Veeam Backup for Microsoft Office 365

Version 3.0

User Guide

April, 2019

> **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 the feedback from our customers. It is important not only to help you quickly with your technical issues, but it is our mission to listen to your input and build products that incorporate your suggestions.

Customer Support

Should you have a technical concern, suggestion or question, visit the Veeam Customer Support Portal at www.veeam.com/support.html to open a case, search our knowledge base, reference documentation, manage your license or obtain the latest product release.

Company Contacts

For the most up to date information about company contacts and offices location, visit www.veeam.com/contacts.html.

Online Support

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

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

About This Document

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

Information hereinafter is applicable to Veeam Backup for Microsoft Office 365 version 3.0 until it is replaced with a newer version of the product.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.

Revision History

Revision #	Date	Change Summary
Revision 1	4/2/2019	Initial version of the document for Veeam Backup for Microsoft Office 365 3.0.

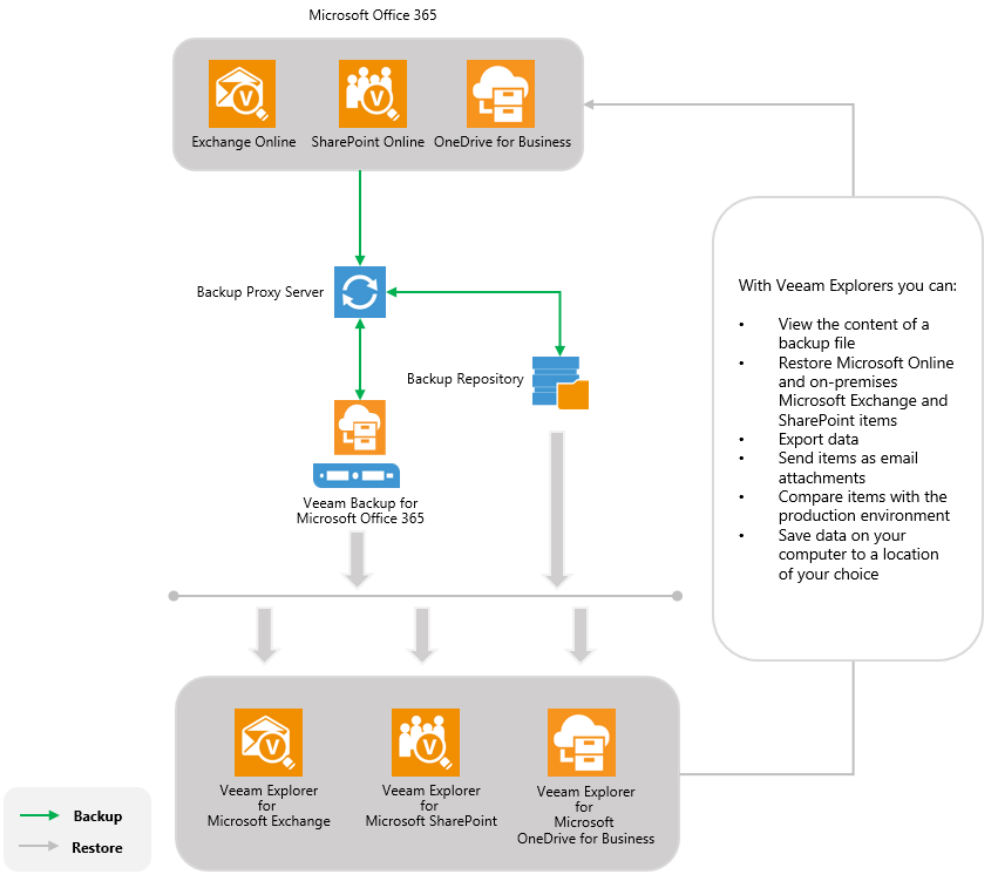
About Veeam Backup for Microsoft Office 365

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

The solution allows you to:

- Back up different types of Microsoft Office 365 and on-premises Microsoft objects such as *Groups*, *Sites*, *Users* and *Organizations*.
- Customize a schedule according to which new backups should be created.
- Restore your data from backups using Veeam Explorer for Microsoft Exchange, Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft OneDrive for Business.
- Review statistical information about backup and restore sessions.
- Use built-in data protection reports.
- Use Veeam Backup for Microsoft Office 365 as a service for service providers and their tenants.

The following figure shows a simplified example of the environment consisting of a Microsoft Office 365 organization, the data of which is being collected and backed up to a backup repository by Veeam Backup for Microsoft Office 365 via the backup proxy server. Next, Veeam Explorers are used to view the content of a backup file and restore, export, save or send data as required.



What's New

The following new features and enhancements have been implemented in Veeam Backup for Microsoft Office 365 version 3.0:

- Up to 30x faster incremental backups for SharePoint Online and OneDrive for Business.
- Backup flexibility for SharePoint Online — personal sites within organizations can now be excluded or included from/to a backup in a bulk.
- Improved security for Office 365 backups and restores with support for multi-factor authentication.
- Flexible protection of services within your Office 365 organization, including exclusive service accounts for Exchange Online and SharePoint Online.
- Internet proxy server support.
- Built-in Office 365 data protection reports.
- Snapshot-based retention — extends the available retention types.
- Extended search options in the backup job wizard. Now it is possible to search for objects by name, email alias and office location.
- On-demand backup jobs — to create backup jobs without a schedule and run them upon request.
- The ability to rename existing organizations — to keep a clean view on multiple tenant organizations presented in Veeam Backup for Microsoft Office 365.

Planning and Preparation

Continue with this section to learn more about configuring your environment before installing Veeam Backup for Microsoft Office 365.

System Requirements

The following system requirements are applicable to Veeam Backup for Microsoft Office 365 3.0 and must be considered thoroughly prior to the application deployment.

Supported Microsoft Exchange Organizations

Microsoft Exchange Version	Comments
Microsoft Office 365 Exchange Online	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.

NOTE:

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

Supported Microsoft SharePoint Organizations

Microsoft SharePoint Version	Comments
Microsoft Office 365 SharePoint Online	For more information about system requirements and limitations for Microsoft Office 365, see this Microsoft article.
Microsoft SharePoint Server 2019 (experimental), 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

Veeam Backup for Microsoft Office 365 Server

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. ▪ *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
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. ▪ Mail restore requires Veeam Explorer for Microsoft Exchange that is part of Veeam Backup & Replication 9.5 Update 4 or Veeam Backup for Microsoft Office 3.0. ▪ To use PowerShell cmdlets for backup and/or restore, Windows PowerShell 2.0 or higher is required. When using Windows 2012 or 2012R2, Windows PowerShell 2.0 Engine must be installed regardless of the current PowerShell version. ▪ For more information about Microsoft Office 365 system requirements and limitations, see this Microsoft article. ▪ Mail backup is supported for Microsoft Exchange 2013/2016/2019.

IMPORTANT!

Consider the following:

- When you install Veeam Explorer for Microsoft Exchange, Veeam Explorer for Microsoft SharePoint (including Veeam Explorer for Microsoft OneDrive for Business) and Veeam Backup for Microsoft Office 365 on different servers, the OS version on computers with Veeam Explorers must be the same or higher than the OS version on a computer with Veeam Backup for Microsoft Office 365.
- Veeam Explorers can only be installed on a machine hosting Veeam Backup for Microsoft Office 365 3.0 or the *Veeam Backup for Microsoft Office 365 Console* component. You can also use a machine with Veeam Backup & Replication 9.5 Update 4 (or higher) that is deployed either along with any of the above components, or as an independent solution.

Backup Proxy Server

A backup proxy server can be a physical or virtual machine with the Microsoft Windows operating system. For more information about backup proxy servers, see Backup Proxy Servers.

IMPORTANT!

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

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. ▪ *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.
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 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.

Used Ports

The following table lists network ports that must be opened to manage inbound/outbound requests from/to various system components of Veeam Backup for Microsoft Office 365.

From	To	Protocol	Port	Notes
Veeam Backup for Microsoft Office 365 Server	**Microsoft Exchange Online**	TCP	80, 443	To connect to Microsoft Exchange Online organizations.
	Microsoft SharePoint Online	TCP	80, 443	To connect to Microsoft SharePoint Online organizations.
	On-premises Microsoft SharePoint Server	HTTP (HTTPS)	5985 (5986 — used by default)	To connect to on-premises Microsoft SharePoint organizations via the WinRM port.
	On-premises Microsoft Exchange Server	TCP	80, 443	To connect to on-premises Microsoft Exchange organizations.
	Backup Proxy Server	TCP	9193 (used by default)	Must be opened on a backup proxy server to manage inbound/outbound traffic when interacting with the Veeam Backup for Microsoft Office 365 server.
	Veeam Auto-update Server	HTTPS	443	To access the auto-update server and the licensing server. For more information, see Checking for Updates and Installing License.
Components	**Veeam Backup for Microsoft Office 365 Server**	TCP	9191	Must be opened on a Veeam Backup for Microsoft Office 365 server 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)
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	Must be opened on a Veeam Backup for Microsoft Office 365 server to manage inbound/outbound traffic when interacting with: ▪ Veeam Explorer for Microsoft Exchange ▪ Veeam Explorer for Microsoft SharePoint

Backup Proxy Server	**Veeam Backup for Microsoft Office 365 Server**	TCP	9191	Must be opened on a Veeam Backup for Microsoft Office 365 server to manage inbound/outbound traffic when interacting with backup proxy servers. This port can be changed, as described in Editing Backup Proxy Server.
	Microsoft Exchange Online	TCP	80, 443	To connect to Microsoft Exchange Online via EWS (Exchange Web Services).
	On-premises Microsoft SharePoint	HTTP (HTTPS)	5985 (5986)	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	Maintains inbound/outbound traffic.

Required Permissions

Continue with this section to learn more about configuring user accounts.

Required Permissions for Veeam Backup for Microsoft Office 365

Veeam Backup for Microsoft Office 365 (*Veeam Backup for Microsoft Office 365 Service*) uses the *Local System* account. This account must not be changed for any of the Veeam services.

Required Permissions for Microsoft SharePoint and OneDrive for Business Organizations

The account you are using to connect to Microsoft SharePoint organizations (on-premises or Online) must belong to that organization and must conform to the following:

- For *on-premises Microsoft SharePoint* organizations.

  The account being used must be a member of the *Farm Administrator* group and must have the *Site Collection Administrator* role. This role can be assigned either automatically, when adding a new organization with SharePoint services, or manually, as described in Microsoft Organizations Management.

- For *Microsoft SharePoint Online* organizations.

  The account being used must have either the *Global Administrator* role or *SharePoint Administrator* role.

If you prefer to use PowerShell to assign the *SharePoint Administrator* role for organizations with SharePoint Online services, you can 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 MSOL module can be downloaded from this Microsoft page.

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

Required Permissions for Microsoft Exchange Organizations

The account you are using to connect to Microsoft Exchange organizations (on-premises or Online) must belong to that organization; having a mailbox in such an organization is optional.

This account must have the following Exchange roles assigned:

- The *Role Management* role. To grant *ApplicationImpersonation* role.
- The *ApplicationImpersonation* role. To assign this role, the account being used must be a member of the *Organization Management* group.

  This role can be assigned by using any of the following methods:

  - Automatically, when adding organizations with Exchange data.
  - Manually, by using Exchange Management PowerShell cmdlets.
  - Via the Microsoft Exchange control panel. For more information, see this Microsoft article.
- The *Organization Configuration* role. To manage role assignments.
- The *View-Only Configuration* role. To obtain necessary configuration parameters.
- The *View-Only Recipients* role. To view mailbox recipients (required for backup job creation).
- *MailboxSearch* or *MailRecipients* roles. To back up groups.

Assigning ApplicationImpersonation Role via PowerShell

For On-Premises Microsoft Organizations

To assign the *ApplicationImpersonation* role for on-premises organizations via PowerShell, do the following:

1. Connect to the Exchange server.

```
$UserCredential = Get-Credential
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri
http://exchangeServerName/PowerShell/ -Authentication Kerberos -Credential
$UserCredential
Import-PSSession $Session
```

2. Run the following cmdlet to grant the role.

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

For Microsoft Office 365 Organizations

To assign the *ApplicationImpersonation* role for Online organizations via PowerShell, do the following:

1. Connect to the Exchange server.

```
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri
https://outlook.office365.com/powershell-liveid/ -Credential $Credential  -
Authentication Basic -AllowRedirection
Import-PSSession $Session
```

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
```

Required Permissions for Restore

For more information about how to configure user accounts to restore data, see:

- Required Permissions in Veeam Explorer for Microsoft Exchange
- Required Permissions in Veeam Explorer for Microsoft SharePoint

Considerations and Limitations

This section covers considerations and known limitations of Veeam Backup for Microsoft Office 365.

Infrastructure

- Microsoft Windows 2008 operating system is not supported; Windows 2008 R2 SP1 is the minimum supported version.
- Using FAT32 is not recommended due to the limited database size (4GB). Use NTFS or ReFS instead.
- For Microsoft Outlook, the preliminary releases such as *Insider releases* or releases provided by *Monthly Channel Updates* are not supported; Veeam 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.
- A symbolic link configured as a mapped drive is not supported as a repository target.
- 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

- Backup of *In-Place Hold Items* is not supported for on-premises Microsoft Exchange 2013.
- When backing up a public folder, only the root hierarchy mailbox will be available.
- 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.

Restore

- Restore of multiple objects is not supported for public folders.
- Cross-tenant restores in Office 365 is only possible for Exchange Online objects, not for SharePoint sites.
- To restore *In-Place Hold Items* or *Litigation Hold Items* to the original location consider the following:
    - Restore of *In-Place Hold Items* is not supported for on-premises Microsoft Exchange Server 2013 due to EWS limitations.
    - To restore *In-Place Hold Items* of Exchange 2016/2019 mailboxes, these mailboxes must have *In-Place Hold* enabled and applied at least once with the *DiscoveryHolds* system folder creation. Otherwise, restore of *In-Place Hold Items* will fail with the following error: "*Failed to*

restore In-Place Hold Items. Restore of In-Place Hold Items into Exchange 2013 is not supported".

For more information about enabling *In-Place Hold* and *Litigation Hold*, see this Microsoft article.

Licensing and License Types

Veeam Backup for Microsoft Office 365 is licensed per user account of every organization added to the program scope.

A user account consists of:

- *Microsoft Exchange Online or on-premises Microsoft Exchange*

  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*

  OneDrive for Business user licenses are associated with email accounts. This means you cannot use the same license to back up one user email and another user OneDrive for Business account. Note that OneDrive (without *for Business*) is a separate storage service and is not supported in this solution.

- *Microsoft SharePoint Online or on-premises Microsoft SharePoint*

  Each SharePoint user in your Office 365 subscription (or on-premises deployment) that has been granted access to the SharePoint sites needs to be licensed to back up and protect your SharePoint environment. 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 for such a user.

A license is not required for:

- *Shared, resource and group mailboxes*

  Veeam also considers managed mailboxes that have at least one restore point that was created within the last 31 days. If you do not archive a mailbox for 31 days, its license will be revoked and can be applied to another mailbox.

- *Group SharePoint sites*

- *External SharePoint users*

  An external SharePoint user is a user from outside your Office 365 subscription to whom you have given access to one or more sites, files or folders. External authenticated users are limited to basic collaboration tasks, and external anonymous users can edit or view specific documents when given specific permissions.

NOTE:

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

Grace Period

To ensure a smooth license update and provide sufficient time to install a new license file, Veeam offers a grace period. A grace period is a period of time during which the product keeps working in a full-version mode after the license has expired, or the number of mailboxes exceeds the number covered by the license.

License Types

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

- Subscription License

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

- Rental License

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

- Not For Resale License

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

- Evaluation License

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

Subscription License

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

License Expired

Grace period of 1 month granted after the expiration of license for purpose of renewal. During this period, the program functionality is not limited by any means. 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 your 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 process of no more than 10 user accounts or 10% of the license count (whichever is greater) granted if your subscription license has exceeded its limit by up to 10 user accounts or up to 10% of the license count.

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

The grace period in this case equals 1 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 corresponding messages will be displayed in the UI and written to the log.

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

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. Such a license type is distributed only to service providers.

> **NOTE:**
>
> When using a rental license, all user accounts the object of which have been backed up will not consume a license until the first day of the following month.

License Expired

Grace period of 1 month granted after the expiration of license for purpose of renewal. During this period, the program functionality is not limited by any means. 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 your 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 process of no more than 10 user accounts or 10% of the license count (whichever is greater) granted if your rental license has exceeded its limit by up to 10 user accounts or up to 10% of the license count.

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

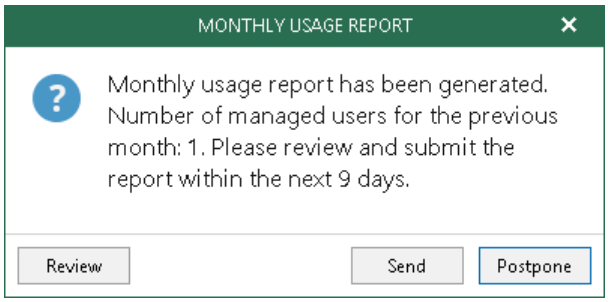
The grace period in this case equals 2 months. After this period, processing of excessive user accounts (in FIFO queue) will be stopped; no more extra accounts will be queued for processing. The corresponding messages will be displayed in the UI and written to the log.

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 program scope.

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



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

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

Managing Reports

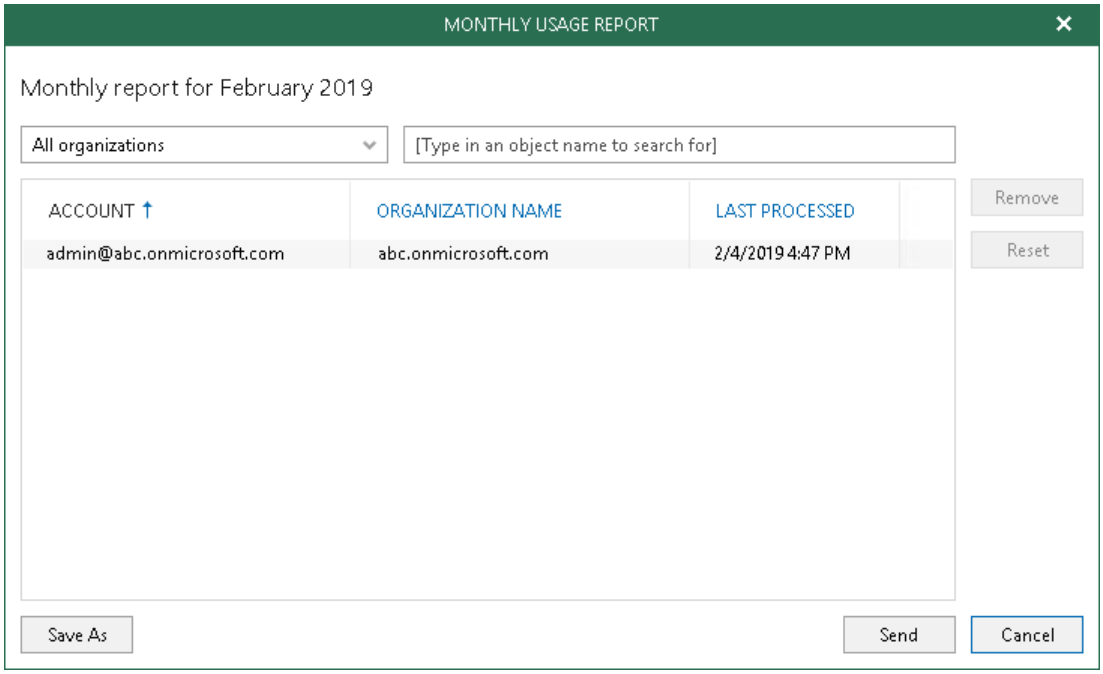
To review details of a report, click **Review** in the lower-left corner of the **Monthly Usage Report** dialog.

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

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

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

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


MONTHLY USAGE REPORT
Monthly report for February 2019
All organizations
[Type in an object name to search for]
ACCOUNT
ORGANIZATION NAME
LAST PROCESSED
admin@abc.onmicrosoft.com
abc.onmicrosoft.com
2/4/2019 4:47 PM
Remove
Reset
Save As
Send
Cancel

Not For Resale License

Not For Resale (NFR) license is a free, 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

The 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

Continue with this section to learn how to deploy Veeam Backup for Microsoft Office 365.

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.Archiver.Service* (display name in the *services.msc* console — *Veeam Backup for Microsoft Office 365 Service*).

    Controls global configuration settings.
  - *Veeam.Archiver.Proxy* (display name in the *services.msc* console — *Veeam Backup Proxy for Microsoft Office 365 Service*).

    Manages backup proxy servers.
  - *Veeam.Archiver.RESTful.Service* (display name in the *services.msc* console — *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 to restore Microsoft Exchange items.

  For more information, see the Veeam Explorer for Microsoft Exchange section of the Veeam Explorers User Guide.
- `VeeamExplorerForSharePoint.msi` — installs Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft OneDrive for Business to restore Microsoft SharePoint and OneDrive items.

  For more information, see the Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft OneDrive for Business sections of the Veeam Explorers User Guide.

The solution can be deployed on virtual or physical machines, or directly to cloud platforms such as Azure or Amazon Web Services.

NOTE:

Consider the following:

- If you have been participating in the public beta testing program of Veeam Backup for Microsoft Office 365, be sure to uninstall the pre-release (*BETA*) versions of Veeam Backup for Microsoft Office 365, Veeam Explorer for Microsoft Exchange and Veeam Explorer for Microsoft SharePoint. In addition, remove both the *C:|VeeamRepository* and *C:|ProgramData|Veeam|Backup365* directories.
- To use the solution in a 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 Exchange server.

Configuring Veeam Backup for Microsoft Office 365 Environment

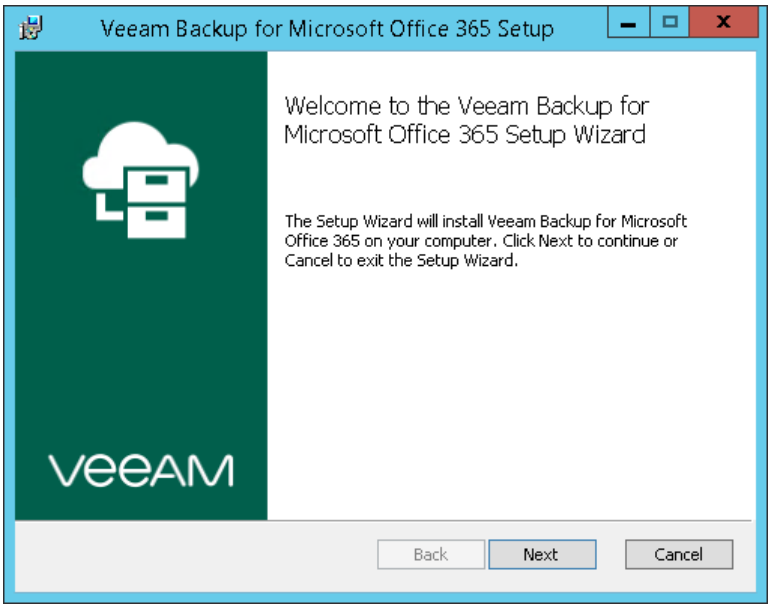
To configure a Veeam Backup for Microsoft Office 365 environment, do the following:

- Install Veeam Backup for Microsoft Office 365, Veeam Explorer for Microsoft Exchange and Veeam Explorer for Microsoft SharePoint, as described in Deployment.
- Add Microsoft Office 365, on-premises Microsoft SharePoint and on-premises Microsoft Exchange organizations to the program scope, as described in Microsoft Organizations Management.
- Configure additional backup proxy servers, as described in Backup Proxy Servers.
- Configure backup repositories, as described in Backup Repositories.
- Configure backup jobs, as described in Data Backup.
- (For service providers and tenants) Manage your Office 365 data, as described in Office 365 Backup as a Service.

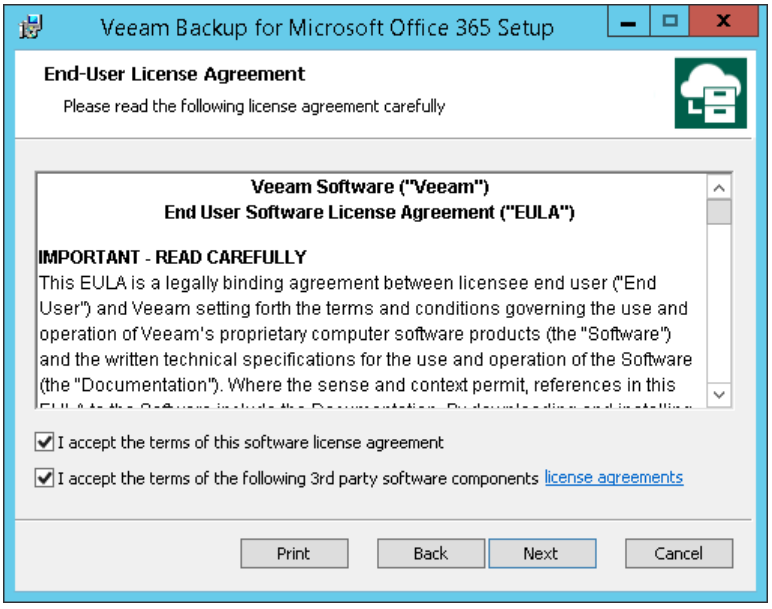
Installing Veeam Backup for Microsoft Office 365

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

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

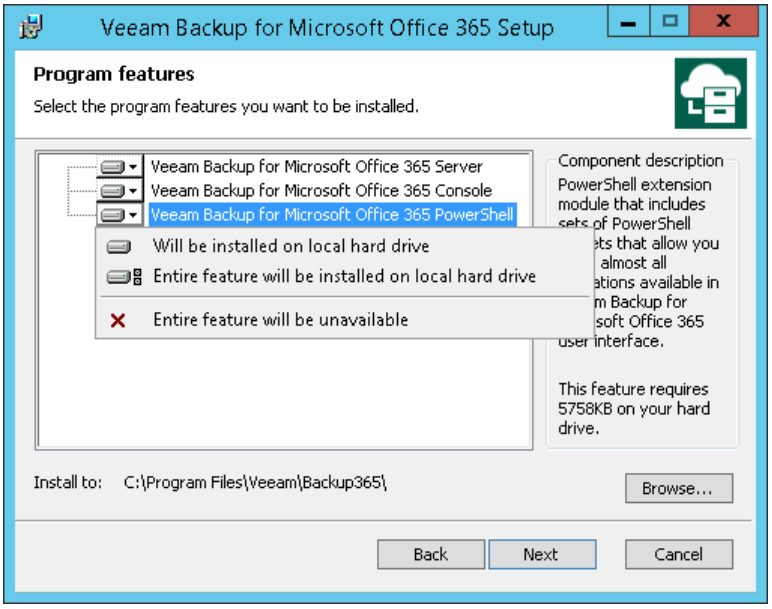


2. Read and accept **License Agreement**.

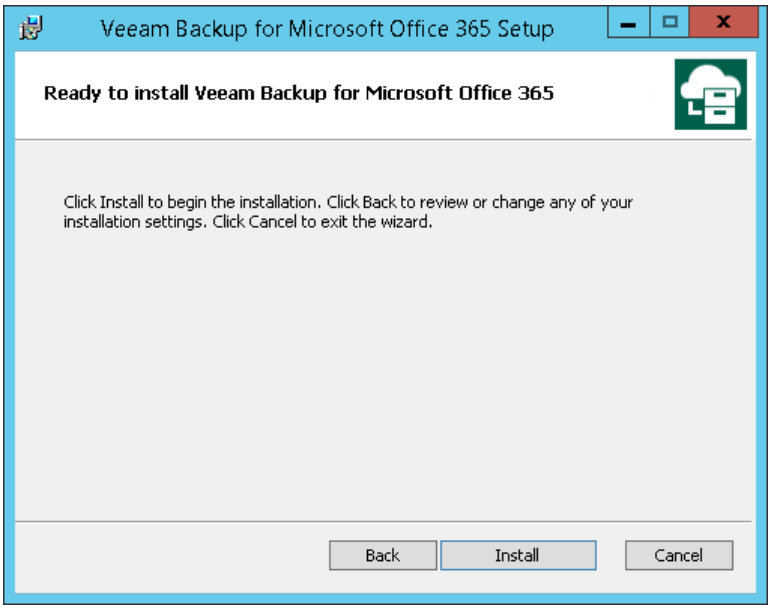


3. Select system components to install.

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



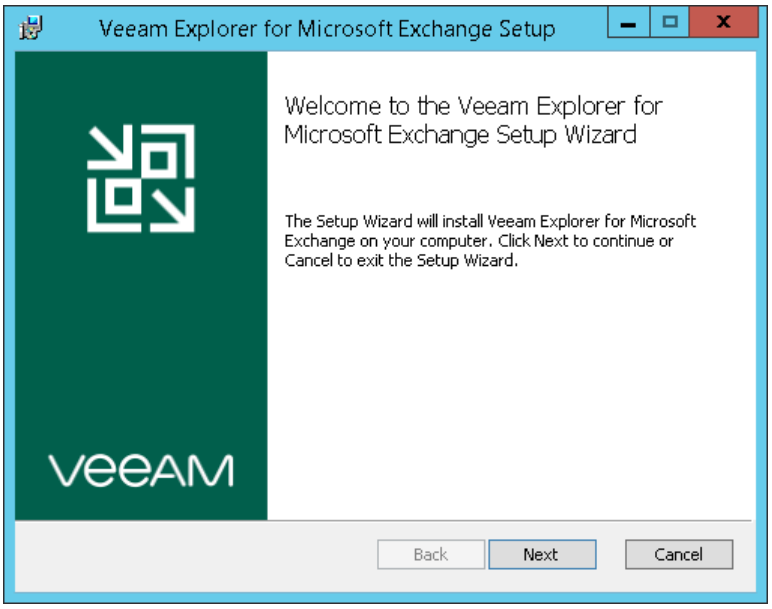
4. Click **Install**.



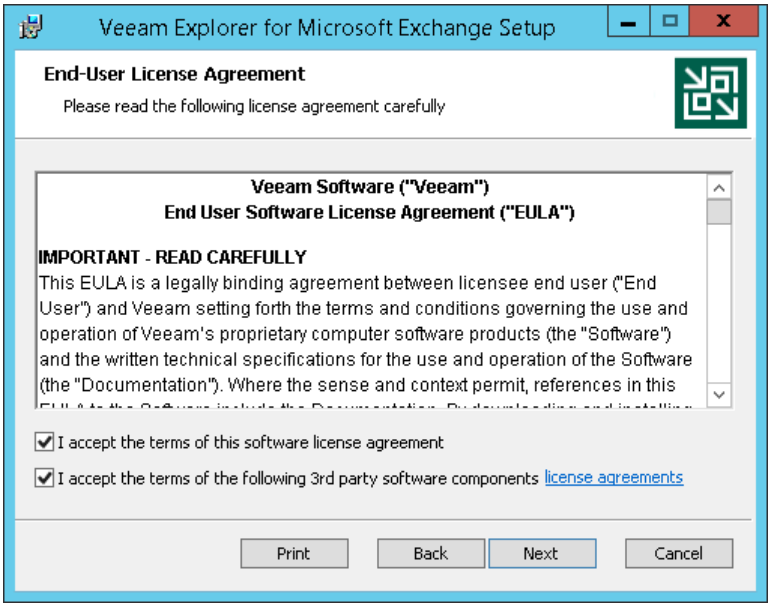
Installing Veeam Explorer for Microsoft Exchange

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

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

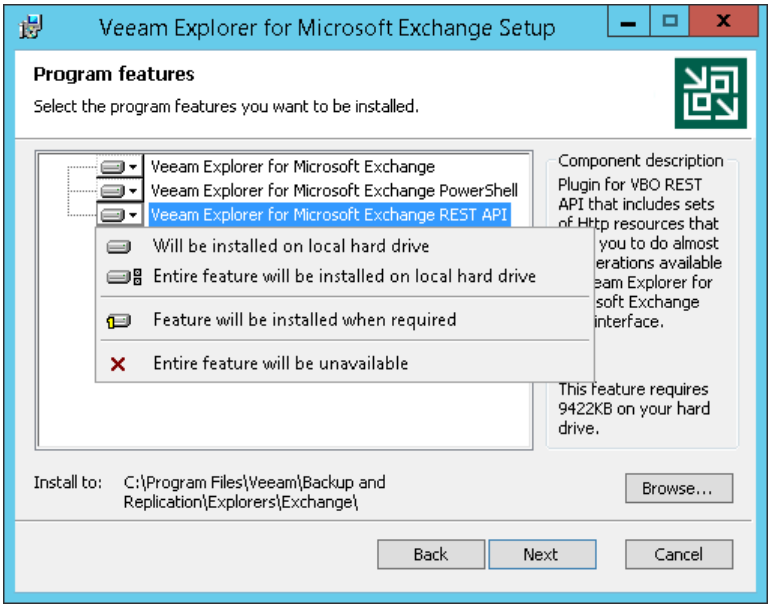


2. Read and accept **License Agreement**.

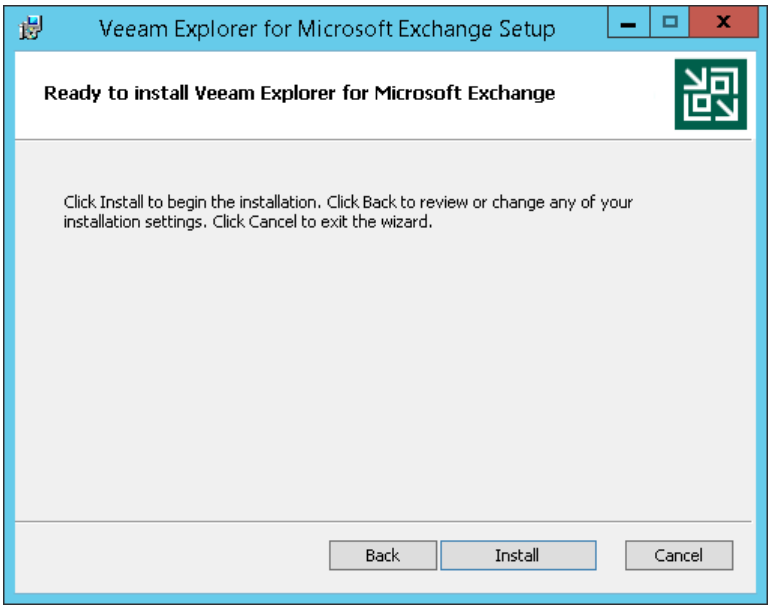


3. Select system components to install.

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



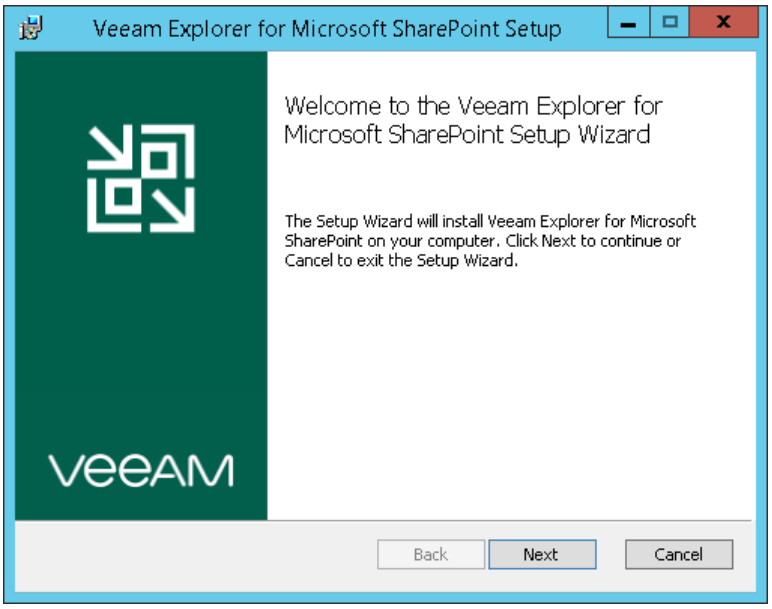
4. Click **Install**.



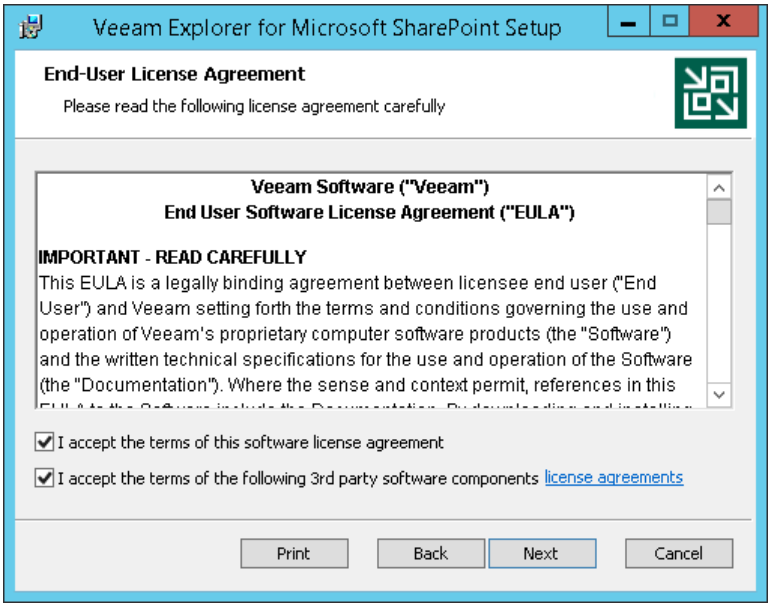
Installing Veeam Explorer for Microsoft SharePoint

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

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

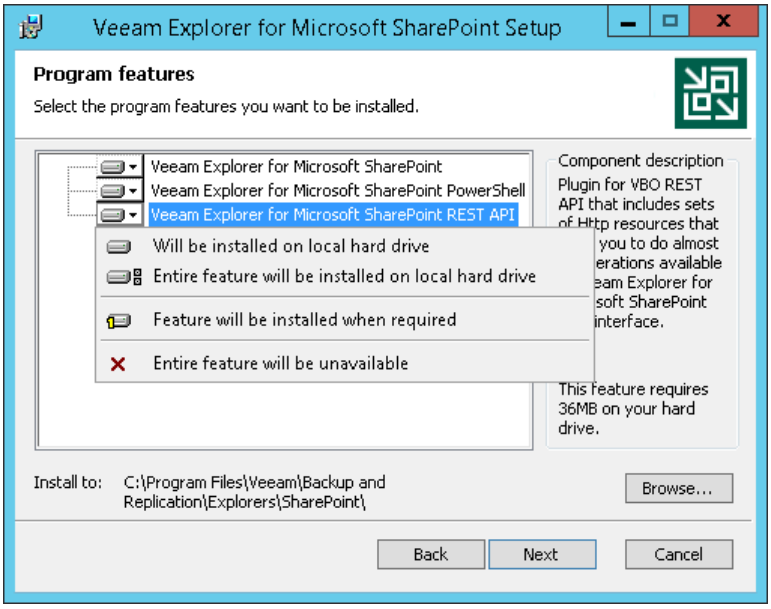


2. Read and accept **License Agreement**.

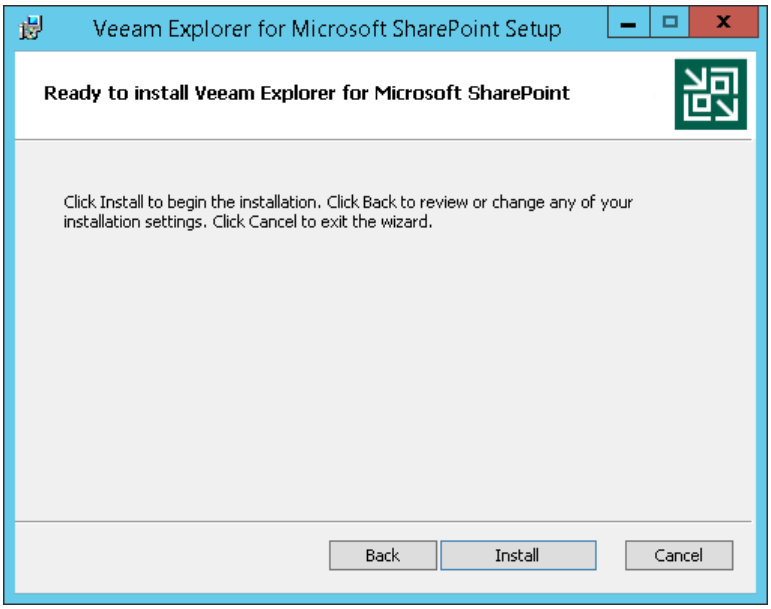


3. Select system components to install.

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



4. Click **Install**.



NOTE:

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

Installing in Unattended Mode

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

The syntax of running an MSI package is as follows:

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

The following table comprises available system components and their corresponding feature names for *Veeam Backup for Microsoft Office 365*.

Component	Feature name
Server	BR_OFFICE365
Console	CONSOLE_OFFICE365
PowerShell	PS_OFFICE365

The following table comprises available system components and their corresponding feature names for *Veeam Explorer for Microsoft Exchange*.

Component	Feature name
UI	BR_EXCHANGEEXPLORER

The following table comprises available system components and their corresponding feature names for *Veeam Explorer for Microsoft SharePoint*.

Component	Feature name
UI	BR_SHAREPOINTEXPLORER
PowerShell	PS_SHAREPOINTEXPLORER

Examples

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

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

To install *Veeam Explorer for Microsoft Exchange* along with the *UI* and *PowerShell* components.

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

To install *Veeam Explorer for Microsoft SharePoint* along with the *UI* and *PowerShell* components.

