Contents

CONTACTING VEEAM SOFTWARE ......................................................................................... 8
ABOUT VEEAM BACKUP FOR MICROSOFT 365 ..................................................................... 9
ABOUT THIS DOCUMENT ....................................................................................................... 10
PLANNING AND PREPARATION .......................................................................................... 11
   System Requirements ........................................................................................................ 12
   Used Ports ......................................................................................................................... 17
   Required Permissions ........................................................................................................ 22
      Veeam Backup Account Permissions ............................................................................. 23
      Azure AD Application Permissions ................................................................................. 28
      Amazon S3 Storage Permissions ..................................................................................... 37
      Azure Archive Storage Permissions ............................................................................... 40
      Permissions Changelog ............................................................................................... 41
   Considerations and Limitations ....................................................................................... 44
   Supported Azure Storage Account Types ......................................................................... 49
   Supported Amazon S3 Storage Classes ............................................................................ 50
LICENSING AND LICENSE TYPES ...................................................................................... 51
   Subscription License ......................................................................................................... 53
   Rental License .................................................................................................................. 54
      Managing Monthly Usage Report ................................................................................. 55
   Not For Resale License ...................................................................................................... 57
   Evaluation License ........................................................................................................... 58
   Integration with Veeam Service Provider Console ......................................................... 59
DEPLOYMENT .......................................................................................................................... 60
   Downloading Installation Package ................................................................................. 61
   Installing Veeam Backup for Microsoft 365 and Veeam Explorers ................................. 62
   Installing REST API on Separate Computer ................................................................... 66
   Installing Veeam Explorers for Tenants .......................................................................... 70
   Installing in Unattended Mode ....................................................................................... 74
   Deploying to Azure and AWS ......................................................................................... 77
   Updating Veeam Backup for Microsoft 365 .................................................................... 78
      Automatic Update .......................................................................................................... 79
      Checking for Updates .................................................................................................... 80
   Installing and Updating License ...................................................................................... 82
   Upgrading to Veeam Backup for Microsoft 365 6.0 ....................................................... 84
   Uninstalling Veeam Backup for Microsoft 365 ............................................................... 88
LAUNCHING VEEAM BACKUP FOR MICROSOFT 365 ....................................................... 89
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Interface</td>
<td></td>
</tr>
<tr>
<td>Current Session</td>
<td></td>
</tr>
<tr>
<td><strong>CONFIGURATION</strong></td>
<td></td>
</tr>
<tr>
<td>General Settings</td>
<td></td>
</tr>
<tr>
<td>Folder Exclusions</td>
<td>97</td>
</tr>
<tr>
<td>Session History</td>
<td>98</td>
</tr>
<tr>
<td>REST API Settings</td>
<td>99</td>
</tr>
<tr>
<td>Restore Portal Settings</td>
<td>101</td>
</tr>
<tr>
<td>Notification Settings</td>
<td>109</td>
</tr>
<tr>
<td>Security Settings</td>
<td></td>
</tr>
<tr>
<td>Authentication Settings</td>
<td>111</td>
</tr>
<tr>
<td>New Versions and Automatic Updates</td>
<td>114</td>
</tr>
<tr>
<td>Global Internet Proxy Server Settings</td>
<td>116</td>
</tr>
<tr>
<td>Configuring REST API and Restore Portal on Separate Computer</td>
<td>118</td>
</tr>
<tr>
<td>SSL Certificates Overview</td>
<td>121</td>
</tr>
<tr>
<td>SSL Certificate Usage Scenarios</td>
<td>122</td>
</tr>
<tr>
<td>Installing SSL Certificates</td>
<td>124</td>
</tr>
<tr>
<td>Backup Infrastructure</td>
<td>127</td>
</tr>
<tr>
<td>Backup Proxy Servers</td>
<td>128</td>
</tr>
<tr>
<td>Backup Repositories</td>
<td>142</td>
</tr>
<tr>
<td>Object Storage Repositories</td>
<td>161</td>
</tr>
<tr>
<td>Credentials</td>
<td>206</td>
</tr>
<tr>
<td>Managing Cloud Credentials</td>
<td>207</td>
</tr>
<tr>
<td>Managing Encryption Passwords</td>
<td>217</td>
</tr>
<tr>
<td><strong>ORGANIZATION MANAGEMENT</strong></td>
<td>219</td>
</tr>
<tr>
<td>Microsoft 365 Organizations</td>
<td></td>
</tr>
<tr>
<td>Adding Organizations with Modern App-Only Authentication</td>
<td>221</td>
</tr>
<tr>
<td>Adding Organizations with Modern Authentication and Legacy Protocols</td>
<td>234</td>
</tr>
<tr>
<td>Adding Organizations with Basic Authentication</td>
<td>243</td>
</tr>
<tr>
<td>On-Premises Microsoft Organizations</td>
<td></td>
</tr>
<tr>
<td>Step 1. Launch Add Organization Wizard</td>
<td>251</td>
</tr>
<tr>
<td>Step 2. Select Organization Deployment Type</td>
<td>252</td>
</tr>
<tr>
<td>Step 3. Specify Microsoft Exchange Connection Settings</td>
<td>253</td>
</tr>
<tr>
<td>Step 4. Specify Microsoft SharePoint Connection Settings</td>
<td>255</td>
</tr>
<tr>
<td>Step 5. Finish Working with Wizard</td>
<td>257</td>
</tr>
<tr>
<td>Hybrid Organizations</td>
<td></td>
</tr>
<tr>
<td>Backup of TeamsMessagesData Folder</td>
<td>258</td>
</tr>
<tr>
<td>Backup of Team Chats Using Teams Export APIs</td>
<td>259</td>
</tr>
<tr>
<td>Backup Accounts</td>
<td>261</td>
</tr>
<tr>
<td></td>
<td>263</td>
</tr>
</tbody>
</table>
Extending Availability of Retrieved Data ................................................................. 339

DATA RESTORE ........................................................................................................ 340
  Exploring Backup Jobs ....................................................................................... 341
  Exploring Single Organization ......................................................................... 342
  Exploring All Organizations ............................................................................ 344
  Exploring Point In Time .................................................................................. 346
  Exploring Retrieved Data ................................................................................ 347

BACKUP, BACKUP COPY, RETRIEVE AND RESTORE STATISTICS .................... 348
  Viewing Backup and Backup Copy Session Metrics .................................. 349
  Viewing Retrieve Session Metrics .................................................................. 351
  Viewing Restore Session Metrics .................................................................. 352

REPORTING ................................................................................................................ 353
  Creating Mailbox Protection Reports ............................................................ 354
  Creating Storage Consumption Reports ....................................................... 356
  Creating License Overview Reports .............................................................. 358
  Creating User Protection Reports .................................................................. 360

MANAGING LOG FILES ......................................................................................... 362
  Collecting Log Files ......................................................................................... 364
  Enabling Extended Logging Mode .................................................................... 366

BACKUP AS SERVICE FOR MICROSOFT 365 ..................................................... 368
  For Service Providers ....................................................................................... 369
    Configuring Veeam Backup for Microsoft 365 ............................................ 370
  For Tenants ....................................................................................................... 371
    Exploring Backups in Veeam Explorers ...................................................... 372

DATA RESTORE USING RESTORE PORTAL .................................................. 373
  Restore Portal Usage Scenarios ....................................................................... 374
  How Restore Portal Works .............................................................................. 375
  Considerations and Limitations ....................................................................... 376
  Configuration ..................................................................................................... 377
    Adding Restore Operator Role ...................................................................... 379
    Editing Restore Operator Role Settings ....................................................... 389
    Removing Restore Operator Role .................................................................. 390
  Launching Restore Portal .................................................................................. 391
    User Interface ................................................................................................. 393
    Managing Notifications .................................................................................. 397
    Changing Restore Operator Scope ............................................................... 398
  Performing Restore ............................................................................................ 399
    Using Restore List .......................................................................................... 401
    Exchange Restore........................................................................................... 403
SharePoint Restore............................................................................................................. 405
OneDrive Restore ........................................................................................................... 407

DATA RESTORE USING VEEAM EXPLORERS ..................................................................... 408
Contacting Veeam Software

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

Customer Support

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

Company Contacts

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

Online Support

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

- Full documentation set: veeam.com/documentation-guides-datasheets.html
- Veeam R&D Forums: forums.veeam.com
About Veeam Backup for Microsoft 365

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

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

The document applies to Veeam Backup for Microsoft 365 version 6.0 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 365 and on-premises Microsoft organizations users.
Planning and Preparation

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

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

Supported Microsoft Exchange Organizations

The following table lists supported Microsoft Exchange versions:

<table>
<thead>
<tr>
<th>Microsoft Exchange</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft 365 Exchange Online</td>
<td>Microsoft 365 and Office 365 service families, standalone services and plans for Business, Education, and Government* hosted by Microsoft are supported. For more information about system requirements and limitations for Microsoft 365, see <a href="#">this Microsoft article</a>.</td>
</tr>
<tr>
<td>Microsoft Exchange Server 2019 (compatibility support), 2016 or 2013 (on-premises)</td>
<td>For more information about limitations for backup and restore of mail items, see <a href="#">Considerations and Limitations</a>.</td>
</tr>
</tbody>
</table>

*Government support is experimental.

**NOTE**

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

Supported Microsoft SharePoint Organizations

The following table lists supported Microsoft SharePoint versions:

<table>
<thead>
<tr>
<th>Microsoft SharePoint</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft 365 SharePoint Online</td>
<td>Microsoft 365 and Office 365 service families, standalone services and plans for Business, Education, and Government* hosted by Microsoft are supported. For more information about system requirements and limitations for Microsoft 365, see <a href="#">this Microsoft article</a>.</td>
</tr>
</tbody>
</table>
| Microsoft SharePoint Server 2019, 2016 | For more information about hardware and software requirements for Microsoft SharePoint Server 2019/2016, see:  
  - Hardware and software requirements for SharePoint Server 2016  
  - Hardware and software requirements for SharePoint Server 2019 |
Veeam Backup for Microsoft 365 Server

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

<table>
<thead>
<tr>
<th>Specification</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware</strong></td>
<td>The following hardware is required:</td>
</tr>
<tr>
<td></td>
<td>• <strong>CPU:</strong> any modern multi-core x64 processor, 8 cores minimum.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Memory:</strong> 16 GB RAM minimum. Additional RAM and CPU resources improve backup, restore and search performance.</td>
</tr>
<tr>
<td></td>
<td>Host with Veeam Backup for Microsoft 365 also requires a minimum size of 16 GB of RAM for VMs with dynamic memory allocation.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disk Space:</strong> 500 MB for product installation and additional free space for the configuration database (depending on the number of organizations, jobs and sessions) and product logs.</td>
</tr>
<tr>
<td><strong>OS</strong></td>
<td>Only 64-bit version of the following operating systems are supported:</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows Server 2022</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows Server 2019</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows Server 2016</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows Server 2012 R2</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows 10 21H2 and earlier</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows 11</td>
</tr>
</tbody>
</table>

Veeam Backup for Microsoft 365 server can be deployed on the following core editions:

• Microsoft Windows Server 2022
• Microsoft Windows Server 2019 LTSC, 1809
• Microsoft Windows Server 2016 LTSC, 1709
• Microsoft Windows Server 2012 R2
• Microsoft Windows Server 2012

*Government support is experimental.
The following software is required:

- Microsoft .NET Framework 4.7.2 or later.
- Windows C Runtime and Update (UCRT) in Windows. For more information, see this Microsoft article.
- To use PowerShell cmdlets for backup and restore, Windows PowerShell 5.1 or later is required.
- For more information about Microsoft 365 system requirements and limitations, see this Microsoft article.

