsoft Exchange 2010	☒ Not configured
Microsoft Exchange 2013	☒ Not configured
Microsoft Exchange 2016 or later	☒ Not configured

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:

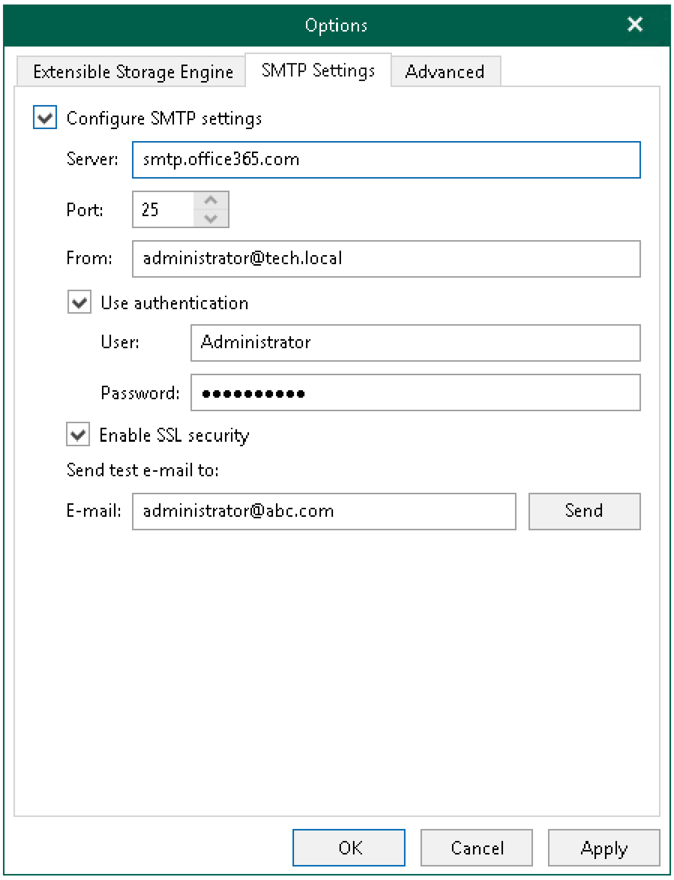
1. Go to the main menu and click **General Options**.
2. Open the **SMTP Settings** tab.
3. Select the **Configure SMTP settings** check box and do the following:
   a. In the **Server** field, specify a DNS name or IP address of the SMTP server.

   b. In the **Port** field, specify a port number of the specified AMTP 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**.



☑ Configure SMTP settings

Server: smtp.office365.com

Port: 25

From: administrator@tech.local

☑ Use authentication

User: Administrator

Password: ●●●●●●●●●●●

☑ Enable SSL security

Send test e-mail to:

E-mail: administrator@abc.com [Send]

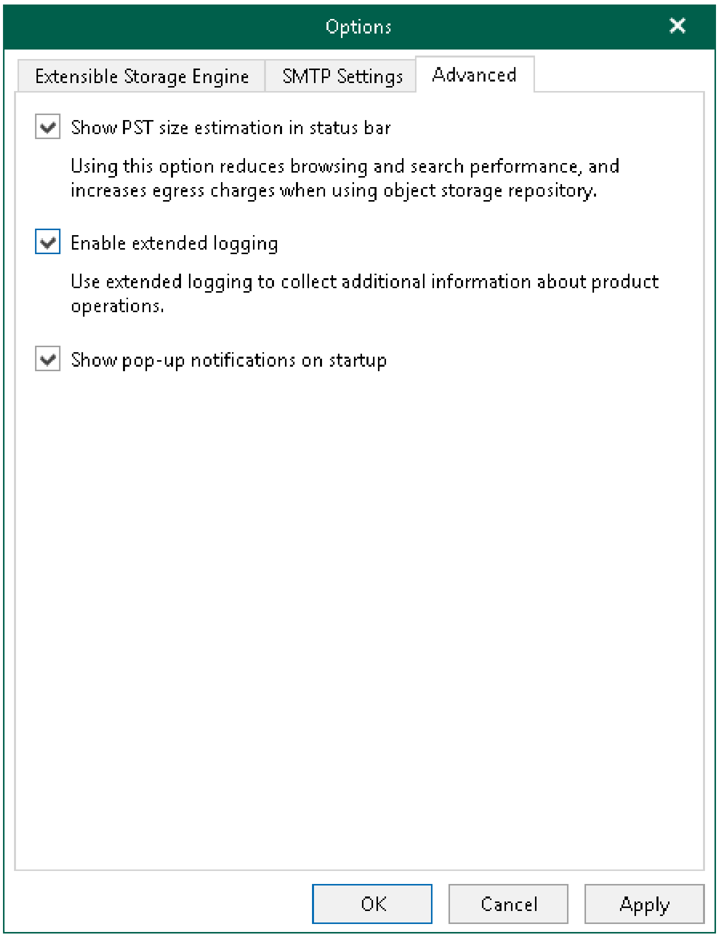
Advanced Settings

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. Click the **Advanced** tab.
3. Select the **Show PST size estimation in status bar** check box if you want to see the estimated size of the Outlook database file in the status bar.
4. Select the **Enable extended logging** check box 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.
5. By default, Veeam Explorer for Microsoft Exchange displays notifications when loading backups from object storage repositories. If you want to disable these notifications, clear the **Show pop-up notifications on startup** check box.



☑ Show PST size estimation in status bar

Using this option reduces browsing and search performance, and increases egress charges when using object storage repository.

☑ Enable extended logging

Use extended logging to collect additional information about product operations.

☑ Show pop-up notifications on startup

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.

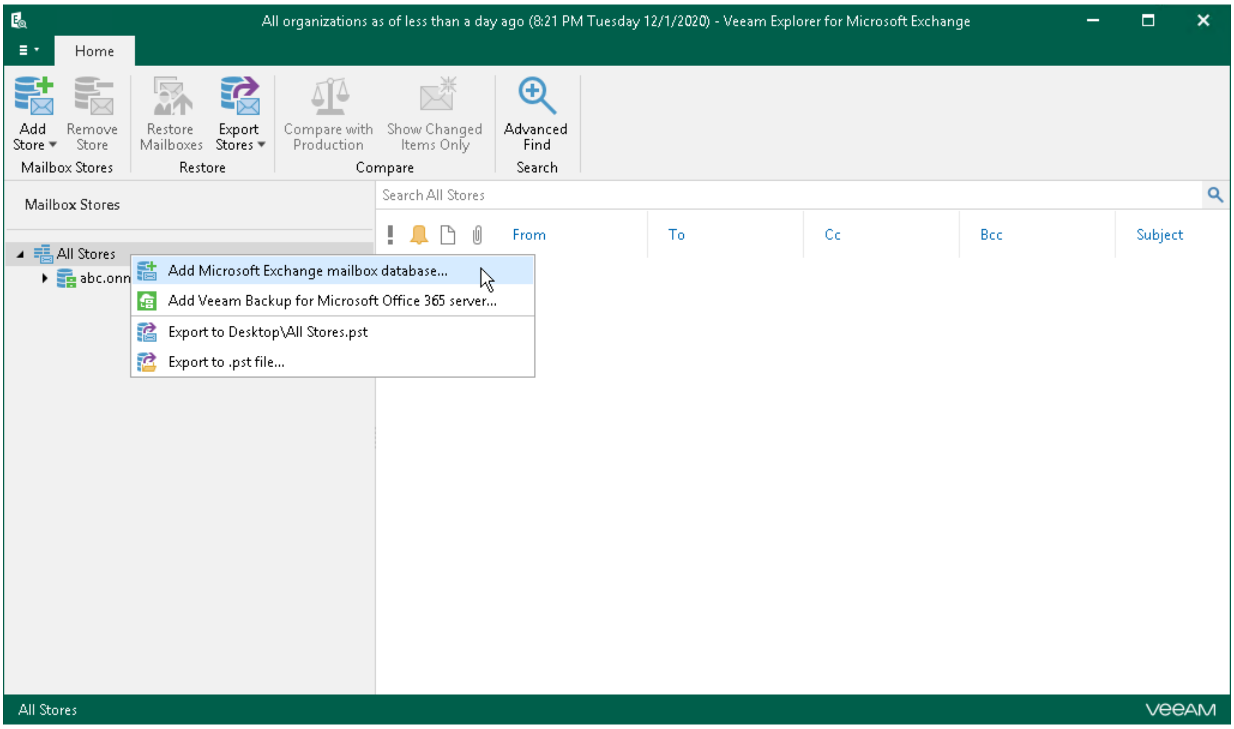
Adding Microsoft Exchange Stores

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 wail 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 **Add Microsoft Exchange mailbox database**.
2. Click **Browse** to specify the path to the `.edb` file and Exchange logs folder.



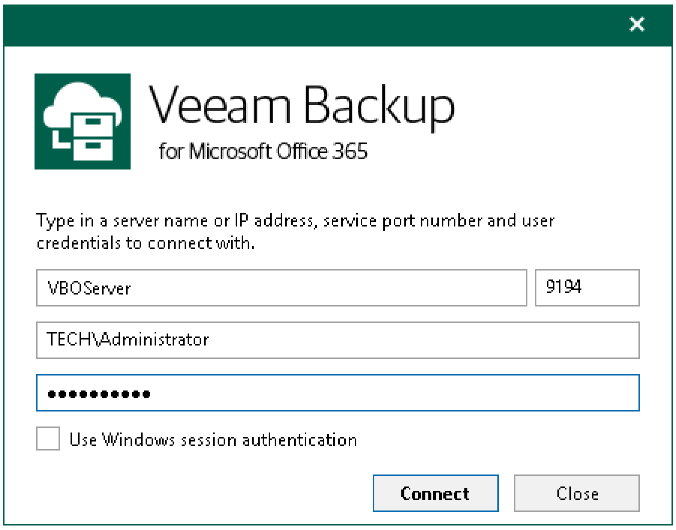
Adding Veeam Backup for Microsoft Office 365 Server

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**.



Type in a server name or IP address, service port number and user credentials to connect with.

VBOServer 9194

TECH\Administrator

•••••••••••

□ Use Windows session authentication

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.

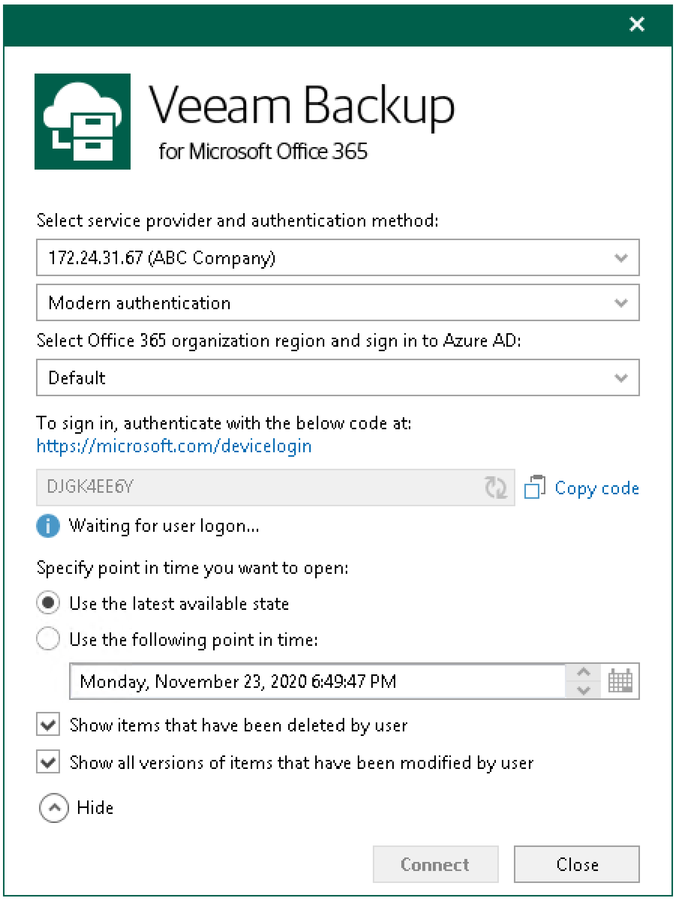
   For *Basic authentication*, you must enter a user name and password to connect to the service provider server.
6. Select a point-in-time state as of which you want to load Office 365 backups.

   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**.



Select service provider and authentication method:

172.24.31.67 (ABC Company)

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

DJGK4EE6Y

Waiting for user logon...

Specify point in time you want to open:

● Use the latest available state

○ Use the following point in time:

Monday, November 23, 2020 6:49:47 PM

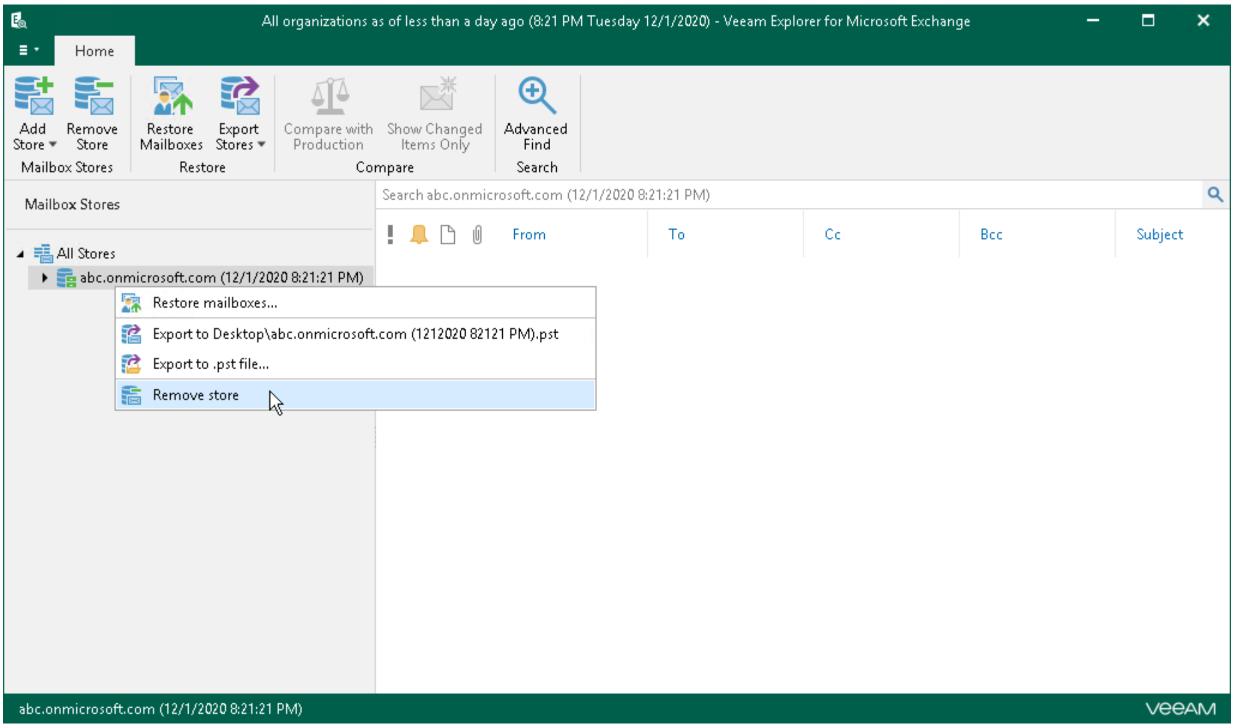
☑ Show items that have been deleted by user

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

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**.


All organizations as of less than a day ago (8:21 PM Tuesday 12/1/2020) - Veeam Explorer for Microsoft Exchange
Home
Add Store
Remove Store
Mailbox Stores
Restore Mailboxes
Export Stores
Restore
Compare with Production
Show Changed Items Only
Compare
Advanced Find
Search
Mailbox Stores
Search abc.onmicrosoft.com (12/1/2020 8:21:21 PM)
From
To
Cc
Bcc
Subject
All Stores
abc.onmicrosoft.com (12/1/2020 8:21:21 PM)
Restore mailboxes...
Export to Desktop\abc.onmicrosoft.com (1212020 82121 PM).pst
Export to .pst file...
Remove store
abc.onmicrosoft.com (12/1/2020 8:21:21 PM)
veeam

Restore

This section explains how to restore data to Microsoft Office 365 and on-premises Microsoft organizations.

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

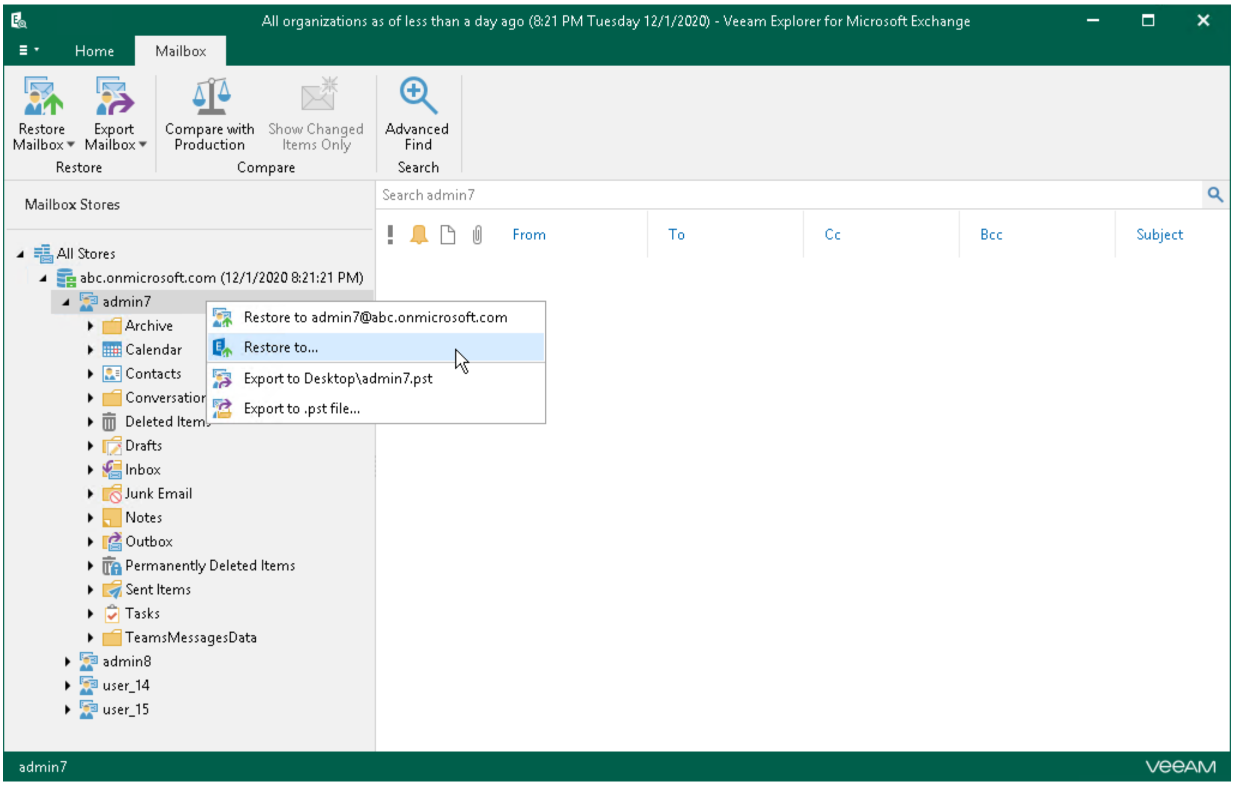
To restore the selected Exchange mailbox, do the following:

1. Launch the Restore wizard.
2. Specify a target mailbox.
3. Select an authentication method.
4. Log in 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 pane, 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** 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.

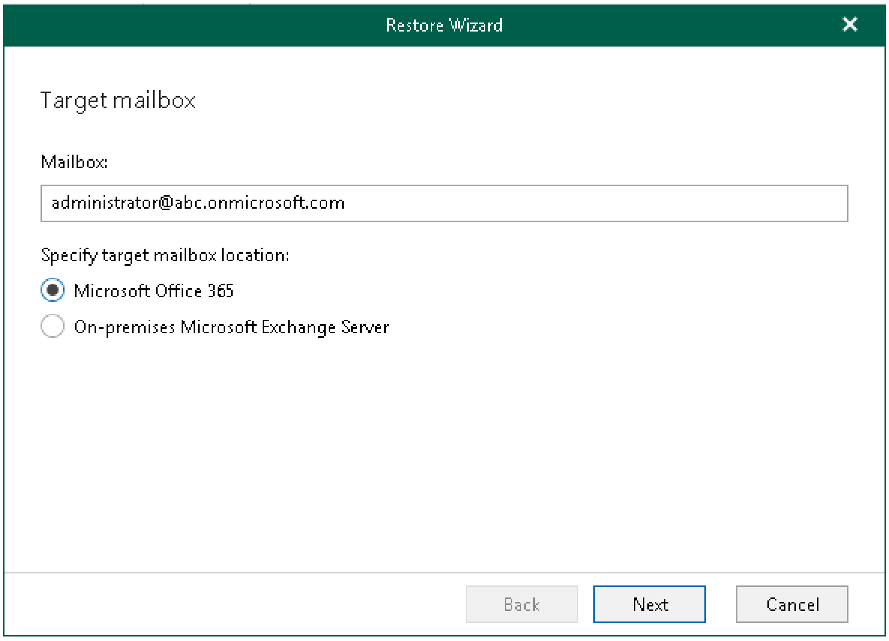
To specify mailbox settings, do the following:

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 example, *administrator@xyz.onmicrosoft.com* to restore a mailbox to the *xyz.onmicrosoft.com* organization.

2. Select **Microsoft Office 365** 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.



Mailbox: administrator@abc.onmicrosoft.com

Specify target mailbox location:

● Microsoft Office 365

○ On-premises Microsoft Exchange Server

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.

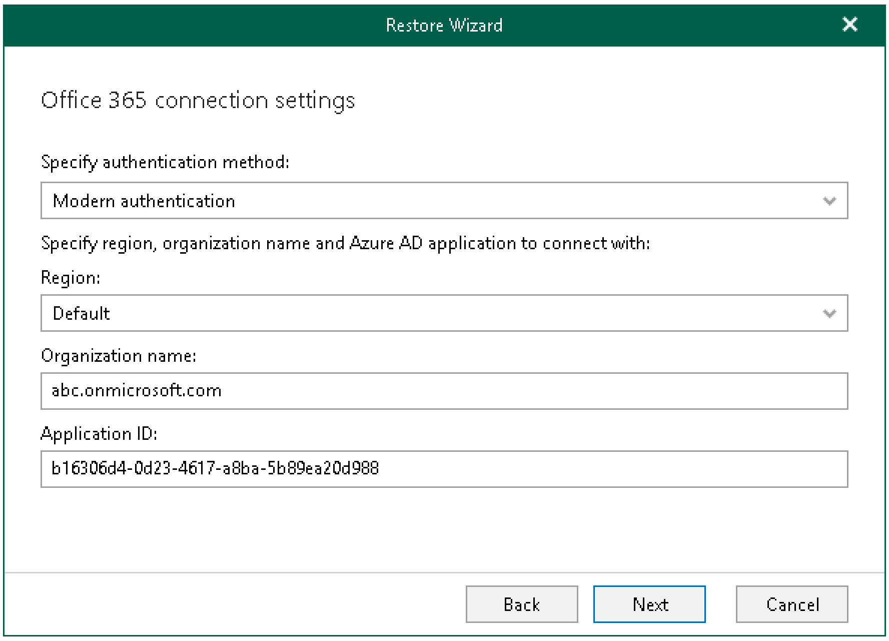
2. From the **Region** drop-down list, select a region to which your Exchange Online organization belongs.

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

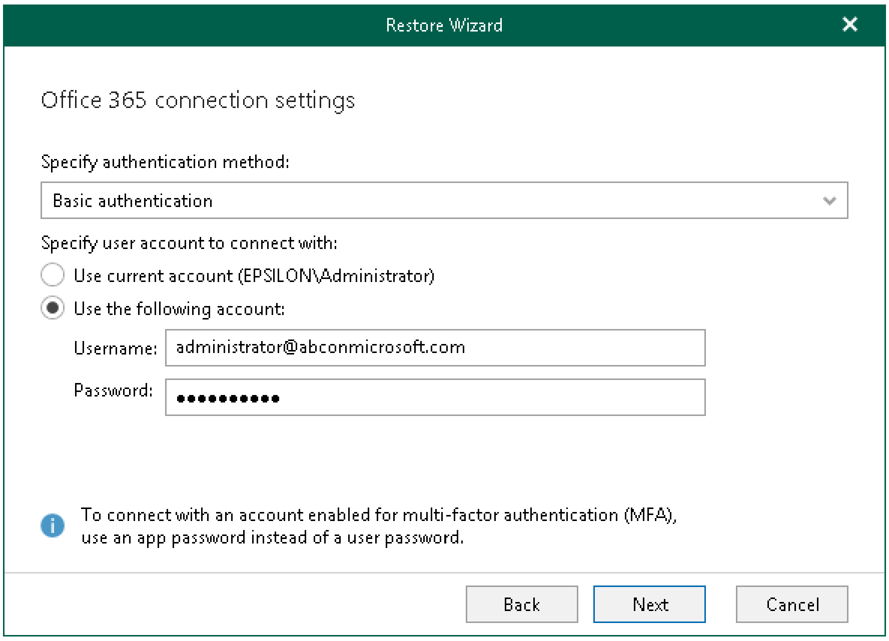
Application ID: b16306d4-0d23-4617-a8ba-5b89ea20d988

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 (EPSILON\Administrator)

● Use the following account:

Username: administrator@abconmicrosoft.com

Password: •••••••••••

To connect with an account enabled for multi-factor authentication (MFA), use an app password instead of a user password.

Step 4. Log In 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 365 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.

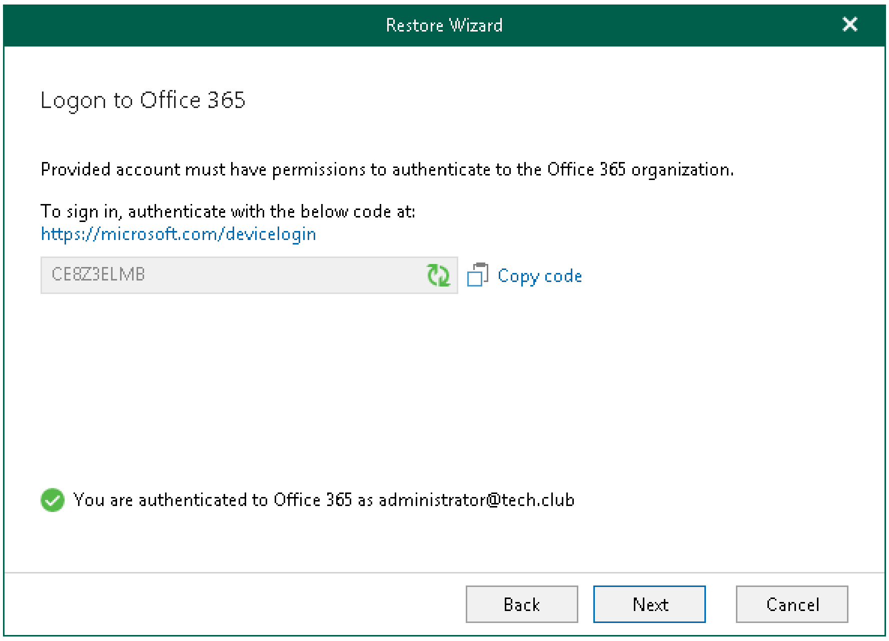
2. Click the link to the Microsoft portal.

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 required permissions assigned. For more information, see Required Permissions.

   Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see Required Azure AD Application Settings.

4. Return to the **Restore Wizard** window and click **Next**.



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

CE8Z3ELMB

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

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.

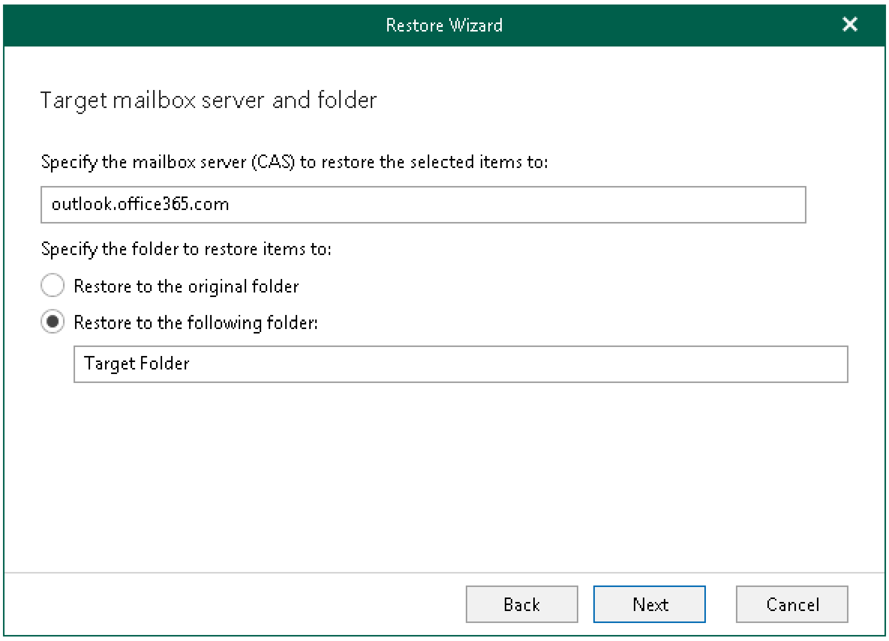
To provide a CAS server and target folder, do the following:

1. Specify a CAS server name or 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 custom 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.



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:

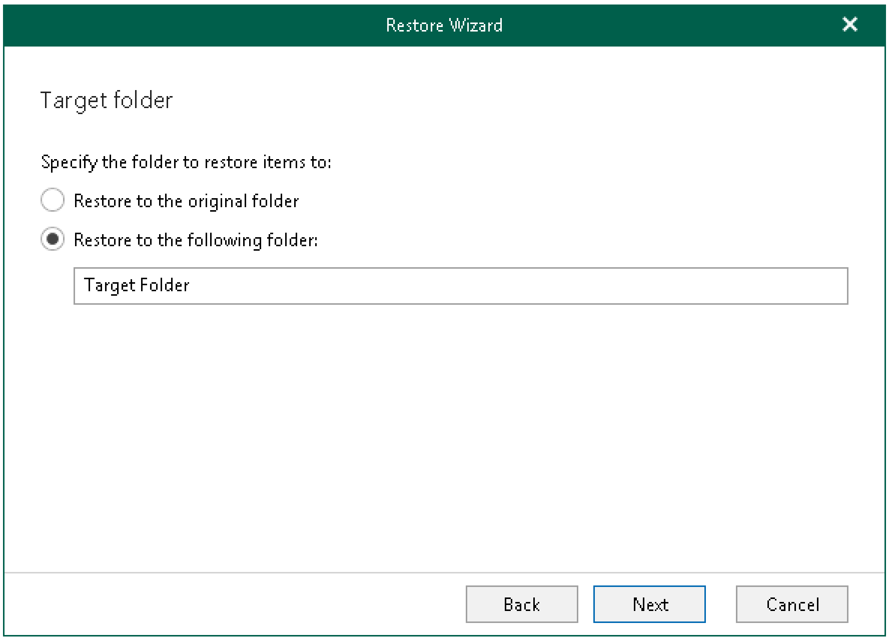
Target Folder

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 custom 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.



Specify the folder to restore items to:

○ Restore to the original folder

● Restore to the following folder:

Target Folder

Step 7. Specify Restore Options

At this step of the wizard, select restore options and click **Restore**.

You can select the following options:

- **Changed items**

  Select this check box if you want to restore items that have been changed. When you select this option, Veeam Explorer for Microsoft Exchange overwrites existing items in your target location.

- **Missing Items**

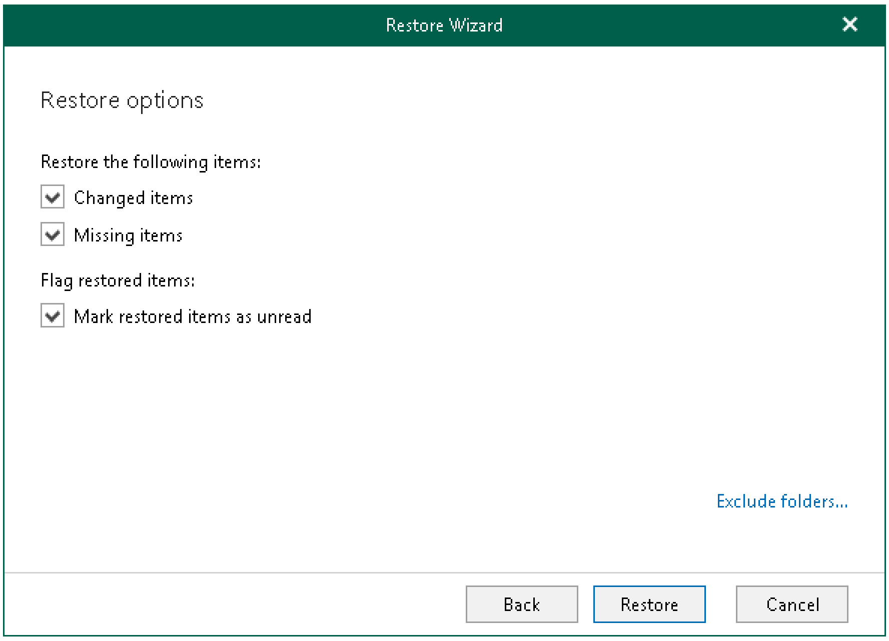
  Select this check box if you want to restore items that are missed in your target location. For example, some of the items were removed and you want to restore them from the backup.

- **Mark restored items as unread**

  Select this check box if you want to mark each restored item as unread.

To prevent certain folders from being restored, click the **Exclude folders** link and select folders to exclude.

> **NOTE:**
>
> The **Exclude folders** link is not available when restoring folders and items.



Restore options

Restore the following items:

☑ Changed items

☑ Missing items

Flag restored items:

☑ Mark restored items as unread

Restoring Multiple Mailboxes

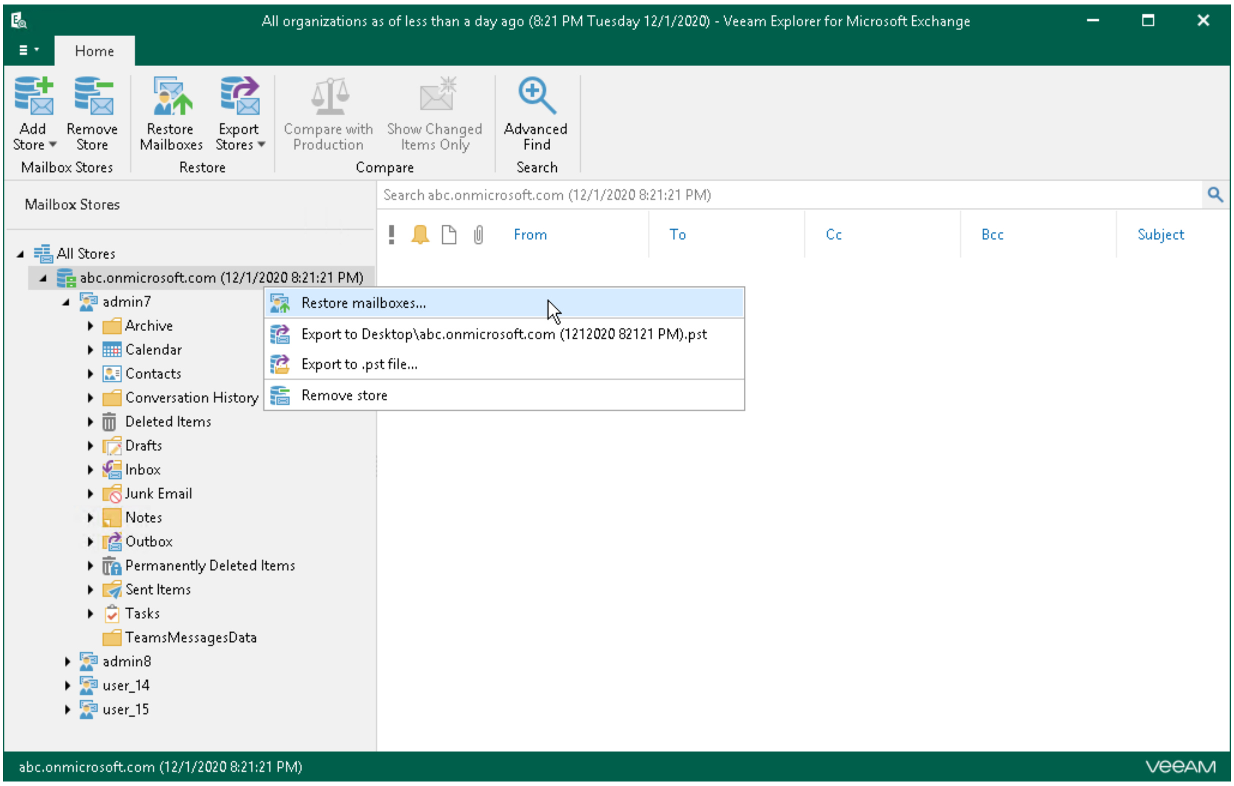
To restore multiple Exchange mailboxes, do the following:

1. Launch the Restore wizard.
2. Select an authentication method.
3. Log in 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 pane, select an organization (container) whose mailboxes 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:

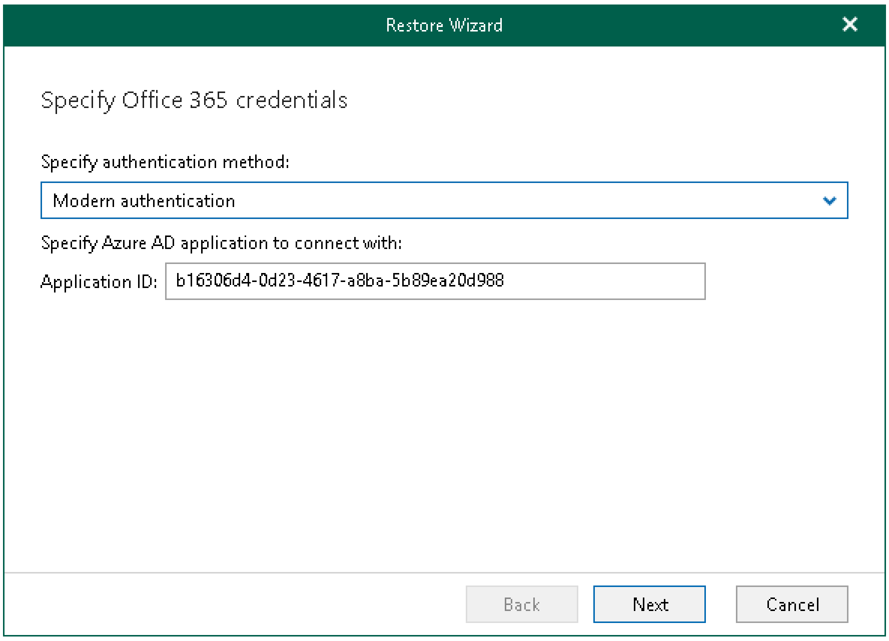
1. From the **Specify authentication method** drop-down list, select *Modern authentication*.

   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.



Specify Office 365 credentials

Specify authentication method: Modern authentication

Specify Azure AD application to connect with:

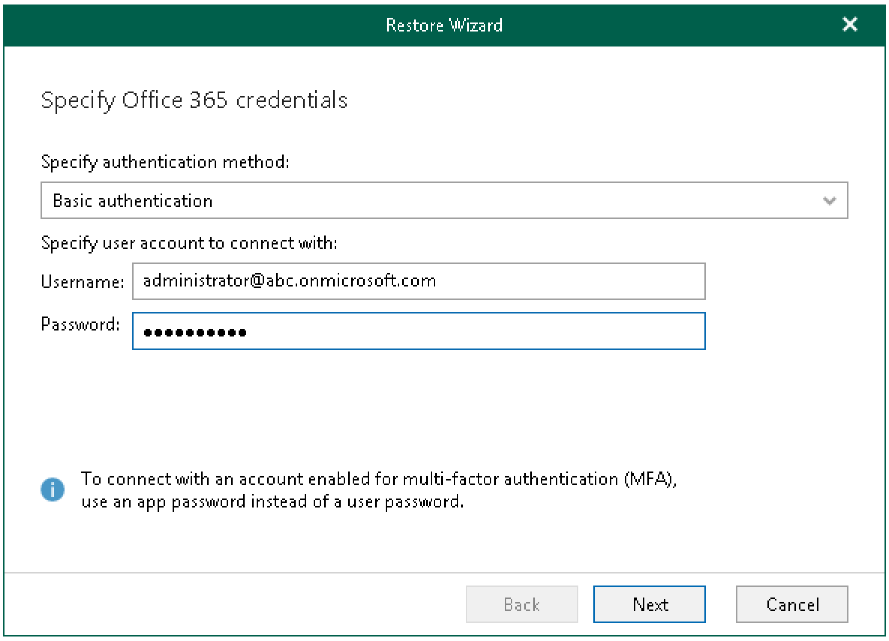
Application ID: b16306d4-0d23-4617-a8ba-5b89ea20d988

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.



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.

Step 3. Log In 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 365 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.

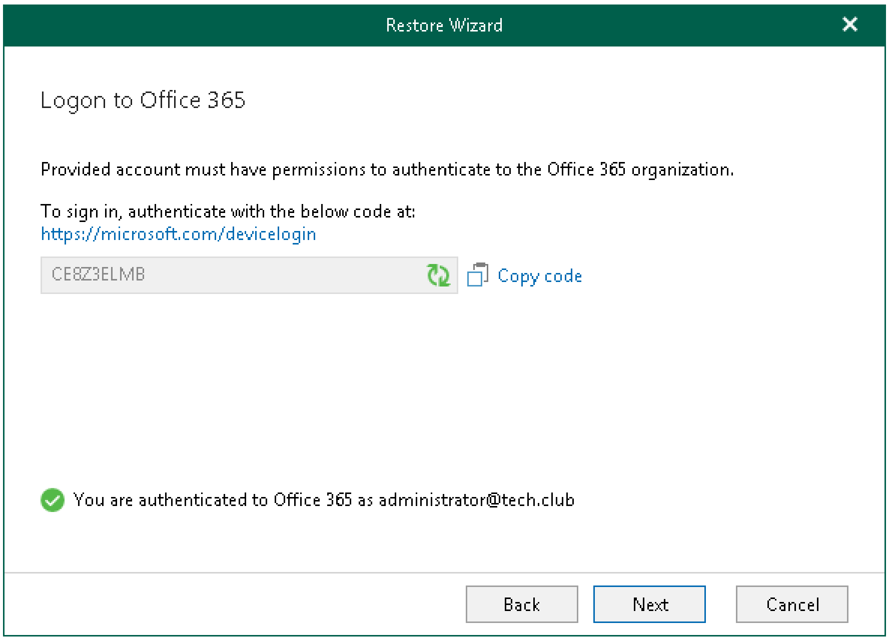
2. Click the link to the Microsoft portal.

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 required permissions assigned. For more information, see Required Permissions.

   Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see Required Azure AD Application Settings.

4. Return to the **Restore Wizard** window and click **Next**.



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

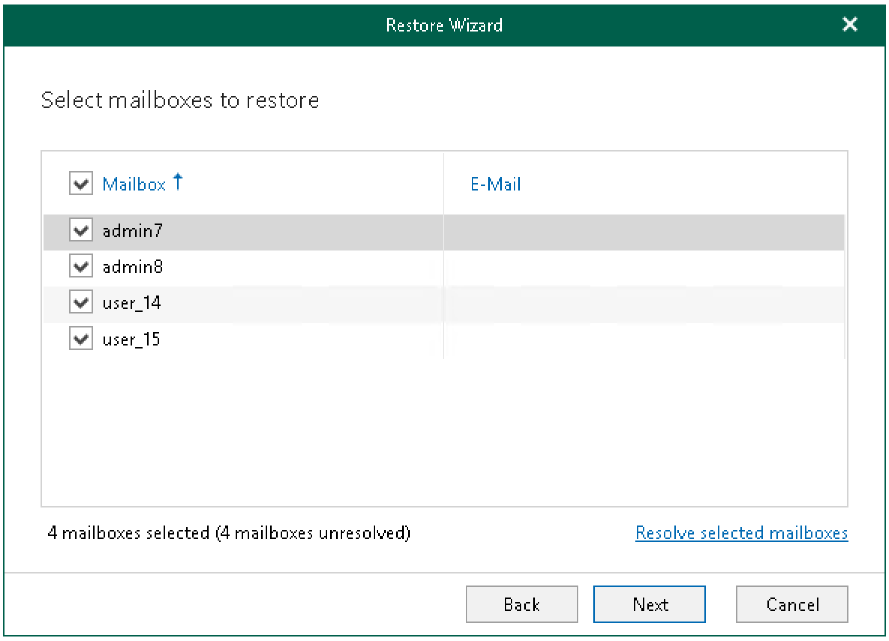
CE8Z3ELMB

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

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**.



☑ Mailbox	E-Mail
☑ admin7	
☑ admin8	
☑ user_14	
☑ user_15	

4 mailboxes selected (4 mailboxes unresolved)

Step 5. Select Restore Options

At this step of the wizard, select restore options and click **Restore**.

You can select the following options:

- **Changed items**

  Select this check box if you want to restore items that have been changed. When you select this option, Veeam Explorer for Microsoft Exchange overwrites existing items in your target location.

- **Missing Items**

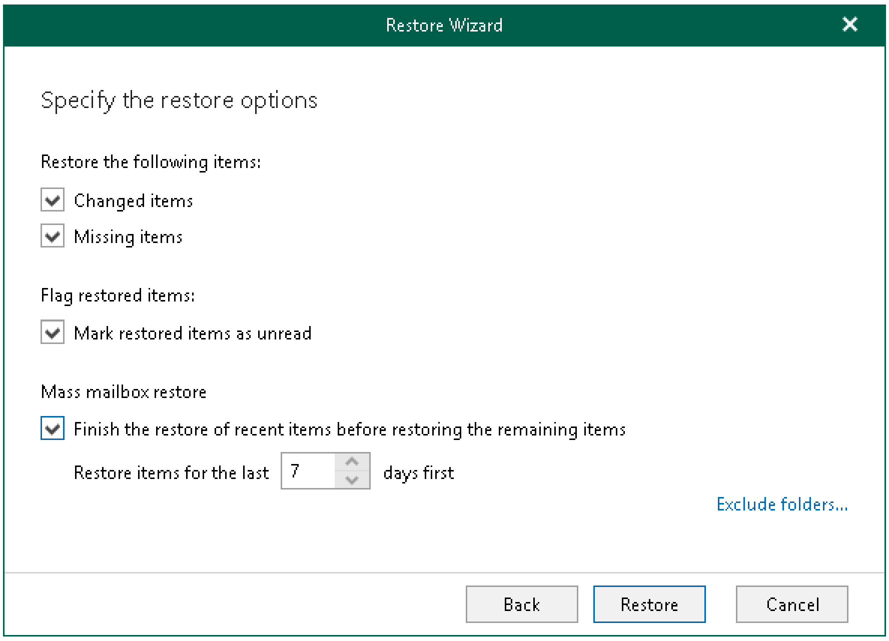
  Select this check box if you want to restore items that are missed in your target location. For example, some of the items were removed and you want to restore them from the backup.

- **Mark restored items as unread**

  Select this check box if you want to mark each restored item 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.



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

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

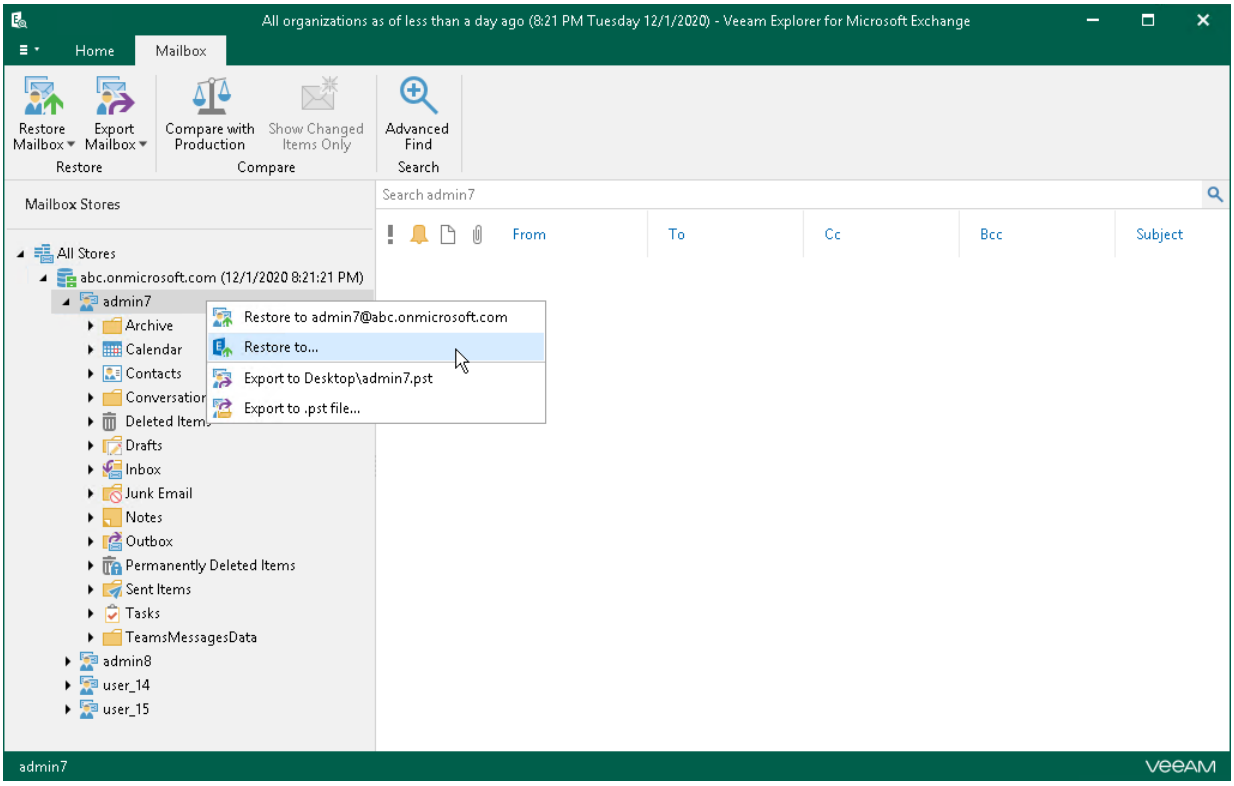
To restore mailboxes, folders and items, do the following:

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 pane, 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** or right-click a mailbox, folder or an item and select **Restore to**.



Step 2. Specify Target Mailbox

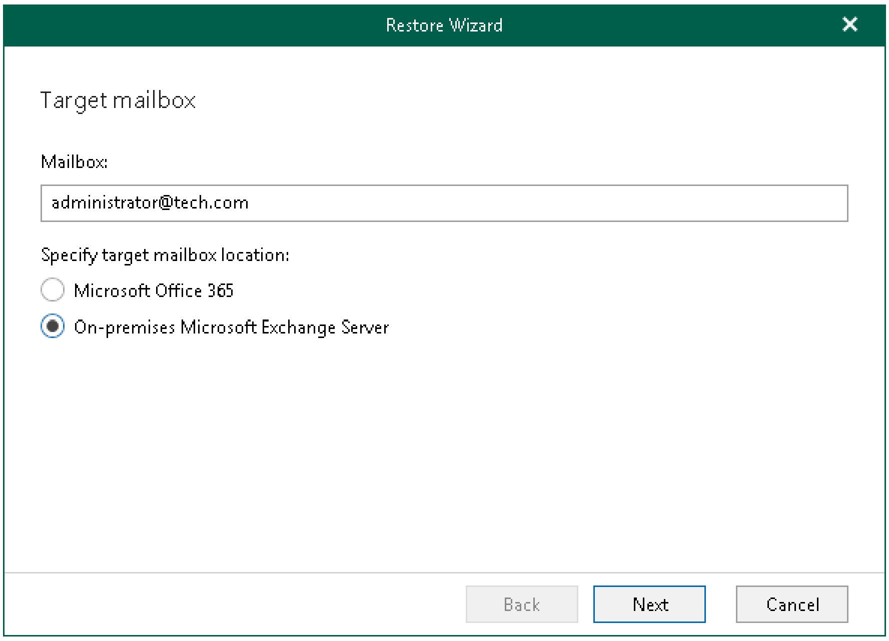
At this step of the wizard, specify the target mailbox and mailbox location.

To specify mailbox settings, do the following:

1. In the **Mailbox** field, enter a mailbox name to which you want to restore data.

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

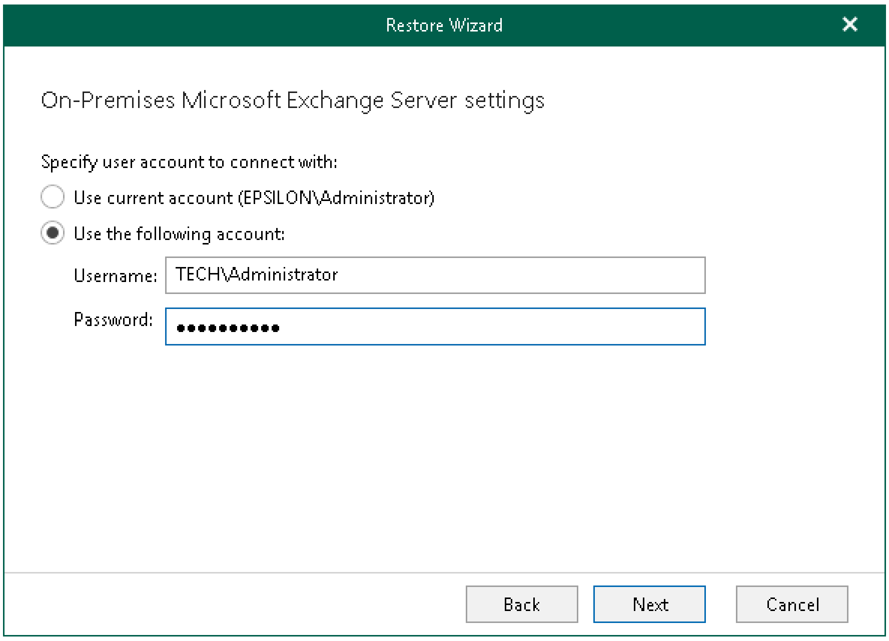
Specify target mailbox location:

○ Microsoft Office 365

● On-premises Microsoft Exchange Server

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.



On-Premises Microsoft Exchange Server settings

Specify user account to connect with:

○ Use current account (EPSILON\Administrator)

● Use the following account:

Username: TECH\Administrator

Password: ●●●●●●●●●●●

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.

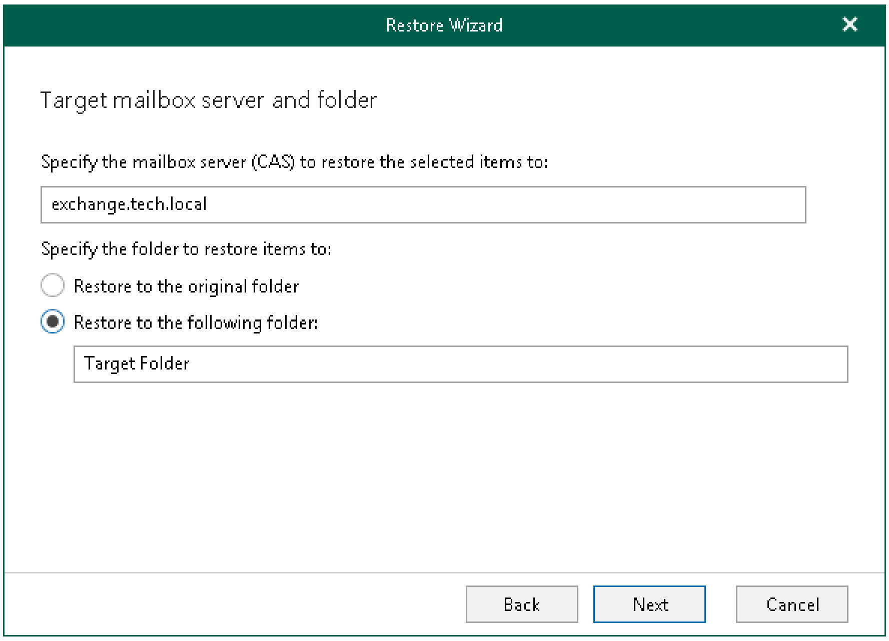
To provide a CAS server and target folder, do the following:

1. Specify a CAS server name or 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 custom 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.



Target mailbox server and folder

Specify the mailbox server (CAS) to restore the selected items to:

exchange.tech.local

Specify the folder to restore items to:

○ Restore to the original folder

● Restore to the following folder:

Target Folder

Step 5. Specify Restore Options

At this step of the wizard, select restore options and click **Restore**.

You can select the following options:

- **Changed items**

  Select this check box if you want to restore items that have been changed. When you select this option, Veeam Explorer for Microsoft Exchange overwrites existing items in your target location.

- **Missing Items**

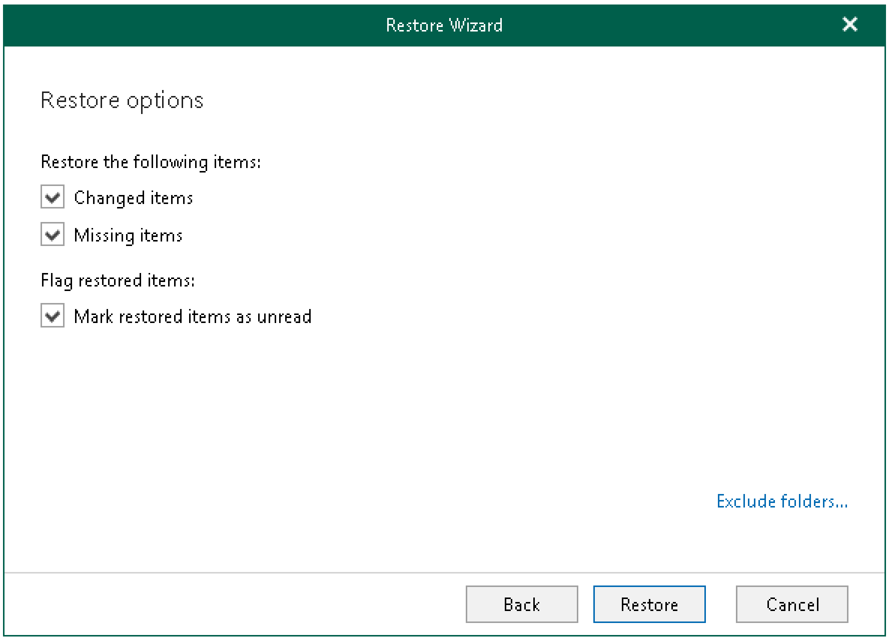
  Select this check box if you want to restore items that are missed in your target location. For example, some of the items were removed and you want to restore them from the backup.

- **Mark restored items as unread**

  Select this check box if you want to mark each restored item 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.



Restore options

Restore the following items:

☑ Changed items

☑ Missing items

Flag restored items:

☑ Mark restored items as unread

Restoring Multiple mailboxes

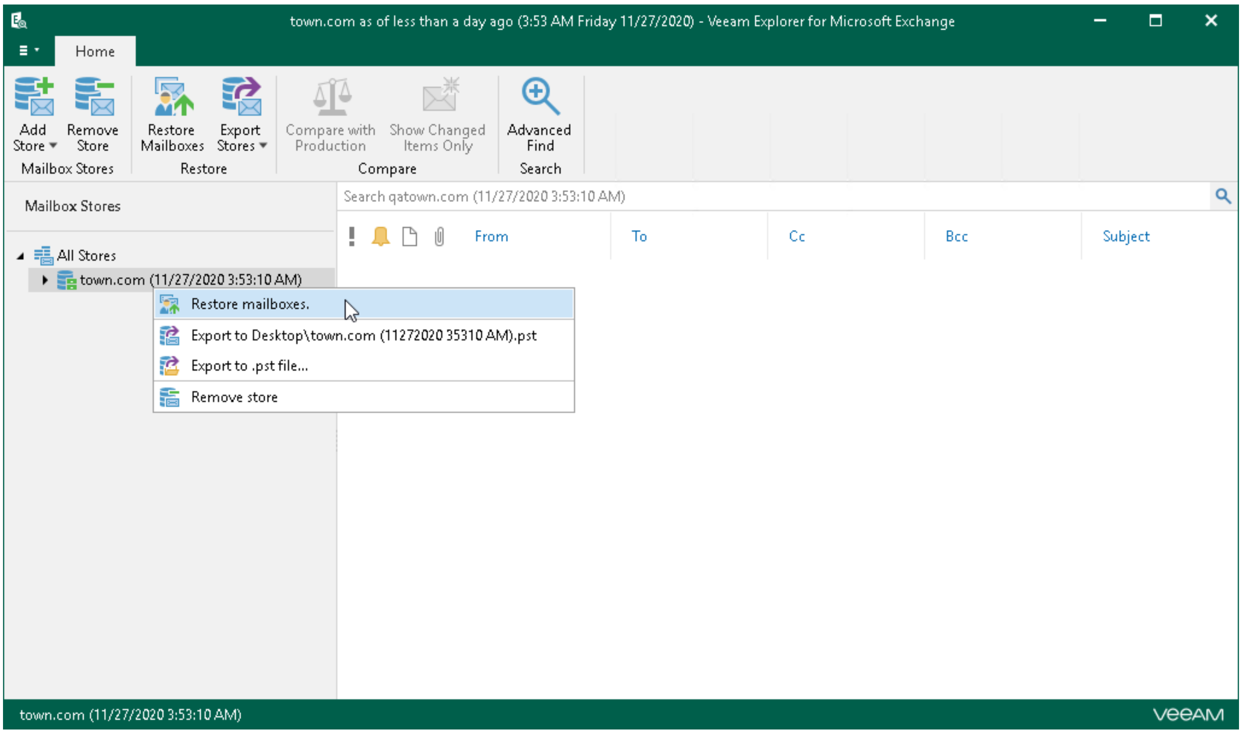
To restore multiple Exchange mailboxes, do the following:

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

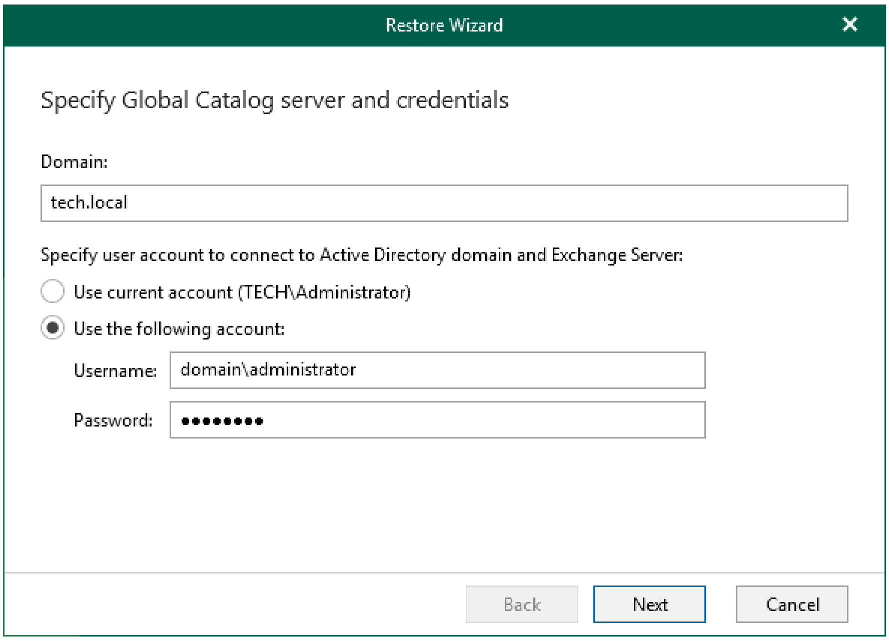
To launch the **Restore** wizard, do the following:

1. In the navigation pane, select a mailbox store whose mailboxes you want to restore.
2. On the **Home** tab, select **Restore Mailboxes** or right-click a mailbox store and select **Restore mailboxes**.


town.com as of less than a day ago (3:53 AM Friday 11/27/2020) - Veeam Explorer for Microsoft Exchange
Home
Add Store
Remove Store
Mailbox Stores
Restore Mailboxes
Export Stores
Restore
Compare with Production
Show Changed Items Only
Compare
Advanced Find
Search
Mailbox Stores
Search qatown.com (11/27/2020 3:53:10 AM)
From
To
Cc
Bcc
Subject
All Stores
town.com (11/27/2020 3:53:10 AM)
Restore mailboxes.
Export to Desktop\town.com (11272020 35310 AM).pst
Export to .pst file...
Remove store
town.com (11/27/2020 3:53:10 AM)
veeam

Step 2. Specify Domain and Credentials

At this step of the wizard, enter a domain name where your CAS server resides and provide credentials.