```
msiexec /i VeeamExplorerForSharePoint.msi /qn ADDLOCAL=BR_SHAREPOINTEXPLORER,
PS_SHAREPOINTEXPLORER ACCEPT_THIRDPARTY_LICENSES=1 ACCEPT_EULA=1
```

NOTE:

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

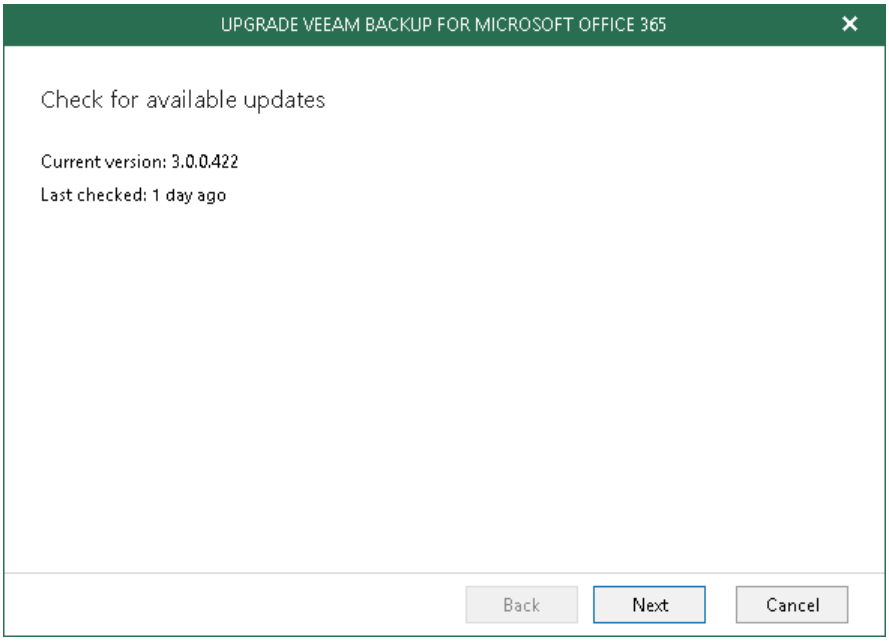
Checking for Updates

Continue with this section to learn more about upgrading the current version of the application with a newer one.

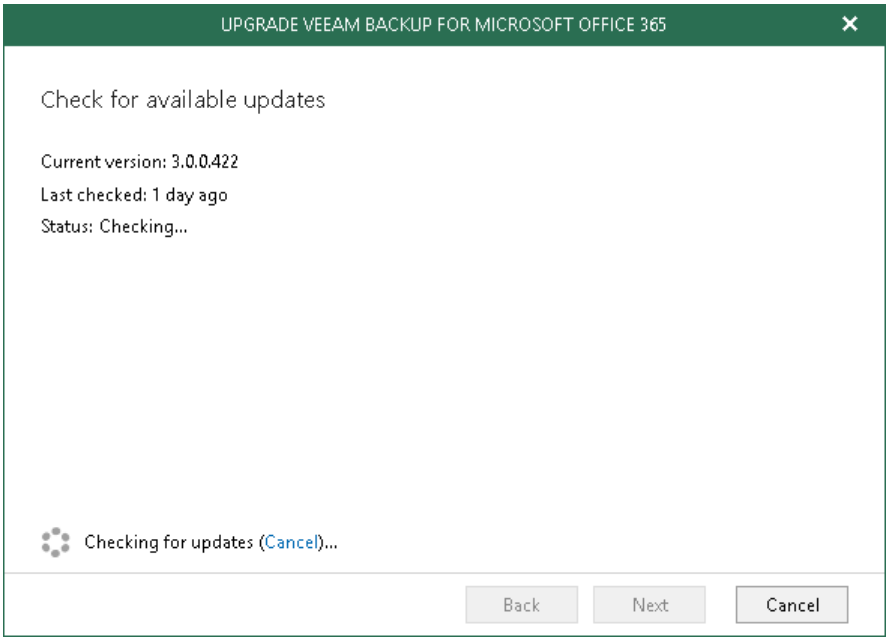
To upgrade the application, do the following:

1. Go to the main menu and click **Upgrade**.
2. At the **Check for available updates** step, click **Next**.

   Make sure to open the port required to access the Veeam auto-update server. For more information, see Used Ports.



3. Wait until Veeam checks whether a newer version is available. To abort the request, click **Cancel**.



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

During the upgrade, Veeam closes the Veeam Backup for Microsoft Office 365 console, whereupon you will be offered to go through the setup steps, as described in Installing Veeam Backup for Microsoft Office 365.

5. Once the installation is complete, launch Veeam Backup for Microsoft Office 365, as described in Launching Veeam Backup for Microsoft Office 365.

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** checkbox on the **Updates** tab, as described in Configuring Update Notifications.

Deploying to Azure and AWS

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

1. Install Veeam Backup for Microsoft Office 365 on an Azure or AWS virtual machine, as described in Installing Veeam Backup for Microsoft Office 365.
2. Configure additional backup proxy servers, as described in Configuring Backup Proxy Servers.
3. Configure backup repositories, as described in Configuring Backup Repositories.
4. Install Veeam Explorer for Microsoft Exchange and Veeam Explorer for Microsoft SharePoint, as described in Installing Veeam Explorer for Microsoft Exchange and Installing Veeam Explorer for Microsoft SharePoint.

After deployment is complete, you can:

- Add Online 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.

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 the *Community Edition* mode that allows you to process up to 10 user accounts in all organizations including 1TB of Microsoft SharePoint data. The *Community Edition* mode suggests using the community license, which is not limited in time, nor imposes any limitations in terms of program functionality.

Installing License

To install a fully-functional license, do the following:

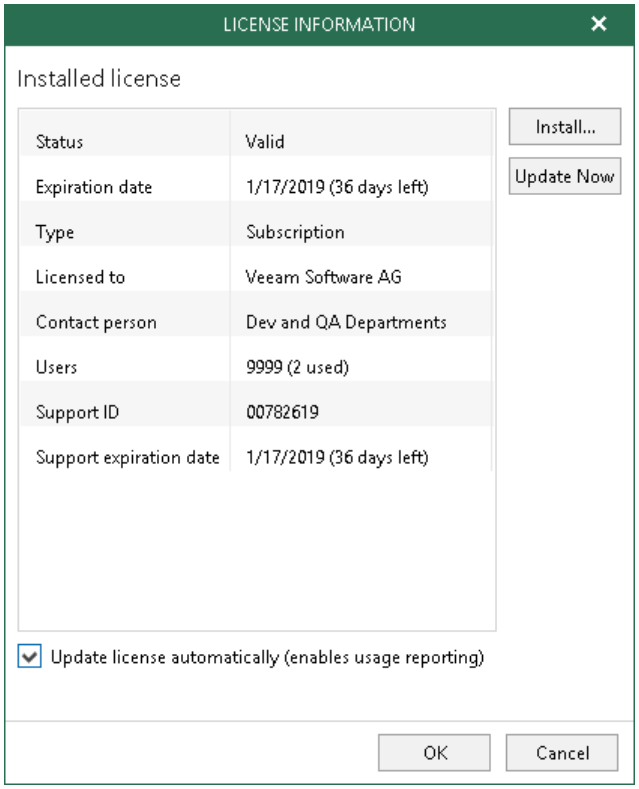
1. Go to the main menu > **License**.
2. In the **License Information** dialog, click **Install** and specify a path to the *.lic* file.

Updating License

To update an existing license with a newer one, click **Update now** on the right-hand side and wait until a new license is downloaded and installed. As an example, updating a license allows you to extend the number of user accounts supported by your current license.

To automatically install a new license, select the **Update license automatically** checkbox.

> **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.



Uninstalling Veeam Backup for Microsoft Office 365

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

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

NOTE:

The backup data in your repositories will not be affected when uninstalling Veeam Backup for Microsoft Office 365.

Upgrading to Veeam Backup for Microsoft Office 365 3.0

Application upgrade to version 3.0 is supported for the following versions of the application:

- Veeam Backup for Microsoft Office 365 1.5 (product builds 1.5.0.1099, 1.5.0.1309 and 1.5.0.1318).
- Veeam Backup for Microsoft Office 365 2.0 (product builds 2.0.0.567, 2.0.0.594 and 2.0.0.814).

Upgrading Application

To upgrade Veeam Backup for Microsoft Office 365, install Veeam Backup for Microsoft Office 365 version 3.0, 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

After you install Veeam Backup for Microsoft Office 365 version 3.0, the following objects will be marked as **Out of Date**:

- Backup repositories
- Backup proxy servers (except for the default one, as it will be upgraded automatically).
- Backup jobs

> **NOTE:**
>
> The upgrade of backup jobs created with the 2.0 version is only required if these jobs contain Microsoft SharePoint sites.

To continue working with any of these objects, make sure to upgrade them manually, as described in:

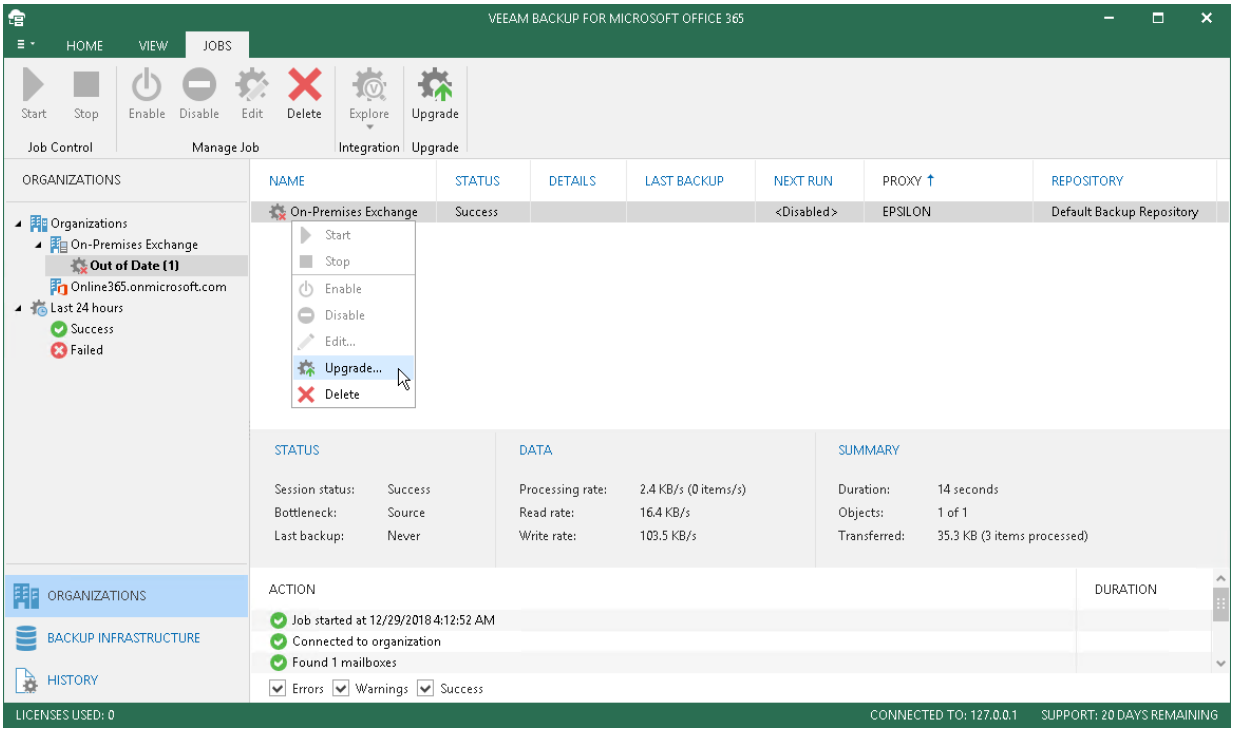
- Upgrading Backup Repositories
- Upgrading Backup Proxy Servers
- Upgrading Backup Jobs

> **NOTE:**
>
> Consider the following regarding the upgrade:
>
> - All modifications made to the `Config.xml` file manually will be lost.
> - No statistical information will be shown in storage consumption reports. For more information, see Generating Storage Consumption Reports.

Upgrading Backup Jobs

To upgrade the backup jobs, do the following:

1. Go to the **Organizations** view.
2. Select the **Out of Date** node.
3. In the preview pane, select a backup job to upgrade.
4. On the **Jobs** tab, click **Upgrade** or right-click a backup job and select **Upgrade**.



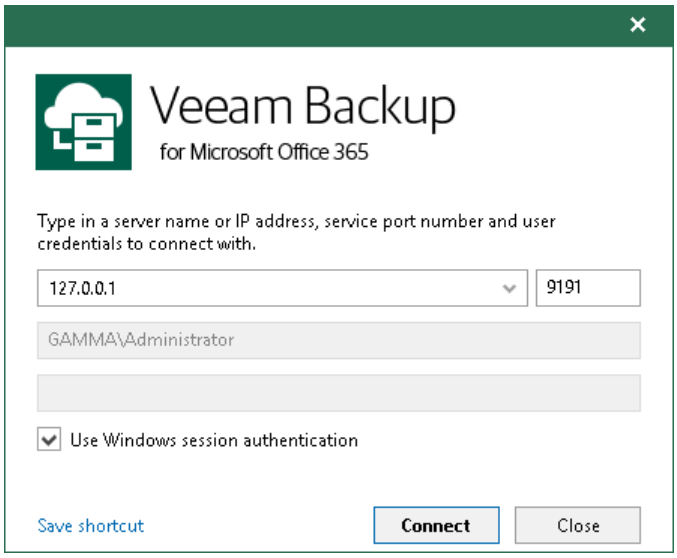
Launching Veeam Backup for Microsoft Office 365

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

1. The target Veeam Backup for Microsoft Office 365 server name or IP-address.
2. The port number via which to connect to the server.
3. User credentials under which to connect to the server.

   The account you are using must be a member of the **Local Administrator** group on a target server. To use your current account, select **Use Windows session authentication**.

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



Launching via Command Line

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

- **/local=true**

  To connect to Veeam Backup for Microsoft Office 356 that is installed on a local machine using the *Local System* account.

  Example:

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

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

  To connect to Veeam Backup for Microsoft Office 356 that is installed on a remote machine using the **/host** and **/port** parameters.

  Example:

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

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

  To connect to Veeam Backup for Microsoft Office 356 that is installed on a remote machine using the **/host** and **/port** parameters.

  You can also provide an account under which to launch Veeam Backup for Microsoft Office 365 using the **/account=<domain\accountName>** format.

  Example:

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

Understanding User Interface

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

Main Menu

The main menu comprises the following options:

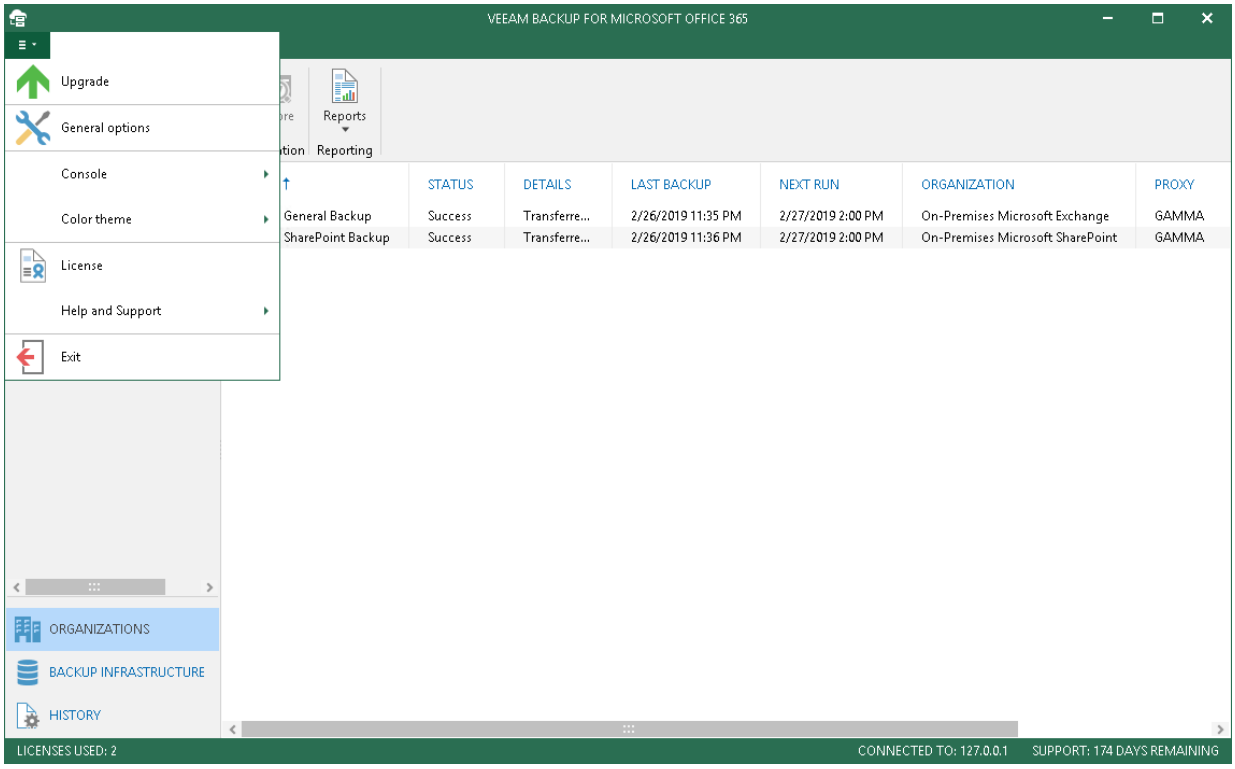
- **Upgrade**. Allows you to upgrade Veeam Backup for Microsoft Office 365.

  For more information, see Checking for Updates.
- **General Options**. Allows you to configure general application options.

  For more information, see Application Settings and Components.
- **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.

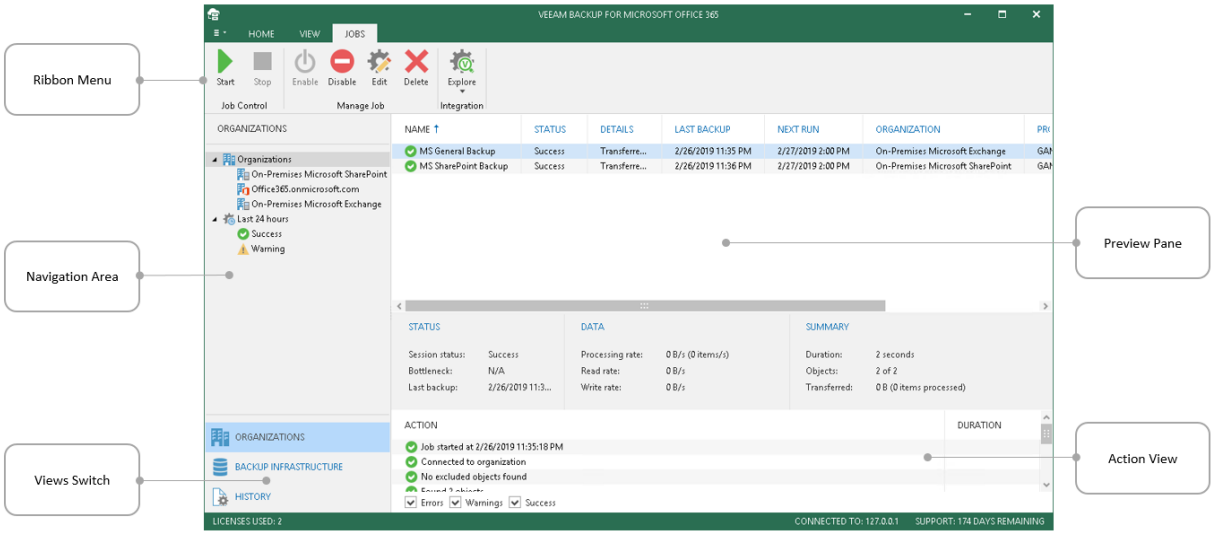
    For more information, see Log Files Export.
  - **About**. Shows product information.
- **Exit**. Closes the program.



Main Application Window

The main application window can be divided into five categories:

1. The ribbon menu, 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, both of which show the backup job progress.
    - The **Jobs** tab contains commands specific for backup jobs.
    - The **Backup Proxy** tab contains commands specific for backup proxies and backup repositories.
2. The navigation area, 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 view switch, which allows you to switch among the infrastructure views such as **Organizations**, **Backup Infrastructure** and **History**.
5. The action view, which allows you to view details about backup jobs results.



TIP:

To open online help, press F1 in any Veeam Backup for Microsoft Office 365 wizard or window. You will be redirected to the corresponding section of the user guide.

Application Settings and Components

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

General Application Settings

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

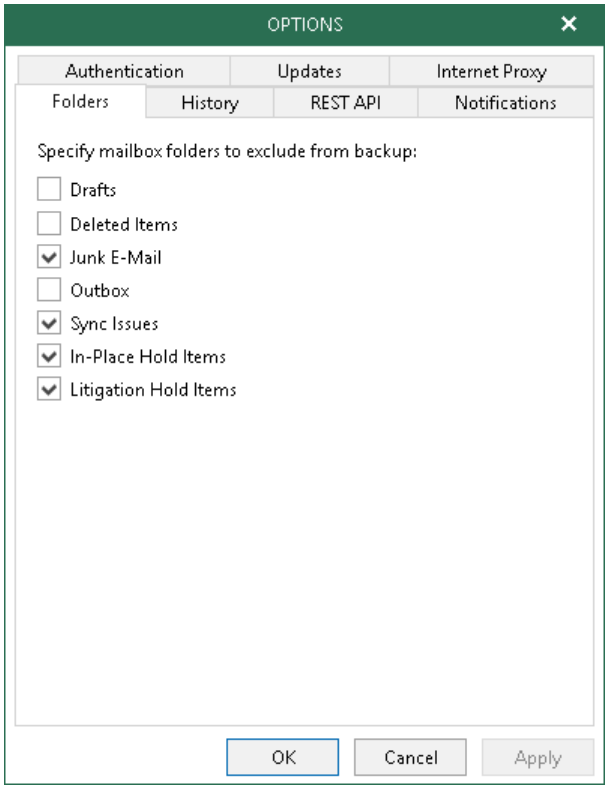
Excluding Folders

Veeam Backup for Microsoft Office 365 allows you to exclude certain folders from a backup.

To exclude a folder, do the following:

1. Go to the main menu and click **General Options**.
2. Go to the **Folders** tab.
3. Select folders you want to exclude and click **OK**.

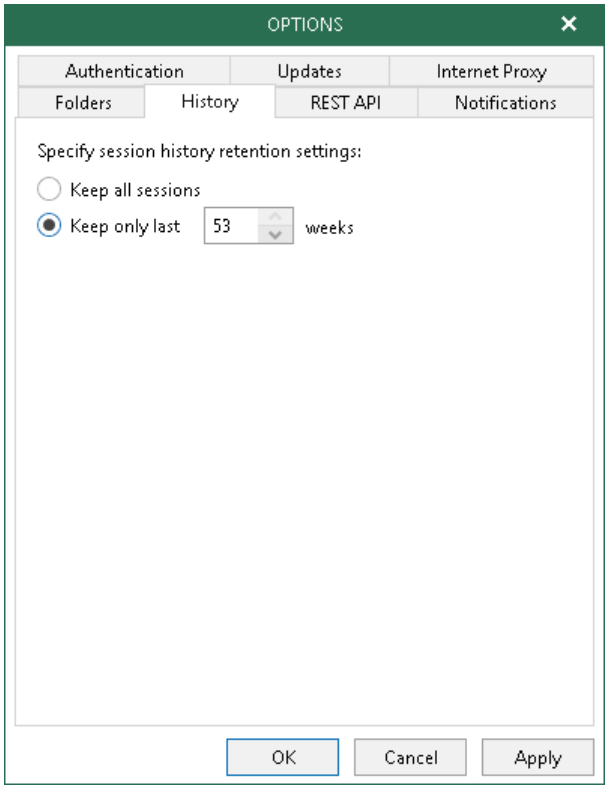
> **NOTE:**
>
> When you select **Deleted Items**, both *deleted* and *permanently* deleted items will be excluded.



Configuring Session Data History

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

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



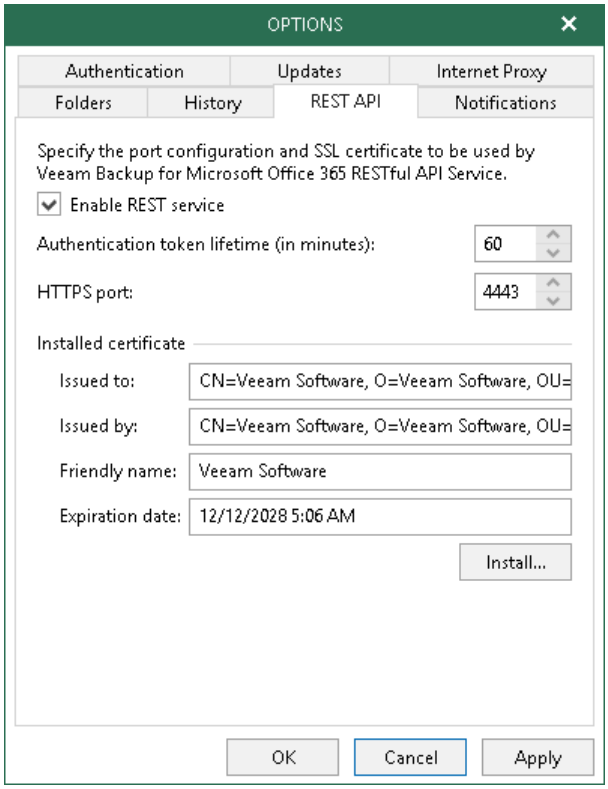
Configuring RESTful API Settings

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

1. Go to the main menu and click **General Options**.
2. Go to the **REST API** tab.
3. Select the **Enable REST Service** checkbox.
4. In the **Authentication token lifetime (in minutes)** field, specify the lifetime value for the authentication token provided by the server.

   RESTful API authorization is based on the OAuth 2.0 Authorization Framework.
5. In the **HTTPS port** field, specify the port number.
6. Click **Install**.

   For more information about installing certificates, see Installing SSL Certificate.

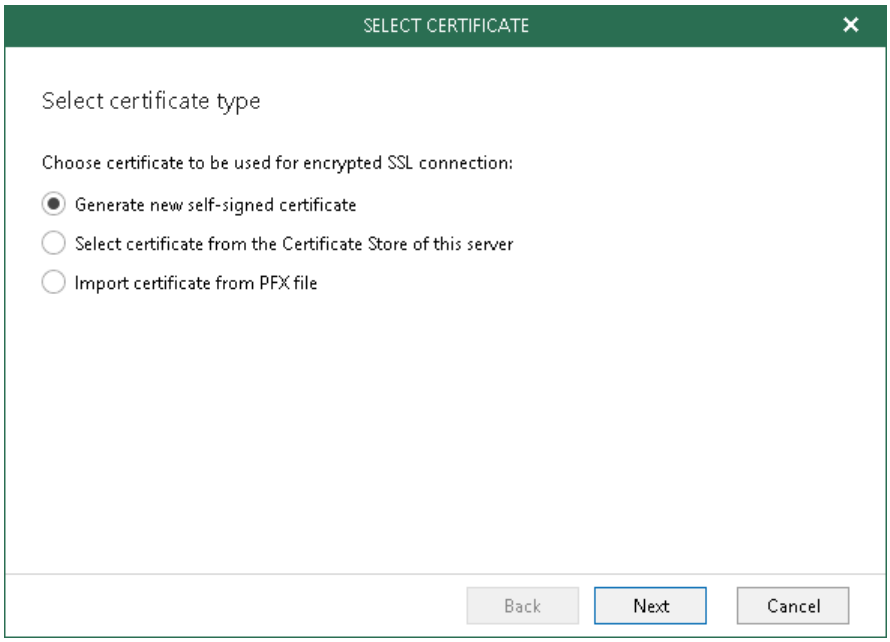


Installing SSL Certificate

An SSL certificate is required when configuring RESTful API settings or enabling user authentication with organization credentials for tenants.

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

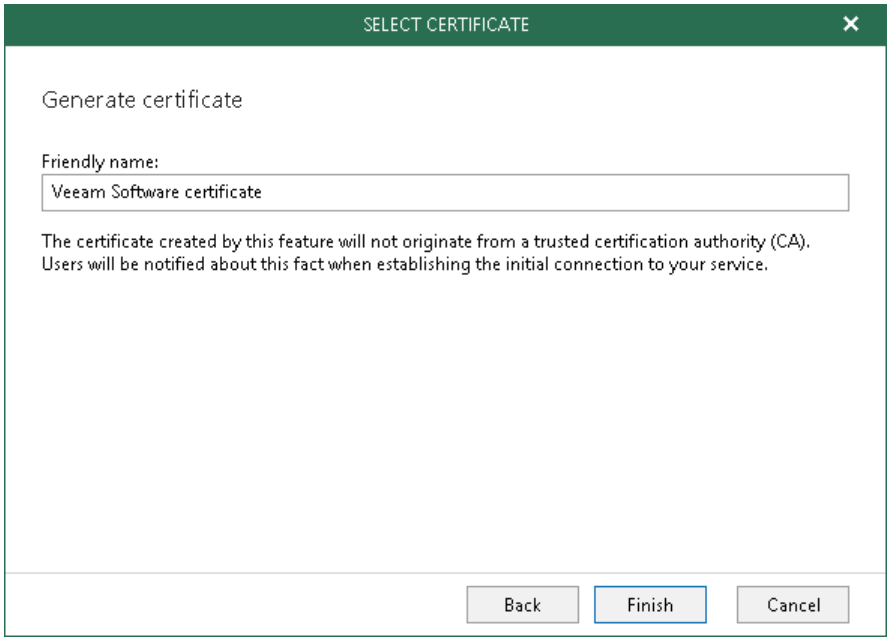
- Generate new self-signed certificate
- Select certificate from the Certificate Store of this server
- Import certificate from the PFX file



Generating New Certificate

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

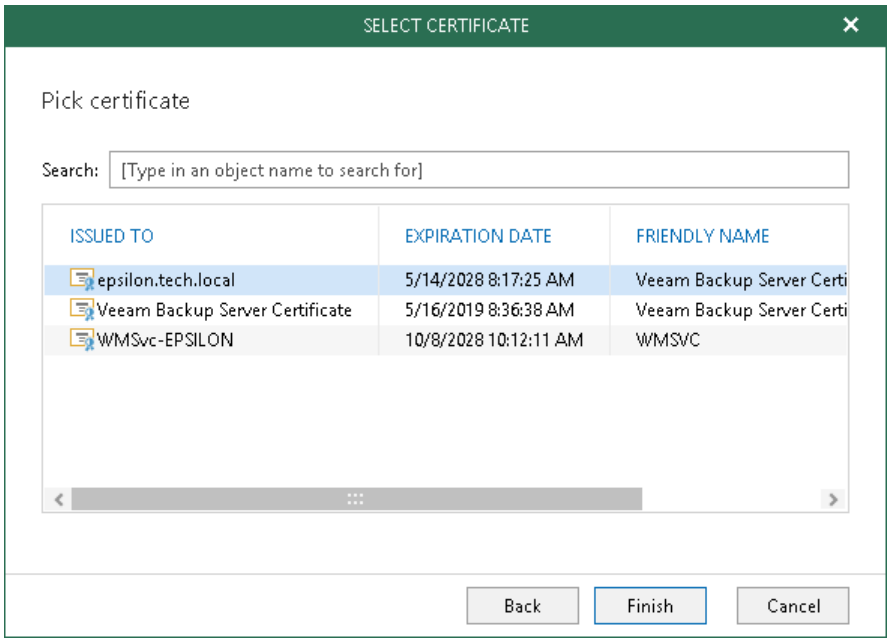
Once generated, the certificate data will be automatically added to the **Installed certificate** section of the **Options** dialog.



Selecting Certificate

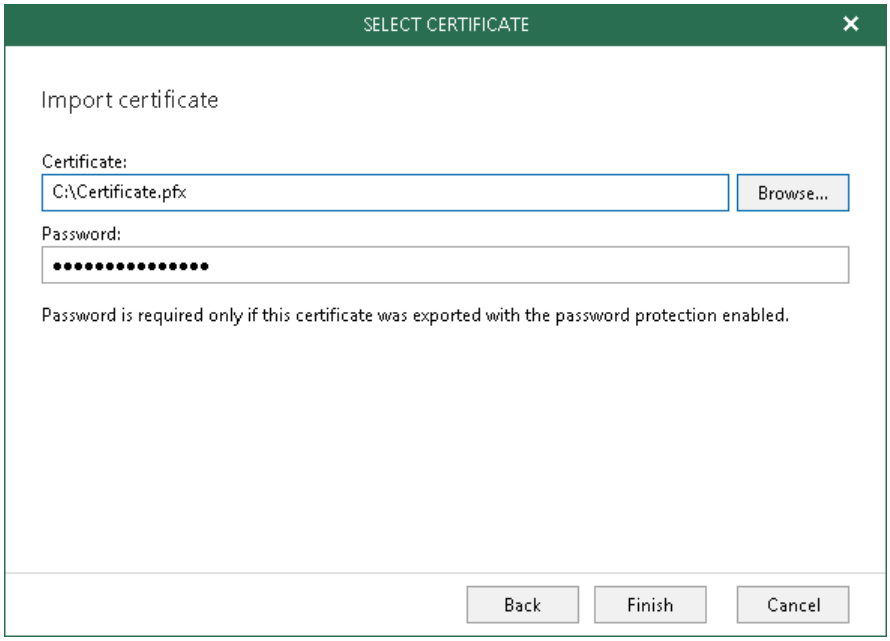
To select an existing certificate from the certificate store, choose a certificate you want to use and click **Finish**.

Once selected, the certificate data will be automatically added to the **Installed certificate** section of the **Options** dialog.



Importing Certificate

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



Configuring Notification Settings

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

> **NOTE:**
>
> Notifications about backup job completion results are sent from a backup proxy server, which you select at the Specify Backup Proxy and Repository step of the new backup job wizard. For more information about backup proxy servers, see Backup Proxy Servers.

To configure email notifications, do the following:

1. Go to the main menu and click **General Options**.
2. Go to the **Notifications** tab.
3. Select the **Enable e-mail notifications**. checkbox.
4. Specify the address of a server you want to use as an SMTP server.
5. To provide advanced settings, click **Advanced** and specify the following:
   - A port number of an STMP server you want to use.

     By default, Veeam Backup for Microsoft Office 365 establishes a connection to **smtp.office365.com** via port **587**. For more information, see this Microsoft article.
   - Select the **Connect Using SSL** checkbox to establish a secure connection.
   - Select the **The SMTP server requires authentication** checkbox and provide authentication credentials.
6. In the **From** field, specify the email address to be shown as a sender.