**IMPORTANT**

Consider the following:

- When you install Veeam Explorer for Microsoft Exchange, Veeam Explorer for Microsoft SharePoint (including Veeam Explorer for Microsoft OneDrive for Business), Veeam Explorer for Microsoft Teams and Veeam Backup for Microsoft 365 on different servers, the OS version on computers with Veeam Explorers must be the same or later than the OS version on a computer with Veeam Backup for Microsoft 365.
- Veeam Explorers can only be installed on a machine hosting Veeam Backup for Microsoft 365 6.0 or the Veeam Backup for Microsoft 365 Console component. You can also use a machine with Veeam Backup & Replication 10 or later that is deployed either along with any of these components, or as an independent solution.
- The account you want to use for launching Veeam Backup for Microsoft 365 must be a member of the Local Administrator group on a computer with Veeam Backup for Microsoft 365.

**Host with REST API**

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

<table>
<thead>
<tr>
<th>Specification</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Software</strong></td>
<td>The following software is required:</td>
</tr>
<tr>
<td></td>
<td>- Microsoft .NET Framework 4.7.2 or later.</td>
</tr>
<tr>
<td></td>
<td>- Windows C Runtime and Update (UCRT) in Windows. For more information, see this Microsoft article.</td>
</tr>
<tr>
<td></td>
<td>- To use PowerShell cmdlets for backup and restore, Windows PowerShell 5.1 or later is required.</td>
</tr>
<tr>
<td></td>
<td>- For more information about Microsoft 365 system requirements and limitations, see this Microsoft article.</td>
</tr>
<tr>
<td><strong>Hardware</strong></td>
<td>The following hardware is required:</td>
</tr>
<tr>
<td></td>
<td>- <strong>CPU</strong>: any modern multi-core x64 processor, 8 cores minimum.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Memory</strong>: 16 GB RAM minimum. Additional RAM and CPU resources improve backup, restore and search performance.</td>
</tr>
<tr>
<td></td>
<td>Veeam Backup for Microsoft 365 REST server also requires a minimum size of 16 GB of RAM for VMs with dynamic memory allocation.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Disk Space</strong>: 500 MB for product installation and additional free space for the configuration database (depending on the number of organizations, jobs and sessions) and product logs.</td>
</tr>
</tbody>
</table>
### OS

Only 64-bit version of the following operating systems are supported:
- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows 10 21H2 and earlier
- Microsoft Windows 11

Veeam Backup for Microsoft 365 server can be deployed on the following core editions:
- Microsoft Windows Server 2022
- Microsoft Windows Server 2019 LTSC, 1809
- Microsoft Windows Server 2016 LTSC, 1709
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012

### Software

The following software is required:
- Microsoft .NET Framework 4.7.2 or later.
- Windows C Runtime and Update (UCRT) in Windows. For more information, see [this Microsoft article](#).

### Backup Proxy Server

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

<table>
<thead>
<tr>
<th>Specification</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td>The following hardware is required:</td>
</tr>
<tr>
<td></td>
<td>• <strong>CPU</strong>: any modern multi-core x64 processor, 8 cores minimum.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Memory</strong>: 16 GB RAM minimum. Additional RAM and CPU resources improve backup, restore and search performance.</td>
</tr>
<tr>
<td></td>
<td>Veeam Backup for Microsoft 365 backup proxy server also requires a minimum size of 16 GB of RAM for VMs with dynamic memory allocation.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disk space</strong>: 300 MB for backup proxy installation and additional free space for configuration database (depending on the number of organizations, jobs and sessions) and backup proxy logs.</td>
</tr>
<tr>
<td>Specification</td>
<td>Requirement</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| OS            | Only 64-bit version of the following operating systems are supported:  
|               | - Microsoft Windows Server 2022  
|               | - Microsoft Windows Server 2019  
|               | - Microsoft Windows Server 2016  
|               | - Microsoft Windows Server 2012 R2  
|               | - Microsoft Windows Server 2012  
|               | - Microsoft Windows 10 21H2 and earlier  
|               | - Microsoft Windows 11  
|               | Proxy servers can be deployed to the following core editions:  
|               | - Microsoft Windows Server 2022  
|               | - Microsoft Windows Server 2019 LTSC, 1809  
|               | - Microsoft Windows Server 2016 LTSC, 1709  
|               | - Microsoft Windows Server 2012 R2  
|               | - Microsoft Windows Server 2012  
| Other         | The following components are required:  
|               | - Microsoft .NET Framework 4.7.2 or later.  
|               | - Windows C Runtime and Update (UCRT) in Windows. For more information, see this Microsoft article.  
|               | For a machine used as a workgroup backup proxy, the following settings are required:  
|               | - The Remote Registry service must run on the target machine. The service startup type must be set to Automatic.  
|               | - Backup proxy server ports must be opened in Windows Firewall. |
## Used Ports

The following table lists required ports that must be opened for inbound/outbound requests in Veeam Backup for Microsoft 365. For more information about Microsoft 365 URLs and IP address ranges, see [this Microsoft article](#).

**NOTE**

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

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Protocol</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veeam Backup for Microsoft 365 Server</td>
<td>Microsoft Exchange Online</td>
<td>TCP</td>
<td>443</td>
<td>Required to connect to Microsoft Exchange Online organizations. The endpoints are: outlook.office365.com and autodiscover-s.outlook.com.</td>
</tr>
<tr>
<td>Microsoft SharePoint Online</td>
<td>TCP</td>
<td>443</td>
<td>Required to connect to Microsoft SharePoint Online organizations. The endpoints are: &lt;tenant&gt;.sharepoint.com, &lt;tenant&gt;-my.sharepoint.com and &lt;tenant&gt;-admin.sharepoint.com.</td>
<td></td>
</tr>
<tr>
<td>On-premises Microsoft SharePoint Server</td>
<td>HTTP (HTTPS)</td>
<td>5985 (5986 — used by default)</td>
<td>Required to connect to on-premises Microsoft SharePoint organizations through the WinRM port.</td>
<td></td>
</tr>
<tr>
<td>On-premises Microsoft Exchange Server</td>
<td>TCP</td>
<td>80 or 443</td>
<td>Required to connect to on-premises Microsoft Exchange organizations.</td>
<td></td>
</tr>
<tr>
<td>Backup Proxy Server</td>
<td>TCP</td>
<td>9193 (used by default)</td>
<td>Required to manage inbound/outbound traffic when interacting with the Veeam Backup for Microsoft 365 server. Make sure to open this port on a backup proxy server.</td>
<td></td>
</tr>
<tr>
<td>From</td>
<td>To</td>
<td>Protocol</td>
<td>Port</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------</td>
<td>----------</td>
<td>------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TCP</td>
<td>445</td>
<td></td>
<td></td>
<td>This port is used to:&lt;br&gt;• Install and manage the Veeam.Archiver.Proxy service on a target proxy machine.&lt;br&gt;• Perform RPC requests.</td>
</tr>
<tr>
<td>Veeam Auto-update Server</td>
<td>HTTPS</td>
<td>443</td>
<td></td>
<td>Required to access the auto-update server and licensing server. For more information, see Updating Veeam Backup for Microsoft 365 and Installing and Updating License.&lt;br&gt;The endpoints are: <a href="https://vbo.butler.veeam.com">https://vbo.butler.veeam.com</a> and download2.veeam.com.</td>
</tr>
<tr>
<td>TCP</td>
<td>443</td>
<td></td>
<td></td>
<td>Required to work with any of the object storage repositories.</td>
</tr>
<tr>
<td>S3 Compatible object storage</td>
<td></td>
<td>TCP</td>
<td>443</td>
<td></td>
</tr>
<tr>
<td>Amazon S3 object storage / IBM Cloud Object Storage</td>
<td>TCP</td>
<td>443</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Azure Blob storage</td>
<td></td>
<td>TCP</td>
<td>443</td>
<td>Required to connect to Microsoft 365.&lt;br&gt;The endpoints are: graph.microsoft.com, graph.windows.net and login.microsoftonline.com.</td>
</tr>
<tr>
<td>Microsoft 365</td>
<td></td>
<td>TCP</td>
<td>443</td>
<td>Required to send email notifications using an SMTP server.&lt;br&gt;The endpoint is smtp.office365.com.</td>
</tr>
<tr>
<td>From</td>
<td>To</td>
<td>Protocol</td>
<td>Port</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>----</td>
<td>----------</td>
<td>------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Veeam Backup for Microsoft 365 components | Veeam Backup for Microsoft 365 Server | TCP | 9191 | Required to manage inbound/outbound traffic when interacting with the following components:  
- REST API  
- PowerShell  
- Veeam.Archiver.Shell (UI)  
- [Optionally] A remote management server (if any)  
Make sure to open port on the Veeam Backup for Microsoft 365 server. |
| Veeam Explorer for Microsoft Exchange | Veeam Backup for Microsoft 365 Server | TCP | 9194 | Required to manage inbound/outbound traffic when interacting with Veeam Explorer for Microsoft Exchange.  
Make sure to open this port on the Veeam Backup for Microsoft 365 server. |
| Microsoft Exchange Online | Veeam Backup for Microsoft 365 Server | TCP | 9194 | Required to restore Microsoft Exchange data. |
| SMTP Server | Veeam Backup for Microsoft 365 Server | TCP | 25 or 465 or 587 | Required to send email notifications using an SMTP server.  
The endpoint is smtp.office365.com. |
| Veeam Explorer for Microsoft SharePoint (including Veeam Explorer for Microsoft OneDrive for Business) | Veeam Backup for Microsoft 365 Server | TCP | 9194 | Required to manage inbound/outbound traffic when interacting with Veeam Explorer for Microsoft SharePoint.  
Make sure to open this port on the Veeam Backup for Microsoft 365 server. |
<p>| Microsoft SharePoint Online | Veeam Backup for Microsoft 365 Server | TCP | 9194 | Required to restore Microsoft SharePoint data. |</p>
<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Protocol</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Server</td>
<td>Veeam Backup for Microsoft 365 Server</td>
<td>TCP</td>
<td>25 or 465 or 587</td>
<td>Required to send email notifications using an SMTP server. The endpoint is smtp.office365.com.</td>
</tr>
<tr>
<td>Veeam Explorer for Microsoft Teams</td>
<td>Veeam Backup for Microsoft 365 Server</td>
<td>TCP</td>
<td>9194</td>
<td>Required to manage inbound/outbound traffic when interacting with Veeam Explorer for Microsoft Teams. Make sure to open this port on the Veeam Backup for Microsoft 365 server.</td>
</tr>
<tr>
<td>Microsoft Teams Online</td>
<td>TCP</td>
<td>443</td>
<td></td>
<td>Required to restore Microsoft Teams data. The endpoint is developer.microsoft.com.</td>
</tr>
<tr>
<td>SMTP Server</td>
<td>TCP</td>
<td>25 or 465 or 587</td>
<td>Required to send email notifications using an SMTP server. The endpoint is smtp.office365.com.</td>
<td></td>
</tr>
<tr>
<td>Backup Proxy Server</td>
<td>Veeam Backup for Microsoft 365 Server</td>
<td>TCP</td>
<td>9191</td>
<td>Required to manage inbound/outbound traffic when interacting with backup proxy servers. Make sure to open this port on the Veeam Backup for Microsoft 365 server. You can also change this port. For more information, see Editing Backup Proxy Server.</td>
</tr>
<tr>
<td>Microsoft Exchange Online</td>
<td>TCP</td>
<td>443</td>
<td></td>
<td>Required to connect to Microsoft Exchange Online through EWS (Exchange Web Services). The endpoints are: outlook.office365.com and autodiscover-s.outlook.com.</td>
</tr>
<tr>
<td>From</td>
<td>To</td>
<td>Protocol</td>
<td>Port</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------</td>
<td>----------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>On-premises Microsoft SharePoint</td>
<td>HTTP (HTTPS)</td>
<td>5985 (5986)</td>
<td>Required to connect to on-premises Microsoft SharePoint organizations through the WinRM port.</td>
<td></td>
</tr>
<tr>
<td>On-premises Microsoft Exchange Server</td>
<td>TCP</td>
<td>80 or 443</td>
<td>Required to connect to on-premises Microsoft Exchange organizations.</td>
<td></td>
</tr>
<tr>
<td>S3 Compatible object storage</td>
<td>TCP</td>
<td>443</td>
<td>Required to work with any of the object storage repositories.</td>
<td></td>
</tr>
<tr>
<td>Amazon S3 object storage / IBM Cloud Object Storage</td>
<td>TCP</td>
<td>443</td>
<td>The endpoint is &lt;account&gt;.blob.core.windows.net.</td>
<td></td>
</tr>
<tr>
<td>Azure Blob storage</td>
<td>TCP</td>
<td>443</td>
<td>Required to connect to Microsoft 365.</td>
<td></td>
</tr>
<tr>
<td>Microsoft 365</td>
<td>TCP</td>
<td>443</td>
<td>The endpoints are: graph.microsoft.com, graph.windows.net and login.microsoftonline.com.</td>
<td></td>
</tr>
<tr>
<td>SMTP Server</td>
<td>TCP</td>
<td>25 or 465 or 587</td>
<td>Required to send email notifications using an SMTP server.</td>
<td></td>
</tr>
<tr>
<td>Cloud Gateway</td>
<td>TCP</td>
<td>9194</td>
<td>Required to maintain inbound/outbound traffic.</td>
<td></td>
</tr>
<tr>
<td>Web Browser</td>
<td>Veeam Backup for Microsoft 365 REST API</td>
<td>HTTPS</td>
<td>4443 (used by default)</td>
<td>Required to connect to Restore Portal. You can also use different port.</td>
</tr>
<tr>
<td>Host with REST API</td>
<td>Veeam Backup for Microsoft 365 Server</td>
<td>TCP</td>
<td>9194</td>
<td>Required for Restore Portal to work.</td>
</tr>
</tbody>
</table>
Required Permissions