Specify Global Catalog server and credentials

Domain: tech.local

Specify user account to connect to Active Directory domain and Exchange Server:

○ Use current account (TECH\Administrator)

● Use the following account:

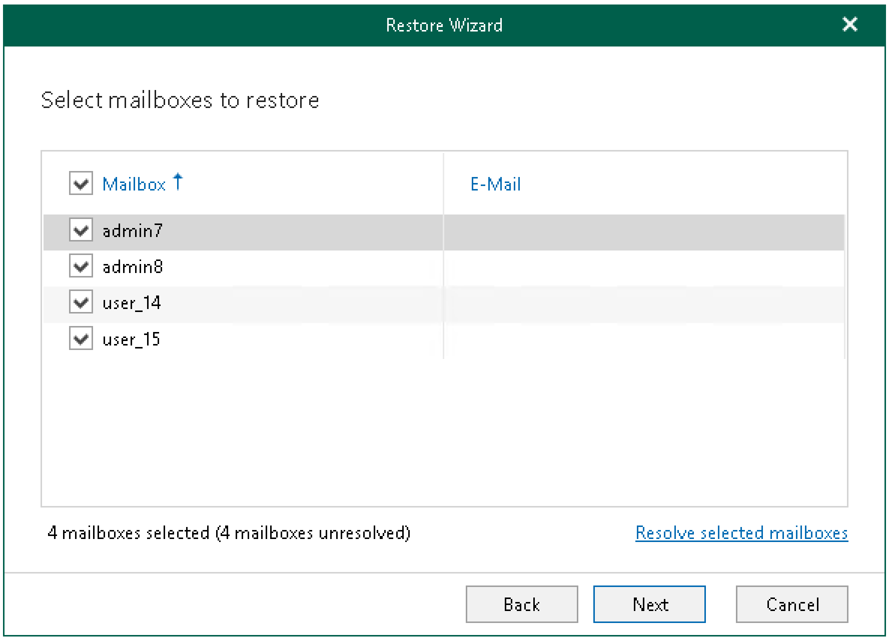
Username: domain\administrator

Password: ••••••••

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**.

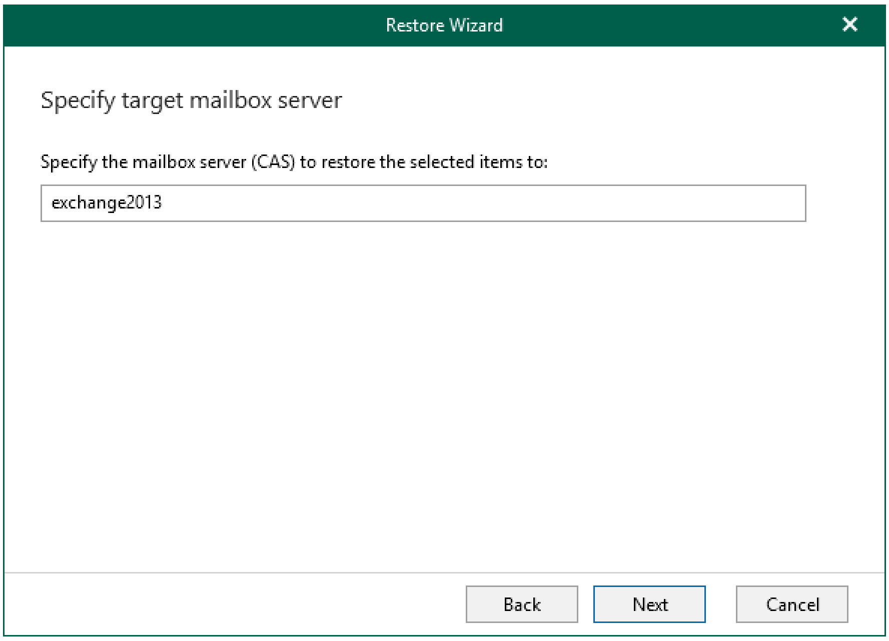


☑ Mailbox ↑	E-Mail
☑ admin7	
☑ admin8	
☑ user_14	
☑ user_15	

4 mailboxes selected (4 mailboxes unresolved)

Step 4. Specify Target Mailbox Server

At this step of the wizard, specify a target server to which you want to restore mailboxes.



Restore Wizard

Specify target mailbox server

Specify the mailbox server (CAS) to restore the selected items to:

exchange2013

Step 5. Select Restore Options

At this step of the wizard, select restore options and click **Restore**.

You can select the following options:

- **Changed items**

  Select this check box if you want to restore items that have been changed. When you select this option, Veeam Explorer for Microsoft Exchange overwrites existing items in your target location.

- **Missing Items**

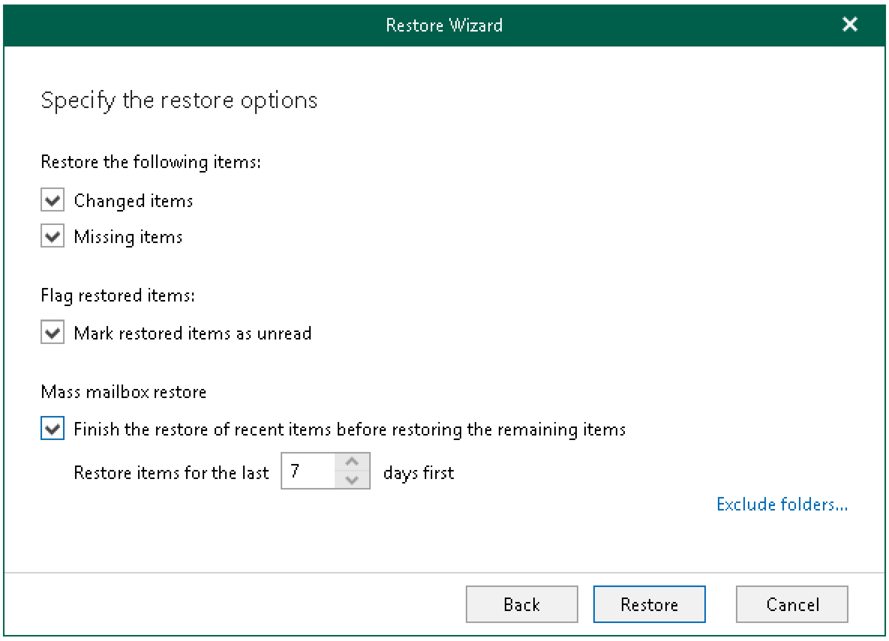
  Select this check box if you want to restore items that are missed in your target location. For example, some of the items were removed and you want to restore them from the backup.

- **Mark restored items as unread**

  Select this check box if you want to mark each restored item 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

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 in to Office 365.

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. In the navigation pane, 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:

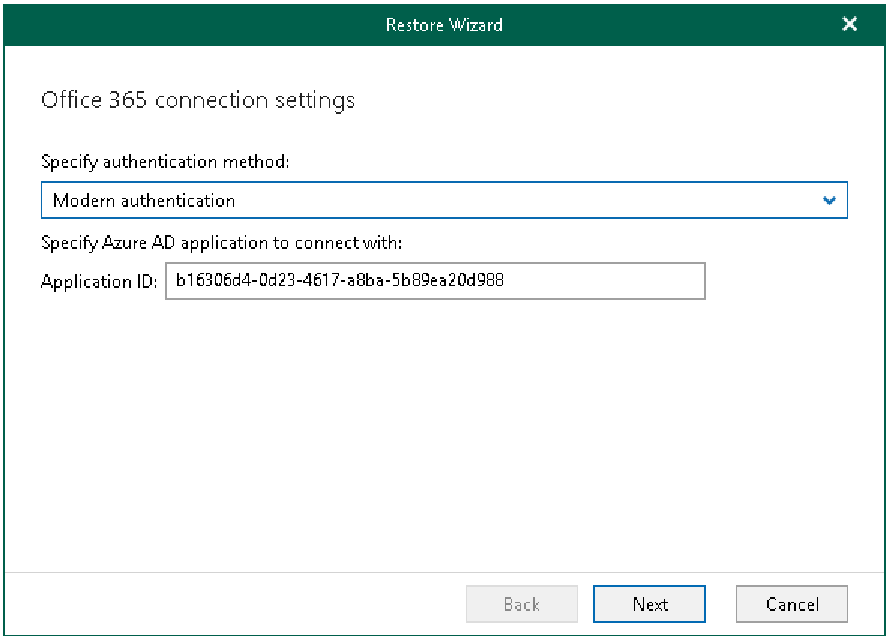
1. From the **Specify authentication method** drop-down list, select *Modern authentication*.

   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.



Office 365 connection settings

Specify authentication method: Modern authentication

Specify Azure AD application to connect with:

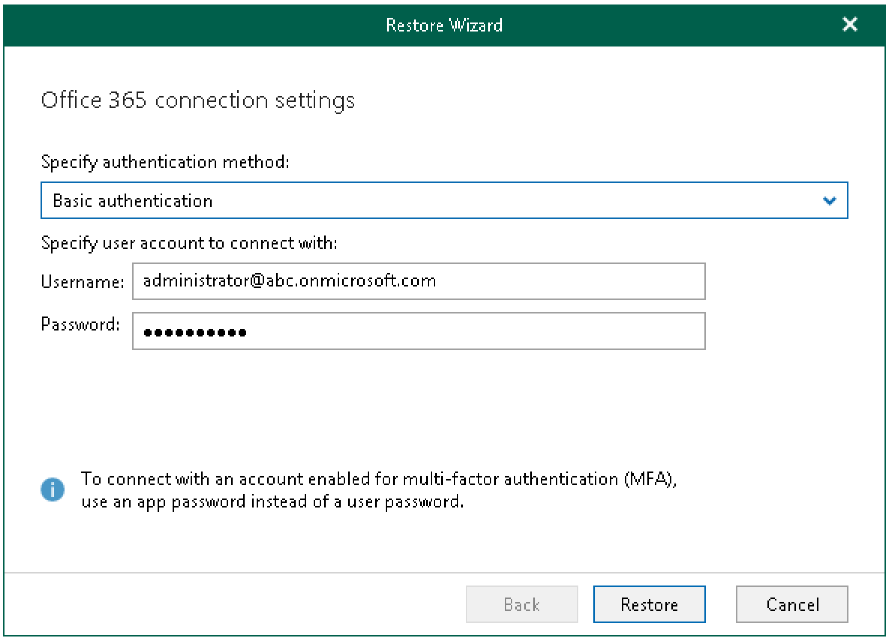
Application ID: b16306d4-0d23-4617-a8ba-5b89ea20d988

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 **Restore**.

   Make that the account that you use has both the *Exchange Admin* and the *Global Admin* roles.



Office 365 connection settings

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.

Step 3. Log In 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 365 organization, do the following:

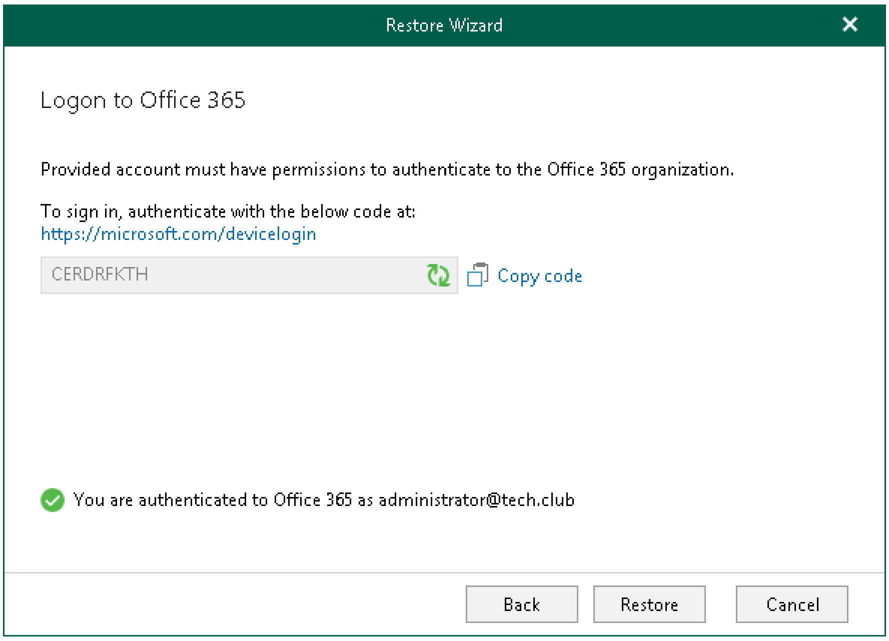
1. Click **Copy code** to copy an authentication code.

   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**.



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

CERDRFKTH

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

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.

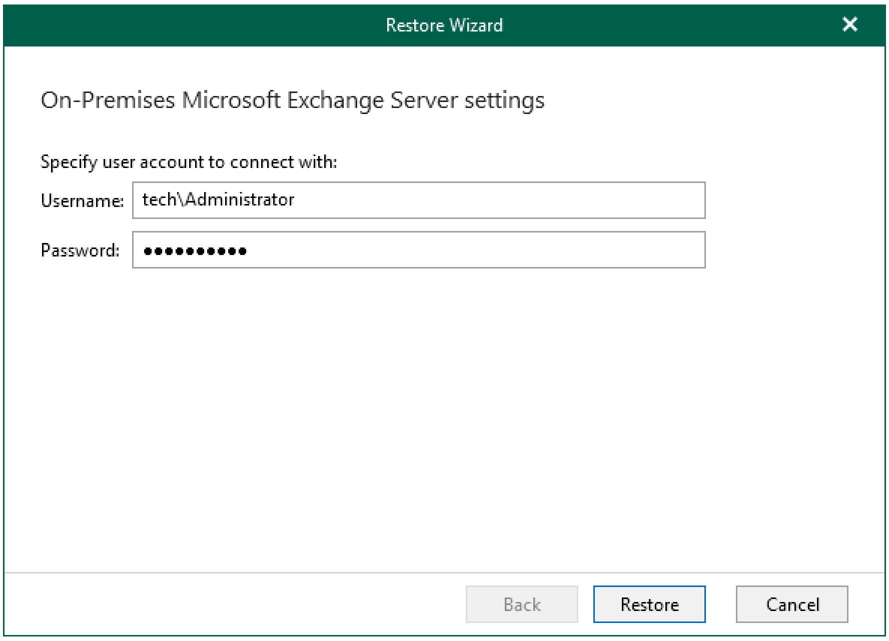
Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. In the navigation pane, 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.



Specify user account to connect with:

Username: tech\Administrator

Password: ●●●●●●●●●●●

Export

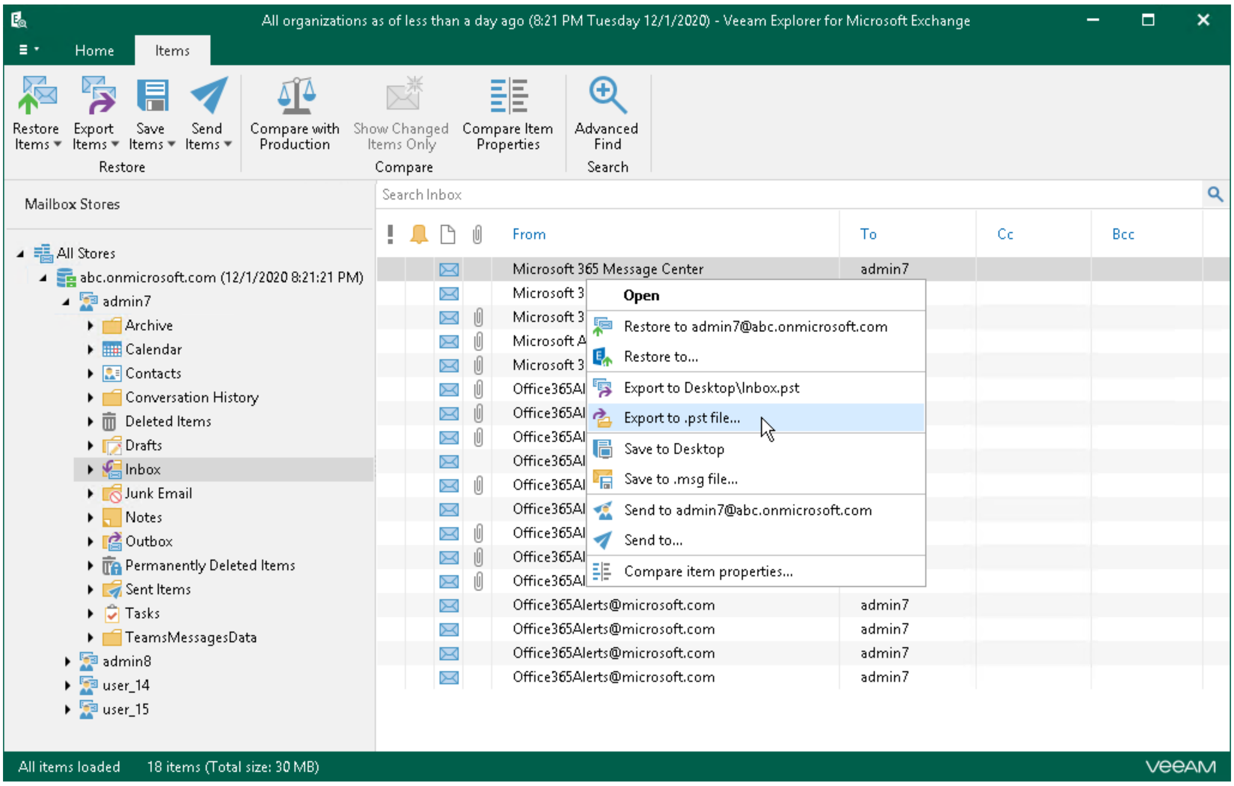
Continue with this section to learn more about exporting Microsoft Exchange data.

> **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/Export Items > Export to .pst file** or right-click a folder/item and select **Export to .pst file**.



From	To	Cc	Bcc
Microsoft 365 Message Center	admin7		
Microsoft 3			
Microsoft 3			
Microsoft A			
Microsoft 3			
Office365Al			
Office365Al			
Office365Al			
Office365Al			
Office365Al			
Office365Al			
Office365Al			
Office365Al			
Office365Al			
Office365Alerts@microsoft.com	admin7		
Office365Alerts@microsoft.com	admin7		
Office365Alerts@microsoft.com	admin7		
Office365Alerts@microsoft.com	admin7		

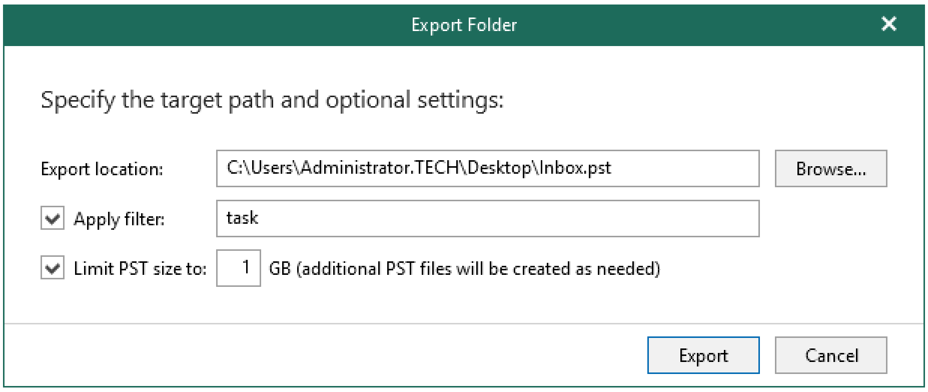
3. In the **Export Folder**/**Export Mail Items** window, do the following:
   a. In the **Export location** field, specify the name and location for the new *.pst* file.
   b. Select the **Apply filter** check box and enter keywords to export only those items that match specified criteria. To provide 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.

c. 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.



Specify the target path and optional settings:

Export location: C:\Users\Administrator.TECH\Desktop\Inbox.pst

☑ Apply filter: task

☑ Limit PST size to: 1 GB (additional PST files will be created as needed)

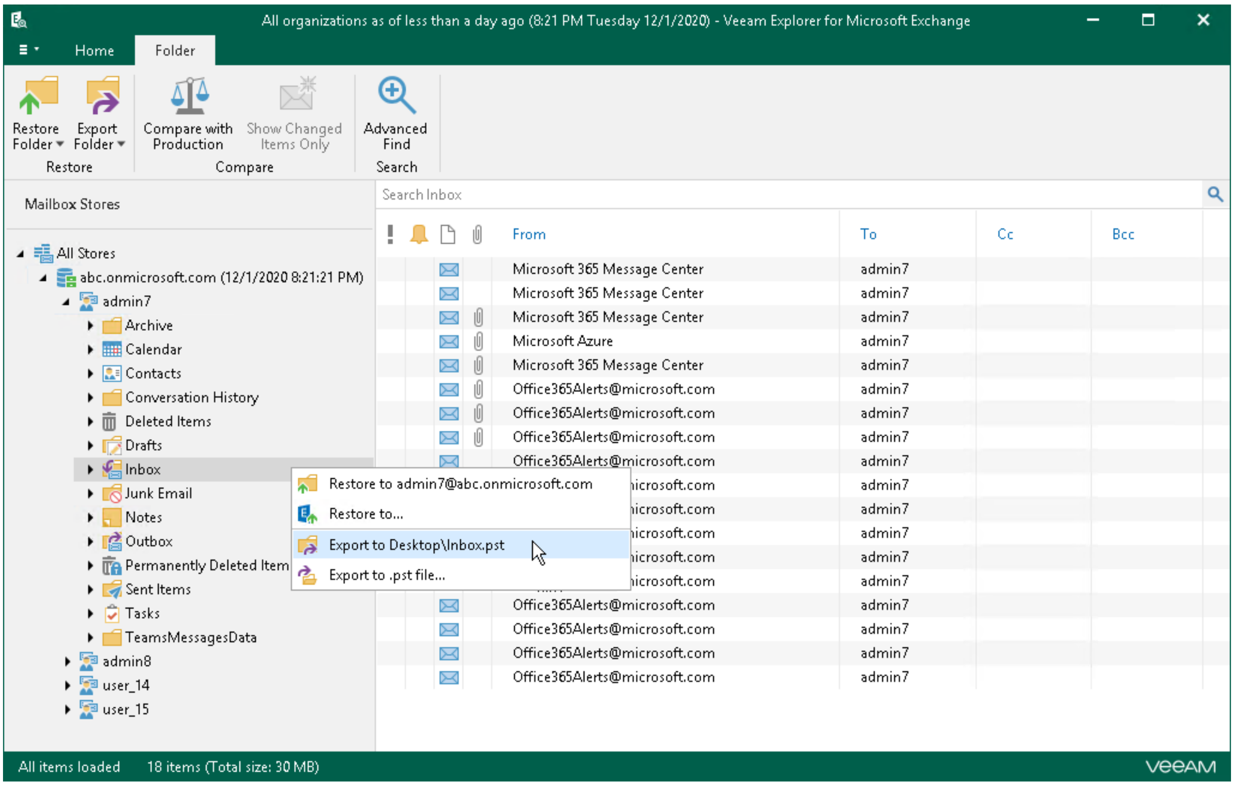
Using 1-Click Export

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.

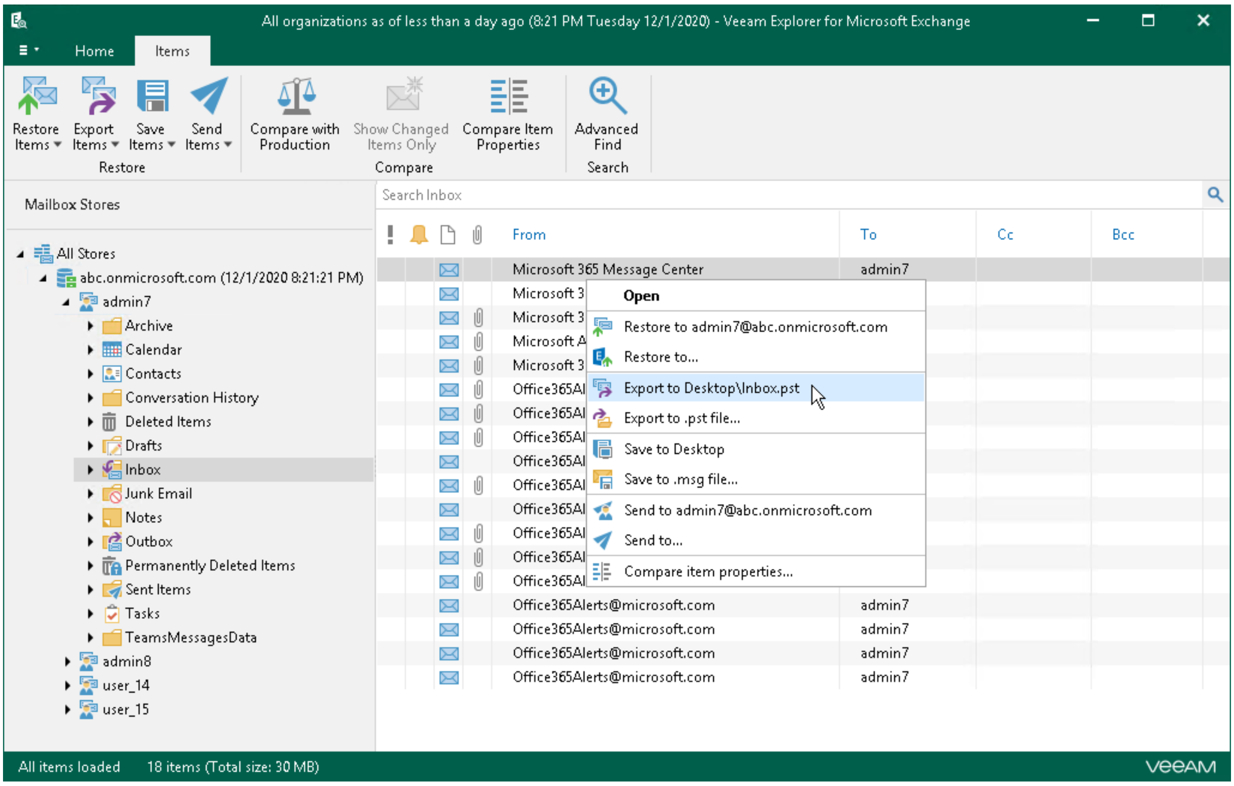
Depending on the object type you want to export, do the following:

- To export a folder, select it in the navigation pane and click **Export Folder** > **Export to <default_location>\<original_folder_name>.pst** on the **Folder** tab. Alternatively, in the navigation pane, right-click a folder and select **Export to <default_location>\<original_folder_name>.pst**.

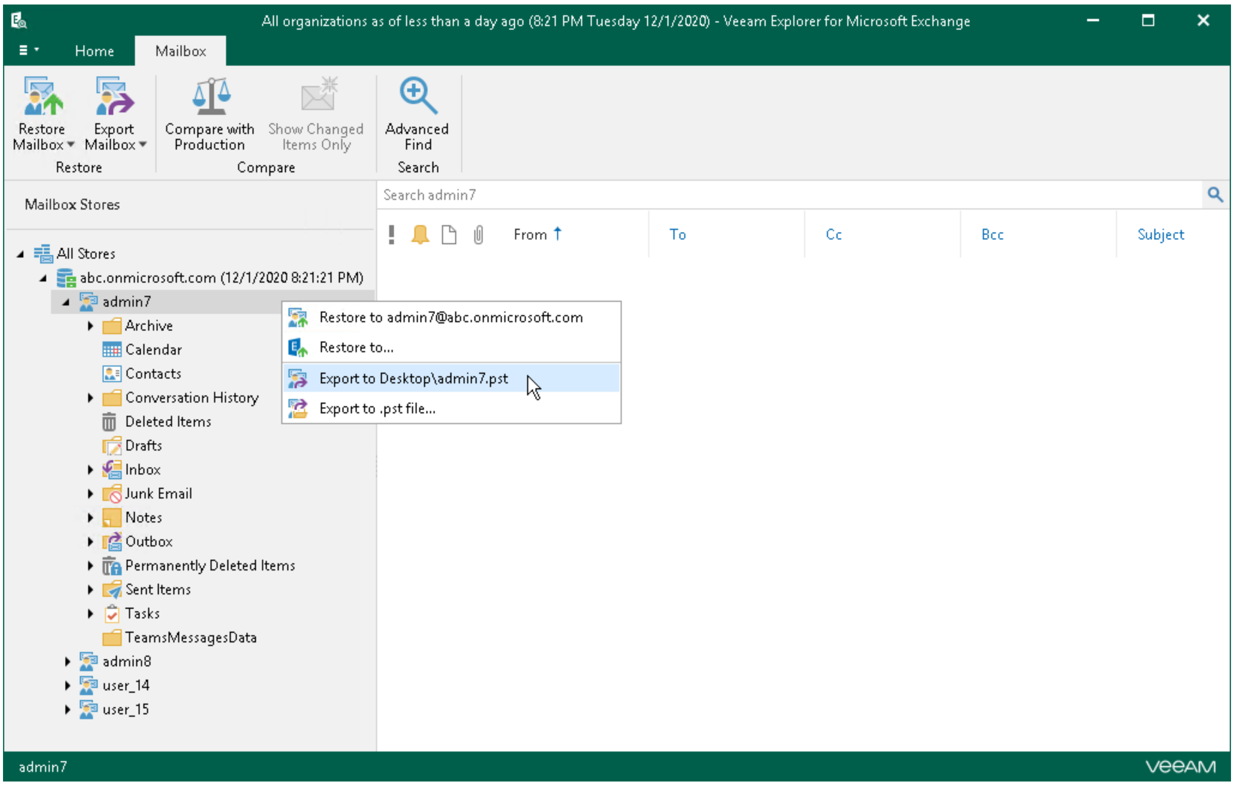


From	To	Cc	Bcc
Microsoft 365 Message Center	admin7		
Microsoft 365 Message Center	admin7		
Microsoft 365 Message Center	admin7		
Microsoft Azure	admin7		
Microsoft 365 Message Center	admin7		
Office365Alerts@microsoft.com	admin7		
Office365Alerts@microsoft.com	admin7		
Office365Alerts@microsoft.com	admin7		
Office365Alerts@microsoft.com	admin7		
icrosoft.com	admin7		
icrosoft.com	admin7		
icrosoft.com	admin7		
icrosoft.com	admin7		
icrosoft.com	admin7		
Office365Alerts@microsoft.com	admin7		
Office365Alerts@microsoft.com	admin7		
Office365Alerts@microsoft.com	admin7		
Office365Alerts@microsoft.com	admin7		

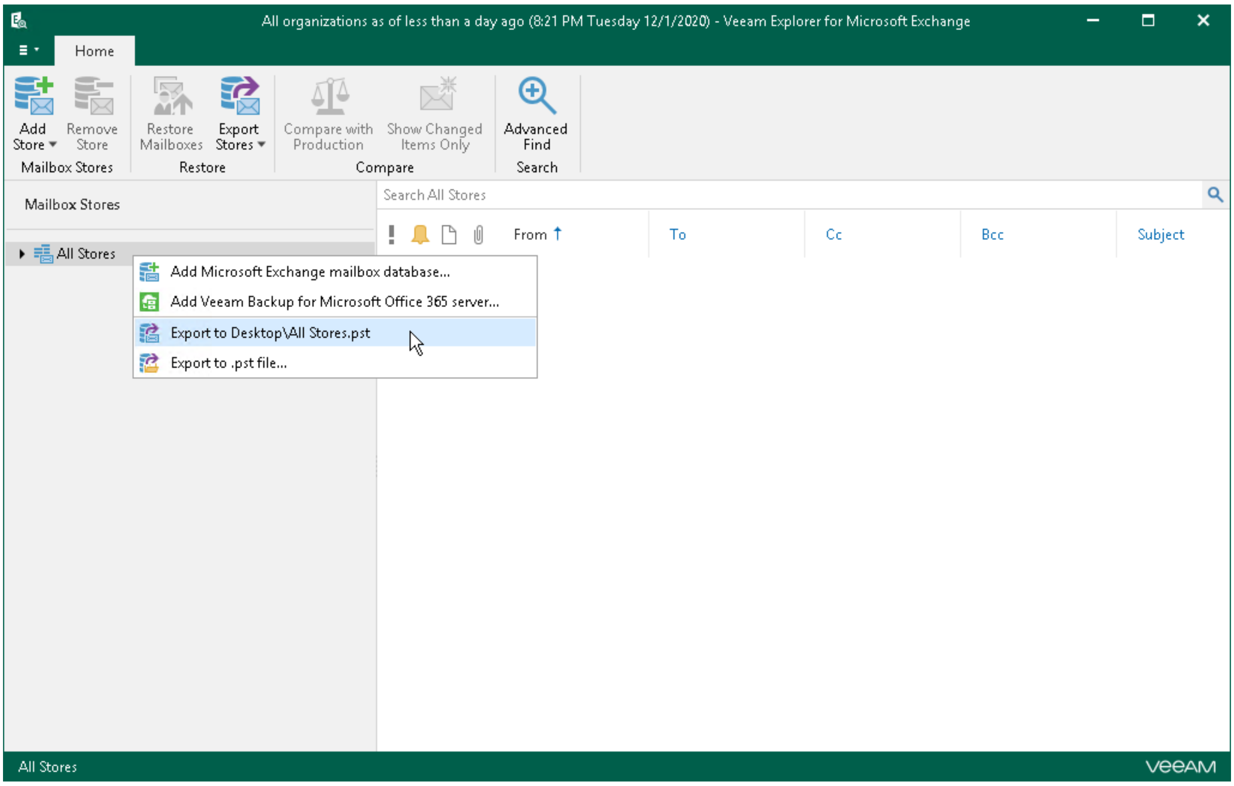
- To export an item, select it in the preview pane and click **Export Items** > **Export to <default_location>\<original_folder_name>.pst** on the **Items** tab. Alternatively, in the preview pane, right-click an item and select **Export to <default_location>\<original_folder_name>.pst**.



- To export a mailbox, select it in the navigation pane and click **Export Mailbox** > **Export to <default_location>\<original_mailbox_name>.pst** on the **Mailbox** tab. Alternatively, in the navigation pane, right-click a mailbox and select **Export to <default_location>\<original_folder_name>.pst**.



- 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.

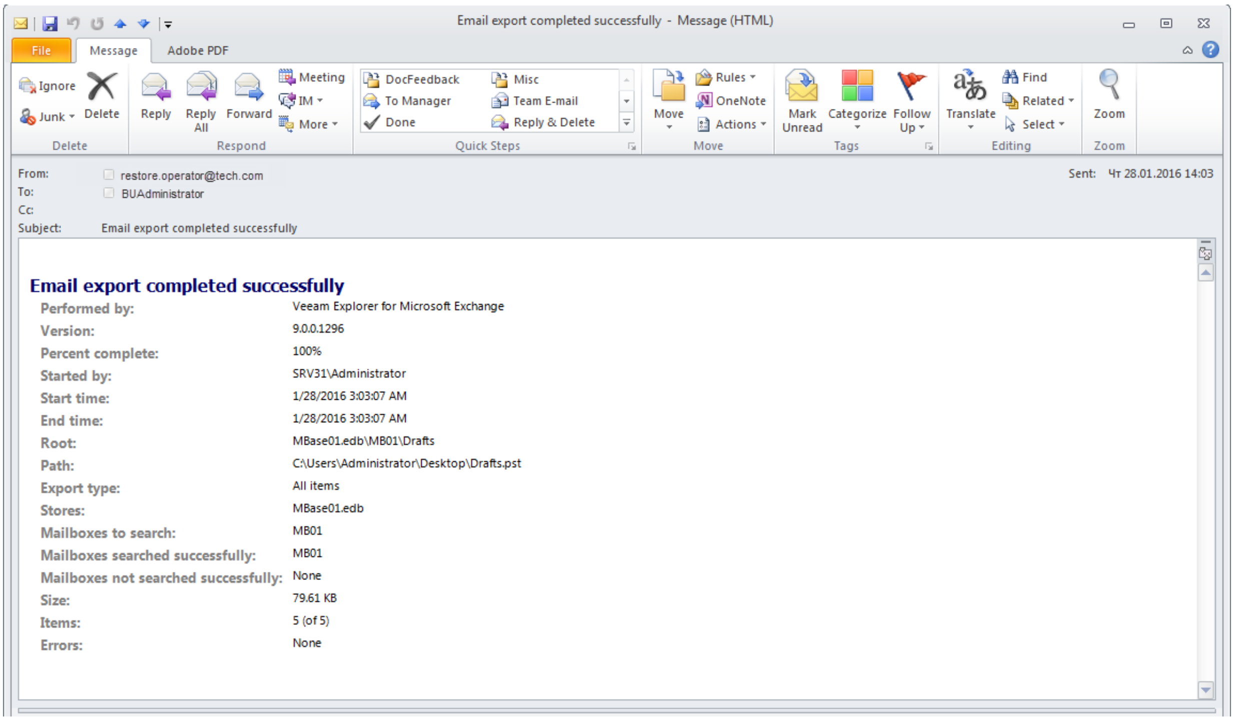
  - The recipient is always the user account provided in Veeam Backup & Replication notification settings when using only Veeam Backup & Replication settings.

  - 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 *.pst* 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.

Report field	Description
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.



From: restore.operator@tech.com
To: BUAdministrator
Cc:
Subject: Email export completed successfully
Sent: Чт 28.01.2016 14:03

Email export completed successfully

Performed by:	Veeam Explorer for Microsoft Exchange
Version:	9.0.0.1296
Percent complete:	100%
Started by:	SRV31\Administrator
Start time:	1/28/2016 3:03:07 AM
End time:	1/28/2016 3:03:07 AM
Root:	MBase01.edb\MB01\Drafts
Path:	C:\Users\Administrator\Desktop\Drafts.pst
Export type:	All items
Stores:	MBase01.edb
Mailboxes to search:	MB01
Mailboxes searched successfully:	MB01
Mailboxes not searched successfully:	None
Size:	79.61 KB
Items:	5 (of 5)
Errors:	None

Compare

This section explains how to compare data in a backup file with that of the production state.

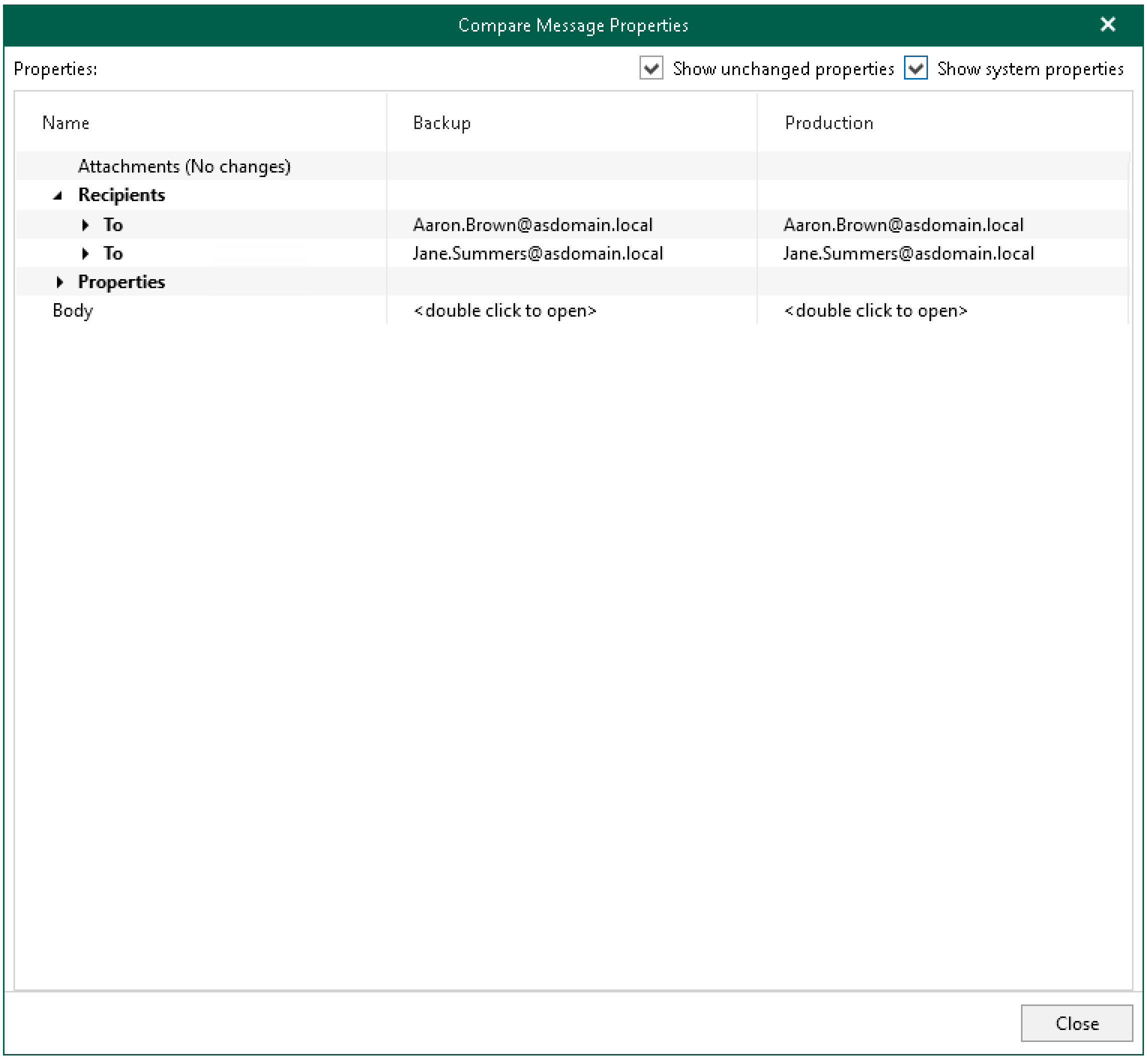
1. In the navigation pane, select an object and click **Compare with Production** on the toolbar.
2. Proceed to either Compare to Office 365 Organizations or Compare to On-Premises Microsoft Servers.
3. After the authorization process is complete, click **Show Changed Items Only** on the toolbar to view 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>

Compare to Office 365 Organizations

To compare data with your production Office 365 organizations, do the following:

1. Select an authentication method.
2. Log in 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:

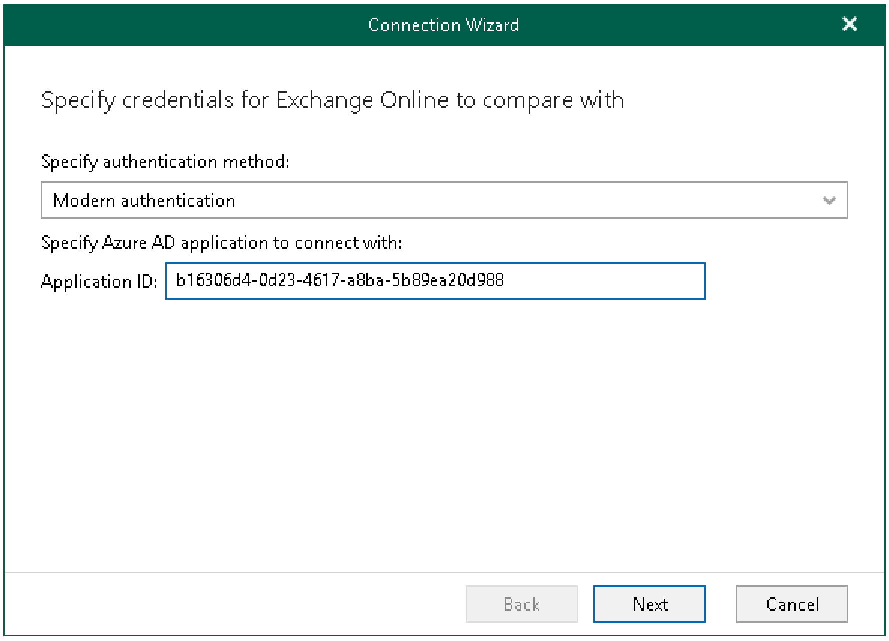
1. From the **Specify authentication method** drop-down list, select *Modern authentication*.

   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.



Specify credentials for Exchange Online to compare with

Specify authentication method:

Modern authentication

Specify Azure AD application to connect with:

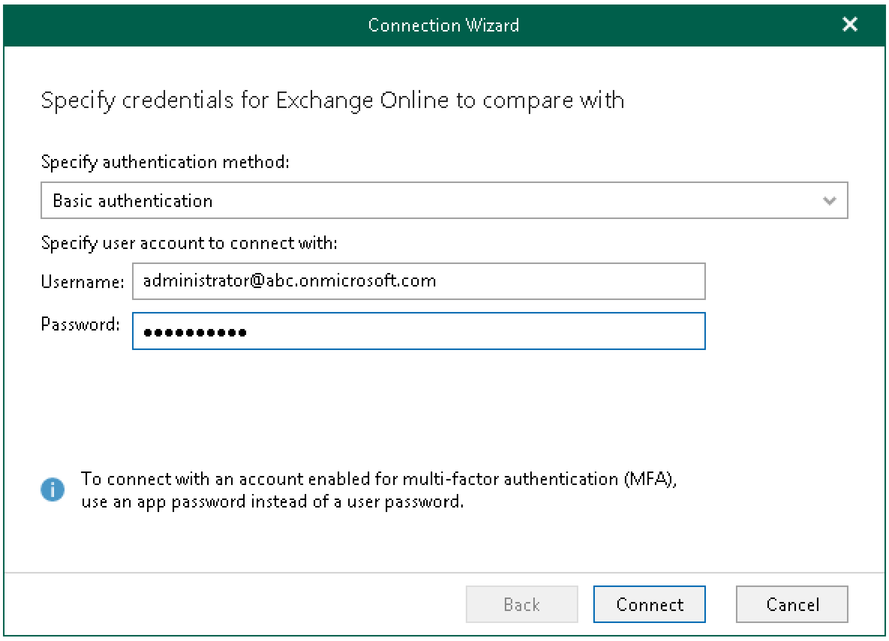
Application ID: b16306d4-0d23-4617-a8ba-5b89ea20d988

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.



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.

Step 2. Log In 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 365 organization, do the following:

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

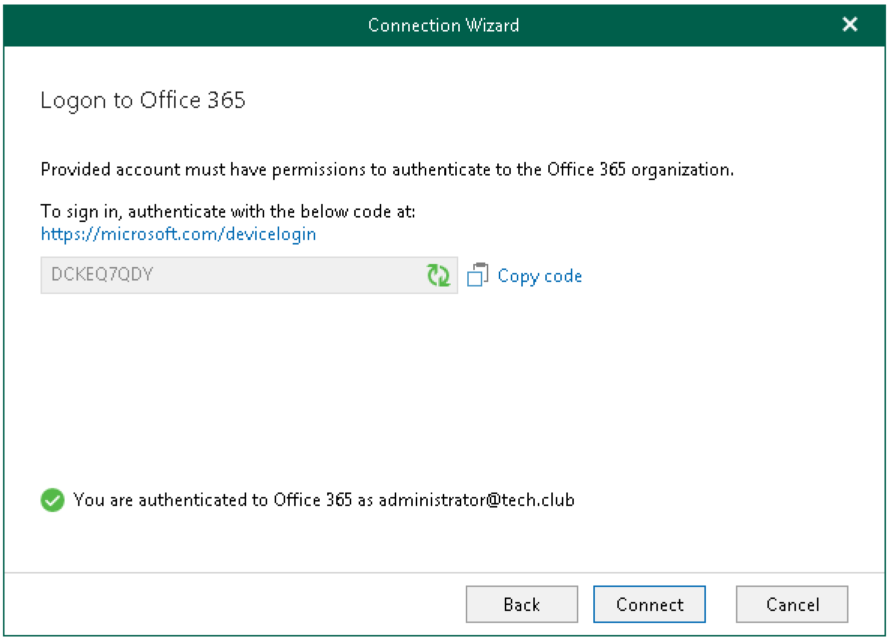
   Mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.

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

DCKEQ7QDY

Copy code

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

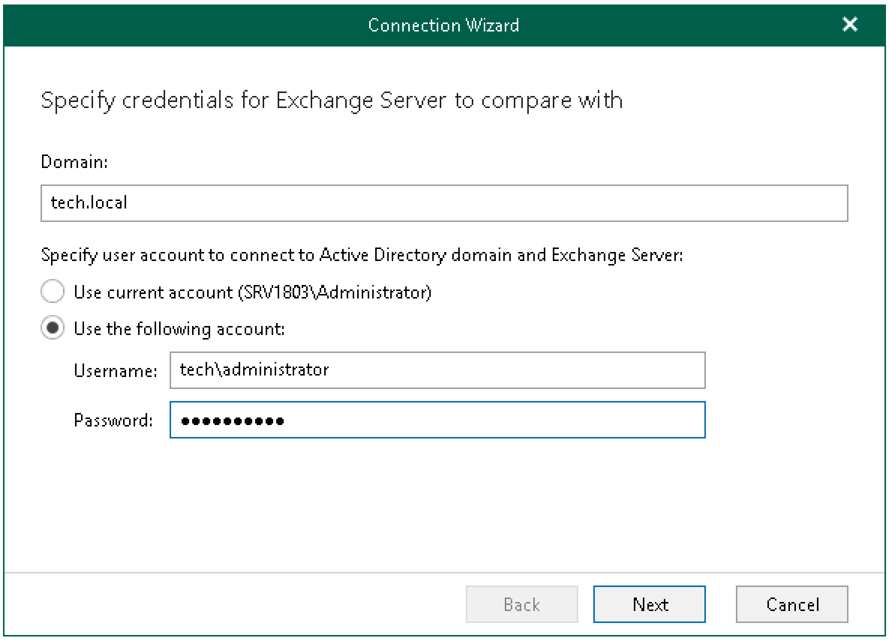
Compare to On-Premises Microsoft Servers

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.



Specify credentials for Exchange Server to compare with

Domain: tech.local

Specify user account to connect to Active Directory domain and Exchange Server:

○ Use current account (SRV1803\Administrator)

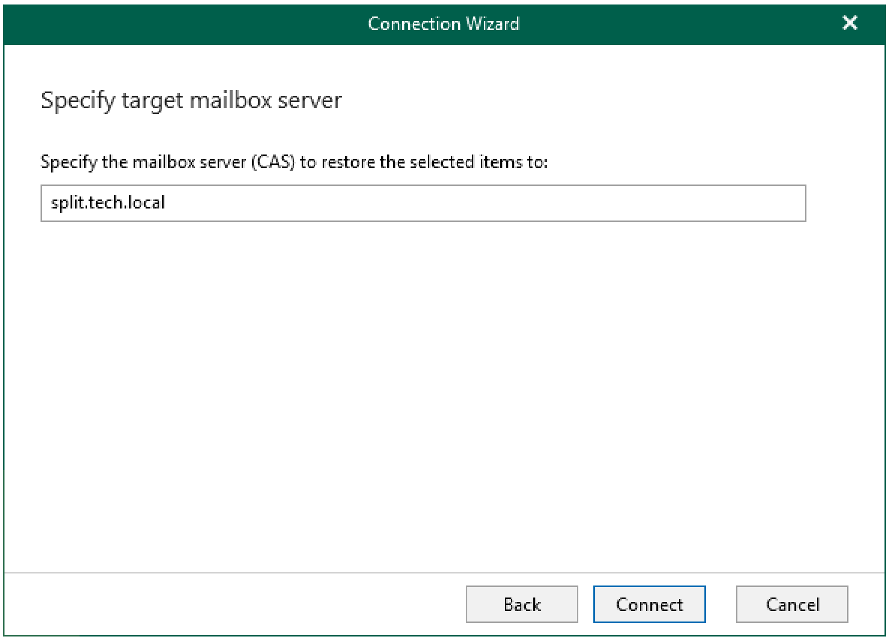
● Use the following account:

Username: tech\administrator

Password: ●●●●●●●●●●●

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**.



Specify the mailbox server (CAS) to restore the selected items to:

split.tech.local

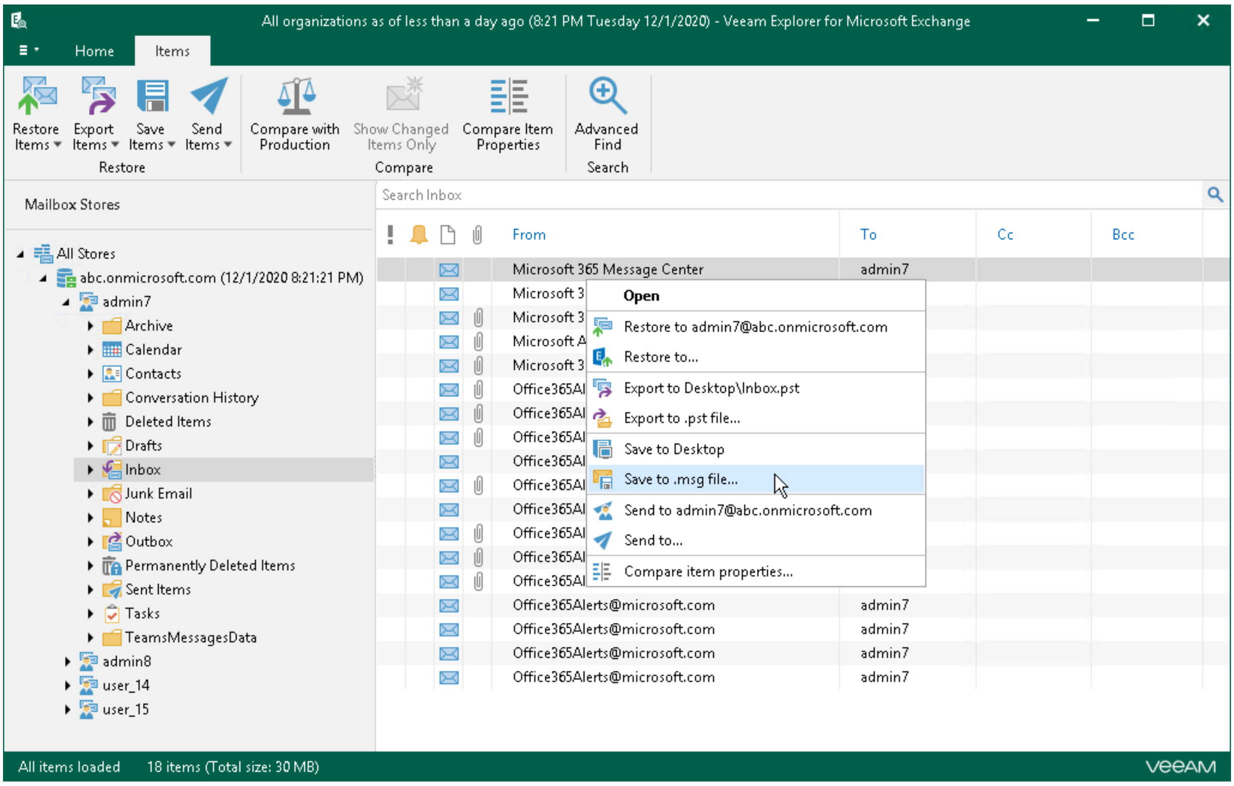
Saving Microsoft Exchange Items

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

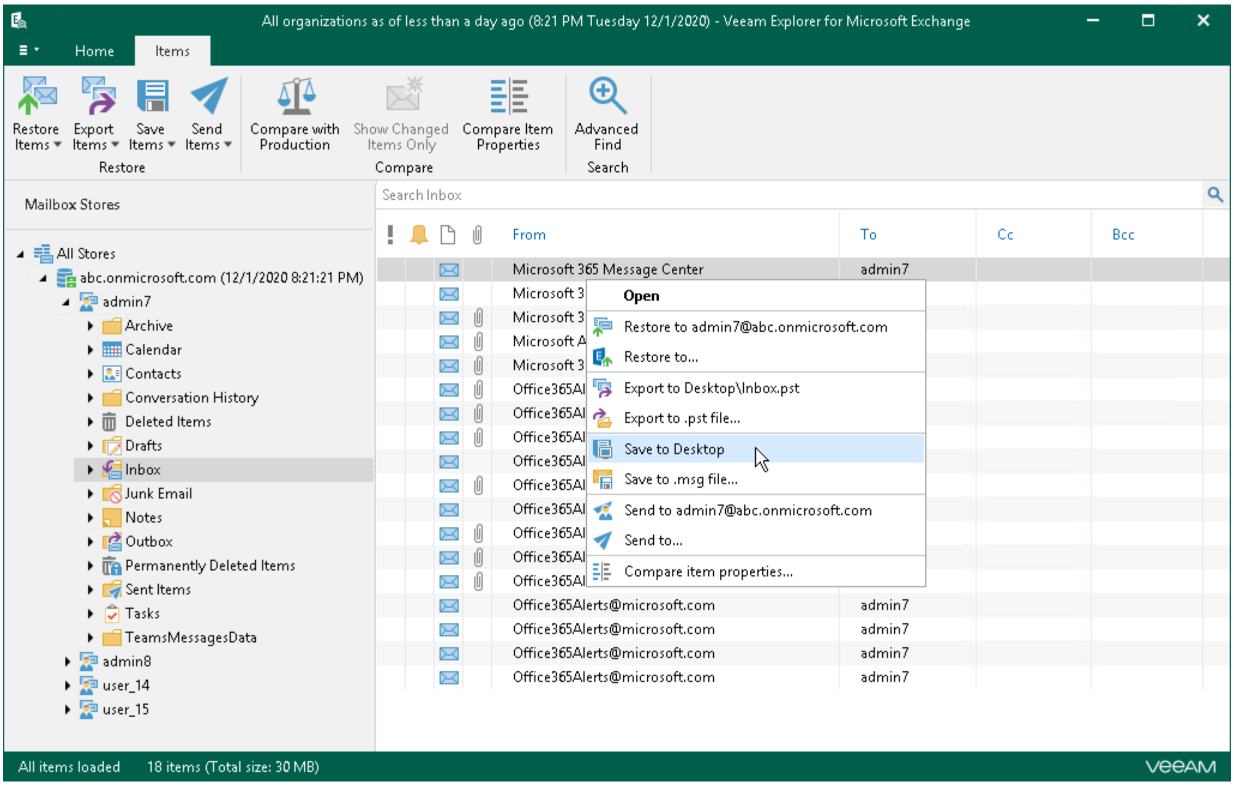
To save your Exchange data, do the following:

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

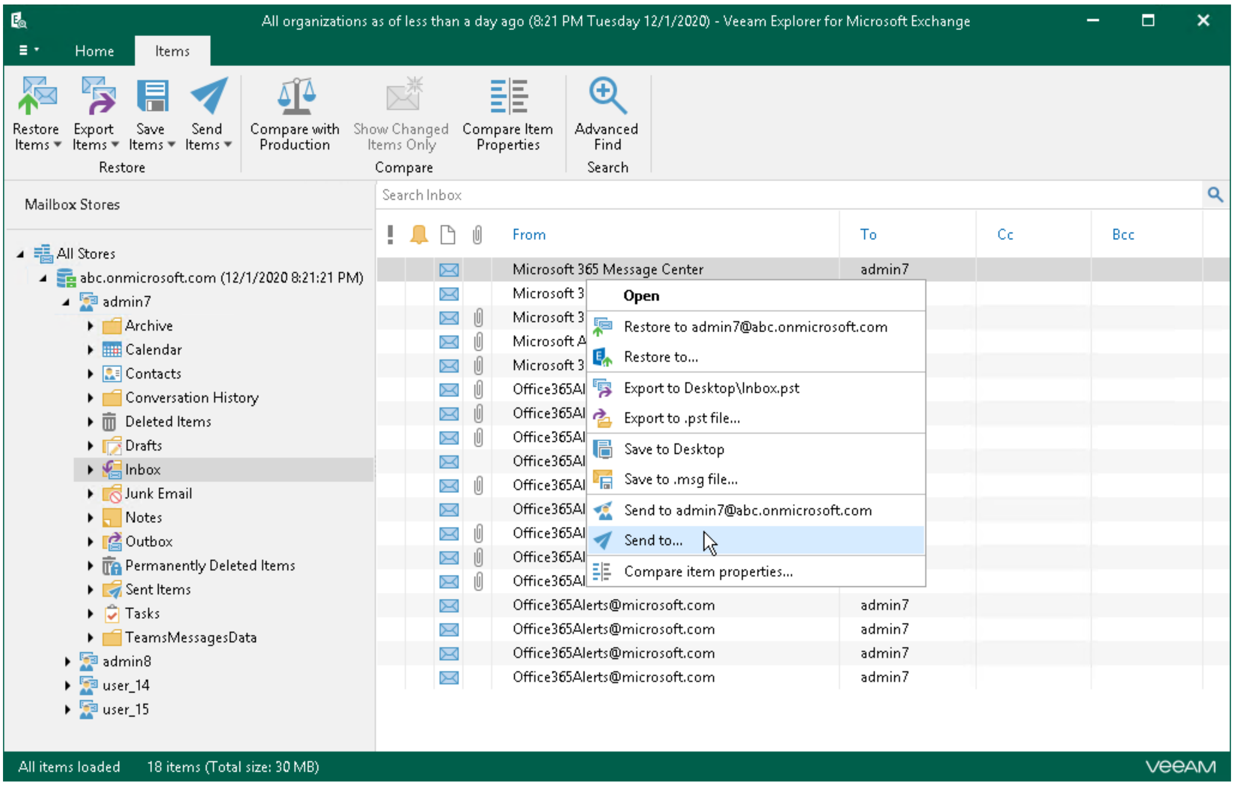
Veeam Explorer for Microsoft Exchange allows you to send Exchange items via email.