7. In the **To** filed, specify the email address for a notification recipient.

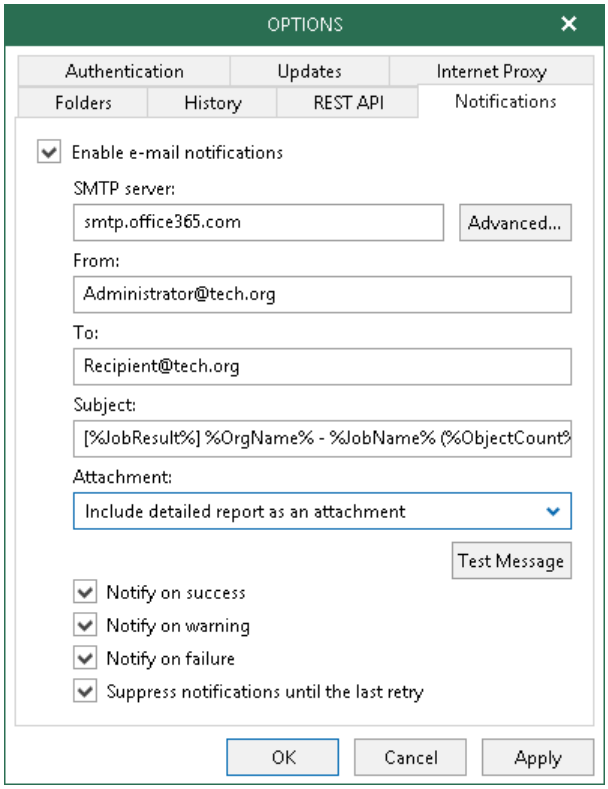
   To specify multiple email addresses, use semicolon.
8. By default, a notification **Subject** will be as follows: *[%JobResult%] %OrgName% - %JobName% (%MailboxCount% mailboxes), %Issues% issues.*

   Where:
   - %JobResult%. A backup job result (Success, Warning, Failed).
   - %OrgName%. An Office 365 organization for which the job was configured.
   - %JobName%. The backup job name.
   - %MailboxCount%. The number of processed mailboxes.
   - %Issues%. The number of mailboxes with *Failed* or *Warning* states.
   - %Time%. Date and time of backup job completion.
9. In the **Attachment** drop-down list, select whether to include a detailed report as an attachment to the email.

   Mind that such a report is only sent if contains more than 1000 users.
10. Click **Test Message** to send a test message.

By default, system notifications are sent every time a backup job completes its sessions with any of the following states: *Success*, *Warning* and *Failure*. To turn off unwanted notifications, clear the corresponding checkboxes.

If a backup job is configured to perform retry attempts, you can select the **Suppress notifications until last retry** checkbox to send notifications only after the last attempt.



Configuring Authentication Settings

Tenants must authenticate themselves to view and recover their backups located on the service provider side.

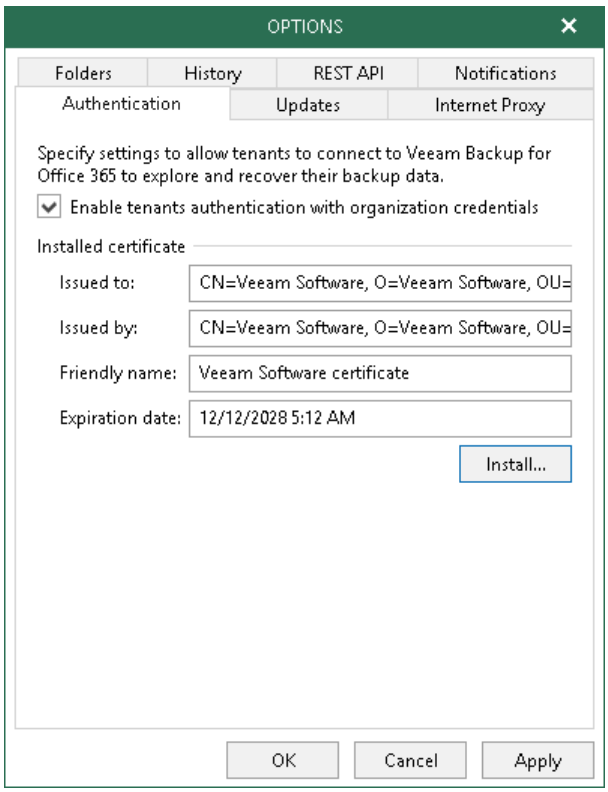
To enable tenant authentication, do the following:

1. Go to the main menu and click **General Options**.
2. Go to the **Authentication** tab.
3. Select the **Enable authentication with organization credentials** checkbox.
4. Click **Install** to specify an SSL certificate.

   You can generate a new certificate or select an existing one using the **Select Certificate** wizard, as described in Installing SSL Certificate.

TIP:

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



Configuring Update Notifications Settings

To configure notifications of a newer version of the application, do the following:

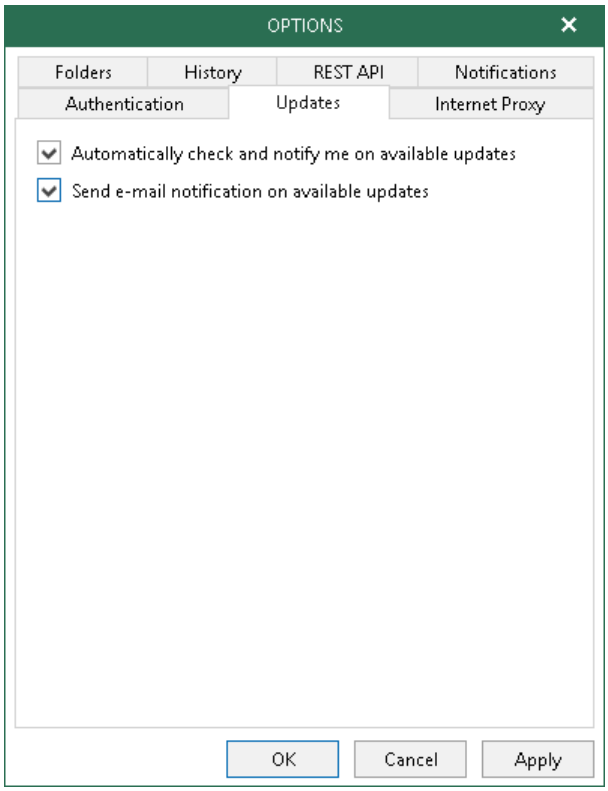
1. Go to the main menu and click **General Options**.
2. Go to the **Updates** tab.
3. Select the following checkboxes:
    - **Automatically check and notify me on available updates**.

      To be notified via a dialog message.
    - **Send e-mail notification on available updates**.

      To be notified via an email message. The recipient address will be taken from the SMTP configuration settings. For more information, see Configuring Notification Settings.

TIP:

To manually check for a new version, see Checking for Updates.



Configuring Global Internet Proxy Server Settings

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

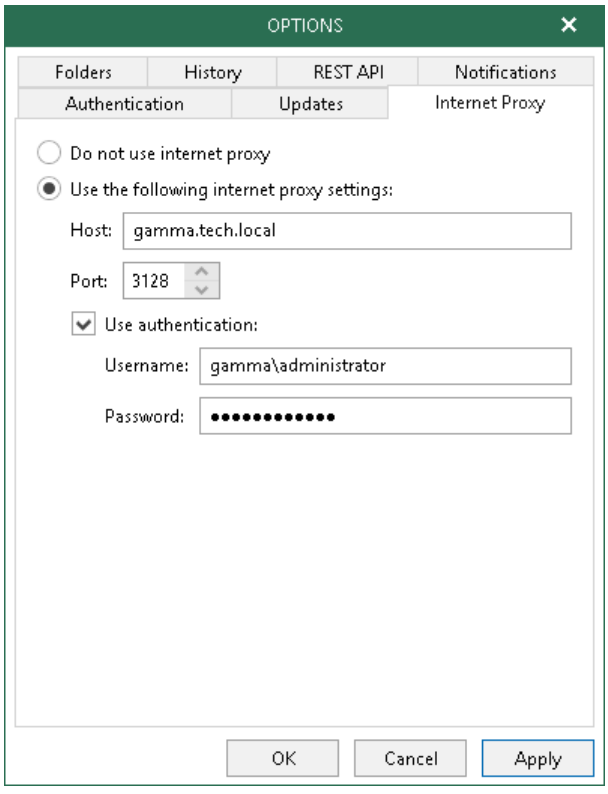
To set up an internet proxy server, do the following:

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

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

TIP:

In addition to configuring an internet proxy server for your 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.



Backup Proxy Servers

A backup proxy server does the following:

- It helps you leverage network traffic when backing up or restoring organizations data.
- It hosts a backup repository where the backed up data is stored.

A backup proxy server participates in the event of the following:

- When backing up data of Microsoft Office 365 and on-premises Microsoft organizations.
- When working with the backup content via Veeam Explorers.

Consider the following:

- A default backup proxy server is the machine running Veeam Backup for Microsoft Office 365, that is, the management server.

  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 deployed on a physical or virtual machine.
- A server with Veeam Backup for Microsoft Office 365 and backup proxy servers must be deployed within the same or a trusted domain.
- Each backup proxy server can process one or several organizations.
- An organization can be processed by one or several backup proxies.
- A backup proxy server is responsible for sending email notifications about backup job completion results.

  To send email notifications, backup proxy servers use the same SMTP server that is configured, as described in Configuring Notification Settings.
- No backup proxy server is involved when:
  - You add a new organization to the program scope, as described in Microsoft Organizations Management.
  - You create a mailbox protection report, as described in Creating Mailbox Protection Reports.

Adding Backup Proxy Servers

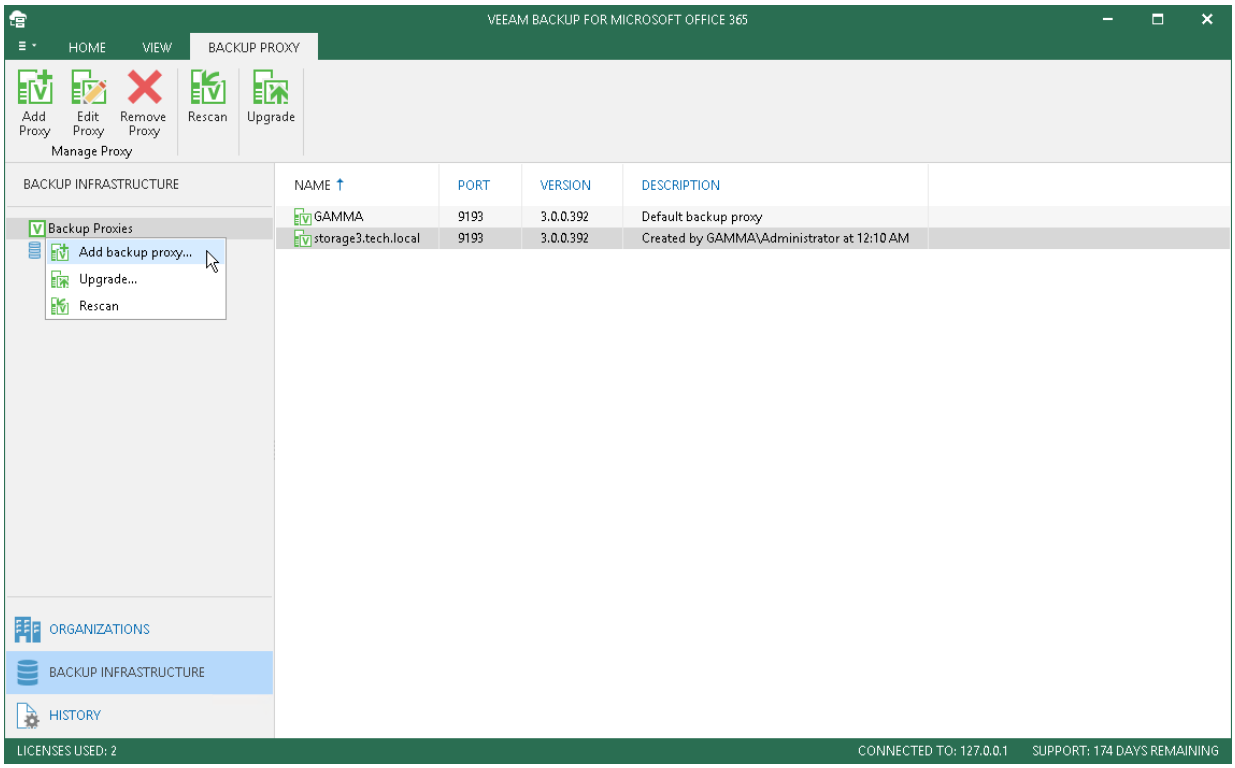
Continue with this section to learn how to add a new backup proxy server to your environment.

Consider the following:

- When a new backup proxy server is being added, Veeam installs the *Veeam.Archiver.Proxy* service (display name in the *services.msc* console — *Veeam Backup Proxy for Microsoft Office 365 Service*) on that machine to manage inbound/outbound traffic.
- Once you have added a new backup proxy server, you can utilize its capacities to store your backup data by creating a new backup repository on such a proxy. For more information, see Adding Backup Repositories.
- If a server that is used as a backup proxy does not have direct access to the internet, you can configure an internet proxy server to be utilized as a gateway. For more information, see Configuring Internet Proxy Server for Backup Proxies.

To add a new backup proxy server, do the following:

1. Go to **Backup Infrastructure > Backup Proxies**.
2. On the **Backup Proxy** tab, click **Add Proxy** or right-click a backup proxy server and select **Add backup proxy**.
3. Proceed to Specify Proxy Server Address.

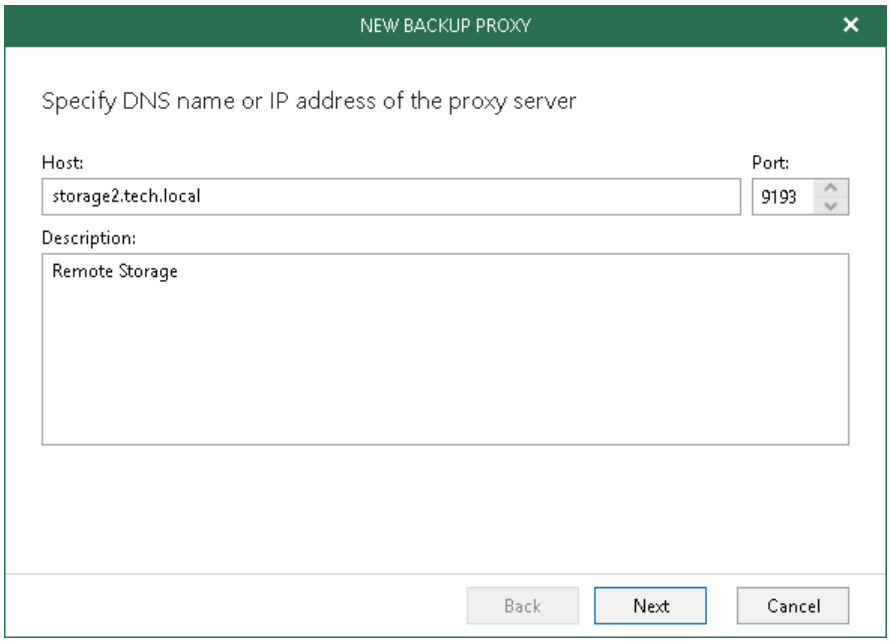


Step 1. Specify Backup Proxy Server Address

At this step of the wizard, specify the following:

- A DNS name or IP address of a server to be used as a proxy.
- The port number of the specified server.

- Optional description.



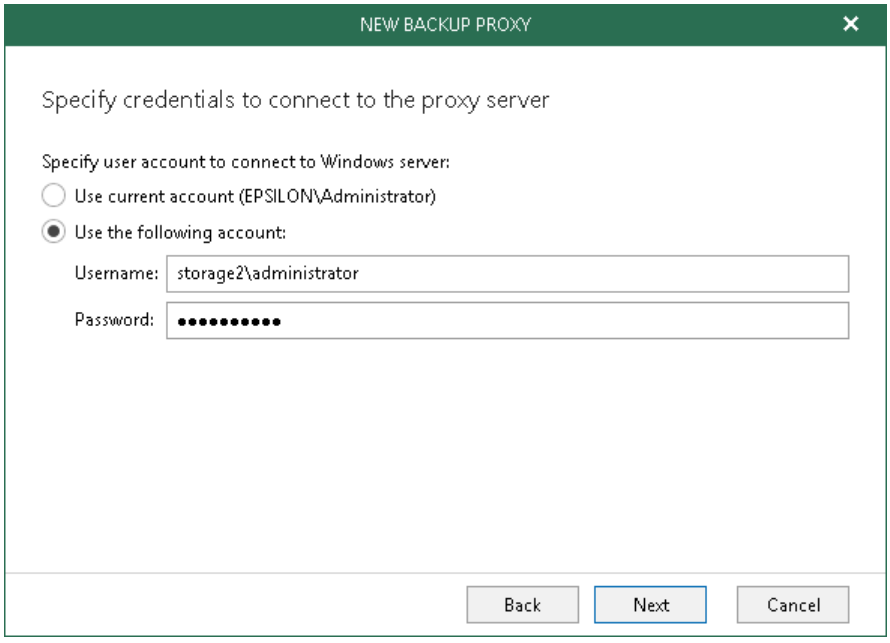
Step 2. Specify Authentication Credentials

At this step of the wizard, specify an account to connect to the server that you want to use as a backup proxy.

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

Click **Next**, wait until Veeam verifies connection and configuration settings and click **Finish**.

Once a new proxy is added, you will be prompted to create a new backup repository. For more information, see Adding Backup Repository.



Editing Backup Proxy Servers

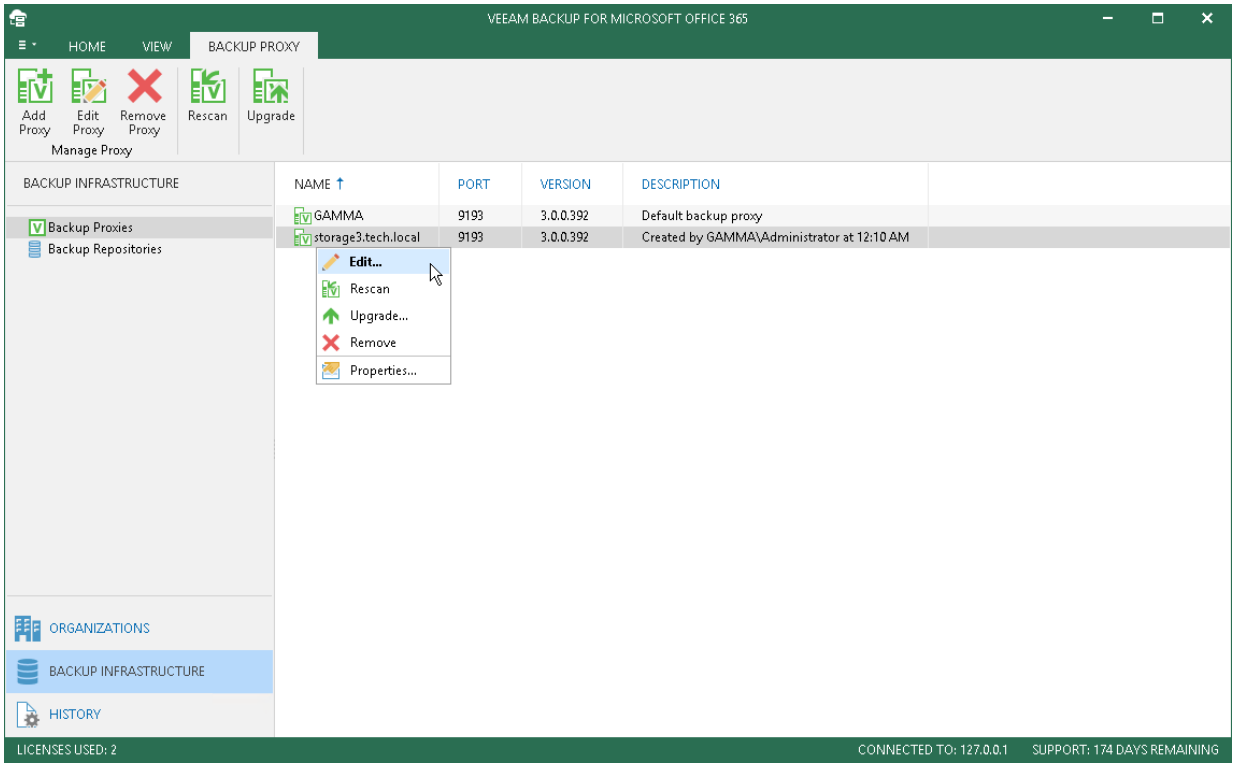
To edit backup proxy server settings, do the following:

1. Go to **Backup Infrastructure > Backup Proxies**.
2. In the preview pane, select a backup proxy server to edit.
3. On the **Backup Proxy** tab, click **Edit Proxy** or right-click a backup proxy server and select **Edit**.

NOTE:

Consider the following:

- Editing the host server is prohibited.
- The **Edit** command is unavailable if a backup proxy server needs to be upgraded, as described in Upgrading Backup Proxy Servers.



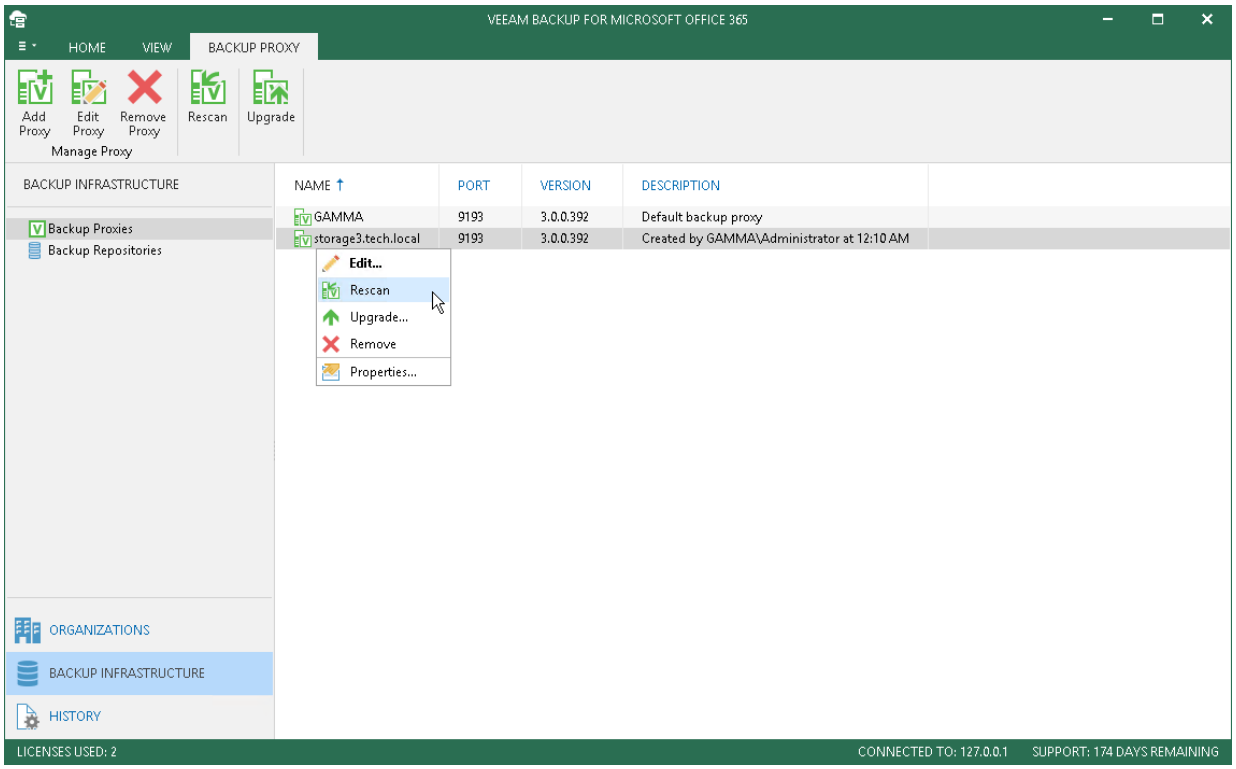
Rescanning Backup Proxy Servers

Backup proxy servers can go offline for a variety of different reasons. If some proxies are offline, you may need to perform manual rescan of such proxies.

To rescan a backup proxy server, do the following:

1. Go to **Backup Infrastructure > Backup Proxies**.
2. In the preview pane, select a backup proxy server to rescan.
3. On the **Backup Proxy** tab, click **Rescan** or right-click a backup proxy server and select **Rescan**.

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



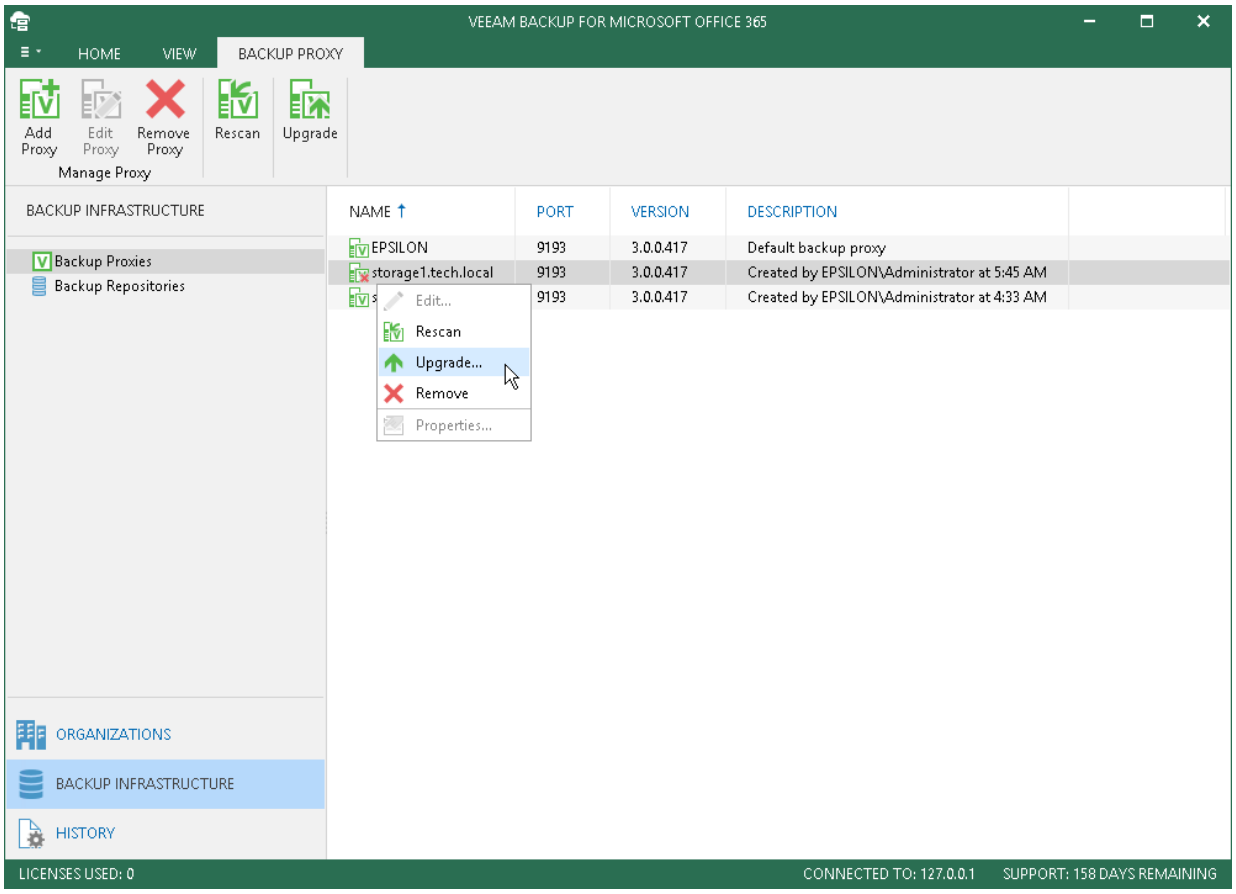
Upgrading Backup Proxy Servers

To communicate with backup proxy servers, Veeam uses the proprietary service — *Veeam.Archiver.Proxy* (display name in the *services.msc* console — *Veeam Backup Proxy for Microsoft Office 365 Service*) that is installed on a proxy machine during the addition of a new backup proxy server. If this component becomes outdated, you will have to upgrade it manually.

To upgrade the component, do the following:

1. Go to **Backup Infrastructure > Backup Proxies**.
2. In the preview pane, select a backup proxy server to upgrade.
3. On the **Backup Proxy** tab, click **Upgrade** or right-click a backup proxy server and select **Upgrade**.

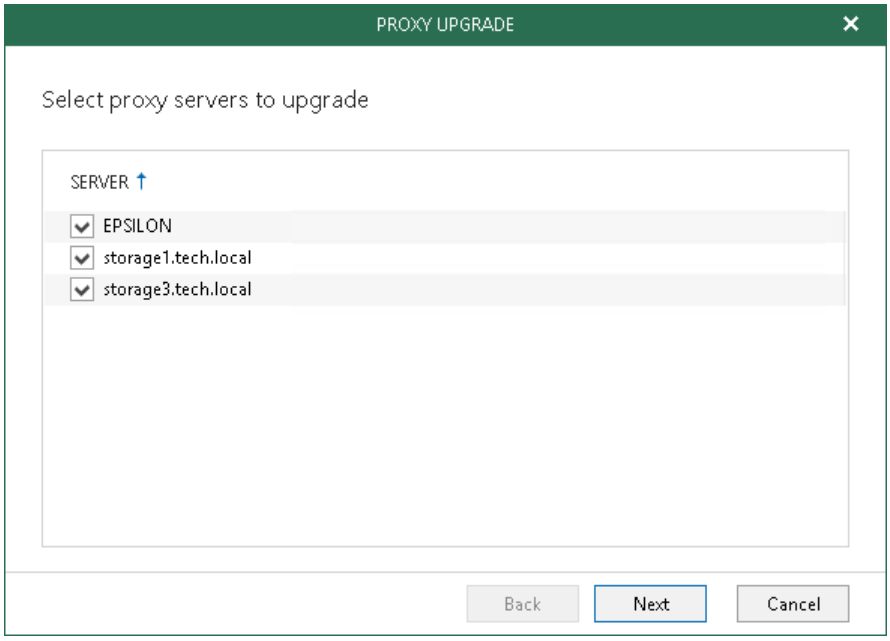
   To upgrade all backup proxy servers simultaneously, select the **Backup Proxies** node and click **Upgrade**.
4. Proceed to Select Backup Proxy Server to Upgrade.



Step 1. Select Backup Proxy Server to Upgrade

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

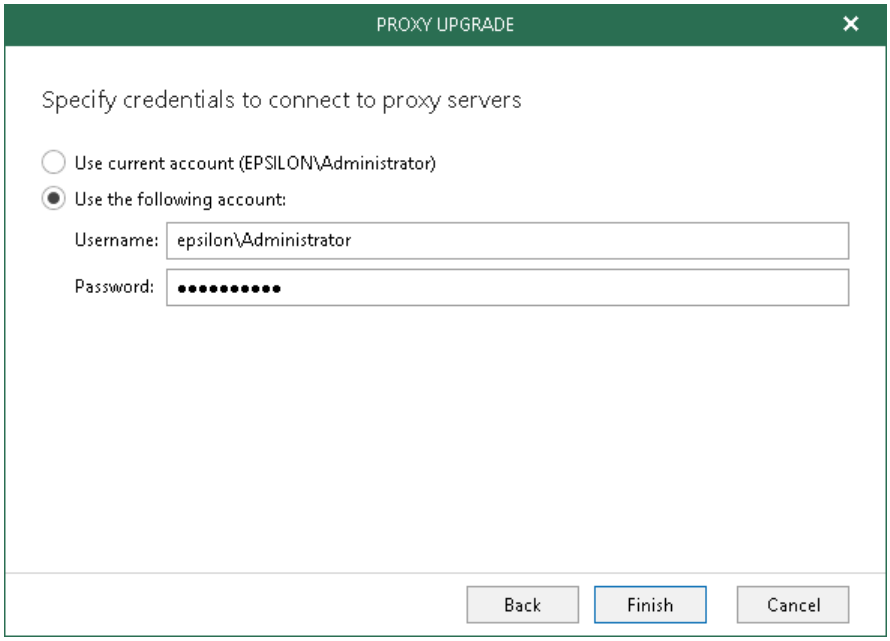
The default backup proxy server will be upgraded automatically.



Step 2. Specify Credentials

At this step of the wizard, specify authentication credentials to access the backup proxy server.

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



Removing Backup Proxy Servers

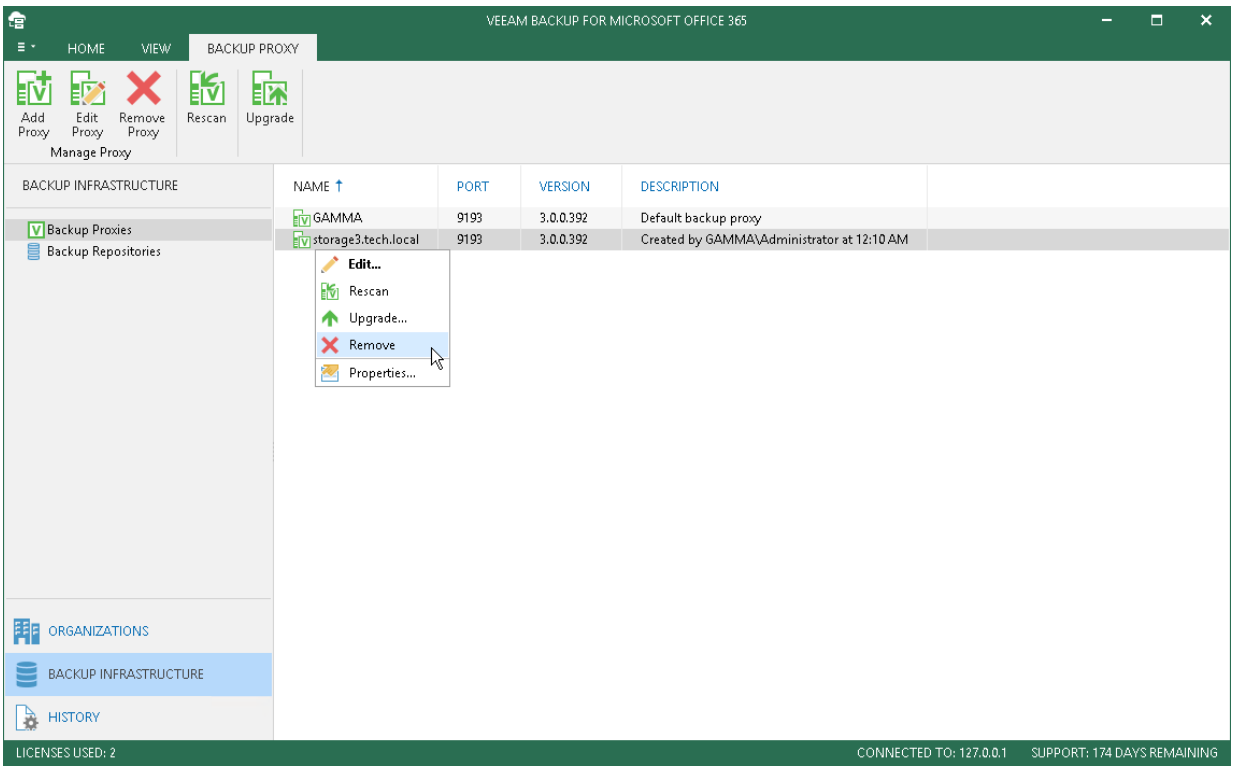
Continue with this section to learn how to remove a backup proxy server from the Veeam Backup for Microsoft Office 365 configuration.

Consider the following:

- The default backup proxy server — a machine on which Veeam Backup for Microsoft Office 365 is deployed — cannot be removed.
- The *Veeam.Archiver.Proxy* component (display name — *Veeam Backup Proxy for Microsoft Office 365 Service*) will be uninstalled from the target server.
- Log files and the actual backup data will be preserved.

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

1. Go to **Backup Infrastructure > Backup Proxies**.
2. In the preview pane, select a backup proxy server to remove.
3. On the **Backup Proxy** tab, click **Remove Proxy** or right-click a backup proxy server and select **Remove**.



Modifying Backup Proxy Server Properties

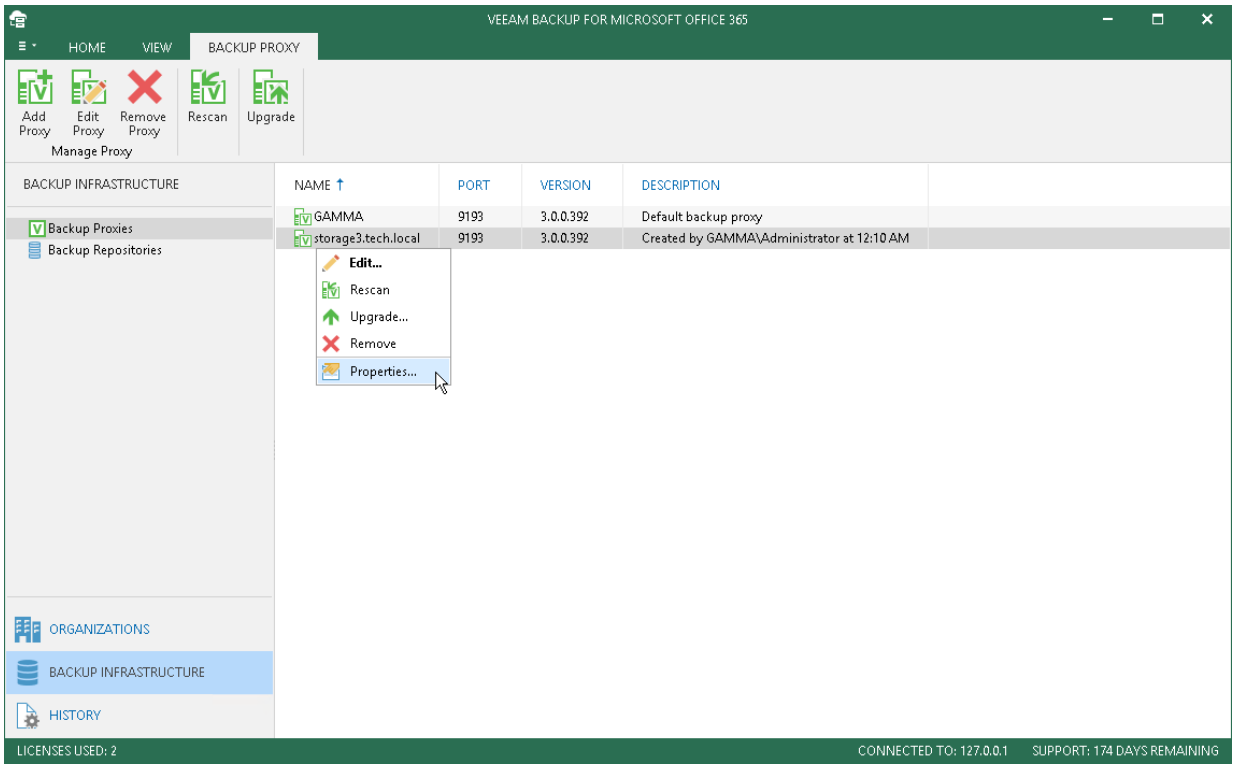
Continue with this section to learn more about configuring backup proxy server properties.

To configure backup proxy server properties, do the following:

1. Go to **Backup Infrastructure**.
2. Select the **Backup Proxies** node.
3. In the preview pane, right-click a backup proxy server, select **Properties** and proceed to:
    - Configuring Threads and Network Bandwidth
    - Configuring Internet Proxy Server for Backup Proxies

NOTE:

The **Properties** command is unavailable if a backup proxy server needs to be upgraded, as described in Upgrading Backup Proxy Servers.



Configuring Threads and Network Bandwidth

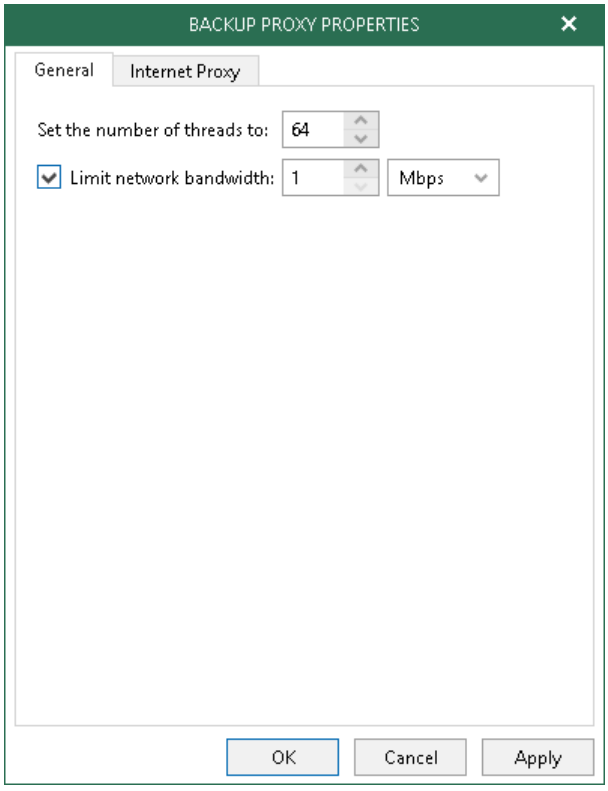
Continue with this section to learn more about configuring threads and the network bandwidth limit.

Consider the following:

- A thread defines the total number of proxy server threads that are responsible for handling the backup data transfer to/from backup repositories. By default, 64 threads are used. Depending on your environment configuration and capacities (e.g. 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 allows you to explicitly define the number of threads that your infrastructure is potentially able to handle without losing performance.
- A network bandwidth limit (i.e. the maximum amount of data that can be transferred across a given path) is applied per backup proxy server, not per thread.

To set up the number of threads along with the network bandwidth limit:

1. On the **General** tab, provide the following:
    - In the **Set the number of threads to** field, specify the number of threads you want to use.
    - Select the **Limit network bandwidth** checkbox and specify the required network bandwidth limit.
2. Click **OK** to save the settings.



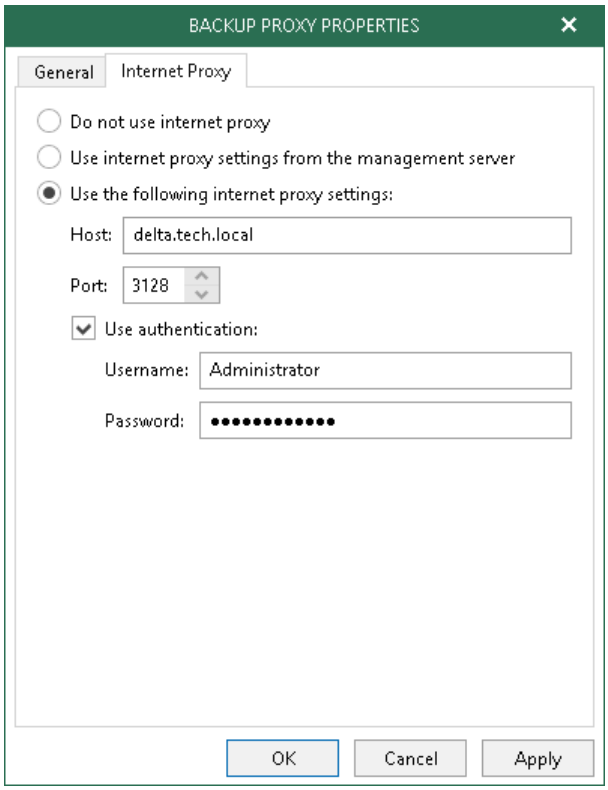
Configuring Internet Proxy Server for Backup Proxies

Continue with this section to learn more about assigning 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:
    a) **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.