Microsoft Organizations

To protect your data using Veeam Backup for Microsoft 365, you use Veeam Backup account and Azure AD application. Depending on configuration of Microsoft 365 organizations and the restrictions on using legacy authentication protocols, you can add organizations using either modern app-only authentication, or modern authentication method with legacy protocols allowed, or basic authentication.

When you add Microsoft 365 organization using the modern app-only authentication method, you use only Azure AD application to establish and maintain connection between Veeam Backup for Microsoft 365 and Microsoft 365 organizations and perform a backup and restore from/to such organizations.

When you add Microsoft 365 organization using modern authentication with legacy protocols allowed, you use both Veeam Backup account and Azure AD application to establish and maintain connection between Veeam Backup for Microsoft 365 and Microsoft 365 organizations and perform a backup and restore from/to such organizations. You use MFA-enabled Microsoft 365 user account as Veeam Backup account.

When you add Microsoft 365 organization using basic authentication or an on-premises Microsoft organization, you use Veeam Backup account to establish and maintain connection between Veeam Backup for Microsoft 365 and such organizations and perform a backup and restore.

Depending on authentication methods you use, you must grant permissions to Veeam Backup account or Azure AD application, or both accounts.

Restore Portal

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

Azure Archiver Appliance

If you want to use the Azure archiver appliance when Veeam Backup for Microsoft 365 copies backed-up data from Azure Blob storage to Azure Archive storage, you must assign the required roles to a user account that you use to create Azure AD application for the Microsoft Azure service account. For more information, see Permissions for Azure Archiver Appliance.

Amazon S3 Storage

If you store Microsoft 365 and on-premises Microsoft organization backups in Amazon S3 object storage, you must grant permissions to a user account that you use to access Amazon buckets and folders. For more information, see Amazon S3 Storage Permissions.

Azure Archive Storage

If you create an instance of Microsoft 365 and on-premises Microsoft organization backups in Azure Blob Storage Archive access tier, you must grant permissions to a user account that you use to access Azure archive storage. For more information, see Azure Archive Storage Permissions.
Veeam Backup Account Permissions

When you add Microsoft 365 organization using either modern authentication method with legacy protocols allowed or basic authentication, you use Veeam Backup account. Also you use Veeam Backup account for on-premises Microsoft Exchange and on-premises Microsoft SharePoint organizations.

To provide Veeam Backup for Microsoft 365 with the ability to work with Microsoft Exchange organizations, Microsoft SharePoint and OneDrive for Business organizations, and protect Microsoft Teams data, you must grant the following permissions to the Veeam Backup account:

- **Microsoft Exchange Organizations**
  Roles and permissions required to work with Microsoft Exchange organizations.

- **Microsoft SharePoint and OneDrive for Business**
  Roles and permissions required to work with Microsoft SharePoint and OneDrive for Business organizations.

- **Microsoft Teams**
  Roles and permissions required to protect Microsoft Teams data.

Microsoft Exchange Organizations

The following table lists the required roles and permissions that must be assigned to the Veeam Backup account that you want to use for working with Microsoft Exchange organizations. The table lists roles required by Veeam Backup for Microsoft 365 when you add Microsoft 365 organizations using modern authentication with legacy protocols allowed or basic authentication and on-premises Microsoft organizations.

Consider the following:

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

**NOTE**

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

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role Management</td>
<td>Required to grant the ApplicationImpersonation role.</td>
</tr>
<tr>
<td>ApplicationImpersonation</td>
<td>Required to back up Exchange data.</td>
</tr>
<tr>
<td>Organization Configuration</td>
<td>Required to manage role assignments.</td>
</tr>
</tbody>
</table>
### Role Description Table

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View-Only Configuration</td>
<td>Required to obtain necessary configuration parameters.</td>
</tr>
<tr>
<td>View-Only Recipients</td>
<td>Required to view mailbox recipients.</td>
</tr>
<tr>
<td>Mailbox Search or Mail</td>
<td>Required to back up groups.</td>
</tr>
<tr>
<td>Recipients</td>
<td></td>
</tr>
<tr>
<td>Owner</td>
<td>Required to back up/restore public folders.</td>
</tr>
</tbody>
</table>

### Granting ApplicationImpersonation Role in PowerShell

#### For On-Premises Microsoft Exchange Organizations

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

1. Connect to the Exchange server. For more information, see this Microsoft article.
2. Run the following cmdlet to grant the role.

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

#### For Microsoft 365 Exchange Organizations

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

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

   ```powershell
   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).