> **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:

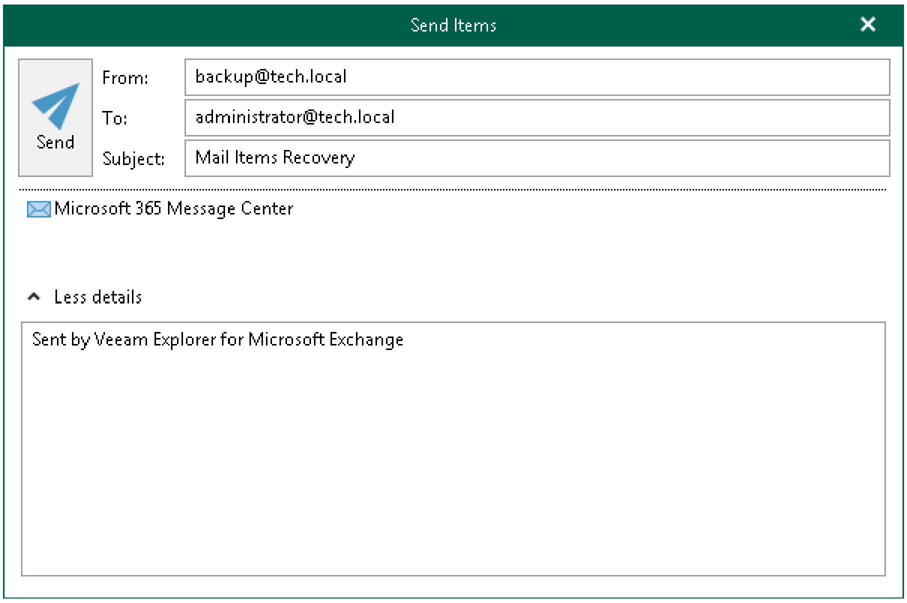
1. In the navigation pane, select a folder.
2. In the preview pane, select items to send.

   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**.



From: backup@tech.local

To: administrator@tech.local

Subject: Mail Items Recovery

Microsoft 365 Message Center

Sent by Veeam Explorer for Microsoft Exchange

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 to 3270	Used by iSCSI initiator to connect to the iSCSI target.

Required Permissions

The following table lists required permissions for data restore.

Operation	Required Roles and Permissions
Restore to on-premises Microsoft SharePoint	To restore data to on-premises SharePoint, make sure to configure user accounts as follows: • The account must be granted *Full Control* to connect to the target SharePoint server. • The account must be assigned either the *Site Administrator* or *System Account* role to restore user permissions. • If permissions of items being restored are inherited from the parent one, the account must be granted *Full Control*. • 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 *Contribute* and *Full Control*.
Restore to Microsoft Office 365	To restore data to SharePoint Online, the user account must have the *SharePoint Administrator* role. Consider the following: • For restore of personal SharePoint sites using the modern authentication method, make sure to select the **Allow users to run custom script on personal sites** option in the SharePoint admin center. For more information, see Microsoft Docs. • Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see Required Azure AD Application Settings. • For data restore using the modern authentication method, the account used to log in to Microsoft Office 365 must have the *Global Administrator* or *SharePoint Administrator* role assigned. • During restore, Veeam Backup for Microsoft Office 365 automatically assigns the *Site Collection Administrator* role to the user account.

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

Restore of 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.

Restore of 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.

Restore of 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.

Restore of 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.

Restore of 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:

1. 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.
2. 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):

1. 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*.
2. 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 disable these notifications, clear the **Show pop-up notifications on startup** 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.

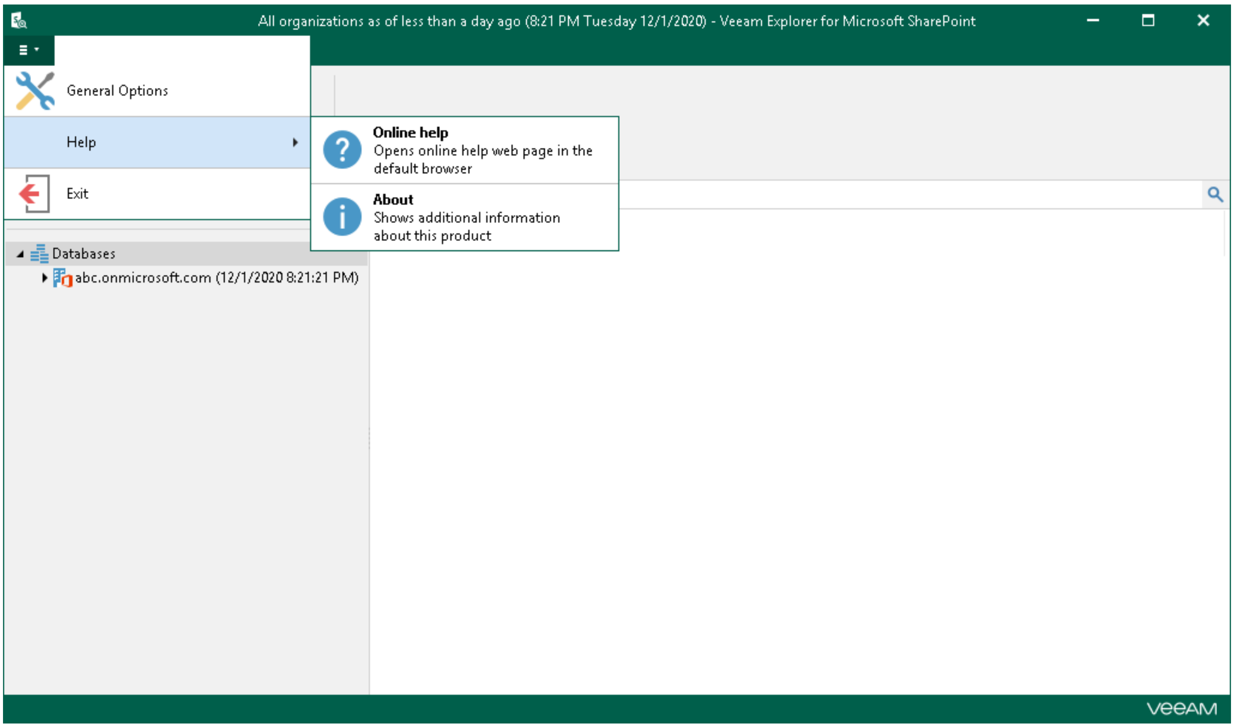
Understanding User Interface

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:

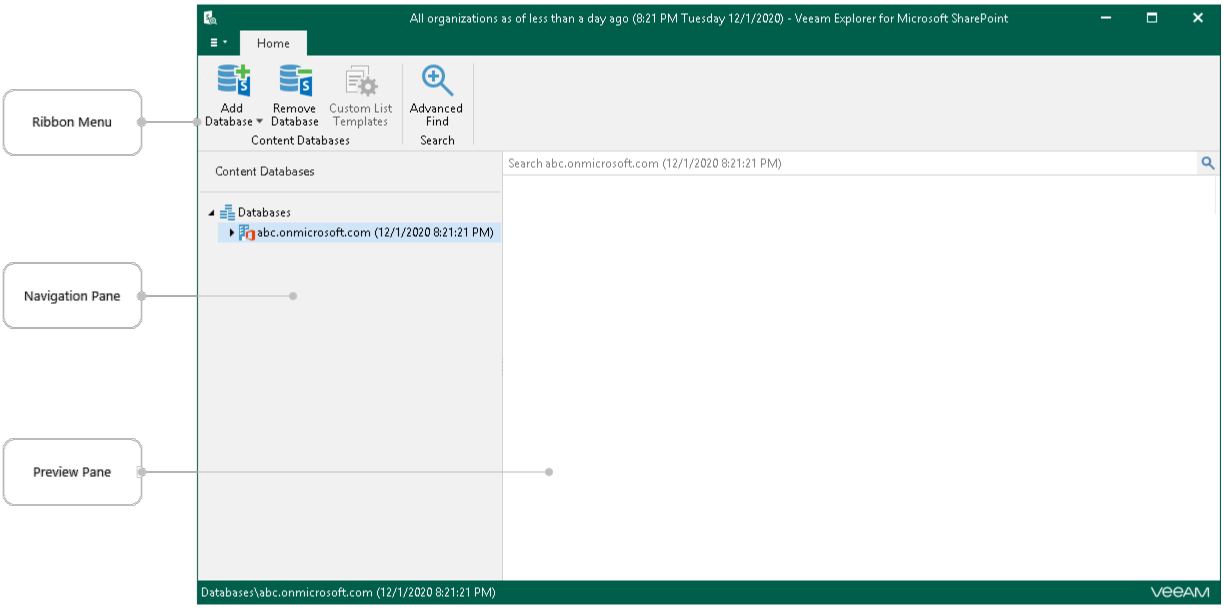
- **General Options**. Allows you to configure program options.
- **Help**.
  - **Online help**. Opens the online web help page.
  - **About**. Shows information about the product.
- **Exit**. Closes the program.


All organizations as of less than a day ago (8:21 PM Tuesday 12/1/2020) - Veeam Explorer for Microsoft SharePoint
General Options
Help
Exit
Online help
Opens online help web page in the default browser
About
Shows additional information about this product
Databases
abc.onmicrosoft.com (12/1/2020 8:21:21 PM)
veeAM

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.


Ribbon Menu
Navigation Pane
Preview Pane
All organizations as of less than a day ago (8:21 PM Tuesday 12/1/2020) - Veeam Explorer for Microsoft SharePoint
Home
Add Database
Remove Database
Custom List Templates
Content Databases
Advanced Find
Search
Content Databases
Search abc.onmicrosoft.com (12/1/2020 8:21:21 PM)
Databases
abc.onmicrosoft.com (12/1/2020 8:21:21 PM)
Databases\abc.onmicrosoft.com (12/1/2020 8:21:21 PM)
veeam

Browsing, Searching and Viewing Items

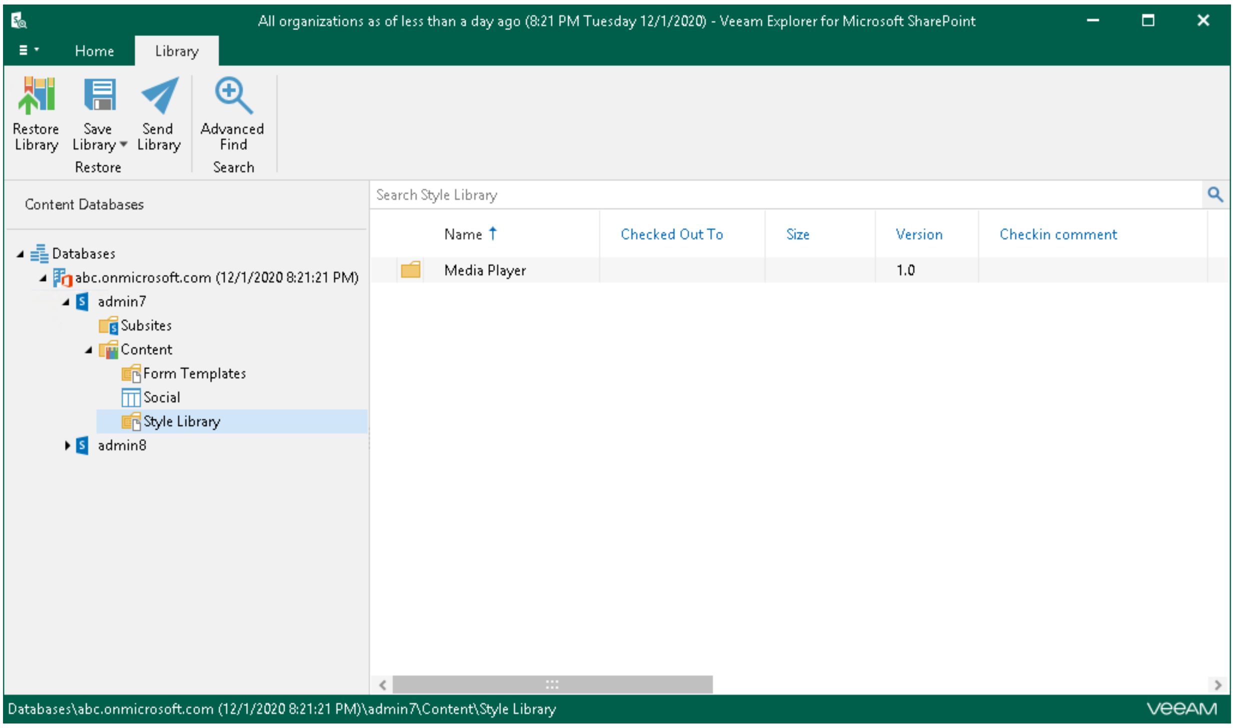
Continue with this section to learn more about:

- 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.



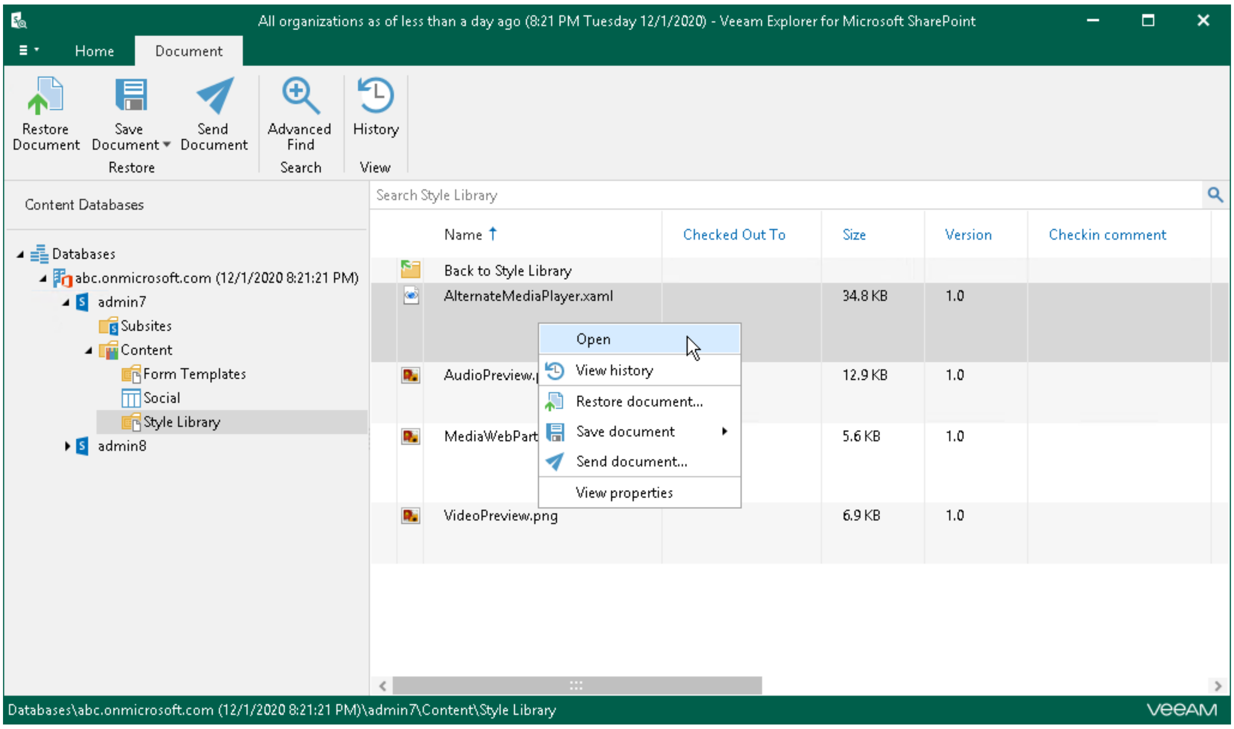
Name	Checked Out To	Size	Version	Checkin comment
Media Player			1.0	

Databases\abc.onmicrosoft.com (12/1/2020 8:21:21 PM)\admin7\Content\Style Library

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**.



Name	Checked Out To	Size	Version	Checkin comment
Back to Style Library				
AlternateMediaPlayer.xaml		34.8 KB	1.0	
AudioPreview.[…]		12.9 KB	1.0	
MediaWebPart[…]		5.6 KB	1.0	
VideoPreview.png		6.9 KB	1.0	

Searching

The search mechanism allows you to find items matching specified search criteria.

To search for required items, do the following:

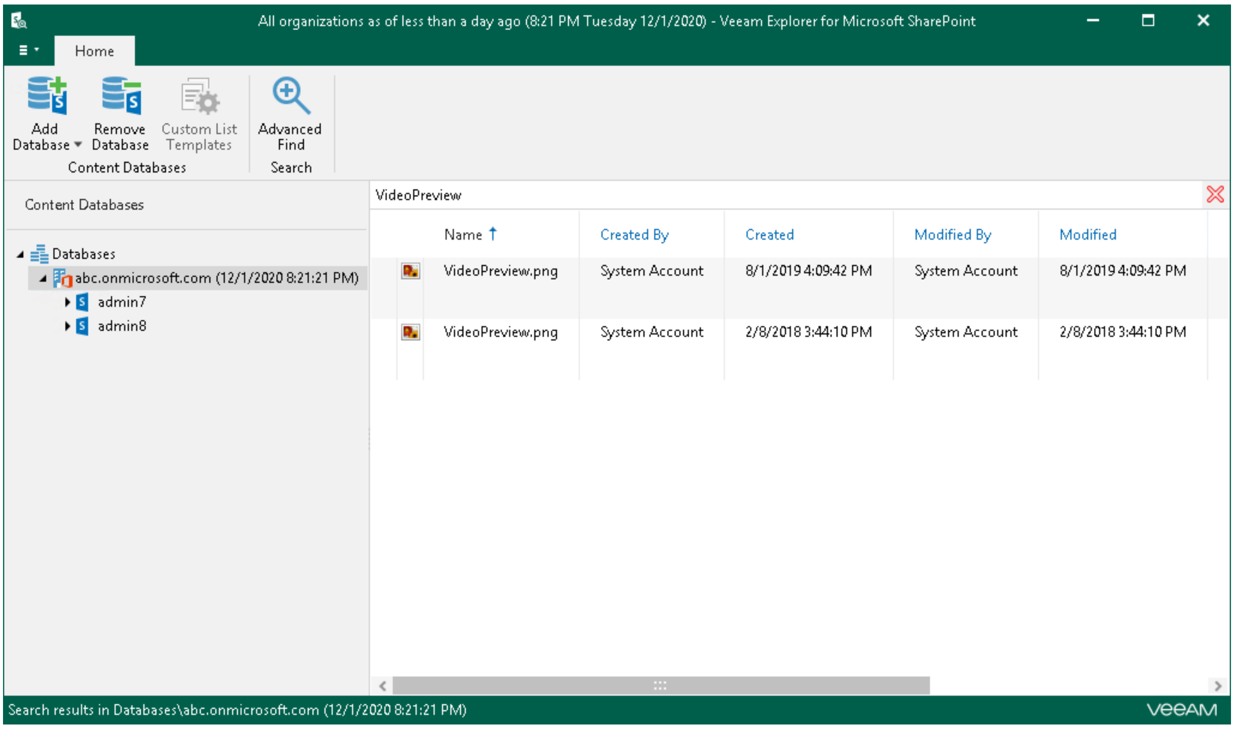
1. In the navigation pane. select an object in which you want to find your data.
2. Enter a search query to the search field at the top of the preview pane.

> **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.



All organizations as of less than a day ago (8:21 PM Tuesday 12/1/2020) - Veeam Explorer for Microsoft SharePoint
Home
Add Database
Remove Database
Custom List Templates
Content Databases
Advanced Find
Search
Content Databases
Databases
abc.onmicrosoft.com (12/1/2020 8:21:21 PM)
admin7
admin8
VideoPreview
Search results in Databases\abc.onmicrosoft.com (12/1/2020 8:21:21 PM)
veeam

Name	Created By	Created	Modified By	Modified
VideoPreview.png	System Account	8/1/2019 4:09:42 PM	System Account	8/1/2019 4:09:42 PM
VideoPreview.png	System Account	2/8/2018 3:44:10 PM	System Account	2/8/2018 3:44:10 PM

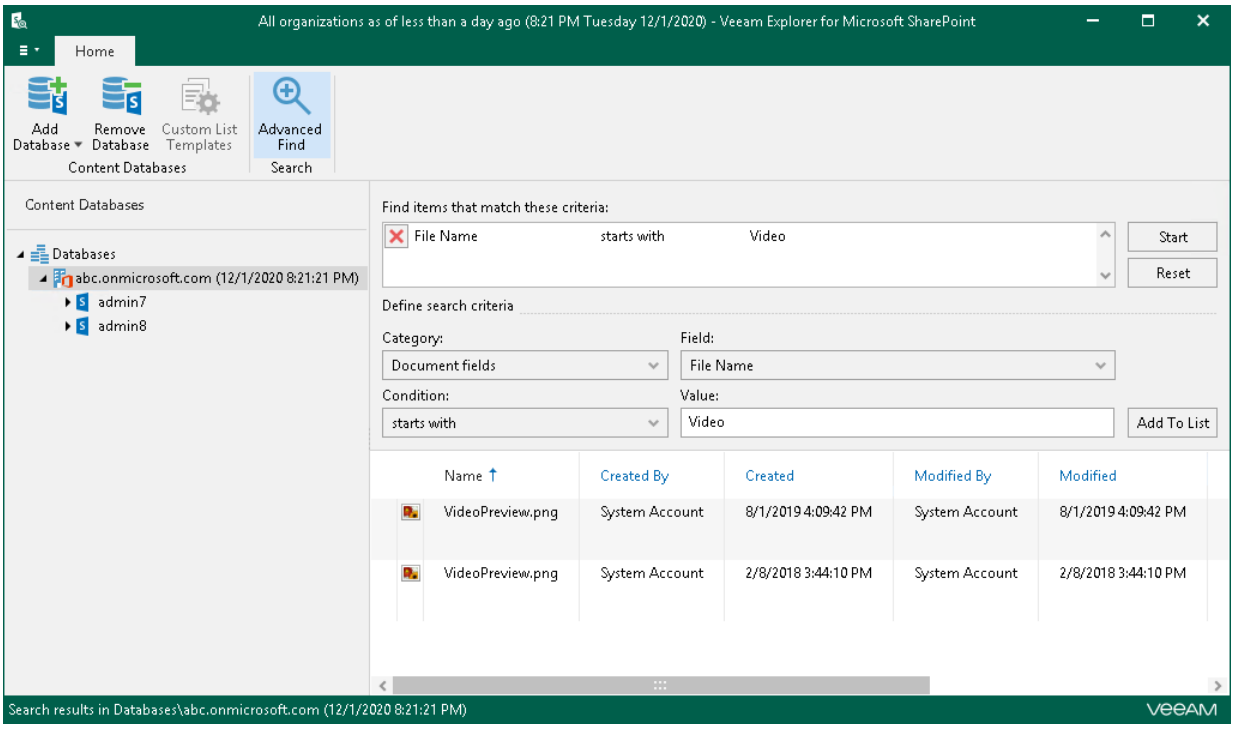
Using Advanced Find Capabilities

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 **Add to List**, then click **Start**.

To remove a filter, click the cross mark next to it. To remove all configured filters, click **Reset**.


All organizations as of less than a day ago (8:21 PM Tuesday 12/1/2020) - Veeam Explorer for Microsoft SharePoint
Home
Add Database
Remove Database
Custom List Templates
Content Databases
Advanced Find
Search
Content Databases
Databases
abc.onmicrosoft.com (12/1/2020 8:21:21 PM)
admin7
admin8
Start
Reset
Add To List
Search results in Databases\abc.onmicrosoft.com (12/1/2020 8:21:21 PM)
veeam

Find items that match these criteria:

☒ File Name starts with Video

Define search criteria

Category: Document fields

Field: File Name

Condition: starts with

Value: Video

Name ↑	Created By	Created	Modified By	Modified
VideoPreview.png	System Account	8/1/2019 4:09:42 PM	System Account	8/1/2019 4:09:42 PM
VideoPreview.png	System Account	2/8/2018 3:44:10 PM	System Account	2/8/2018 3:44:10 PM

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 an SQL server belongs to an untrusted domain, connection will not be possible.
- If an SQL server belongs to a trusted domain, only the *SQL Server authentication* method is available.
- If both an 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.

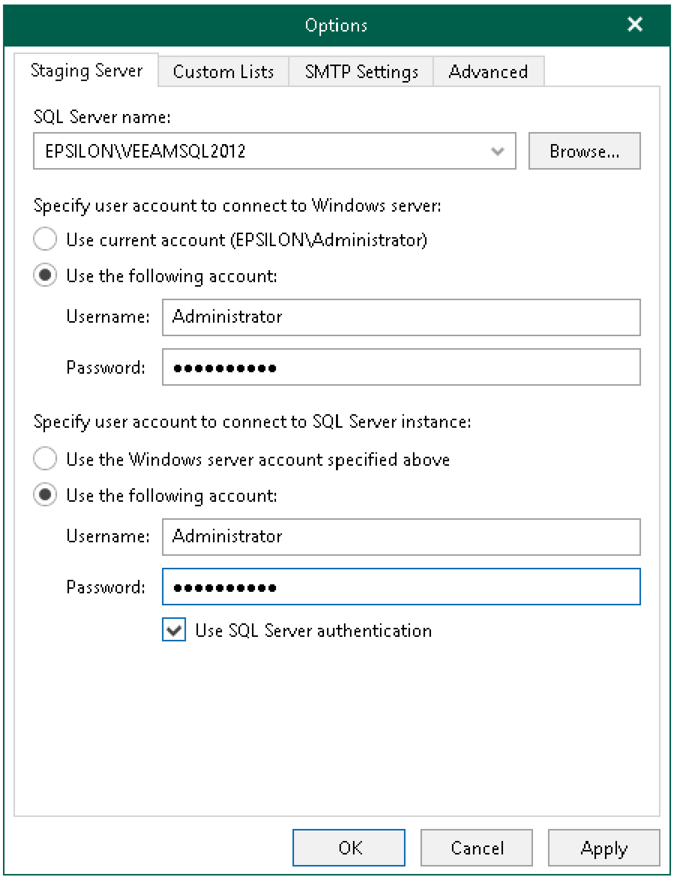
  b. Open its properties and select the **Delegation** tab. Select **Trust this computer for delegation to specified services only** and **Use any authentication protocol** options for the **cifs** service on a computer with Veeam Explorer.

  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 an 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 an SQL server instance.



SQL Server name: EPSILON\VEEAMSQL2012

Specify user account to connect to Windows server:

○ Use current account (EPSILON\Administrator)

● Use the following account:

Username: Administrator

Password: ●●●●●●●●●●

Specify user account to connect to SQL Server instance:

○ Use the Windows server account specified above

● Use the following account:

Username: Administrator

Password: ●●●●●●●●●●

☑ Use SQL Server authentication

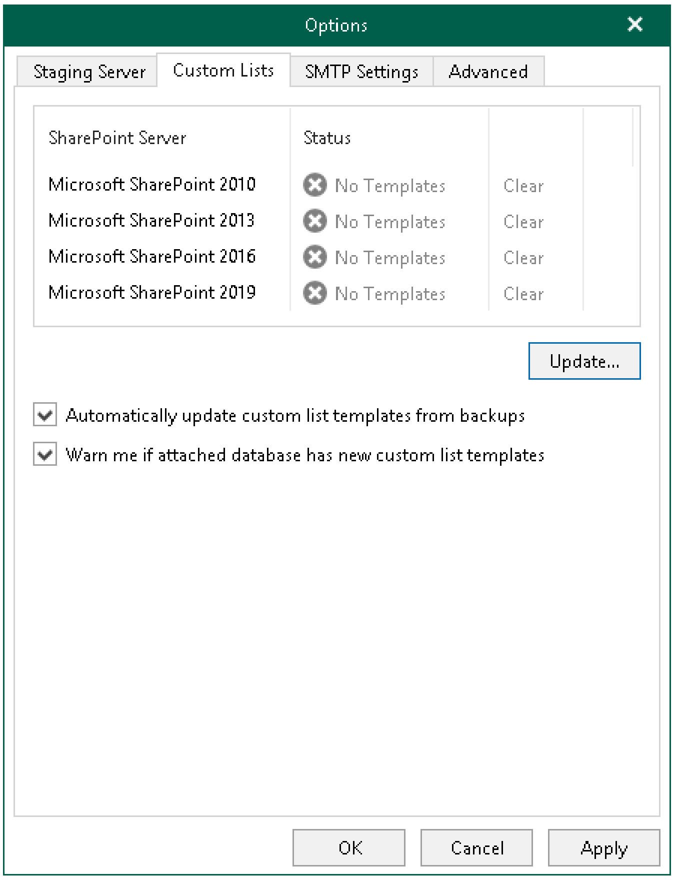
Custom Lists

Veeam Explorer for Microsoft SharePoint supports obtaining custom list templates from backups created in Veeam Backup & Replication 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.

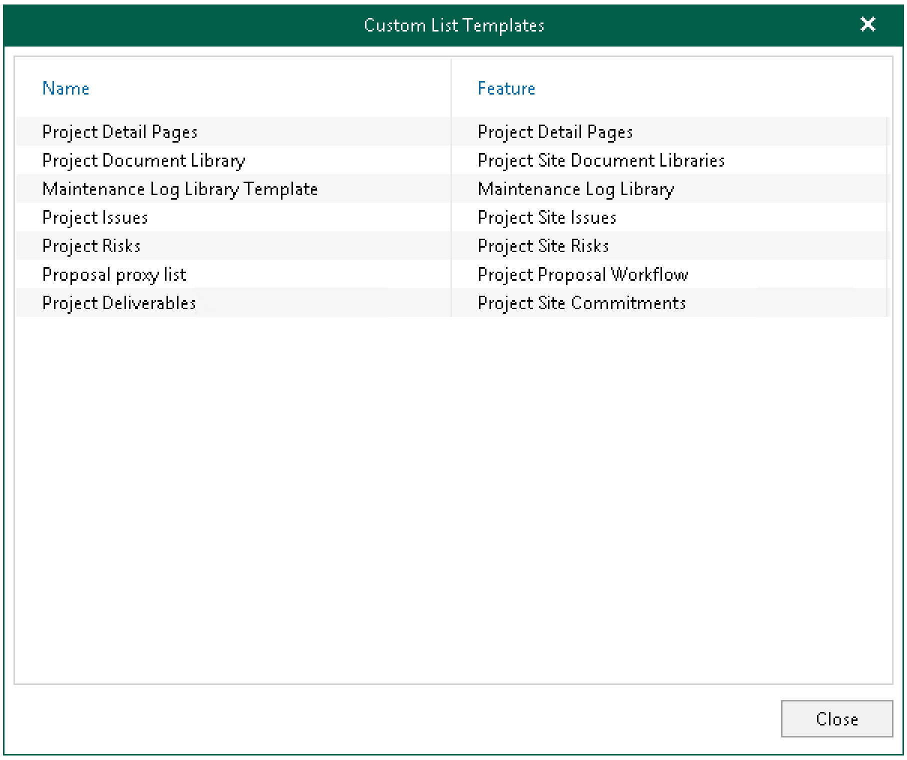


SharePoint Server	Status	
Microsoft SharePoint 2010	☒ No Templates	Clear
Microsoft SharePoint 2013	☒ No Templates	Clear
Microsoft SharePoint 2016	☒ No Templates	Clear
Microsoft SharePoint 2019	☒ No Templates	Clear

☑ Automatically update custom list templates from backups

☑ Warn me if attached database has new custom list templates

See the figure below showing you what custom list templates are available.



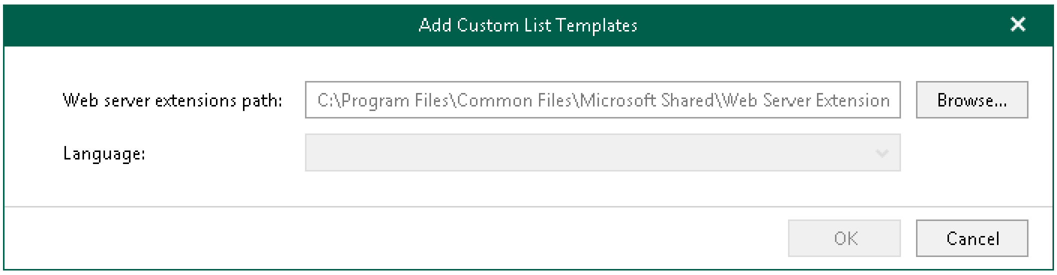
Name	Feature
Project Detail Pages	Project Detail Pages
Project Document Library	Project Site Document Libraries
Maintenance Log Library Template	Maintenance Log Library
Project Issues	Project Site Issues
Project Risks	Project Site Risks
Proposal proxy list	Project Proposal Workflow
Project Deliverables	Project Site Commitments

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.



Web server extensions path: C:\Program Files\Common Files\Microsoft Shared\Web Server Extension

Language:

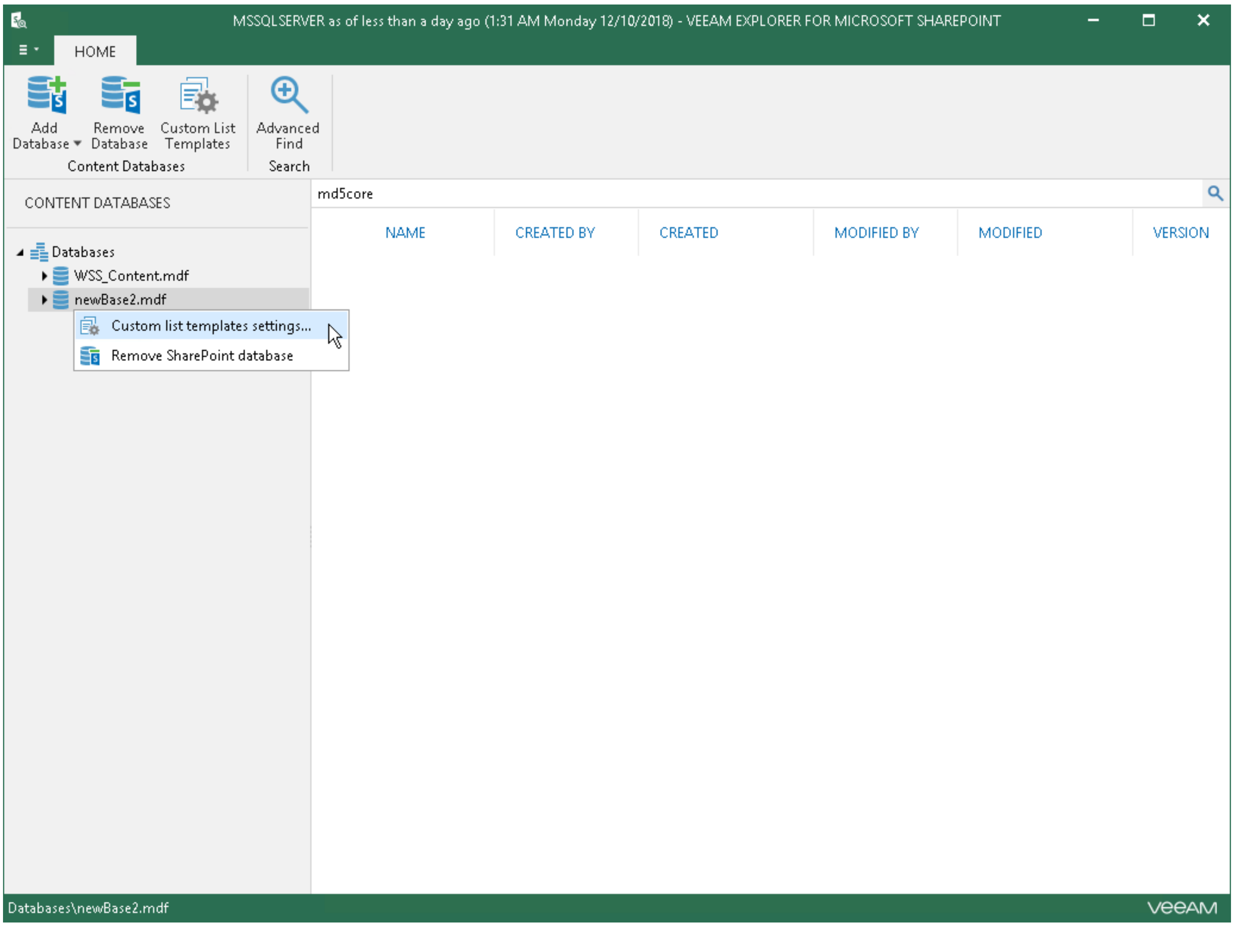
Importing Templates Using Ribbon Menu

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**.

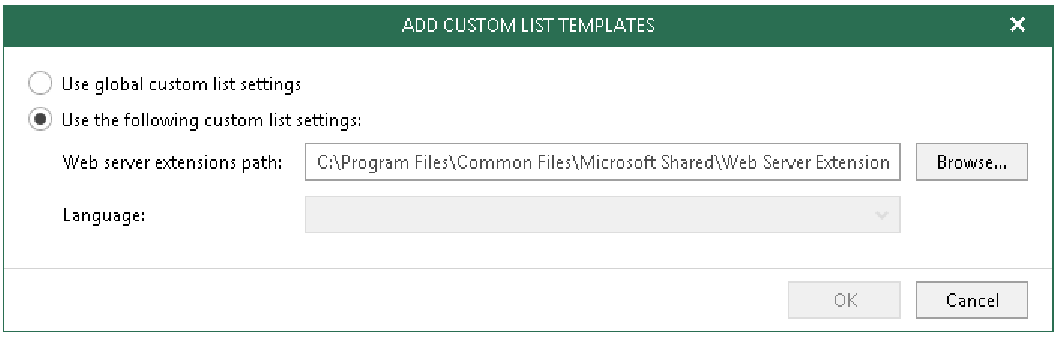


3. Choose how you want your templates to be applied:

   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.



ADD CUSTOM LIST TEMPLATES

○ Use global custom list settings

● Use the following custom list settings:

Web server extensions path: C:\Program Files\Common Files\Microsoft Shared\Web Server Extension

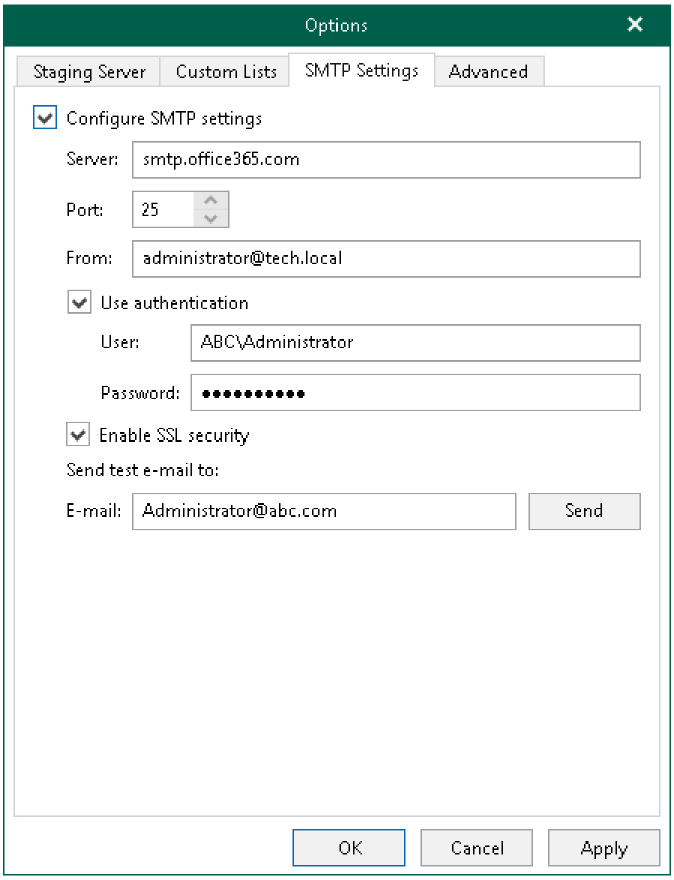
Language:

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**.



☑ Configure SMTP settings

Server: smtp.office365.com

Port: 25

From: administrator@tech.local

☑ Use authentication

User: ABC\Administrator

Password: ●●●●●●●●●●●

☑ Enable SSL security

Send test e-mail to:

E-mail: Administrator@abc.com

Advanced Settings

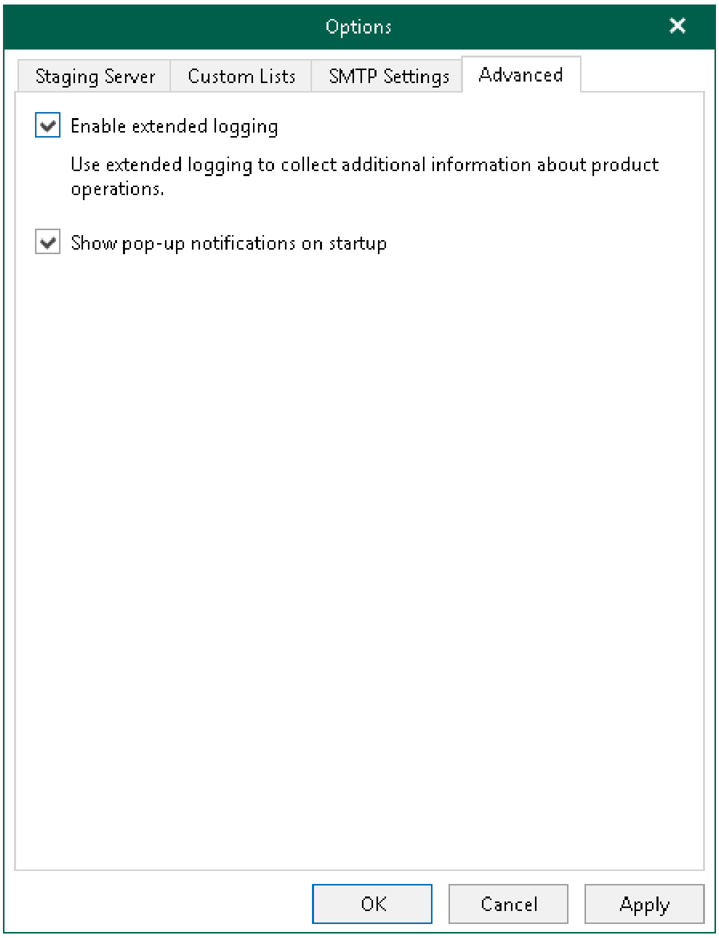
This section explains how to configure advanced settings of the application.

To configure advanced settings, do the following:

1. Go to the main menu and click **General Options**.
2. Click the **Advanced** tab.
3. 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.
4. By default, Veeam Explorer for Microsoft SharePoint displays notifications when loading backups from object storage repositories. If you want to disable these notifications, clear the **Show pop-up notifications on startup** check box.

   Applicable to backups created in Veeam Backup for Microsoft Office 365.



☑ Enable extended logging

Use extended logging to collect additional information about product operations.

☑ Show pop-up notifications on startup

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

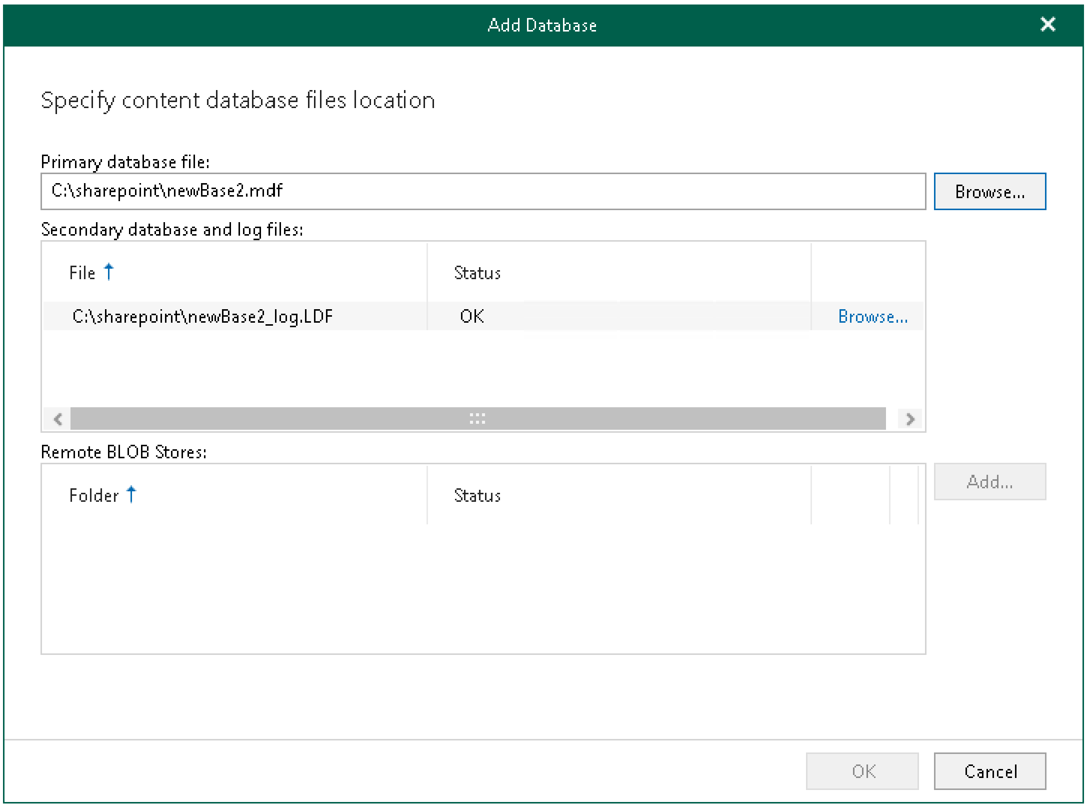
Continue with this section to learn more about the addition of Microsoft SharePoint databases to the application scope manually.

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 database** on the toolbar or right-click the root **Databases** 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

Secondary database and log files:

File	Status	
C:\sharepoint\newBase2_log.LDF	OK	Browse...

Remote BLOB Stores:

Folder	Status

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 database** or right-click the root **Databases** node and select **Veeam Backup for Microsoft Office 365 database**.
2. Specify the database file location and log directory.
3. Click **Open**.

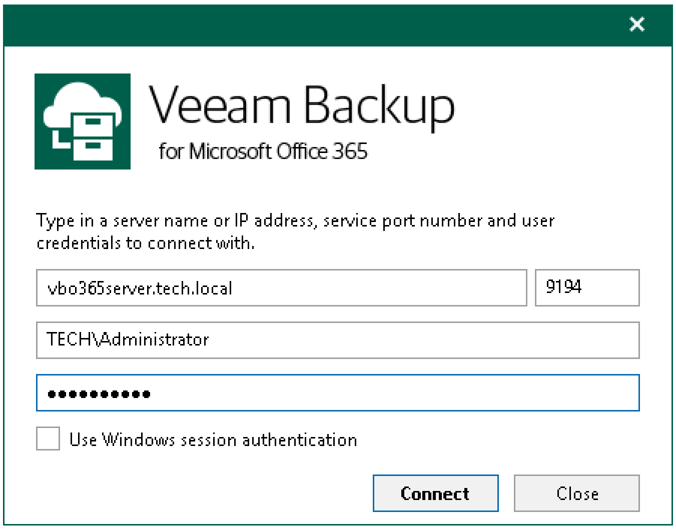
> **NOTE:**
> Make sure you have disabled the **Veeam Backup Proxy for Microsoft Office 365** service when adding local databases. You can stop this service by using the `services.msc` console. If you try to add a database having this service still in progress, you will receive an error message and will 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**.



Type in a server name or IP address, service port number and user credentials to connect with.

vbo365server.tech.local 9194

TECH\Administrator

●●●●●●●●●●●

□ Use Windows session authentication

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.

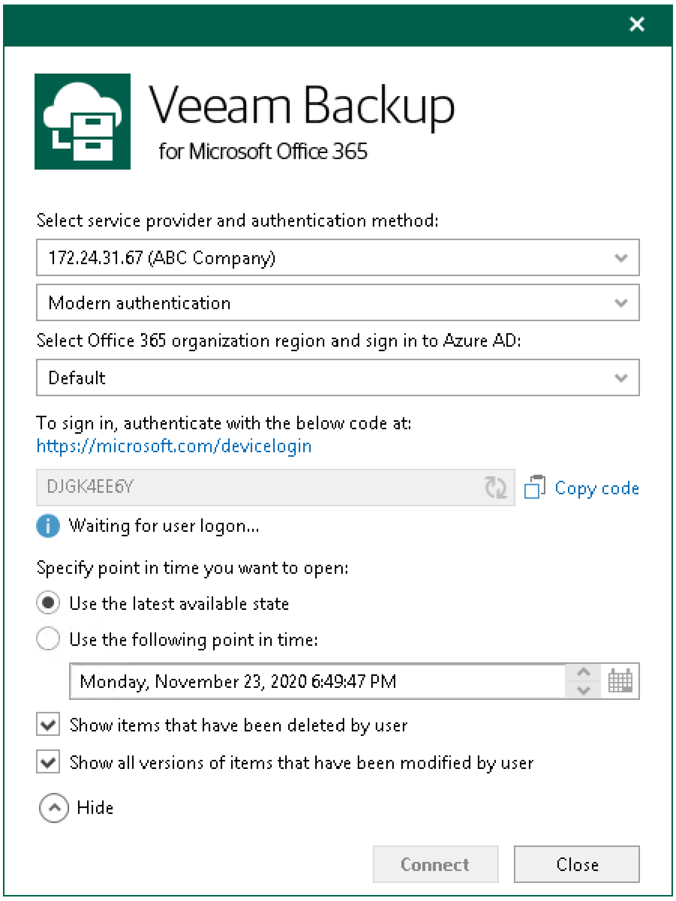
   For *Basic authentication*, you must enter a user name and password to connect to the service provider server.
6. Select a point-in-time state as of which you want to load Office 365 backups.

   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**.



Select service provider and authentication method:

172.24.31.67 (ABC Company)

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

DJGK4EE6Y

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:

Monday, November 23, 2020 6:49:47 PM

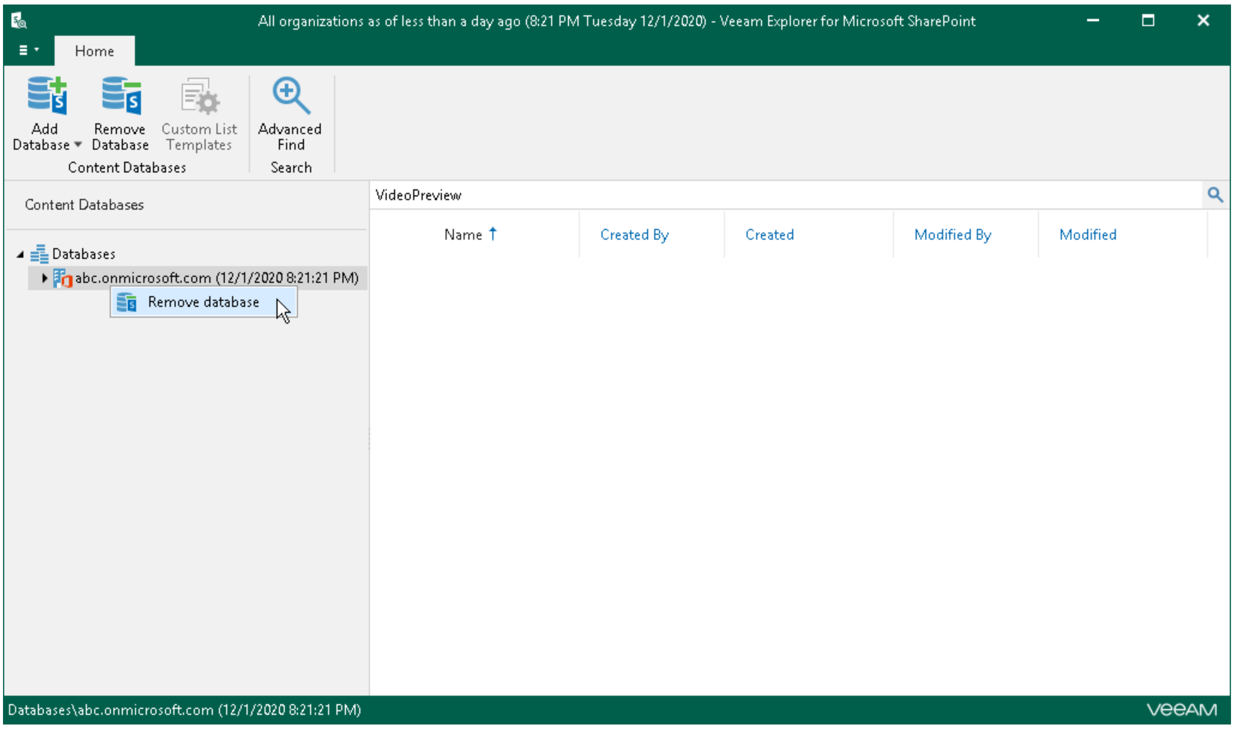
☑ Show items that have been deleted by user

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

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 database**.


All organizations as of less than a day ago (8:21 PM Tuesday 12/1/2020) - Veeam Explorer for Microsoft SharePoint
Home
Add Database
Remove Database
Custom List Templates
Content Databases
Advanced Find
Search
Content Databases
Databases
abc.onmicrosoft.com (12/1/2020 8:21:21 PM)
Remove database
VideoPreview
Name
Created By
Created
Modified By
Modified
Databases\abc.onmicrosoft.com (12/1/2020 8:21:21 PM)
veeam

Restore

This section explains how to restore data to Microsoft Office 365 and on-premises Microsoft organizations.

Restoring Sites

To restore Microsoft SharePoint sites, do the following:

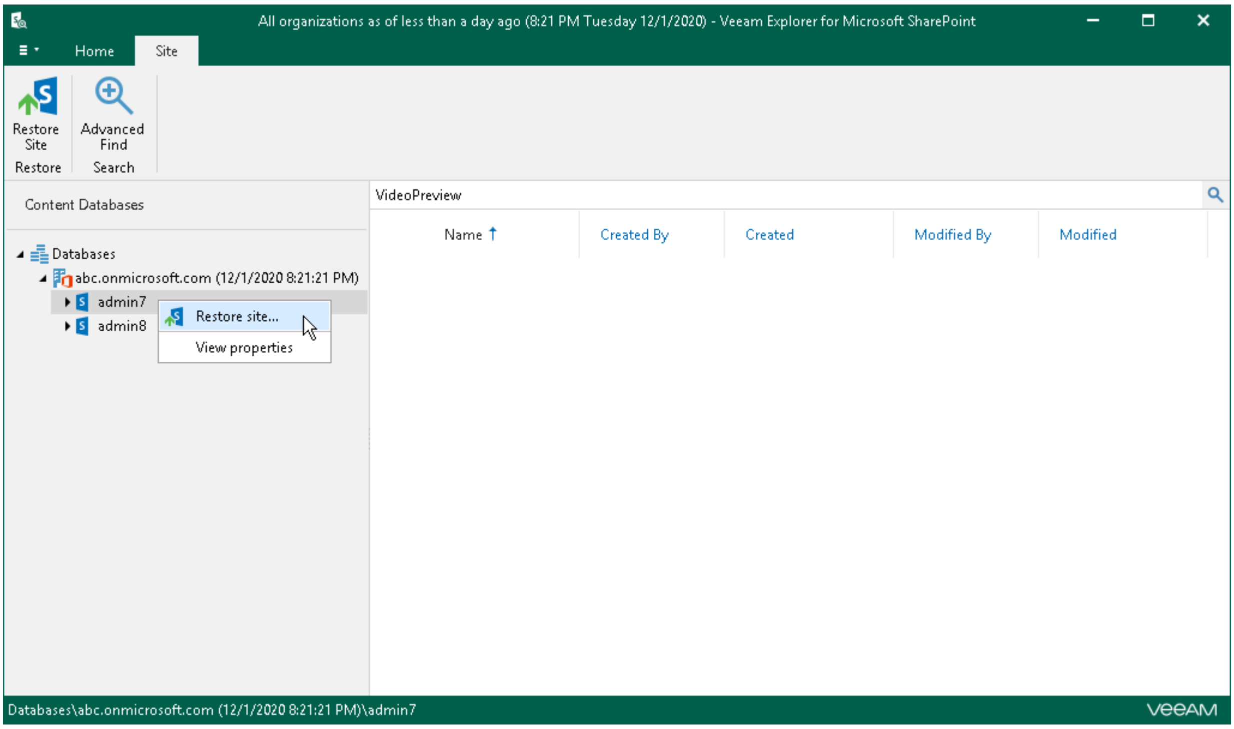
1. Launch the Restore wizard.
2. Select an authentication method.
3. Log in to Office 365.
4. Specify a target site.
5. Specify restore options.

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. In the navigation pane, select a site that you want to restore.
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.


All organizations as of less than a day ago (8:21 PM Tuesday 12/1/2020) - Veeam Explorer for Microsoft SharePoint
Home
Site
Restore Site
Advanced Find
Restore
Search
Content Databases
Databases
abc.onmicrosoft.com (12/1/2020 8:21:21 PM)
admin7
admin8
Restore site...
View properties
VideoPreview
Name
Created By
Created
Modified By
Modified
Databases\abc.onmicrosoft.com (12/1/2020 8:21:21 PM)\admin7
veeam

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:

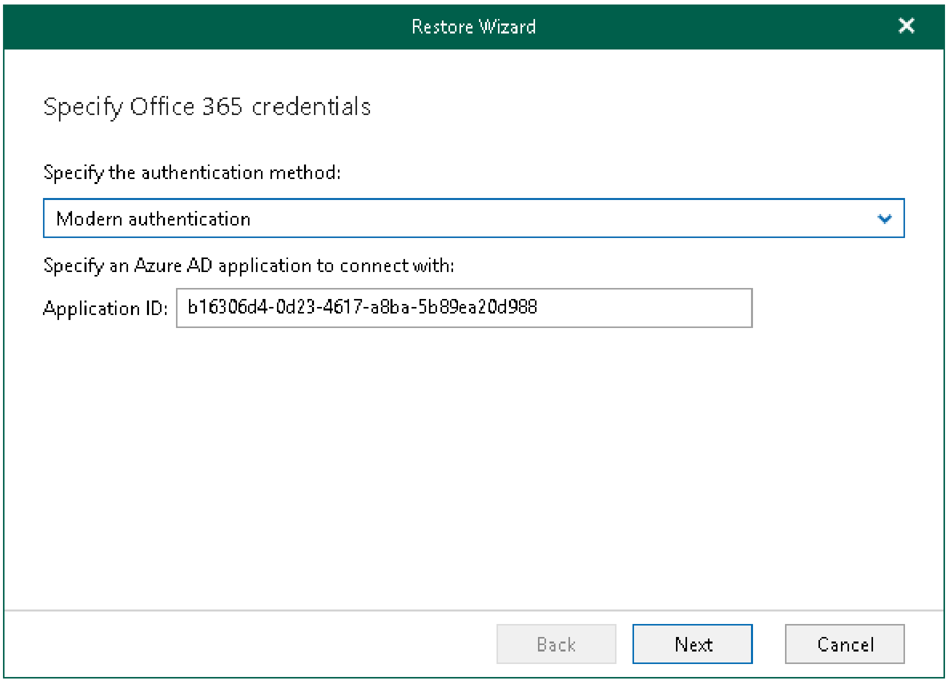
1. From the **Specify the authentication method** drop-down list, select *Modern authentication*.

   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 object 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 SharePoint 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.



Specify Office 365 credentials

Specify the authentication method:

Modern authentication

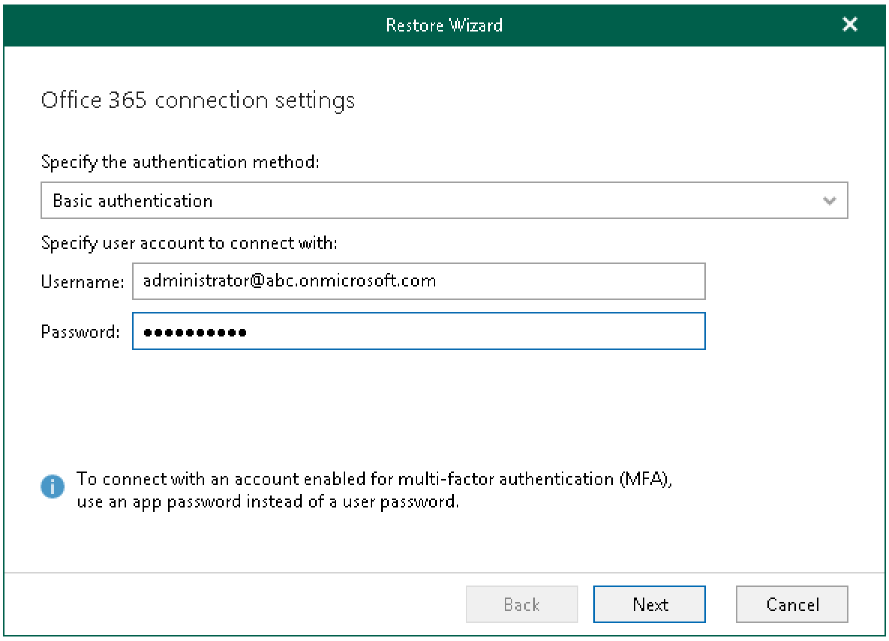
Specify an Azure AD application to connect with:

Application ID: b16306d4-0d23-4617-a8ba-5b89ea20d988

Basic Authentication

To use basic authentication, do the following:

1. From the **Specify the authentication method** drop-down list, select *Basic authentication*.
2. Enter credentials to connect to the SharePoint organization.



Office 365 connection settings

Specify the authentication method: Basic authentication

Specify user account to connect with:

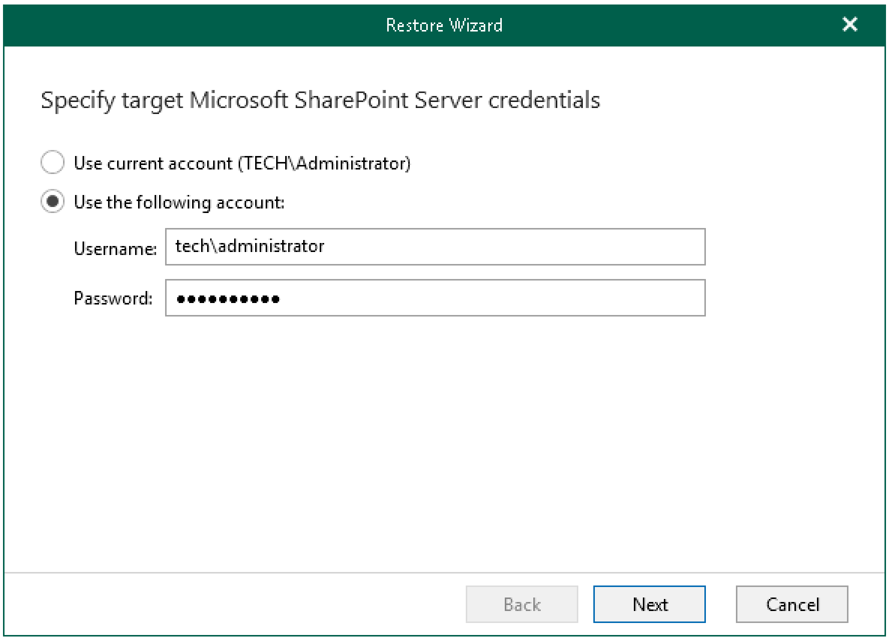
Username: administrator@abc.onmicrosoft.com

Password: ●●●●●●●●●●●

To connect with an account enabled for multi-factor authentication (MFA), use an app password instead of a user password.