    b) **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.
    c) **Use the following internet proxy settings**. Select this option to set up a dedicated internet proxy server and provide the following:
        - DNS name (or IP address) of a server that has access to the internet and which you want to use as an internet proxy.
        - A port number via which to connect to the specified server.
        - Select the **Use authentication** checkbox to authenticate yourself on a server and provide authentication credentials.
3. Click **OK** to save the settings.



Backup Repositories

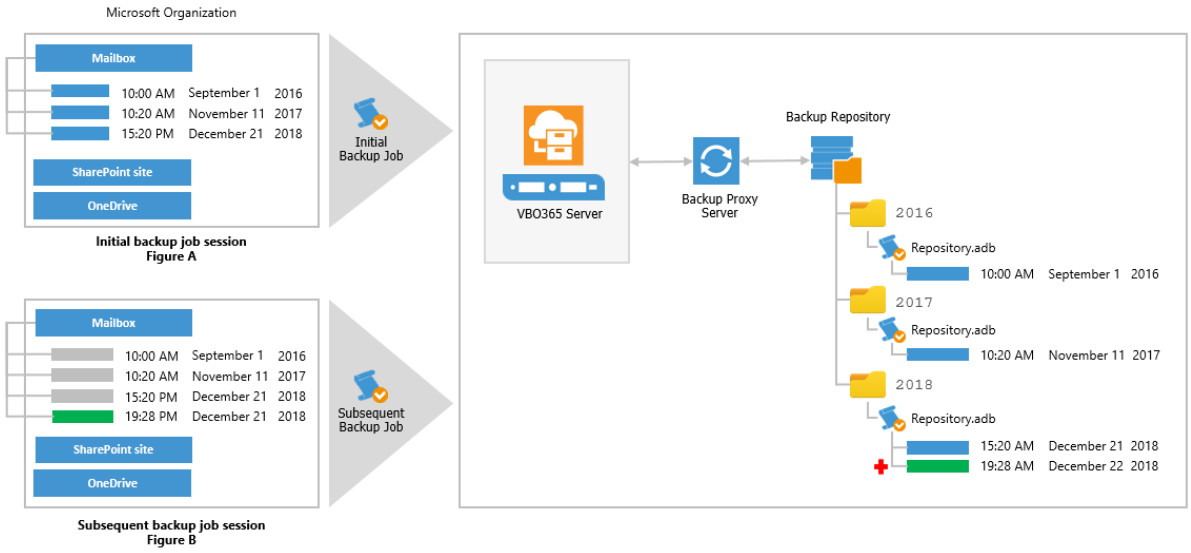
Backup repositories are used to store Microsoft Office 365 and on-premises Microsoft organization backups created by Veeam Backup for Microsoft Office 365.

The structure of a backup repository consists of folders named after the year of items that are being backed up.

Each folder contains a `repository.adb` file, which is the database file that keeps your Office 365 organizations data, and a set of auxiliary files such as checkpoints and repository configuration settings.

All the data is kept according to the retention policy, which is configured when adding a new backup repository. For more information, see Understanding Retention Policy.

The following figure shows how items are added to backup repositories, depending on the backup job session type.



On the left-hand side, you see a Microsoft organization comprising three different object types:

- An Exchange mailbox consisting of three email messages, each of which has its own last modification time.
- A SharePoint site.
- OneDrive.

On the right-hand side is a production environment consisting of a management server, backup proxy server and a backup repository.

The *initial backup job session* collects all the data from the Microsoft organization and places it to a corresponding directory in your backup repository. Sorting is based upon the year of an item being backed up. That said, three items being backed up during the initial backup job session (represented as blue blocks in the *figure A*), will be backed up to the `repository.adb` file which will be placed to folders *2016*, *2017* and *2018*.

Suppose at **19:28 PM** on **December 21, 2018**, a user has received a new email message (represented as a green block in the *figure B*) and the *subsequent backup job session* is scheduled right after the moment, the message has been received. In such a scenario, only that new message is going to be backed up, whereas processing of another three messages (represented as gray blocks in the *figure B*) will be skipped, as these messages have already been backed up earlier and did not change since the last backup session.

The new email message that has been received at **19:28 PM** on **December 21, 2018** will be added to the `repository.adb` file located in the *2018* directory.

Such an approach repeats itself on each subsequent backup job session and is intended to back up only new or modified items.

The same rules apply to Microsoft SharePoint and Microsoft OneDrive for Business organizations as well.

Understanding Retention Policy

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

The following retention types are available:

- Item-Level Retention

  To keep an item until its creation time or last modification time is within the retention coverage.

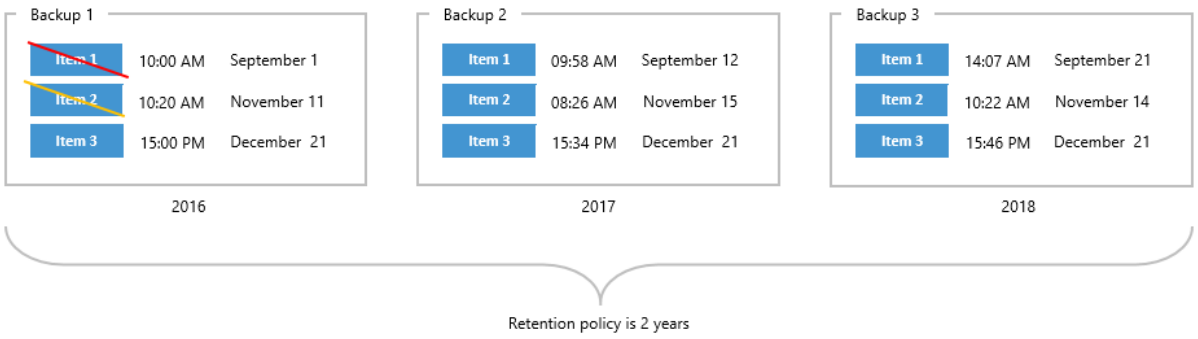
- Snapshot-Based Retention

  To keep an item until its latest restore point is within the retention coverage.

Item-Level Retention Type

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

The following figure demonstrates three simplified backup files, each of which 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 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, as it was last modified exactly at **10:00 AM** on **September 1, 2016**.

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 removes the **Item 2** because its age equals *2 years and 10 minutes* which exceeds the specified threshold.

The aforementioned algorithm repeats itself until no other items left in a repository, whereupon Veeam completely removes such a repository from the hard drive.

> **NOTE:**
>
> Consider that a backup job does not archive items, the last modification time of which exceeds the specified retention period.

Snapshot-Based Retention Type

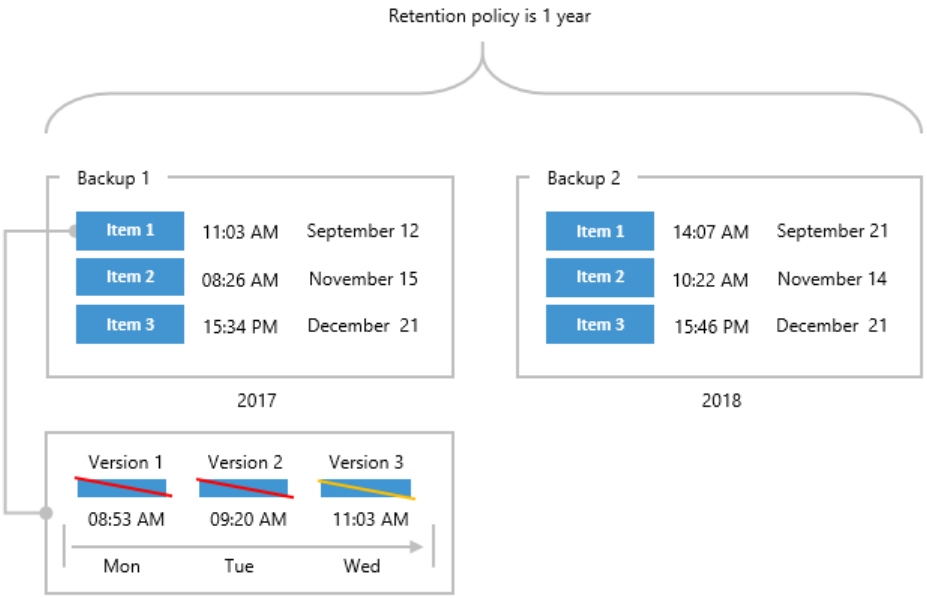
Data removal from backup repositories with the *Snapshot-Based Retention* type occurs every time the latest restore point of an item in a backup file goes beyond the retention coverage.

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

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

For example, the following figure represents two backup files consisting of three items each, where each item has its own backup date. Consider the **Item 1** of the **Backup 1** storage to be an email message, the attributes of which have been modified three times in the production environment; each modification was made on different days (*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.



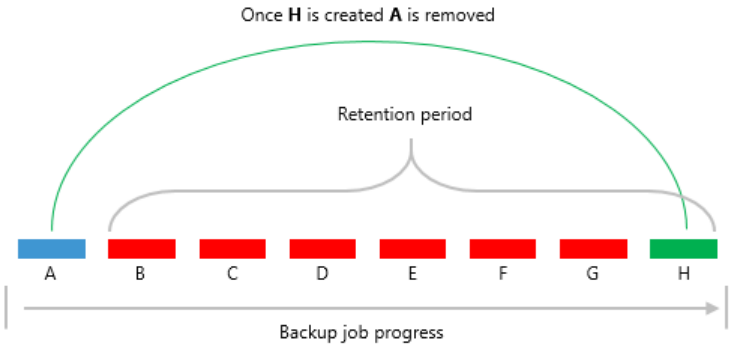
According to the figure above, if the retention policy is **1 year** and said to be applied at **10:00 AM** on **September 12, 2018**, then all the item versions that exceed the specified retention threshold will be removed from the backup repository. As per example, these versions would be the **Version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

Such an approach repeats itself until no other items (or versions of items) left in a repository, whereupon Veeam 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 preserves the latest backup state until the next successful backup of such a mailbox, SharePoint or OneDrive item is created.

The following figure demonstrates an example, wherein there is 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 may 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 figure, wherein there are 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 (*Figure 1*).

Once the latest restore point is out of the retention scope and thus can safely be removed, the item *A* — the parent item of the latest restore point *A2* — will be removed as well (*Figure 2*).

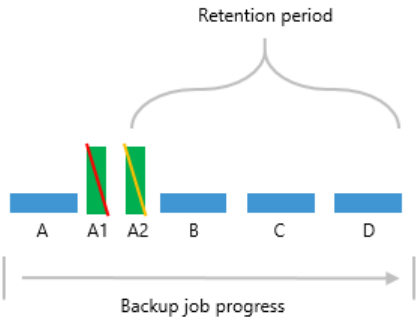


Figure 1

Figure 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 figure shows an example, wherein the mailbox *A* has been removed because it was already out of the retention scope (*Figure 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 (*Figure 2*).

The same is applicable to Microsoft SharePoint and OneDrive for Business.

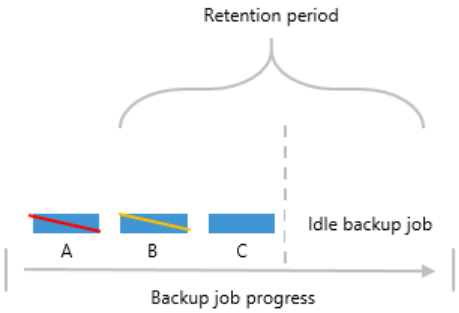


Figure 1

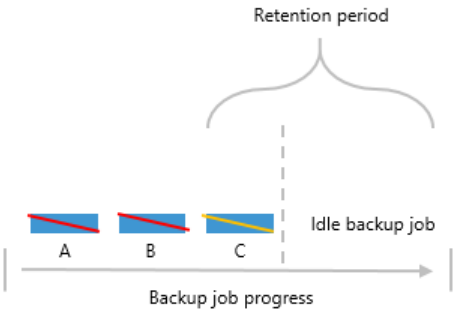


Figure 2

Adding Backup Repositories

Continue with this section to learn how to add a new backup repository.

The following types of backup repositories are supported:

- A local directory on a backup proxy server.

  The 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 server, including external USB/eSATA drives and raw device mapping (RDM) volumes.

- Storage Area Network (SAN).

  A backup server must be connected to the SAN fabric via hardware, virtual HBA or software iSCSI initiator.

- An SMB 3.0 share (experimental support).

- Azure and/or AWS virtual machines.

  For more information about deploying the solution on to either of these platforms, see Deploying on Azure and AWS.

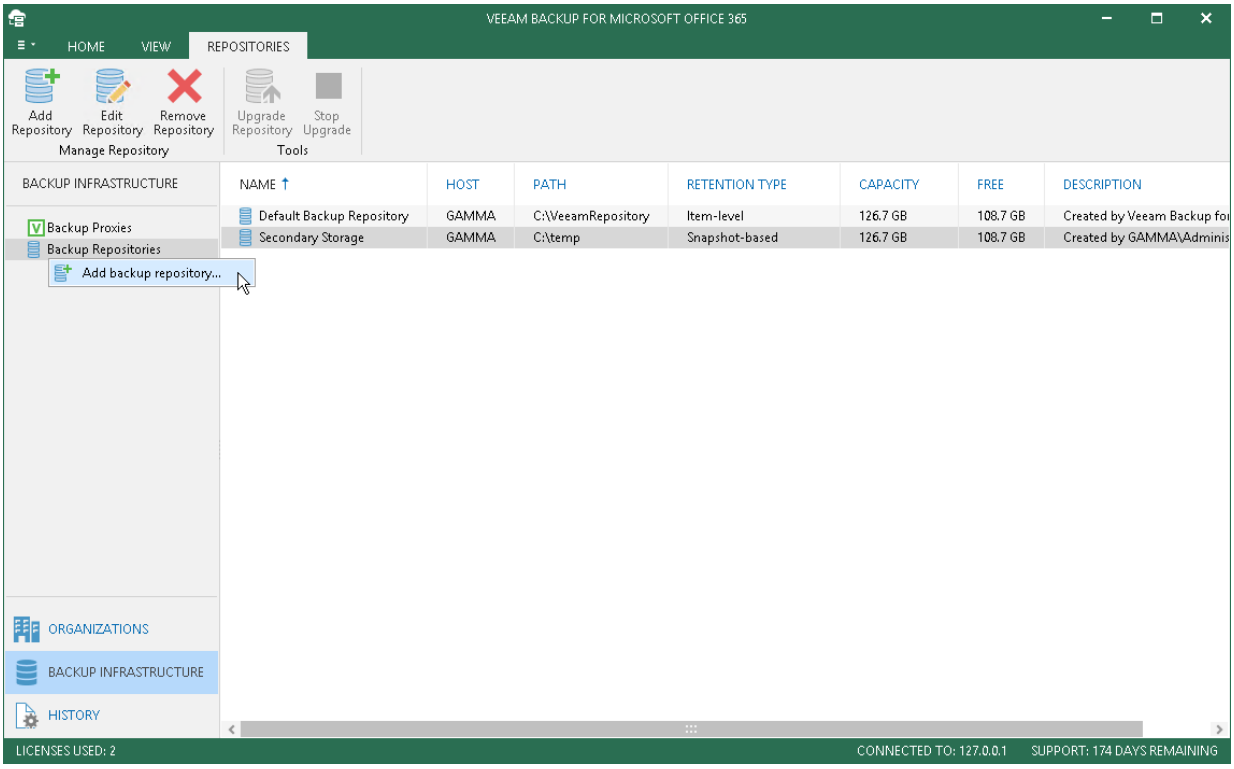
IMPORTANT!

Consider the following:

- To set up a network *drive\UNC* path to the repository on a network share, ensure that the *Local System* account has the *Read* and *Write* privileges to access that share.
- Storage volumes that host the archive repository must be formatted with NTFS or ReFS.
- To use an SMB 3.0 share, make sure you are using Microsoft Windows 8 or Microsoft Windows 2012 or higher.

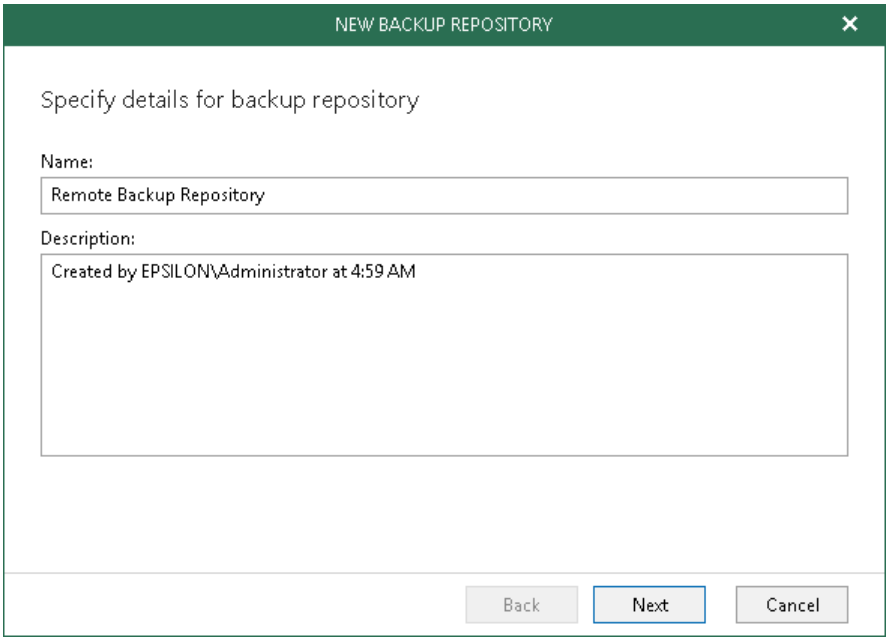
To add a new backup repository, do the following:

1. Go to **Backup Infrastructure > Backup Repositories**.
2. On the **Repositories** tab, click **Add Repository** or right-click a backup repository and select **Add backup repository**.
3. Proceed to Specify Backup Repository Name.



Step 1. Specify Backup Repository Name

At this step of the wizard, specify a new name for the backup repository and provide optional description.



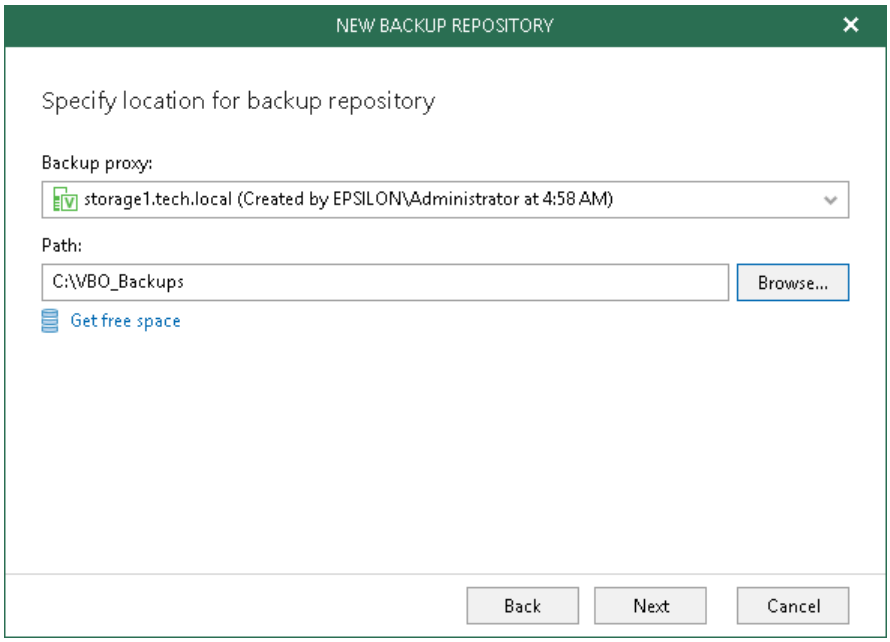
Step 2. Specify Backup Proxy Server

At this step of the wizard, do the following:

- Select a backup proxy server. For more information, see Backup Proxy Servers.
- Specify a directory on the selected proxy server to store your backup data.
- To know the available space, click **Get free space**.

NOTE:

To use a network share folder, provide a path manually. Network share browsing is not supported.



Step 3. Specify Retention Policy

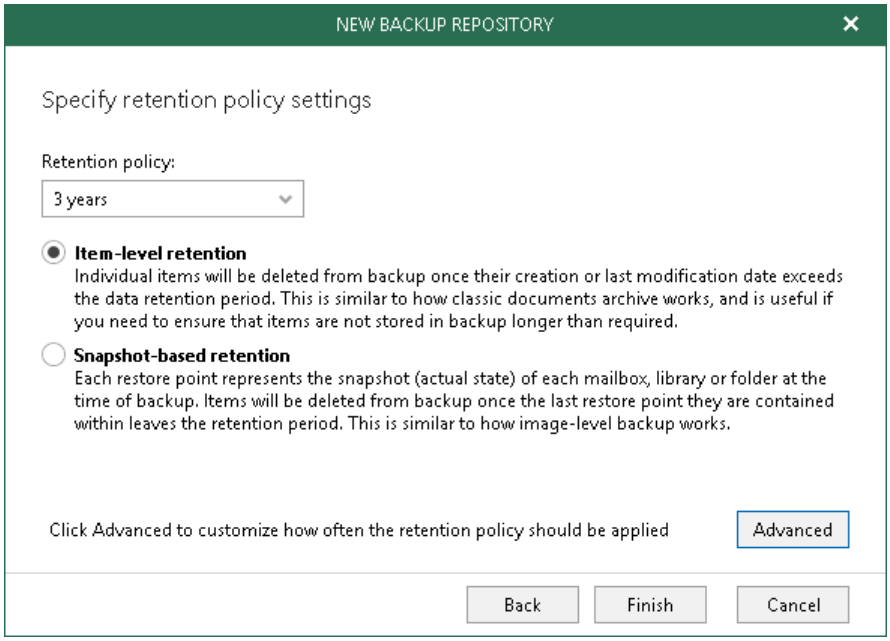
At this step of the wizard, specify retention policy settings.

- In the **Retention policy** drop-down list, specify how long your data should be stored in a backup repository.
- Choose a retention policy type:
  - **Item-level retention**. To keep an item until its creation time or last modification time is within the retention coverage.
  - **Snapshot-based retention**. To keep an item until its latest restore point is within the retention coverage.
- Click **Advanced** to specify when to apply a retention policy. You can select to apply a retention policy on a daily basis, or monthly.

For more information about retention policies, see Understanding Retention Policy.

IMPORTANT!

The retention type of a backup repository cannot be changed in future.



Editing Backup Repository Settings

Continue with this section to learn how to edit backup repository settings.

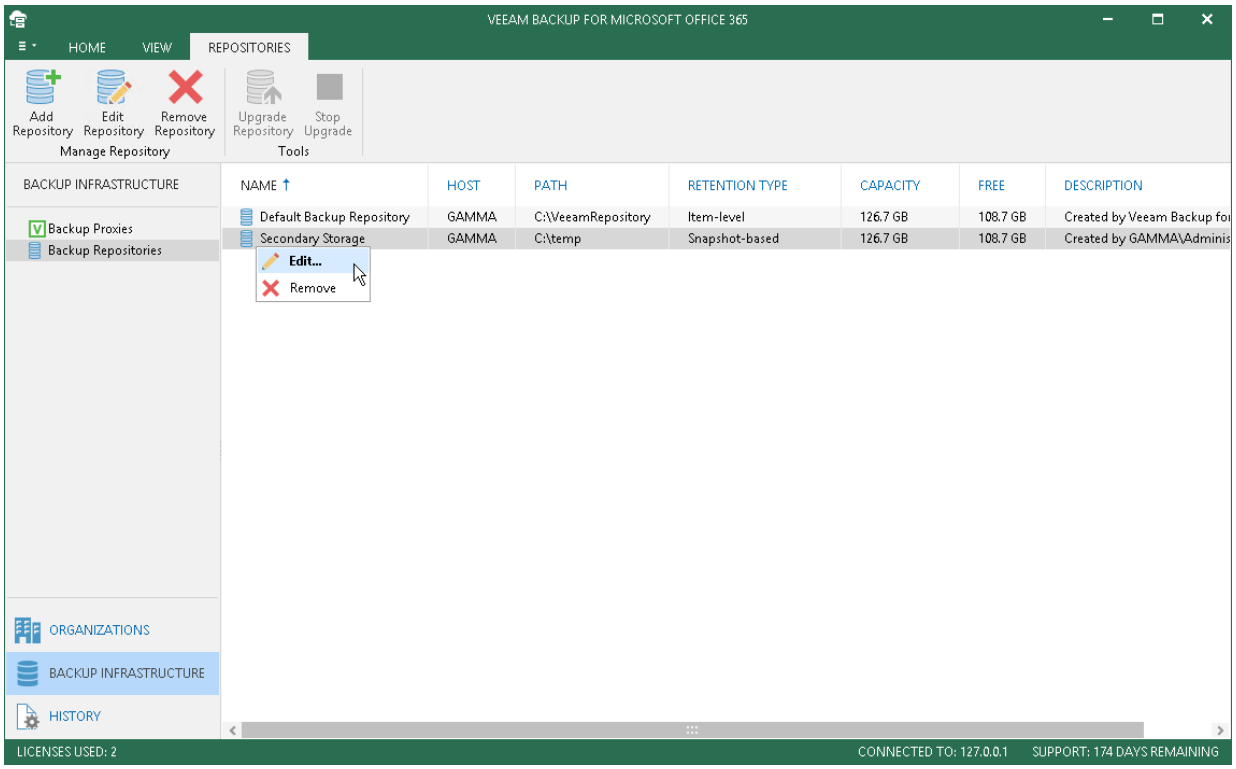
To edit backup repository settings, do the following:

1. Go to **Backup Infrastructure > Backup Repositories**.
2. In the preview pane, select a backup repository to edit.
3. On the **Repositories** tab, click **Edit Repository** or right-click a backup repository and select **Edit**.

NOTE:

Consider the following:

- Changing the existing backup proxy server and the path is prohibited after the repository was initially created.
- The retention type of an existing backup repository cannot be changed.
- The **Edit** command is unavailable if a backup repository is out of date. For more information on how to upgrade a backup repository, see Upgrading Backup Repositories.



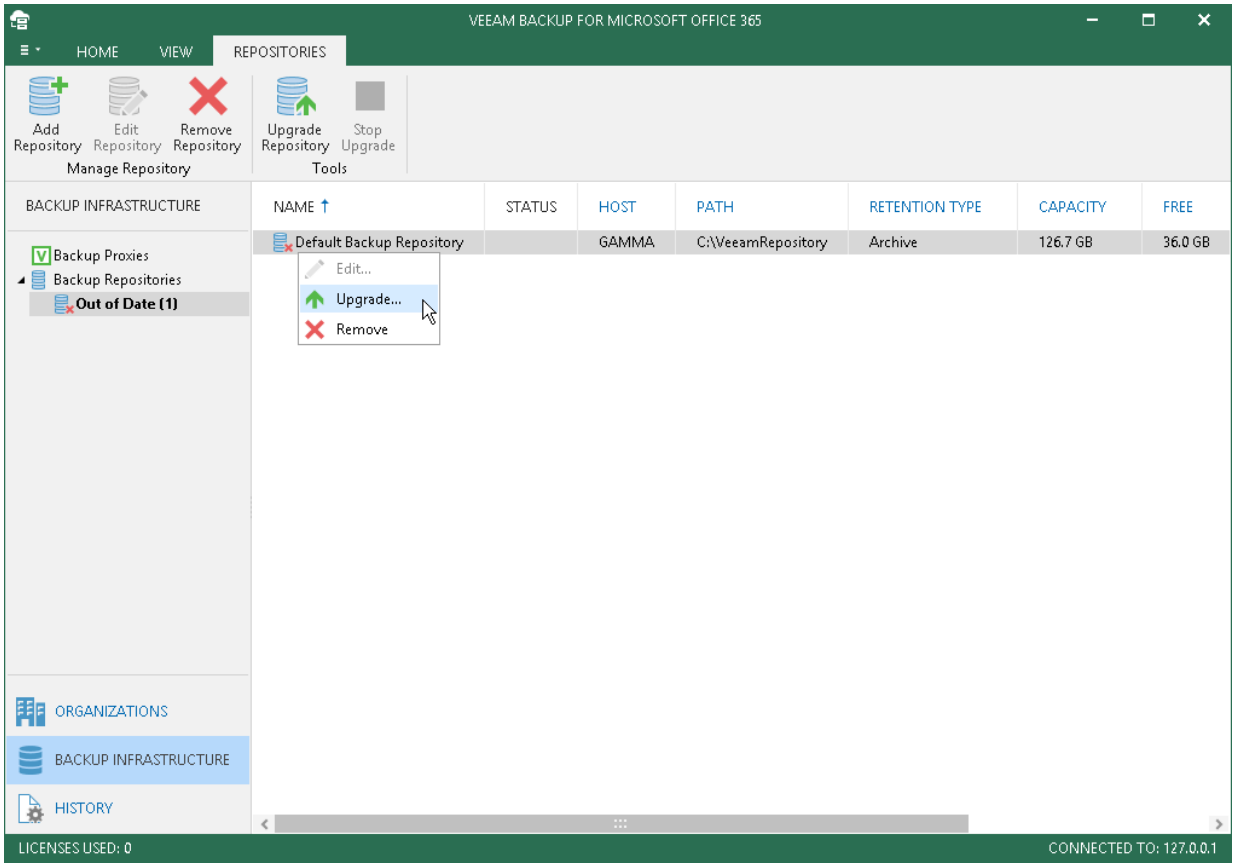
Upgrading Backup Repositories

When you upgrade Veeam Backup for Microsoft Office 365 with a newer version, all the repositories configured in your environment will be marked as out of date and will have to be upgraded manually.

To upgrade backup repositories, do the following:

1. Go to **Backup Infrastructure > Backup Repositories > Out of Date**.
2. In the preview pane, select a backup repository to upgrade.
3. On the **Repositories** tab, click **Upgrade Repository** or right-click a backup repository and select **Upgrade**.

   To cancel an upgrade, click **Stop Upgrade** on the toolbar.



Removing Backup Repositories

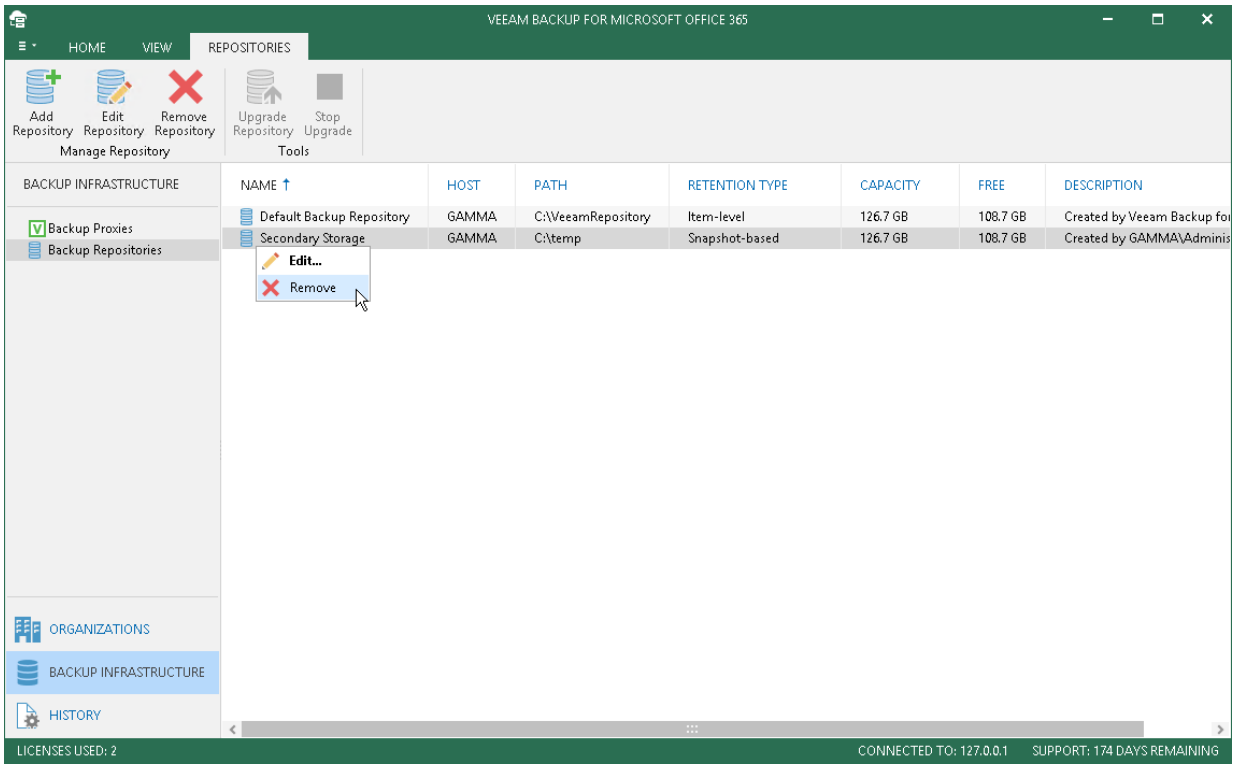
Continue with this section to learn more about removing a backup repository from the application scope.

Consider the following:

- Existing backup files will not be removed.
- Before removing a repository, make sure to re-map all the associated backup jobs to another backup repository. The restore points located in a repository which is being removed will become unavailable.
- The default backup repository — a machine on which Veeam Backup for Microsoft Office 365 is deployed — cannot be removed.

To remove a repository, do the following:

1. Go to **Backup Infrastructure > Backup Repositories**.
2. In the preview pane, select a backup repository to remove.
3. On the **Repositories** tab, click **Remove Repository** or right-click a backup repository and select **Remove**.