```powershell
Get-ManagementRoleAssignment -Role "ApplicationImpersonation"
```
To remove the role, use the following cmdlet (for both on-premises and Online organizations).

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

Creating and Configuring New Authentication Policy for Exchange Online Organizations

To protect your Microsoft 365 organization data properly when you add an organization using either modern authentication with legacy protocols allowed or basic authentication, you need to create a new authentication policy with the `AllowBasicAuthPowershell` and `AllowBasicAuthWebService` parameters enabled for the Veeam Backup account. To do this, use the following code snippet.

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

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

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

Microsoft SharePoint and OneDrive for Business

The following tables list the required roles and permissions that must be assigned to the Veeam Backup account that you want to use for working with Microsoft SharePoint and OneDrive for Business organizations. The section lists roles required by Veeam Backup for Microsoft 365 when you add Microsoft 365 organizations using modern authentication with legacy protocols allowed or basic authentication and on-premises Microsoft organizations.

Consider the following:

- To add Microsoft SharePoint Online organizations, make sure that the `LegacyAuthProtocolsEnabled` setting is enabled.
  
  To enable this setting, use the following cmdlet.

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

For more information about the `Set-SPOTenant` cmdlet, see this Microsoft article.

- The account you are using to add on-premises Microsoft SharePoint and Microsoft SharePoint Online organizations must be a member of these organizations.
NOTE
For more information about permissions required to restore Microsoft SharePoint data from backups created by Veeam Backup for Microsoft 365, see Required Permissions for Veeam Explorer for Microsoft SharePoint.

On-Premises Microsoft SharePoint Organizations

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

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
<th>Misc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Collection Administrator</td>
<td>Required to back up Microsoft SharePoint Sites.</td>
<td>The account must be a member of the Farm Administrator group.</td>
</tr>
</tbody>
</table>

Microsoft SharePoint Online Organizations

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

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
<th>Misc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SharePoint Admin</td>
<td>Required to back up Microsoft SharePoint Sites.</td>
<td>You can assign the Global Admin role that overrides these roles.</td>
</tr>
<tr>
<td>View-only Configuration</td>
<td>Required to get a list of available groups and users.</td>
<td></td>
</tr>
<tr>
<td>View-Only Recipients</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Granting SharePoint Administrator Role in PowerShell

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

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

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

The MSOL module can be downloaded from this Microsoft page.
Microsoft Teams

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

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

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

**NOTE**

Consider the following:

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

Veeam Backup for Microsoft 365 requires that you grant permissions to Azure AD applications to back up and restore data from/to your Microsoft 365 organizations. Azure AD applications must have different permissions in organizations with modern app-only authentication and organizations with modern authentication and legacy protocols. For more information, see the following sections:

- Permissions for Modern App-Only Authentication
- Permissions for Modern Authentication and Legacy Protocols

If you allow users to perform self-service restore using Restore Portal, they will authenticate to the portal with their Microsoft 365 user account credentials. Veeam Backup for Microsoft 365 requires Azure AD application to be configured and granted permissions to ensure such authentication. For more information, see Permissions for Authentication to Restore Portal.

If you want to use the Azure archiver appliance when Veeam Backup for Microsoft 365 copies backed-up data from Azure Blob storage to Azure Archive storage, you must assign the required roles to a user account that you use to create Azure AD application for the Microsoft Azure service account. For more information, see Permissions for Azure Archiver Appliance.

For more information about permissions in Azure, see this Microsoft article.

Permissions for Modern App-Only Authentication

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

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

- Backup
- Restore Using Device Code Flow
- Restore Using Application Certificate

Make sure that you assign the required roles to the user account that the Azure AD application will use to log in to Microsoft 365.

For more information on how to check permissions for Office 365 Exchange Online API, see Checking Permissions for Office 365 Exchange Online API.

For more information on how to configure Azure AD application settings in Microsoft Azure to perform data restore, see Configuring Azure AD Application Settings.

For more information about permissions for Azure AD applications that you add as backup applications, see Backup Application Permissions.
Required User Account Roles for Azure AD Applications

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

- **Global Administrator** — required for adding organizations with modern app-only authentication, creating backup applications, registering Azure AD application for Restore Portal and creating Azure AD application for the Microsoft Azure service account.

- **ApplicationImpersonation** and **Global Administrator** or **Exchange Administrator** — required for data restore with Veeam Explorer for Microsoft Exchange.

- **Global Administrator** or **SharePoint Administrator** — required for data restore with Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft OneDrive for Business.

- **Global Administrator** or **Teams Administrator** — required for data restore with Veeam Explorer for Microsoft Teams.

- **Global Administrator** — required for establishing a connection to a service provider in the **Backup as Service for Microsoft 365** scenario.

Permissions for Backup

All listed permissions are of the **Application** type.

<table>
<thead>
<tr>
<th>API</th>
<th>Permission name</th>
<th>Exchange Online</th>
<th>SharePoint Online and OneDrive for Business</th>
<th>Microsoft Teams</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Microsoft Graph</strong></td>
<td>Directory.Read.All</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>Querying Azure AD for organization properties, the list of users and groups and their properties.</td>
</tr>
<tr>
<td></td>
<td>Group.Read.All</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>Querying Azure AD for the list of groups and group sites.</td>
</tr>
<tr>
<td></td>
<td>Sites.Read.All</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>Querying Azure AD for the list of sites and getting download URLs for files and their versions.</td>
</tr>
<tr>
<td></td>
<td>TeamSettings.ReadWrite.All</td>
<td></td>
<td></td>
<td>✔</td>
<td>Accessing archived teams.</td>
</tr>
<tr>
<td>API</td>
<td>Permission name</td>
<td>Exchange Online</td>
<td>SharePoint Online and OneDrive for Business</td>
<td>Microsoft Teams</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------------------------------</td>
<td>-----------------</td>
<td>---------------------------------------------</td>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>ChannelMessage.Read.All</td>
<td></td>
<td></td>
<td>✔</td>
<td>Accessing all Teams public channel messages.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> This permission is only required if you want to back up team chats using Teams Export APIs. For more information, see Organization Object Types.</td>
</tr>
<tr>
<td>Office 365 Exchange Online</td>
<td>full_access_as_app</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>Reading mailboxes content.</td>
</tr>
<tr>
<td>SharePoint</td>
<td>Sites.FullControl.All</td>
<td></td>
<td></td>
<td>✔</td>
<td>Reading SharePoint sites and OneDrive accounts content.</td>
</tr>
<tr>
<td></td>
<td>User.Read.All</td>
<td></td>
<td></td>
<td>✔</td>
<td>Reading OneDrive accounts (getting site IDs).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> This permission is not used to back up Microsoft Teams data, but you must grant it along with SharePoint Online and OneDrive for Business permission to add Microsoft 365 organization successfully.</td>
</tr>
</tbody>
</table>

¹You can check permissions for Office 365 Exchange Online API. For more information, see Checking Permissions for Office 365 Exchange Online API.
Permissions for Restore

**NOTE**
To restore data using Azure AD application, make sure that you configure the Azure AD application settings. For more information, see Configuring Azure AD Application Settings.

### Restore Using Device Code Flow

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

<table>
<thead>
<tr>
<th>API</th>
<th>Permission name</th>
<th>Exchange Online</th>
<th>SharePoint Online and OneDrive for Business</th>
<th>Microsoft Teams</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Graph</td>
<td>Directory.Read.All</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>Querying Azure AD for organization properties, the list of users and groups and their properties.</td>
</tr>
<tr>
<td></td>
<td>Group.ReadWrite.All</td>
<td></td>
<td></td>
<td>✔</td>
<td>Recreating in Azure AD an associated group in case of teams restore.</td>
</tr>
<tr>
<td></td>
<td>Sites.Read.All</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>Accessing sites of the applications that are installed from the SharePoint store.</td>
</tr>
<tr>
<td></td>
<td>Directory.ReadWrite.All</td>
<td></td>
<td></td>
<td>✔</td>
<td>Setting the preferred data location when creating a new M365 group for a multi-geo tenant in case of teams restore.</td>
</tr>
<tr>
<td></td>
<td>offline_access</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>Obtaining a refresh token from Azure AD.</td>
</tr>
<tr>
<td>Office 365 Exchange Online</td>
<td>EWS.AccessAsUser.All</td>
<td>✔</td>
<td></td>
<td></td>
<td>Accessing mailboxes as the signed-in user (impersonation) through EWS.</td>
</tr>
<tr>
<td>API</td>
<td>Permission name</td>
<td>Exchange Online</td>
<td>SharePoint Online and OneDrive for Business</td>
<td>Microsoft Teams</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------------</td>
<td>-----------------</td>
<td>---------------------------------------------</td>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>full_access_as_user</td>
<td></td>
<td></td>
<td></td>
<td>Reading the current state and restoring mailboxes content.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✔</td>
<td></td>
<td></td>
<td>This permission is only required when you add an organization in the Germany region.</td>
</tr>
<tr>
<td>SharePoint</td>
<td>AllSites.FullControl</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>Reading the current state and restoring SharePoint sites and OneDrive accounts content.</td>
</tr>
<tr>
<td></td>
<td>User.Read.All</td>
<td></td>
<td></td>
<td>✔</td>
<td>Resolving OneDrive accounts (getting site IDs).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Note: This permission is not required to restore SharePoint Online data.</td>
</tr>
</tbody>
</table>

You can check permissions for Office 365 Exchange Online API. For more information, see Checking Permissions for Office 365 Exchange Online API.

### Restore Using Application Certificate

All listed permissions are of the Application type and required for data restore using Restore Portal and through REST API and PowerShell.

<table>
<thead>
<tr>
<th>API</th>
<th>Permission name</th>
<th>Exchange Online</th>
<th>SharePoint Online and OneDrive for Business</th>
<th>Microsoft Teams</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Graph</td>
<td>Directory.Read.All</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>Querying Azure AD for organization properties, the list of users and groups and their properties.</td>
</tr>
<tr>
<td>API</td>
<td>Permission name</td>
<td>Exchange Online</td>
<td>SharePoint Online and OneDrive for Business</td>
<td>Microsoft Teams</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------------------</td>
<td>-----------------</td>
<td>---------------------------------------------</td>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Group.ReadWrite.All</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>Recreating in Azure AD an associated group in case of a deleted team site restore. <strong>Note:</strong> This permission is only required for restore of SharePoint site data through REST API and PowerShell.</td>
</tr>
<tr>
<td></td>
<td>Sites.Read.All</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>Accessing sites of the applications that are installed from the SharePoint store.</td>
</tr>
<tr>
<td>Office 365 Exchange Online</td>
<td>full_access_as_app</td>
<td>✔</td>
<td></td>
<td></td>
<td>Reading the current state and restoring mailboxes content.</td>
</tr>
<tr>
<td>SharePoint</td>
<td>Sites.FullControl.All</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>Reading the current state and restoring SharePoint sites and OneDrive accounts content.</td>
</tr>
<tr>
<td></td>
<td>User.Read.All</td>
<td></td>
<td></td>
<td>✔</td>
<td>Resolving OneDrive accounts (getting site IDs). <strong>Note:</strong> This permission is not required to restore SharePoint Online data.</td>
</tr>
</tbody>
</table>

1You can check permissions for Office 365 Exchange Online API. For more information, see Checking Permissions for Office 365 Exchange Online API.

Checking Permissions for Office 365 Exchange Online API

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

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

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

1. Sign in to the Azure portal.

2. Go to Azure Active Directory > App registrations, and select an application.

3. Select Authentication > Advanced settings > Allow public client flows and set the Enable the following mobile and desktop flows option to Yes. For more information on application settings, see this Microsoft article.

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

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

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

Backup Application Permissions

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

**NOTE**

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

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

<table>
<thead>
<tr>
<th>API</th>
<th>Permission name</th>
<th>Exchange Online</th>
<th>SharePoint Online and OneDrive for Business</th>
<th>Microsoft Teams</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Graph</td>
<td>Sites.Read.All</td>
<td></td>
<td></td>
<td></td>
<td>Getting download URLs for files and their versions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> In the Microsoft Azure China region, the Sites.ReadWrite.All permission is used instead.</td>
</tr>
<tr>
<td>SharePoint</td>
<td>Sites.FullControl.All</td>
<td></td>
<td></td>
<td>✔</td>
<td>Reading SharePoint sites and OneDrive accounts content.</td>
</tr>
<tr>
<td></td>
<td>User.Read.All</td>
<td></td>
<td></td>
<td>✔</td>
<td>Reading OneDrive accounts (getting site IDs).</td>
</tr>
</tbody>
</table>
Permissions for Modern Authentication and Legacy Protocols

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

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

<table>
<thead>
<tr>
<th>API</th>
<th>Permission name</th>
<th>Exchange Online</th>
<th>SharePoint Online and OneDrive for Business</th>
<th>Microsoft Teams</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Graph</td>
<td>Directory.Read.All</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>Querying Azure AD for organization properties, the list of users and groups and their properties.</td>
</tr>
<tr>
<td></td>
<td>Group.Read.All</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>Querying Azure AD for the list of groups and group sites.</td>
</tr>
<tr>
<td></td>
<td>TeamSettings.ReadWrite.All</td>
<td></td>
<td>✔</td>
<td></td>
<td>Accessing archived teams.</td>
</tr>
<tr>
<td></td>
<td>Sites.Read.All</td>
<td></td>
<td>✔</td>
<td></td>
<td>Accessing sites of the applications that are installed from the SharePoint store.</td>
</tr>
<tr>
<td>Office 365 Exchange Online</td>
<td>full_access_as_app</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>Reading mailboxes content.</td>
</tr>
<tr>
<td>SharePoint</td>
<td>Sites.FullControl.All</td>
<td></td>
<td></td>
<td></td>
<td>Reading SharePoint sites and OneDrive accounts content.</td>
</tr>
<tr>
<td></td>
<td>User.Read.All</td>
<td></td>
<td></td>
<td></td>
<td>Reading OneDrive accounts (getting site IDs).</td>
</tr>
</tbody>
</table>
Permissions for Authentication to Restore Portal

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

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

All listed permissions are of the *Delegated* type.

<table>
<thead>
<tr>
<th>API</th>
<th>Permission name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Microsoft Graph</strong></td>
<td>User.Read</td>
<td>Sign in and read user profile.</td>
</tr>
<tr>
<td><strong>&lt;Azure AD application&gt;</strong></td>
<td>access_as_user</td>
<td>Obtain an access token on behalf of the user to implement On-Behalf-Of flow. For more information about On-Behalf-Of flow, see this Microsoft article. For more information on how to expose a web API, see this Microsoft article.</td>
</tr>
</tbody>
</table>

Permissions for Azure Archiver Appliance

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

The user account that you use to create Azure AD application for the Microsoft Azure service account must have the *Global Administrator* role, must be *Owner* and must not be *Contributor* of Microsoft Azure subscription that you selected for the Microsoft Azure service account.
Amazon S3 Storage Permissions

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

Permissions for S3 Standard and S3 Standard-IA Storage Classes

The following are required permissions to use Amazon S3 object storage repository (S3 Standard and S3 Standard-IA storage classes):

- For Amazon S3 object storage