On-Premises Organizations

To authenticate on an on-premises Microsoft SharePoint server, provide a user name and password.



Specify target Microsoft SharePoint Server credentials

○ Use current account (TECH\Administrator)

● Use the following account:

Username: tech\administrator

Password: ●●●●●●●●●●●

Step 3. Log In 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 365 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.

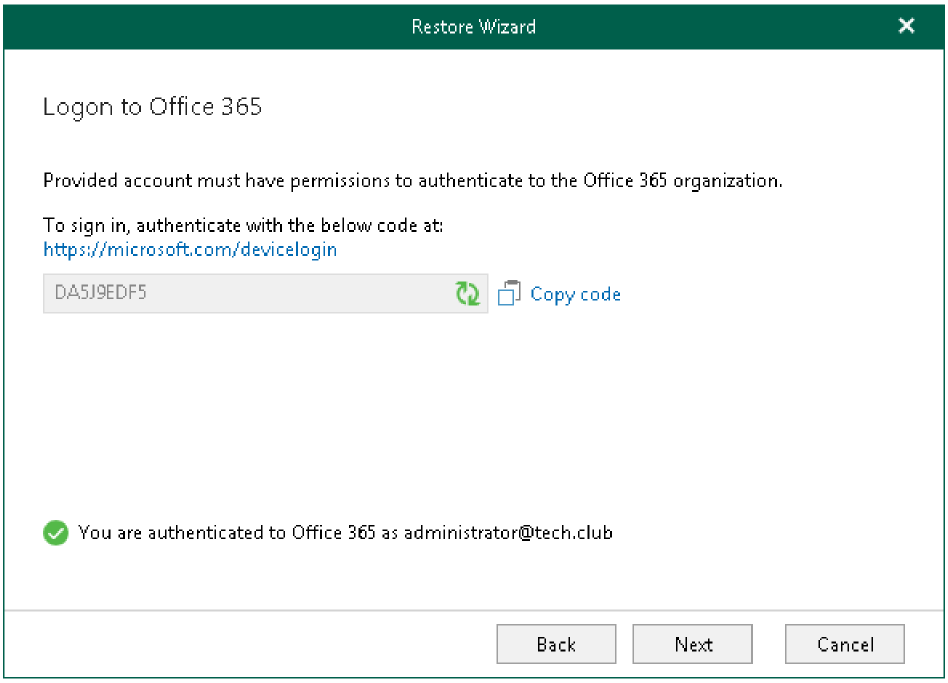
2. Click the link to the Microsoft portal.

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 required permissions assigned. For more information, see Required Permissions.

   Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see Required Azure AD Application Settings.

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, authenticate with the below code at:
https://microsoft.com/devicelogin

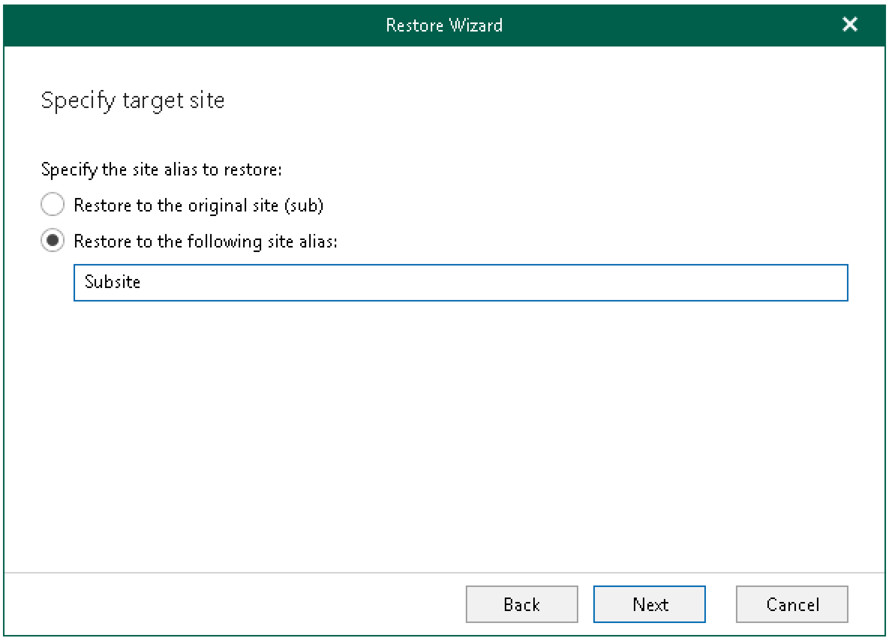
DA5J9EDF5

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

Step 4. Specify Target Site

At this step of the wizard, specify a target site alias that you want to use for a restore.

> **NOTE:**
>
> When restoring site collections, make sure that such collections exist in the target location; Veeam Explorer for Microsoft SharePoint does not create site collections.



Restore Wizard

Specify target site

Specify the site alias to restore:

○ Restore to the original site (sub)

● Restore to the following site alias:

Subsite

Step 5. Specify Restore Options

At this step of the wizard, select restore options and click **Restore**.

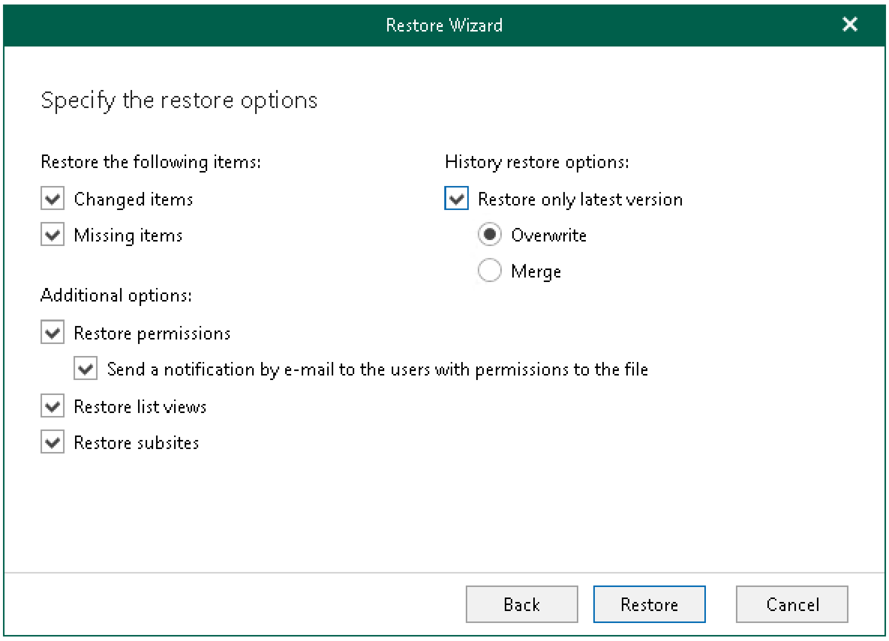
You can select the following options:

- **Changed items**. Allows you to recover data that has been modified in your production environment.
- **Missing items**. Allows you to recover missing items.
- **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.
- **Restore list views.** Allows you to recover your list views.
- **Restore subsites.** Allows you to restore your subsites.
- **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 permissions 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

Restoring Document Libraries and Lists

To restore Microsoft SharePoint document libraries and lists, do the following:

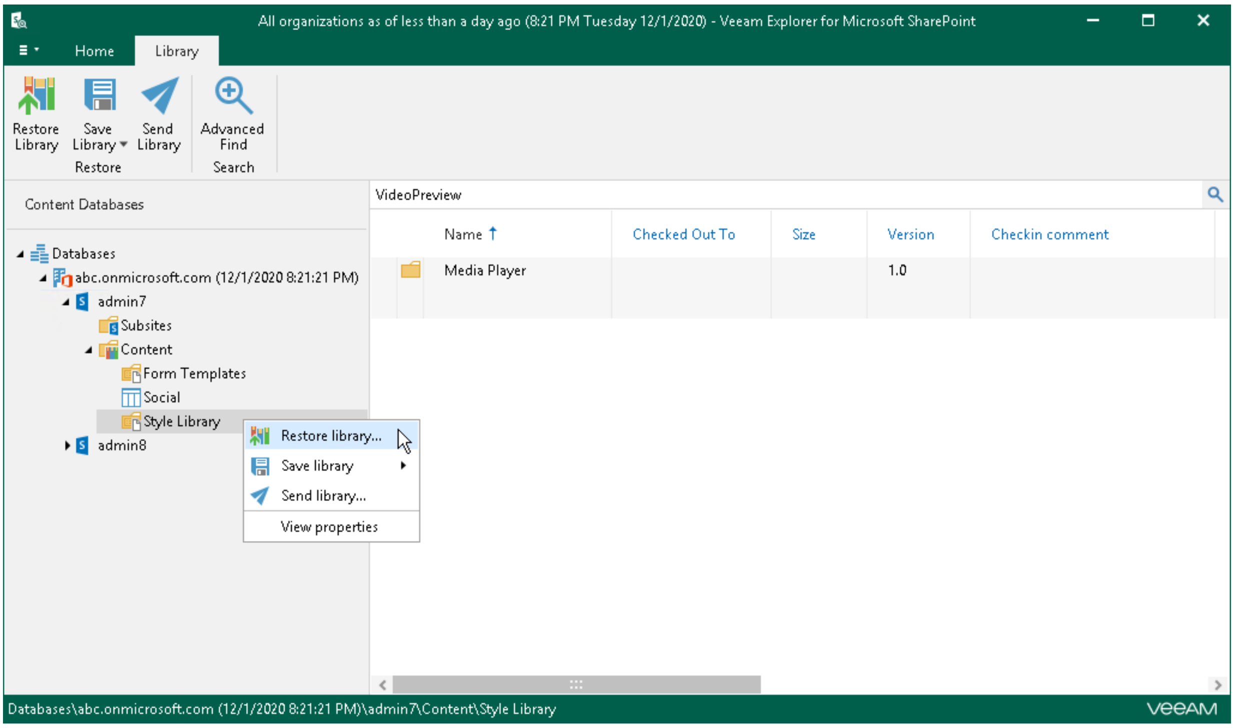
1. Launch the restore wizard.
2. Select an authentication method.
3. Log in to Office 365.
4. Specify a target list.
5. Specify restore options.

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. In the navigation pane, select a library or list that you want to restore.
2. On the **Library** tab, select **Restore Library** or **Restore List** or right-click a library or list and select **Restore library** or **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:

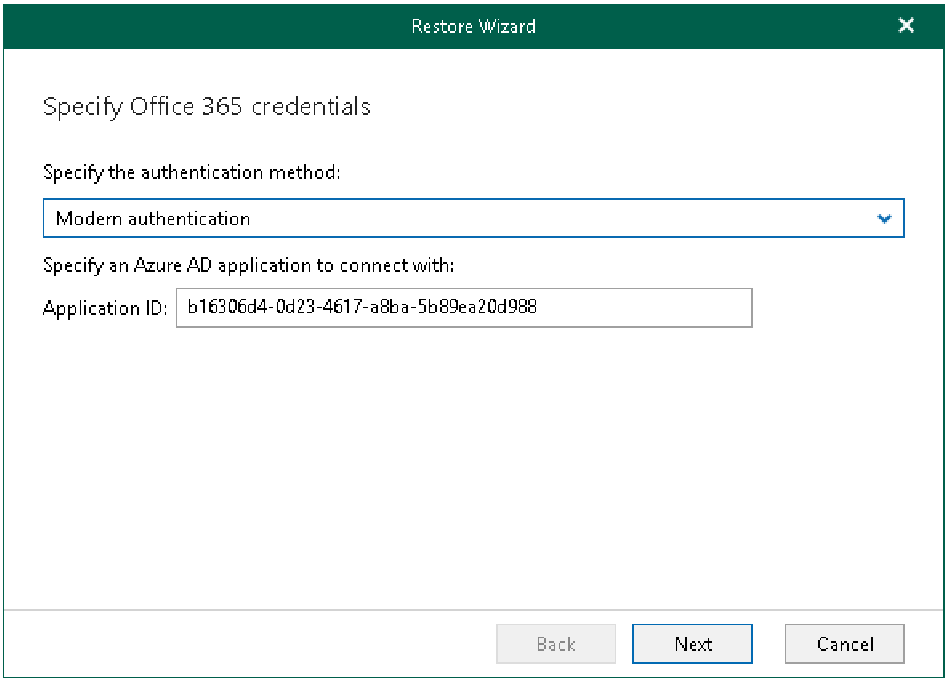
1. From the **Specify the authentication method** drop-down list, select *Modern authentication*.

   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 object 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 SharePoint 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 the authentication method: Modern authentication

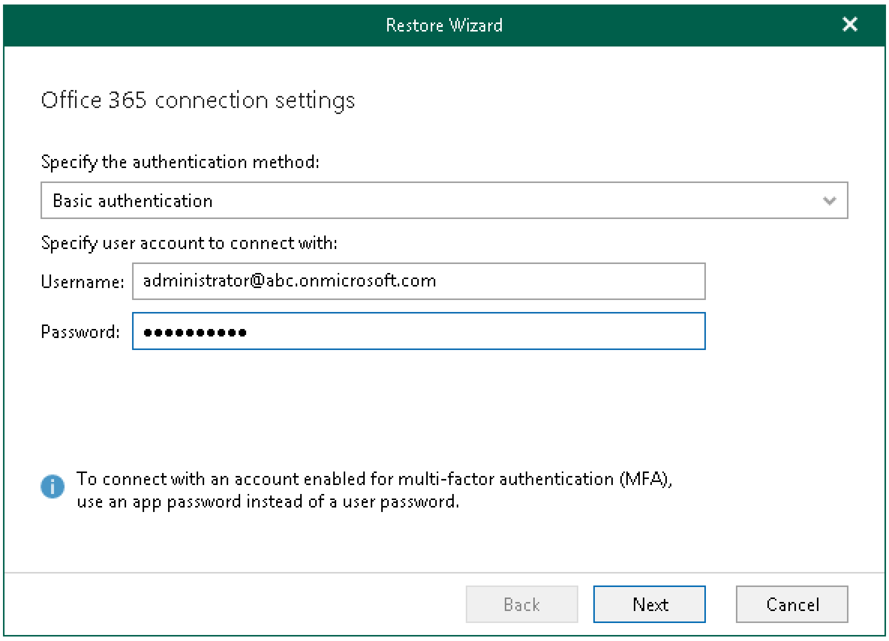
Specify an Azure AD application to connect with:

Application ID: b16306d4-0d23-4617-a8ba-5b89ea20d988

Basic Authentication

To use basic authentication, do the following:

1. From the **Specify the authentication method** drop-down list, select *Basic authentication*.
2. Enter credentials to connect to the SharePoint organization.



Office 365 connection settings

Specify the authentication method: Basic authentication

Specify user account to connect with:

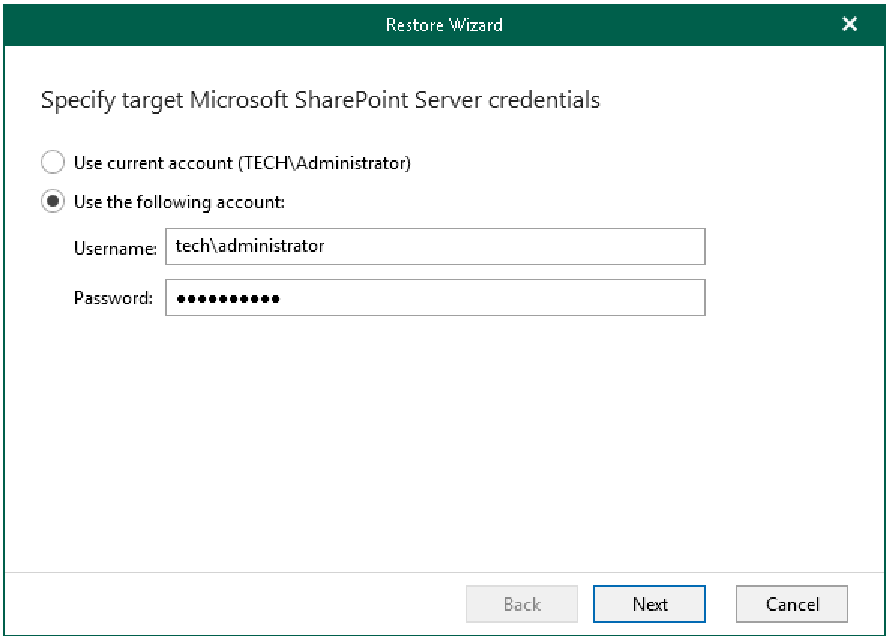
Username: administrator@abc.onmicrosoft.com

Password: ●●●●●●●●●●●

To connect with an account enabled for multi-factor authentication (MFA), use an app password instead of a user password.

On-Premises Organizations

To authenticate on an on-premises Microsoft SharePoint server, provide a user name and password.



Specify target Microsoft SharePoint Server credentials

○ Use current account (TECH\Administrator)

● Use the following account:

Username: tech\administrator

Password: ●●●●●●●●●●●

Step 3. Log In 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 365 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.

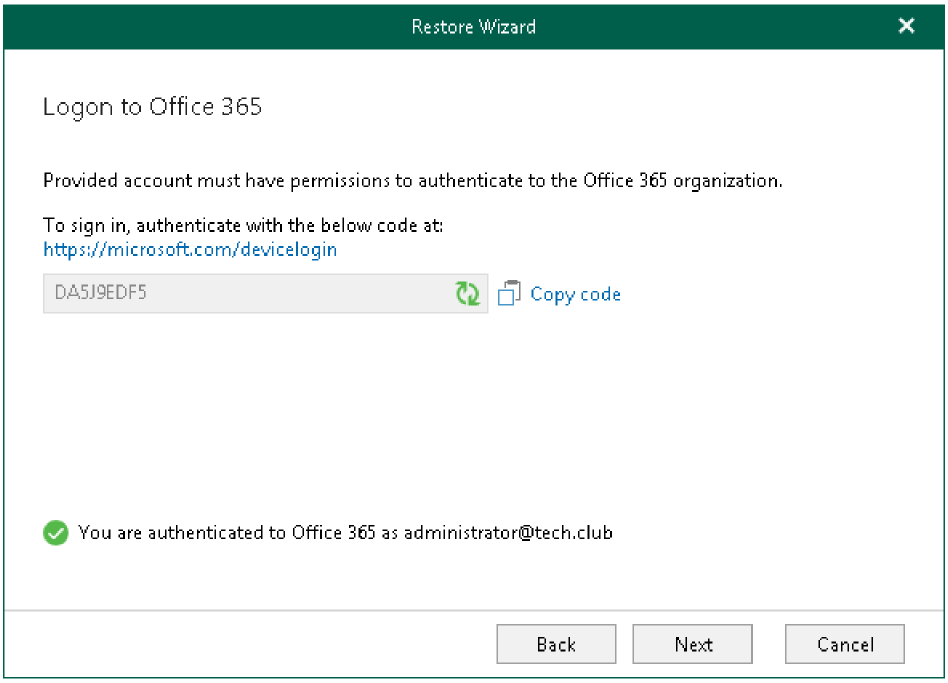
2. Click the link to the Microsoft portal.

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 required permissions assigned. For more information, see Required Permissions.

   Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see Required Azure AD Application Settings.

4. Return to the **Restore Wizard** window and click **Next**.



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

DA5J9EDF5

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

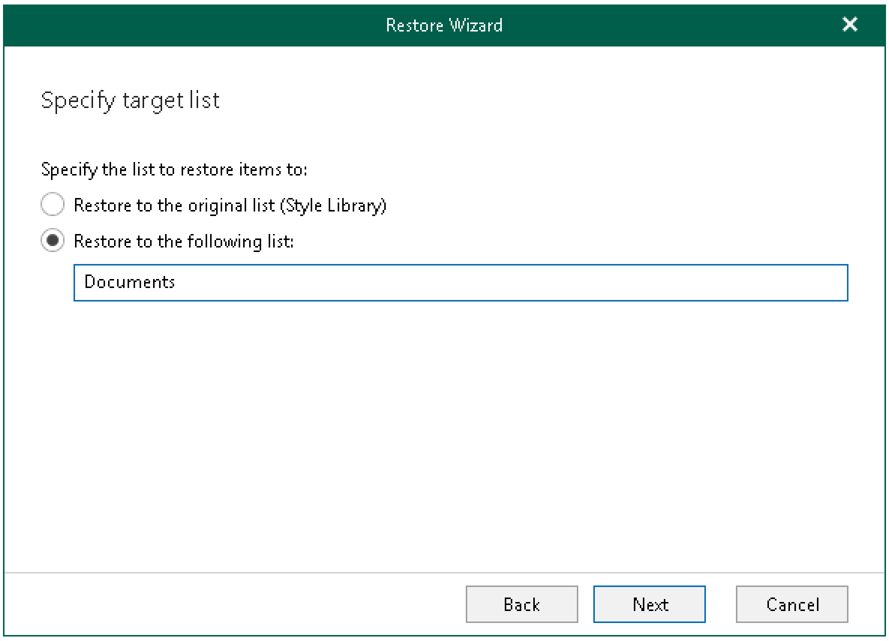
Step 4. Specify Target List

At this step of the wizard, select whether to restore data to the original list or specify a custom list.

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.



Specify target list

Specify the list to restore items to:

○ Restore to the original list (Style Library)

● Restore to the following list:

Documents

Step 5. Specify Restore Options

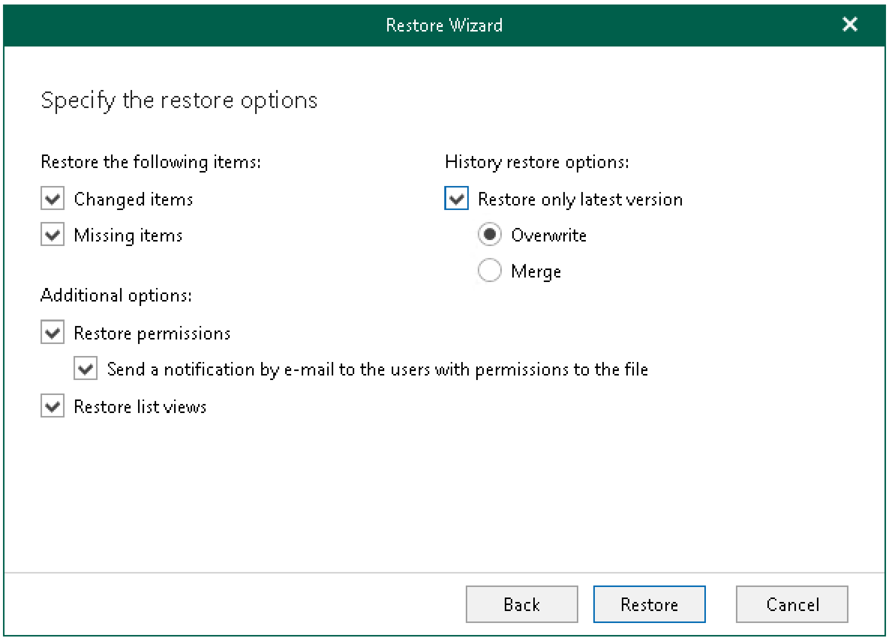
At this step of the wizard, select restore options and click **Restore**.

You can select the following options:

- **Changed items**. Allows you to recover data that has been modified in your production environment.
- **Missing items**. Allows you to recover missing items.
- **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.
- **Restore list views.** Allows you to recover your list views.
- **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 permissions 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.



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

History restore options:

☑ Restore only latest version

● Overwrite

○ Merge

Restoring Documents and List Items

To restore Microsoft SharePoint documents and list items, do the following:

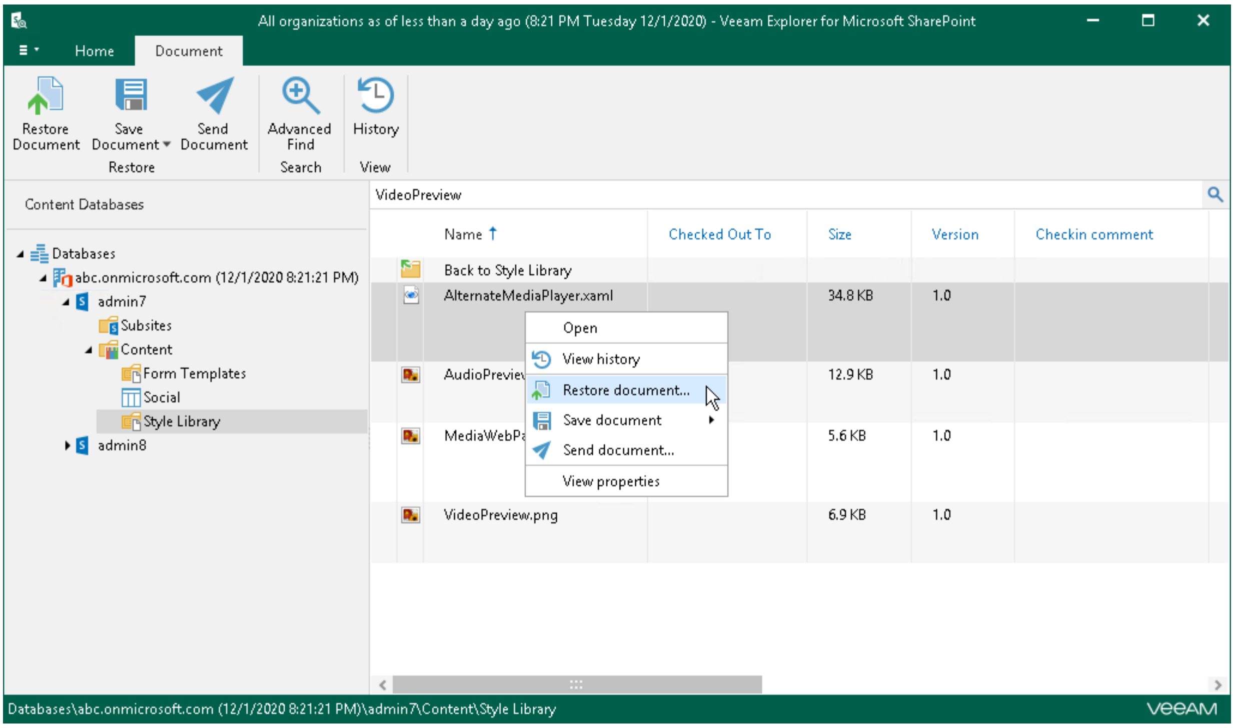
1. Launch the Restore wizard.
2. Select an authentication method.
3. Log in to Office 365.
4. Specify a target list.
5. Specify restore options.

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. In the navigation pane, select a document or list item that you want to restore.
2. On the **Document** tab, select **Restore Document** or **Restore Item** or right-click an object and select **Restore document** or **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.



Name	Checked Out To	Size	Version	Checkin comment
Back to Style Library				
AlternateMediaPlayer.xaml		34.8 KB	1.0	
AudioPreviev		12.9 KB	1.0	
MediaWebPa		5.6 KB	1.0	
VideoPreview.png		6.9 KB	1.0	

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:

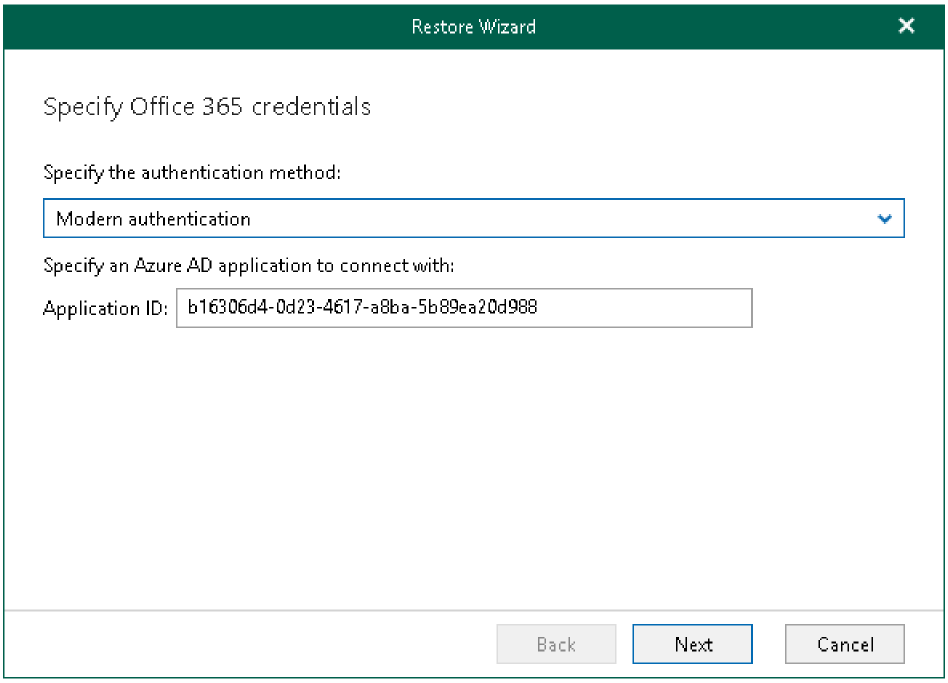
1. From the **Specify the authentication method** drop-down list, select *Modern authentication*.

   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.



Specify Office 365 credentials

Specify the authentication method:

Modern authentication

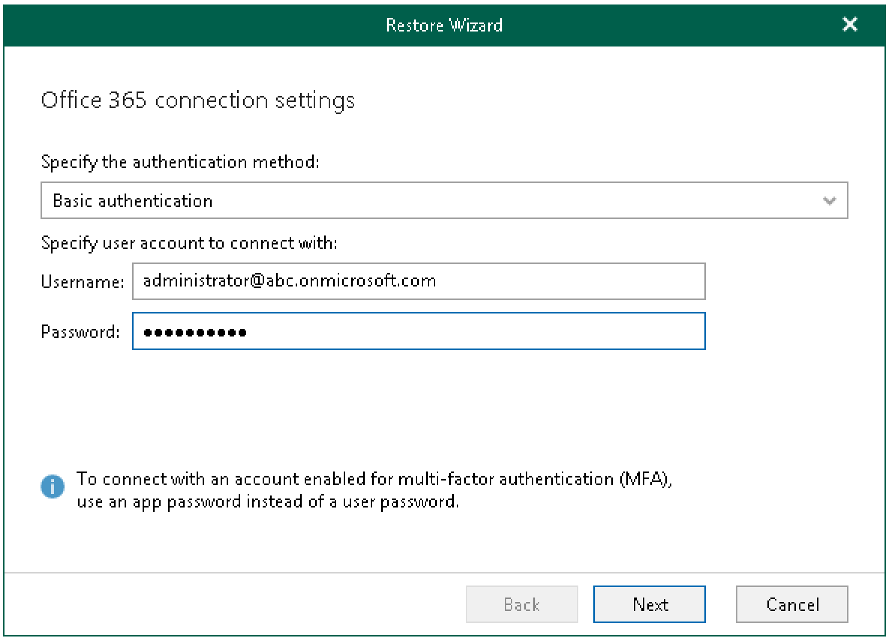
Specify an Azure AD application to connect with:

Application ID: b16306d4-0d23-4617-a8ba-5b89ea20d988

Basic Authentication

To use basic authentication, do the following:

1. From the **Specify the authentication method** drop-down list, select *Basic authentication*.
2. Enter credentials to connect to the SharePoint organization.



Office 365 connection settings

Specify the authentication method: Basic authentication

Specify user account to connect with:

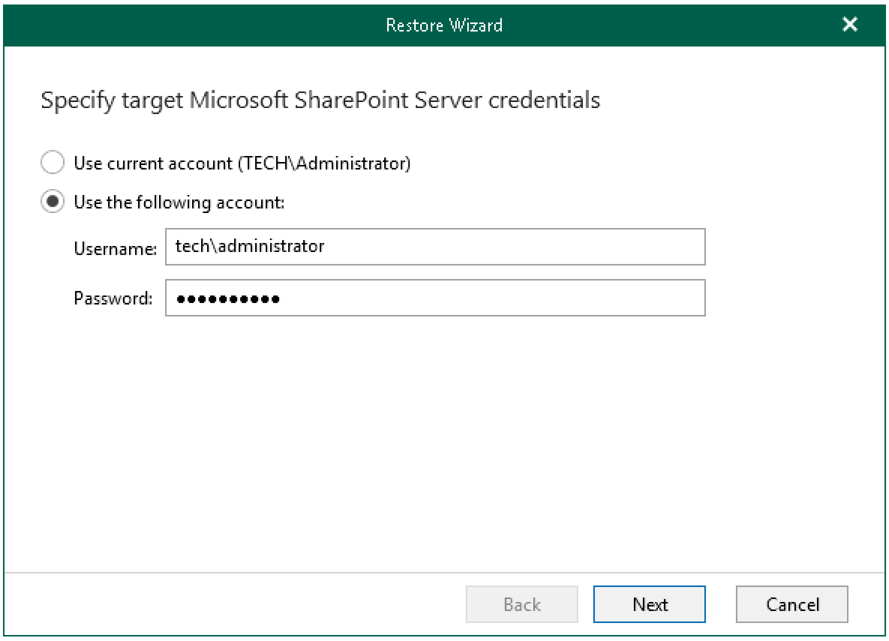
Username: administrator@abc.onmicrosoft.com

Password: ●●●●●●●●●●●

To connect with an account enabled for multi-factor authentication (MFA), use an app password instead of a user password.

On-Premises Organizations

To authenticate on an on-premises Microsoft SharePoint server, provide a user name and password.



Specify target Microsoft SharePoint Server credentials

○ Use current account (TECH\Administrator)

● Use the following account:

Username: tech\administrator

Password: ●●●●●●●●●●●

Step 3. Log In 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 365 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.

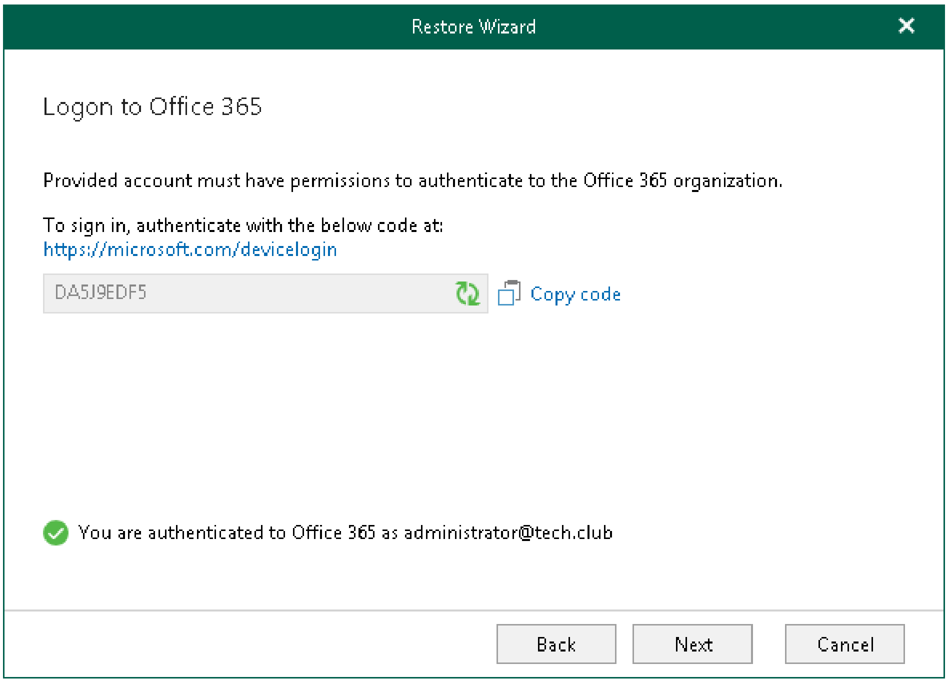
2. Click the link to the Microsoft portal.

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 required permissions assigned. For more information, see Required Permissions.

   Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see Required Azure AD Application Settings.

4. Return to the **Restore Wizard** window and click **Next**.



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

DA5J9EDF5 Copy code

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

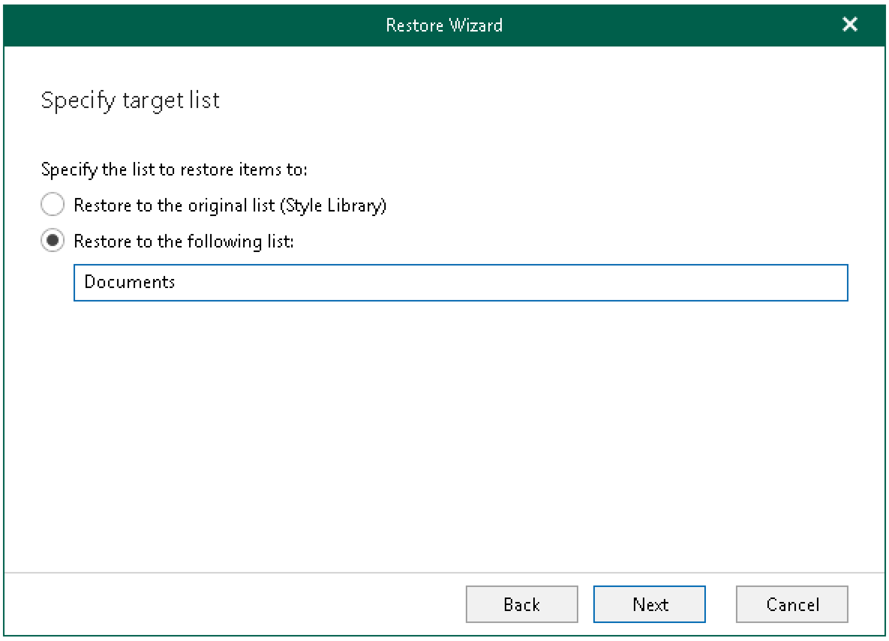
Step 4. Specify Target List

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 (Style Library)

● Restore to the following list:

Documents

Step 5. Specify Restore Options

At this step of the wizard, select restore options and click **Restore**.

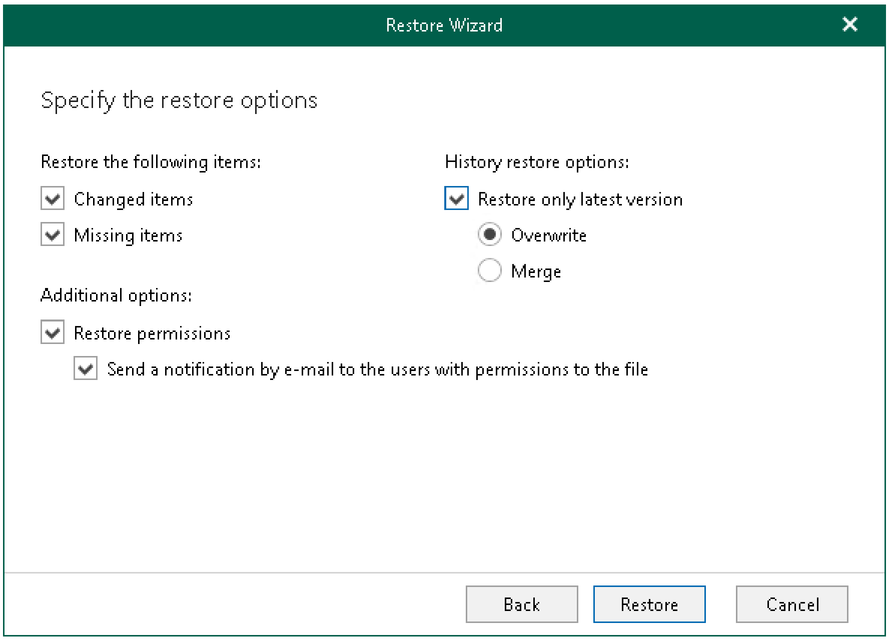
You can select the following options:

- **Changed items**. Allows you to recover data that has been modified in your production environment.
- **Missing items**. Allows you to recover missing items.
- **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.
- **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 permissions 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.



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

History restore options:

☑ Restore only latest version

● Overwrite

○ Merge

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. The operation is available only for backups created in Veeam Backup & Replication.
- Make sure to read Unsupported SharePoint Lists before exporting Microsoft SharePoint lists.

Exporting Microsoft SharePoint Data

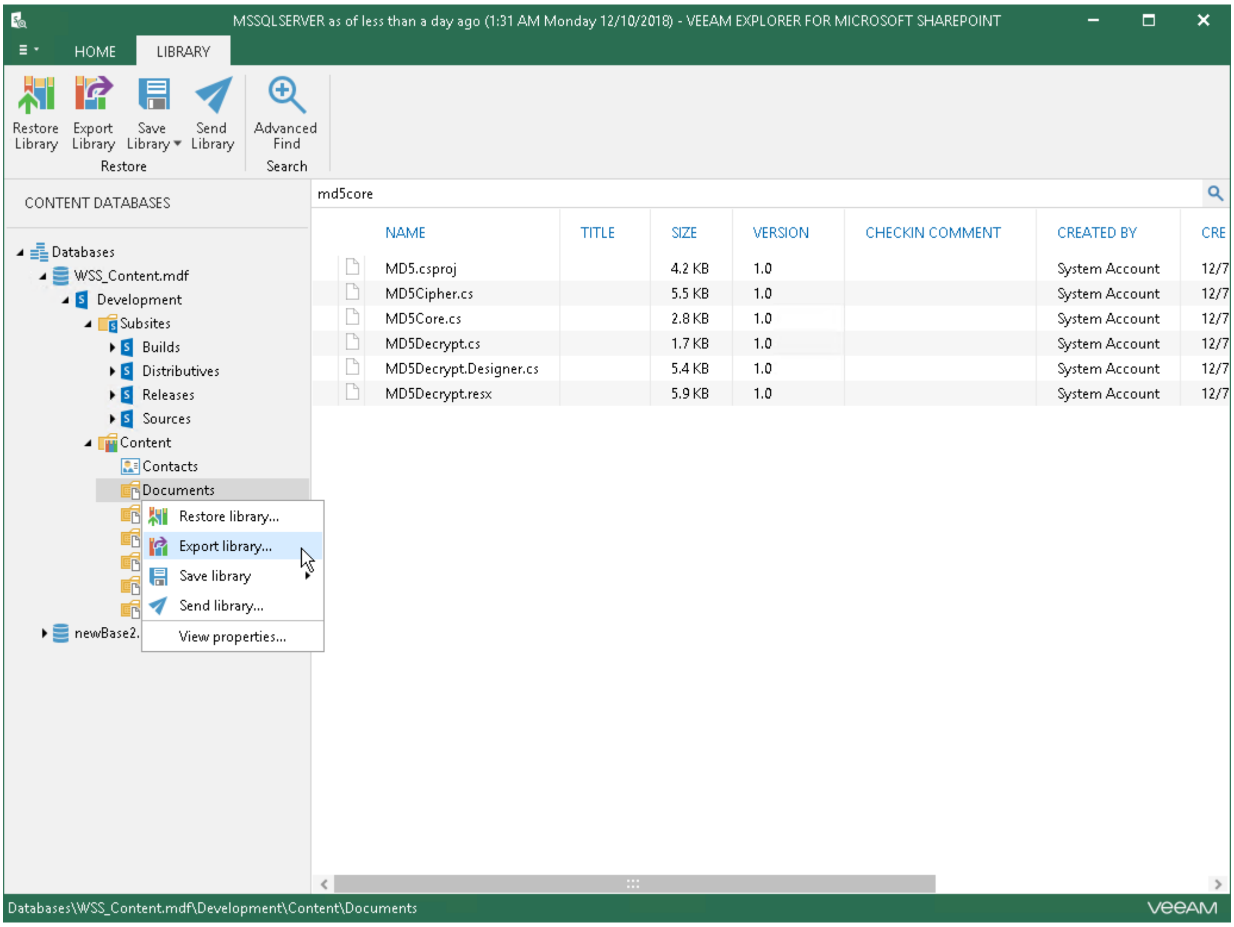
Veeam Explorer for Microsoft SharePoint allows you to export SharePoint document libraries and lists.

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 that you want to export.
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.



NAME	TITLE	SIZE	VERSION	CHECKIN COMMENT	CREATED BY	CRE
MD5.csproj		4.2 KB	1.0		System Account	12/7
MD5Cipher.cs		5.5 KB	1.0		System Account	12/7
MD5Core.cs		2.8 KB	1.0		System Account	12/7
MD5Decrypt.cs		1.7 KB	1.0		System Account	12/7
MD5Decrypt.Designer.cs		5.4 KB	1.0		System Account	12/7
MD5Decrypt.resx		5.9 KB	1.0		System Account	12/7