Configuration Database

To store general application settings and configuration parameters of various system components, Veeam uses the configuration database located in the *C:|ProgramData|Veeam|Backup365|ConfigDB* directory on a Veeam Backup for Microsoft Office 365 server.

For consistency purposes, some required pieces of management server configuration data are periodically replicated to the proxy server configuration database, which is located in the *C:|ProgramData|Veeam|Backup365|ProxyDb* directory on a proxy machine. Proxy settings are stored in the `Proxy.xml` file located in the same directory.

Microsoft Organizations Management

Continue with this section to learn more about adding, editing, renaming and removing Microsoft Office 365 and on-premises Microsoft organizations.

To connect to 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.

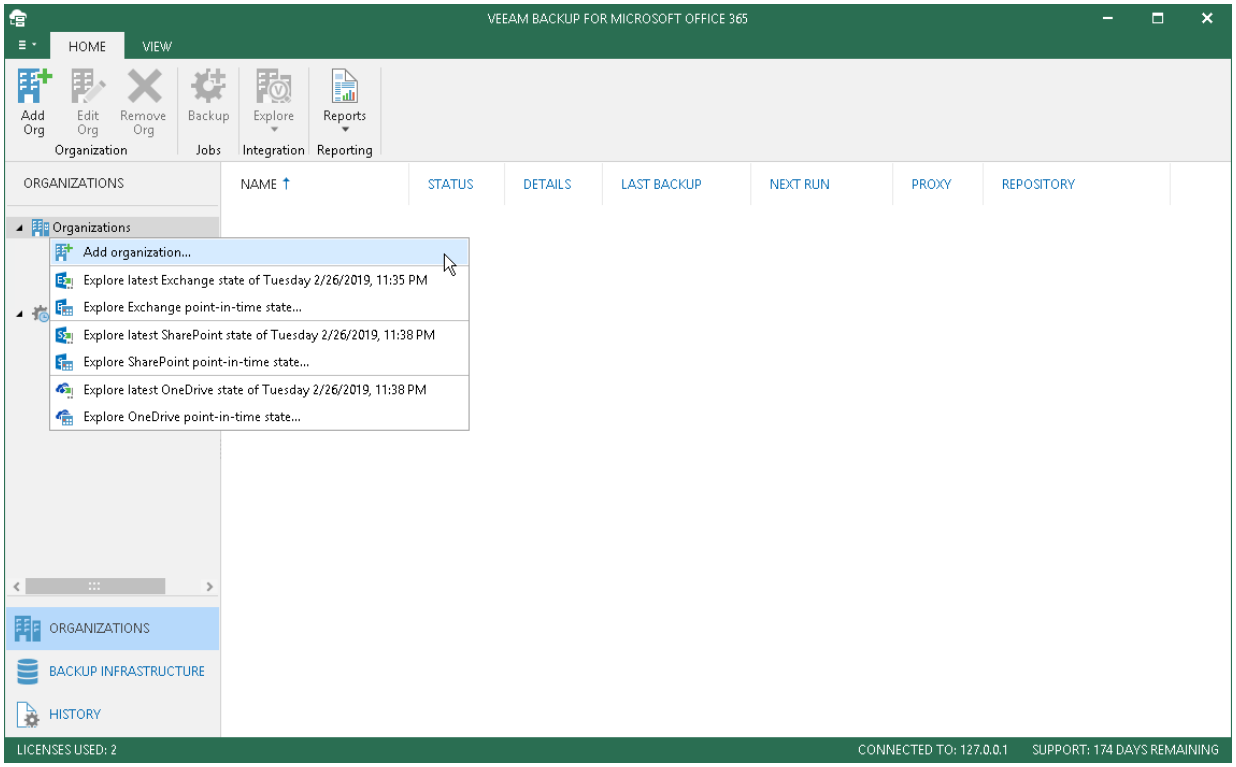
  For more information on how to configure *Windows Remote Management*, see this Microsoft article.
- Microsoft Graph to connect to Microsoft Office 365 organizations.

Adding Microsoft Office 365 Organizations

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

1. In the **Organizations** view, click **Add Org** on the toolbar or right-click the root **Organizations** node and select **Add organization**.
2. Proceed to Select Organization Deployment Type.

> **NOTE:**
>
> Make sure to read the Understanding Microsoft Graph article before adding Microsoft Office 365 organizations.



Understanding Microsoft Graph

To access Azure Active Directory resources and retrieve information about your Microsoft Office 365 organizations, Veeam utilizes Microsoft Graph API. For more information about Microsoft Graph, see this Microsoft article.

Connecting to Microsoft Graph

To connect to Microsoft Graph, Veeam uses three different approaches involving three different application types:

- The default Microsoft application

  To be used when selecting the **Basic authentication** option at the Specify Connection Settings step.

- Custom application created by Veeam

  To be used when selecting the **Basic authentication** option at the Specify Connection Settings step for *China* and *Germany* regions.

- Custom application created by user

  To be used when selecting the **Modern authentication** option at the Specify Connection Settings step for organizations with enabled Multi-factor authentication (MFA).

Using Default Microsoft Application

The default application is installed by default by Microsoft and allows Veeam to connect to Microsoft Office 365 organizations that belong to any Microsoft Azure region except for *China* or *Germany* regions.

Using Veeam Backup for Microsoft Office 365 Application

To connect to Microsoft Office 365 organizations that belong to *China* or *Germany* regions, Veeam uses the proprietary application — *Veeam Backup for Microsoft Office 365*.

This application is installed automatically after you select the **Basic authentication** checkbox at the Specify Connection Settings step of the **Add Organization** wizard and provides Veeam with the appropriate permission set to work with your Microsoft Office 365 organizations data.

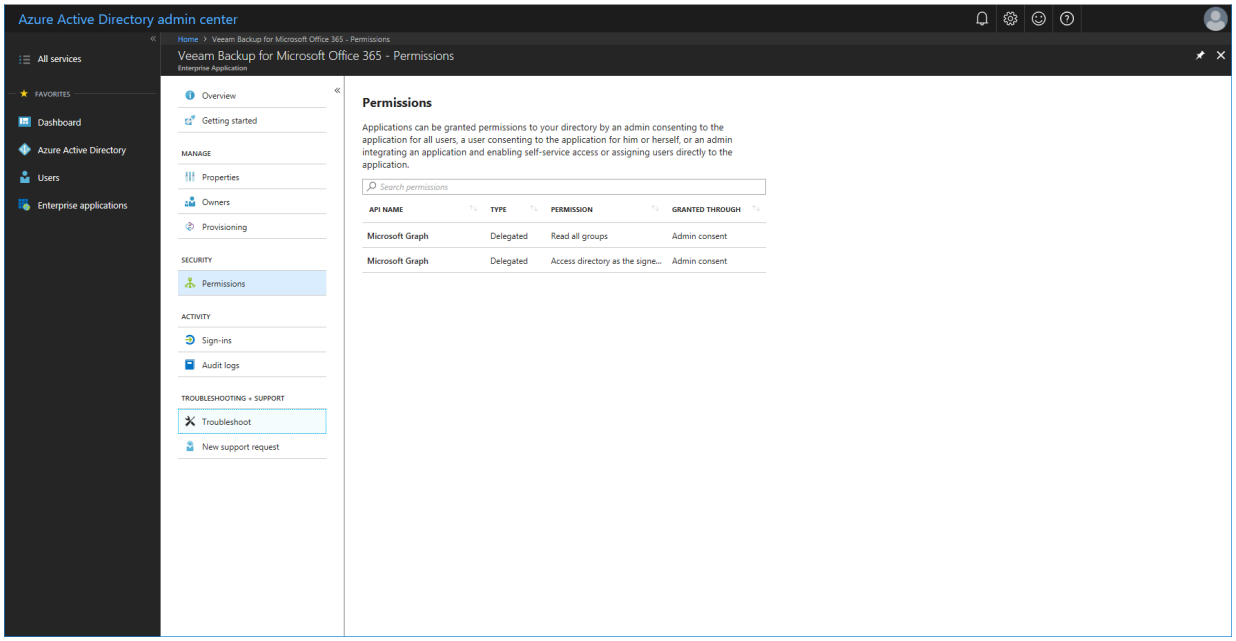
To install the application, Veeam requires either of the following roles to be assigned to your Microsoft Office 365 account:

- *Application administrator*. For more information about this role, see this Microsoft article.
- *Cloud application administrator*. For more information about this role, see this Microsoft article.

To assign any of these roles, open your Azure Active Directory portal, go to **Azure Active Directory** > **Users** > **%User%** > **Directory role** and click **Add role**.

Once installed, the application can be found in the **Enterprise applications** - **All applications** section of your Azure Active Directory admin center.

To see what permissions were given to the application, click the *Veeam Backup for Microsoft Office 365* application name and select **Permissions**.



Using Custom Application

If your Microsoft Office 365 organizations use Multi-factor authentication (MFA), you must create a custom application in your Azure Active Directory portal in advance. Such an application will be utilized by Veeam to access Microsoft Graph API and retrieve your Microsoft Office 365 organizations data.

For more information on how to create a custom application, see this Microsoft article.

The following mandatory API access and permissions must be granted to the application:

- *Microsoft Graph* API access with the following minimum required permissions:
  - *Read all groups*
  - *Read directory data*
- *Microsoft Exchange Online* API access (only required when using a certificate at the Specify Credentials step) with the following minimum required permissions:
  - *Use Exchange Web Services with full access to all mailboxes*
- *Microsoft SharePoint Online* API access (only required when using a certificate at the Specify Credentials step) with the following minimum required permissions:
  - *Have full control of all site collections*

For more information on how to configure API access and assign appropriate permissions, see this Microsoft article.

Microsoft Graph Requests

The following types of requests are used when working with Microsoft Graph:

- Retrieve the properties and relationships of currently authenticated organization. For more information, see this Microsoft article.
- Get groups and directory roles that the user is a direct member of. For more information, see this Microsoft article.
- Retrieve a list of user objects. For more information, see this Microsoft article.
- List all the groups available in an organization. For more information, see this Microsoft article.

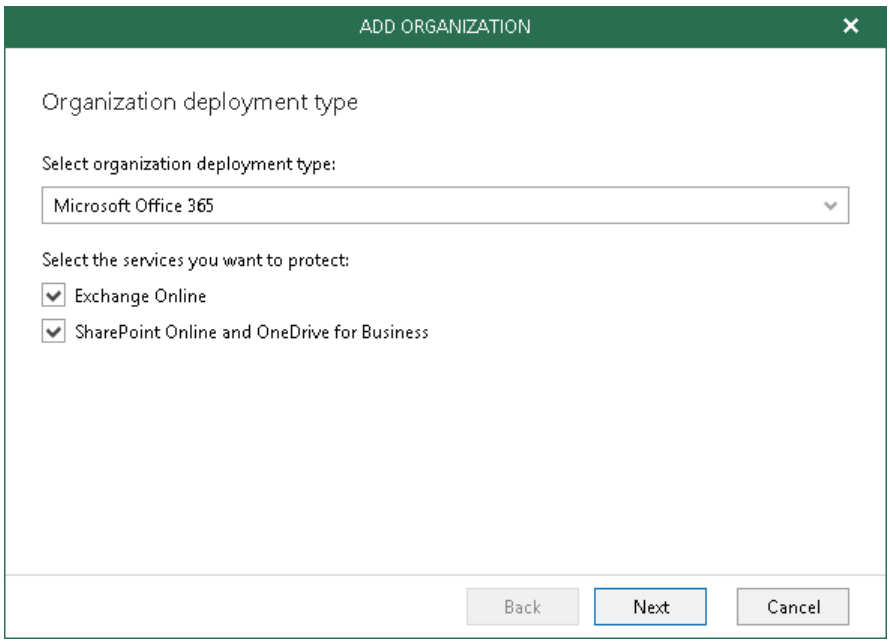
Step 1. Select Organization Deployment Type

At this step of the wizard, do the following:

1. In the **Select organization deployment type** drop-down list, select **Microsoft Office 365**.
2. Select services to back up:
   - **Exchange Online**

     To back up Microsoft Exchange Online.
   - **SharePoint Online and OneDrive for Business**

     To back up Microsoft SharePoint Online and Microsoft OneDrive for Business.



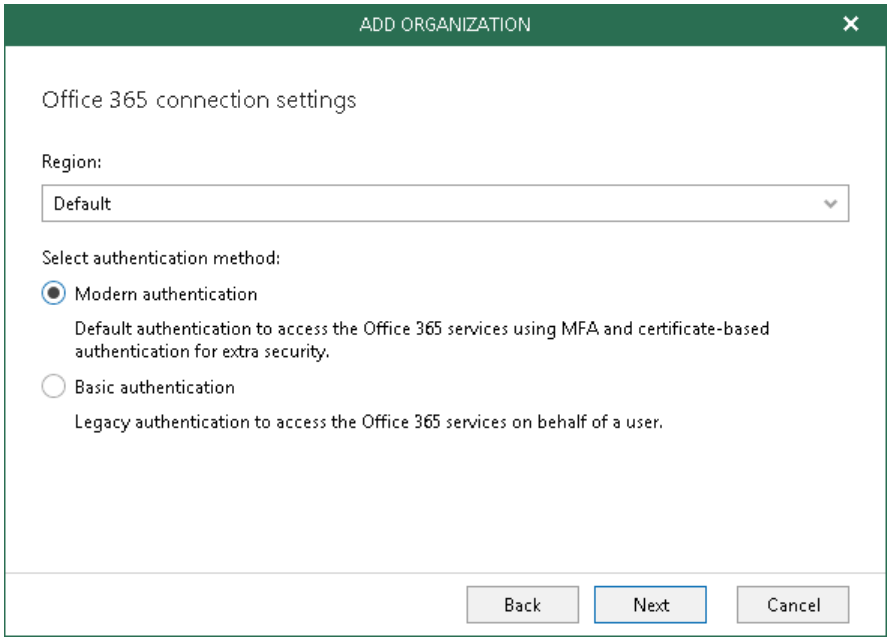
Step 2. Specify Connection Settings

At this step of the wizard, specify the following:

- Microsoft Azure region your organization belongs to.
- Choose an authentication method:
  - **Modern authentication**. Use this option to connect to Microsoft Office 365 organizations with enabled Multi-factor authentication (MFA).

    Make sure to register a custom Azure application upfront, as described in Connecting to Microsoft Graph.
  - **Basic authentication**. Use this option to connect to Microsoft Office 365 organizations with non-enabled Multi-factor authentication.

    To connect to Microsoft Office 365 organizations that belong to *China* or *Germany* regions, Veeam uses a custom application deployed in Azure Active Directory, as described in Connecting to Microsoft Graph.



Step 3. Specify Authentication Credentials

Depending on the authentication type that has been selected at the previous step, either of the following dialogs will appear:

- Basic authentication
- Modern authentication

Basic Authentication

At this step of the wizard, do the following:

- Specify authentication credentials to connect to the Microsoft Office 365 organization.

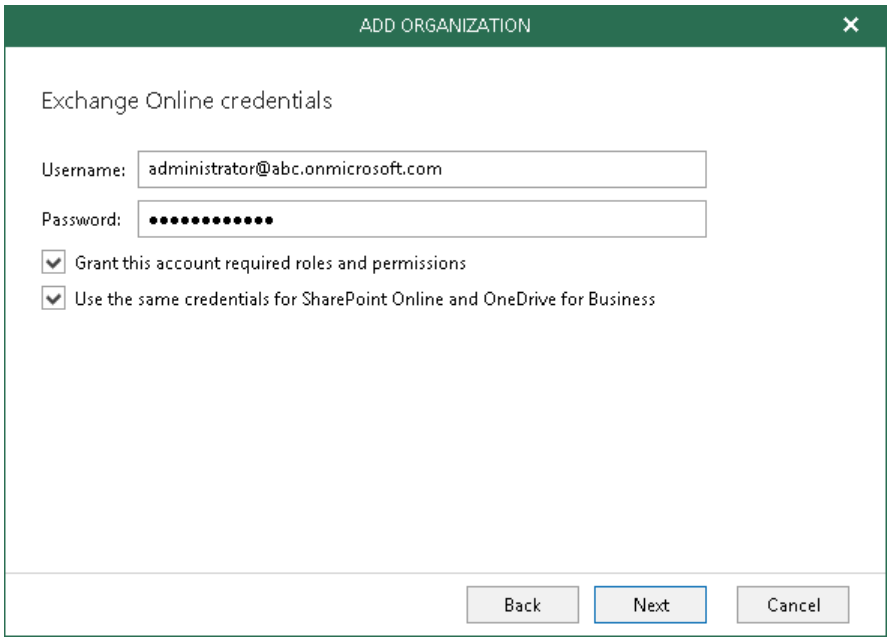
  The user account must be provided in either of the following formats: *user@domain*.com or *user@domain.onmicrosoft.com*.

- Select the **Grant this account required roles and permissions** checkbox to automatically grant required permissions and assign appropriate roles to the account.

- Select the **Use the same credentials for SharePoint Online and OneDrive for Business** checkbox if you want to use the same credentials to access your Microsoft SharePoint Online and OneDrive for Business data. This checkbox is only available if both organization types have been selected at the Select Organization Deployment Type step.

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

Click **Next** and wait for a connection to be established. Once established, the organization being added will appear in the **Organizations** view, under the **Organizations** node.



Modern Authentication

At this step of the wizard, do the following:

- In the **Application ID** field, specify the identification number of the application you have created, as described in Connecting to Microsoft Graph.

  You can find this number in application settings of your Azure Active Directory, as described in this Microsoft article.

- Choose an authentication method.

  You can select either **Application secret** or **Application certificate**:

  a) 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. For more information, see 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.

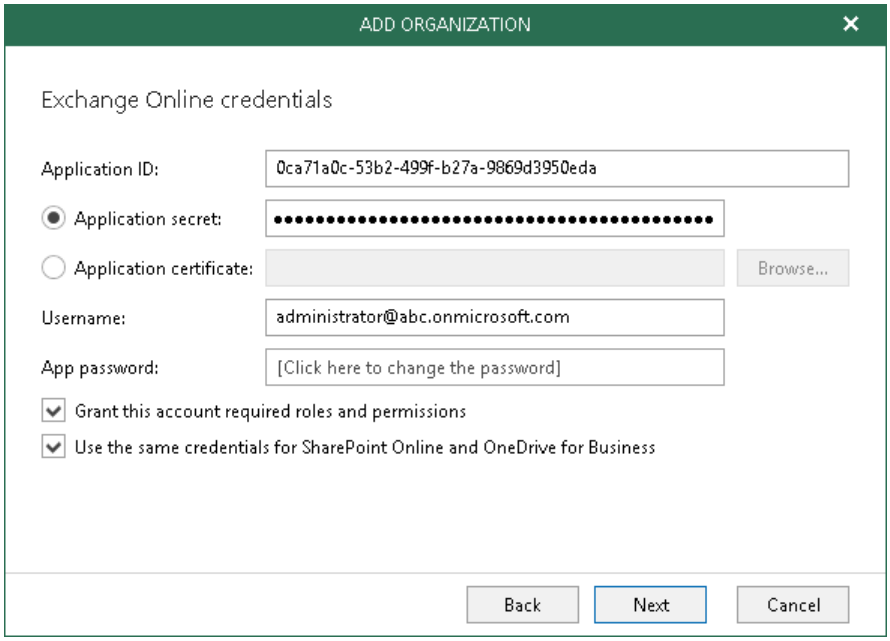
  b) To use a certificate, switch to the **Application certificate** option and click **Browse** to select an existing certificate or import a certificate from a *.pfx* file.

  To be able to use a certificate, you must upload it to the Azure portal first. For more information on how to upload a certificate, see this Microsoft article.

- In the **Username** field, specify your Microsoft Office 365 account name.
- In the **App password** field, specify the app password that was generated upon enabling Multi-factor authentication (MFA), as described in this Microsoft article.
- Select the **Grant this account required roles and permissions** checkbox to automatically grant required permissions and assign appropriate roles to the account.
- Select the **Use the same credentials for SharePoint Online and OneDrive for Business** checkbox if you want to use the same credentials to access your Microsoft SharePoint Online and OneDrive for Business data. This checkbox is only available if both organization types have been selected at the Select Organization Deployment Type step.

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

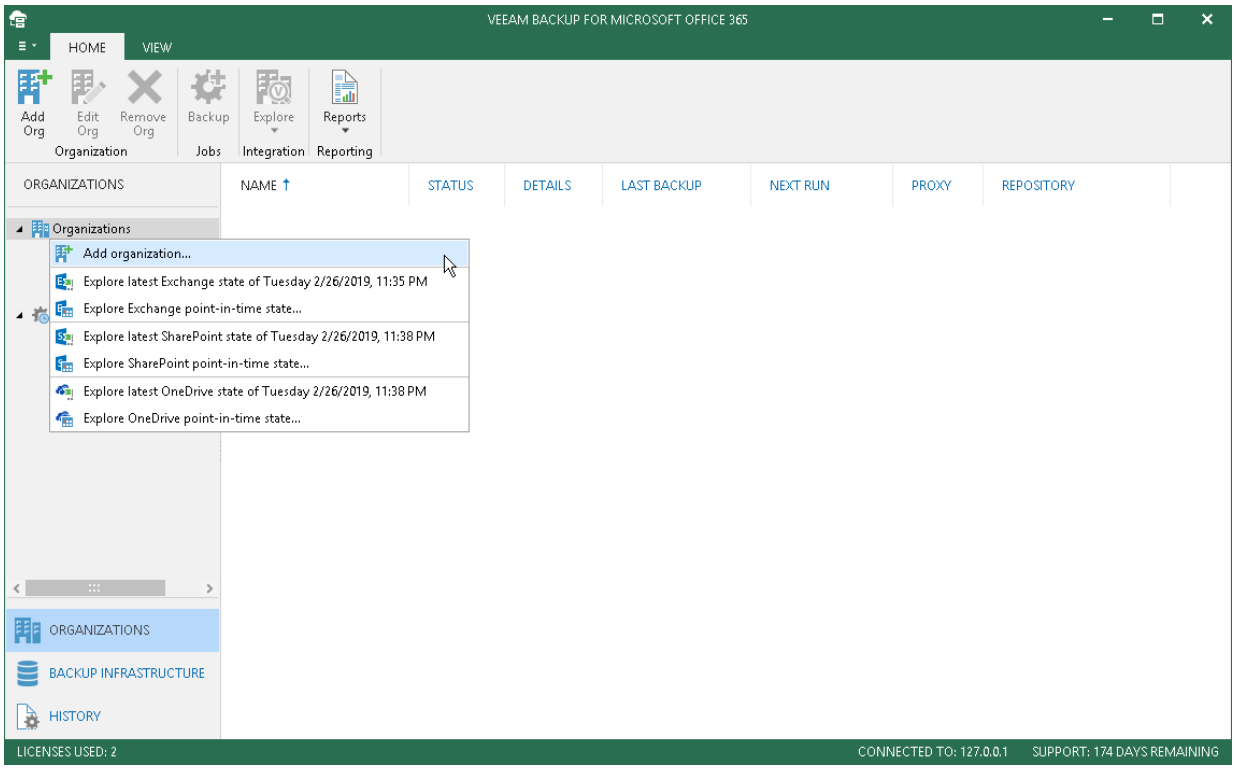
Click **Next** and wait for a connection to be established. Once established, the organization being added will appear in the **Organizations** view, under the **Organizations** node.


ADD ORGANIZATION
Exchange Online credentials
Application ID:
0ca71a0c-53b2-499f-b27a-9869d3950eda
Application secret:
Application certificate:
Browse...
Username:
administrator@abc.onmicrosoft.com
App password:
[Click here to change the password]
Grant this account required roles and permissions
Use the same credentials for SharePoint Online and OneDrive for Business
Back
Next
Cancel

Adding On-Premises Microsoft Organizations

To add a new on-premises Microsoft Exchange or on-premises Microsoft SharePoint organization to the program scope, do the following:

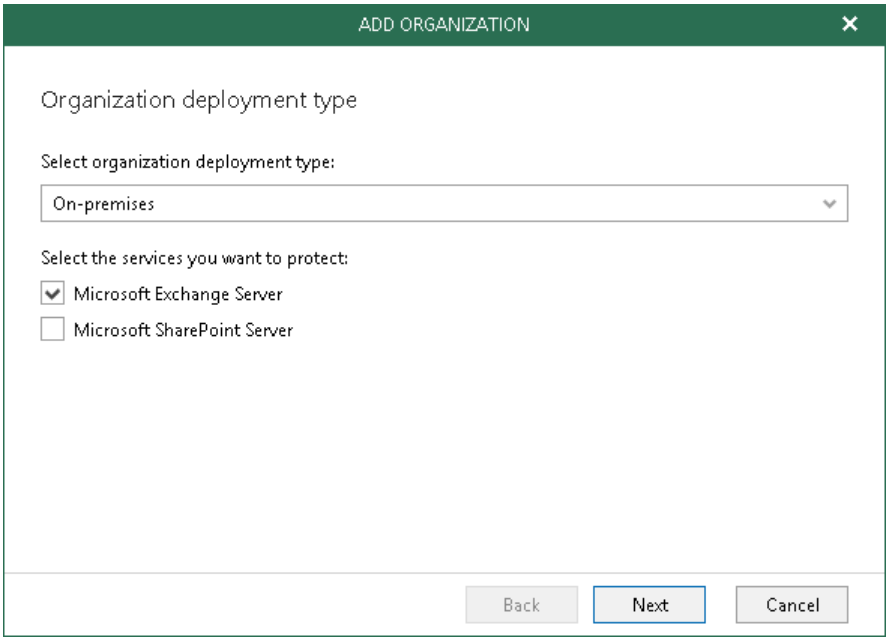
1. In the **Organizations** view, click **Add Org** on the toolbar or right-click the root **Organizations** node and select **Add organization**.
2. Depending on the organization type, proceed to:
    - Adding On-Premises Microsoft Exchange Organization
    - Adding On-Premises Microsoft SharePoint Organization
    - Adding On-Premises Organizations of Both Types



Adding On-Premises Microsoft Exchange Organization

To add a new on-premises Microsoft Exchange organization, do the following:

1. In the **Select organization deployment type** drop-down list, select **On-premises**.
2. Select the **Microsoft Exchange Server** checkbox.



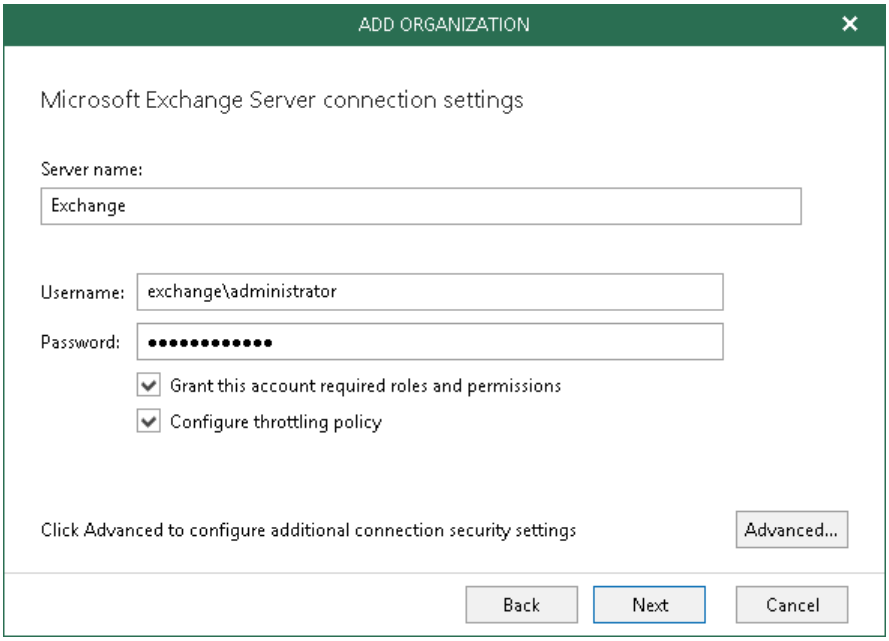
3. Specify a Microsoft Exchange server name.
4. Specify authentication credentials to connect to the Microsoft Exchange server using either of the following formats: *domain|account* or *account@domain*.

   For more information, see Required Permissions.