```json
{
   "s3:ListAllMyBuckets",
   "s3:GetBucketLocation"
}
```

- For a bucket

```json
{
   "s3:ListBucket"
}
```

- For an object

```json
{
   "s3:PutObject",
   "s3:GetObject",
   "s3:DeleteObject",
   "s3:AbortMultipartUpload"
}
```

For examples, see this Veeam KB article. For more information on permissions, see this Amazon article.
Permissions for S3 Glacier and S3 Glacier Deep Archive Storage Classes

The following are required permissions to use Amazon S3 object storage repository (S3 Glacier and S3 Glacier Deep Archive storage classes):

- For EC2 instance

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

- For Amazon S3 object storage

```
{  
  "s3:ListAllMyBuckets",
  "s3:GetBucketLocation"
}
```
• For a bucket

```json
{
  "s3:ListBucket",
  "s3:ListBucketMultipartUploads",
  "s3:GetBucketObjectLockConfiguration"
}
```

• For an object

```json
{
  "s3:PutObject",
  "s3:GetObject",
  "s3:DeleteObject",
  "s3:AbortMultipartUpload",
  "s3:ListMultipartUploadParts",
  "s3:RestoreObject",
  "s3:GetObjectVersion"
}
```
Azure Archive Storage Permissions

The following are required permissions to use Azure Archive storage:

```
{
  "properties": {
    "roleName": "CUSTOM_ROLE_MINIMAL_PERMISSIONS",
    "description": "CUSTOM_ROLE_MINIMAL_PERMISSIONS",
    "assignableScopes": [
      "/subscriptions/111111-1111-1111-0000-00000000000"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Authorization/*/read",
          "Microsoft.Compute/locations/**",
          "Microsoft.Compute/virtualMachines/**",
          "Microsoft.Network/locations/**",
          "Microsoft.Network/networkInterfaces/**",
          "Microsoft.Network/networkSecurityGroups/read",
          "Microsoft.Network/networkSecurityGroups/write",
          "Microsoft.Network/publicIPAddresses/join/action",
          "Microsoft.Network/publicIPAddresses/read",
          "Microsoft.Network/publicIPAddresses/write",
          "Microsoft.Network/publicIPAddresses/delete",
          "Microsoft.Network/virtualNetworks/read",
          "Microsoft.Network/virtualNetworks/write",
          "Microsoft.Network/virtualNetworks/subnets/join/action",
          "Microsoft.Storage/storageAccounts/listKeys/action",
          "Microsoft.Storage/storageAccounts/read",
          "Microsoft.Resources/deployments/**",
          "Microsoft.Resources/subscriptions/resourceGroups/read",
          "Microsoft.Resources/checkResourceName/action",
          "Microsoft.Resources/subscriptions/resourceGroups/write",
          "Microsoft.Resources/subscriptions/locations/read"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```
Permissions Changelog

You can learn what was changed in permissions required for Veeam Backup for Microsoft 365 6.0 comparing to version 5.0.

Azure AD Application Permissions

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

<table>
<thead>
<tr>
<th>API</th>
<th>Permission name</th>
<th>Type</th>
<th>Usage</th>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Microsoft Graph</strong></td>
<td><strong>Sites.Read.All</strong></td>
<td>Application</td>
<td>Backup</td>
<td>Querying Azure AD for the list of sites and getting download URLs for files and their versions.</td>
<td>new</td>
</tr>
<tr>
<td></td>
<td><strong>Sites.Read.All</strong></td>
<td>Delegated</td>
<td>Restore</td>
<td>Accessing sites of the applications that are installed from the SharePoint store.</td>
<td>new</td>
</tr>
<tr>
<td></td>
<td><strong>Sites.Read.All</strong></td>
<td>Application</td>
<td>Restore</td>
<td>Accessing sites of the applications that are installed from the SharePoint store.</td>
<td>new</td>
</tr>
<tr>
<td></td>
<td><strong>Sites.ReadWrite.All</strong></td>
<td>Application</td>
<td>Backup</td>
<td>Querying Azure AD for the list of sites and getting download URLs for files and their versions.</td>
<td>removed</td>
</tr>
<tr>
<td></td>
<td><strong>TeamSettings.ReadWrite.All</strong></td>
<td>Application</td>
<td>Restore</td>
<td>Restoring teams to the archived state.</td>
<td>removed</td>
</tr>
<tr>
<td></td>
<td><strong>Directory.ReadWrite.All</strong></td>
<td>Delegated</td>
<td>Restore</td>
<td>Setting the preferred data location when creating a new M365 group for a multi-geo tenant in case of teams restore.</td>
<td>new</td>
</tr>
</tbody>
</table>
The following table lists changes in permissions for modern authentication and legacy protocols:

<table>
<thead>
<tr>
<th>API</th>
<th>Permission name</th>
<th>Type</th>
<th>Usage</th>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Graph</td>
<td>Sites.Read.All</td>
<td>Application</td>
<td>Backup</td>
<td>Accessing sites of the applications that are installed from the SharePoint store.</td>
<td>new</td>
</tr>
</tbody>
</table>

If you allow users to perform self-service restore using Restore Portal, they will authenticate to the portal with their Microsoft 365 user account credentials. Veeam Backup for Microsoft 365 requires Azure AD application to be configured and granted permissions to ensure such authentication. For more information, see Permissions for Authentication to Restore Portal.

If you want to use the Azure archiver appliance when Veeam Backup for Microsoft 365 copies backed-up data from Azure Blob storage to Azure Archive storage, you must assign the required roles to a user account that you use to create Azure AD application for the Microsoft Azure service account. For more information, see Permissions for Azure Archiver Appliance.
Amazon S3 Storage Permissions

If you create an instance of your backed-up data in Amazon S3 Glacier or Amazon S3 Glacier Deep Archive storage, you must grant permissions to a user account that you use to access Amazon buckets and folders. For more information, see Amazon S3 Storage Permissions.

Azure Archive Storage

If you create an instance of Microsoft 365 and on-premises Microsoft organization backups in Azure Blob Storage Archive access tier, you must grant permissions to a user account that you use to access Azure archive storage. For more information, see Azure Archive Storage Permissions.
Considerations and Limitations

This section lists considerations and known limitations in Veeam Backup for Microsoft 365 6.0.

**NOTE**

For the complete list of known issues and limitations in Veeam Backup for Microsoft 365 6.0, see Release Notes. For limitations in Veeam Backup for Microsoft 365 functionality when protecting organizations with modern app-only authentication, see this Veeam KB article.

**Infrastructure**

- The Veeam Backup for Microsoft 365 RESTful API Service, Veeam Backup for Microsoft 365 Service and Veeam Backup Proxy for Microsoft 365 Service must be started using the Local System account.

- You cannot change the name of the Veeam Backup for Microsoft 365 server or change domains of the server without resetting the configuration.

- If the organization has multiple domains, they must be configured as a mesh to cross authenticate to download content from all domains with the service account. For more information, see this Microsoft article.

- Veeam Backup for Microsoft 365 does not support encryption at-rest for the following types of backup repositories:
  - A local directory on a backup proxy server.
  - Direct Attached Storage (DAS) connected to the backup proxy server.
  - Storage Area Network (SAN).
  - Network Attached Storage (SMB shares version 3.0 or later).

- [For Microsoft Outlook] Update channels such as Beta Channel, Current Channel, or Monthly Enterprise Channel are not supported; Veeam Backup for Microsoft 365 supports only RTM/GA versions. For more information, see this Microsoft article.

- If the Veeam Backup for Microsoft 365 console and a management server are deployed on different machines, make sure that the management server is trusted for delegation. For more information, see this Microsoft article.

- If any of the machines with any of the Veeam Backup for Microsoft 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 listed has occurred on a server that acts as a backup proxy server, then such a server becomes Offline in the Veeam Backup for Microsoft 365 console. To make a server available, re-add it. For more information, see Adding Backup Proxy Servers.

- IPv6 is not supported for Microsoft Azure China region.

- Adding Microsoft 365 organizations using modern authentication with legacy protocols allowed is not supported for Microsoft Azure China region.

- Adding Microsoft 365 organizations using modern app-only authentication is not supported for Microsoft Azure Germany region.

- Microsoft Teams service is not supported for organizations in the Microsoft Azure China and Germany regions.
Backup of team chats using Teams Export APIs is not supported for Microsoft organizations in the Microsoft Azure China, Germany, US Government GCC and US Government GCC High regions.

Notifications about backup jobs completion results may not work properly for Microsoft Azure China and Germany regions.

If you roll back the successful automatic update of the remote Veeam Backup for Microsoft 365 Console and PowerShell components, the Veeam Backup for Microsoft 365 server will not re-update these components.