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
```

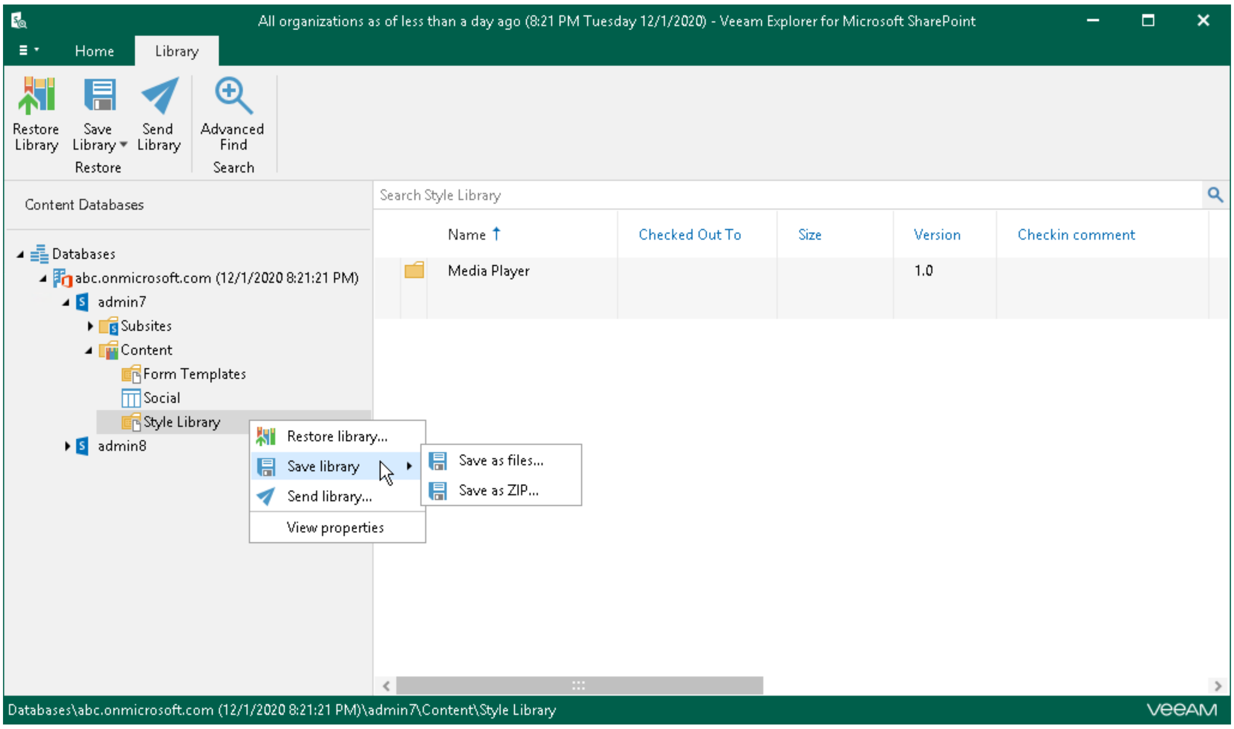
Saving Microsoft SharePoint Documents and Libraries

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 that you want to save.
2. On the **Library** tab, select **Save Library** > **Save as files** or **Save Library** > **Save as ZIP** or right-click an object and select **Save Library** > **Save as 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 as files** or **Save Document > Save as ZIP**.



Sending Microsoft SharePoint Documents and Libraries

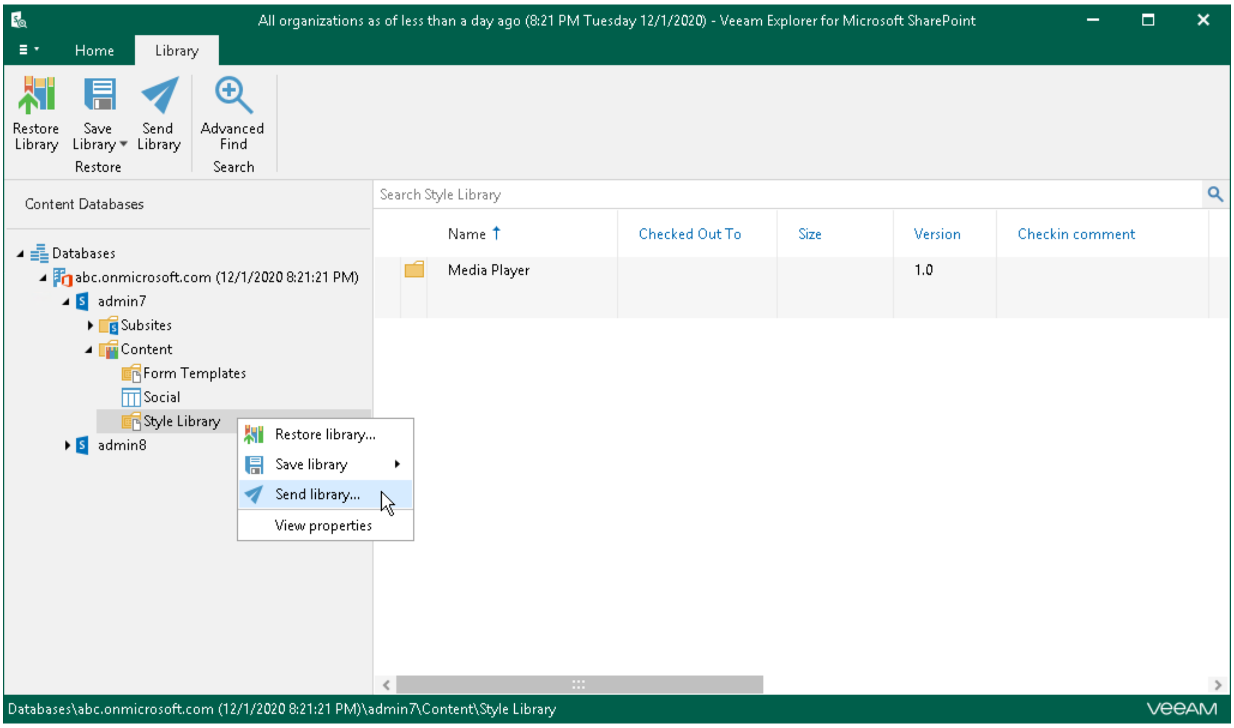
Veeam Explorer for Microsoft SharePoint allows you to send libraries or library documents to the specified recipients via email.

> **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 that you want to send.
2. On the **Library** tab, click **Send Library** or right-click an object and select **Send library**.

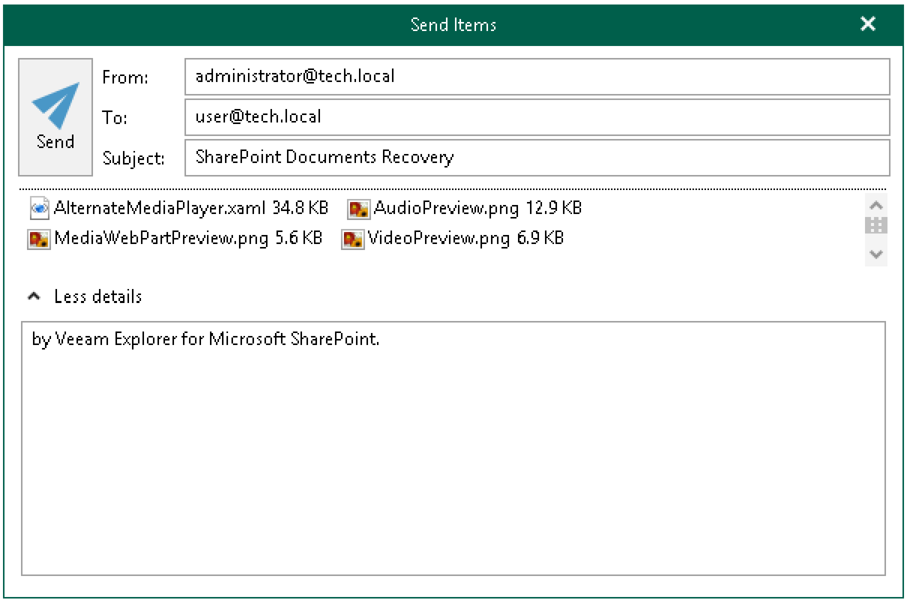
   To send documents from a library, select a document in the preview pane and click **Send Document**.



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**.



From: administrator@tech.local

To: user@tech.local

Subject: SharePoint Documents Recovery

AlternateMediaPlayer.xaml 34.8 KB

AudioPreview.png 12.9 KB

MediaWebPartPreview.png 5.6 KB

VideoPreview.png 6.9 KB

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

ID	List Name	Version
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

ID	List Name	Version
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

ID	List Name	Version
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 & 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 disable these notifications, clear the **Show pop-up notifications on startup** 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.

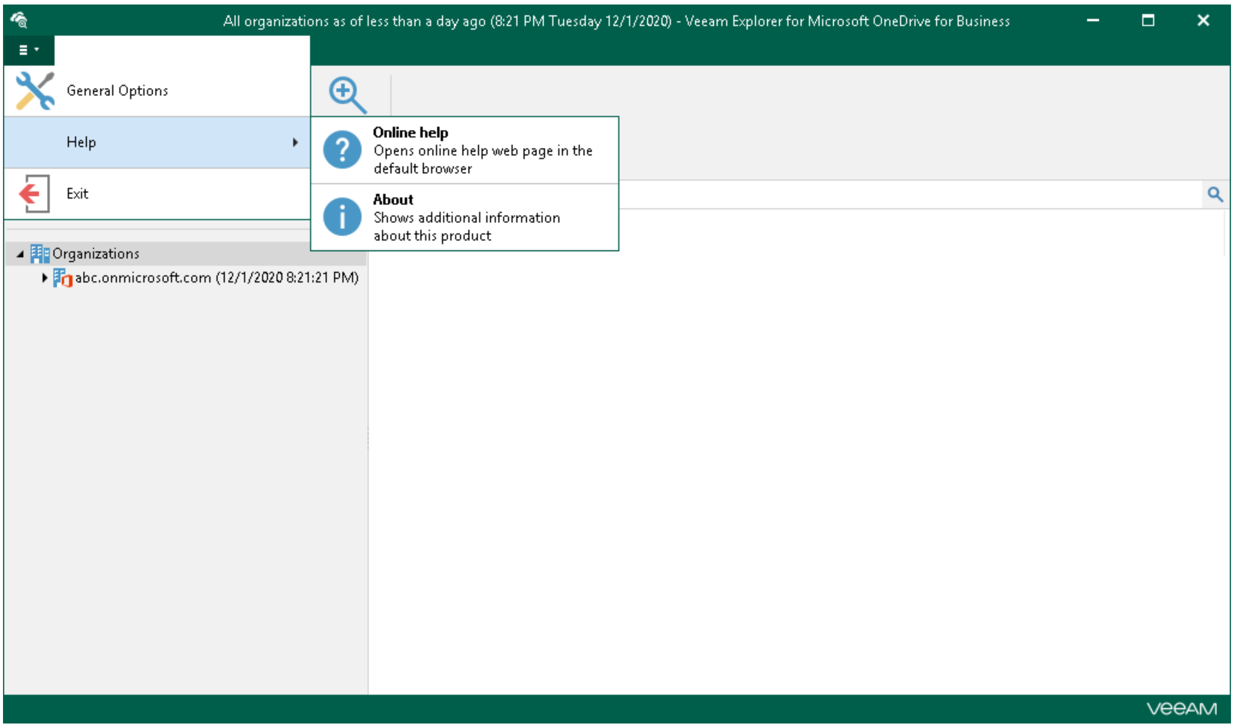
Understanding User Interface

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.



All organizations as of less than a day ago (8:21 PM Tuesday 12/1/2020) - Veeam Explorer for Microsoft OneDrive for Business

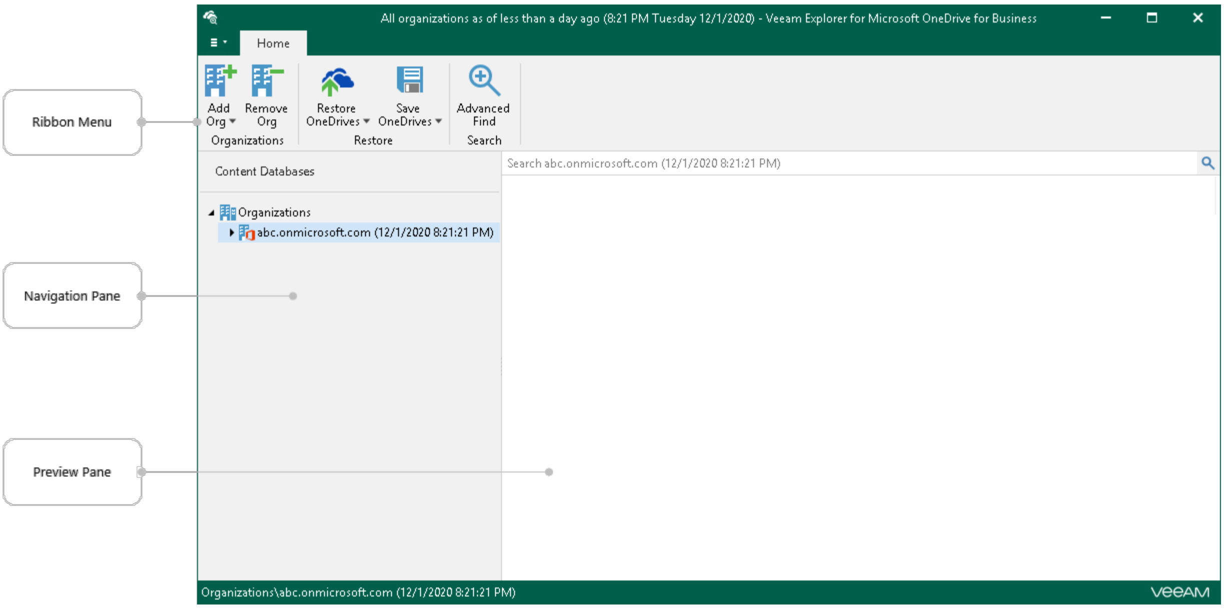
Online help
Opens online help web page in the default browser

About
Shows additional information about this product

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.


Ribbon Menu
Navigation Pane
Preview Pane
All organizations as of less than a day ago (8:21 PM Tuesday 12/1/2020) - Veeam Explorer for Microsoft OneDrive for Business
Home
Add Org
Remove Org
Organizations
Restore OneDrives
Save OneDrives
Restore
Advanced Find
Search
Content Databases
Organizations
abc.onmicrosoft.com (12/1/2020 8:21:21 PM)
Search abc.onmicrosoft.com (12/1/2020 8:21:21 PM)
Organizations\abc.onmicrosoft.com (12/1/2020 8:21:21 PM)
veeam

Browsing, Searching and Viewing Items

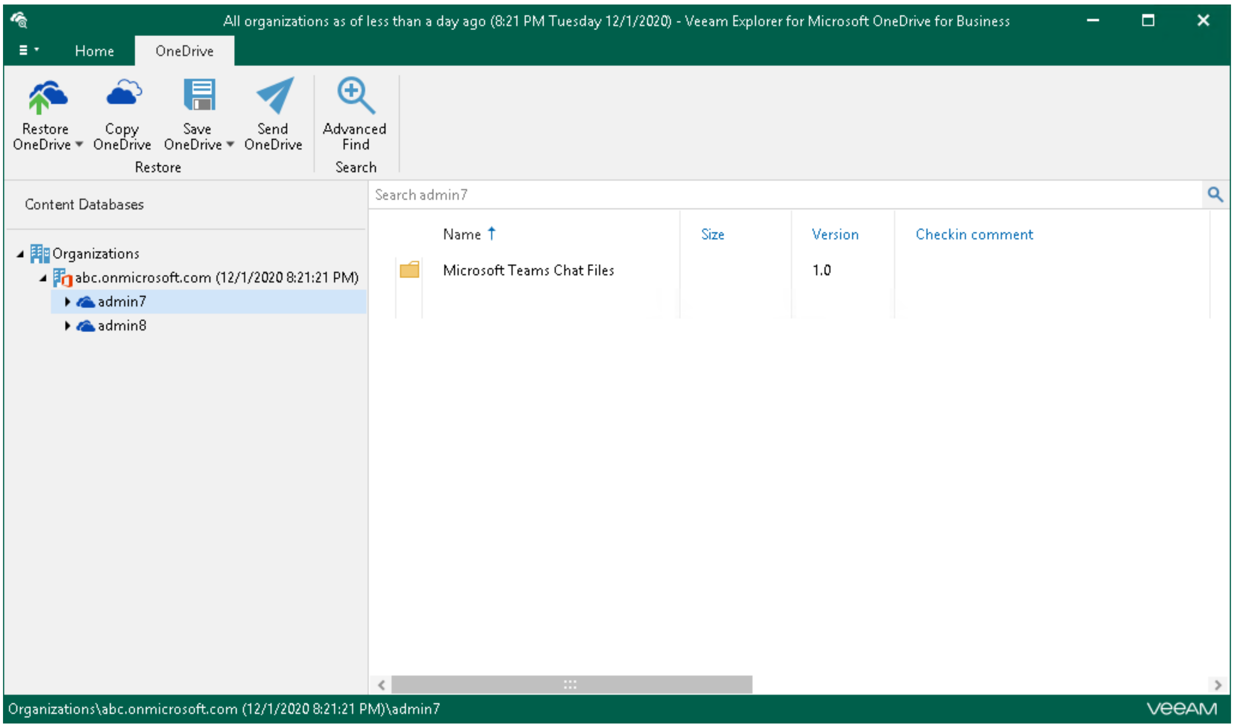
Continue with this section to learn more about:

- 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.

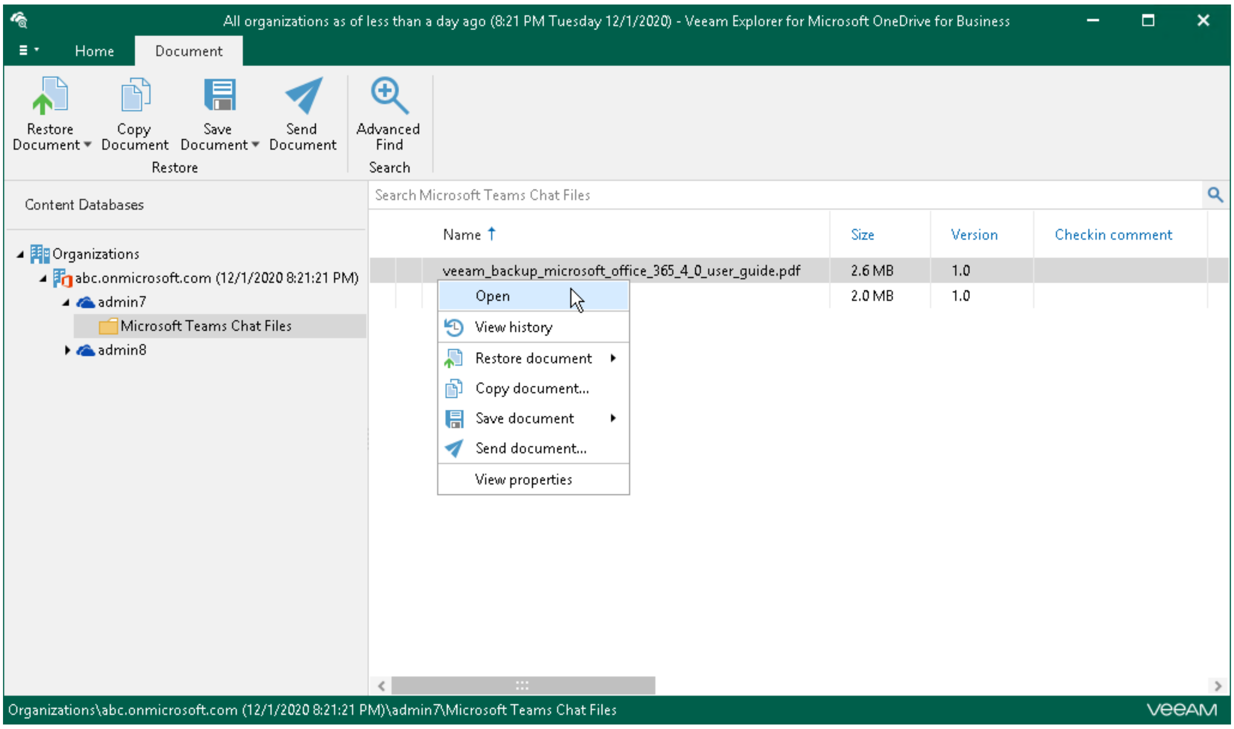

All organizations as of less than a day ago (8:21 PM Tuesday 12/1/2020) - Veeam Explorer for Microsoft OneDrive for Business
Home
OneDrive
Restore OneDrive
Copy OneDrive
Save OneDrive
Send OneDrive
Restore
Advanced Find
Search
Content Databases
Organizations
abc.onmicrosoft.com (12/1/2020 8:21:21 PM)
admin7
admin8
Search admin7
Organizations\abc.onmicrosoft.com (12/1/2020 8:21:21 PM)\admin7
veeam

Name	Size	Version	Checkin comment
Microsoft Teams Chat Files		1.0	

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**.


All organizations as of less than a day ago (8:21 PM Tuesday 12/1/2020) - Veeam Explorer for Microsoft OneDrive for Business
Home
Document
Restore Document
Copy Document
Save Document
Send Document
Restore
Advanced Find
Search
Content Databases
Organizations
abc.onmicrosoft.com (12/1/2020 8:21:21 PM)
admin7
Microsoft Teams Chat Files
admin8
Search Microsoft Teams Chat Files
Name
Size
Version
Checkin comment
veeam_backup_microsoft_office_365_4_0_user_guide.pdf
2.6 MB
1.0
2.0 MB
1.0
Open
View history
Restore document
Copy document...
Save document
Send document...
View properties
Organizations\abc.onmicrosoft.com (12/1/2020 8:21:21 PM)\admin7\Microsoft Teams Chat Files
veeam

Searching

The search mechanism allows you to find items matching specified search criteria.

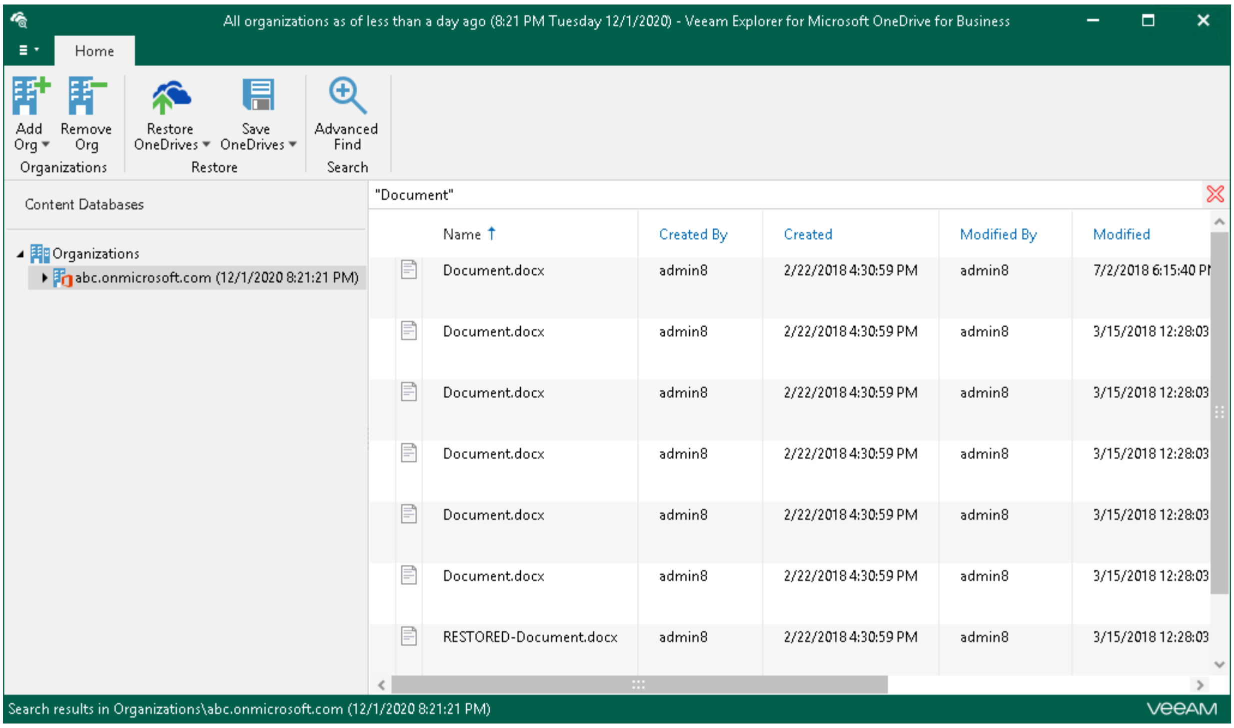
To search for required items, do the following:

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 ?.



All organizations as of less than a day ago (8:21 PM Tuesday 12/1/2020) - Veeam Explorer for Microsoft OneDrive for Business

"Document"

Name	Created By	Created	Modified By	Modified
Document.docx	admin8	2/22/2018 4:30:59 PM	admin8	7/2/2018 6:15:40 P
Document.docx	admin8	2/22/2018 4:30:59 PM	admin8	3/15/2018 12:28:03
Document.docx	admin8	2/22/2018 4:30:59 PM	admin8	3/15/2018 12:28:03
Document.docx	admin8	2/22/2018 4:30:59 PM	admin8	3/15/2018 12:28:03
Document.docx	admin8	2/22/2018 4:30:59 PM	admin8	3/15/2018 12:28:03
Document.docx	admin8	2/22/2018 4:30:59 PM	admin8	3/15/2018 12:28:03
RESTORED-Document.docx	admin8	2/22/2018 4:30:59 PM	admin8	3/15/2018 12:28:03

Search results in Organizations\abc.onmicrosoft.com (12/1/2020 8:21:21 PM)

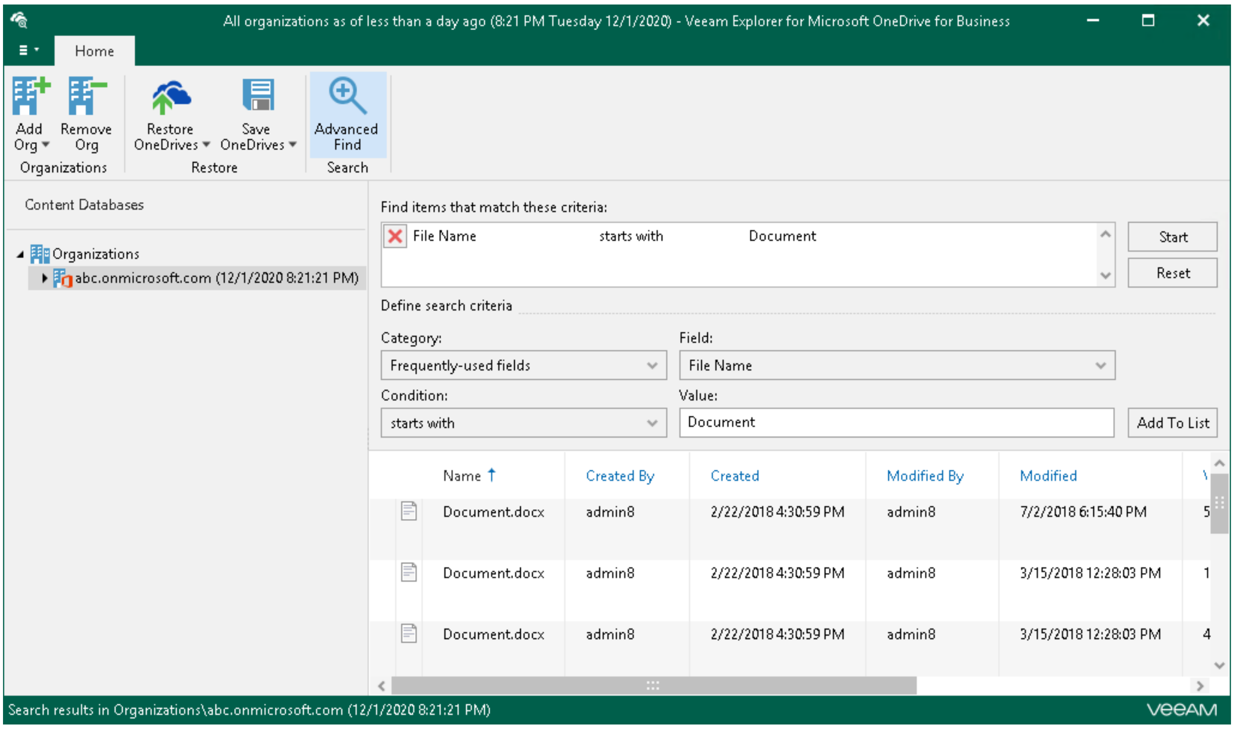
Using Advanced Find Capabilities

The **Advanced Find** mechanism allows you to define your search criteria more precisely.

For example, to find an object that starts with the word *Document*, 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 **Add To List**, then click **Start**.

To remove a filter, click the cross mark next to it. To remove all configured filters, click **Reset**.



All organizations as of less than a day ago (8:21 PM Tuesday 12/1/2020) - Veeam Explorer for Microsoft OneDrive for Business

Find items that match these criteria:

☒ File Name starts with Document

Define search criteria

Category: Frequently-used fields

Field: File Name

Condition: starts with

Value: Document

Name	Created By	Created	Modified By	Modified
Document.docx	admin8	2/22/2018 4:30:59 PM	admin8	7/2/2018 6:15:40 PM
Document.docx	admin8	2/22/2018 4:30:59 PM	admin8	3/15/2018 12:28:03 PM
Document.docx	admin8	2/22/2018 4:30:59 PM	admin8	3/15/2018 12:28:03 PM

Search results in Organizations\abc.onmicrosoft.com (12/1/2020 8:21:21 PM)

General Application Settings

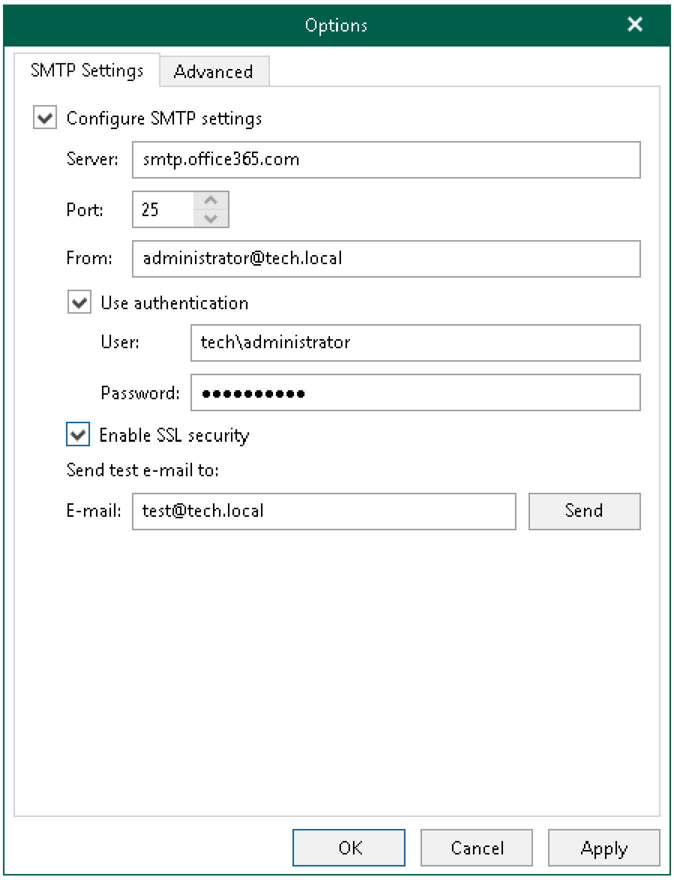
Continue with this section to learn more about configuring general application settings and components.

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**.



☑ Configure SMTP settings

Server: smtp.office365.com

Port: 25

From: administrator@tech.local

☑ Use authentication

User: tech\administrator

Password: ●●●●●●●●●●●

☑ Enable SSL security

Send test e-mail to:

E-mail: test@tech.local

Advanced Settings

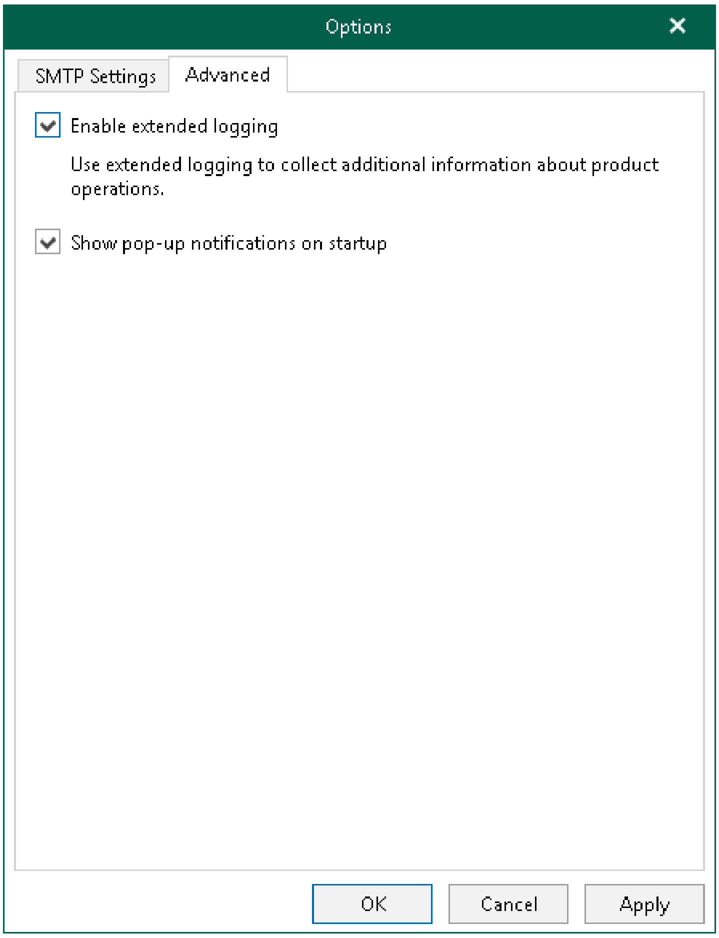
This section explains how to configure advanced settings of the application.

To configure advanced settings, do the following:

1. Go to the main menu and click **General Options**.
2. Click the **Advanced** tab.
3. 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.
4. By default, Veeam Explorer for Microsoft OneDrive for Business displays notifications when loading backups from object storage repositories. If you want to disable these notifications, clear the **Show pop-up notifications on startup** check box.

   Applicable to backups created in Veeam Backup for Microsoft Office 365.



☑ Enable extended logging

Use extended logging to collect additional information about product operations.

☑ Show pop-up notifications on startup

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

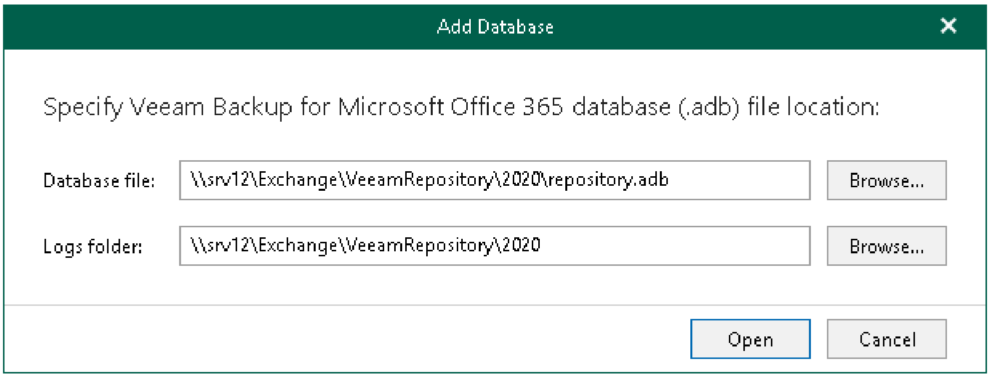
To manually add databases that store Microsoft Office 365 organization data, do the following:

1. On the ribbon, click **Add Org** > **Veeam Backup for Microsoft Office 365 database**.

   Alternatively, in the preview pane, right-click **Organizations** and select **Veeam Backup for Microsoft Office 365 database**.

2. Specify the database file location and log directory.

3. Click **Open**.



Specify Veeam Backup for Microsoft Office 365 database (.adb) file location:

Database file: \\srv12\Exchange\VeeamRepository\2020\repository.adb

Logs folder: \\srv12\Exchange\VeeamRepository\2020

Adding Veeam Backup for Microsoft Office 365 Server

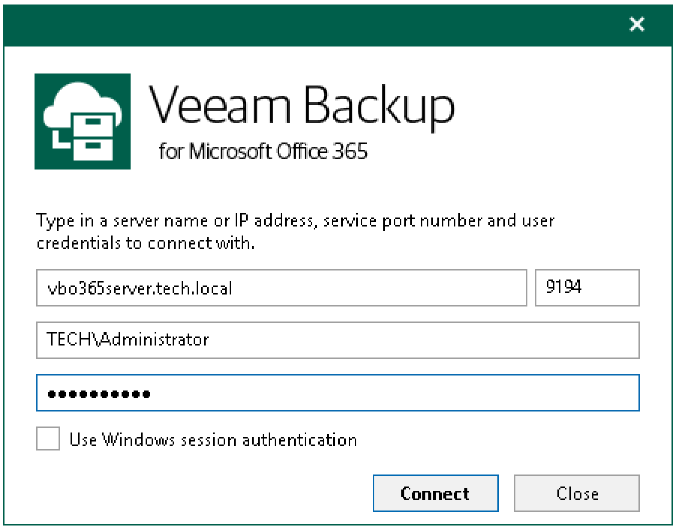
You can use Veeam Explorer for Microsoft OneDrive for Business to connect to another Veeam Backup for Microsoft Office 365 server and add its databases to the Veeam Explorer for Microsoft OneDrive for Business scope.

To connect to another Veeam Backup for Microsoft Office 365 server, do the following:

1. On the ribbon, click **Add Org** > **Veeam Backup for Microsoft Office 365 server**.

   Alternatively, in the preview pane, right-click **Organizations** and select **Veeam Backup for Microsoft Office 365 server**.

2. Specify settings to connect to the Veeam Backup for Microsoft Office 365 server and click **Connect**.



Type in a server name or IP address, service port number and user credentials to connect with.

vbo365server.tech.local

9194

TECH\Administrator

●●●●●●●●●●

□ Use Windows session authentication

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 ribbon, click **Add Store** > **Veeam Backup for Microsoft Office 365 service provider**.

   Alternatively, in the preview pane, right-click **Organizations** and select **Veeam Backup for Microsoft Office 365 service provider**.

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.

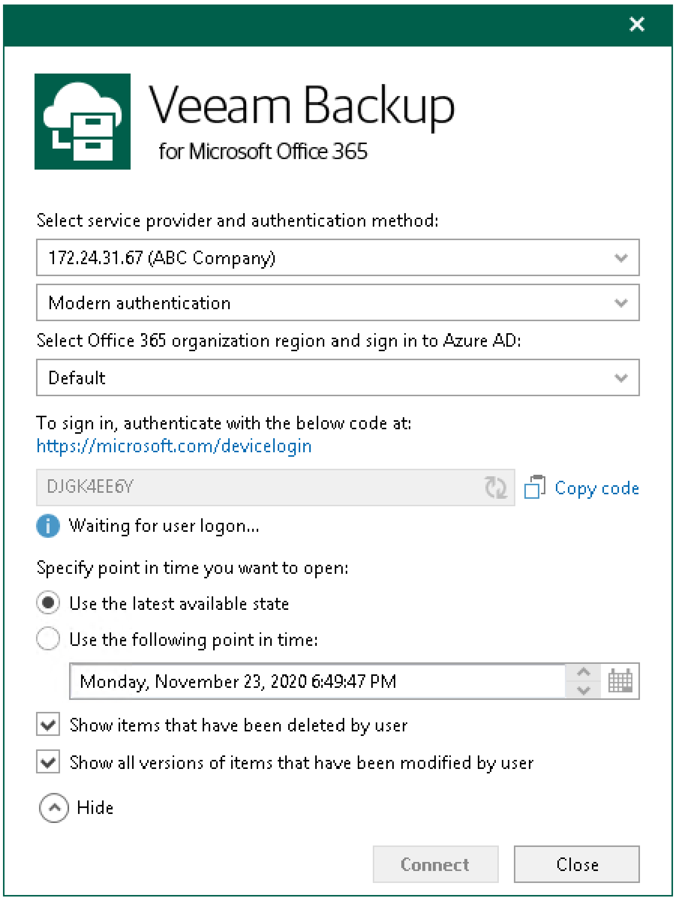
6. Select a point-in-time state as of which you want to load Office 365 backups.

   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:

172.24.31.67 (ABC Company)

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

DJGK4EE6Y

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:

Monday, November 23, 2020 6:49:47 PM

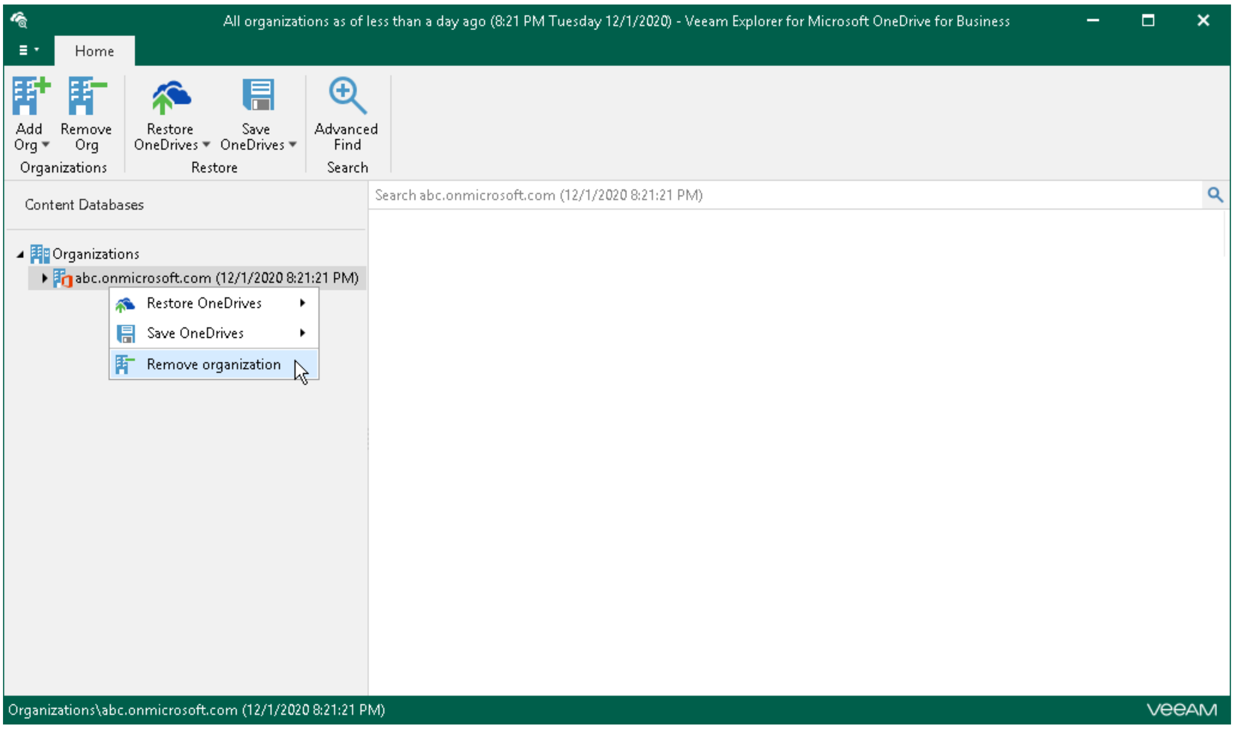
☑ Show items that have been deleted by user

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

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**.


All organizations as of less than a day ago (8:21 PM Tuesday 12/1/2020) - Veeam Explorer for Microsoft OneDrive for Business
Home
Add Org
Remove Org
Organizations
Restore OneDrives
Save OneDrives
Restore
Advanced Find
Search
Content Databases
Search abc.onmicrosoft.com (12/1/2020 8:21:21 PM)
Organizations
abc.onmicrosoft.com (12/1/2020 8:21:21 PM)
Restore OneDrives
Save OneDrives
Remove organization
Organizations\abc.onmicrosoft.com (12/1/2020 8:21:21 PM)
veeam

Restore

This section explains how to restore data to Microsoft Office 365 and on-premises Microsoft organizations.

Restoring Single OneDrive

To restore data of a single OneDrive, do the following:

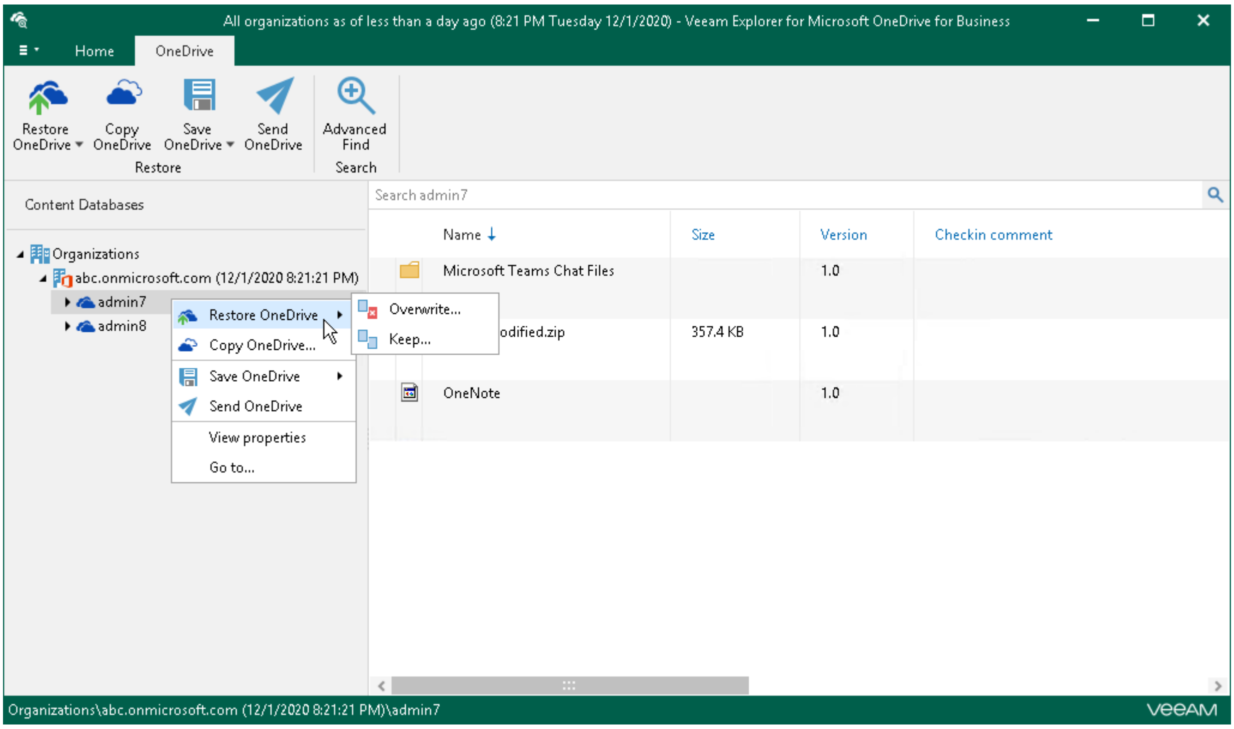
1. Launch the Restore wizard.
2. Select an authentication method.
3. Log in to Office 365.

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. Select an object that you want to restore:
   - To restore OneDrive, select the necessary OneDrive in the inventory pane.
   - To restore a folder, select the necessary folder in the inventory pane.
   - To restore a document, select a folder that contains the document in the inventory pane and select the document in the preview pane.
2. On the **OneDrive/Folder/Document** tab, click **Restore OneDrive/Restore Folder/Restore Document and select one of the following options:**
   - **Overwrite** — to completely overwrite existing OneDrive data.
   - **Keep** — to preserve existing data and recover items with the *RESTORED* prefix (`RESTORED-<file_name>.ext`).

Alternatively, right-click an object that you want to restore and select **Restore OneDrive/Restore folder/Restore document** > **Overwrite** or **Restore OneDrive/Restore folder/Restore document** > **Keep**.



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:

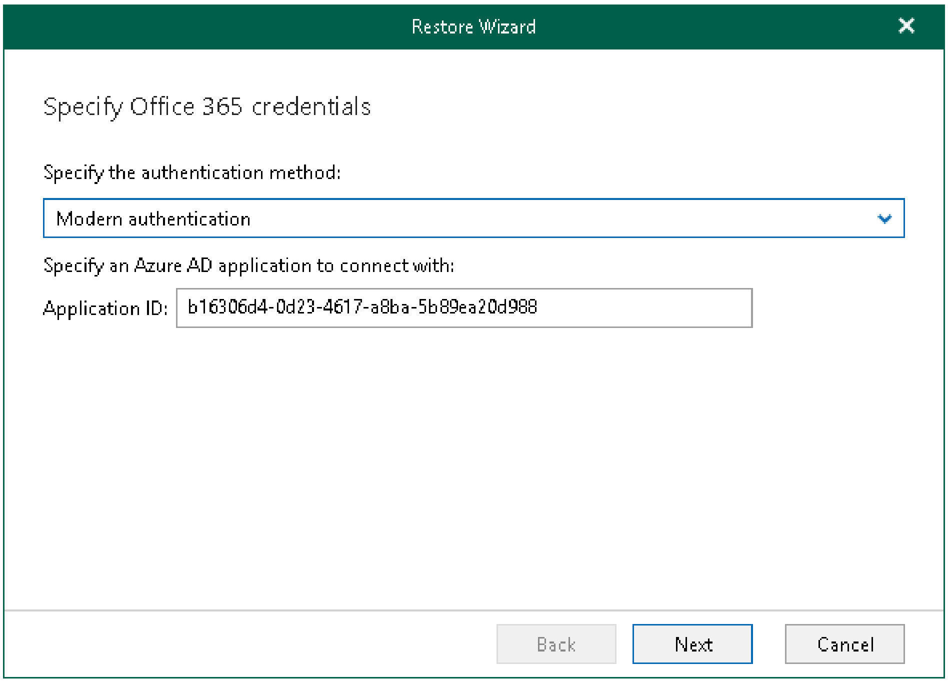
1. From the **Specify the authentication method** drop-down list, select *Modern authentication*.

   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 object 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 OneDrive for Business 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.



Specify Office 365 credentials

Specify the authentication method: Modern authentication

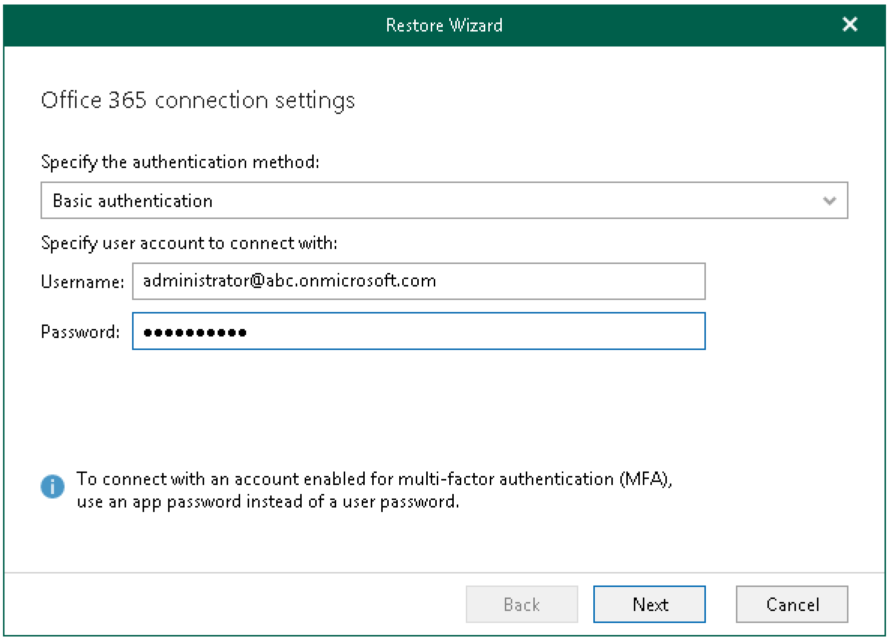
Specify an Azure AD application to connect with:

Application ID: b16306d4-0d23-4617-a8ba-5b89ea20d988

Basic Authentication

To use basic authentication, do the following:

1. From the **Specify the authentication method** drop-down list, select *Basic authentication*.
2. Enter credentials to connect to the SharePoint organization.



Office 365 connection settings

Specify the authentication method: Basic authentication

Specify user account to connect with:

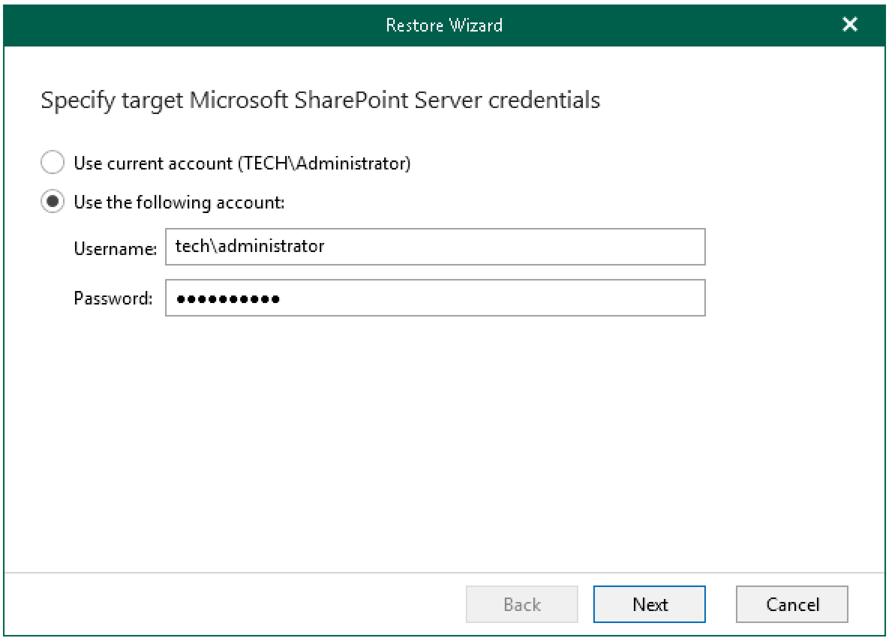
Username: administrator@abc.onmicrosoft.com

Password: ●●●●●●●●●●●

To connect with an account enabled for multi-factor authentication (MFA), use an app password instead of a user password.

On-Premises Organizations

To authenticate on an on-premises Microsoft SharePoint server, provide a user name and password.



Specify target Microsoft SharePoint Server credentials

○ Use current account (TECH\Administrator)

● Use the following account:

Username: tech\administrator

Password: ●●●●●●●●●●●

Step 3. Log In to Office 365

This step is only available if you have selected the *Modern authentication* option at the previous step of the wizard.

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

To sign in to the Microsoft Office 365 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.

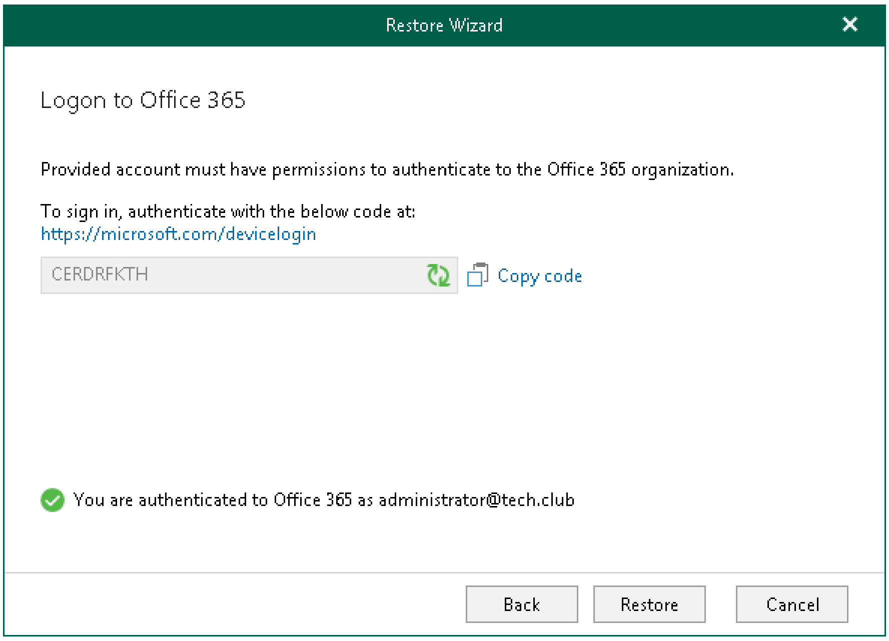
2. Click the link to the Microsoft portal.

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 required permissions assigned. For Veeam Explorer for Microsoft OneDrive for Business, required permissions are the same as for Veeam Explorer for Microsoft SharePoint. For more information, see Required Permissions.

   Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see Required Azure AD Application Settings.

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

CERDRFKTH

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

Restoring Multiple OneDrives

To restore multiple OneDrives, do the following:

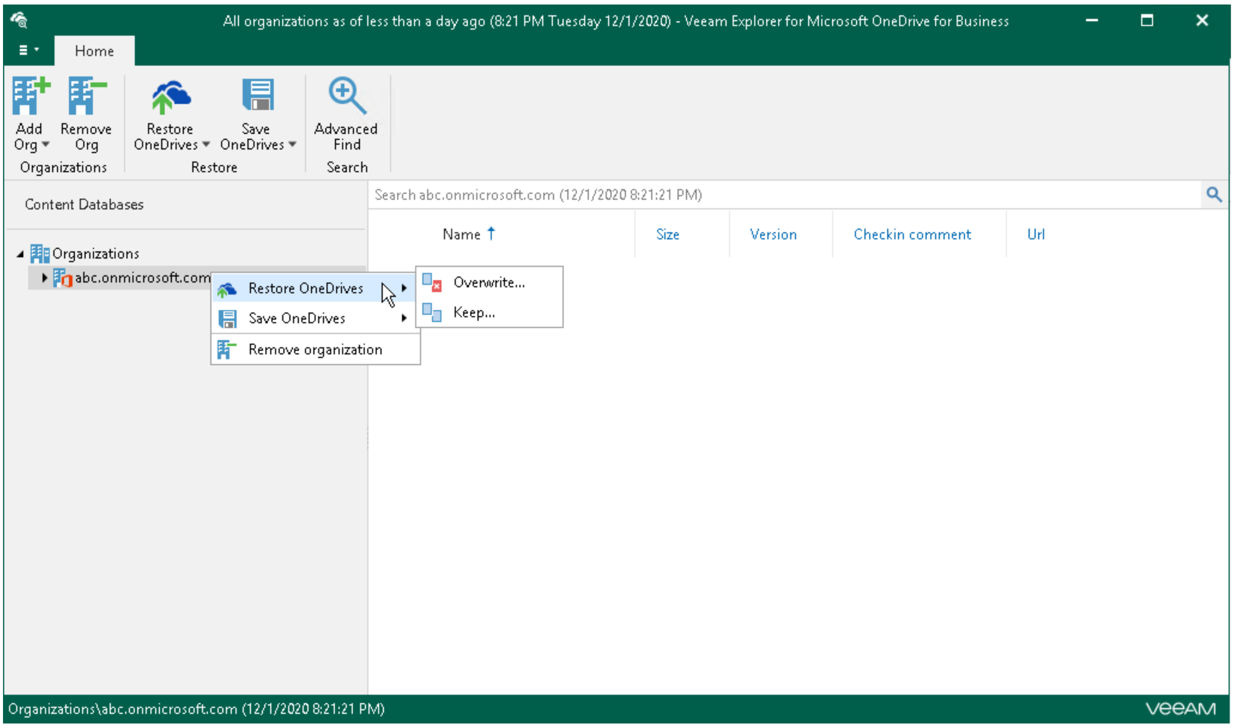
1. Launch the Restore wizard.
2. Select an authentication method.
3. Log in to Office 365.
4. Select OneDrives.

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. In the navigation pane, select an organization 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`).

Alternatively, in the navigation pane, right-click an organization with OneDrives and select **Restore OneDrives** > **Overwrite** or **Restore OneDrives** > **Keep**.



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:

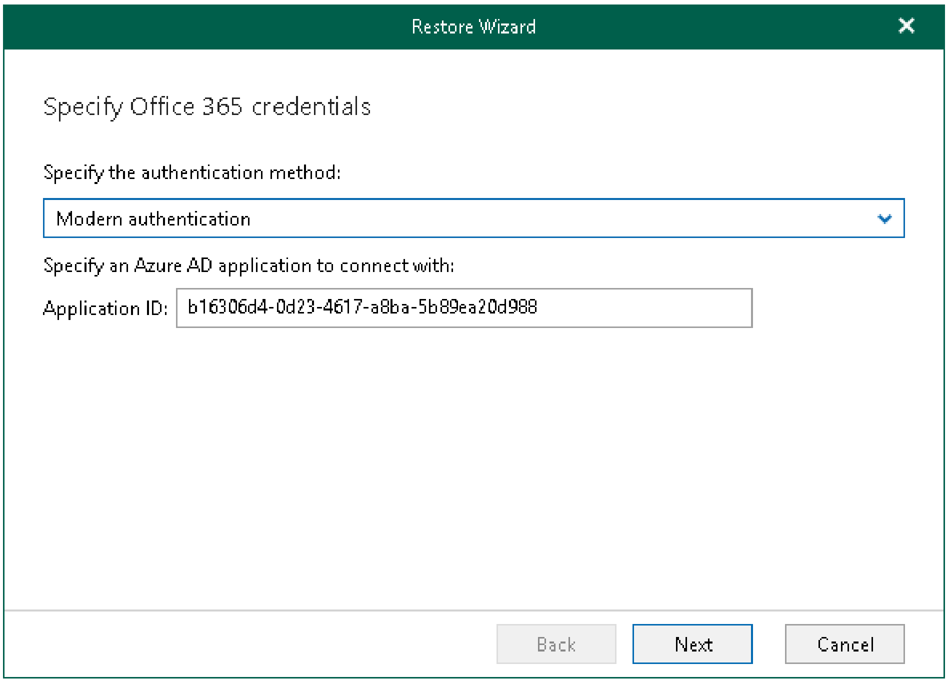
1. From the **Specify the authentication method** drop-down list, select *Modern authentication*.

   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 object 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 OneDrive for Business 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 the authentication method: Modern authentication

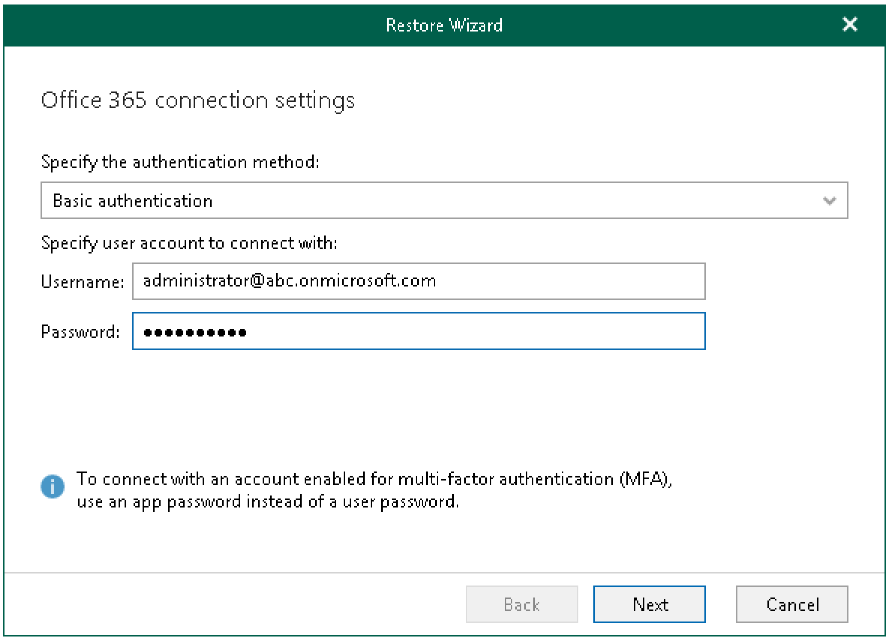
Specify an Azure AD application to connect with:

Application ID: b16306d4-0d23-4617-a8ba-5b89ea20d988

Basic Authentication

To use basic authentication, do the following:

1. From the **Specify the authentication method** drop-down list, select *Basic authentication*.
2. Enter credentials to connect to the SharePoint organization.



Office 365 connection settings

Specify the authentication method: Basic authentication

Specify user account to connect with:

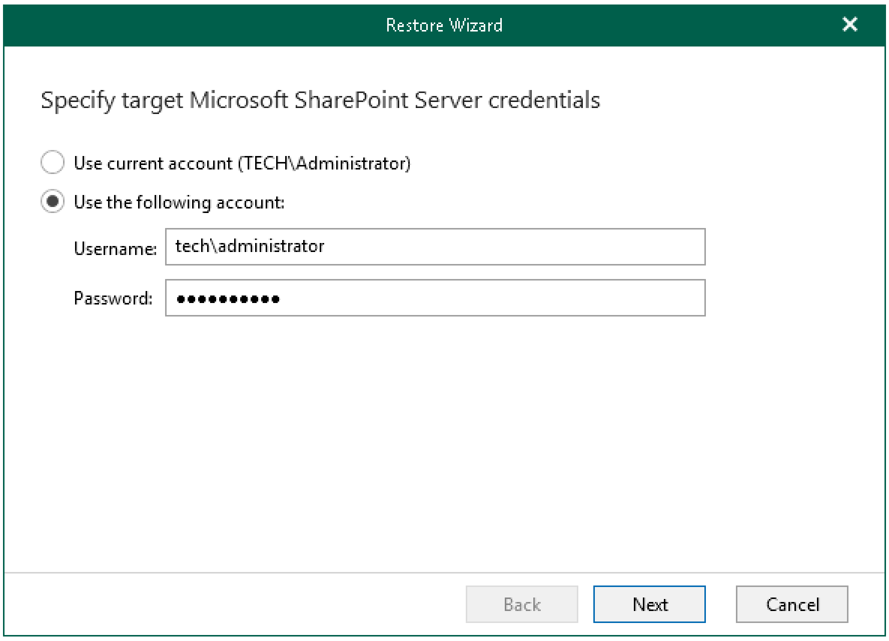
Username: administrator@abc.onmicrosoft.com

Password: ●●●●●●●●●●●

To connect with an account enabled for multi-factor authentication (MFA), use an app password instead of a user password.

On-Premises Organizations

To authenticate on an on-premises Microsoft SharePoint server, provide a user name and password.



Specify target Microsoft SharePoint Server credentials

○ Use current account (TECH\Administrator)

● Use the following account:

Username: tech\administrator

Password: ●●●●●●●●●●●

Step 3. Log In to Office 365

This step is only available if you have selected the *Modern authentication* option at the previous step of the wizard.

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

To sign in to the Microsoft Office 365 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.

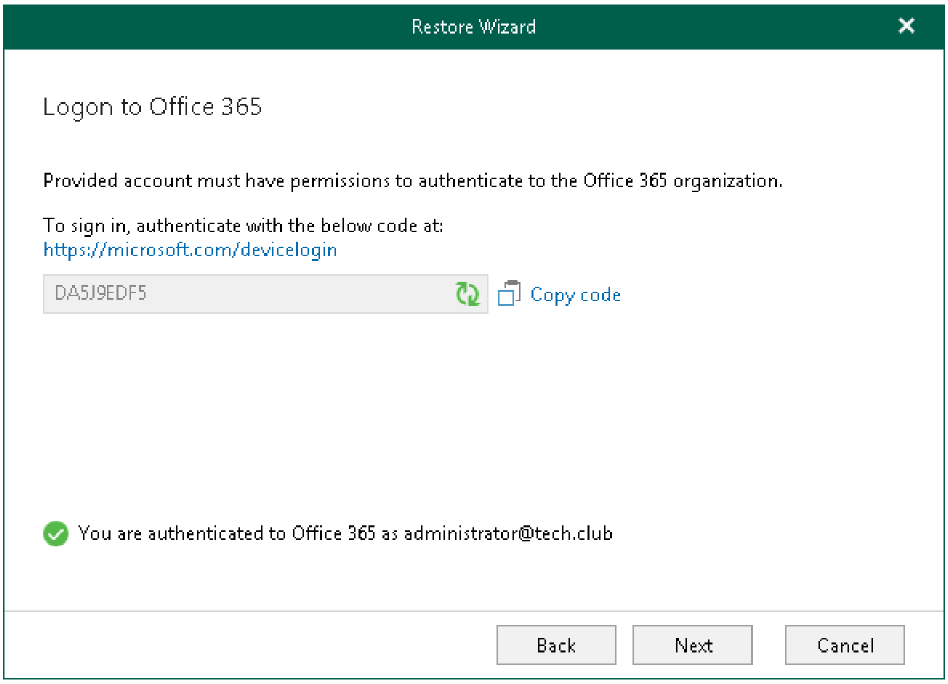
2. Click the link to the Microsoft portal.

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 required permissions assigned. For Veeam Explorer for Microsoft OneDrive for Business, required permissions are the same as for Veeam Explorer for Microsoft SharePoint. For more information, see Required Permissions.

   Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see Required Azure AD Application Settings.

4. Return to the **Restore Wizard** window and click **Next**.



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

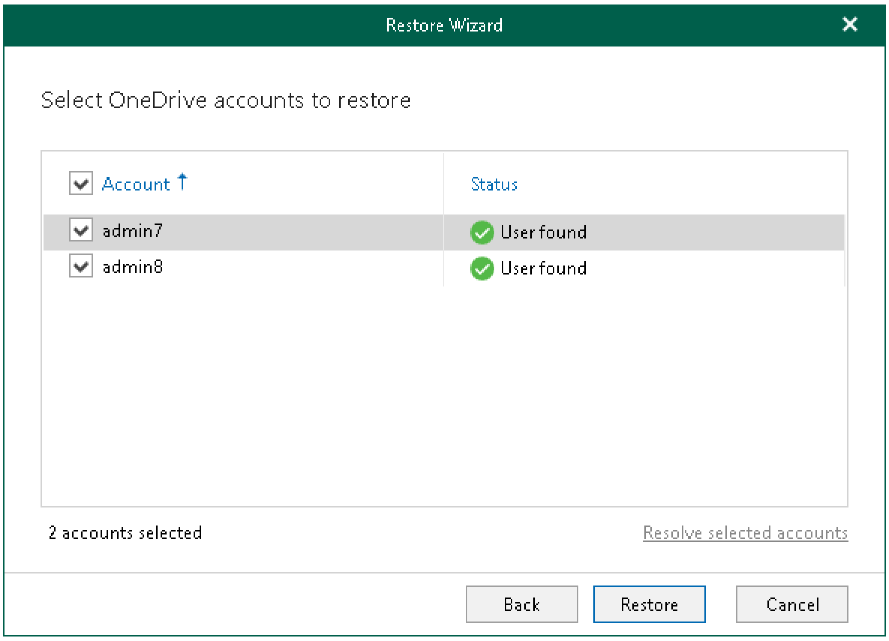
DA5J9EDF5

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

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 user accounts whose OneDrives you want to restore exist, click **Resolve selected accounts**.



Select OneDrive accounts to restore

☑ Account ↑	Status
☑ admin7	✓ User found
☑ admin8	✓ User found

2 accounts selected

Copy

This section explains how to copy OneDrive data to a different location.

To copy OneDrive data to the same or different user, do the following:

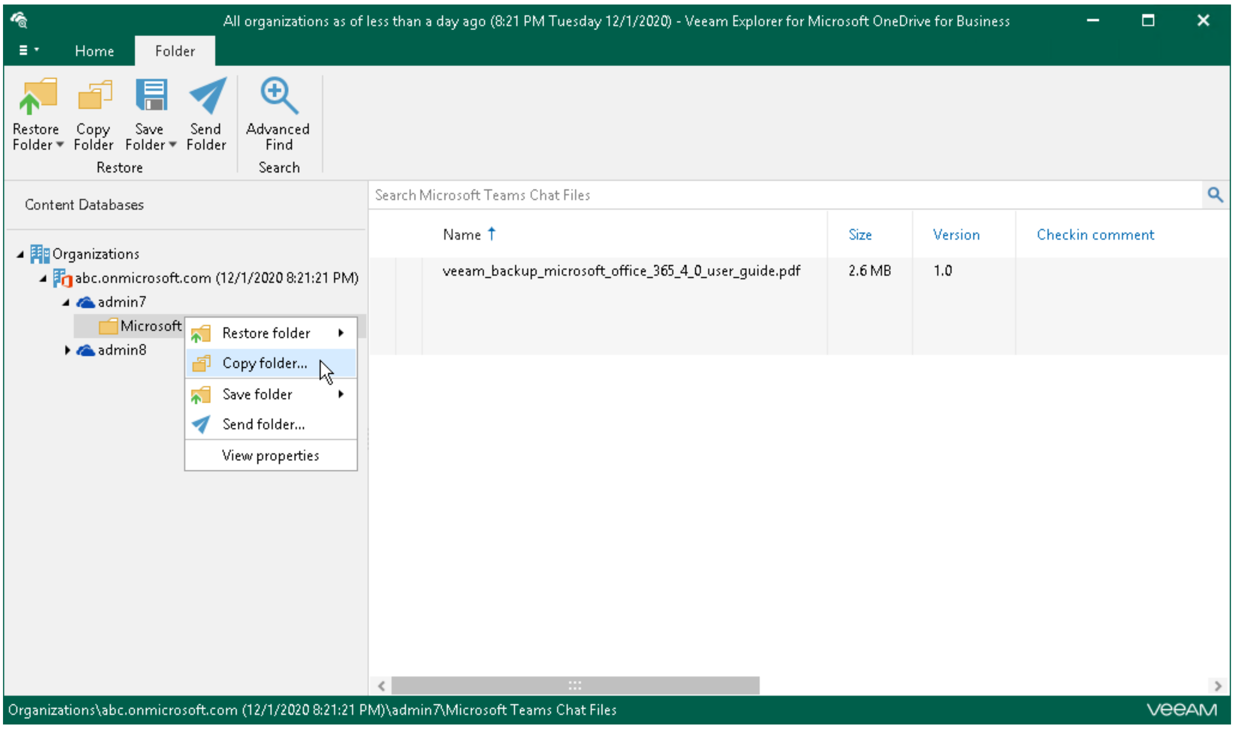
1. Launch the Restore wizard.
2. Select an authentication method.
3. Log in to Office 365.
4. Specify a target user.
5. Specify a target folder.
6. Specify restore options.

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

1. Select an object that you want to copy:
   - To copy OneDrive, select the necessary OneDrive in the inventory pane.
   - To copy a folder, select the necessary folder in the inventory pane.
   - To copy a document, select a folder that contains the document in the inventory pane and select the document in the preview pane.
2. On the **OneDrive/Folder/Document** tab, click **Copy OneDrive**/**Copy Folder**/**Copy Document**.

Alternatively, right-click an object and select **Copy OneDrive**/**Copy folder**/**Copy document**.


All organizations as of less than a day ago (8:21 PM Tuesday 12/1/2020) - Veeam Explorer for Microsoft OneDrive for Business

Organizations\abc.onmicrosoft.com (12/1/2020 8:21:21 PM)\admin7\Microsoft Teams Chat Files

Name	Size	Version	Checkin comment
veeam_backup_microsoft_office_365_4_0_user_guide.pdf	2.6 MB	1.0	

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:

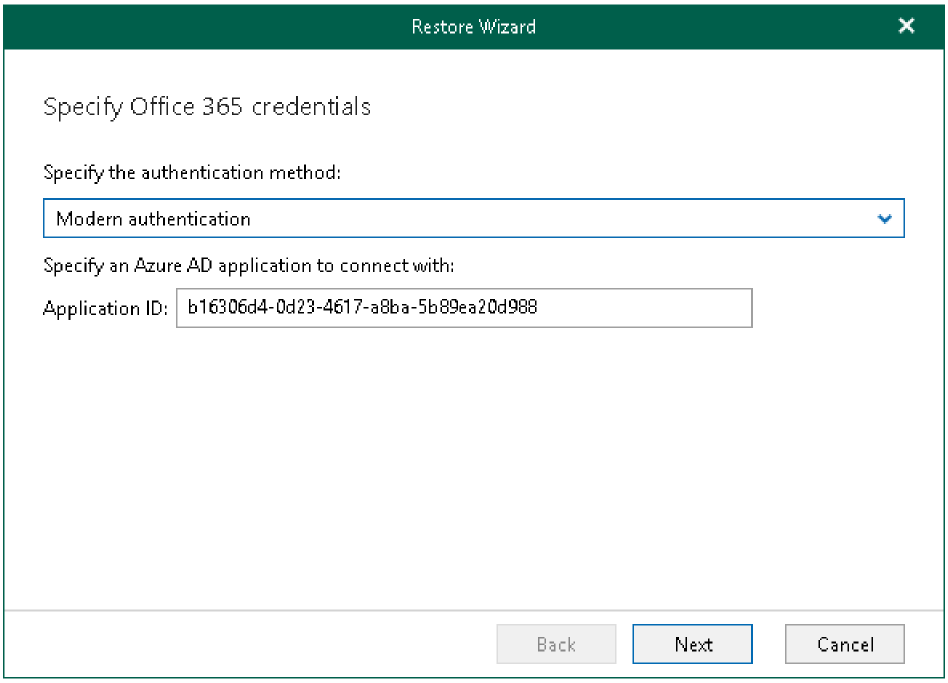
1. From the **Specify authentication method** drop-down list, select *Modern authentication*.

   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 object 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 OneDrive for Business 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 the authentication method:

Modern authentication

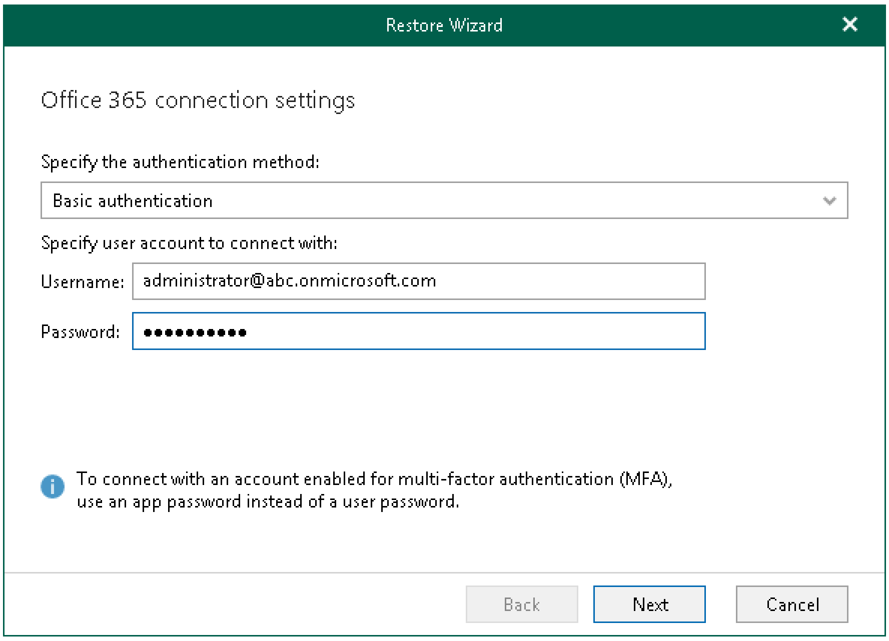
Specify an Azure AD application to connect with:

Application ID: b16306d4-0d23-4617-a8ba-5b89ea20d988

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.



Office 365 connection settings

Specify the authentication method: Basic authentication

Specify user account to connect with:

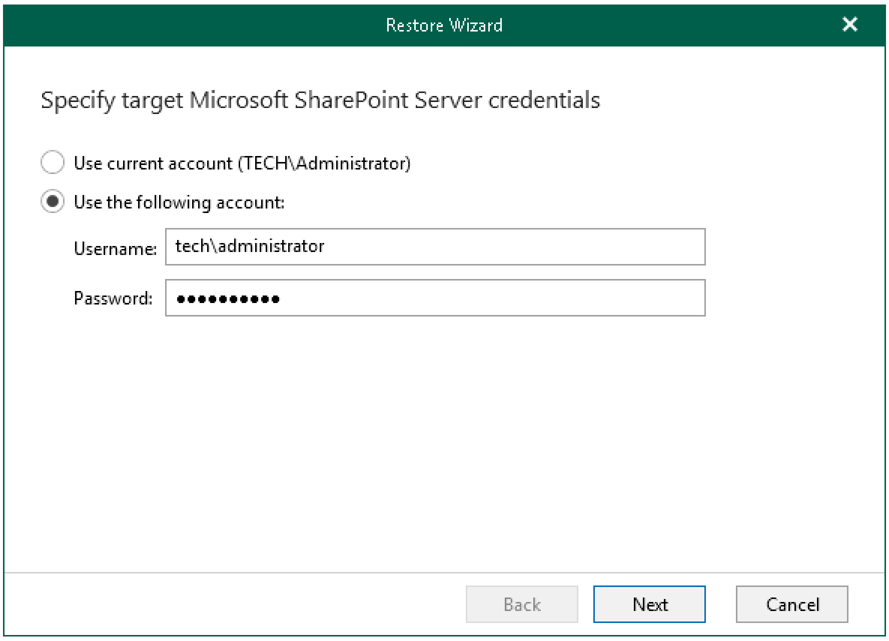
Username: administrator@abc.onmicrosoft.com

Password: ●●●●●●●●●●●

To connect with an account enabled for multi-factor authentication (MFA), use an app password instead of a user password.

On-Premises Organizations

To authenticate on an on-premises Microsoft SharePoint server, provide a user name and password.



Specify target Microsoft SharePoint Server credentials