5. Select the **Grant this account required roles and permissions** checkbox to automatically assign the following roles (if none of these have been assigned earlier):
   - *View-Only Configuration*
   - *View-Only Recipient*
   - *ApplicationImpersonation*

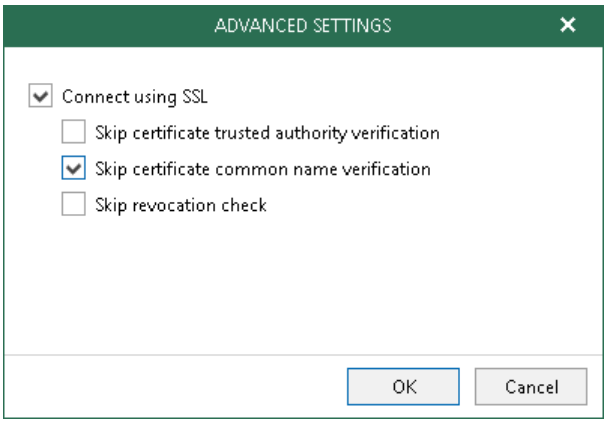
IMPORTANT!

To be able to assign these roles (or verify whether any of these are already assigned), make sure the account you are using has been granted both the *Organization Management* and *Role Management* roles upfront. Otherwise, the addition of an organization will fail.

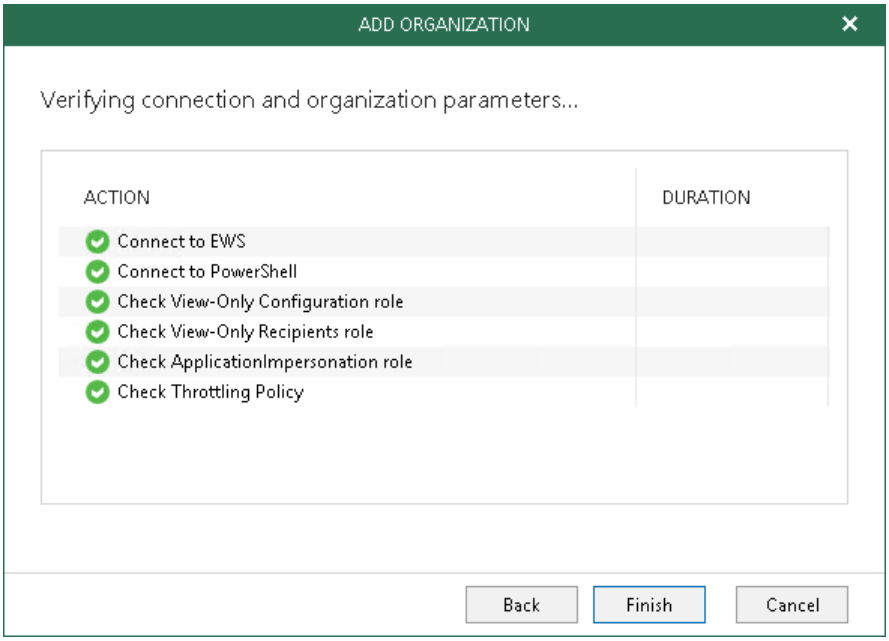
6. Select the **Configure throttling policy** checkbox to set the throttling policy for the account being used to *Unlimited*.



7. By default, Veeam establishes an SSL connection. To change this or skip one or more SSL verifications, click **Advanced** and select verifications to skip:
   - **Skip certificate trusted authority verification**
   - **Skip certificate common name verification**
   - **Skip revocation check**



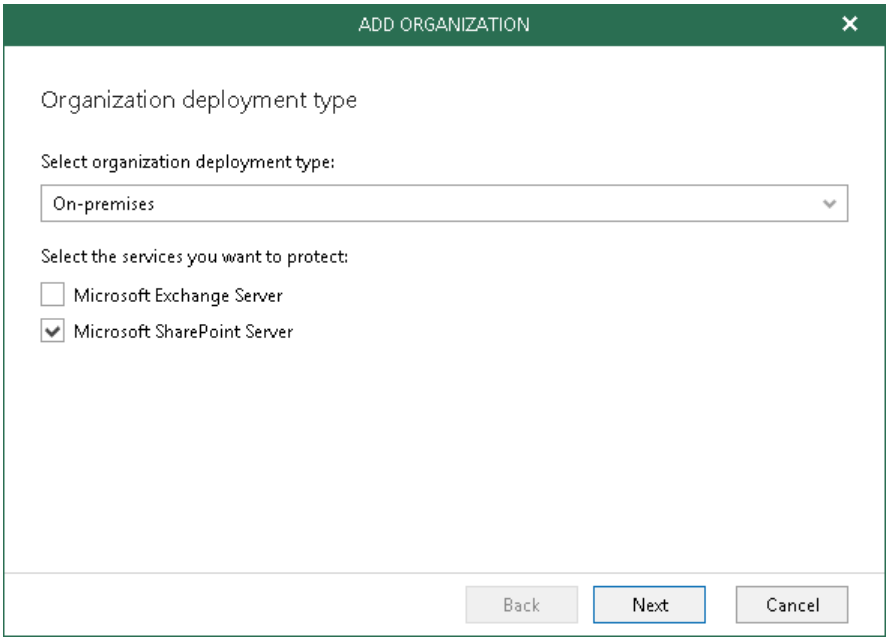
8. Wait for a connection to be established and click **Finish**.


ADD ORGANIZATION
Verifying connection and organization parameters...
ACTION
DURATION
Connect to EWS
Connect to PowerShell
Check View-Only Configuration role
Check View-Only Recipients role
Check ApplicationImpersonation role
Check Throttling Policy
Back
Finish
Cancel

Adding On-Premises Microsoft SharePoint Organization

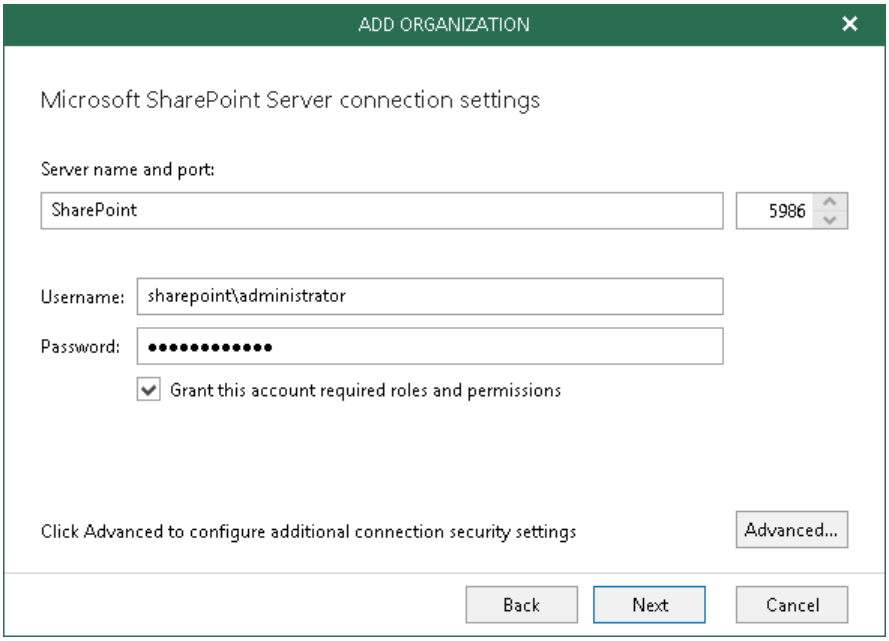
To add a new on-premises Microsoft SharePoint organization, do the following:

1. In the **Select organization deployment type** drop-down list, select **On-premises**.
2. Select the **Microsoft SharePoint Server** checkbox.

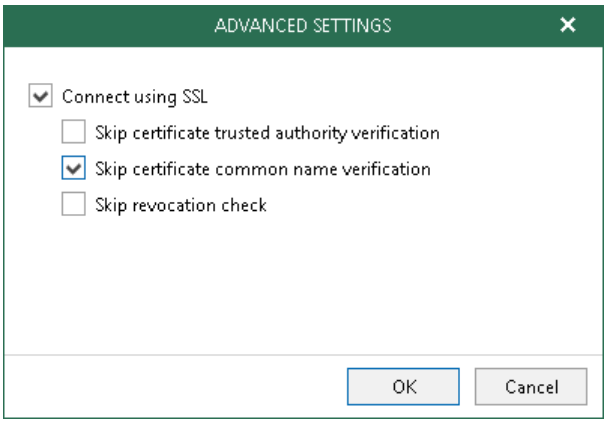


3. Specify a Microsoft SharePoint server name and the WinRM port.
4. Specify authentication credentials to connect to the Microsoft SharePoint server using either of the following formats: *domain|account* or *account@domain*.

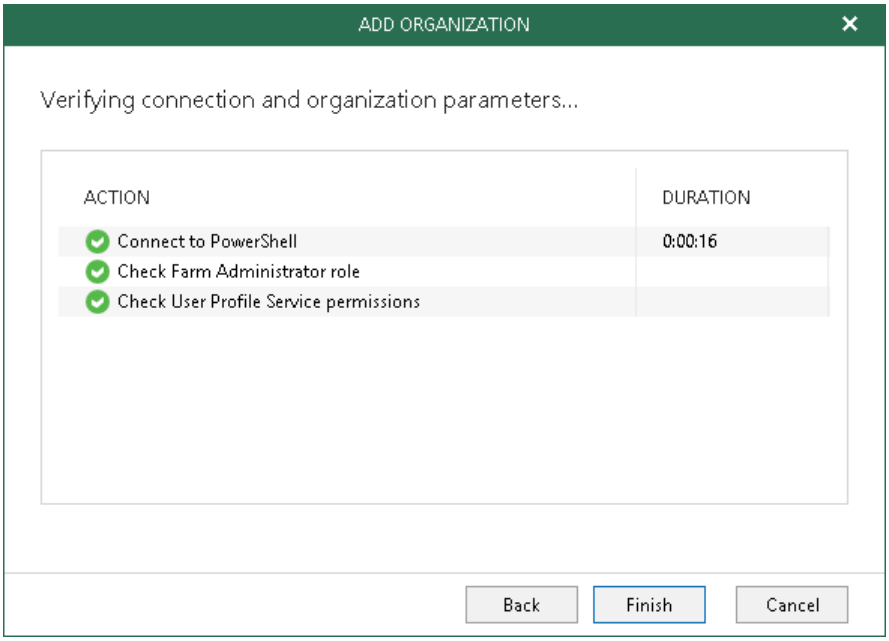
   For more information, see Required Permissions.
5. Select the **Grant this account required roles and permissions** checkbox to automatically add a user to the SharePoint *Site Collection Administrators* group and grant this user administrative privileges to access Microsoft SharePoint sites. This option also grants access to the *User Profile* service to work with OneDrive data.



6. By default, Veeam establishes an SSL connection. To change this or skip one or more SSL verifications, click **Advanced** and select verifications to skip:
   - **Skip certificate trusted authority verification**
   - **Skip certificate common name verification**
   - **Skip revocation check**



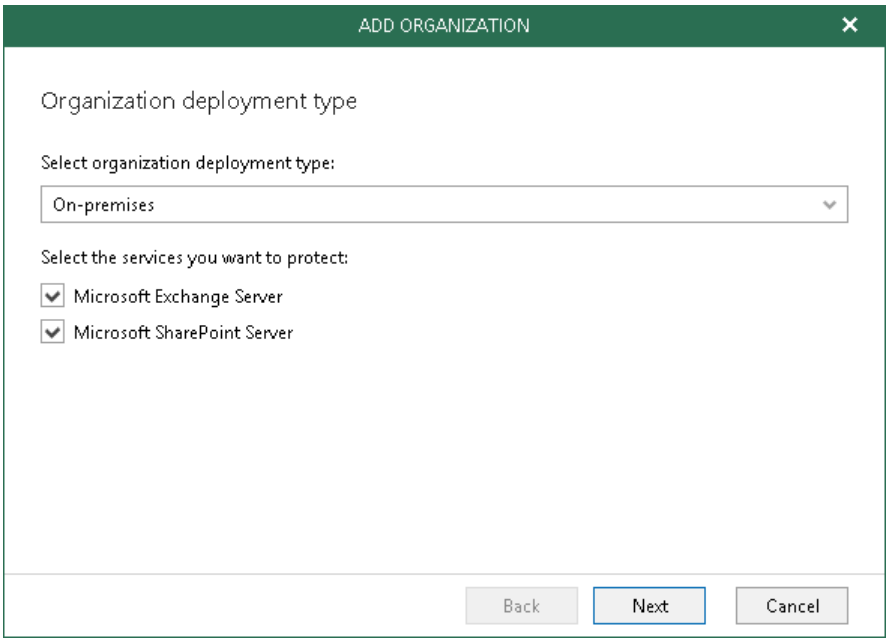
7. Wait for a connection to be established and click **Finish**.


ADD ORGANIZATION
Verifying connection and organization parameters...
ACTION
DURATION
Connect to PowerShell
0:00:16
Check Farm Administrator role
Check User Profile Service permissions
Back
Finish
Cancel

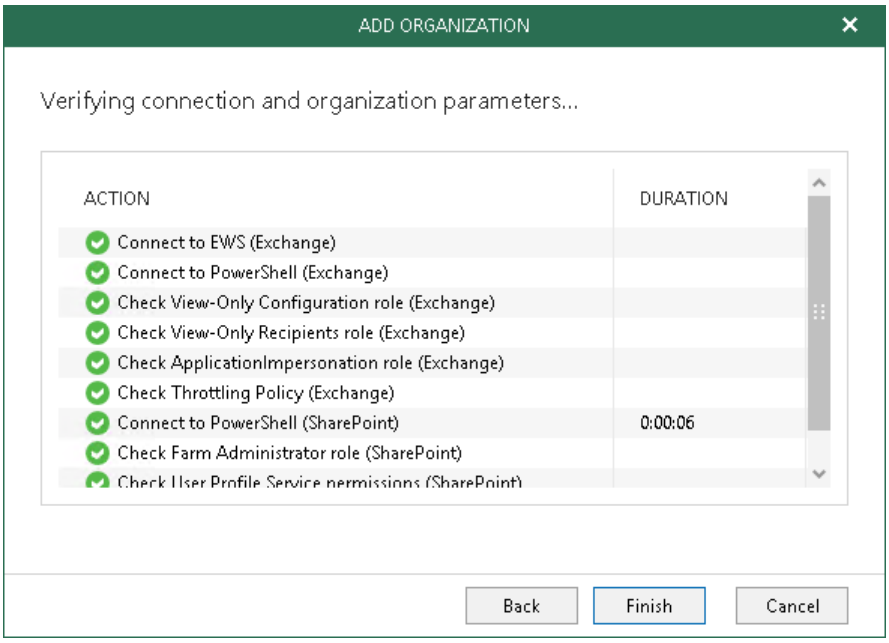
Adding On-Premises Organizations of Both Types

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

1. In the **Select organization deployment type** drop-down list, select **On-premises**.
2. Select both **Microsoft SharePoint Server** and **Microsoft Exchange Server** checkboxes and click **Next**.



3. Sequentially perform the steps described in Adding On-Premises Microsoft Exchange Organization and Adding On-Premises Microsoft SharePoint Organization.
4. Wait for a connection to be established and click **Finish**.



Adding Hybrid Organizations

You can add Microsoft Office 365, on-premises Microsoft SharePoint and on-premises Microsoft Exchange organizations simultaneously by using the same wizard.

The addition of a new hybrid organization supports the following scenarios:

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

To select services of which to create a new hybrid organization, combine the following checkboxes based on the scenarios above:

- **Exchange Online**

  To back up Microsoft Exchange Online data.

- **Microsoft Exchange Server**

  To back up on-premises Microsoft Exchange data.

- **SharePoint Online and OneDrive for Business**

  To back up Microsoft SharePoint Online and OneDrive for Business data.

- **Microsoft SharePoint Server**

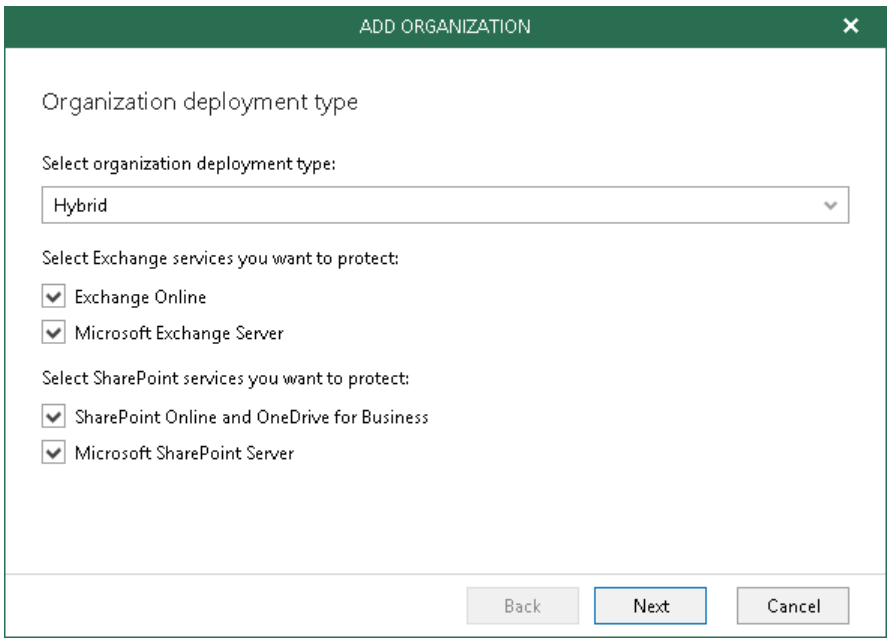
  To back up on-premises Microsoft SharePoint data.

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

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

NOTE:

Services being combined into a new hybrid organization must belong to the same Microsoft Office 365 organization.



Understanding Password Encryption

To protect sensitive data of your Online and on-premises Microsoft organizations, Veeam encrypts the password of every organization added to the scope according to the following:

- Encryption is based upon using the machine key generated under the *Local System* account under which the *Veeam.Archiver.Service* (display name — Veeam *Backup for Microsoft Office 365 Service*) is running.
- An encrypted key is stored in the configuration database on the Veeam Backup for Microsoft Office 365 management server and replicated to backup proxy servers responsible for processing associated organizations.
- An encrypted password can only be decrypted by the *Local System* account.

Editing Organization Parameters

You can edit the following organization parameters:

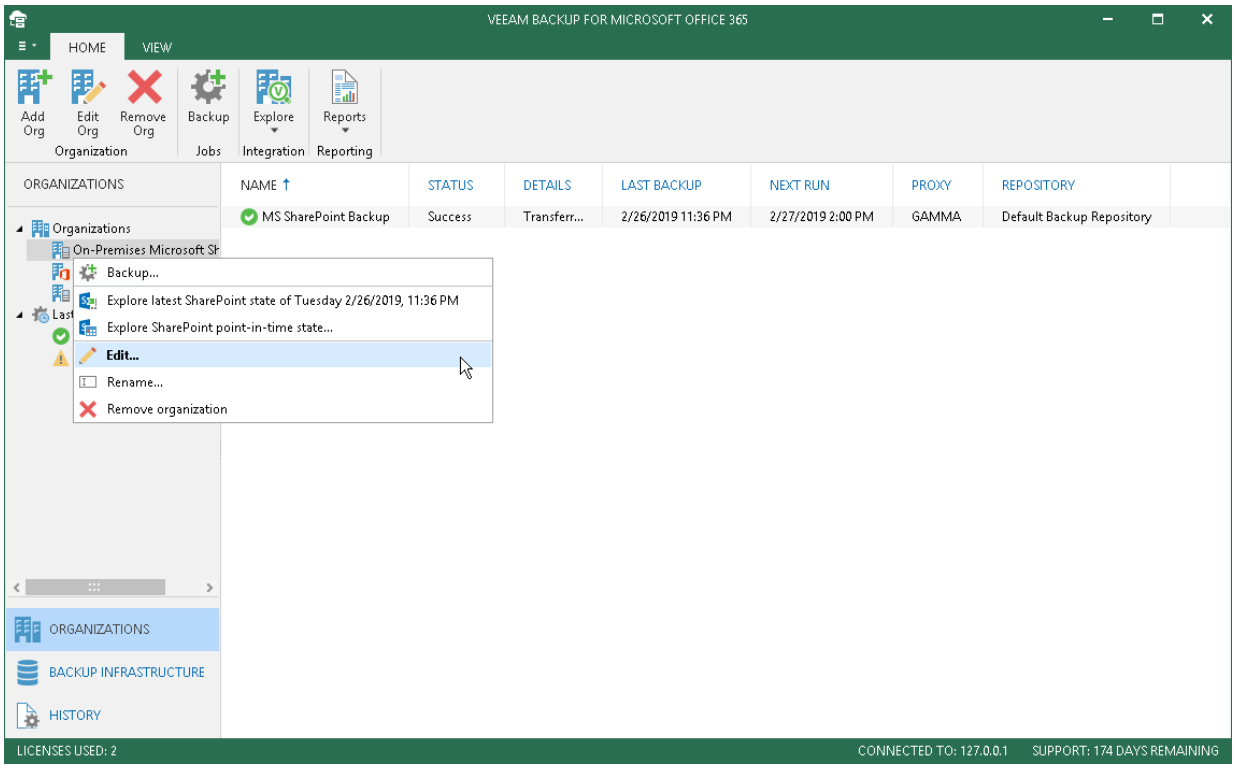
- Organization deployment type.

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

- User name and/or password.
- Permissions given to the account.

To edit organization parameters, do the following:

1. Go to the **Organizations** view.
2. In the navigation pane, select an organization to edit.
3. On the **Home** tab, click **Edit Org** or right-click an organization and select **Edit**.

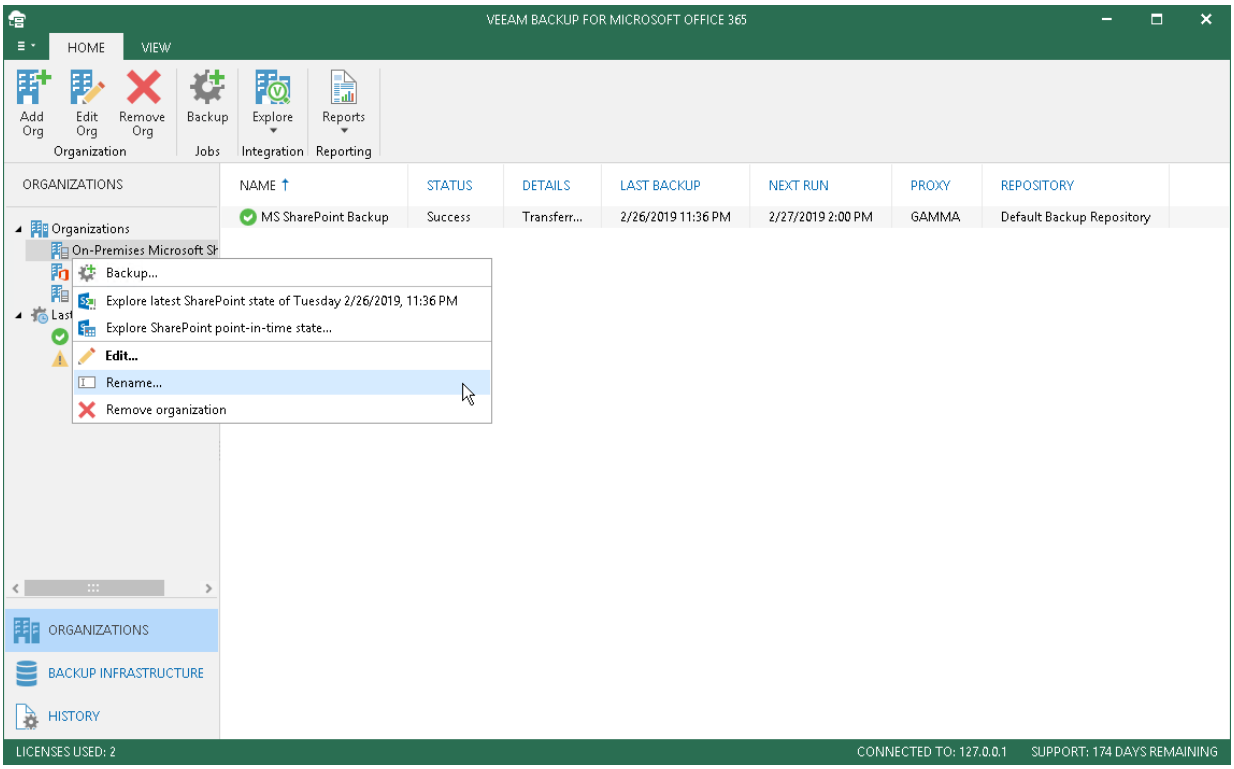


Renaming Organizations

You can rename an organization so that it would be displayed in Veeam Backup for Microsoft Office 365 under alias.

To rename an organization, do the following:

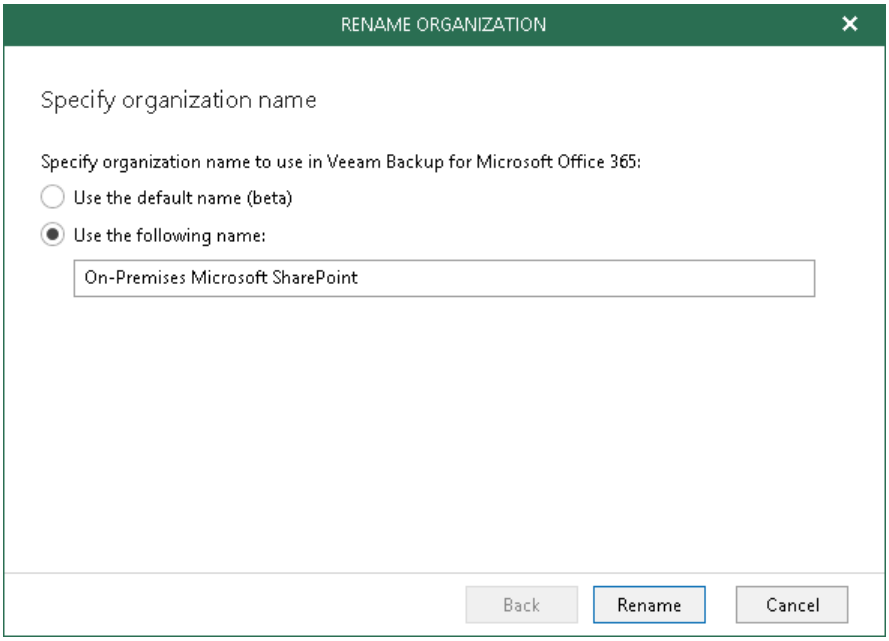
1. Go to the **Organizations** view.
2. Right-click an organization and select **Rename**.



3. In the **Rename Organization** wizard, select either of the following options:
   - **Use the default name**. To continue using the default organization name.
   - **Use the following name**. To use a custom name.

     When selecting this option, provide a new name and click **Rename**.

     Consider that when creating a Mailbox Protection Reports, organizations will be shown with their original names.

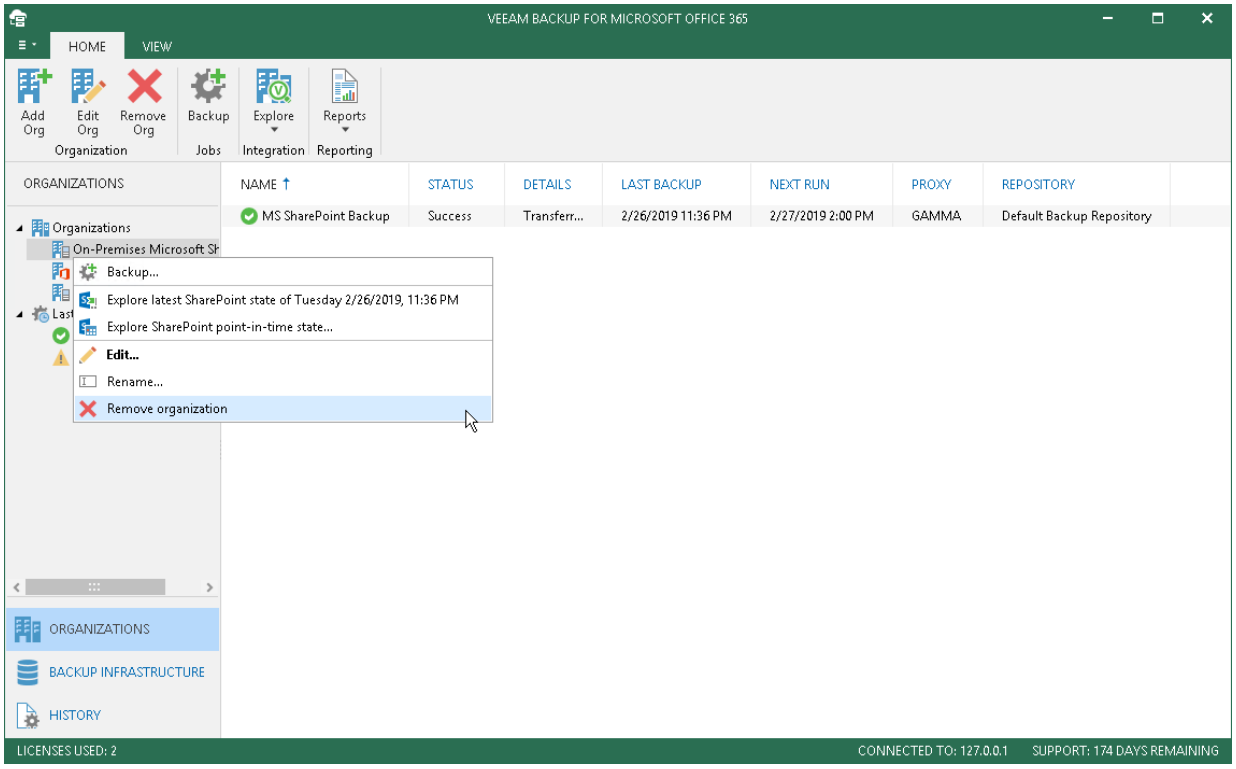

RENAME ORGANIZATION
Specify organization name
Specify organization name to use in Veeam Backup for Microsoft Office 365:
Use the default name (beta)
Use the following name:
On-Premises Microsoft SharePoint
Back
Rename
Cancel

Removing Organizations

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

To remove an organization, do the following:

1. Go to the **Organizations** view.
2. In the preview pane, select an organization to remove.
3. On the **Home** tab, click **Remove Org** or right-click an organization and select **Remove organization**.



Data Backup

Continue with this section to learn more about creating backups of Microsoft Office 365 and on-premises Microsoft organizations.

Information provided hereinafter can also be applied when creating backups using cloud platforms such as Azure or AWS. For more information on how to deploy the Veeam Backup for Microsoft Office 365 solution to these platforms, see Deploying to Azure and AWS.

Understanding Organization Object Types

This section explains object types and their corresponding processing and exclusion options that you can select when creating and configuring a backup job in Veeam Backup for Microsoft Office 365.

The following object types are available:

- Groups

  Consists of Office 365 groups (available only in Microsoft Office 365 organizations), security groups, distribution groups and dynamic distribution groups.

- Users

  Consists of users, shared mailboxes (available only in Microsoft Office 365 and Microsoft Exchange organizations) and public mailboxes (available only in Microsoft Office 365 and Microsoft Exchange organizations).

- Sites

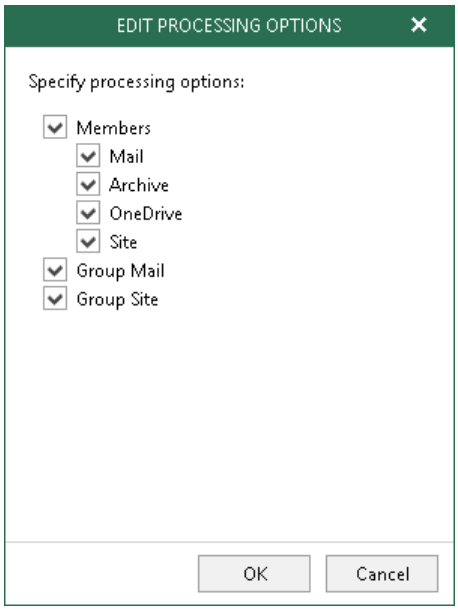
  Consists of Microsoft SharePoint sites and subsites.

- Organizations

  Consists of organization objects and their corresponding processing options.

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

Processing and exclusion options can be selected at the Select Objects to Backup and Select Objects to Exclude steps respectively.



Groups

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

Group Type	Processing/exclusion options for Microsoft Office 365 organizations	Processing/exclusion options for on-premises Microsoft Exchange organizations
O365 group (available only in Office 365 organizations)	When configuring Office 365 organizations, the following set of processing/exclusion options is available: ▪ 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:

Consider the following:

- Groups are not available in on-premises Microsoft SharePoint organizations.
- Current version of the application supports mail-enabled security groups only.

Users

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

User Type	Processing/exclusion options for Microsoft Office 365 organizations	Processing/exclusion options for on-premises Microsoft Exchange organizations	Processing/exclusion 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

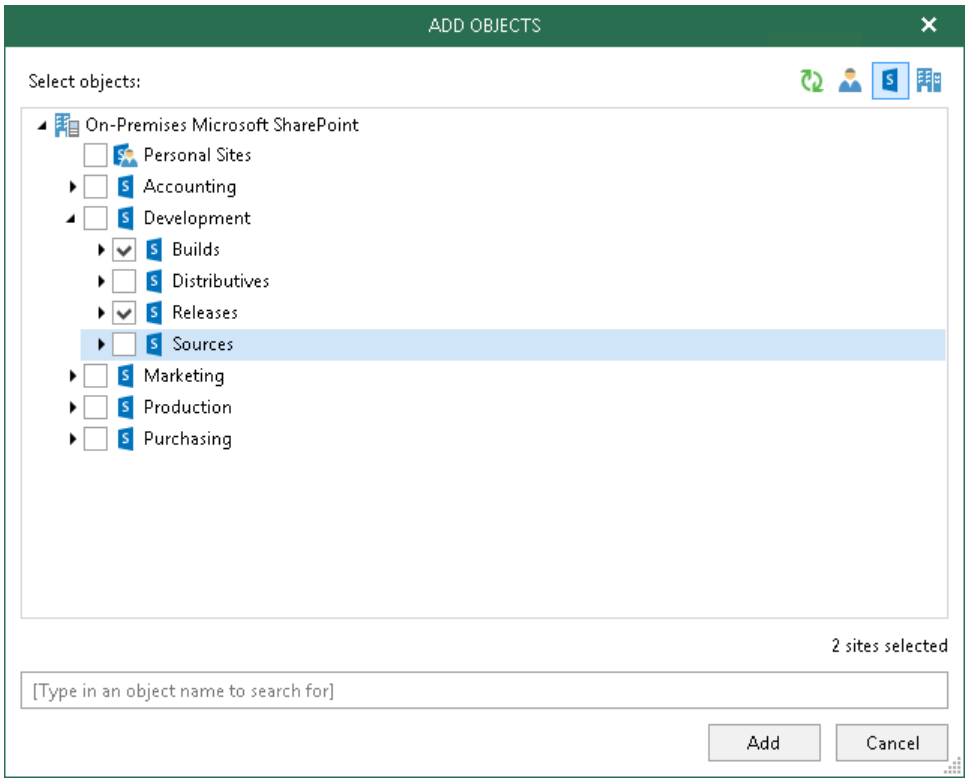
Public mailbox (available only in Office 365 and Exchange organizations)			

Sites

Consider the following:

- Objects of this type do not have any processing/exclusion options.
- Objects of this type are not available in on-premises Microsoft Exchange organizations.
- You can only select either the *root* site, or any of its *subsites*, as Veeam does not allow selecting *subsites* along with the *root* site at the same time.

  As an example, in the following figure you can only select either *Development*, which automatically selects all of its subsites, or you can select, for example, *Builds* and *Releases*. In the latter case, the root *Development* site will be deselected.



Organizations

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

Processing/exclusion options for Microsoft Office 365 organizations	Processing/exclusion options for on-premises Microsoft Exchange organizations	Processing/exclusion options for on-premises Microsoft SharePoint organizations
Mail, *Archive*, *OneDrive* and *Site*	*Mail* and *Archive*	*OneDrive* and *Site*

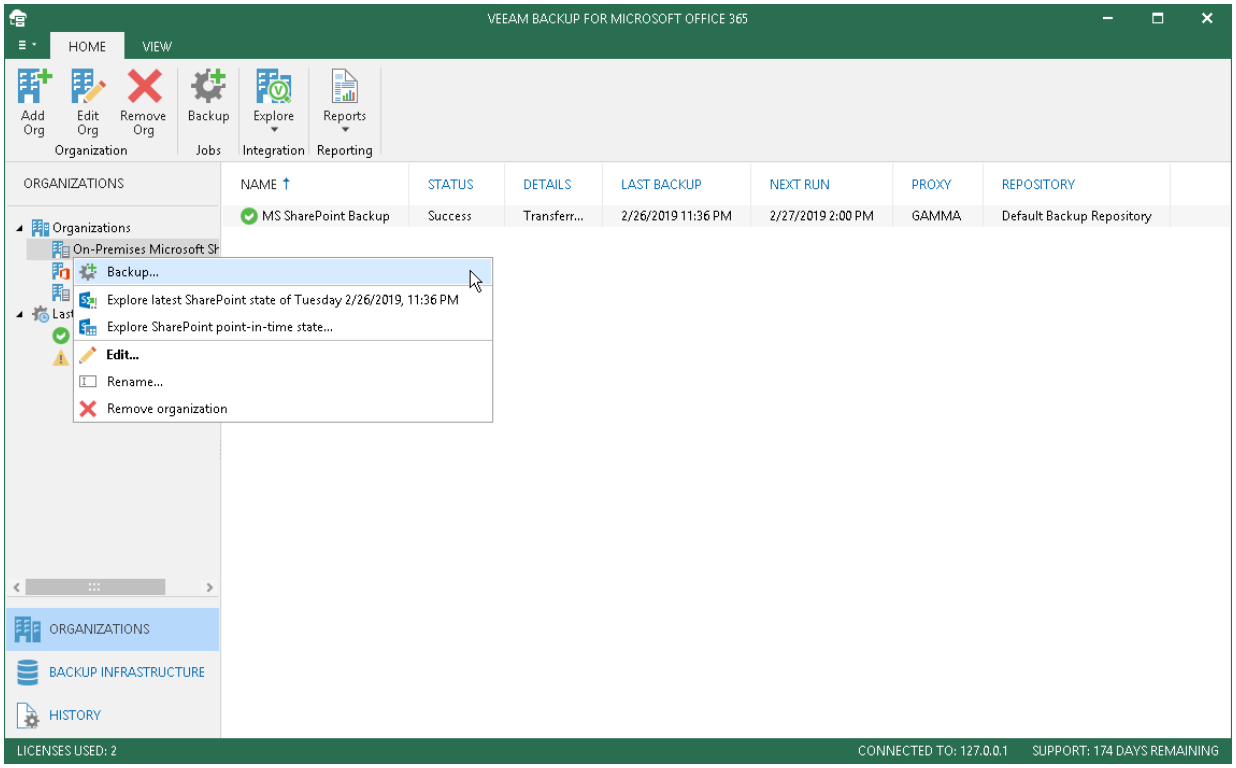
Creating Backup Job

This section explains how to create a new backup job to back up data of your Microsoft Office 365 and on-premises Microsoft organizations.

> **TIP:**
>
> Before you begin with this section, consider reading:
>
> - Understanding Organization Object Types — to learn more about available object types and their corresponding processing and exclusion options.
> - Backup Repositories — to learn how Veeam Backup for Microsoft Office 365 stores its backups.

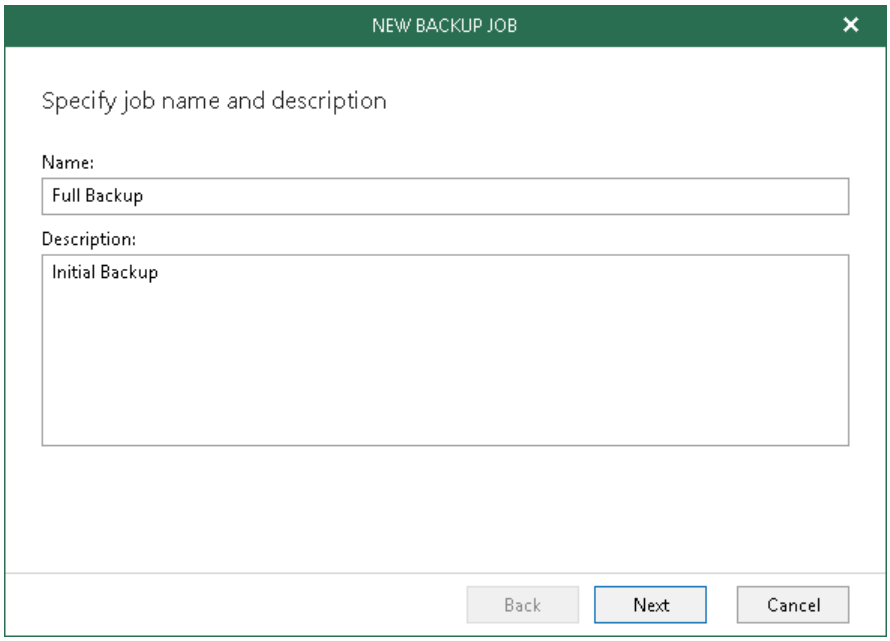
To create a new backup job, do the following:

1. Go to the **Organizations** view.
2. In the navigation pane, select an organization to back up.
3. On the **Home** tab, click **Backup** on the toolbar or right-click an organization and select **Backup**.
4. Proceed to Specify Backup Job Name.



Step 1. Specify Backup Job Name

At this step of the wizard, specify the job name and optional description.



Step 2. Select Objects to Backup

At this step of the wizard, select either of the following options:

- Back up entire organization
- Back up the following objects

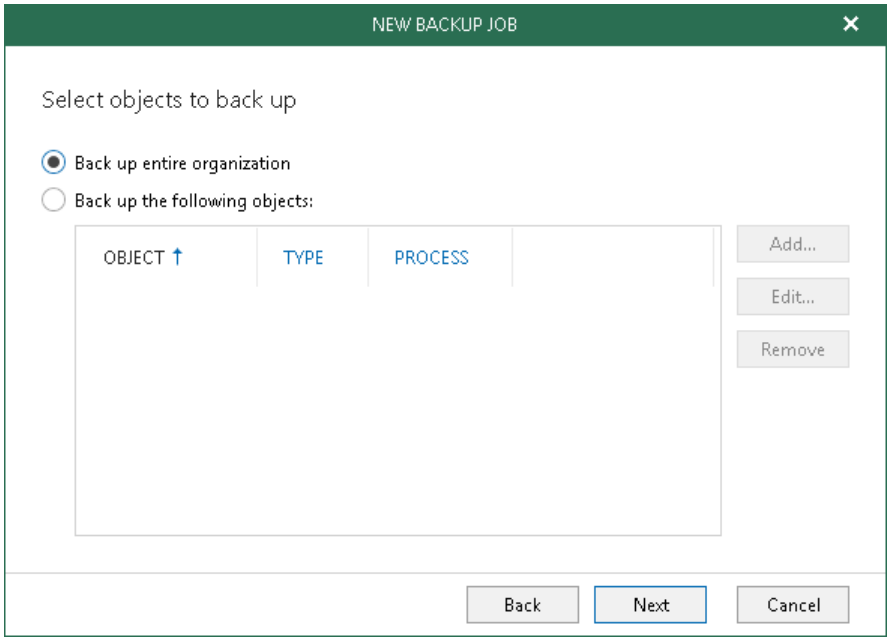
Back Up Entire Organization