Backup Repositories

- A symbolic link that is configured as a mapped drive is not supported.
- Storage volumes that host backup repositories must be formatted with NTFS or ReFS.
- You should not use 3rd party encryption software for backups in backup repositories as this may lead to unpredictable system behavior and inevitable data loss.
- Primary Storage Hardware Systems both with and without deduplication or compression are only supported for the certified operating systems. Make sure that the operating system you use is included in the Certified for Windows Server list. For more information, see this Microsoft article.
- Software Defined Storage Systems without deduplication or compression are only supported for the certified operating systems. Make sure that the operating system you use is included in the Certified for Windows Server list. For more information, see this Microsoft article.
- Software Defined Storage Systems with enabled deduplication or compression are not supported.
- Based on the format of the used Microsoft JET Database, deduplication backup storage appliances are not supported.
- For Microsoft Windows operating system or other operating systems, the file system internal deduplication is not supported.
- SMB shares version 3.0 are only supported when they are within the Microsoft Exchange Storage definition. For more information, see this Microsoft article.
- If you already backed up team chats using Teams Export APIs, you must not change a backup proxy server where backups are stored to another backup proxy server for which usage of Teams Export APIs for team chats backup is not enabled yet.

Object Storage Repositories

- Veeam Backup for Microsoft 365 does not support the $root container in Azure Blob storage.
- Veeam Backup for Microsoft 365 does not support Lifecycle policy in Amazon AWS Data Management.
- Make sure the S3 Compatible device you are adding supports AWS S3 Signature Version 4. For more information about authentication requests, see this Amazon article.
- Veeam Backup for Microsoft 365 allows you to migrate data from a local backup repository to an object storage repository, but not vice versa. For more information, see the Move-VBOEntityData section of the Veeam Backup for Microsoft 365 PowerShell Reference.
- Veeam Backup for Microsoft 365 does not support object lock for the S3 Compatible bucket.
Backup

- To back up user mailboxes, make sure that a mailbox has a valid Microsoft 365 license. Otherwise a backup job will fail with the following error: "Error: Mailbox doesn't have a valid Microsoft 365 license".

- To back up public folder mailboxes, the Veeam Backup account must have a valid Exchange Online license and an active mailbox within the Microsoft 365 organization.

- To back up SharePoint and OneDrive for Business objects, make sure that a user account has a valid Microsoft 365 license with SharePoint plan enabled. Otherwise a backup job will fail with the following error: "User %name% does not have a valid Microsoft 365 license with SharePoint plan enabled".

- Veeam Backup for Microsoft 365 backs up public folders that are located under the IPM_SUBTREE folder only.

- Project Web Apps are not supported for backup.

- On-premises service accounts cannot be used for multi-factor authentication.

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

- You can select only the root public mailbox when backing up public mailboxes. The child folders of the selected public mailbox will be backed up as well.

- If you modify a retention policy tag for a folder, Veeam Backup for Microsoft 365 will perform full synchronization of that folder during the subsequent backup job session. For more information, see this Microsoft article.

- A SharePoint Site Collection hierarchy is not supported if the root site was not configured. Make sure to configure the root site in advance using a SharePoint site template of your choice. Otherwise, the following error occurs: Error: Failed to find web template ID for: STS#1. This organization account might be missing a valid SharePoint license. Web configuration is not complete.

- SharePoint site collection recycle bin is not supported for backup.

- When backing up Microsoft Exchange mailboxes, Veeam Backup for Microsoft 365 does not create a new version of an item if the Read/Unread property of such item was changed. That said, the Read/Unread property of each of the backed-up items always remains exactly the same as it was during the initial backup.

- As part of Microsoft Teams data backup, Veeam Backup for Microsoft 365 backs up only the following types of channel tabs: Website, Planner, Word, Excel, PowerPoint, Visio, PDF, Document Library, OneNote, SharePoint, Stream, Forms, Power BI, Power Automate (ex Flow) and Azure DevOps.

- When you perform backup of Microsoft Teams data, Veeam Backup for Microsoft 365 does not back up the following objects:
  - Private channels.
  - One-on-one and group chats.
    For more information about chats in Microsoft Teams, see this Microsoft article. You can use Veeam Explorer for Microsoft Exchange to explore data from user mailboxes and view chat messages as MSG files.
  - Audio and video calls.
  - Video recordings saved to Microsoft Stream.
  - Contacts.
  - Calendar: information about meetings and meeting chats.
- Code snippets in posts.
- Banner notifications in posts.
- Data of applications added as channel tabs (such as Website, Planner, Word, Excel, PowerPoint, Visio, PDF, Document Library, OneNote, SharePoint, Stream, Forms, Power BI, Power Automate and Azure DevOps) and other 3rd party applications if their data does not reside in the SharePoint document library of the team.

- Backup of team chats using Teams Export APIs is only supported for Microsoft 365 organizations with modern app-only authentication.
- Veeam Backup for Microsoft 365 may not backup OneNote notebooks if their size is more than 2 GB. For more information, see this Microsoft article.
- External SharePoint lists are not supported for backup. For more information, see this Microsoft article.

**Restore**

**NOTE**

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

- Veeam Explorer for Microsoft Exchange
- Veeam Explorer for Microsoft SharePoint
- Veeam Explorer for Microsoft Teams

- SharePoint sites with a red ‘X’ over the symbol mean that there is an empty sector of the template and supported content is available in the subsites.
- Microsoft Teams messages cannot be restored directly back to Teams.
- Veeam Backup for Microsoft 365 restores public folders that are located under the `IPM_SUBTREE` folder only.
- Bulk restore (restore of multiple objects) is not supported for public folder mailboxes. Use the regular per-object restore instead.
- Bulk restore of Exchange mailboxes can be performed to the original location only. Use a single mailbox, folder or item restore if you want to restore such objects to another location.
- To restore *In-Place Hold Items* or *Litigation Hold Items* to the original location, consider the following:
  - Restore of *In-Place Hold Items* is not supported for on-premises Microsoft Exchange Server 2013 due to EWS limitations.
  - To restore *In-Place Hold Items* of Exchange 2016/2019 mailboxes, these mailboxes must have *In-Place Hold* enabled and applied at least once with the *DiscoveryHolds* system folder creation. Otherwise, restore of *In-Place Hold Items* will fail with the following error: "Failed to restore In-Place Hold Items. Restore of In-Place Hold Items into Exchange 2013 is not supported".
- For more information about enabling *In-Place Hold* and *Litigation Hold*, see this Microsoft article.

- Restore of OneNote notebooks from backups of Microsoft SharePoint, Microsoft OneDrive for Business and Microsoft Teams data for organizations with modern app-only authentication is not supported.
- Restore of OneNote tabs from backups of Microsoft Teams data may fail with the “Configuration size exceeded. Provided: ‘4117’ bytes MaxAllowed: ‘4096’ bytes” error if the OneNote tab name includes non-Latin or special characters.
- If a SharePoint site includes a hidden list, such list is not displayed in Veeam Explorer for Microsoft SharePoint after a site backup and thus, cannot be restored.

- Before restoring team data using Veeam Explorer for Microsoft Teams or team sites using Veeam Explorer for Microsoft SharePoint for a tenant organization with modern app-only authentication, make sure that a user account used for authorization has access to the root SharePoint site of this tenant organization.
Supported Azure Storage Account Types

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

Standard Performance Tier

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

<table>
<thead>
<tr>
<th>Supported Storage Account Type</th>
<th>Supported Services</th>
<th>Supported Access Tiers</th>
</tr>
</thead>
<tbody>
<tr>
<td>General-purpose V2</td>
<td>Blob</td>
<td>Hot, Cool, Archive</td>
</tr>
<tr>
<td>General-purpose V1</td>
<td>Blob</td>
<td>N/A</td>
</tr>
<tr>
<td>Blob Storage</td>
<td>Blob (block blobs and append blobs only)</td>
<td>Hot, Cool, Archive</td>
</tr>
</tbody>
</table>

**NOTE**

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

Premium Performance Tier

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

<table>
<thead>
<tr>
<th>Supported Storage Account Type</th>
<th>Supported Services</th>
<th>Supported Access Tiers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block Blob Storage</td>
<td>Blob (block blobs and append blobs only)</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Supported Amazon S3 Storage Classes

Veeam Backup for Microsoft 365 supports the following Amazon S3 Storage Classes:

- Amazon S3 Standard (S3 Standard)
  Use this storage class for general-purpose storage of frequently accessed data.

- Amazon S3 Standard-Infrequent Access (S3 Standard-IA)
  Use this storage class for long-lived, but less frequently accessed data.

- Amazon S3 Glacier (S3 Glacier)
  Use this storage class for data archiving. Veeam Backup for Microsoft 365 supports this storage class as a target for backup copy jobs.

- Amazon S3 Glacier Deep Archive (S3 Glacier Deep Archive)
  Use this storage class for archiving data that may be rarely accessed. Veeam Backup for Microsoft 365 supports this storage class as a target for backup copy jobs.
Licensing and License Types

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

A user account consists of:

- **Microsoft Exchange Online and on-premises Microsoft Exchange mailboxes**
  Such a mailbox can be a personal mailbox, an Online Archive mailbox or both — you will only need one Veeam license per user.

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

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

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

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

The Veeam license is not required for:

- **Shared, resource and group mailboxes**
  Shared and resource mailboxes do not consume units in the Veeam license if such mailboxes do not have a Microsoft 365 license assigned.

- **External SharePoint users**
  An external SharePoint user is a user from outside your Microsoft 365 subscription 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**

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

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

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

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

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

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

**NOTE**

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

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

License Expired

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

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

License Exceeded

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

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

The grace period in this case is not limited and lasts during the whole term of the subscription.
Rental License

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

Understanding New User Status

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

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

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

License Expired

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

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

License Exceeded

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

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

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

The restore abilities will continue to function regardless of the grace period state.
Managing Monthly Usage Report

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

On the first day of each month and for the next 4 days you will receive the notification message. During this period, the notification message will appear every time you launch Veeam Backup for Microsoft 365 until you send your reports to Veeam.

**NOTE**

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

Do one of the following:

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

After this 5-days period, Veeam Backup for Microsoft 365 stops displaying the notification message and you will not be able to send a monthly usage report to Veeam from the Veeam Backup for Microsoft 365 user interface. The report will be sent to Veeam automatically. You will still be able to review the report — Veeam Backup for Microsoft 365 automatically saves it to the `%ProgramData%\Veeam\Backup365\Reports` folder in PDF and CSV formats.

Managing Reports

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

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

In the Monthly Usage Report window, you can do the following to manage filters and perform other required actions:

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

  To undo removing, click **Reset**.

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

- To send the report to Veeam, click **Send**.