○ Use current account (TECH\Administrator)

● Use the following account:

Username: tech\administrator

Password: ●●●●●●●●●●●

Step 3. Log In to Office 365

This step is only available if you have selected the *Modern authentication* option at the previous step of the wizard.

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

To sign in to the Microsoft Office 365 organization, do the following:

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

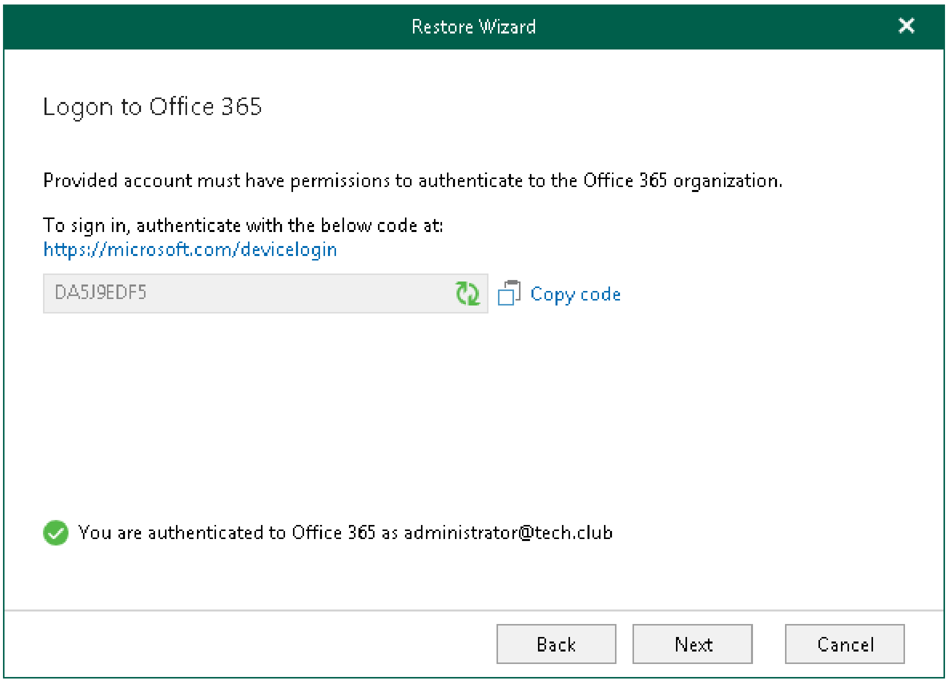
   Mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.

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**.



Logon to Office 365

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

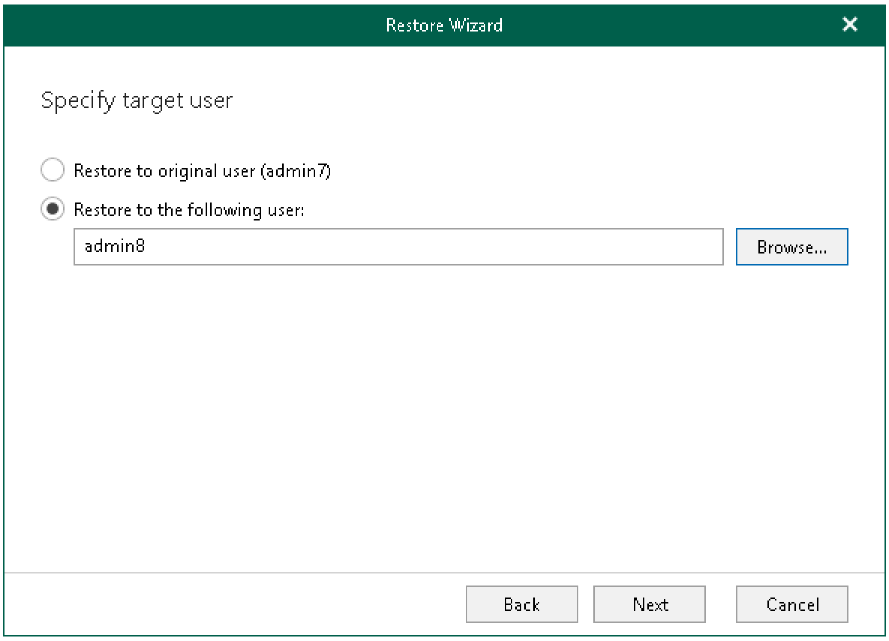
To sign in, authenticate with the below code at:
https://microsoft.com/devicelogin

DA5J9EDF5

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

Step 4. Specify Target User

At this step of the wizard, specify a target user where you want to copy data.



Specify target user

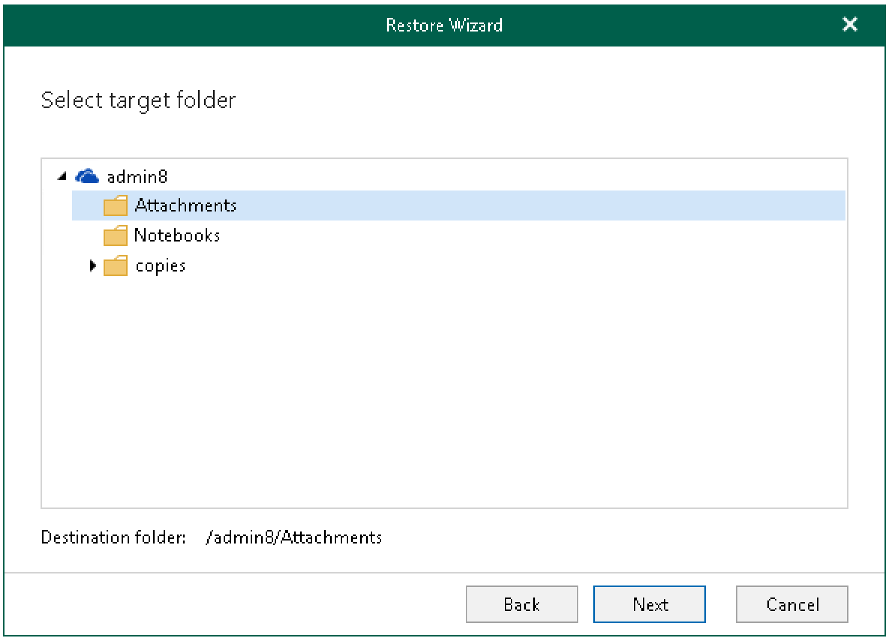
○ Restore to original user (admin7)

● Restore to the following user:

admin8

Step 5. Specify Target Folder

At this step of the wizard, specify the target directory to which you want to copy data.



Destination folder: /admin8/Attachments

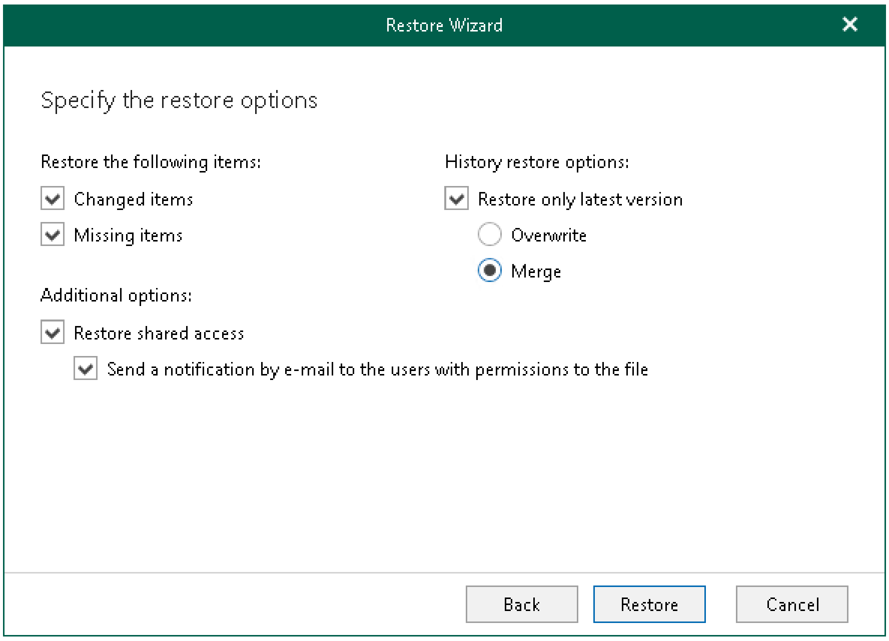
Step 6. Specify Restore Options

At this step of the wizard, select restore options and click **Restore**.

You can select the following options:

- **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.



Restore Wizard

Specify the restore 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

Saving Microsoft OneDrives

Veeam Explorer for Microsoft OneDrive for Business allows you to save OneDrive content to the specified location.

To save OneDrive data, do the following:

1. Choose what data you want to save:

   - If you want to save data of multiple OneDrives, select an organization with OneDrives in the inventory pane, click **Save OneDrives** on the **Home** tab and select how you want to save data:

     - **Save as files**. Select this option if you want to save each file separately to a specified location.

     - **Save as ZIP**. Select this option if you want to add saved files to a ZIP archive and save the resulting archive to a specified location. Veeam Explorer for Microsoft OneDrive for Business will save files to an archive with the *archive.zip* name.

     Alternatively, in the inventory pane, right-click an organization with OneDrives and select **Save OneDrives** > **Save as files** or **Save OneDrives** > **Save as ZIP**.

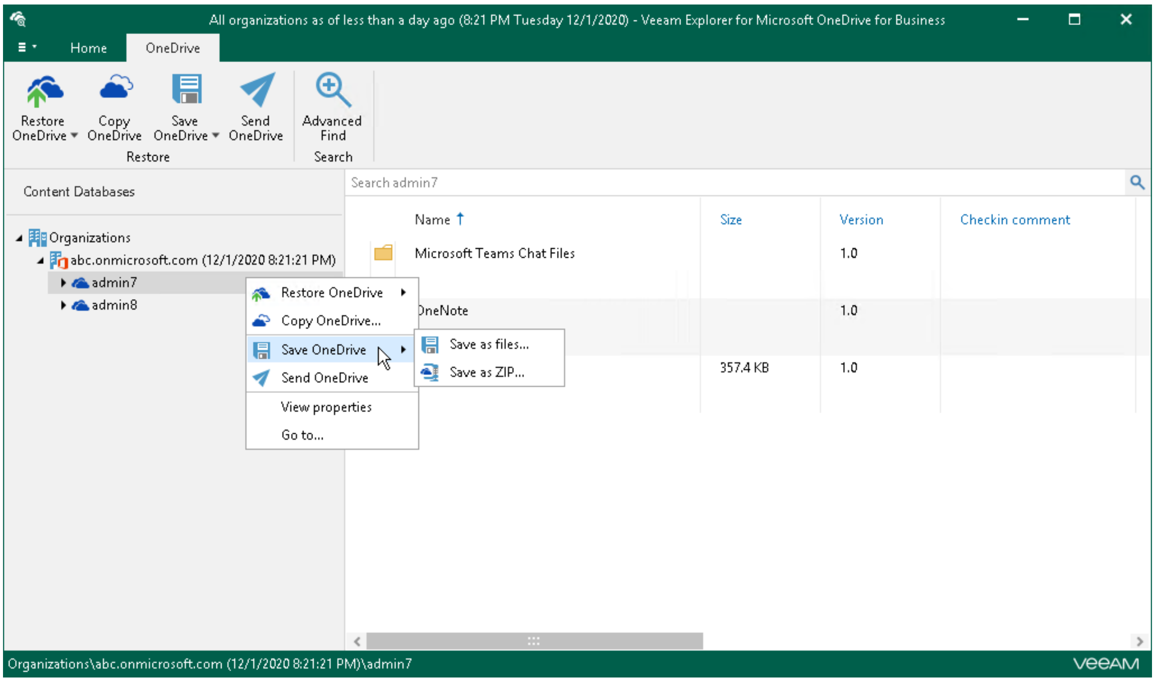
     To specify what data to save and where to save data, follow the steps of the **Save OneDrives** wizard as described in the steps 2-3 of this procedure.

   - If you want to save data of specific OneDrive, select OneDrive in the inventory pane, click **Save OneDrive** on the **OneDrive** tab and select how you want to save data:

     - **Save as files**. Select this option if you want to save each file separately to a specified location. To specify a location, in the displayed window, browse to the necessary folder and click **Select Folder**.

     - **Save as ZIP**. Select this option if you want to add saved files to a ZIP archive and save the resulting archive to a specified location. To specify a location, in the displayed window, browse to the necessary folder and click **Save**. Veeam Explorer for Microsoft OneDrive for Business will save files to an archive with the *archive.zip* name in this folder.

     Alternatively, in the inventory pane, right-click OneDrive and select **Save OneDrive** > **Save as files** or **Save OneDrive** > **Save as ZIP**.

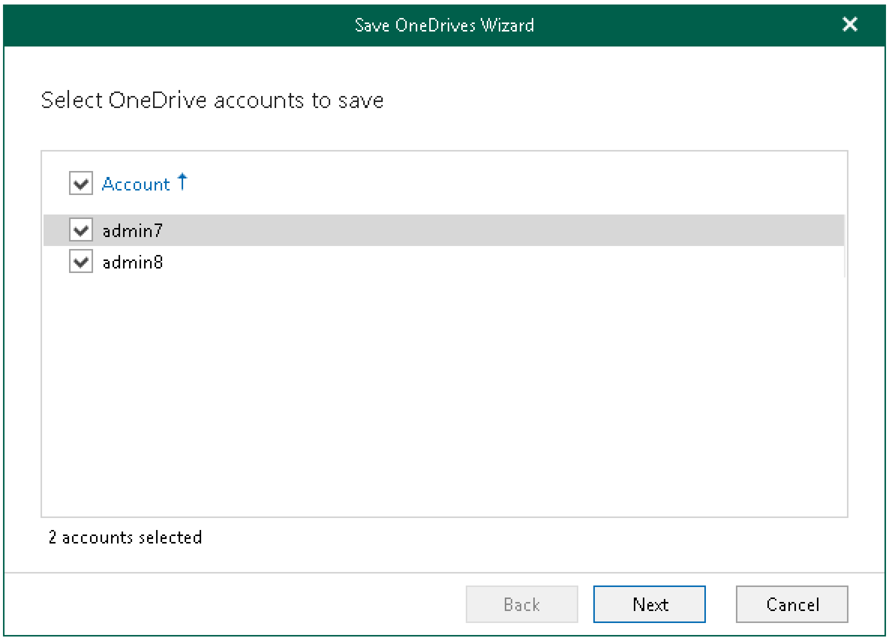


All organizations as of less than a day ago (8:21 PM Tuesday 12/1/2020) - Veeam Explorer for Microsoft OneDrive for Business

Name	Size	Version	Checkin comment
Microsoft Teams Chat Files		1.0	
OneNote		1.0	
	357.4 KB	1.0	

Organizations\abc.onmicrosoft.com (12/1/2020 8:21:21 PM)\admin7

2. [For multiple OneDrives] In the **Save OneDrives** wizard, select OneDrive accounts to save.



Save OneDrives Wizard

Select OneDrive accounts to save

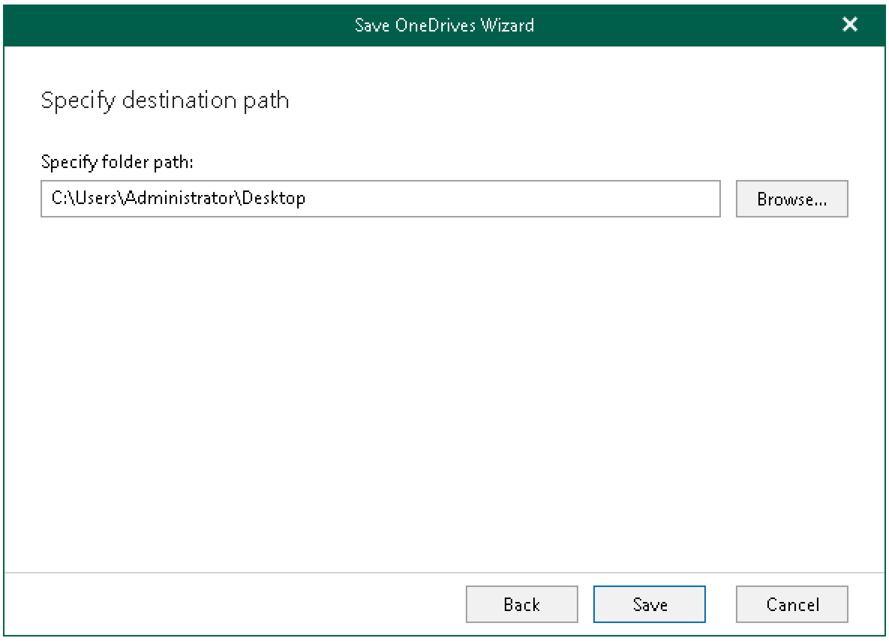
☑ Account ↑

☑ admin7

☑ admin8

2 accounts selected

3. [For multiple OneDrives] Specify a directory where to save OneDrive data and click **Save**.



Save OneDrives Wizard

Specify destination path

Specify folder path: C:\Users\Administrator\Desktop

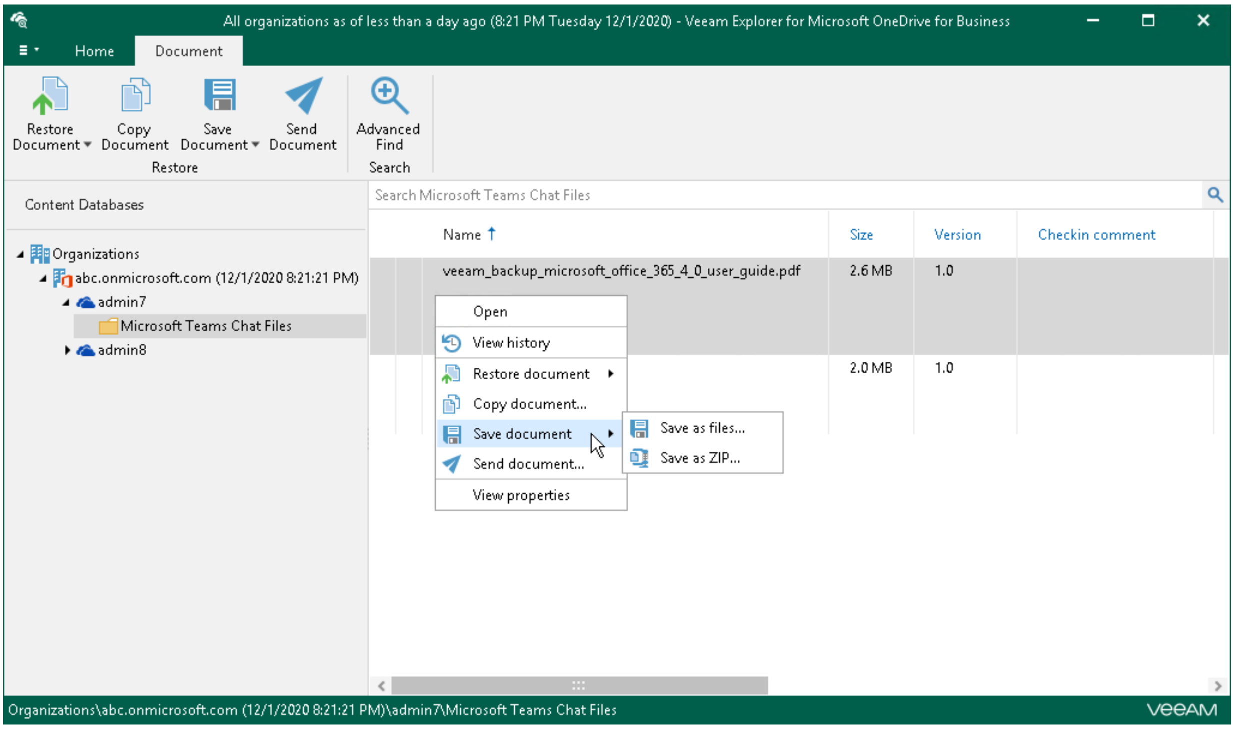
Saving Microsoft OneDrive Documents and Folders

Veeam Explorer for Microsoft OneDrive for Business allows you to save documents and folders located in Microsoft OneDrive to a specified location.

To save a document or folder, do the following:

1. Select an object that you want to save.
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 as files**.

   Select **Save as ZIP** to save OneDrive documents and/or folders to an archive file in the ZIP format.
3. Specify the destination folder and click **Select Folder**.



All organizations as of less than a day ago (8:21 PM Tuesday 12/1/2020) - Veeam Explorer for Microsoft OneDrive for Business

Search Microsoft Teams Chat Files

Name	Size	Version	Checkin comment
veeam_backup_microsoft_office_365_4_0_user_guide.pdf	2.6 MB	1.0	
	2.0 MB	1.0	

Organizations\abc.onmicrosoft.com (12/1/2020 8:21:21 PM)\admin7\Microsoft Teams Chat Files

Sending Microsoft OneDrive Data

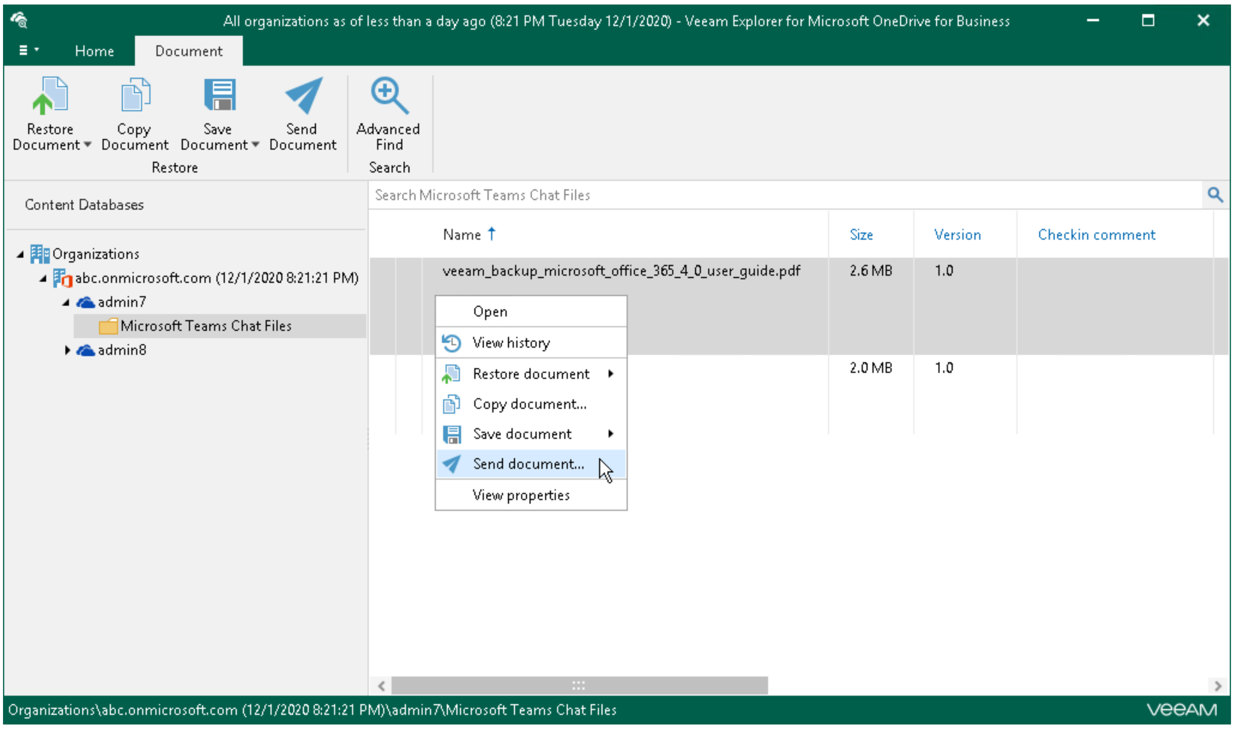
Veeam Explorer for Microsoft OneDrive for Business allows you to send OneDrive data to specified recipients by email.

> **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 data by email, do the following:

1. Select OneDrive, folder or document that you want to send and do either of the following:
   - To send OneDrive, on the **OneDrive** tab, click **Send OneDrive**.
   - To send a folder, on the **Folder** tab, click **Send Folder**.
   - To send a document, on the **Document** tab, click **Send Document**.

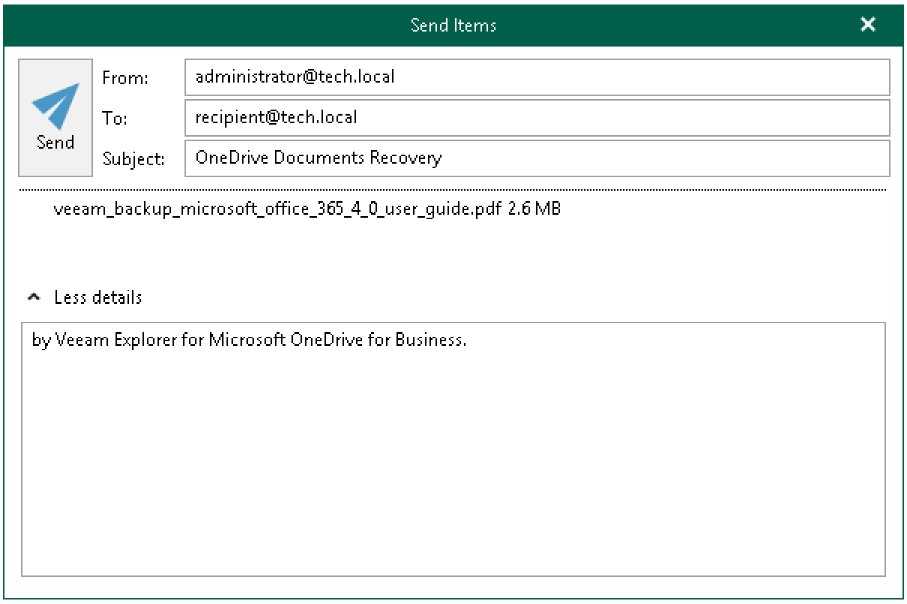
   Alternatively, right-click an object that you want to send and select **Send OneDrive/Send folder/Send document**.


All organizations as of less than a day ago (8:21 PM Tuesday 12/1/2020) - Veeam Explorer for Microsoft OneDrive for Business
Home
Document
Restore Document
Copy Document
Save Document
Send Document
Advanced Find
Restore
Search
Content Databases
Organizations
abc.onmicrosoft.com (12/1/2020 8:21:21 PM)
admin7
Microsoft Teams Chat Files
admin8
Search Microsoft Teams Chat Files
Name
Size
Version
Checkin comment
veeam_backup_microsoft_office_365_4_0_user_guide.pdf
2.6 MB
1.0
2.0 MB
1.0
Open
View history
Restore document
Copy document...
Save document
Send document...
View properties
Organizations\abc.onmicrosoft.com (12/1/2020 8:21:21 PM)\admin7\Microsoft Teams Chat Files
veeam

2. In the **Send Items** window, 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**.



From: administrator@tech.local

To: recipient@tech.local

Subject: OneDrive Documents Recovery

veeam_backup_microsoft_office_365_4_0_user_guide.pdf 2.6 MB

by Veeam Explorer for Microsoft OneDrive for Business.

Veeam Explorer for Microsoft Teams

Veeam Explorer for Microsoft Teams allows you to restore Microsoft Teams 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

Continue with this section to learn how to configure your environment before start using Veeam Explorer for Microsoft Teams:

Required Permissions

The following table lists required permissions for data restore.

Operation	Required Roles and Permissions
Restore to Microsoft Office 365	• The user account must have a Microsoft Office 365 license that permits access to Microsoft Teams API. The minimum sufficient license is Microsoft Teams Exploratory experience. • To restore Microsoft Teams data, the user account must have the *Teams Service Administrator* role. • For data restore using an Azure AD application, make sure that the required settings are specified for the Azure AD application used for restore. For more information, see Required Azure AD Application Settings.

Considerations and Limitations

This section covers considerations and known limitations of Veeam Explorer for Microsoft Teams.

Data Restore

Consider the following when planning to restore Microsoft Teams data:

- Use of modern authentication with legacy protocols allowed is not supported for data restore with Veeam Explorer for Microsoft Teams.
- You can restore Microsoft Teams data to the original organization only.
- Veeam Explorer for Microsoft Teams does not change roles for team owners during restore. For example, you create a backup of your organization, and then change role for a team member from *Member* to *Owner*. In this case, if you restore this team member from the backup, Veeam Explorer for Microsoft Teams will not set their role to *Member*.
- Restore of OneNote notebooks from backups of Microsoft Teams data for organizations with enabled security defaults using multi-factor authentication is not supported.
- When restoring a channel tab, Veeam Explorer for Microsoft Teams does not preserve relation between the link to a file published on the tab and the file itself. You will need to link the tab to the file manually after restore. This limitation does not apply to the scenario where you restore an entire team.
- Veeam Explorer for Microsoft Teams does not restore posts to their original location in the team channel. Instead, Veeam Explorer for Microsoft Teams exports posts to a file of the HTML format, creates a separate tab in the original channel and attaches the HTML file to this tab.

Launching Application and Exploring Backups

To open Veeam Explorer for Microsoft Teams and load backups, do either of the following:

- Use the **Explore** option. For more information, see Data Restore.

  When loading backups located in object storage repositories, Veeam Explorer for Microsoft Teams 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 disable these notifications, clear the **Show pop-up notifications on startup** check box, as described in Configuring Advanced Settings.

- Go to **Start** and click **Veeam Explorer for Microsoft Teams**.

  When you open Veeam Explorer for Microsoft Teams from the **Start** menu, all backed-up databases will be loaded automatically.

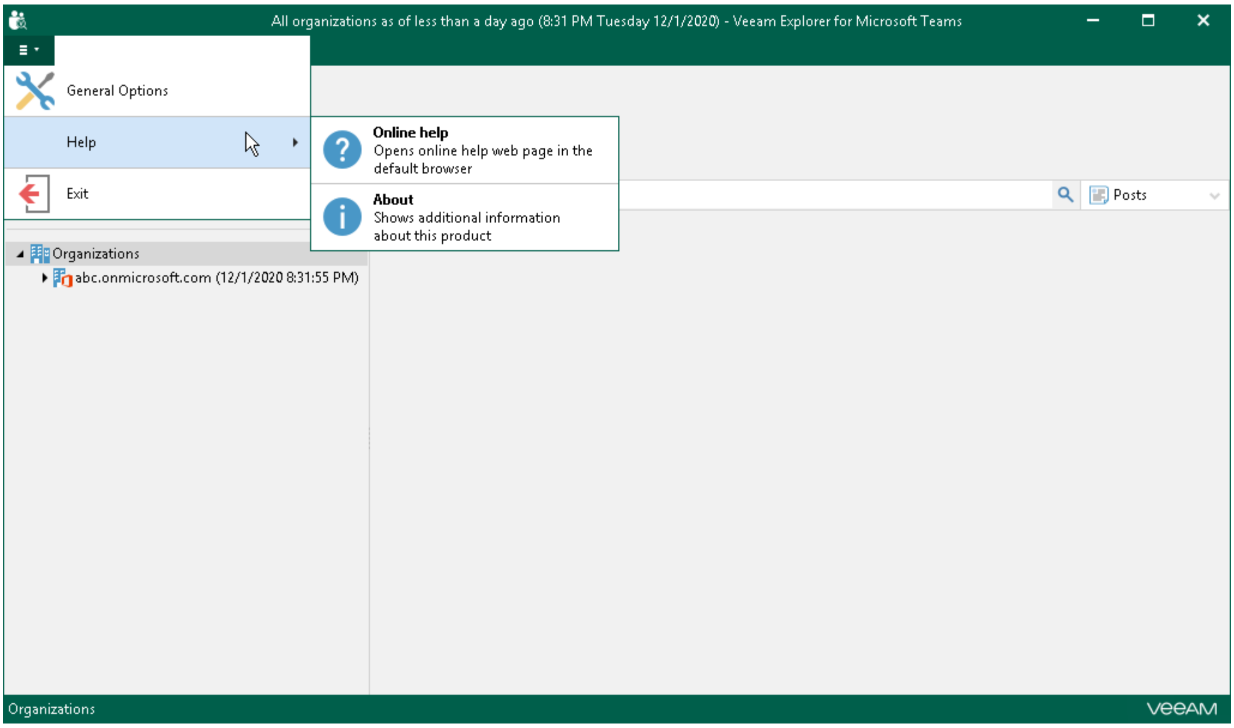
Understanding User Interface

Veeam Explorer for Microsoft Teams 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. For more information, see General Application Settings.
- **Help**.
  - **Online help**. Opens the online web help page.
  - **About**. Shows current product information.
- **Exit**. Closes the program.



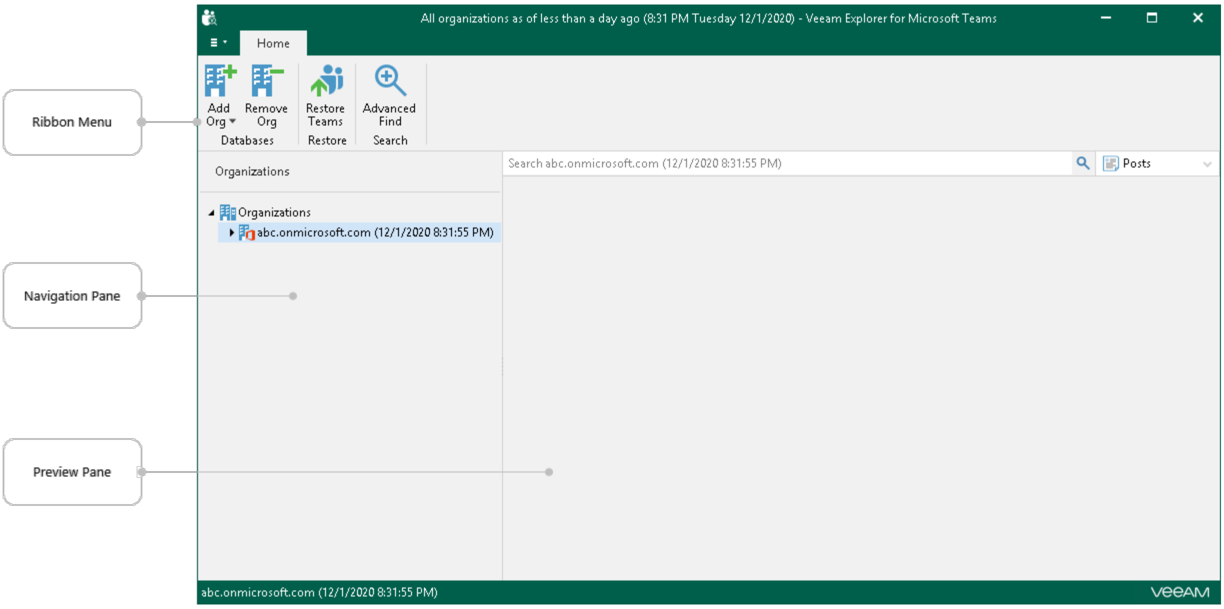
All organizations as of less than a day ago (8:31 PM Tuesday 12/1/2020) - Veeam Explorer for Microsoft Teams

General Options
Help
Exit
Online help
Opens online help web page in the default browser
About
Shows additional information about this product
Posts
Organizations
abc.onmicrosoft.com (12/1/2020 8:31:55 PM)
Organizations
veeam

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 pane, 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 pane.


Ribbon Menu
Navigation Pane
Preview Pane
All organizations as of less than a day ago (8:31 PM Tuesday 12/1/2020) - Veeam Explorer for Microsoft Teams
Home
Add Org
Remove Org
Databases
Restore Teams
Restore
Advanced Find
Search
Organizations
Organizations
abc.onmicrosoft.com (12/1/2020 8:31:55 PM)
Search abc.onmicrosoft.com (12/1/2020 8:31:55 PM)
Posts
abc.onmicrosoft.com (12/1/2020 8:31:55 PM)
veeam

Browsing, Searching and Viewing Items

Continue with this section to learn about the following operations with the backed-up data:

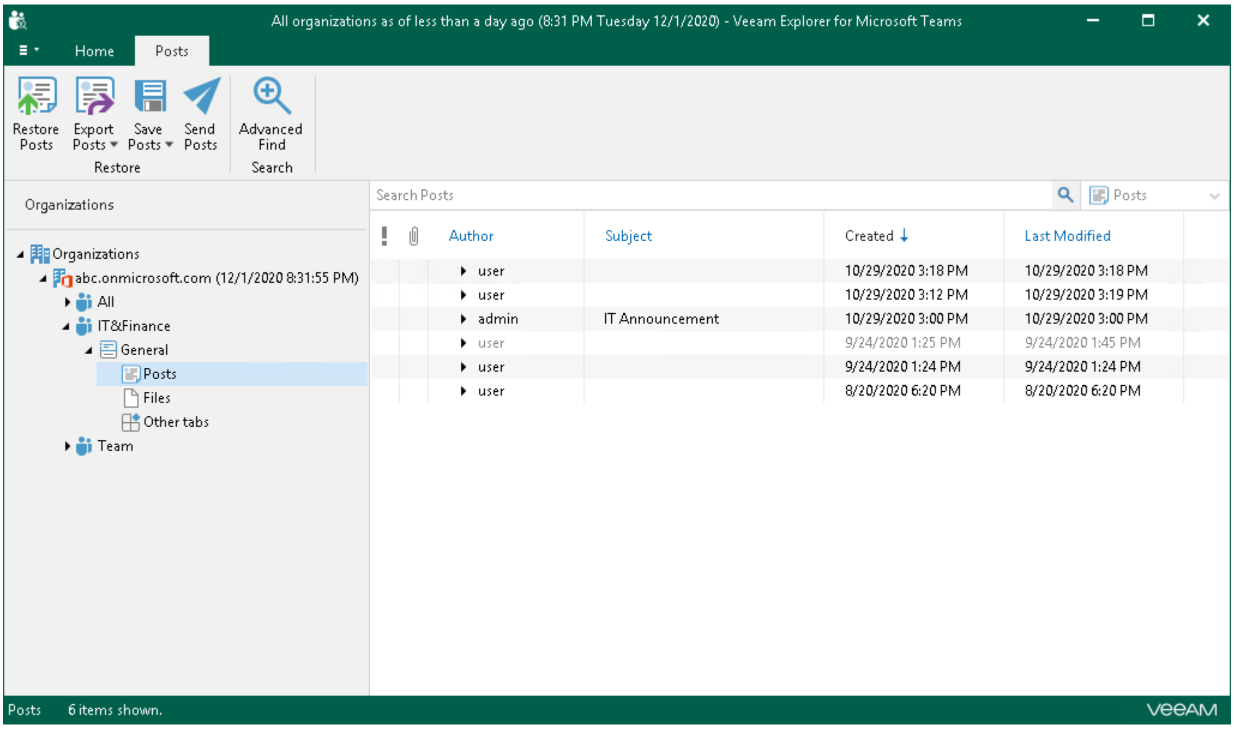
- Browsing backup content
- Viewing team properties
- Opening posts and files
- Searching for objects in a backup file
- Using the advanced search capabilities

Browsing Backups

To view the contents of a backup file, you use the navigation pane which displays the database structure containing your Microsoft Teams objects: teams, channels and channel tabs. Veeam Explorer for Microsoft Teams groups channel tabs in the following nodes of the navigation pane:

- **Posts**. Contains the *Posts* tab of the channel.
- **Files**. Contains the *Files* tab of the channel.
- **Other tabs**. Contains other tabs of the channel that link to sites, documents, applications, and so on.

After you select an object in the navigation pane, you can see its content in the preview pane.



All organizations as of less than a day ago (8:31 PM Tuesday 12/1/2020) - Veeam Explorer for Microsoft Teams

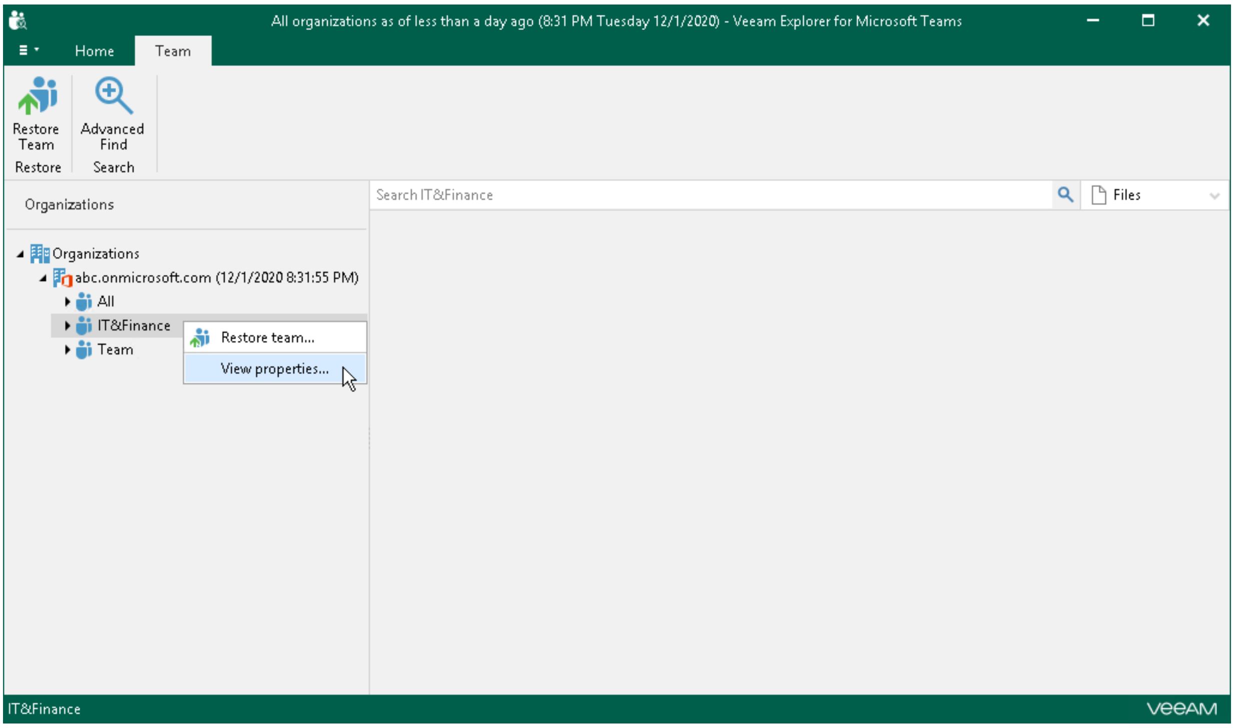
!		Author	Subject	Created ↓	Last Modified
		user		10/29/2020 3:18 PM	10/29/2020 3:18 PM
		user		10/29/2020 3:12 PM	10/29/2020 3:19 PM
		admin	IT Announcement	10/29/2020 3:00 PM	10/29/2020 3:00 PM
		user		9/24/2020 1:25 PM	9/24/2020 1:45 PM
		user		9/24/2020 1:24 PM	9/24/2020 1:24 PM
		user		8/20/2020 6:20 PM	8/20/2020 6:20 PM

Posts 6 items shown.

Viewing Team Properties

You can view properties of a backed-up team. This may be useful, for example, in case you want to decide whether to restore team properties during restore of a team.

To view team properties, in the navigation pane, right-click a necessary team and select **View properties**.



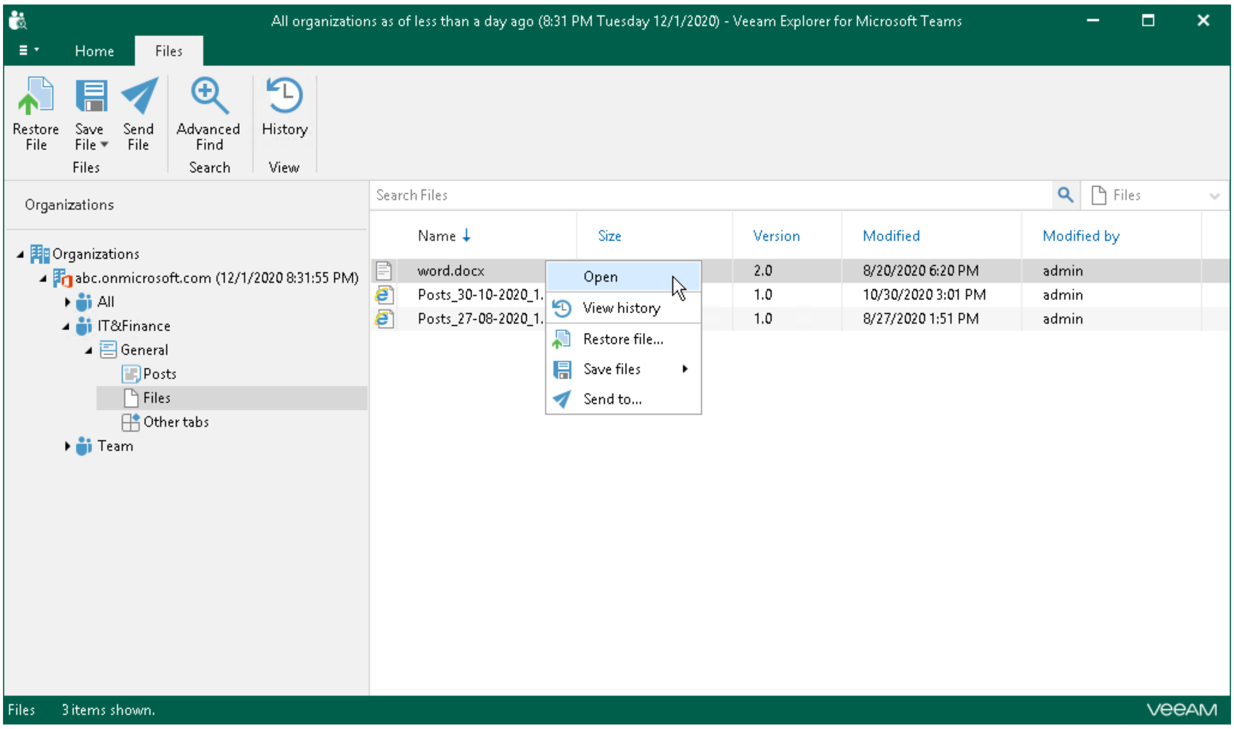
Opening Posts and Files

You can use Veeam Explorer for Microsoft Teams to open backed-up posts and files.

To open a post or file, do the following:

1. In the navigation pane, browse to the channel whose post or file you want to open and click the necessary node: **Posts** or **Files**.

2. In the preview pane, right-click a post or file and select **Open**.



Name	Size	Version	Modified	Modified by
word.docx		2.0	8/20/2020 6:20 PM	admin
Posts_30-10-2020_1.		1.0	10/30/2020 3:01 PM	admin
Posts_27-08-2020_1.		1.0	8/27/2020 1:51 PM	admin

Searching for Objects

The search mechanism allows you to find items (posts, files and tabs) matching specified search criteria.

To search for required items, do the following:

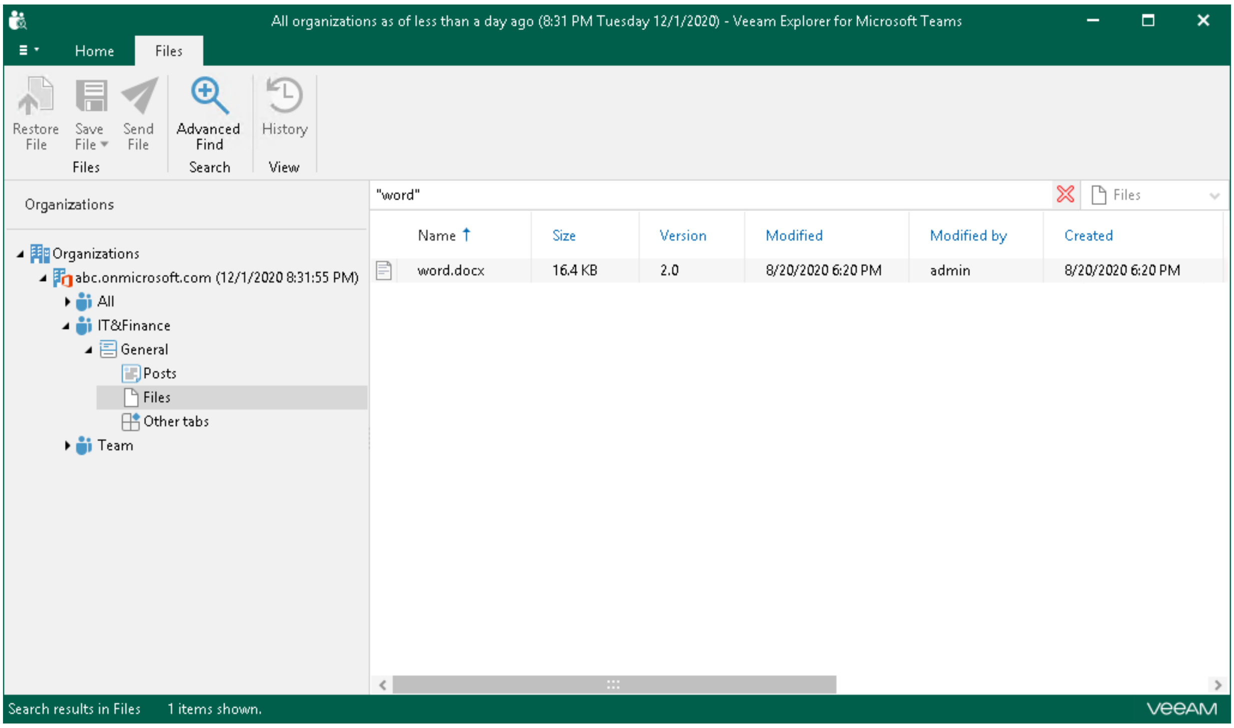
1. In the navigation pane, select a node that contains an item you want to find: **Posts**, **Files** or **Other tabs**.

   Alternatively, in the navigation pane, select a team or channel whose items you want to find. Then, from the drop-down list next to the search field, select what type of items you want to find: *Files*, *Posts* or *Other tabs*.

2. Enter a search query to the search field.

> **NOTE:**
>
> To find the exact phrase, use double quotes. For example, *"Document"*.

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 *?*.



All organizations as of less than a day ago (8:31 PM Tuesday 12/1/2020) - Veeam Explorer for Microsoft Teams

"word"

Name	Size	Version	Modified	Modified by	Created
word.docx	16.4 KB	2.0	8/20/2020 6:20 PM	admin	8/20/2020 6:20 PM

Search results in Files 1 items shown.

Using Advanced Find Capabilities

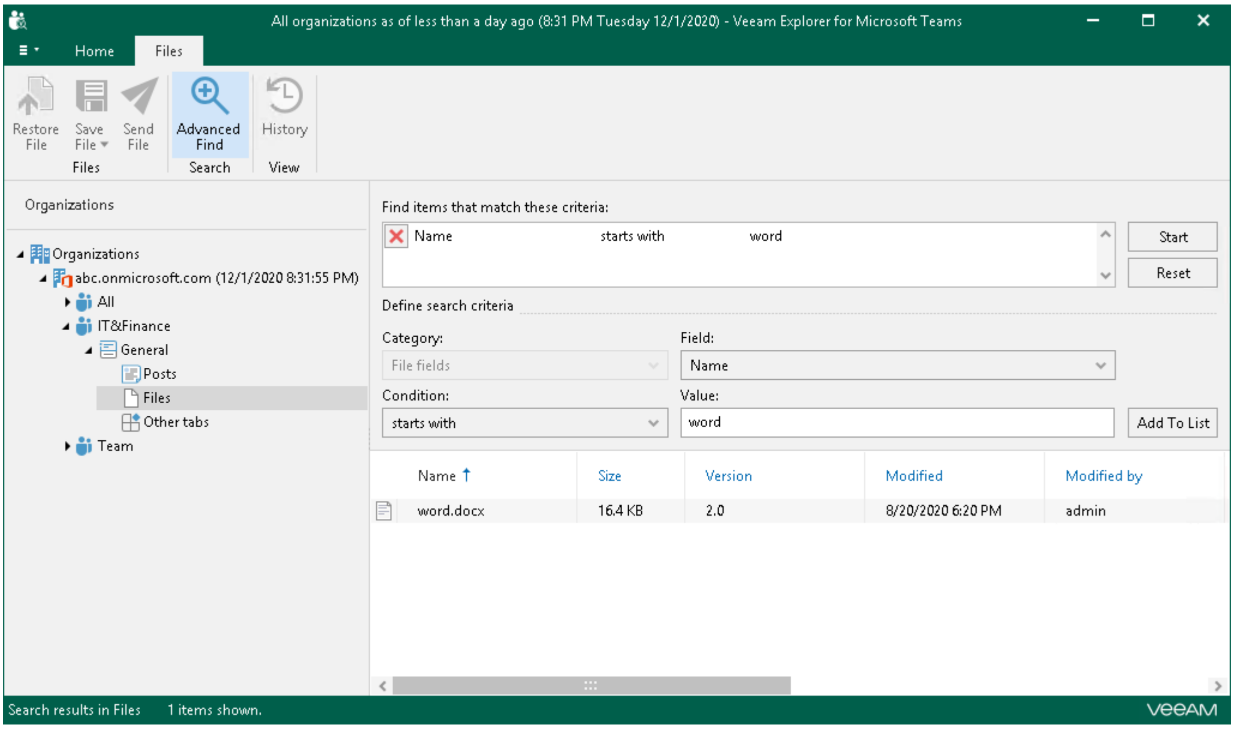
The **Advanced Find** mechanism allows you to define your search criteria more precisely.

> **NOTE:**
>
> The **Advanced Find** mechanism is supported for posts and files only. The mechanism is not supported for tabs.

For example, to find a file whose name starts with *"word"*, do the following:

1. In the preview pane, select a node that contains objects you want to find and click **Advanced Find** on the ribbon.
2. In the **Define search criteria** section, select **Category** > **File fields**.
3. In the **Field** list, select **Name**.
4. In the **Condition** list, select **starts with**.
5. In the **Value** field, specify a file name.
6. Click **Add To List**, then click **Start**.

To remove a filter, click the cross mark next to it. To remove all configured filters, click **Reset**.



Find items that match these criteria:

☒ Name starts with word

Define search criteria

Category: File fields

Field: Name

Condition: starts with

Value: word

Name ↑	Size	Version	Modified	Modified by
word.docx	16.4 KB	2.0	8/20/2020 6:20 PM	admin

General Application Settings

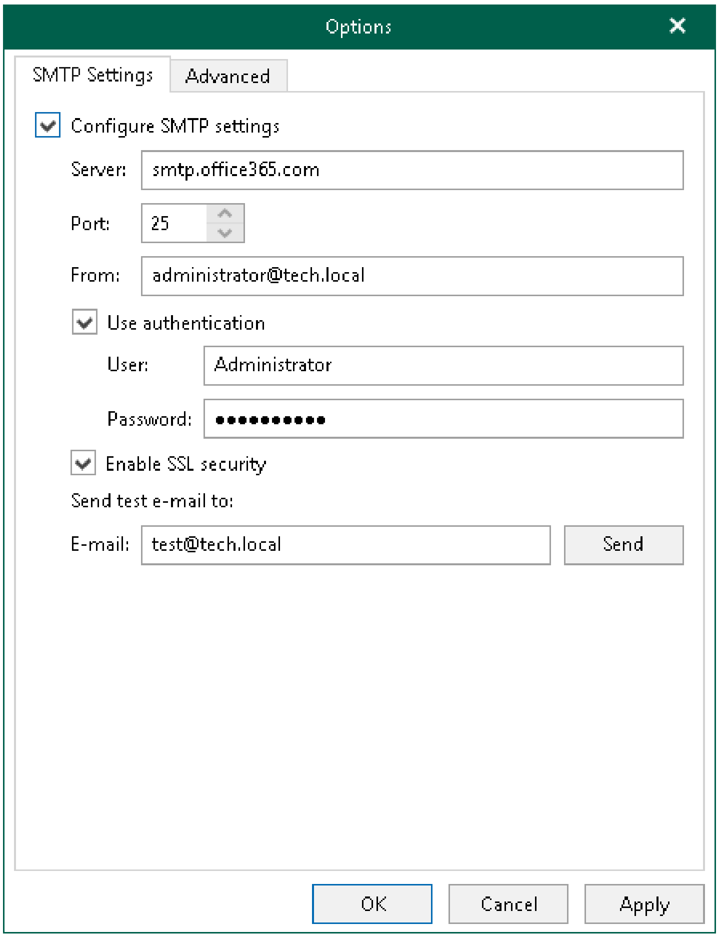
Continue with this section to learn more about configuring general application settings and components.

SMTP Settings

To send Microsoft Teams 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 Microsoft Teams posts or files. For more information, see Sending Posts and Files.
   - Select the **Use authentication** check box If your SMTP server requires SMTP authentication for outgoing mail and provide valid credentials.
   - Select the **Enable SSL security** check box to enable SSL data encryption.
3. In the **Send test e-mail to** section, specify the recipient email address and click **Send** to send a test email message.
4. Click **Apply**.



☑ Configure SMTP settings

Server: smtp.office365.com

Port: 25

From: administrator@tech.local

☑ Use authentication

User: Administrator

Password: ●●●●●●●●●●●

☑ Enable SSL security

Send test e-mail to:

E-mail: test@tech.local

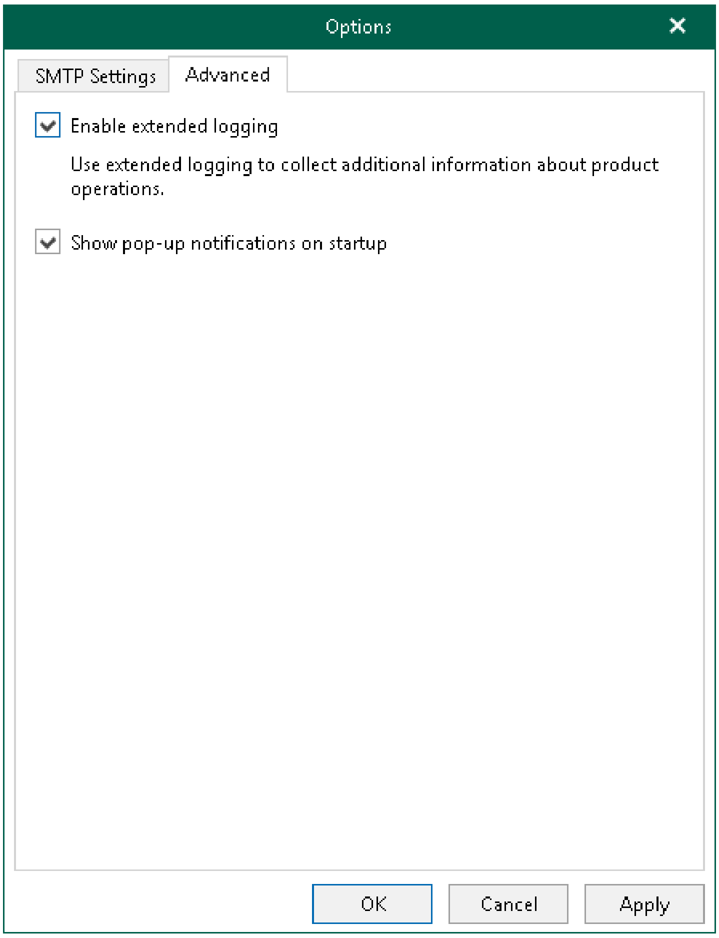
Advanced Settings

Veeam Explorer for Microsoft Teams allows you to configure advanced settings such as extended logging mode and pop-up notifications.

To configure advanced settings, do the following:

1. Go to the main menu and click **General Options**.
2. Click the **Advanced** tab.
3. Select the **Enable extended logging** check box to enable the extended logging mode. In this mode, Veeam Explorer for Microsoft Teams will provide product logs with more details on specific operations.

   After enabling the extended logging mode, you can go back to the application and perform required actions, then collect logs.
4. By default, Veeam Explorer for Microsoft Teams displays notifications when loading backups from object storage repositories. If you want to disable these notifications, clear the **Show pop-up notifications on startup** check box.



☑ Enable extended logging

Use extended logging to collect additional information about product operations.

☑ Show pop-up notifications on startup

Standalone Databases

This section explains how to add standalone databases to the Veeam Explorer for Microsoft Teams 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

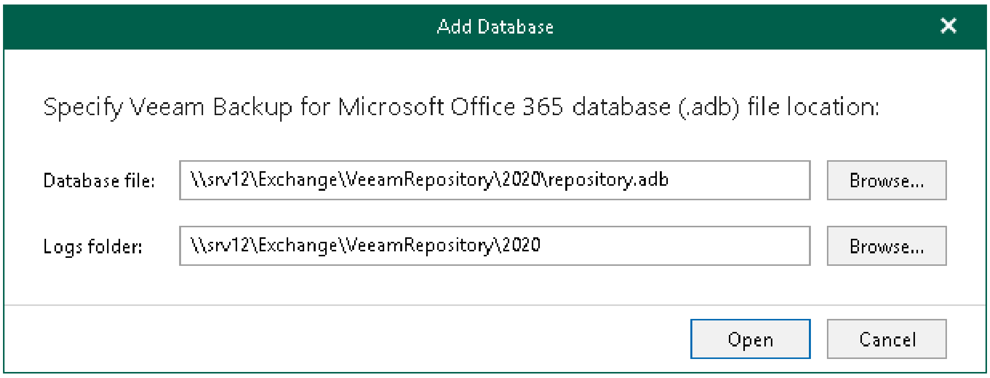
To manually add databases that store Microsoft Office 365 organization data, do the following:

1. On the ribbon, click **Add Org** > **Veeam Backup for Microsoft Office 365 database**.

   Alternatively, in the preview pane, right-click **Organizations** and select **Veeam Backup for Microsoft Office 365 database**.

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: \\srv12\Exchange\VeeamRepository\2020\repository.adb

Logs folder: \\srv12\Exchange\VeeamRepository\2020

Adding Veeam Backup for Microsoft Office 365 Server

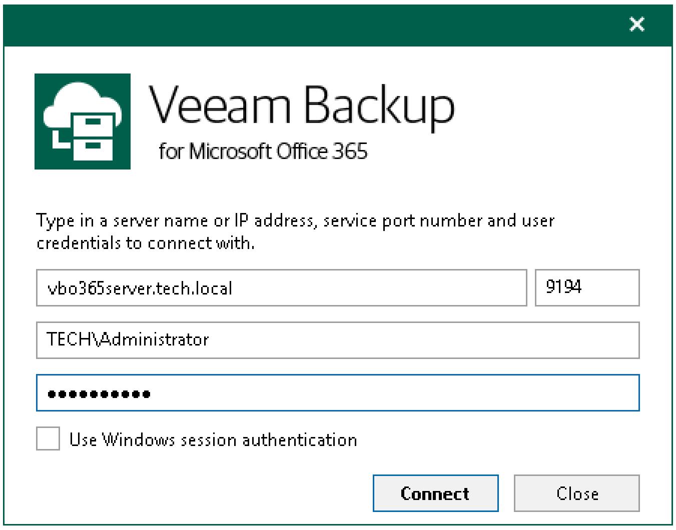
You can use Veeam Explorer for Microsoft Teams to connect to another Veeam Backup for Microsoft Office 365 server and add its databases to the Veeam Explorer scope.

To connect to another Veeam Backup for Microsoft Office 365 server, do the following:

1. On the ribbon, click **Add Org** > **Veeam Backup for Microsoft Office 365 server**.

   Alternatively, in the preview pane, right-click **Organizations** and select **Veeam Backup for Microsoft Office 365 server**.

2. Specify settings to connect to the Veeam Backup for Microsoft Office 365 server and click **Connect**.



Veeam Backup for Microsoft Office 365

Type in a server name or IP address, service port number and user credentials to connect with.

vbo365server.tech.local 9194

TECH\Administrator

●●●●●●●●●●●

□ Use Windows session authentication

Adding Veeam Backup for Microsoft Office 365 Service Provider