The **Back up entire organization** option creates a backup consisting of all the objects of the selected organization except objects processed by other backup jobs.

For example, you create a backup job (*BETA*) to back up an entire Office 365 organization that comprises A, B and C objects. Then, you create another backup job using the **Backup the following items** option and explicitly add both B and C objects to the processing list of this job (*ALPHA*). In such a scenario, both B and C objects will no longer be processed by the *BETA* job. Instead, these objects will be archived by the *ALPHA* job.

> **NOTE:**
>
> You can create only one entire organization backup job per organization.

To create a backup job to back up all the objects of the selected organization, select the **Back up entire organization** option.



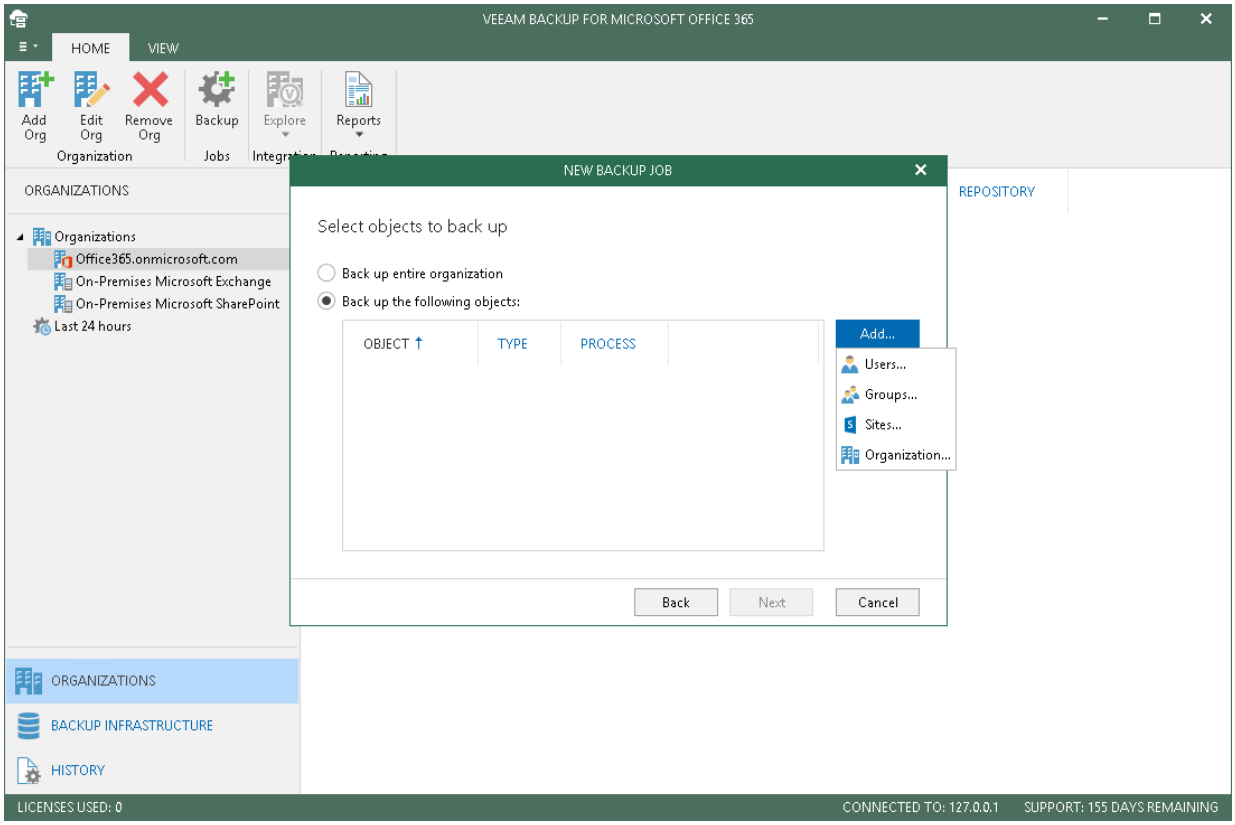
Back Up Following Objects

To choose objects to back up, do the following:

1. Select the **Backup the following objects** option.
2. Click **Add**.
3. Select users, groups, sites and organizations, the data of which you want to back up.

Consider the following:

- When creating a backup job to back up Microsoft Exchange organizations, you will not be able to add *Sites* objects, nor will you be able to add *Groups* objects for on-premises Microsoft SharePoint organizations.
- Due to possible access limitations some *Sites* objects might be unavailable.



Specifying Processing Options

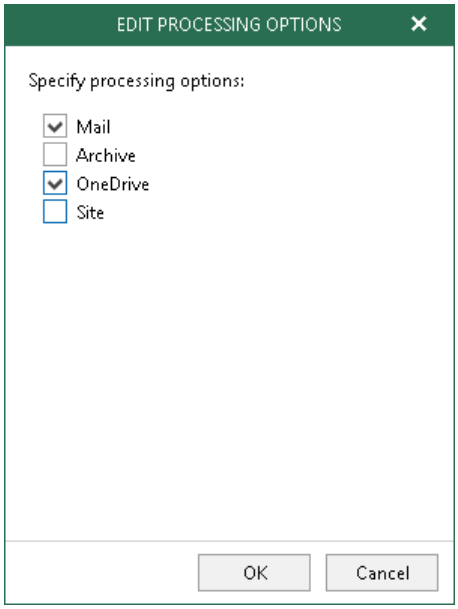
By default, when you add a new object, Veeam selects all processing options of this object. To explicitly specify processing options you need, select an object and click **Edit**. For more information about available object types and their corresponding processing options, see Understanding Organization Object Types.

For example, if you do not want to back up *Archive* and *Site*, do the following:

1. At the **Select objects to backup** step of the wizard, select an object of which you want to edit processing options.
2. Click **Edit**.
3. Deselect **Archive** and **Site**.
4. Click **OK**.

NOTE:

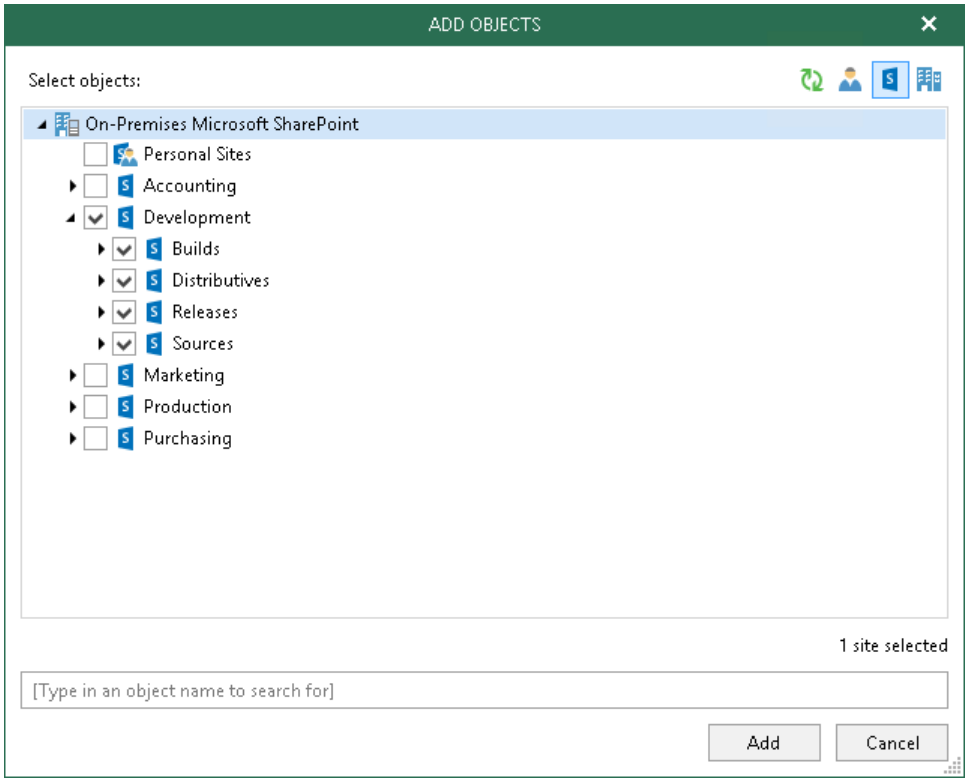
You cannot edit processing options of the *Sites* and *Public Mailbox* object types.



Adding Objects of Different Types

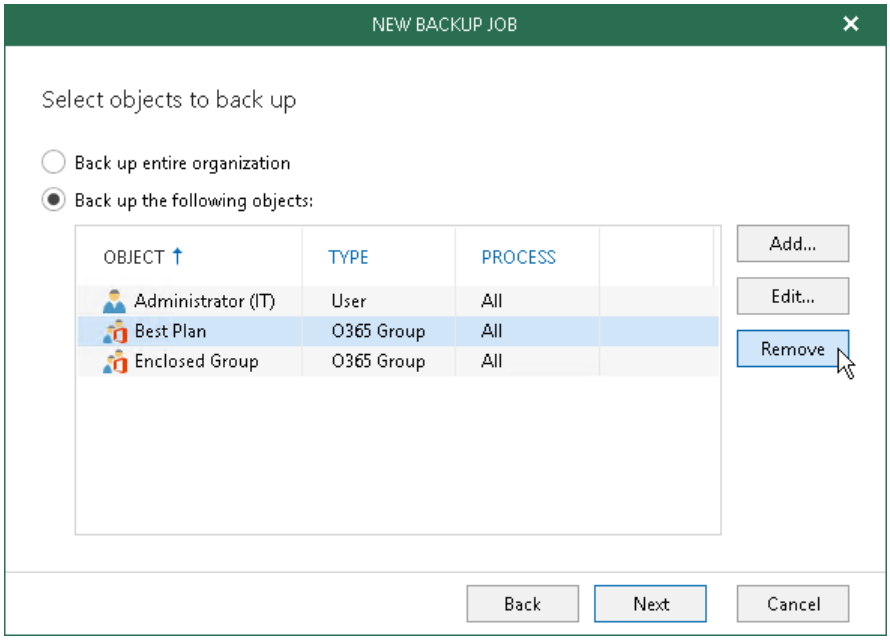
To simultaneously add objects of different types, use the switch group in the upper-right corner of the **Add Objects** dialog.

To quickly find necessary objects, use the search field at the bottom.



Removing Objects

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



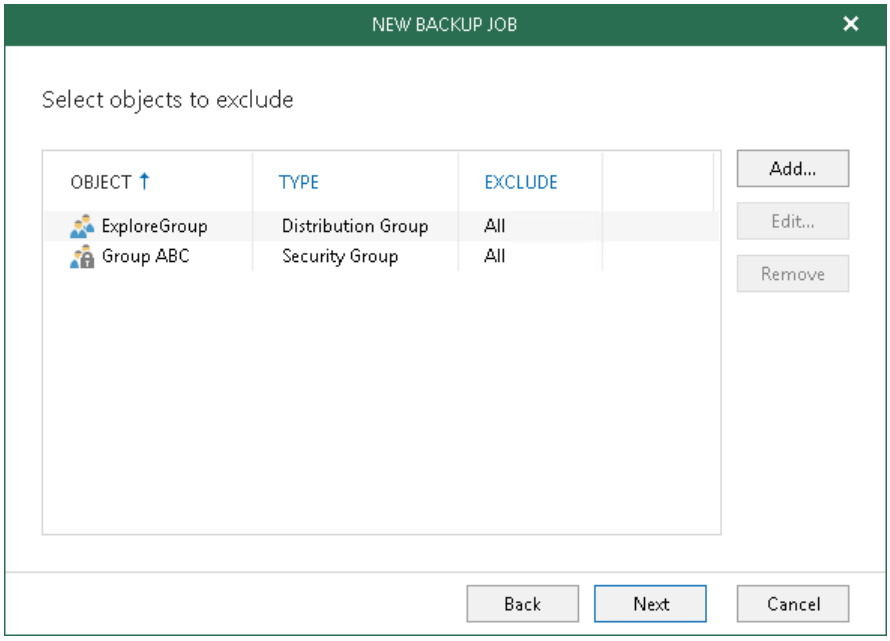
Step 3. Select Objects to Exclude

At this step of the wizard, select objects to exclude.

Consider the following:

- Depending on the organization type, you will not be able to exclude *Sites* objects of on-premises Microsoft Exchange organizations, nor will you be able to exclude *Groups* objects of on-premises Microsoft SharePoint organizations.
- You cannot exclude objects that have been added explicitly by using the **Backup the following objects** option at the Select Objects to Backup step.
- Due to possible access limitations some sites might be unavailable.

To exclude an object, click **Add** and select *Users*, *Groups* or *Sites*.

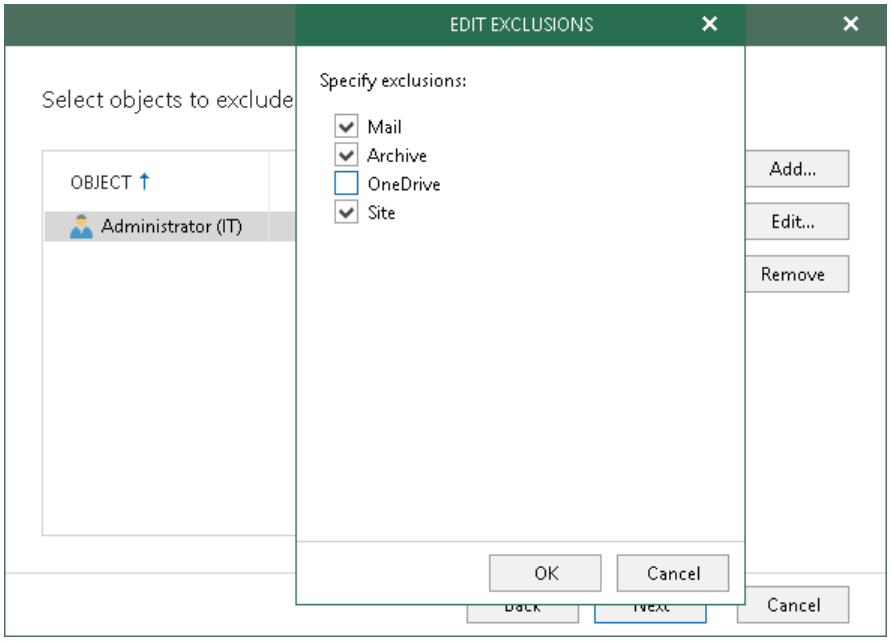


Editing Exclusions

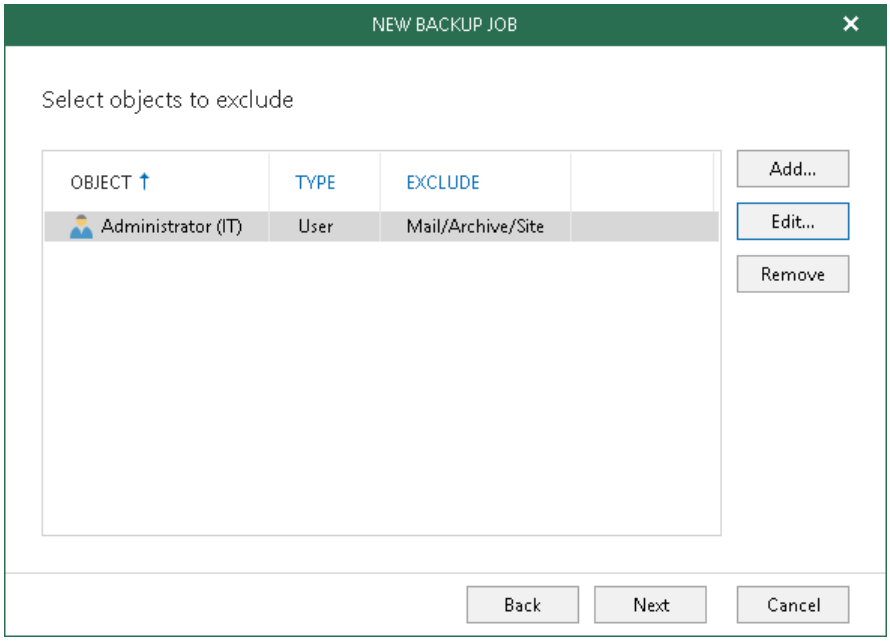
By default, when you exclude an object, Veeam selects all exclusion options of this object. To explicitly specify exclusion options you need, select an object and click **Edit**. For more information about available object types and their corresponding exclusion options, see Understanding Organization Object Types.

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

The following figure shows an example of excluding the *Administrator (IT)* object, of which the *Mail, Archive* and *Site* types will not be backed up. The *OneDrive* type, however, will be backed up since it was deselected in the **Edit Exclusions** dialog and therefore will not be excluded.



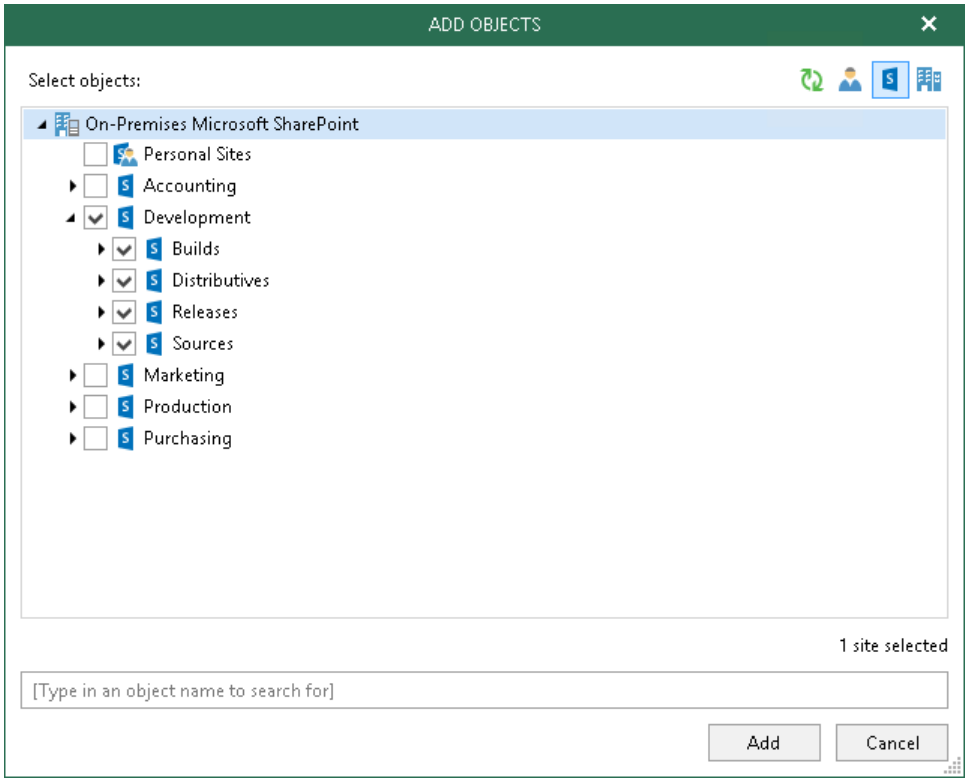
To see what is excluded, refer to the **Exclude** column. As per example below, the excluded types are *Mail*, *Archive* and *Site*.



Adding Objects of Different Types

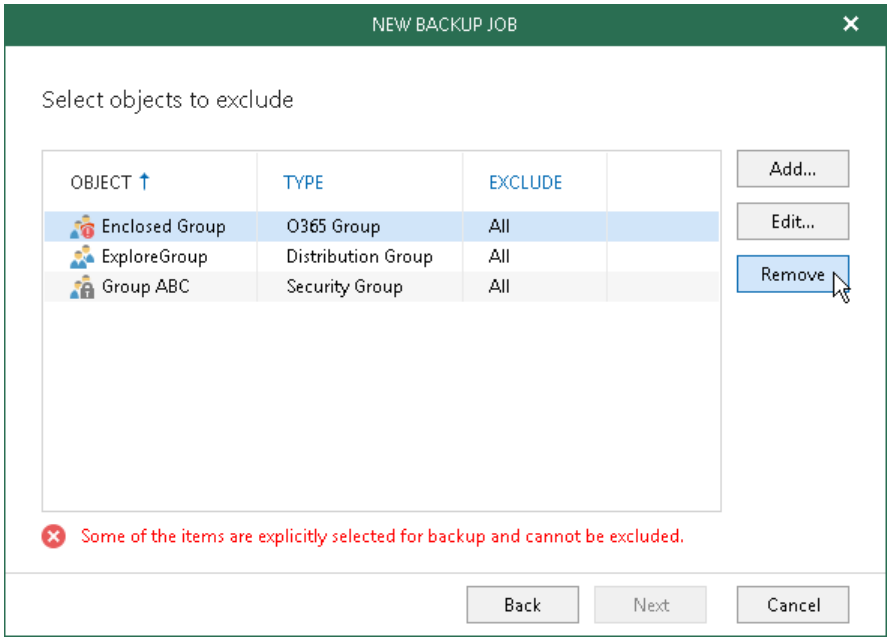
To simultaneously add objects of different types, use the switch group in the upper-right corner of the **Add Objects** dialog.

To quickly find necessary objects, use the search field at the bottom.



Removing Objects

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



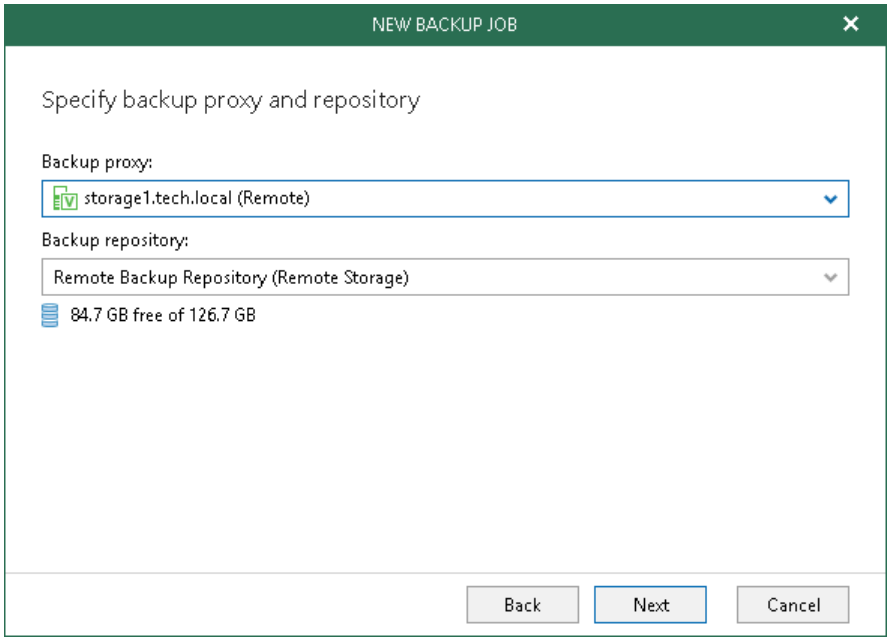
Step 4. Specify Backup Proxy and Repository

At this step of the wizard, do the following:

- Select a backup proxy server.
- Specify a backup repository to store your data.

For more information about backup proxy servers and backup repositories, see Backup Proxy Servers and Backup Repositories.

> **NOTE:**
>
> You cannot use a backup proxy server that is offline.



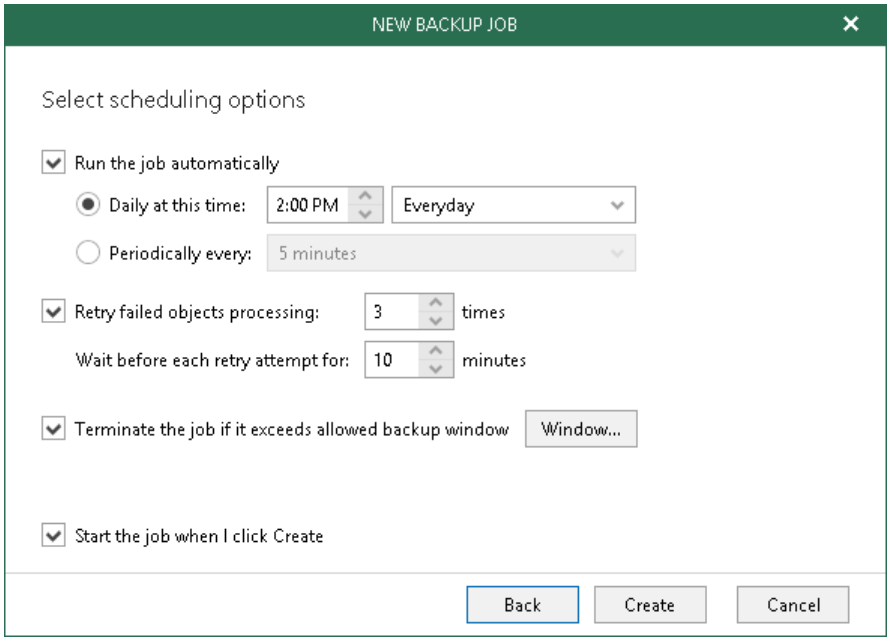
Step 5. Specify Scheduling Options

At this step of the wizard, specify the following:

- To configure automatic execution of a backup job, select the **Run the job automatically** checkbox and customize the schedule you want to be applied.

  Either of the following options is available:

  - **Daily at this time**. To run the job daily at specified hours.
  - **Periodically every**. To run the job every *N* minutes.
- To perform retry attempts, select the **Retry failed objects processing** checkbox and specify the maximum number of retry attempts. In addition, define the time interval to be considered by the system before attempting subsequent retries.
- To define a period when a backup job should (or should not) be executed, select the **Terminate job if it exceeds allowed backup window** checkbox, click **Window** and specify allowed and prohibited hours, as described in Selecting Time Periods.
- To run a backup job upon completion of the wizard, select the **Start the job when I click Create** checkbox.



Selecting Time Periods

When you click **Window**, the **Time Period** dialog will be shown in which you can:

- Set up the *Permitted* execution time frame for the backup job.
- Set up 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 *12AM* to *11:59PM*.

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:

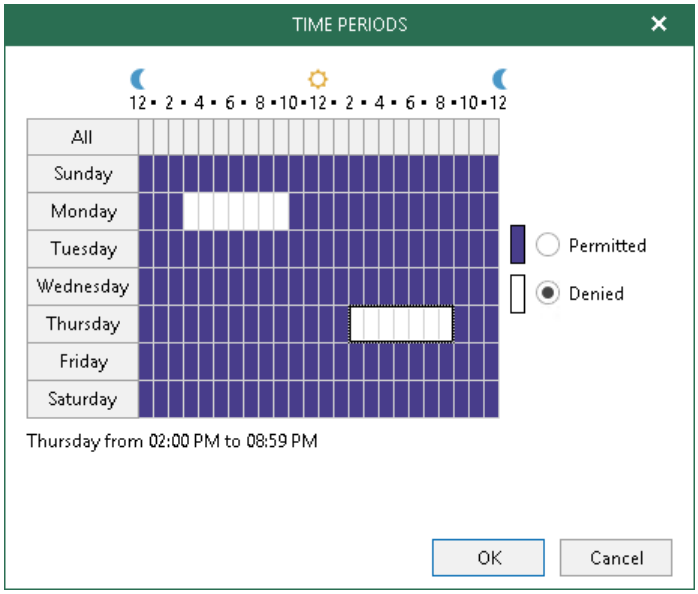
1. Select a block that corresponds to the day of the week (vertical axis) and to the time interval (horizontal axis) on which you want to allow or prohibit the execution of a backup job.

   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, including different days of the week.
   - Click a day of the week in the vertical axis to select all the blocks of the day thereof.
   - Click **All** in the vertical axis to select all the blocks of the entire week.
2. On the right-hand side, select either **Permitted** or **Denied** option to set up the execution rule for the selected blocks.

The following figure shows an example in which it is prohibited to run a backup job on the following days of the week:

- *Monday* from *03:00AM* up until *09:59AM.*
- *Thursday* from *02:00PM* up until *08:59PM.*



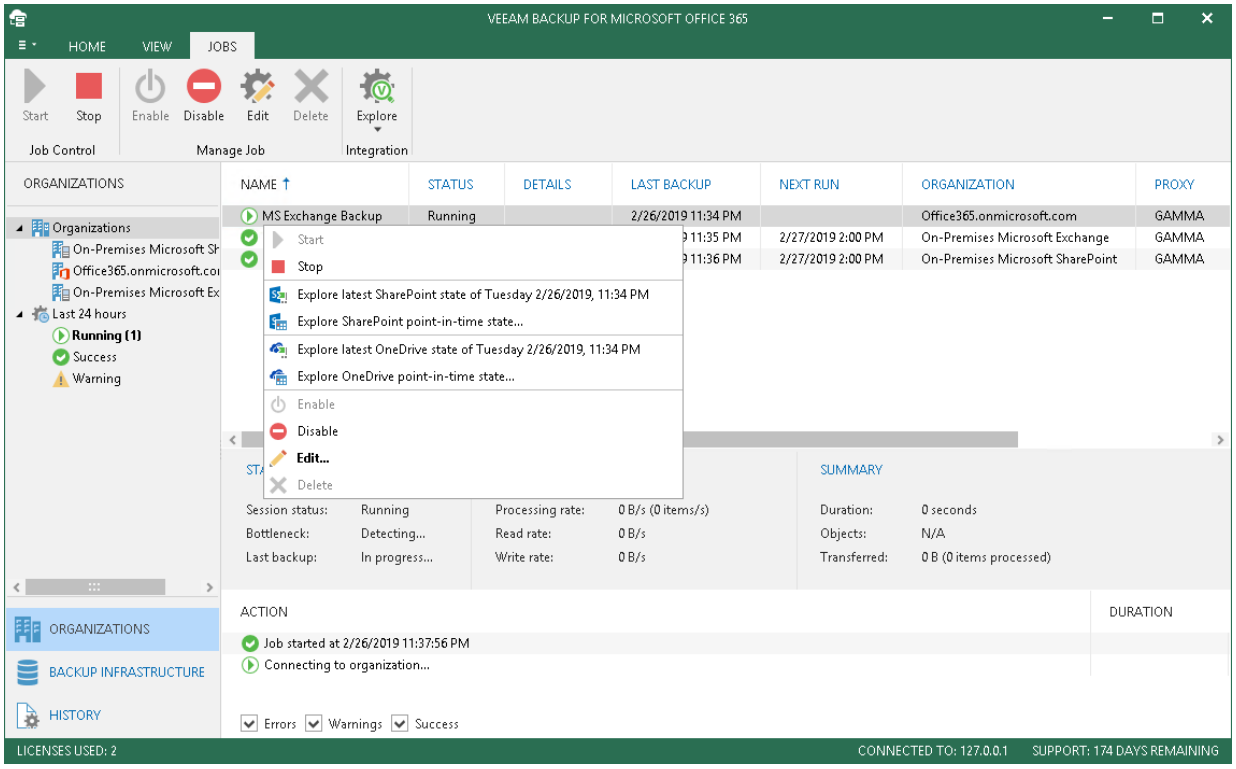
Managing Backup Jobs

To manage a backup job, do the following:

1. Go to the **Organizations** view.
2. In the navigation pane, select an organization.

   Select the root **Organizations** node to see all the backup jobs of each organization.
3. In the preview pane, select a backup job.
4. On the **Jobs** tab or by right-clicking a backup job, select any of the following commands:
   - **Start/Stop**. To start or stop a backup job:
     - The **Stop** command freezes the current backup job state preserving what has already been backed up.
     - The **Start** command runs a job. If a job has been stopped, the **Start** command will continue its session.
   - **Enable/Disable**. To enable or disable a backup job.
     - The **Enable** command enables a backup job if it has previously been disabled so that it can be executed on demand.
     - The **Disable** command disables a backup job.

       When a backup job is disabled, the schedule that you might have configured for this job will not be applied. You can still, however, launch such a disabled job manually by using the **Start** command. Once the session is complete (or if was aborted by the **Stop** command), then such a job will be switched back to *Disabled* until you enable it manually using the **Enable** command.
   - **Edit**. To edit backup job settings.
   - **Delete**. To remove a backup job from the configuration.
   - **Explore latest <Product> state of <date_and_time>**. To launch Veeam Explorer, as described in Data Restore.


VEEAM BACKUP FOR MICROSOFT OFFICE 365
HOME
VIEW
JOBS
Start
Stop
Enable
Disable
Edit
Delete
Explore
Job Control
Manage Job
Integration
ORGANIZATIONS
NAME
STATUS
DETAILS
LAST BACKUP
NEXT RUN
ORGANIZATION
PROXY
MS Exchange Backup
Running
2/26/2019 11:34 PM
Office365.onmicrosoft.com
GAMMA
On-Premises Microsoft Exchange
2/27/2019 2:00 PM
On-Premises Microsoft SharePoint
Explore latest SharePoint state of Tuesday 2/26/2019, 11:34 PM
Explore SharePoint point-in-time state...
Explore latest OneDrive state of Tuesday 2/26/2019, 11:34 PM
Explore OneDrive point-in-time state...
Last 24 hours
Running (1)
Success
Warning
SUMMARY
Session status:
Running
Bottleneck:
Detecting...
Last backup:
In progress...
Processing rate:
0 B/s (0 items/s)
Read rate:
0 B/s
Write rate:
0 B/s
Duration:
0 seconds
Objects:
N/A
Transferred:
0 B (0 items processed)
ACTION
DURATION
Job started at 2/26/2019 11:37:56 PM
Connecting to organization...
Errors
Warnings
Success
BACKUP INFRASTRUCTURE
HISTORY
LICENSES USED: 2
CONNECTED TO: 127.0.0.1
SUPPORT: 174 DAYS REMAINING

Viewing Backup and Restore Sessions Statistics

Each backup or restore session saves its results to the configuration database.

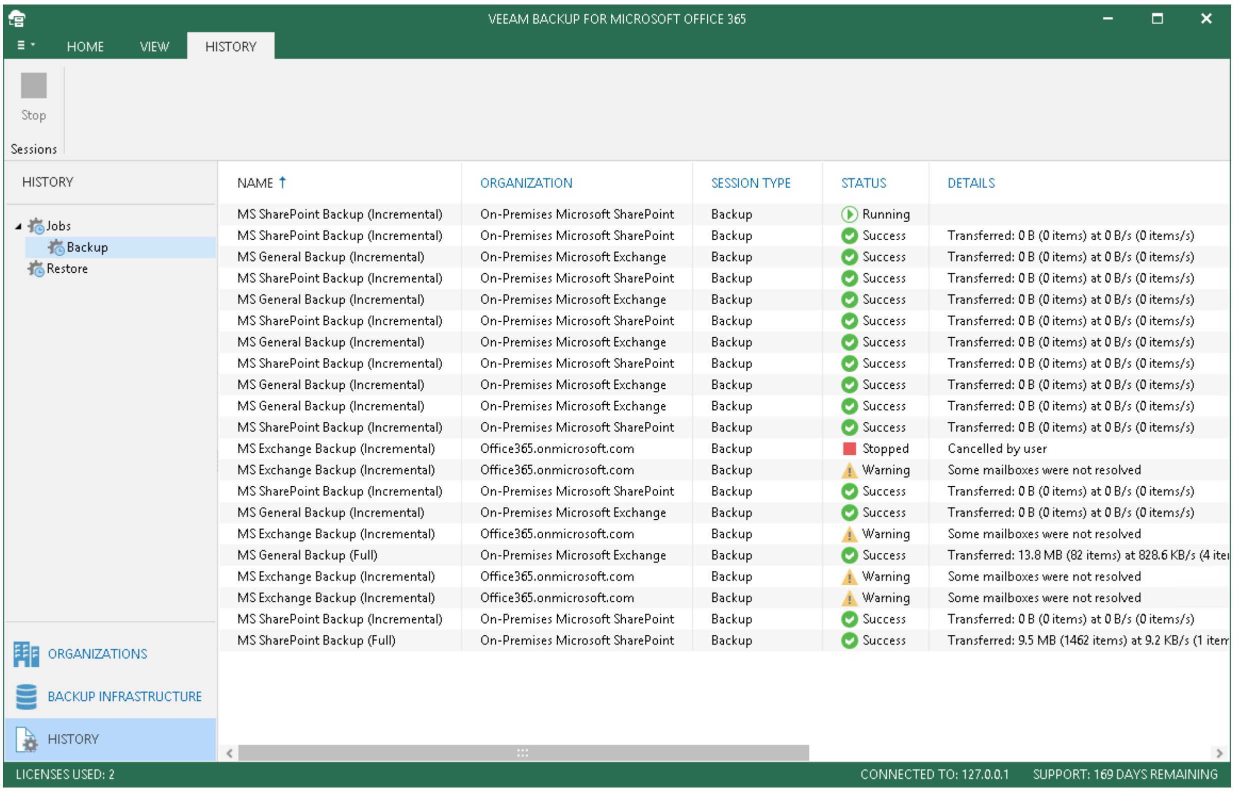
To review the results, go to the **History** view and select either of the following nodes:

- **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 toolbar.

To review session results of only particular type, use the *Success*, *Warnings* or *Errors* checkboxes at the bottom.

> **TIP:**
>
> Session data is stored in the configuration database according to the retention settings, as described in Configuring Session Data History.



Data Restore

To restore your Microsoft Office 365 data, you can use the abilities of Veeam Explorers, as described in:

- Veeam Explorer for Microsoft Exchange

  To explore and recover Microsoft Exchange mailboxes, folders, messages, tasks, contacts and items.
- Veeam Explorer for Microsoft SharePoint

  To explore and recover Microsoft SharePoint sites, libraries and items.
- Veeam Explorer for Microsoft OneDrive for Business

  To explore and recover Microsoft OneDrive for Business items and folders.

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

- Exploring Backup Jobs

  To view the content of a backup file created by the selected backup job.
- Exploring Single Organization

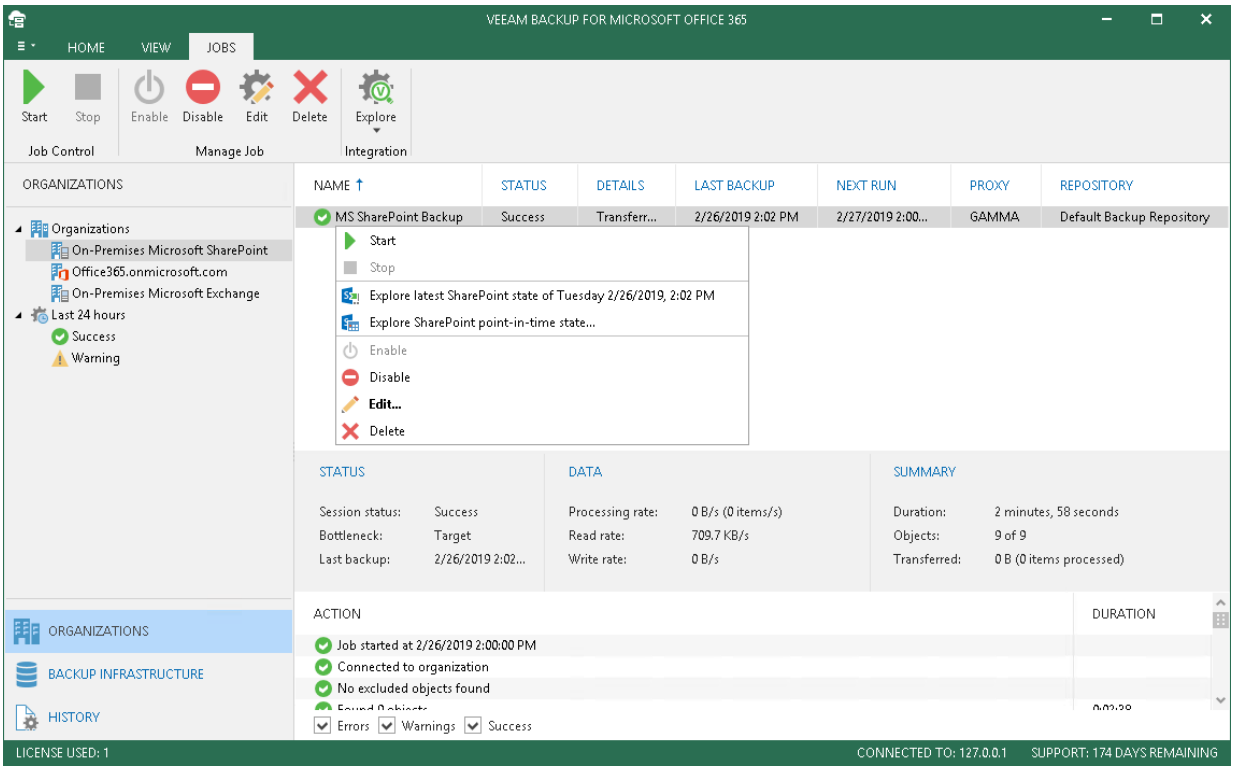
  To view the content of backup files of the selected organization.
- Exploring All Organizations

  To view the content of backup files of each organization added to the scope.

Exploring Backup Jobs

To view the content of a backup file created by the selected backup job, do the following:

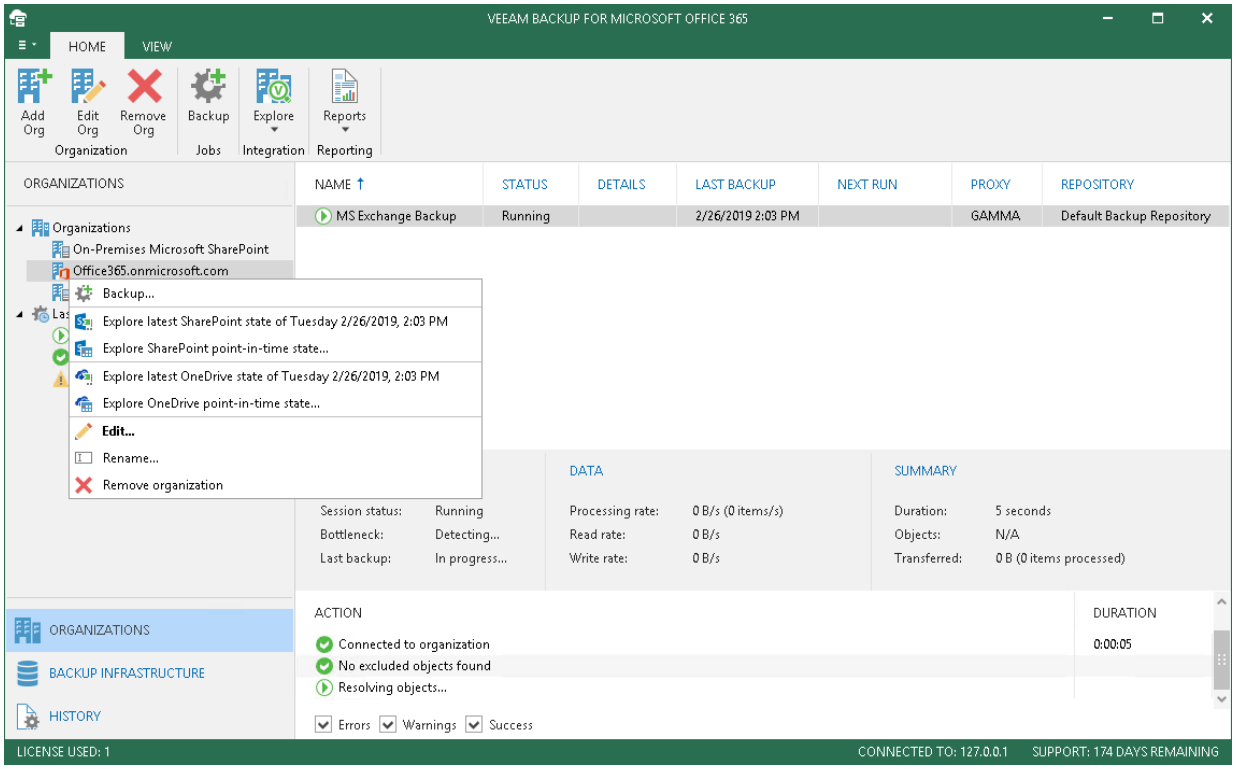
1. In the **Organizations** view, select an organization that contains backup jobs you want to explore.
2. In the preview pane, select a backup job and click **Explore** on the toolbar or right-click a backup job and select either of the following options:
    a) **Explore latest <Product> state of <date_and_time>**. To explore the latest backup state.
    b) **Explore point-in-time state**. To select a point-in-time state. For more information, see Exploring Point-in-time.



Exploring Single Organization