---

**Monthly report for February 2022**

<table>
<thead>
<tr>
<th>Account</th>
<th>Organization Name</th>
<th>Last Processed</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:admin4@ave.onmicrosoft.com">admin4@ave.onmicrosoft.com</a></td>
<td>ave.onmicrosoft.com</td>
<td>2022-02-22 12:38...</td>
</tr>
<tr>
<td><a href="mailto:admin6@ave.onmicrosoft.com">admin6@ave.onmicrosoft.com</a></td>
<td>ave.onmicrosoft.com</td>
<td>2022-02-22 12:38...</td>
</tr>
<tr>
<td><a href="mailto:admin7@abc.onmicrosoft.com">admin7@abc.onmicrosoft.com</a></td>
<td>abc.onmicrosoft.com</td>
<td>2022-02-22 12:38...</td>
</tr>
<tr>
<td><a href="mailto:admin8@abc.onmicrosoft.com">admin8@abc.onmicrosoft.com</a></td>
<td>abc.onmicrosoft.com</td>
<td>2022-02-22 12:38...</td>
</tr>
</tbody>
</table>

---
Not For Resale License

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

License Expired

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

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

License Exceeded

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

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

License Expired

Within a month before the expiration date, you will receive a notification message stating that your license is about to expire. During this period, the product functionality will not be limited by any means. After your license expires, 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.
Integration with Veeam Service Provider Console

Veeam Backup for Microsoft 365 supports integration with *Veeam Service Provider Console* that monitors licenses consumed by Veeam Backup for Microsoft 365 servers and the state of the product services. For more information, see the Integration with Veeam Backup for Microsoft 365 section of the Veeam Service Provider Console Guide for Service Providers.
Deployment

To start working with Veeam Backup for Microsoft 365, you must deploy the solution to your environment. Consider the following:

- If you have been participating in the public beta testing of Veeam Backup for Microsoft 365, make sure to uninstall the pre-release (BETA) versions of Veeam Backup for Microsoft 365 and Veeam Explorers.

- To use the solution in hybrid Exchange deployment or on-premises organizations with SPN and Kerberos authentication, make sure to install Veeam Backup for Microsoft 365 on a server that is located within the domain with the source Microsoft Exchange server.

- The solution can be deployed to virtual or physical machines or directly to cloud platforms such as Azure or Amazon Web Services (AWS).

- Veeam Backup for Microsoft 365 REST API component can be deployed either on a Veeam Backup for Microsoft 365 server or on a separate computer. Installing REST API separately from a Veeam Backup for Microsoft 365 server allows you to decrease the load on infrastructure when exploring and restoring data from backups in a web browser window using the Restore Portal. Restore Portal allows users to perform self-service restore. For more information, see Installing REST API on Separate Computer and Configuring REST API and Restore Portal on Separate Computer.
Downloading Installation Package

You can download the Veeam Backup for Microsoft 365 installation package from the official Veeam website. The installation package consists of the following files:

- **Veeam.Backup365.iso** — opens the Veeam Backup for Microsoft 365 image file that includes the following folders and files:
  - **Backup.** This folder includes the Veeam.Backup365.msi file that installs Veeam Backup for Microsoft 365 including the following services:
    - **Veeam Backup for Microsoft 365 Service**
      Controls global configuration settings.
    - **Veeam Backup Proxy for Microsoft 365 Service**
      Manages backup proxy servers.
    - **Veeam Backup for Microsoft 365 RESTful API Service**
      Processes REST API commands and allows Restore Portal to communicate with Veeam Backup for Microsoft 365. This service is disabled by default and can be enabled. For more information, see [REST API Settings](#).
  - **Explorers.** This folder includes MSI files that install Veeam Explorers:
    - **VeeamExplorerForExchange.msi** — installs Veeam Explorer for Microsoft Exchange.
      For more information, see [Veeam Explorer for Microsoft Exchange](#).
    - **VeeamExplorerForSharePoint.msi** — installs Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft OneDrive for Business.
      For more information, see [Veeam Explorer for Microsoft SharePoint](#) and [Veeam Explorer for Microsoft OneDrive for Business](#).
    - **VeeamExplorerForTeams.msi** — installs Veeam Explorer for Microsoft Teams.
      For more information, see [Veeam Explorer for Microsoft Teams](#).
  - **[Optional] Patches.** If exists, this folder includes MSP files that Windows uses to install patches along with the Veeam Backup for Microsoft 365 and Veeam Explorers installation.
  - **Redistr.** This folder includes Microsoft .NET Framework installation file.
  - **Setup.** This folder includes the *End User License Agreement and 3rd party software notices and information* documents, Veeam.Archiver.Autorun.exe, and other files required for the installation and operation of Veeam Backup for Microsoft 365.
  - **autorun.inf** — includes the setup information.
  - **Veeam.Setup.exe** — launches the Veeam Backup for Microsoft 365 installation wizard.

- **VeeamExplorerForExchange.msi** — installs Veeam Explorer for Microsoft Exchange.
- **VeeamExplorerForSharePoint.msi** — installs Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft OneDrive for Business.
- **VeeamExplorerForTeams.msi** — installs Veeam Explorer for Microsoft Teams.
Installing Veeam Backup for Microsoft 365 and Veeam Explorers

You can simultaneously install Veeam Backup for Microsoft 365 (including Veeam Backup for Microsoft 365 Service, Veeam Backup Proxy for Microsoft 365 Service and Veeam Backup for Microsoft 365 RESTful API Service) and Veeam Explorers on a machine that you want to be a Veeam Backup for Microsoft 365 server.

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

1. Download the Veeam Backup for Microsoft 365 installation package.
3. On the splash screen, click Install.
4. Click **Veeam Backup for Microsoft 365**.

**Veeam Backup for Microsoft 365**
Veeam Backup for Microsoft 365 allows you to backup and restore data of your Microsoft 365 organizations, as well as data of on-premises Microsoft organizations.

**Veeam Backup for Microsoft 365 Console**
The Console is the user interface client for local and remote Veeam Backup for Microsoft 365 servers.

**Veeam Backup for Microsoft 365 PowerShell**
The PowerShell extension includes sets of PowerShell cmdlets that allow you to automate operations available in the Veeam Backup for Microsoft 365 user interface.

**Veeam Backup for Microsoft 365 REST API & Restore Portal**
The RESTful API plugin includes HTTPS resources to perform operations available in the user interface. Restore Portal built on the REST APIs allows you to delegate restore permissions.
5. At the License Agreement step, click the links to read the following documents: End User License Agreement, Licensing policy and 3rd party software notices and information. If you accept the terms of these documents, click I Accept. If you do not accept the terms of these documents, cancel installation and do not use the product.

6. At the System Configuration Check step, wait until the wizard checks the system configuration to find the potential installation problems. You may be prompted to fix the issues to continue the installation.

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

   By default, all Veeam Backup for Microsoft 365 components are installed to the C:\Program Files\Veeam\Backup365 folder. To install to a different location, click Browse and specify a folder.
Veeam Explorers are installed to the C:\Program Files\Veeam\Backup and Replication\Explorers folder. Mind that you cannot specify a different location for Veeam Explorers.

8. Click **Install**.

9. Wait for the installation process to complete and click **Finish** to exit the wizard.
Installing REST API on Separate Computer

NOTE
Consider the following:

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

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

1. Download the Veeam Backup for Microsoft 365 installation package.
3. On the splash screen, click Install.
4. Click Veeam Backup for Microsoft 365 REST API & Restore Portal.

Veeam Backup for Microsoft 365
Veeam Backup for Microsoft 365 allows you to backup and restore data of your Microsoft 365 organizations, as well as data of on-premises Microsoft organizations.

Veeam Backup for Microsoft 365 Console
The Console is the user interface client for local and remote Veeam Backup for Microsoft 365 servers.

Veeam Backup for Microsoft 365 PowerShell
The PowerShell extension includes sets of PowerShell cmdlets that allow you to automate operations available in the Veeam Backup for Microsoft 365 user interface.

Veeam Backup for Microsoft 365 REST API & Restore Portal
The RESTful API plugin includes HTTPS resources to perform operations available in the user interface. Restore Portal built on the REST APIs allows you to delegate restore permissions.

View Documentation
5. At the **License Agreement** step, click the links to read the following documents: *End User License Agreement*, *Licensing policy* and *3rd party software notices and information*. If you accept the terms of these documents, click **I Accept**. If you do not accept the terms of these documents, cancel installation and do not use the product.

6. At the **System Configuration Check** step, wait until the wizard checks the system configuration to find the potential installation problems. You may be prompted to fix the issues to continue the installation.
7. At the **Data Location** step, specify the installation folder.

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

8. Click **Install**.

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

Restore Portal is deployed automatically along with Veeam Backup for Microsoft 365 REST API component installation. After you installed Veeam Backup for Microsoft 365 REST API component on a separate computer, you must configure the REST API and Restore Portal settings. It is required to establish communication and data exchange between **Veeam Backup for Microsoft 365 RESTful API Service** and the Veeam Backup for Microsoft 365 server and allows Restore Portal to communicate with Veeam Backup for Microsoft 365. For more information, see [Configuring REST API and Restore Portal on Separate Computer](#).
Installing Veeam Explorers for Tenants

**NOTE**

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

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

1. Download the Veeam Backup for Microsoft 365 installation package.
3. On the splash screen, click **Install**.
4. Click the **Install Veeam Explorers** link that is only available if you run the installation wizard on a server with Veeam Backup & Replication.
5. At the **License Agreement** step, click the links to read the following documents: *End User License Agreement, Licensing policy* and *3rd party software notices and information*. If you accept the terms of these documents, click **I Accept**. If you do not accept the terms of these documents, cancel installation and do not use the product.

6. At the **System Configuration Check** step, wait until the wizard checks the system configuration to find the potential installation problems. You may be prompted to fix the issues to continue the installation.
7. At the **Ready to install** step, review versions of Veeam Explorers that are ready to install and click **Install**.