You can use Veeam Explorer for Microsoft Teams to 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 Teams 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 ribbon, click **Add Org** > **Veeam Backup for Microsoft Office 365 service provider**.

   Alternatively, in the preview pane, right-click **Organizations** and select **Veeam Backup for Microsoft Office 365 service provider**.

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.

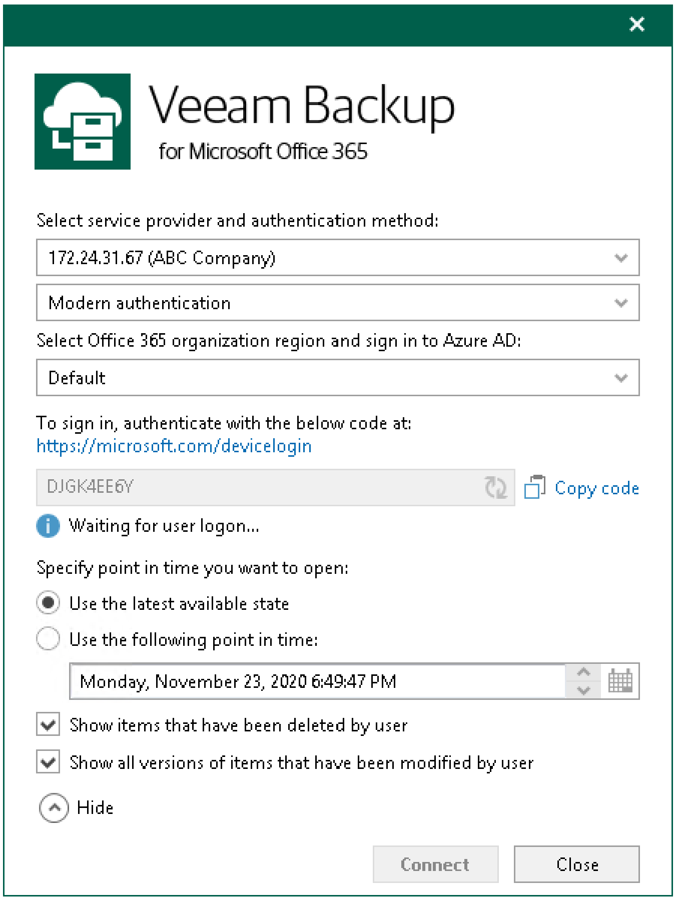
6. Select a point-in-time state as of which you want to load Office 365 backups.

   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**.



Select service provider and authentication method:

172.24.31.67 (ABC Company)

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

DJGK4EE6Y

Waiting for user logon...

Specify point in time you want to open:

● Use the latest available state

○ Use the following point in time:

Monday, November 23, 2020 6:49:47 PM

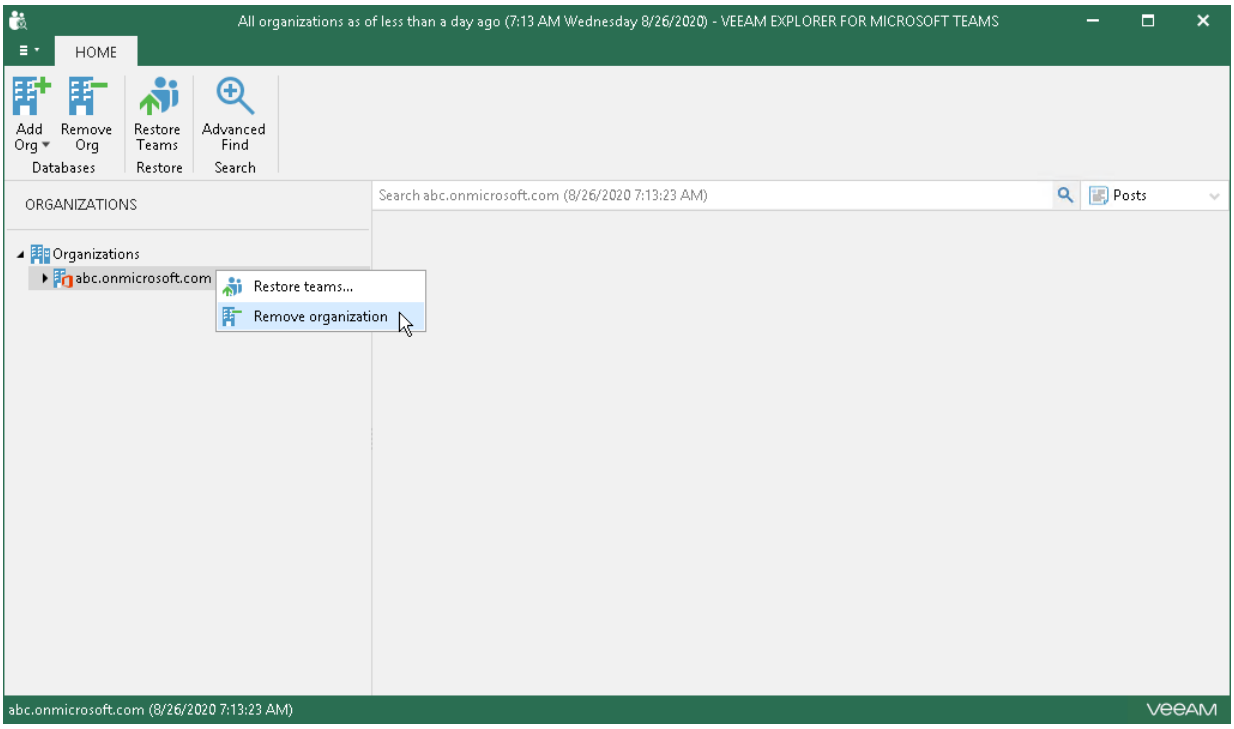
☑ Show items that have been deleted by user

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

Removing Standalone Databases

Veeam Explorer for Microsoft Teams 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**.



All organizations as of less than a day ago (7:13 AM Wednesday 8/26/2020) - VEEAM EXPLORER FOR MICROSOFT TEAMS
HOME
Add Org
Remove Org
Databases
Restore Teams
Restore
Advanced Find
Search
ORGANIZATIONS
Organizations
abc.onmicrosoft.com
Restore teams...
Remove organization
Search abc.onmicrosoft.com (8/26/2020 7:13:23 AM)
Posts
abc.onmicrosoft.com (8/26/2020 7:13:23 AM)
veeam

Data Restore

This section explains how to restore Microsoft Teams data to Microsoft Office 365 organizations.

Restoring Teams

You can use Veeam Explorer for Microsoft Teams to restore all teams of a Microsoft Office 365 organization or a specific team of an organization.

> **TIP:**
>
> Before restoring team data, make sure to read Considerations and Limitations.

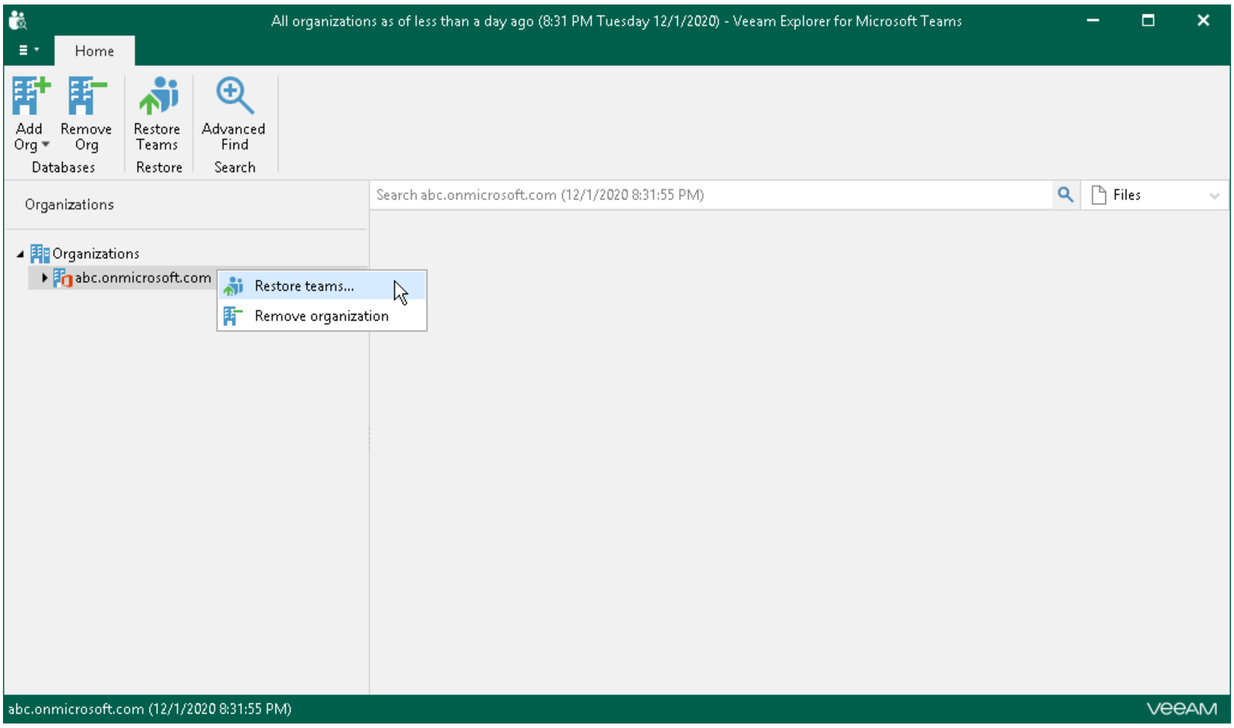
To restore teams, do the following:

1. Launch the Restore wizard.
2. Select an authentication method.
3. Log in to Office 365.
4. Select teams to restore.
5. Specify restore options.
6. Select team members to restore.

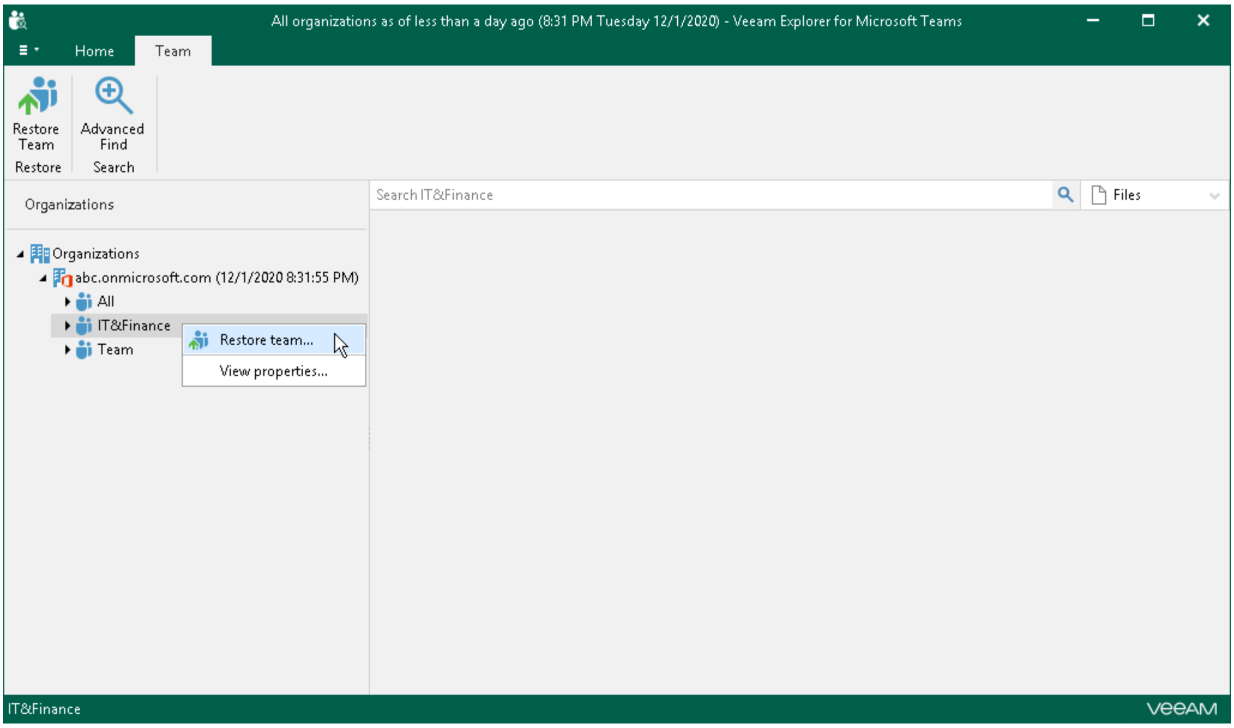
Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

- If you want to restore multiple teams of a Microsoft Office 365 organization, do either of the following:
    - In the navigation pane, select an organization whose teams you want to restore and click **Restore Teams** on the ribbon.
    - In the navigation pane, right-click an organization whose teams you want to restore and select **Restore teams**.


All organizations as of less than a day ago (8:31 PM Tuesday 12/1/2020) - Veeam Explorer for Microsoft Teams
Home
Add Org
Remove Org
Databases
Restore Teams
Restore
Advanced Find
Search
Organizations
Search abc.onmicrosoft.com (12/1/2020 8:31:55 PM)
Files
Organizations
abc.onmicrosoft.com
Restore teams...
Remove organization
abc.onmicrosoft.com (12/1/2020 8:31:55 PM)
veeam

- If you want to restore a specific team, do either of the following:
    - In the navigation pane, select a team that you want to restore and click **Restore Team** on the ribbon.
    - In the navigation pane, right-click a team that you want to restore and select **Restore team**.



Step 2. Select Authentication Method

At this step of the wizard, choose whether you want to use modern or basic authentication and specify authentication settings.

- Modern authentication
- Basic authentication

Modern Authentication

To use modern authentication, do the following:

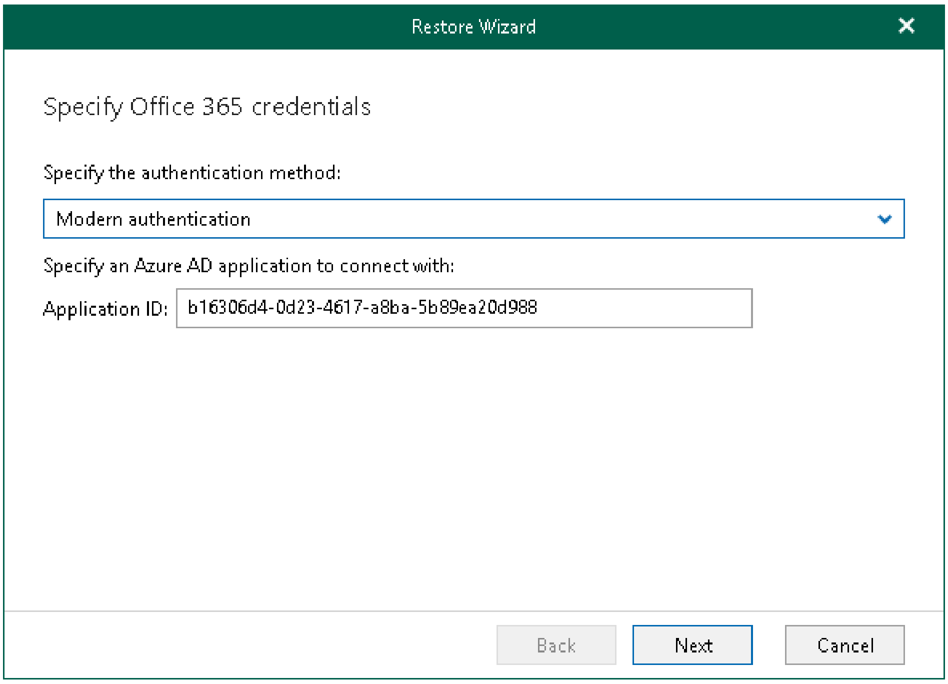
1. From the **Specify the authentication method** drop-down list, select *Modern authentication*.

   This will allow Veeam Backup for Microsoft Office 365 to use an Azure AD application for data restore. Such an application is used to restore the specified team 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 data restore.

   By default, Veeam Explorer for Microsoft Teams 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.



Specify the authentication method: Modern authentication

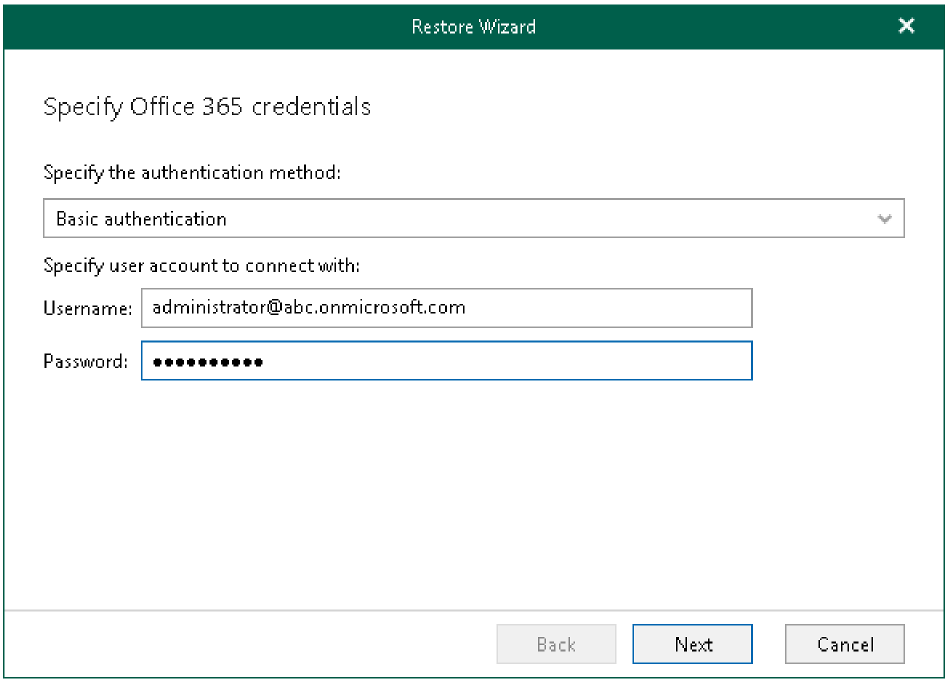
Specify an Azure AD application to connect with:

Application ID: b16306d4-0d23-4617-a8ba-5b89ea20d988

Basic Authentication

To use basic authentication, do the following:

1. From the **Specify the authentication method** drop-down list, select *Basic authentication*.
2. In the **Username** and **Password** fields, enter credentials to connect to the Microsoft Office 365 organization.



Specify Office 365 credentials

Specify the authentication method:

Basic authentication

Specify user account to connect with:

Username: administrator@abc.onmicrosoft.com

Password: ●●●●●●●●●●●

Step 3. Log In to Office 365

This step is available if you selected the *Modern authentication* option at the previous step of the wizard.

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

To sign in to the Microsoft Office 365 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.

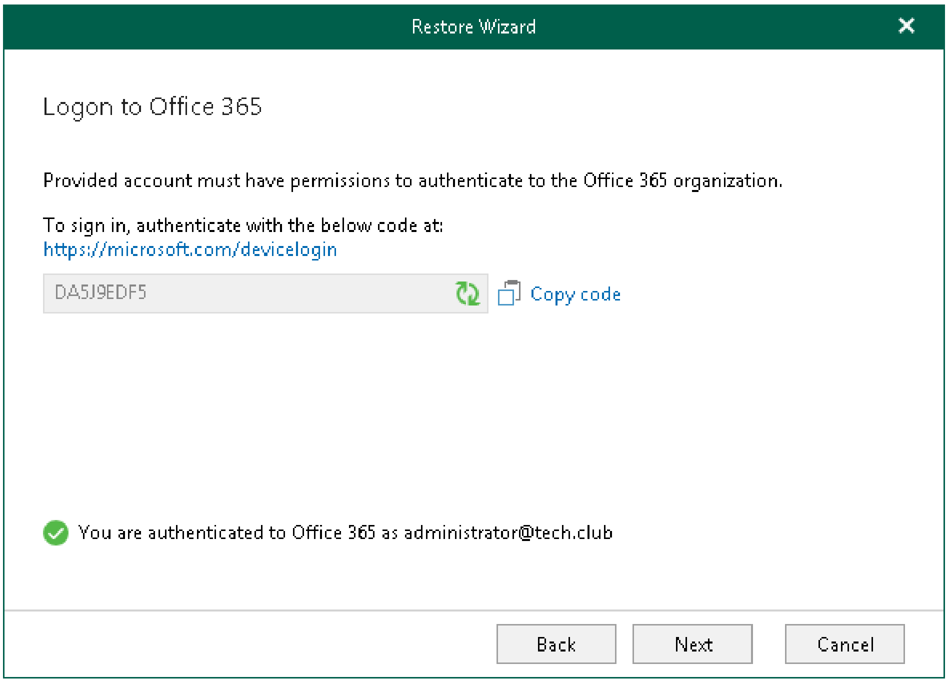
2. Click the link to the Microsoft portal.

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 required permissions assigned. For more information, see Required Permissions.

   Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see Required Azure AD Application Settings.

4. Return to the **Restore Wizard** window and click **Next**.



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

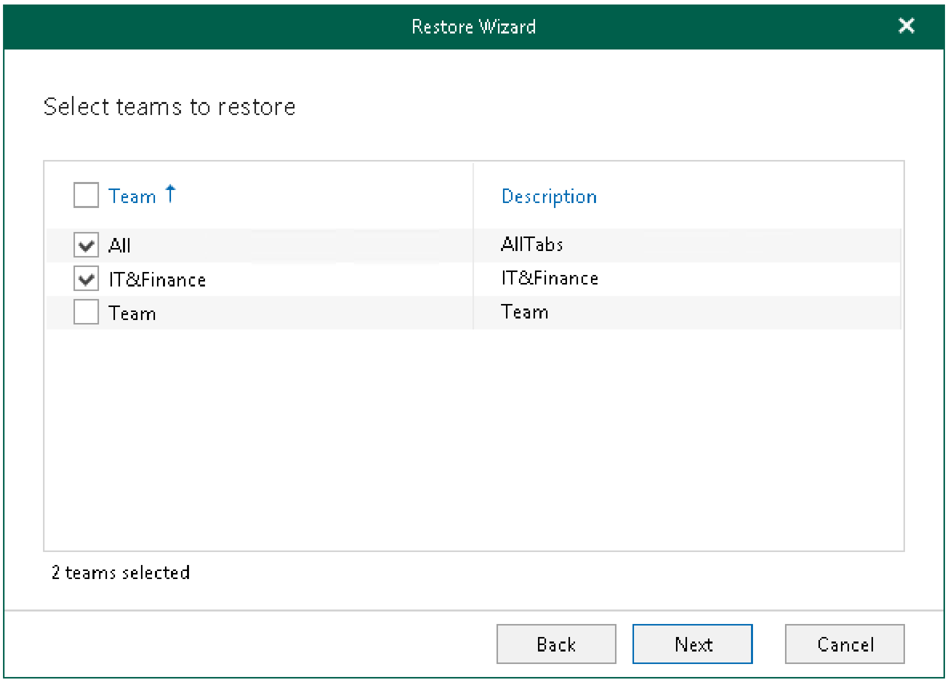
DA5J9EDF5

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

Step 4. Select Teams

This step is available if you launched the **Restore** wizard to restore multiple teams.

At this step of the wizard, select check boxes next to the teams that you want to restore.



Select teams to restore

□ Team ↑	Description
☑ All	AllTabs
☑ IT&Finance	IT&Finance
□ Team	Team

2 teams selected

Step 5. Specify Restore Options

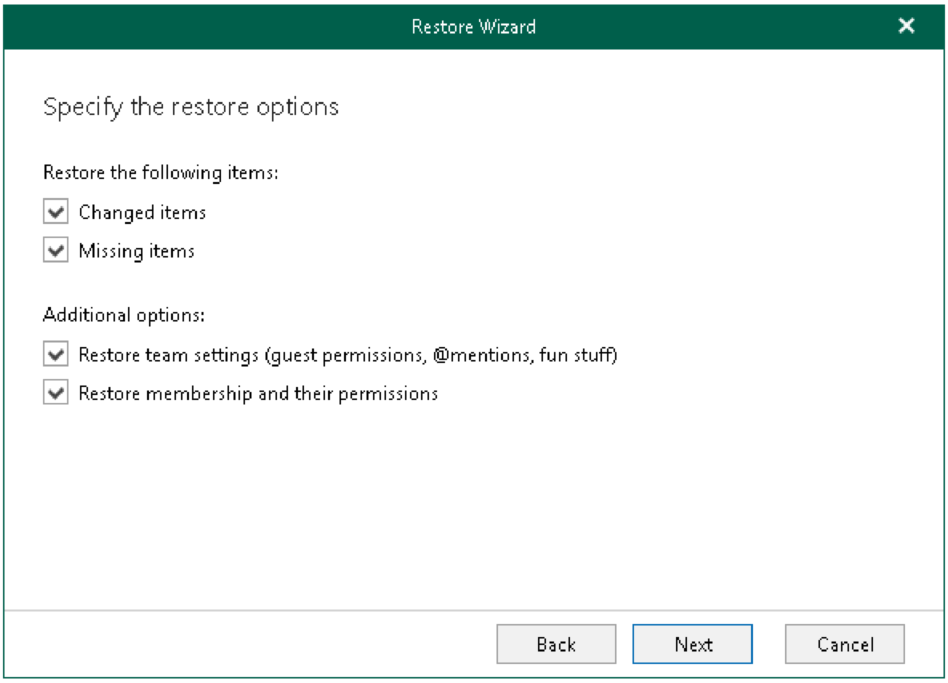
At this step of the wizard, specify data restore options:

1. Select the **Changed items** check box if you want to restore items that have changed since the time when the backup was created. When you select this option, Veeam Explorer for Microsoft Teams overwrites existing items in the original team.
2. Select the **Missing items** check box if you want to restore items that are missing in the original team. For example, some of the items were removed and you want to restore them from the backup.
3. Select the **Restore team settings** check box if you want to replace the current team settings with team settings from the backup.

   You cannot select this check box if you clear both the **Changed items** and **Missing items** check boxes.

   For information on how to view team settings in the backup, see Viewing Team Properties.
4. If you want to restore information about team members and their roles from the backup, make sure that the **Restore membership and their permissions** check box is selected.
   - If you launched the **Restore** wizard to restore a specific team, you will be able to review team members at the next step of the wizard. Click **Next**.
   - If you launched the **Restore** wizard to restore multiple teams, you cannot review team members. Click **Restore** to start the restore process.

> **TIP:**
>
> If you clear the **Restore membership and their permissions** check box, you can start the restore operation immediately. To do this, click **Restore**.


Restore Wizard

Specify the restore options

Restore the following items:

☑ Changed items

☑ Missing items

Additional options:

☑ Restore team settings (guest permissions, @mentions, fun stuff)

☑ Restore membership and their permissions

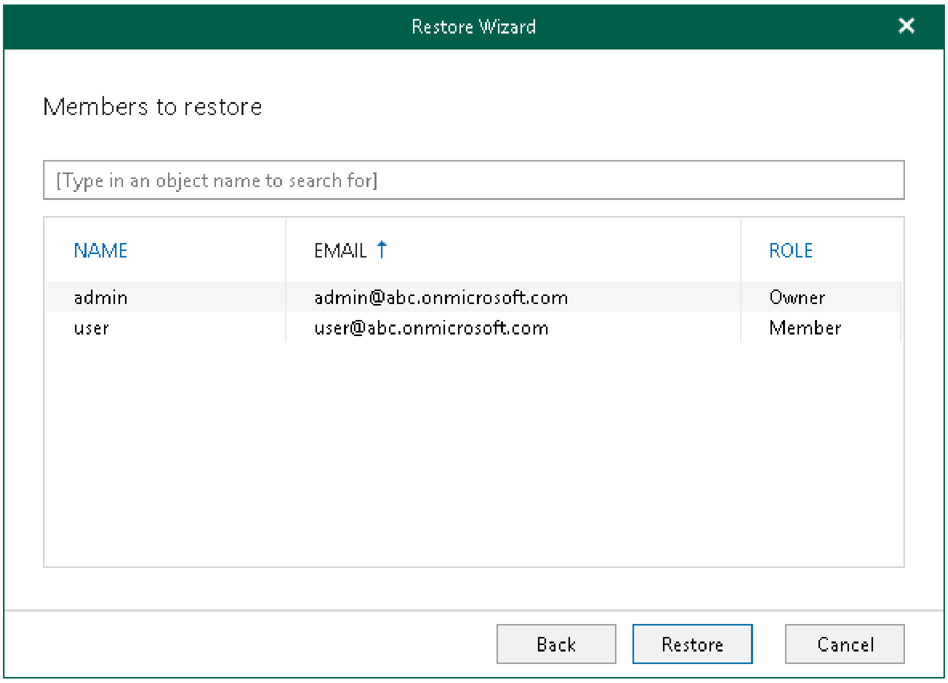
Step 6. Review Team Members

This step is available if you launched the **Restore** wizard to restore a specific team and selected the **Restore membership and their permissions** check box at the previous step of the wizard.

At this step of the wizard, review the list of users whose membership and roles in the team will be restored and click **Restore**.

To quickly find the necessary team members, use the search field at the top of the wizard window.

> **NOTE:**
>
> Veeam Explorer for Microsoft Teams does not change roles for team owners during restore. For example, you create a backup of your organization, and then change role for a team member from *Member* to *Owner*. In this case, if you choose to restore this team member from the backup, Veeam Explorer for Microsoft Teams will not set their role to *Member*.
>
> In the opposite case, if a team member role was changed from *Owner* to *Member* after the backup was created, and you choose to restore team membership from the backup, Veeam Explorer for Microsoft Teams will elevate the role to *Owner* during restore.



NAME	EMAIL ↑	ROLE
admin	admin@abc.onmicrosoft.com	Owner
user	user@abc.onmicrosoft.com	Member

Restoring Channels and Tabs

You can use Veeam Explorer for Microsoft Teams to restore individual channels of a team. You can restore an entire channel or specific tabs of a channel.

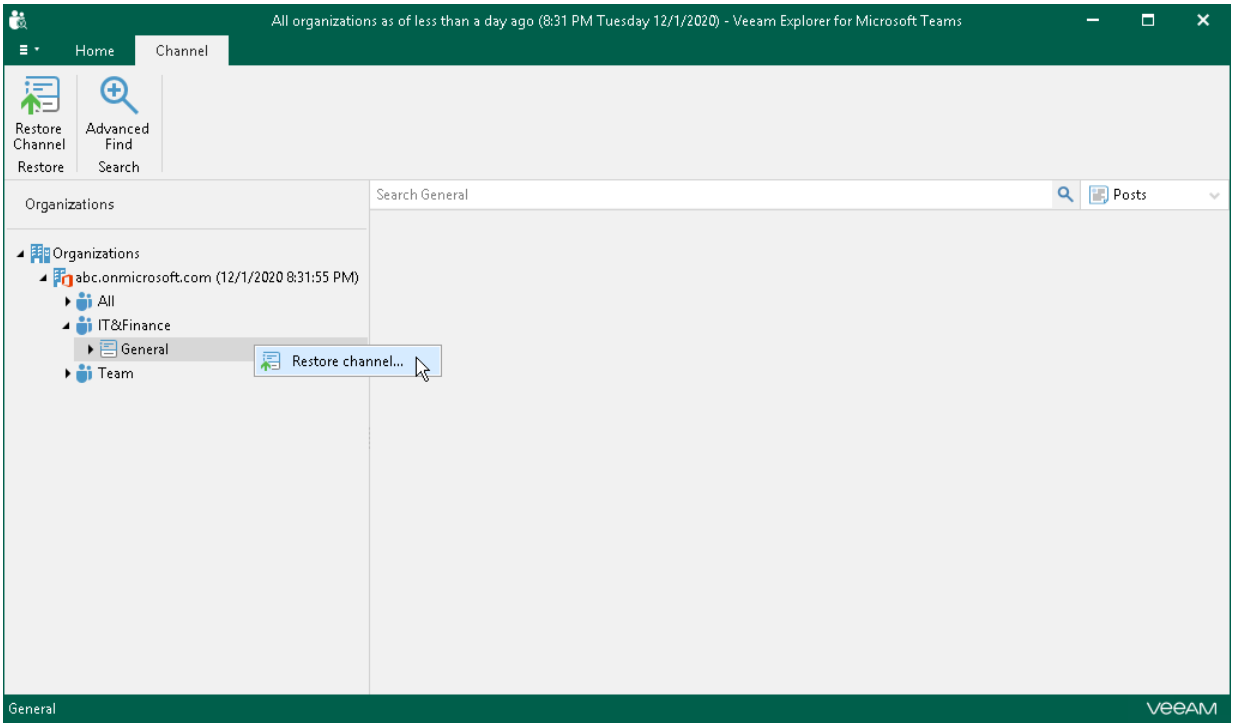
To restore channels and tabs, do the following:

1. Launch the Restore wizard.
2. Select an authentication method.
3. Log in to Office 365.
4. Specify restore options.

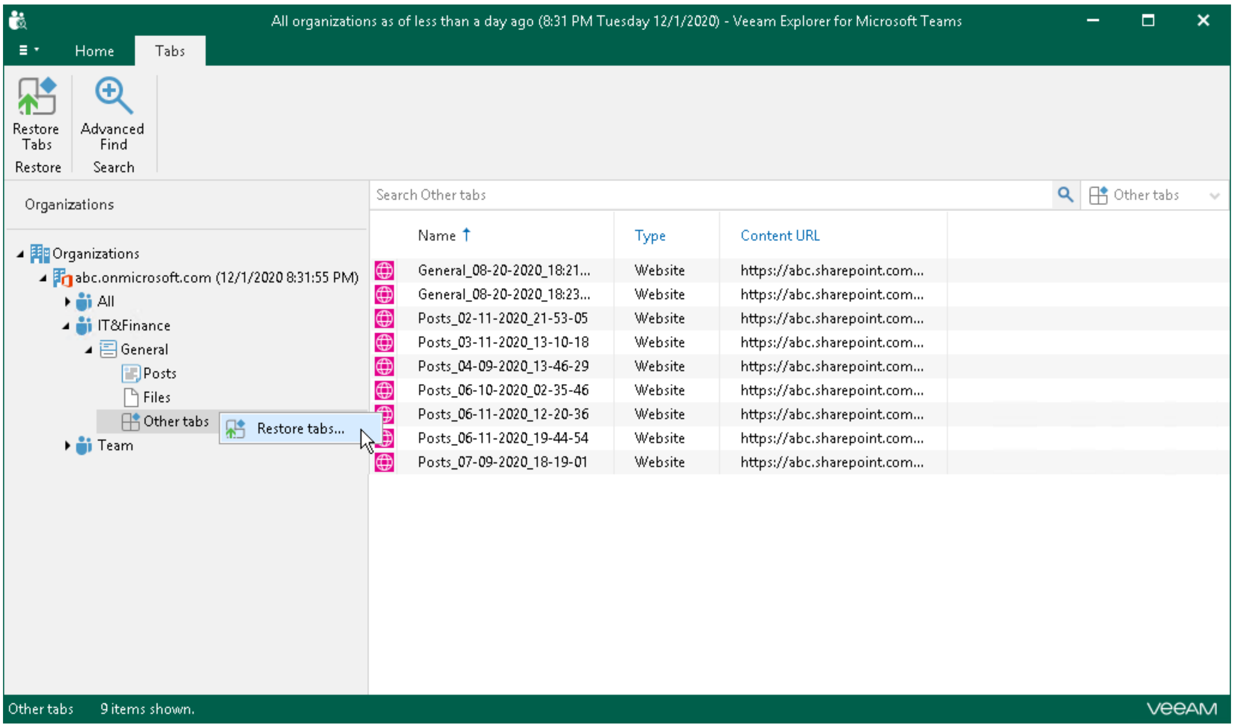
Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

- If you want to restore a channel, do either of the following:
  - In the navigation pane, select a channel that you want to restore and click **Restore Channel** on the ribbon.
  - In the navigation pane, right-click a channel that you want to restore and select **Restore channel**.



- If you want to restore all tabs of a channel, do either of the following:
  - In the navigation pane, expand a channel whose tabs you want to restore, select **Other tabs** and click **Restore Tabs** on the ribbon.
  - In the navigation pane, expand a channel whose tabs you want to restore, right-click **Other tabs** and select **Restore tabs**.



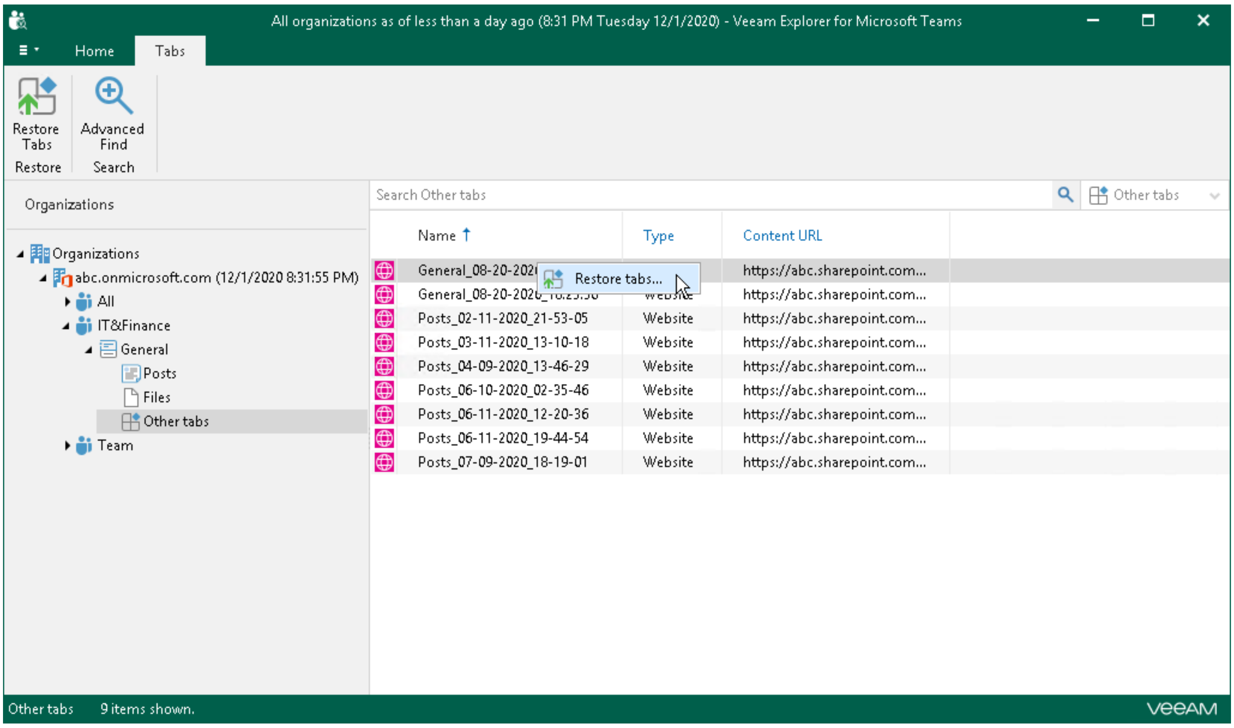
Name	Type	Content URL
General_08-20-2020_18:21...	Website	https://abc.sharepoint.com...
General_08-20-2020_18:23...	Website	https://abc.sharepoint.com...
Posts_02-11-2020_21-53-05	Website	https://abc.sharepoint.com...
Posts_03-11-2020_13-10-18	Website	https://abc.sharepoint.com...
Posts_04-09-2020_13-46-29	Website	https://abc.sharepoint.com...
Posts_06-10-2020_02-35-46	Website	https://abc.sharepoint.com...
Posts_06-11-2020_12-20-36	Website	https://abc.sharepoint.com...
Posts_06-11-2020_19-44-54	Website	https://abc.sharepoint.com...
Posts_07-09-2020_18-19-01	Website	https://abc.sharepoint.com...

- If you want to restore individual tabs of a channel, do the following:

  a. In the navigation pane, expand a channel whose tabs you want to restore and select **Other tabs**.

  b. In the preview pane, select a necessary tab and click **Restore Tabs** on the ribbon or right-click a tab and select **Restore tabs**.

> **TIP:**
>
> To select more than one tab in the preview pane, press and hold the **[CTRL]** key and select the necessary tabs.



Name	Type	Content URL
General_08-20-202		https://abc.sharepoint.com...
General_08-20-202		https://abc.sharepoint.com...
Posts_02-11-2020_21-53-05	Website	https://abc.sharepoint.com...
Posts_03-11-2020_13-10-18	Website	https://abc.sharepoint.com...
Posts_04-09-2020_13-46-29	Website	https://abc.sharepoint.com...
Posts_06-10-2020_02-35-46	Website	https://abc.sharepoint.com...
Posts_06-11-2020_12-20-36	Website	https://abc.sharepoint.com...
Posts_06-11-2020_19-44-54	Website	https://abc.sharepoint.com...
Posts_07-09-2020_18-19-01	Website	https://abc.sharepoint.com...

Step 2. Select Authentication Method

At this step of the wizard, choose whether you want to use modern or basic authentication and specify authentication settings.

- Modern authentication
- Basic authentication

Modern Authentication

To use modern authentication, do the following:

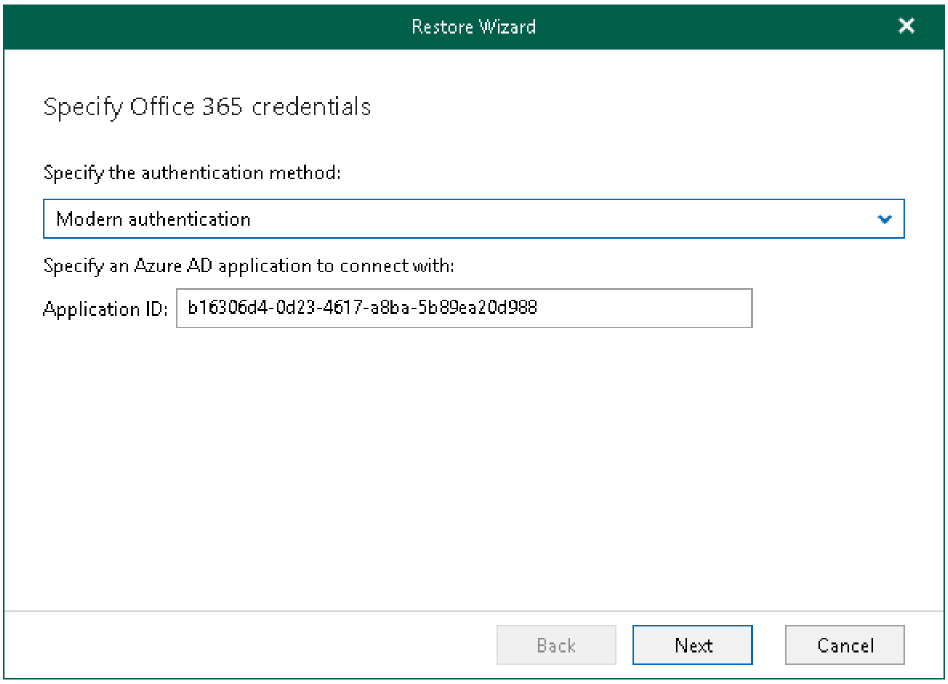
1. From the **Specify the authentication method** drop-down list, select *Modern authentication*.

   This will allow Veeam Backup for Microsoft Office 365 to use an Azure AD application for data restore. Such an application is used to restore the specified team 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 data restore.

   By default, Veeam Explorer for Microsoft Teams 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 the authentication method: Modern authentication

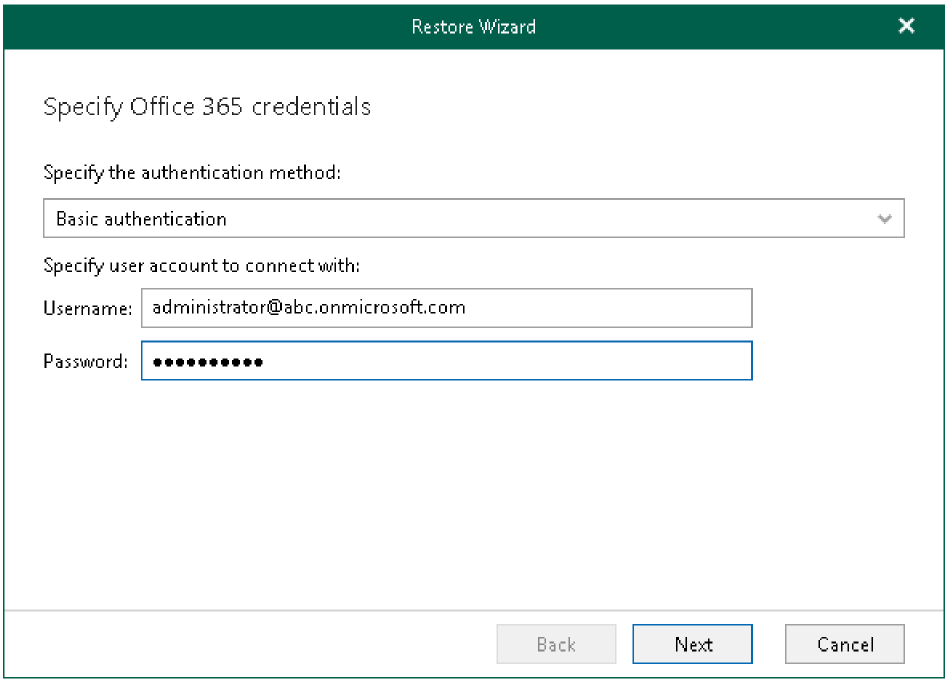
Specify an Azure AD application to connect with:

Application ID: b16306d4-0d23-4617-a8ba-5b89ea20d988

Basic Authentication

To use basic authentication, do the following:

1. From the **Specify the authentication method** drop-down list, select *Basic authentication*.
2. In the **Username** and **Password** fields, enter credentials to connect to the Microsoft Office 365 organization.



Restore Wizard

Specify Office 365 credentials

Specify the authentication method:

Basic authentication

Specify user account to connect with:

Username: administrator@abc.onmicrosoft.com

Password: ●●●●●●●●●●●

Step 3. Log In to Office 365

This step is available if you selected the *Modern authentication* option at the previous step of the wizard.

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

To sign in to the Microsoft Office 365 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.

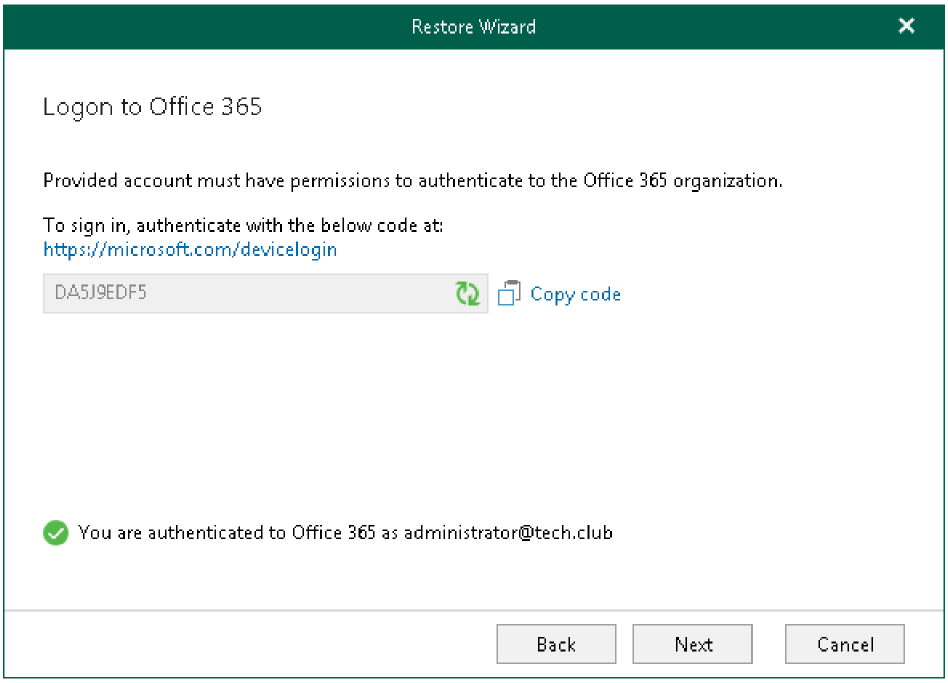
2. Click the link to the Microsoft portal.

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 required permissions assigned. For more information, see Required Permissions.

   Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see Required Azure AD Application Settings.

4. Return to the **Restore Wizard** window and click **Next**.



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

DA5J9EDF5

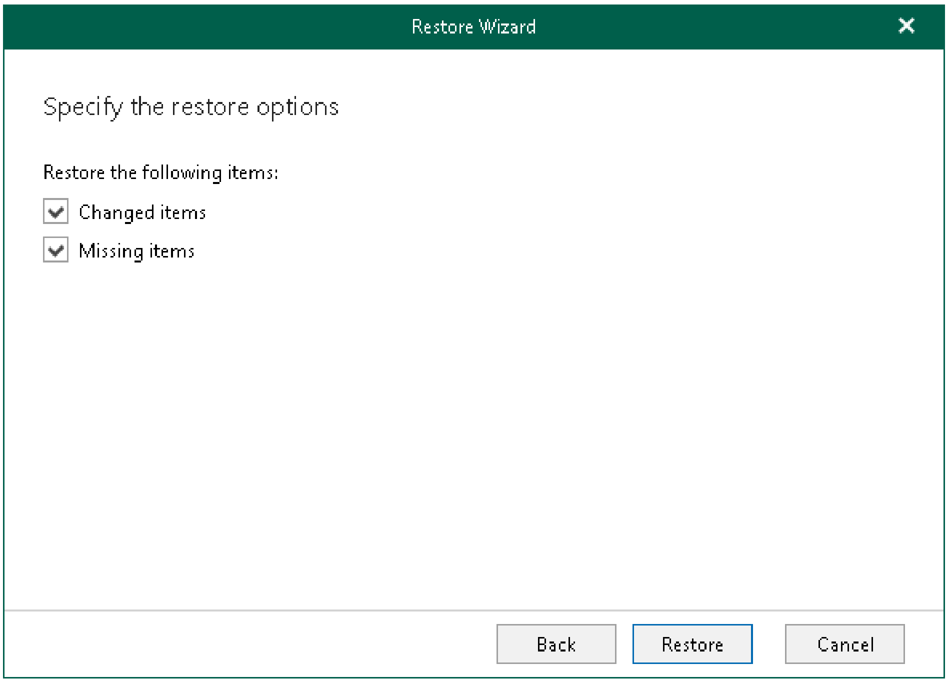
You are authenticated to Office 365 as administrator@tech.club

Step 4. Specify Restore Options

At this step of the wizard, specify data restore options and start the restore process:

1. Select the **Changed items** check box if you want to restore items that have changed since the time when the backup was created. When you select this option, Veeam Explorer for Microsoft Teams overwrites existing items in your target location.
2. Select the **Missing items** check box if you want to restore items that are missing in the target location. For example, some of the items were removed and you want to restore them from the backup.
3. Click **Restore**.

> **NOTE:**
>
> During restore of a tab, Veeam Explorer for Microsoft Teams restores the name of the tab and a link to an object published on the tab. The object itself, for example, a SharePoint site or document, is not restored from the backup in this scenario. To restore such objects along with tabs, consider restoring an entire team. For more information, see Restoring Teams.



Restore Wizard

Specify the restore options

Restore the following items:

☑ Changed items

☑ Missing items

Restoring Posts

You can use Veeam Explorer for Microsoft Teams to restore posts of a team channel. When you restore posts, you can choose to restore all posts of a channel or restore posts published within a specified time period.

> **NOTE:**
>
> Veeam Backup for Microsoft Office 365 does not restore posts to their original location in the team channel. Instead, Veeam Backup for Microsoft Office 365 creates a new tab in the original channel and restores posts to this tab.
>
> If you want to restore posts to another channel, use the export operation. For more information, see Data Export.

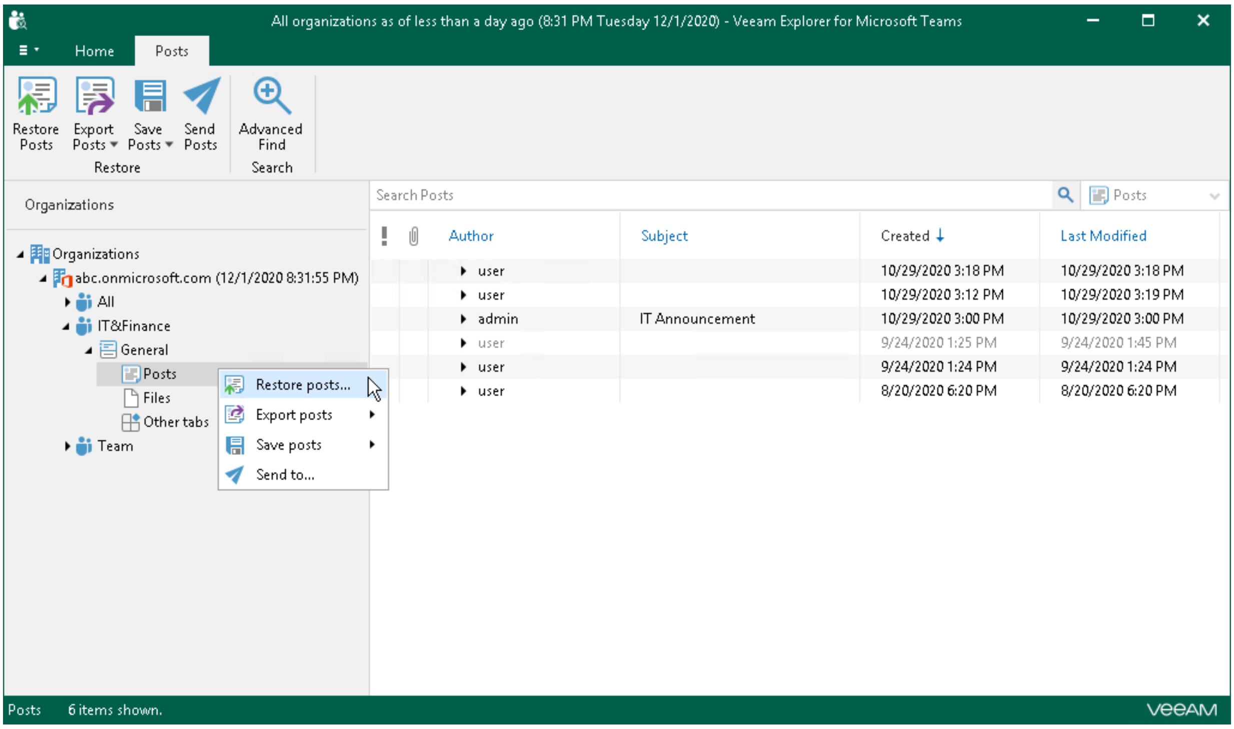
To restore posts, do the following:

1. Launch the Restore wizard.
2. Select an authentication method.
3. Log in to Office 365.
4. Specify restore options.

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do either of the following:

- In the navigation pane, expand a channel whose posts you want to restore, select **Posts** and click **Restore Posts** on the ribbon.
- In the navigation pane, expand a channel whose posts you want to restore, right-click **Posts** and select **Restore posts.**



Author	Subject	Created ↓	Last Modified
user		10/29/2020 3:18 PM	10/29/2020 3:18 PM
user		10/29/2020 3:12 PM	10/29/2020 3:19 PM
admin	IT Announcement	10/29/2020 3:00 PM	10/29/2020 3:00 PM
user		9/24/2020 1:25 PM	9/24/2020 1:45 PM
user		9/24/2020 1:24 PM	9/24/2020 1:24 PM
user		8/20/2020 6:20 PM	8/20/2020 6:20 PM

Step 2. Select Authentication Method

At this step of the wizard, choose whether you want to use modern or basic authentication and specify authentication settings.

- Modern authentication
- Basic authentication

Modern Authentication

To use modern authentication, do the following:

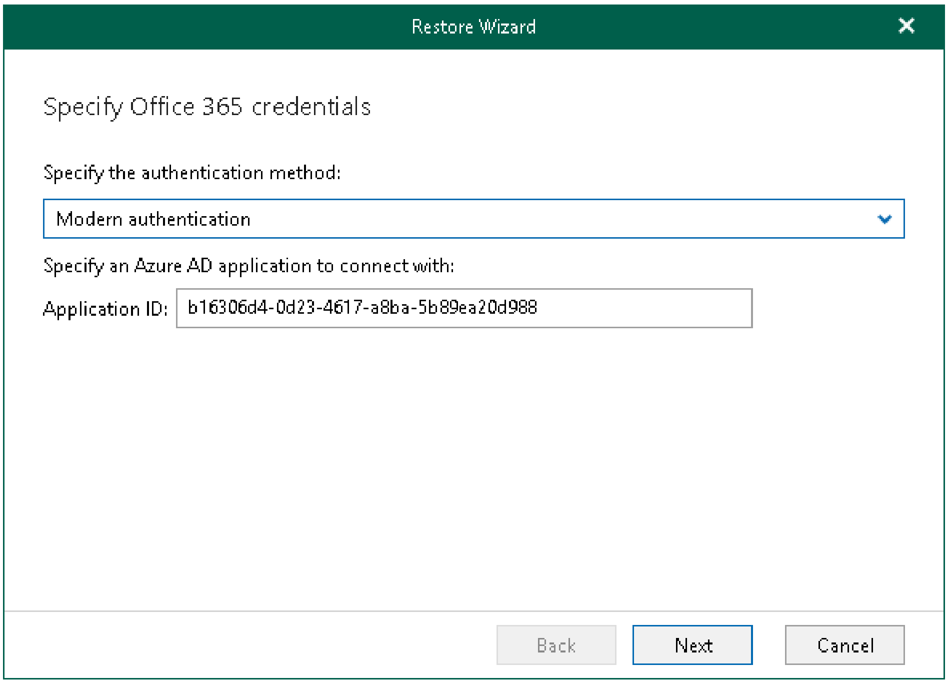
1. From the **Specify the authentication method** drop-down list, select *Modern authentication*.

   This will allow Veeam Backup for Microsoft Office 365 to use an Azure AD application for data restore. Such an application is used to restore the specified team 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 data restore.

   By default, Veeam Explorer for Microsoft Teams 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.



Specify Office 365 credentials

Specify the authentication method: Modern authentication

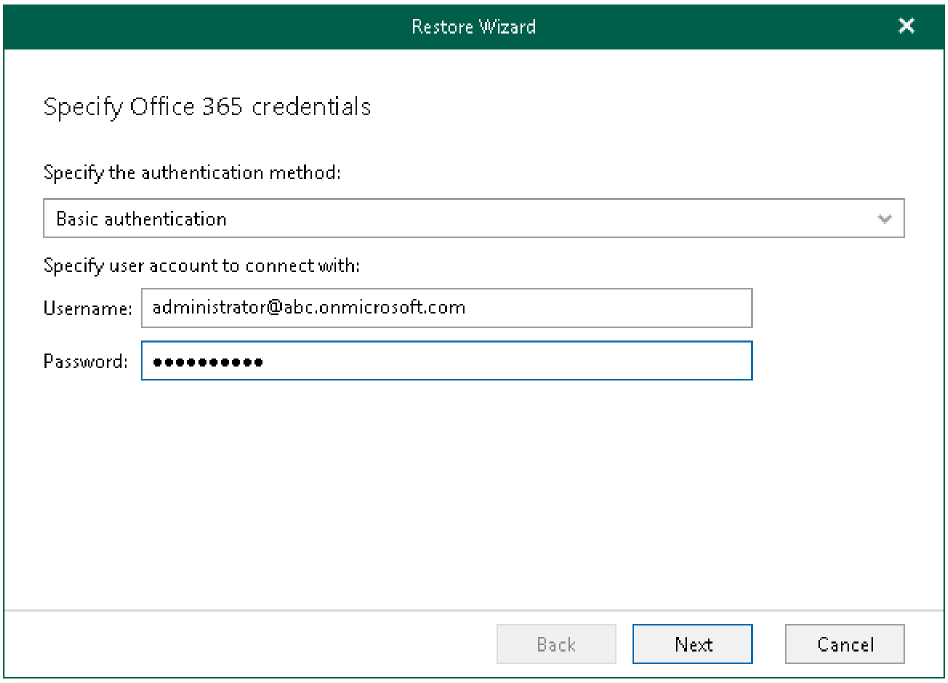
Specify an Azure AD application to connect with:

Application ID: b16306d4-0d23-4617-a8ba-5b89ea20d988

Basic Authentication

To use basic authentication, do the following:

1. From the **Specify the authentication method** drop-down list, select *Basic authentication*.
2. In the **Username** and **Password** fields, enter credentials to connect to the Microsoft Office 365 organization.



Specify Office 365 credentials

Specify the authentication method:

Basic authentication

Specify user account to connect with:

Username: administrator@abc.onmicrosoft.com

Password: ●●●●●●●●●●

Step 3. Log In to Office 365

This step is available if you selected the *Modern authentication* option at the previous step of the wizard.

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

To sign in to the Microsoft Office 365 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.

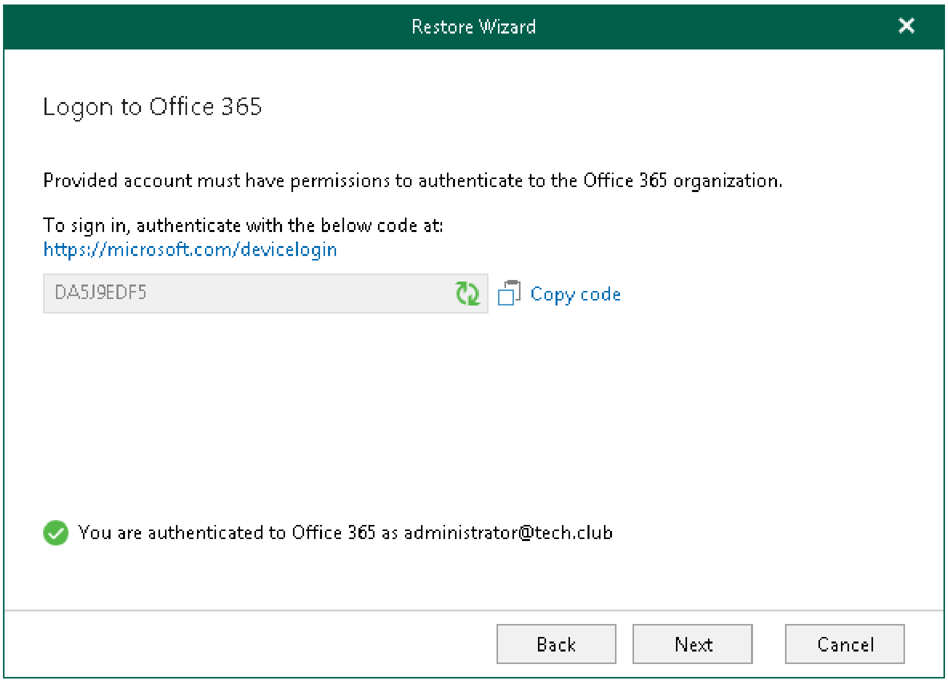
2. Click the link to the Microsoft portal.

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 required permissions assigned. For more information, see Required Permissions.

   Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see Required Azure AD Application Settings.

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, authenticate with the below code at:
https://microsoft.com/devicelogin

DA5J9EDF5

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

Step 4. Specify Restore Options

At this step of the wizard, select restore options and click **Restore**.

You can select one of the following options:

- **Restore all posts**

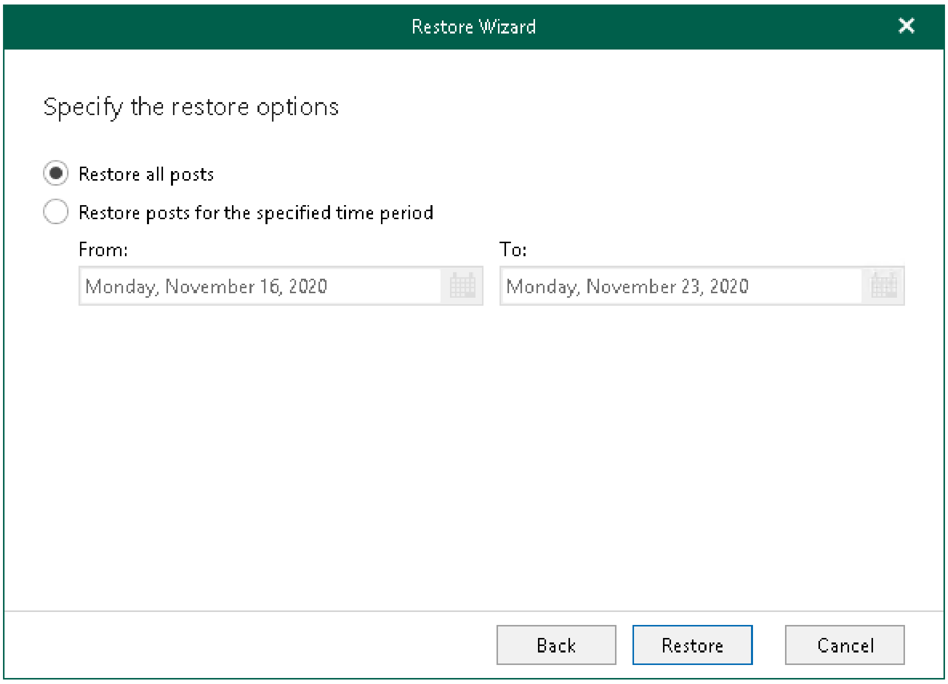
  Select this option if you want to restore all posts published in the channel.

- **Restore posts for the specified time period**

  Select this check box if you want to restore posts published in the channel during the specified time period.

  If you select this option, in the **From** and **To** fields, specify the dates that define the start and end of the desired time period. Veeam Explorer for Microsoft Teams will restore posts whose last modification date belongs to the specified period.

When you restore posts, Veeam Backup for Microsoft Office 365 will create a separate tab in the original team channel and restore posts to this tab.


Restore Wizard

Specify the restore options

● Restore all posts

○ Restore posts for the specified time period

From: Monday, November 16, 2020

To: Monday, November 23, 2020

Restoring Files