To view the content of backup files created by all the backup jobs of the selected organization, do the following:

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



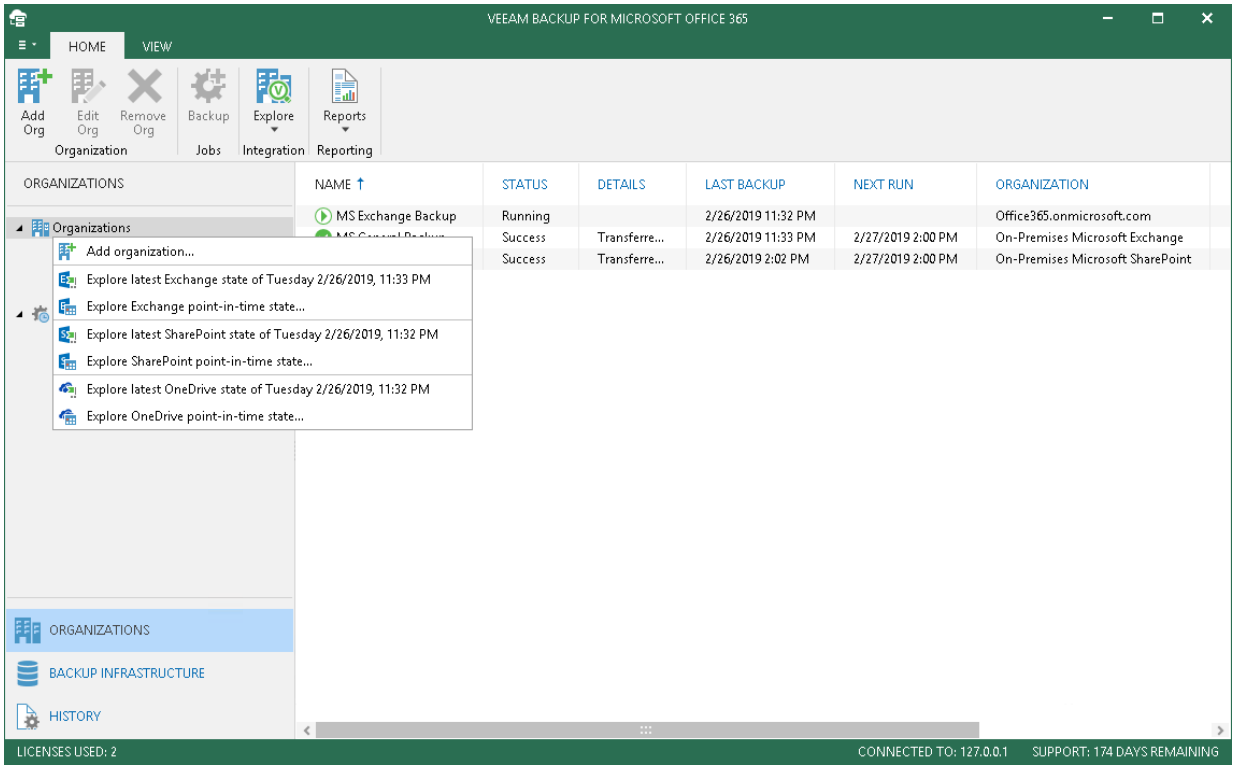
Exploring All Organizations

To view the content of backup files of all the organizations added to the scope, do the following:

- In the **Organizations** view, right click the root **Organizations** node and select either of the following options:

    a) **Explore latest <Product> state of <date_and_time>**. To explore the latest backup state.

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



Exploring Point-In-Time

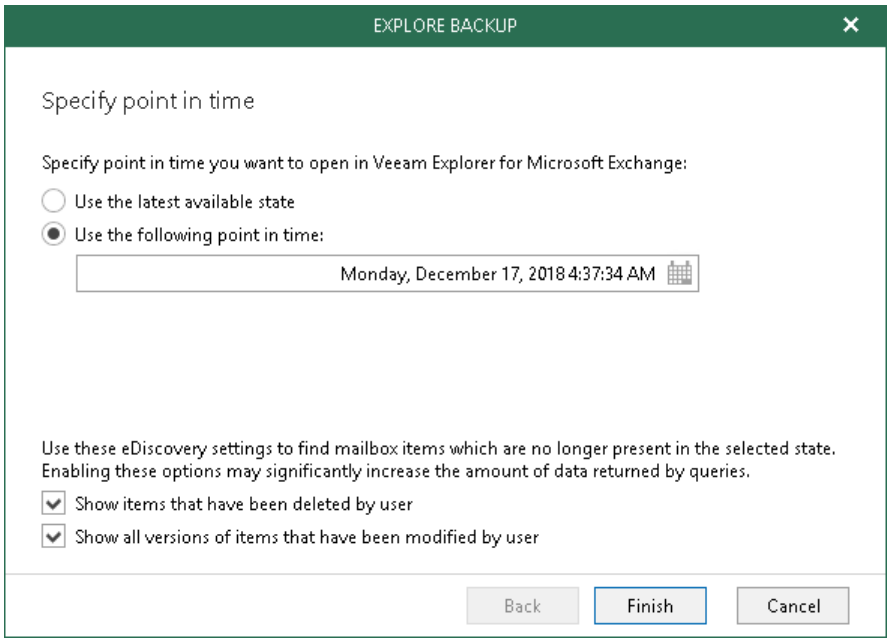
When exploring a point in time state, you can opt for either of the following options:

- **Use the latest available state**. To view the latest state of items in a backup file.
- **Use the following point in time**. To set up a date and time as of which to view data.

To view historic data, select the following checkboxes:

- **Show items that have been deleted by user**. To load removed items.
- **Show all versions of items that have been modified by user**. To load modified items.

> **NOTE:**
>
> Both **Show items that have been deleted by user** and **Show all versions of items that have been modified by user** options retrieve required information from other restore points in your backup repositories and might take additional time to load the data.



Reports

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 users mailboxes of your Microsoft Office 365 and on-premises Microsoft Exchange organizations.

Each report consists of the following fields and shows information per user mailbox.

Field	Description
Description	Shows the static description of a report.
Reporting Date	Shows the date when a report was created.
License Information	Shows the product name and a license type.
Summary	Shows the total number of protected and unprotected users 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. 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:

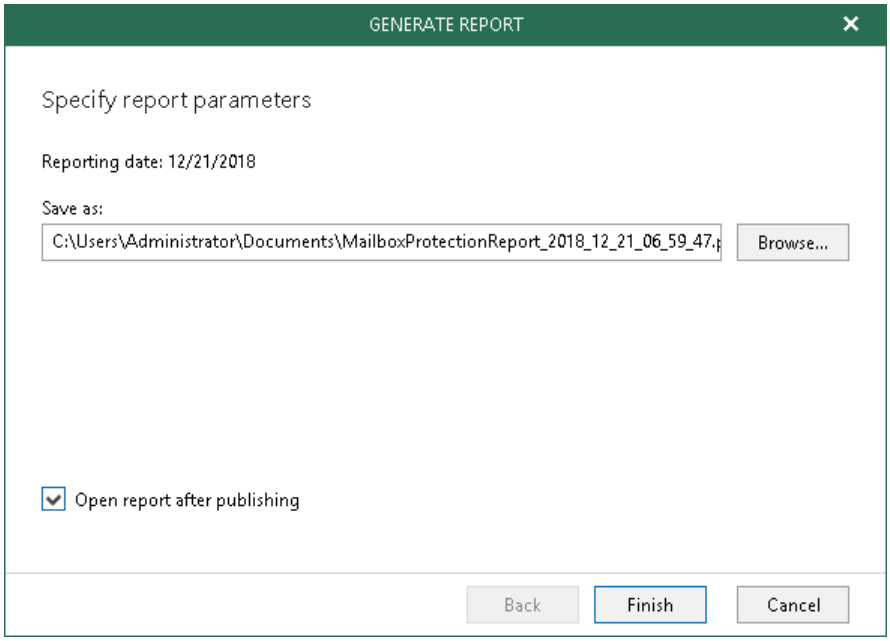
1. In the navigation pane, select an organization for which to create a report.

   You can also select the root **Organizations** node to generate a report for all organizations added to the scope.

2. In the **Organizations** view, on the **Home** tab, select **Reports** > **Mailbox Protection**.
3. 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.

4. Select the **Open report after publishing** checkbox to open the generated report using the default application.
5. Click **Finish**.


GENERATE REPORT
Specify report parameters
Reporting date: 12/21/2018
Save as:
C:\Users\Administrator\Documents\MailboxProtectionReport_2018_12_21_06_59_47.
Browse...
Open report after publishing
Back
Finish
Cancel

Creating Storage Consumption Reports

Storage Consumption reports show statistical information on how much space is occupied in your backup repositories.

Each report consists of the following fields and shows information per backup repository.

Field	Description
Description	Shows the static description of a report.
Reporting Interval	Shows the time interval for which the report was generated.
License Information	Shows the product name and a license type.
Summary	Shows occupied storage space of all backup repositories added to the scope.
Top 5 repositories by storage usage	Shows top 5 repositories the backup data on which occupies the most disk space.
Top 5 repositories by growth	Shows top 5 repositories in which the space is occupied most frequently.
Daily Change Rate (in GB)	Information is shown per backup repository.
Repository Growth (in GB)	

Consider the following:

- Repositories that have no statistical information will not be included in the report. For example:
  - You have added a new backup repository, as described in Adding Backup Repositories.

    Since nothing has been placed to a backup repository after it was added, no statistical information is available, therefore, this repository will not be included in the report.
  - You have upgraded your previous version of Veeam Backup for Microsoft Office 365 with a newer one, as described in Upgrading to Veeam Backup for Microsoft Office 365 3.0.

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

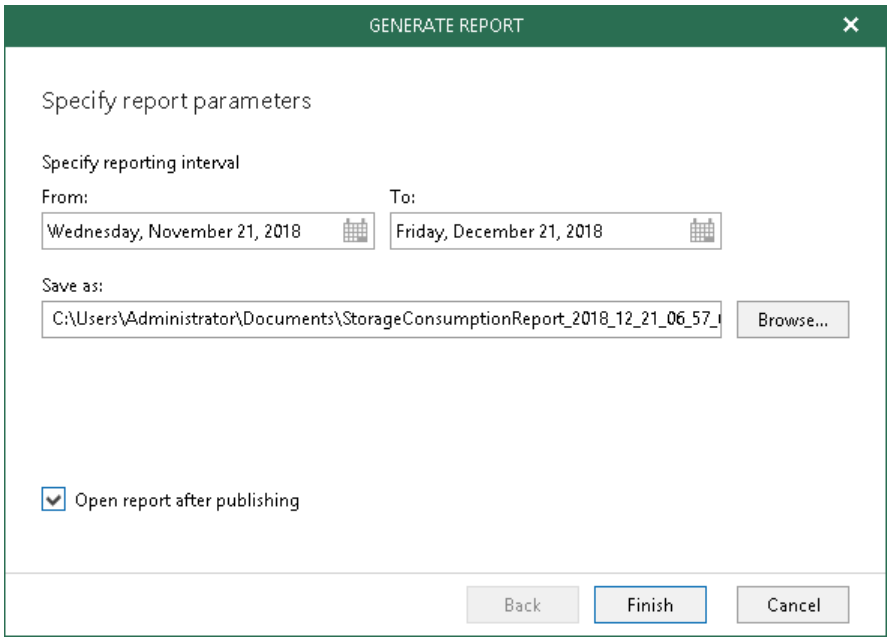
  For example, a report is said to be built starting from *01/01/2019* to *31/01/2019*, and the period from *01/01/2019* to *09/01/2019* is empty (i.e. both the **Daily Change** and **Total Size** values are less than 10MB). In this scenario, such a report will only be showing statistical information starting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

To generate a report for each organization added to the scope, do the following:

1. In the **Organizations** view, on the **Home** tab, select **Reports** > **Storage Consumption**.
2. Set up a time interval.
3. 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.

4. Select the **Open report after publishing** checkbox to open the generated report using the default application.
5. Click **Finish**.



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 the static description of a 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 per license usage	Shows top 5 organizations that consume the license the most.

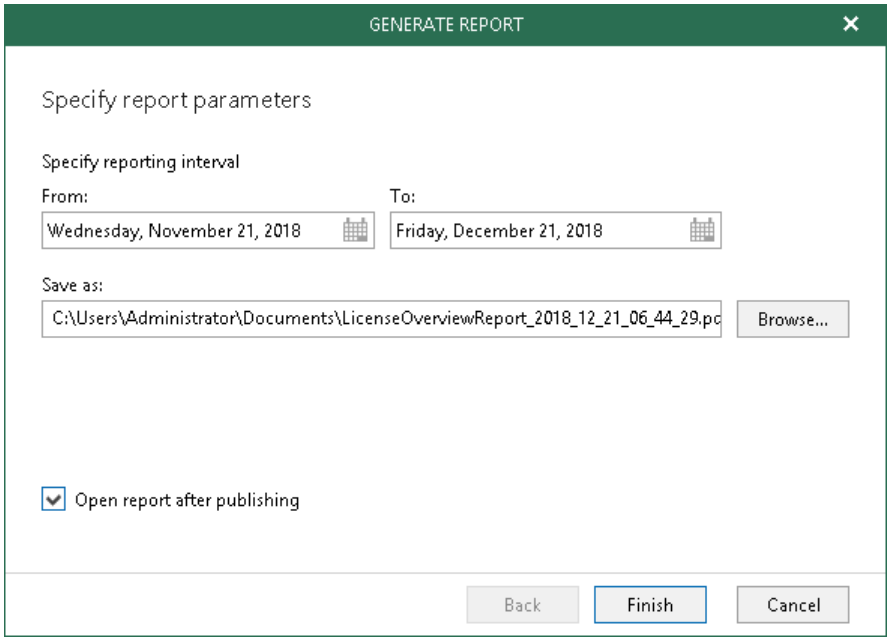
NOTE:

When using a rental license, License Overview reports also show the number of trial licenses per each organization. A trial license applies to each user account the objects of which have been backed up. Such a trial state of an account does not consume your rental license and lasts until the first day of the following month, after which each user account the objects of which have been backed up starts consuming a rental license immediately. For more information, see Rental License and Licensing and License Types.

To generate a report for each organization added to the scope, do the following:

1. In the **Organizations** view, on the **Home** tab, select **Reports** > **License Overview**.
2. Set up a time interval.
3. 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.
4. Select the **Open report after publishing** checkbox to open the generated report using the default application.
5. Click **Finish**.


GENERATE REPORT
Specify report parameters
Specify reporting interval
From:
Wednesday, November 21, 2018
To:
Friday, December 21, 2018
Save as:
C:\Users\Administrator\Documents\LicenseOverviewReport_2018_12_21_06_44_29.pd
Browse...
Open report after publishing
Back
Finish
Cancel

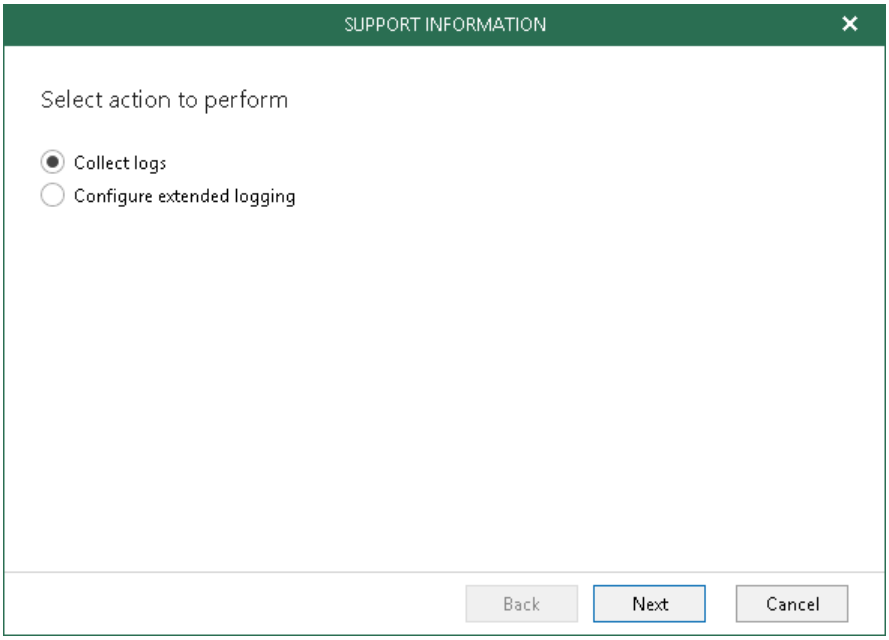
Log Files Export

Log files are used to troubleshoot a variety of different situations when certain application processes may have gotten unexpected results while being executed.

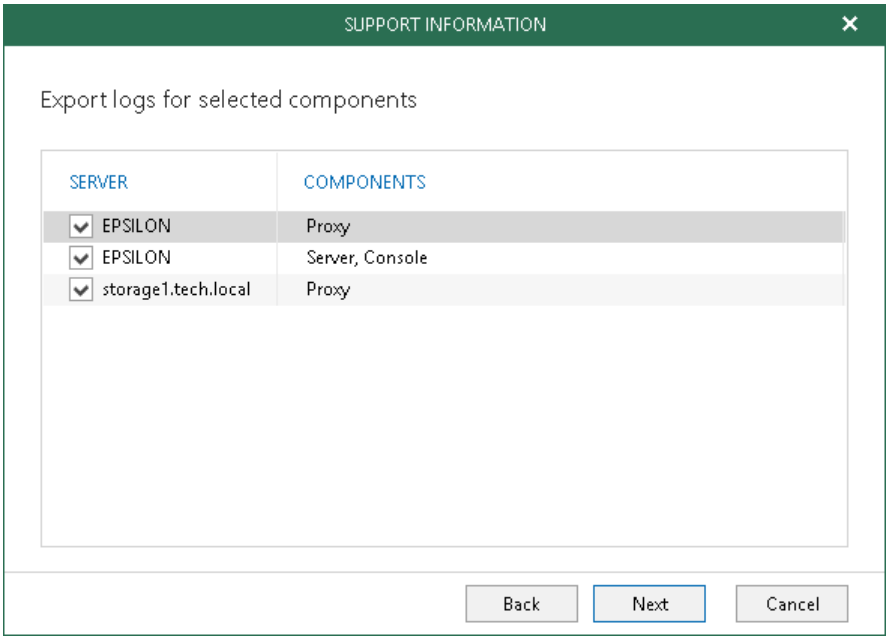
To obtain log files, do the following:

1. Go to the main menu and 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.

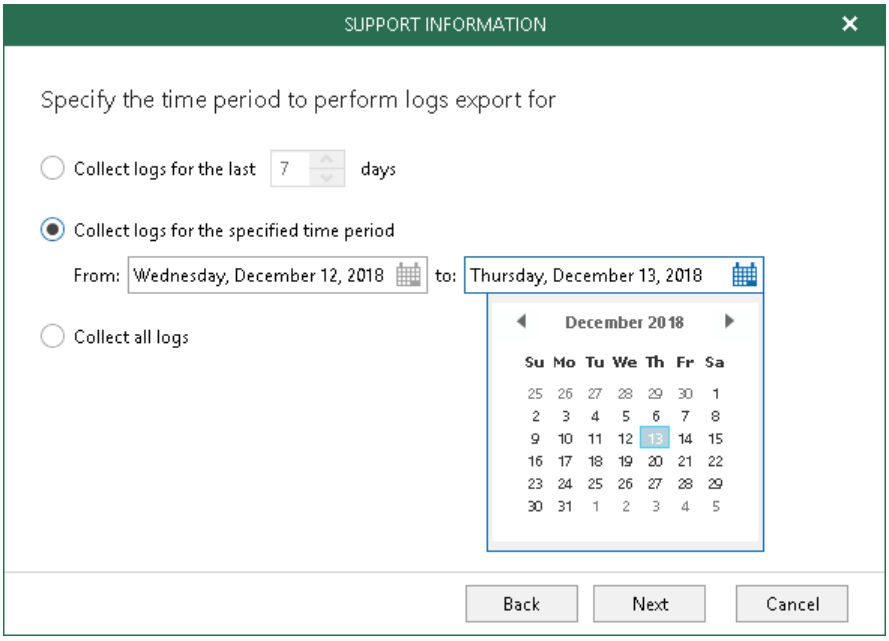


3. Select system components for which to obtain log files.

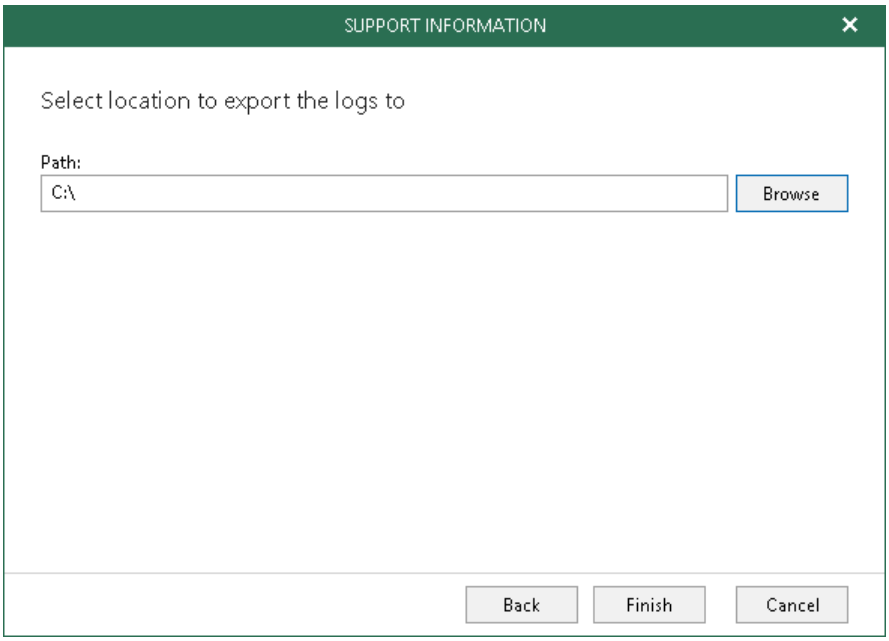


4. Specify a time period for log export:

- 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.



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



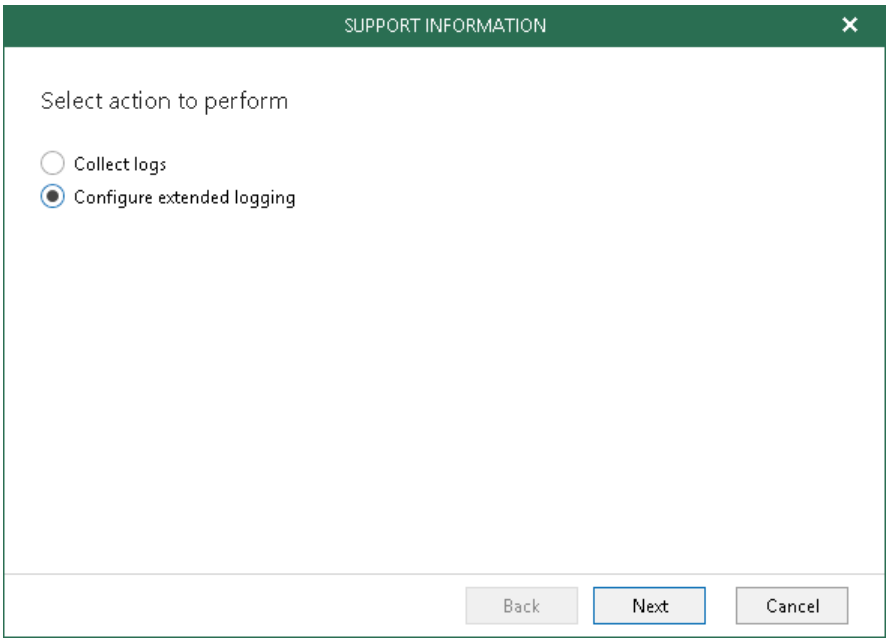
Configuring Extended Logging Mode

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.

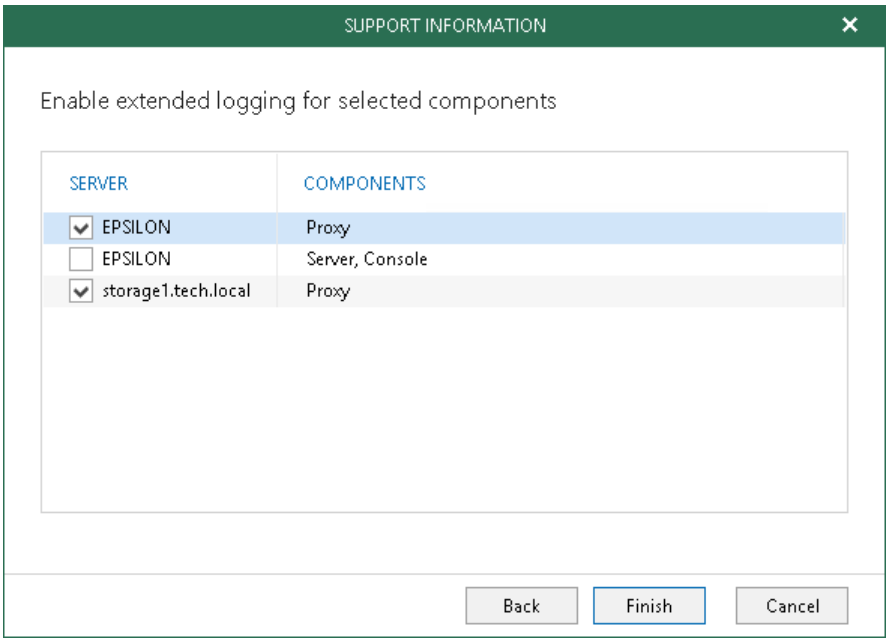
After enabling extended logging mode, you can go back to the application and perform required actions, then collect logs, as described in Log Files Export.

To configure extended logging mode, do the following:

1. Go to the main menu and click **Help and Support > Support Information**.
2. Select the **Configure extended logging** option.



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



Office 365 Backup as a Service

Continue with this section to learn more about configuring *Office 365 Backup as a Service* for service providers and their tenants.

For Service Providers

To configure *Office 365 Backup as a Service* for service providers, do the following:

1. Install Veeam Backup & Replication and Veeam Backup for Microsoft Office 365 version 3.0 on the same *Cloud Connect* server.

   For more information, see the Deployment section of this guide and the Installing Veeam Backup & Replication section of the Veeam Backup & Replication User Guide.

2. Install Veeam Backup & Replication and Veeam Backup for Microsoft Office 365 licenses.

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

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

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

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

5. Add new tenants, as described in the Registering Tenant Accounts section of the Veeam Cloud Connect Administrator Guide.

6. Configure your Veeam Backup for Microsoft Office 365 environment, as described in Configuring Veeam Backup for Microsoft Office 365.

A service provider can use Veeam Backup for 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:**
>
> Make sure to install Veeam Explorer for Microsoft Exchange, Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft OneDrive for Business that come as part of the Veeam Backup for Microsoft Office 365 3.0 distribution package.

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 Options

  To learn how to configure Veeam Backup for Microsoft Office 365 settings.

- Configuring Authentication Settings

  To learn how to allow tenants to perform self-restore procedures.

- Configuring Backup Proxy Servers

  To learn how to configure backup proxy servers.

- Configuring Backup Repositories

  To learn how to configure backup repositories.

- Microsoft Organizations Management

  To learn how to add tenants organizations to the Veeam Backup for Microsoft Office 365 scope.

- Data Backup

  To learn how to back up data of your tenants.

NOTE:

As a service provider, you must obtain Microsoft organization credentials of your tenants. The same credentials will be used by tenants to connect to the Veeam Backup for Microsoft Office 365 server of a service provider via Veeam Explorers for self-service recovery.

For Tenants

To configure *Office 365 Backup as a Service* for tenants, do the following:

1. Add a service provider in Veeam Backup & Replication, as described in the Connecting to Service Providers section of the Veeam Cloud Connect User Guide.
2. Add backups to the Veeam Explorer scope, as described in Exploring Backups in Veeam Explorers.

NOTE:

Mind the following:

- Make sure to install Veeam Explorer for Microsoft Exchange, Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft OneDrive for Business that come as part of the Veeam Backup for Microsoft Office 365 3.0 distribution package.
- By default, tenants are not able to restore anything without the service provider assistance. To be able to perform self-service recovery procedures, a service provider must configure authentication settings for tenants, as described in Configuring Authentication Settings.
- Tenants must provide their service providers with their Microsoft organization credentials so that service providers can connect to tenants organizations. Tenants can use the same credentials when adding a Veeam Backup for Microsoft Office 365 service provider server to the Veeam Explorers scope, as described in Working with Backups in Veeam Explorers.

Exploring Backups in Veeam Explorers

To explore backups located on the service provider side, add such backups in Veeam Explorers, as described in:

- Adding Organization Backups in Veeam Explorer for Microsoft Exchange
- Adding Organization Backups in Veeam Explorer for Microsoft SharePoint
- Adding Organization Backups in Veeam Explorer for Microsoft OneDrive for Business

NOTE:

Make sure to have access to the service provider server to be able to explore your backups. Access can be granted, as described in Configuring Authentication Settings.