You can use Veeam Explorer for Microsoft Teams to restore files of a team channel.

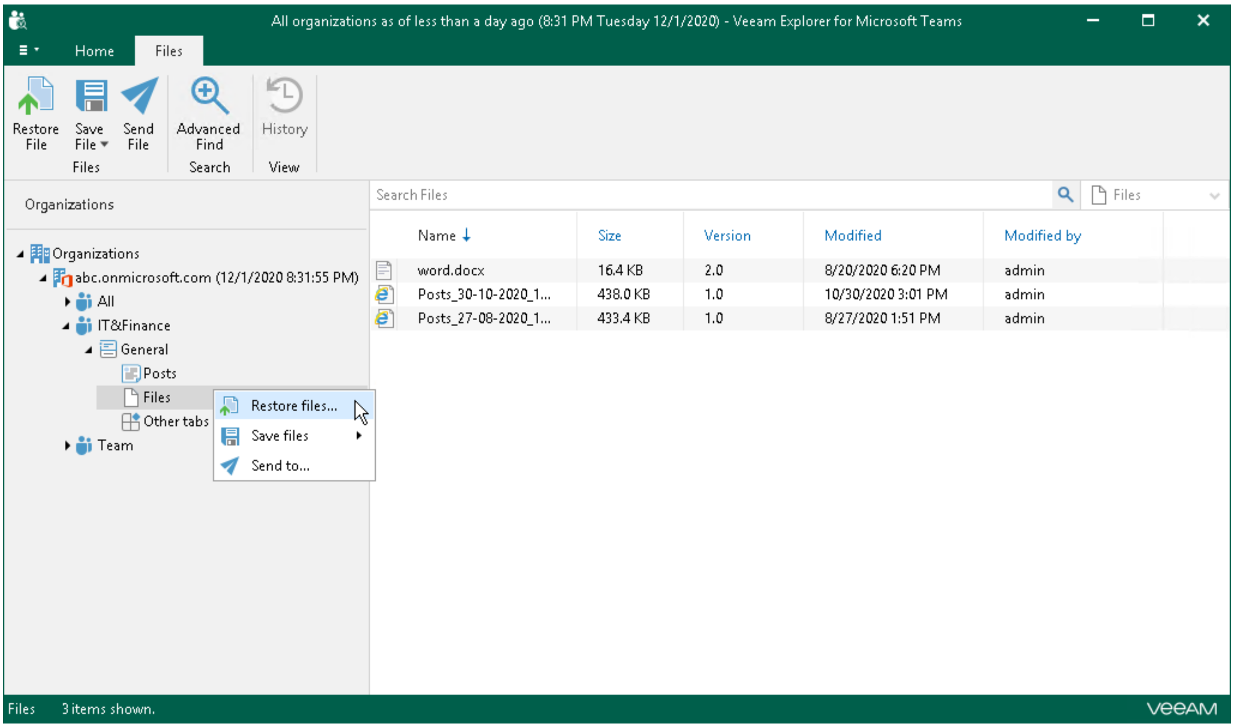
To restore files, do the following:

1. Launch the Restore wizard.
2. Select an authentication method.
3. Log in to Office 365.
4. Specify restore options.

Step 1. Launch Restore Wizard

To launch the **Restore** wizard, do the following:

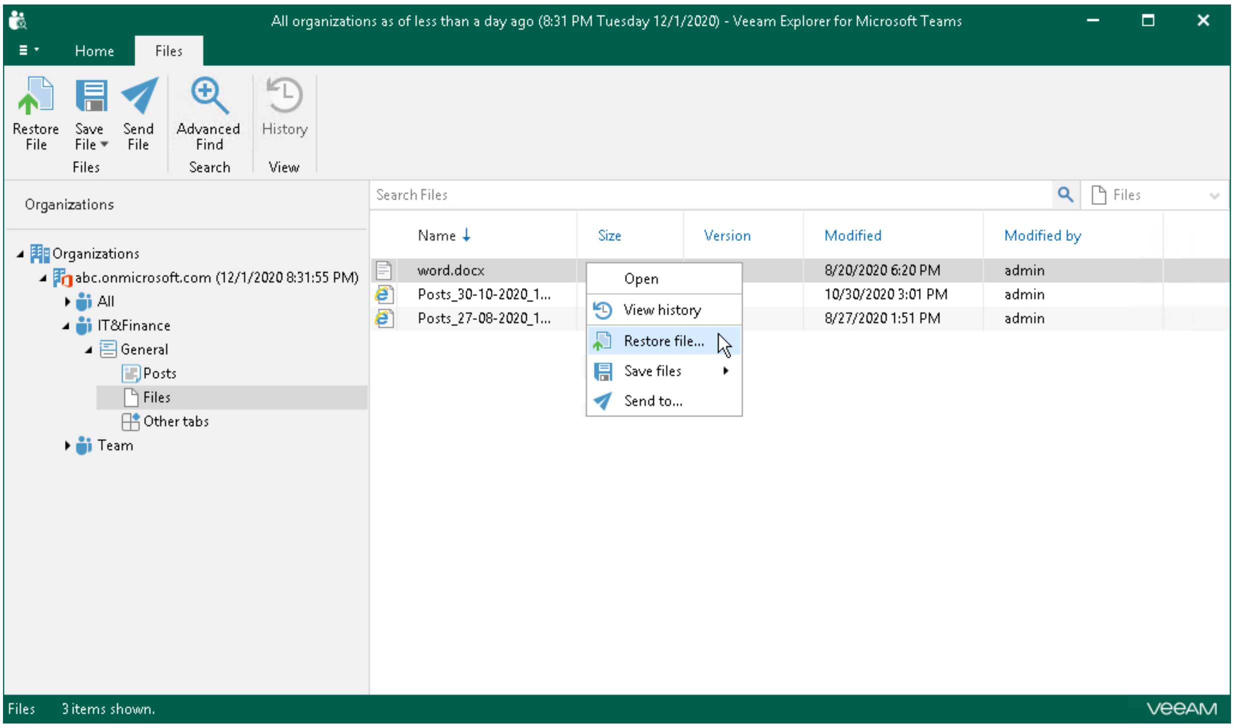
- If you want to restore all files of a channel, do either of the following:
  - In the navigation pane, expand a channel whose files you want to restore and click **Restore File** on the ribbon.
  - In the navigation pane, right-click a channel whose files you want to restore and select **Restore files**.



Name	Size	Version	Modified	Modified by
word.docx	16.4 KB	2.0	8/20/2020 6:20 PM	admin
Posts_30-10-2020_1...	438.0 KB	1.0	10/30/2020 3:01 PM	admin
Posts_27-08-2020_1...	433.4 KB	1.0	8/27/2020 1:51 PM	admin

- If you want to restore individual files, do the following:
  a. In the navigation pane, expand a channel whose files you want to restore and select **Files**.
  b. In the preview pane, select a necessary file and click **Restore File** on the ribbon or right-click a file and select **Restore file**.

> **TIP:**
>
> To select more than one file in the preview pane, press and hold the **[CTRL]** key and select the necessary files.


All organizations as of less than a day ago (8:31 PM Tuesday 12/1/2020) - Veeam Explorer for Microsoft Teams

Name	Size	Version	Modified	Modified by
word.docx			8/20/2020 6:20 PM	admin
Posts_30-10-2020_1...			10/30/2020 3:01 PM	admin
Posts_27-08-2020_1...			8/27/2020 1:51 PM	admin

Files 3 items shown.

Step 2. Select Authentication Method

At this step of the wizard, choose whether you want to use modern or basic authentication and specify authentication settings.

- Modern authentication
- Basic authentication

Modern Authentication

To use modern authentication, do the following:

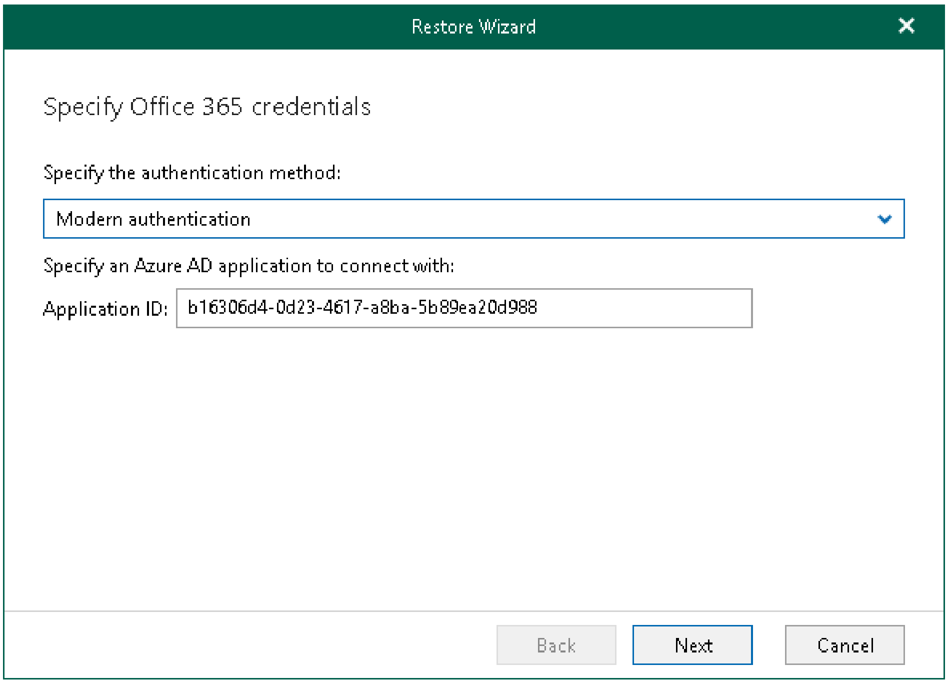
1. From the **Specify the authentication method** drop-down list, select *Modern authentication*.

   This will allow Veeam Backup for Microsoft Office 365 to use an Azure AD application for data restore. Such an application is used to restore the specified team 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 data restore.

   By default, Veeam Explorer for Microsoft Teams 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.



Specify Office 365 credentials

Specify the authentication method:

Modern authentication

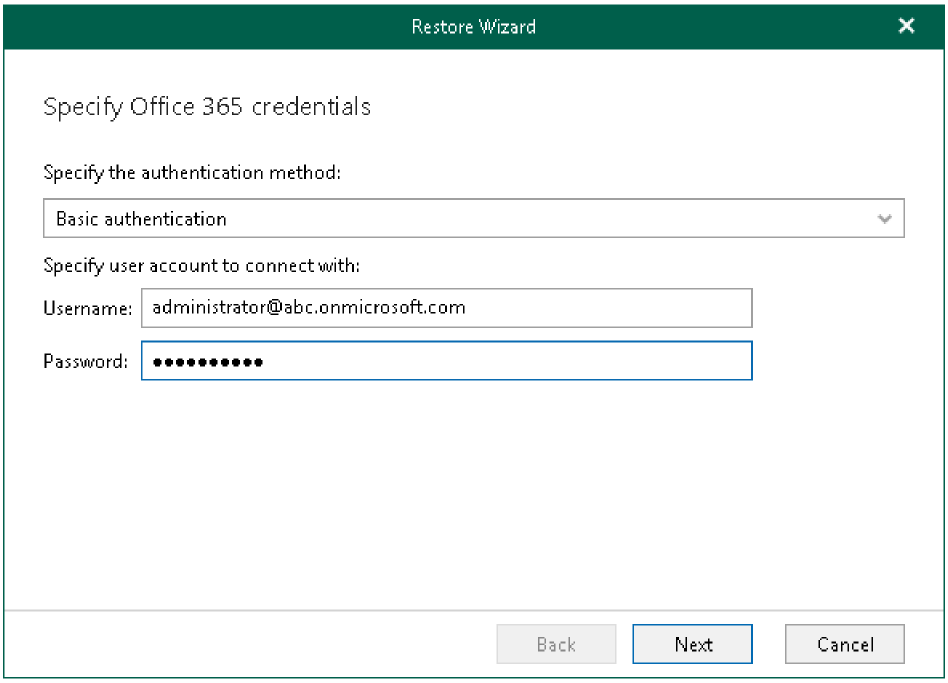
Specify an Azure AD application to connect with:

Application ID: b16306d4-0d23-4617-a8ba-5b89ea20d988

Basic Authentication

To use basic authentication, do the following:

1. From the **Specify the authentication method** drop-down list, select *Basic authentication*.
2. In the **Username** and **Password** fields, enter credentials to connect to the Microsoft Office 365 organization.



Restore Wizard

Specify Office 365 credentials

Specify the authentication method: Basic authentication

Specify user account to connect with:

Username: administrator@abc.onmicrosoft.com

Password: ●●●●●●●●●●

Step 3. Log In to Office 365

This step is available if you selected the *Modern authentication* option at the previous step of the wizard.

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

To sign in to the Microsoft Office 365 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.

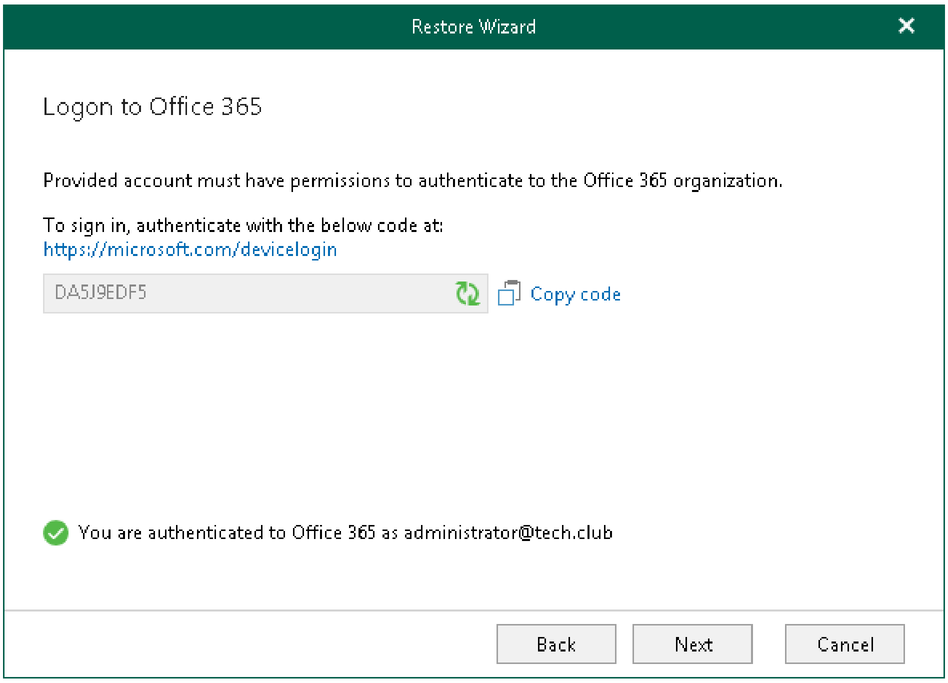
2. Click the link to the Microsoft portal.

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 required permissions assigned. For more information, see Required Permissions.

   Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see Required Azure AD Application Settings.

4. Return to the **Restore Wizard** window and click **Next**.



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

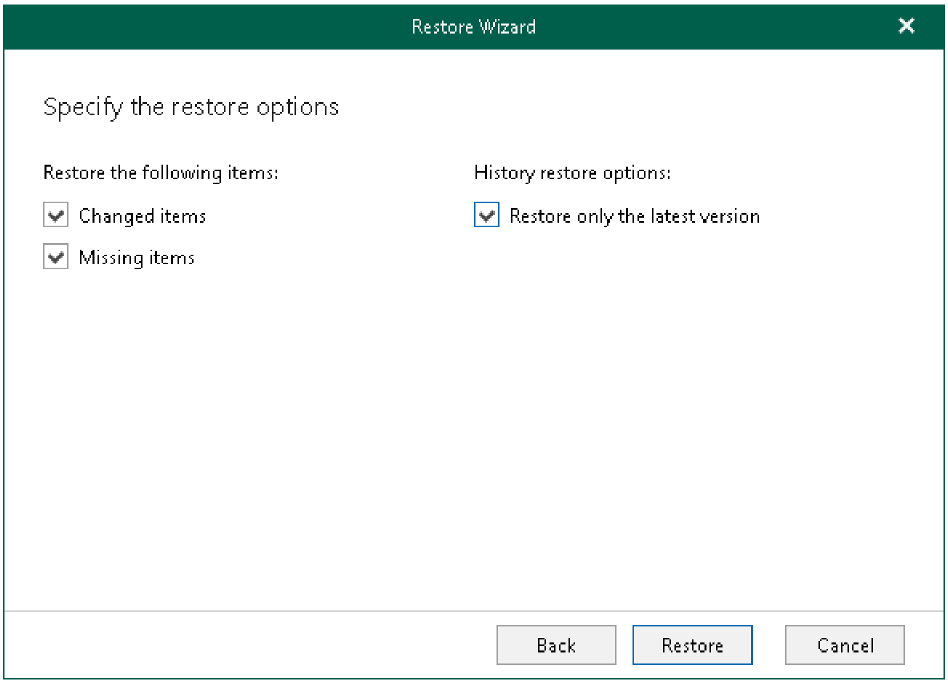
DA5J9EDF5

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

Step 4. Specify Restore Options

At this step of the wizard, specify data restore options and start the restore process:

1. Select the **Changed items** check box if you want to restore items that have changed since the time when the backup was created.
2. Select the **Missing items** check box if you want to restore items that are missing in the target location. For example, some of the items were removed and you want to restore them from the backup.
3. By default, Veeam Explorer for Microsoft Teams restores all versions of backed-up files from the backup. If you want to restore only the latest version of a file, select the **Restore only the latest version** check box. If you select this option, Veeam Explorer for Microsoft Teams will merge original files in the production environment with the latest version of the files in the backup.
4. Click **Restore**.



Restore Wizard

Specify the restore options

Restore the following items:

☑ Changed items

☑ Missing items

History restore options:

☑ Restore only the latest version

Data Export

You can use Veeam Explorer for Microsoft Teams to export posts published in a team channel to a file of the HTML format. You can choose to export all posts of a channel, export posts created during a specified time period or export individual posts.

The export operation can be useful, for example, if you want to restore posts of a team channel to another channel. To do this, you can export posts to an HTML file, publish this file in Microsoft SharePoint and publish a link to this file in a custom tab of the necessary channel.

> **TIP:**
>
> Before exporting data, make sure to read Considerations and Limitations.

Exporting Multiple Posts

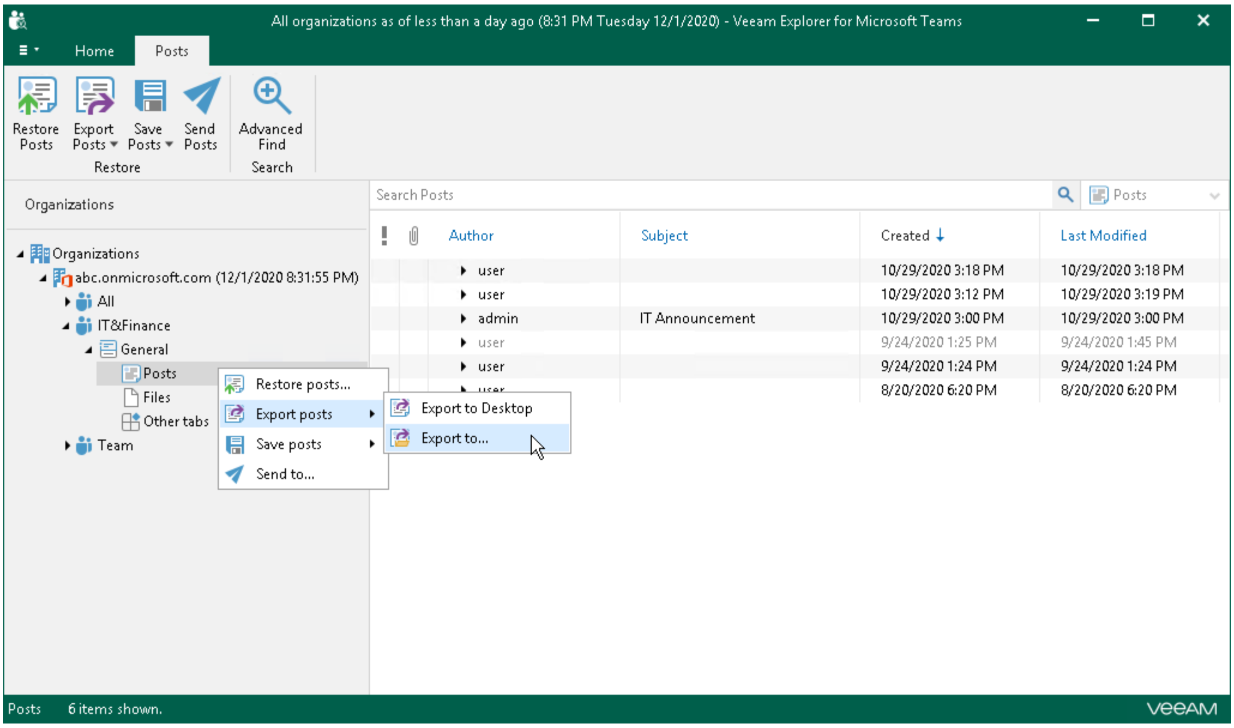
To export posts of a channel, do the following:

1. In the navigation pane, expand a channel whose posts you want to export.
2. In the navigation pane, select **Posts**, click **Export Posts** on the ribbon and select how you want to export posts:

   ○ **Export to Desktop**. Select this option if you want to perform the 1-Click Export operation. Veeam Explorer for Microsoft Teams will immediately export all posts of the channel to the *Desktop* folder.

   ○ **Export to**. Select this option if you want to specify what posts to export and where to export posts.

   Alternatively, in the navigation pane, right-click **Posts** and select **Export posts** > **Export to Desktop** or **Export posts** > **Export to**.



Author	Subject	Created	Last Modified
user		10/29/2020 3:18 PM	10/29/2020 3:18 PM
user		10/29/2020 3:12 PM	10/29/2020 3:19 PM
admin	IT Announcement	10/29/2020 3:00 PM	10/29/2020 3:00 PM
user		9/24/2020 1:25 PM	9/24/2020 1:45 PM
user		9/24/2020 1:24 PM	9/24/2020 1:24 PM
user		8/20/2020 6:20 PM	8/20/2020 6:20 PM

3. If you selected the **Export to** option at the step 2, in the **Export** wizard, do the following:

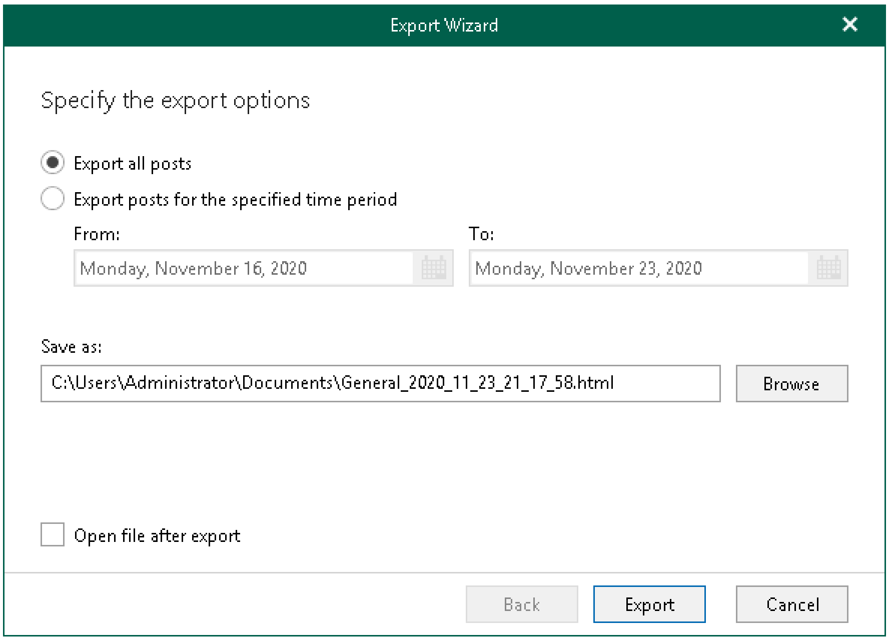
   a. Specify what posts you want to export. You can select from the following options:

      - **Export all posts**. If you select this option, Veeam Explorer for Microsoft Teams will export all posts published in the channel to an HTML file.
      - **Export posts for the specified time period**. If you select this option, you can define a time period when posts that you want to export were created. To do this, specify the start date and end date of the period in the **From** and **To** fields. Veeam Explorer for Microsoft Teams will export posts whose last modification date belongs to the specified period.

   b. In the **Save as** field, click **Browse** and browse to a directory where you want to save an HTML file with exported posts. By default, Veeam Explorer for Microsoft Teams exports posts to a file with the following name: *<Channel_name>_<date_and_time>.html*. For example: *General_2020_08_31_04_47_34.html*.

c. Select the **Open file after export** check box if you want to open the resulting HTML file right after the export operation is completed.

d. Click **Export**.



Export Wizard

Specify the export options

● Export all posts

○ Export posts for the specified time period

From: Monday, November 16, 2020

To: Monday, November 23, 2020

Save as: C:\Users\Administrator\Documents\General_2020_11_23_21_17_58.html

□ Open file after export

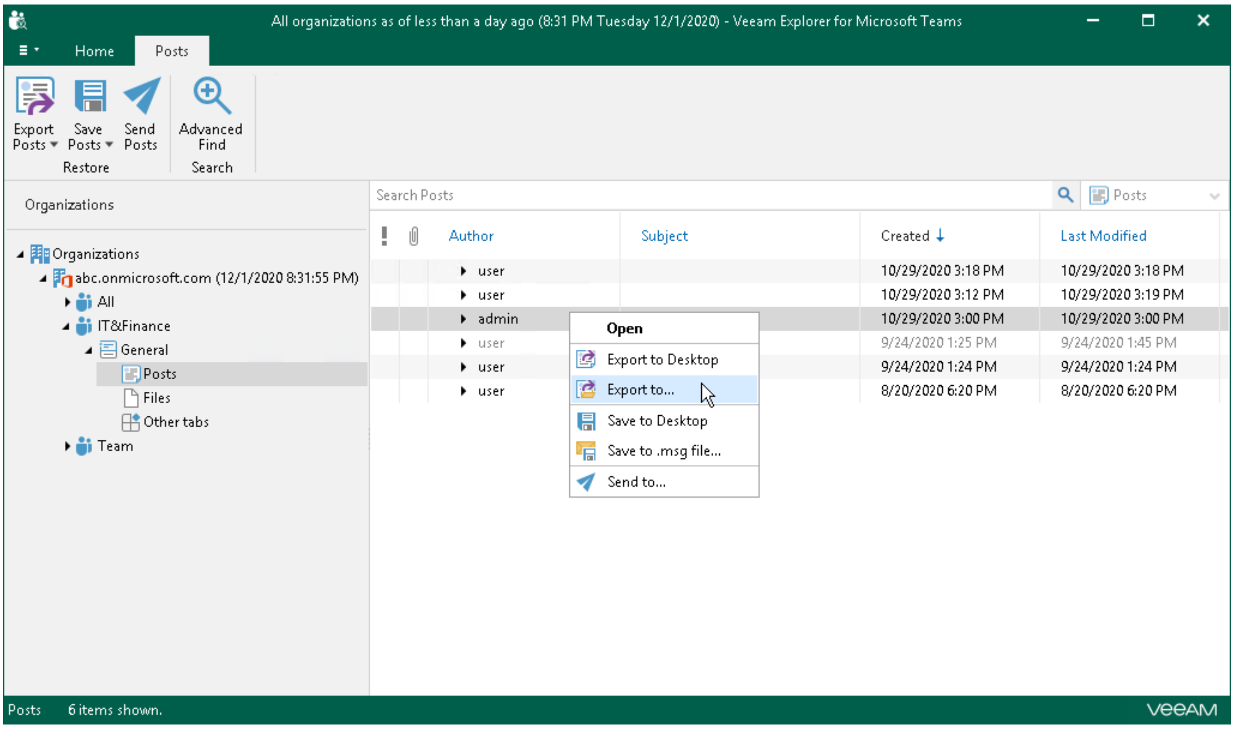
Exporting Individual Posts

To export a specific post of a channel, do the following:

1. In the navigation pane, expand a channel whose post you want to export and click **Posts**.
2. In the preview pane, select a necessary post, click **Export Posts** on the ribbon and select how you want to export the post:
   - **Export to Desktop**. Select this option if you want to perform the 1-Click Export operation. Veeam Explorer for Microsoft Teams will immediately export the post to the *Desktop* folder.
   - **Export to**. Select this option if you want to export the post to a custom location.

   Alternatively, in the preview pane, right-click a necessary post and select **Export to Desktop** or **Export to**.

   > **TIP:**
   >
   > To select more than one post in the preview pane, press and hold the **[CTRL]** key and select the necessary posts.



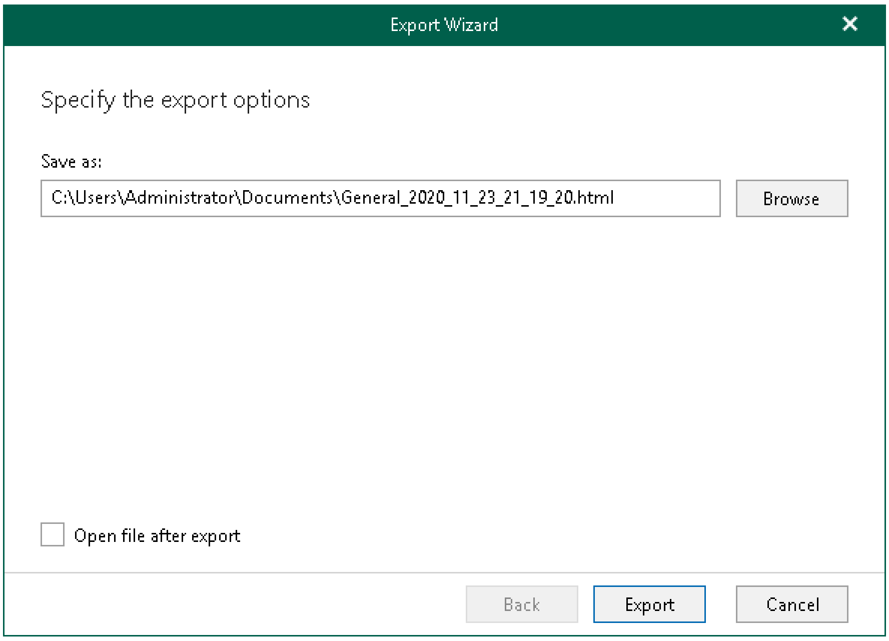
!		Author	Subject	Created	Last Modified
		user		10/29/2020 3:18 PM	10/29/2020 3:18 PM
		user		10/29/2020 3:12 PM	10/29/2020 3:19 PM
		admin		10/29/2020 3:00 PM	10/29/2020 3:00 PM
		user		9/24/2020 1:25 PM	9/24/2020 1:45 PM
		user		9/24/2020 1:24 PM	9/24/2020 1:24 PM
		user		8/20/2020 6:20 PM	8/20/2020 6:20 PM

3. If you selected the **Export to** option at the step 2, in the **Export** wizard, do the following:

   a. In the **Save as** field, click **Browse** and browse to a directory where you want to save an HTML file with exported posts. By default, Veeam Explorer for Microsoft Teams exports posts to a file with the following name: *<Channel_name>_<date_and_time>.html*. For example: *General_2020_08_31_04_47_34.html*.

   b. Select the **Open file after export** check box if you want to open the resulting HTML file right after the export operation is completed.

   c. Click **Export**.



Export Wizard

Specify the export options

Save as:

C:\Users\Administrator\Documents\General_2020_11_23_21_19_20.html

□ Open file after export

Saving Posts

You can use Veeam Explorer for Microsoft Teams to save posts published in a team channel as *Microsoft Exchange Mail Document* (*.msg*) files. You can save all posts of a channel or specific posts. Veeam Explorer for Microsoft Teams saves each post to a separate *.msg* file in the specified location.

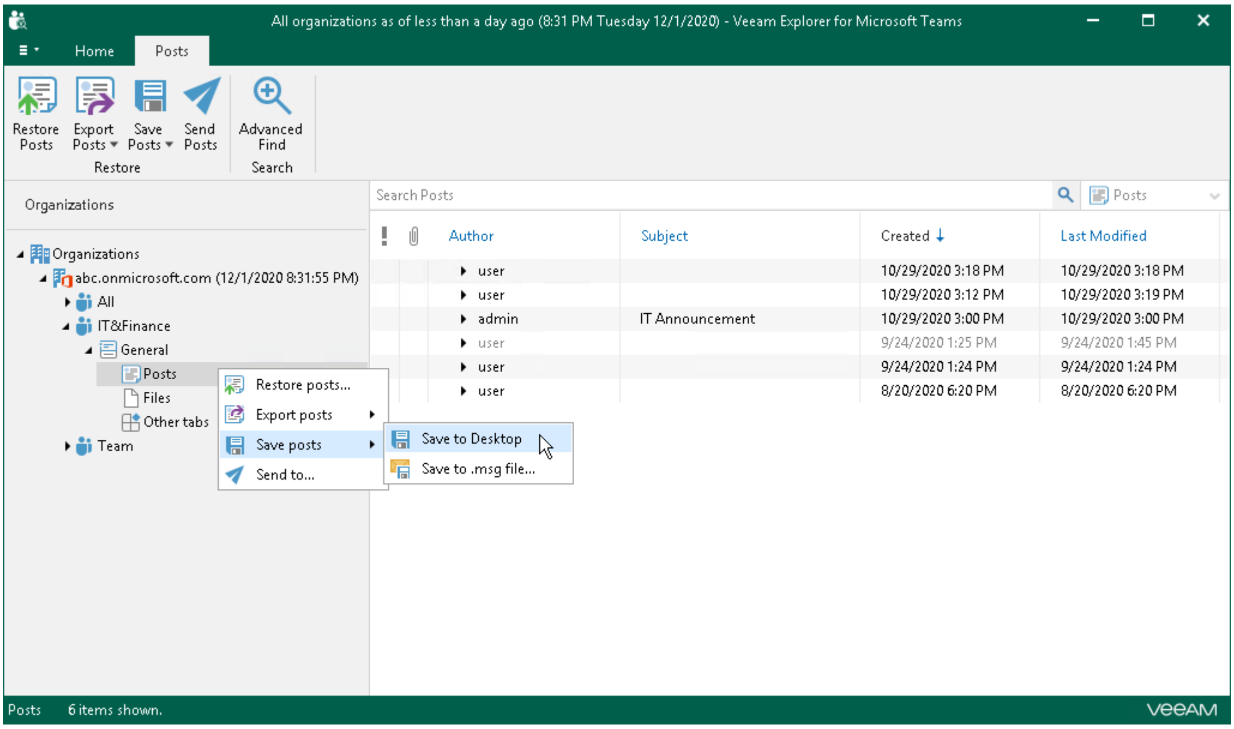
- Saving All Posts of a Channel
- Saving Individual Posts

Saving All Posts of a Channel

To save posts published in a team channel, do the following:

1. In the navigation pane, expand a channel whose posts you want to save.
2. In the navigation pane, select **Posts**, click **Save Posts** on the ribbon and select where you want to save posts:
   - **Save to <folder_name>**. Select this option if you want to perform the 1-Click Save operation. Veeam Explorer for Microsoft Teams will save posts to the latest location that was used when saving posts. If you have not saved posts yet, Veeam Explorer for Microsoft Teams save posts to the *Desktop* folder.
   - **Save to .msg file**. Select this option if you want to save posts to a custom location. To specify a location, in the displayed window, browse to the necessary folder and click **Select Folder**.

   Alternatively, in the navigation pane, right-click **Posts** and select **Save posts** > **Save to <folder_name>** or **Save posts** > **Save to .msg file**.



All organizations as of less than a day ago (8:31 PM Tuesday 12/1/2020) - Veeam Explorer for Microsoft Teams

Author	Subject	Created	Last Modified
user		10/29/2020 3:18 PM	10/29/2020 3:18 PM
user		10/29/2020 3:12 PM	10/29/2020 3:19 PM
admin	IT Announcement	10/29/2020 3:00 PM	10/29/2020 3:00 PM
user		9/24/2020 1:25 PM	9/24/2020 1:45 PM
user		9/24/2020 1:24 PM	9/24/2020 1:24 PM
user		8/20/2020 6:20 PM	8/20/2020 6:20 PM

Posts 6 items shown.

Saving Individual Posts

To save a specific post published in a team channel, do the following:

1. In the navigation pane, expand a channel whose post you want to save and select **Posts**.

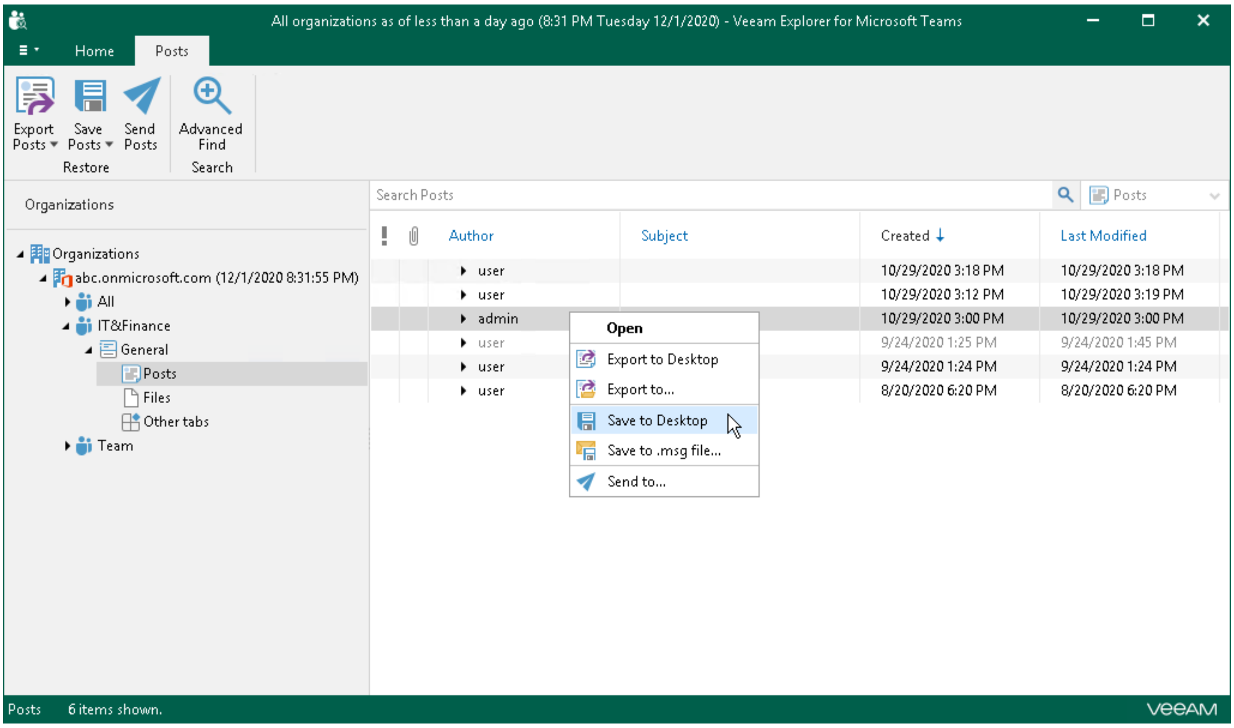
2. In the preview pane, select a necessary post, click **Save Posts** on the ribbon and select where you want to save posts:

   - **Save to <folder_name>**. Select this option if you want to perform the 1-Click Save operation. Veeam Explorer for Microsoft Teams will save posts to the latest location that was used when saving posts. If you have not saved posts yet, Veeam Explorer for Microsoft Teams save posts to the *Desktop* folder.

   - **Save to .msg file**. Select this option if you want to save posts to a custom location. To specify a location, in the displayed window, browse to the necessary folder and click **Select Folder**.

   Alternatively, in the preview pane, right-click a necessary post and select **Save to <folder_name>** or **Save to .msg file**.

   > **TIP:**
   >
   > To select more than one post in the preview pane, press and hold the **[CTRL]** key and select the necessary posts.



Author	Subject	Created	Last Modified
user		10/29/2020 3:18 PM	10/29/2020 3:18 PM
user		10/29/2020 3:12 PM	10/29/2020 3:19 PM
admin		10/29/2020 3:00 PM	10/29/2020 3:00 PM
user		9/24/2020 1:25 PM	9/24/2020 1:45 PM
user		9/24/2020 1:24 PM	9/24/2020 1:24 PM
user		8/20/2020 6:20 PM	8/20/2020 6:20 PM

Saving Files

You can use Veeam Explorer for Microsoft Teams to save files published in a team channel to a specified location. You can save all files of a channel or specific posts.

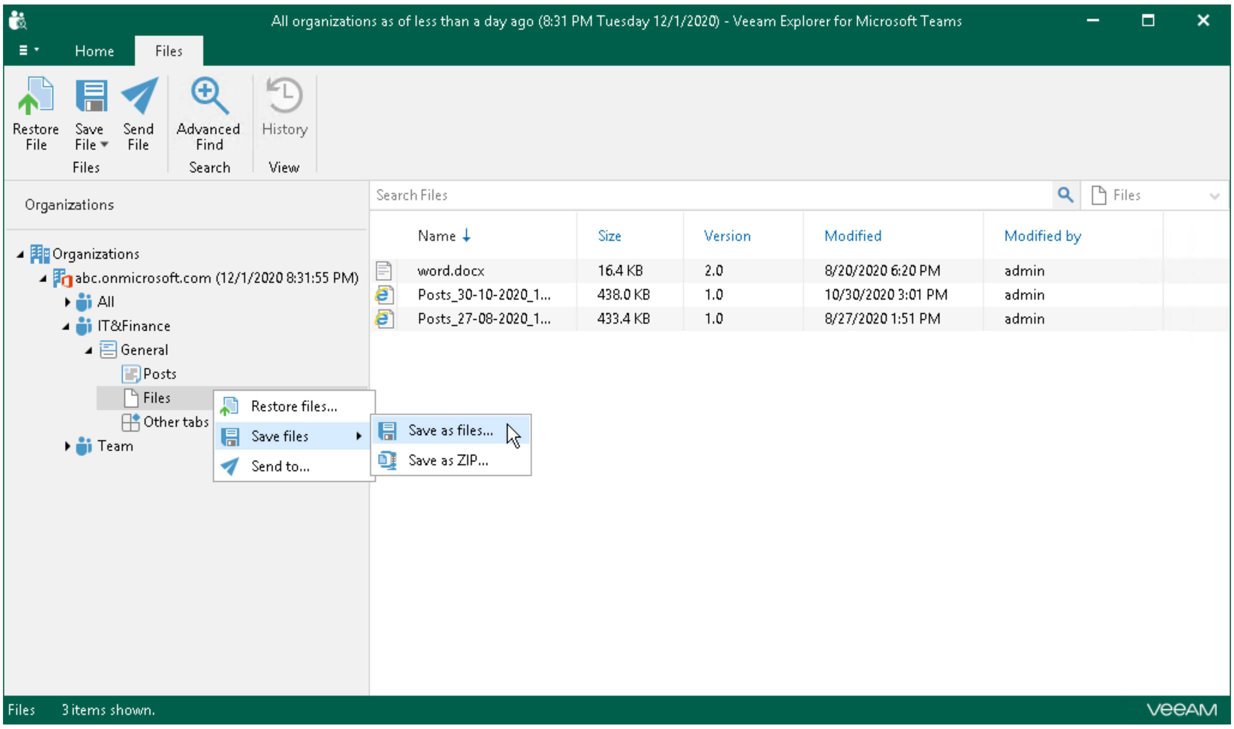
- Saving All Files of a Channel
- Saving Individual Files

Saving All Files of a Channel

To save files published in a team channel, do the following:

1. In the navigation pane, expand a channel whose posts you want to save.
2. In the navigation pane, select **Files**, click **Save File** on the ribbon and select how you want to save files:
   - **Save as files**. Select this option if you want to save each file separately to a specified location. To specify a location, in the displayed window, browse to the necessary folder and click **Select Folder**.
   - **Save as ZIP**. Select this option if you want to add saved files to a ZIP archive and save the resulting archive to a specified location. To specify a location, in the displayed window, browse to the necessary folder and click **Select Folder**. Veeam Explorer for Microsoft Teams will save files to an archive with the *archive.zip* name.

   Alternatively, in the navigation pane, right-click **Files** and select **Save files** > **Save as files** or **Save files** > **Save as ZIP**.



All organizations as of less than a day ago (8:31 PM Tuesday 12/1/2020) - Veeam Explorer for Microsoft Teams

Name	Size	Version	Modified	Modified by
word.docx	16.4 KB	2.0	8/20/2020 6:20 PM	admin
Posts_30-10-2020_1...	438.0 KB	1.0	10/30/2020 3:01 PM	admin
Posts_27-08-2020_1...	433.4 KB	1.0	8/27/2020 1:51 PM	admin

Files 3 items shown.

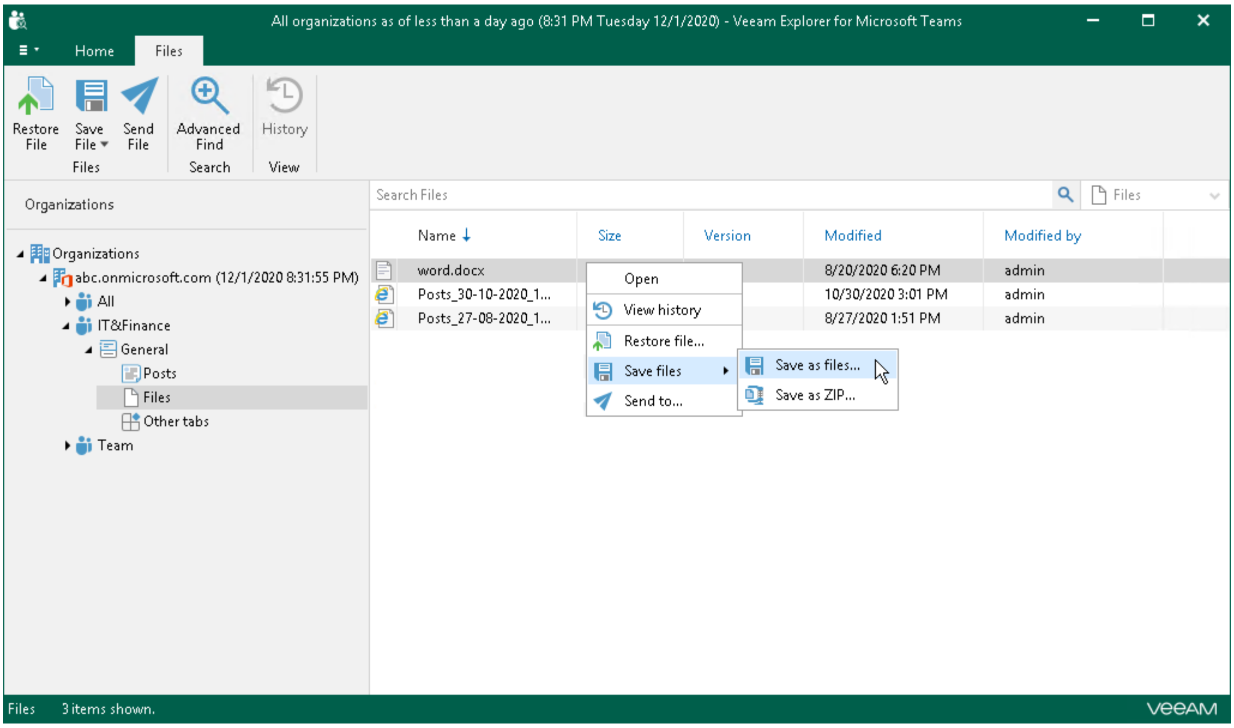
Saving Individual Files

To save a specific file published in a team channel, do the following:

1. In the navigation pane, expand a channel whose post you want to save and select **Files**.
2. In the preview pane, select a necessary file, click **Save File** on the ribbon and select how you want to save files:
   - **Save as files**. Select this option if you want to save each file separately to a specified location. To specify a location, in the displayed window, browse to the necessary folder and click **Select Folder**.
   - **Save as ZIP**. Select this option if you want to add saved files to a ZIP archive and save the resulting archive to a specified location. To specify a location, in the displayed window, browse to the necessary folder and click **Select Folder**. Veeam Explorer for Microsoft Teams will save files to an archive with the *archive.zip* name.

   Alternatively, in the preview pane, right-click a necessary file and select **Save file** > **Save as files** or **Save file** > **Save as ZIP**.

   > **TIP:**
   >
   > To select more than one file in the preview pane, press and hold the **[CTRL]** key and select the necessary files.



Name	Size	Version	Modified	Modified by
word.docx			8/20/2020 6:20 PM	admin
Posts_30-10-2020_1...			10/30/2020 3:01 PM	admin
Posts_27-08-2020_1...			8/27/2020 1:51 PM	admin

Sending Posts and Files

You can use Veeam Explorer for Microsoft Teams to send posts and files published in a team channel to specified recipients by email. You can send all posts or files of a channel or send individual posts or files.

- Sending All Posts or Files of a Channel
- Sending Individual Posts or Files

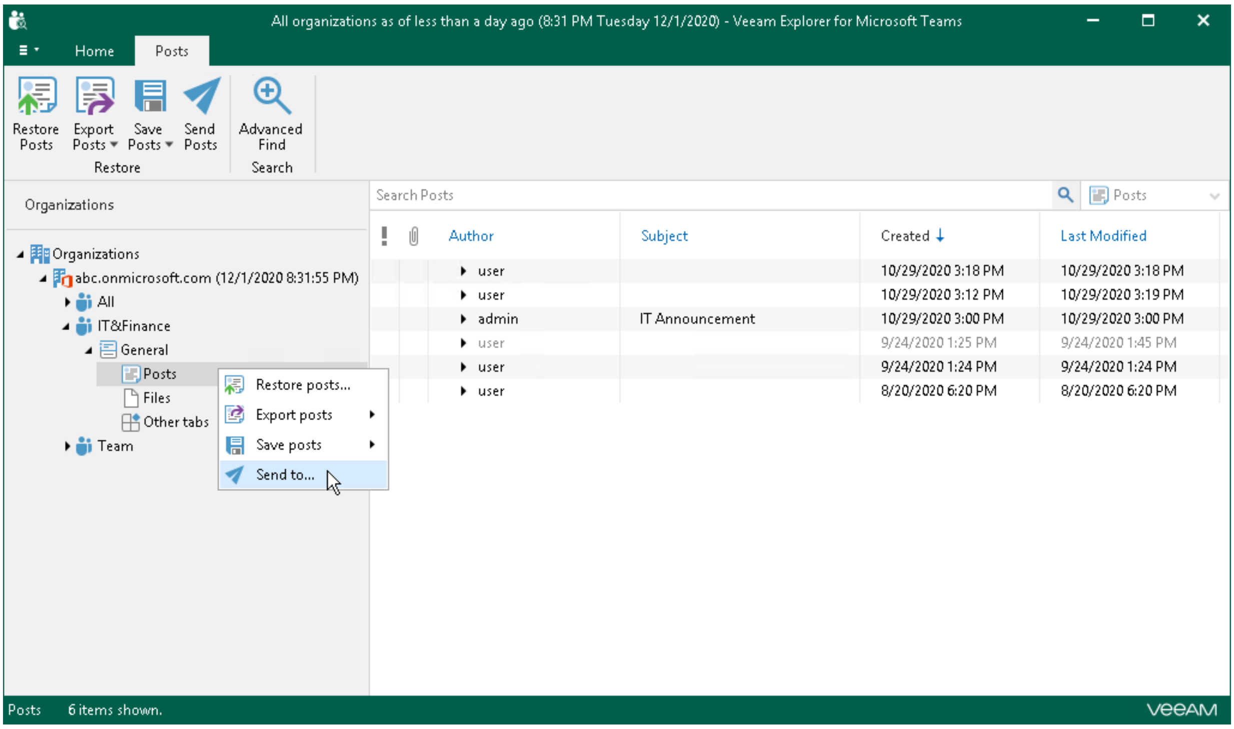
> **TIP:**
>
> Before sending documents, make sure to configure SMTP settings, as described in SMTP Settings. The amount of data you can send at a time depends on your SMTP server configuration.

Sending All Posts or Files of a Channel

To send posts or files of a team channel by email, do the following:

1. In the navigation pane, expand a channel whose posts or files you want to send.
2. In the navigation pane, select **Posts** and click **Send Posts** on the ribbon or select **Files** and click **Send File** on the ribbon.

   Alternatively, in the navigation pane, right-click **Posts** and select **Send to** or right-click **Files** and select **Send to**.



All organizations as of less than a day ago (8:31 PM Tuesday 12/1/2020) - Veeam Explorer for Microsoft Teams

Author	Subject	Created ↓	Last Modified
user		10/29/2020 3:18 PM	10/29/2020 3:18 PM
user		10/29/2020 3:12 PM	10/29/2020 3:19 PM
admin	IT Announcement	10/29/2020 3:00 PM	10/29/2020 3:00 PM
user		9/24/2020 1:25 PM	9/24/2020 1:45 PM
user		9/24/2020 1:24 PM	9/24/2020 1:24 PM
user		8/20/2020 6:20 PM	8/20/2020 6:20 PM

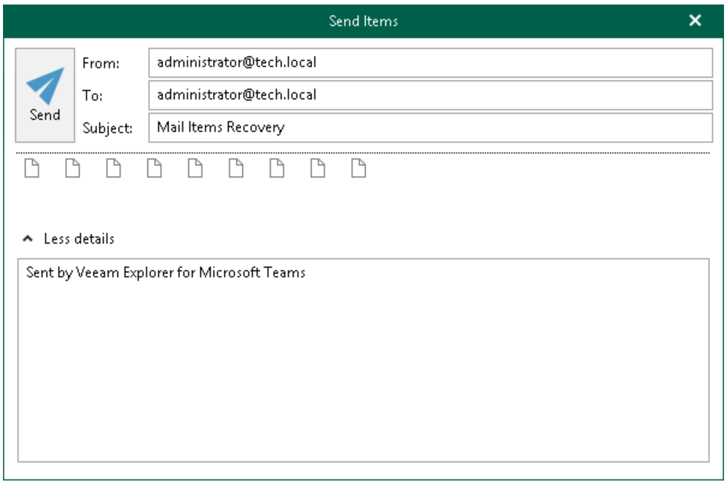
Posts 6 items shown.

3. In case the size of the message with files exceeds the size allowed by your SMTP server configuration, Veeam Explorer for Microsoft Teams will prompt whether you want to send files. In the notification window, click **Yes**.

4. In the **Send Items** window, provide a recipient address.

   The **From** field is filled automatically based on the address you have provided when configuring SMTP settings.

   You can also edit the message subject and body. To edit the message body, click **More details**.



From: administrator@tech.local

To: administrator@tech.local

Subject: Mail Items Recovery

Sent by Veeam Explorer for Microsoft Teams

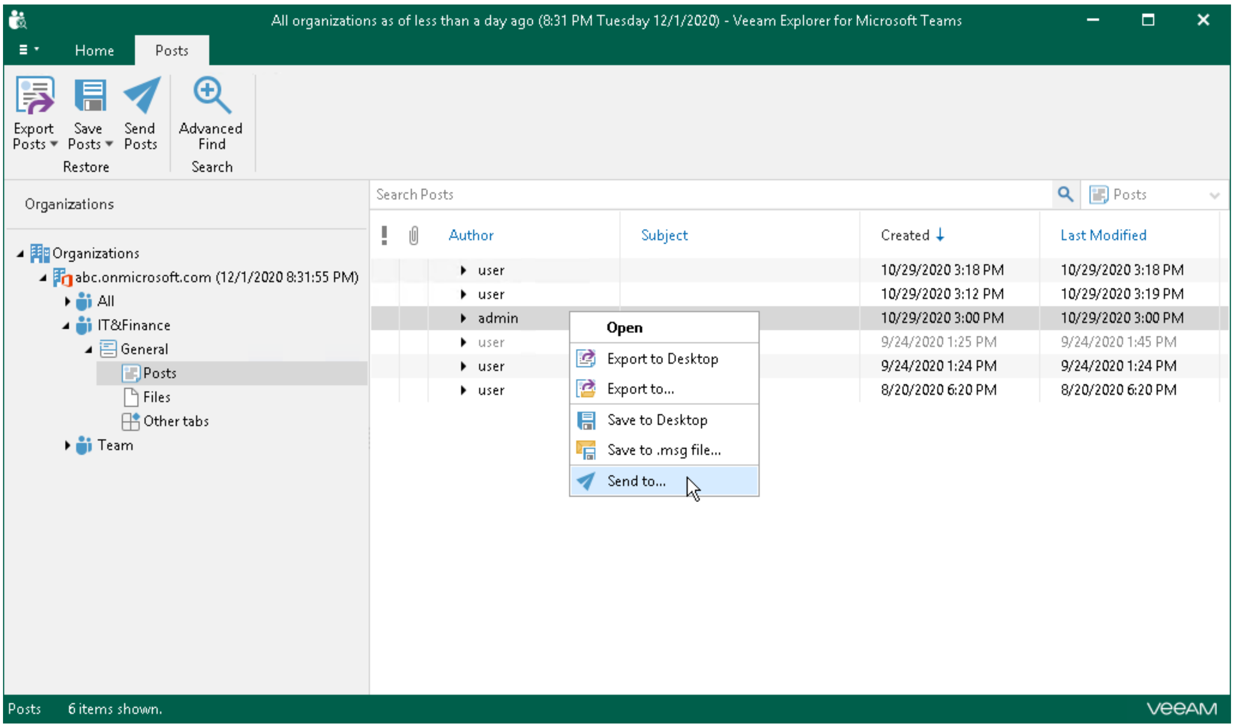
Sending Individual Posts or Files

To send a specific post or file of a team channel by email, do the following:

1. In the navigation pane, expand a channel whose post or file you want to send and select **Posts** or **Files**.

2. In the preview pane, select a necessary post or file and click **Send Posts** or **Send File** on the ribbon.

   Alternatively, in the preview pane, right-click a necessary post or file and select **Send to**.

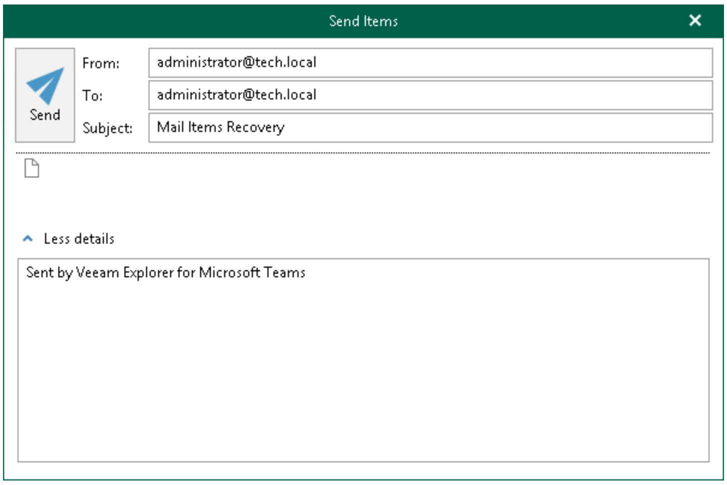


Author	Subject	Created	Last Modified
user		10/29/2020 3:18 PM	10/29/2020 3:18 PM
user		10/29/2020 3:12 PM	10/29/2020 3:19 PM
admin		10/29/2020 3:00 PM	10/29/2020 3:00 PM
user		9/24/2020 1:25 PM	9/24/2020 1:45 PM
user		9/24/2020 1:24 PM	9/24/2020 1:24 PM
user		8/20/2020 6:20 PM	8/20/2020 6:20 PM

3. In the **Send Items** window, provide a recipient address.

   The **From** field is filled automatically based on the address you have provided when configuring SMTP settings.

   You can also edit the message subject and body. To edit the message body, click **More details**.



From: administrator@tech.local

To: administrator@tech.local

Subject: Mail Items Recovery

Sent by Veeam Explorer for Microsoft Teams