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

8. Wait for the installation process to complete and click **Finish** to exit the wizard.
Installing in Unattended Mode

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

Use the following syntax to run an MSI file:

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

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Feature name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>BR_OFFICE365</td>
</tr>
<tr>
<td>Console</td>
<td>CONSOLE_OFFICE365</td>
</tr>
<tr>
<td>PowerShell</td>
<td>PS_OFFICE365</td>
</tr>
<tr>
<td>REST API</td>
<td>REST_OFFICE365</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Feature name</th>
</tr>
</thead>
<tbody>
<tr>
<td>UI</td>
<td>BR_EXCHANGEEXPLORER</td>
</tr>
<tr>
<td>PowerShell</td>
<td>PS_EXCHANGEEXPLORER</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Feature name</th>
</tr>
</thead>
<tbody>
<tr>
<td>UI</td>
<td>BR_SHAREPOINTEXPLORER</td>
</tr>
</tbody>
</table>

**NOTE**

Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft OneDrive for Business are distributed in a single package.
The following table lists components and feature names for *Veeam Explorer for Microsoft Teams*:

<table>
<thead>
<tr>
<th>Component</th>
<th>Feature name</th>
</tr>
</thead>
<tbody>
<tr>
<td>UI</td>
<td>BR_TEAMSEXPLORER</td>
</tr>
<tr>
<td>PowerShell</td>
<td>PS_TEAMSEXPLORER</td>
</tr>
</tbody>
</table>

**Examples**

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

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

To install the *Veeam Backup for Microsoft 365 REST API* component only:

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

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

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

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

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

**NOTE**

Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft OneDrive for Business are distributed in a single package.
To install the *Veeam Explorer for Microsoft Teams, UI* and *PowerShell* components:

```
msiexec /i VeeamExplorerForTeams.msi /qn ADDLOCAL=BR_TEAMSEXPLORER,PS_TEAMSEXPLORER ACCEPT_THIRDPARTY_LICENSES=1 ACCEPT_EULA=1
```
Deploying to Azure and AWS

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

1. Install Veeam Backup for Microsoft 365 on an Azure or AWS virtual machine. For more information, see Installing Veeam Backup for Microsoft 365 and Veeam Explorers.

   Alternatively, you can deploy Veeam Backup for Microsoft 365 from Azure Marketplace and AWS Marketplace.

   When deploying to Azure, you can use F-Series VM Sizes for better performance.

2. Configure additional backup proxy servers. For more information, see Backup Proxy Servers.

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

3. Configure backup repositories. For more information, see Backup Repositories.

After deployment is complete, you can:

- Add Microsoft 365 and on-premises Microsoft organizations to the Veeam Backup for Microsoft 365 scope. For more information, see Organization Management.
- Create new backups. For more information, see Data Backup and Backup Copy.
- View and restore your data. For more information, see Data Restore.
Updating Veeam Backup for Microsoft 365

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

- **Automatically.** Veeam Backup for Microsoft 365 regularly checks Veeam servers for critical updates. If a new critical update is available, Veeam Backup for Microsoft 365 downloads this update in the background and installs it to the backup infrastructure components.

- **Manually.** You can manually check for Veeam Backup for Microsoft 365 and Veeam Explorers updates at any time.
Automatic Update

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

- Veeam Backup for Microsoft 365 server to update Veeam Backup for Microsoft 365, Veeam Explorers, PowerShell, and REST API.
- Backup proxy servers.

**IMPORTANT**

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

At first, the downloaded updates are installed to the Veeam Backup for Microsoft 365 server within the *update window* that is a period of the Veeam Backup for Microsoft 365 server idleness. The following conditions must be met:

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

Veeam Explorers as well as remote *Veeam Backup for Microsoft 365 Console* and *PowerShell* components will be updated only after the Veeam Backup for Microsoft 365 server update completes.

Installation of the downloaded updates to remote backup proxy servers in the Veeam Backup for Microsoft 365 backup infrastructure is performed within the separate update window. Veeam Backup for Microsoft 365 determines a time period when backup, backup copy and retrieval jobs as well as data management jobs are not running on a backup proxy server.

**NOTE**

Update windows for the Veeam Backup for Microsoft 365 server (including the local backup proxy) and remote proxy servers can be different.

Thus, automatic update of Veeam Backup for Microsoft 365 can only be performed when the load on the backup infrastructure components is minimal. If Veeam Backup for Microsoft 365 cannot determine the proper update window during a considerable period of time, you will be prompted to install updates manually. For more information, see *Checking for Updates*.

You can disable automatic update. To do this, clear the *Allow for automatic updates* check box on the *Updates* tab. For more information, see *New Versions and Automatic Updates*.
Checking for Updates

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

1. In the main menu, click **Upgrade**.

2. In the **Check for available updates** step, click **Next**.
   
   Make sure to open the port that is required to access the Veeam auto-update server. For more information, see **Used Ports**.

3. Wait until Veeam Backup for Microsoft 365 checks whether a newer version is available.
   
   To abort the request, click **Cancel**.

4. If available, click the **What's new** links to review details about new features and enhancements of Veeam Backup for Microsoft 365 and Veeam Explorers and click **Install**.
During update, the Veeam Backup for Microsoft 365 console will be closed, whereupon you will be offered to go through the setup steps. For more information, see Installing Veeam Backup for Microsoft 365 and Veeam Explorers.

5. Once installation is complete, launch Veeam Backup for Microsoft 365. For more information, see Launching Veeam Backup for Microsoft 365.

**NOTE**

Veeam Backup for Microsoft 365 is also capable of checking for a newer version of the product automatically. To do this, select the **Automatically check and notify me on available updates** check box on the **Updates** tab. For more information, see New Versions and Automatic Updates.
Installing and Updating License

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

Installing Fully-Functional License

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

The number of user accounts that you will be able to back up depends on the purchase agreement with Veeam sales representatives. You can see how many accounts are available in the Users row of the License Information window.

To install a license, do the following:

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

The Update license automatically (enables usage reporting) check box in the License Information window will be selected automatically.

NOTE

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

- License ID
- Installation ID
- Workload usage counters

Updating License

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

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

To automatically update your current license, select the Update license automatically (enables usage reporting) check box.
**NOTE**

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

### Installed license

<table>
<thead>
<tr>
<th>Status</th>
<th>Valid</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expiration date</td>
<td>9/21/2022 (351 days left)</td>
</tr>
<tr>
<td>Type</td>
<td>Subscription</td>
</tr>
<tr>
<td>Licensed to</td>
<td>Veeam Software GmbH</td>
</tr>
<tr>
<td>Contact person</td>
<td>Dev and QA Departments</td>
</tr>
<tr>
<td>Users</td>
<td>102 (3 used)</td>
</tr>
<tr>
<td>Support ID</td>
<td>00782619</td>
</tr>
<tr>
<td>Support expiration date</td>
<td>9/21/2022 (351 days left)</td>
</tr>
</tbody>
</table>

- **Update license automatically (enables usage reporting)**

[OK] [Cancel]
Upgrading to Veeam Backup for Microsoft 365 6.0

Veeam Backup for Microsoft 365 supports upgrade from the following versions of the product:

- 4.0 (build 4.0.0.1345)
- 4a (builds 4.0.0.1553, 4.0.0.1580)
- 4b (builds 4.0.0.2516, 4.0.0.2549)
- 4c (builds 4.0.1.519, 4.0.1.531, 4.0.1.545, 4.0.1.612, 4.0.1.625)
- 5.0 (builds 5.0.0.1061, 5.0.0.1063)
- 5a (build 5.0.0.1070)
- 5b (builds 5.0.1.179, 5.0.1.207, 5.0.1.225, 5.0.1.252)
- 5c (builds 5.0.2.22, 5.0.2.42)
- 5d (builds 5.0.3.1033, 5.0.3.1035, 5.0.3.1051, 5.0.3.1060, 5.0.3.1063)
- 6.0 (builds 6.0.0.367, 6.0.0.379, 6.0.0.385, 6.0.0.400)

Consider the following:

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

To upgrade Veeam Backup for Microsoft 365 and Veeam Explorers to version 6.0, do the following:

1. Download the Veeam Backup for Microsoft 365 installation package.
3. On the splash screen, click Update.
4. At the **License Agreement** step, click the links to read the following documents: *End User License Agreement*, *Licensing policy* and *3rd party software notices and information*. If you accept the terms of these documents, click **I Accept**. If you do not accept the terms of these documents, cancel installation and do not use the product.

![License Agreement](image)

**License Agreement**

Read the license agreements and accept them to proceed.

Please view, print, or save the documents linked below:

By clicking the 'I Accept' button, I hereby accept the following:

- Agree and consent to the terms of *Veeam License Agreement* and *licensing policy*
- Agree and consent to each of the license agreements of *the 3rd party components* used

![License Agreement](image)

5. At the **System Configuration Check** step, wait until the wizard checks the system configuration to find the potential installation problems. You may be prompted to fix the issues to continue the installation.
6. At the **Ready to install** step, review versions of Veeam Backup for Microsoft 365 components that are ready to upgrade and click **Install**.

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veeam Backup for Microsoft 365 Server</td>
<td>5.0.3.1053 → 6.0.0.339</td>
</tr>
<tr>
<td>Veeam Backup for Microsoft 365 Console</td>
<td>5.0.3.1053 → 6.0.0.339</td>
</tr>
<tr>
<td>Veeam Backup for Microsoft 365 PowerShell</td>
<td>5.0.3.1053 → 6.0.0.339</td>
</tr>
<tr>
<td>Veeam Backup for Microsoft 365 REST API &amp; Restore Portal</td>
<td>5.0.3.1053 → 6.0.0.339</td>
</tr>
</tbody>
</table>

**NOTE**

If you have upgraded Veeam Backup for Microsoft 365 from version 4 and you want to back up Microsoft Teams data, after installing Veeam Explorer for Microsoft Teams, do the following:

1. Edit your Microsoft 365 organization. For more information, see **Editing Organization Settings**.
2. At the **Organization deployment type** step of the wizard, select the **Microsoft Teams** check box. You can select this check box only if both the **Exchange Online** and **SharePoint Online and OneDrive for Business** check boxes are selected.
3. Grant the required permissions to the Veeam Backup account and Azure AD application. For more information, see **Required Permissions**.

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

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

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

- **Backup proxy servers**
  For information on how to upgrade backup proxy servers, see **Upgrading Backup Proxy Servers**
  Consider that a default backup proxy server will be upgraded automatically.

7. Wait for the installation process to complete and click **Finish** to exit the wizard.
Uninstalling Veeam Backup for Microsoft 365

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

1. Stop all restore sessions (if any) in Veeam Explorer for Microsoft Exchange, Veeam Explorer for Microsoft SharePoint, Veeam Explorer for Microsoft OneDrive for Business and Veeam Explorer for Microsoft Teams.

2. Open the Veeam Backup for Microsoft 365 console, go to Backup Infrastructure > Backup Proxies and remove all configured backup proxy servers. For more information, see Removing Backup Proxy Server.

3. From the Start menu, select Control Panel > Programs and Features.

4. In the programs list, right-click Veeam Backup for Microsoft 365 and select Uninstall.

   The Veeam Backup for Microsoft 365 uninstallation wizard runs.

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

   **IMPORTANT**
   
   If you have both Veeam Backup for Microsoft 365 and Veeam Backup & Replication installed, uninstall Veeam Explorers using the procedure in this section of the Veeam Backup & Replication Best Practices Guide.

6. Wait for the uninstallation process to complete and click Finish to exit the wizard.
Launching Veeam Backup for Microsoft 365

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

1. From the Start menu, select Veeam Backup for Microsoft 365.
2. In the displayed window, specify the following:
   - A name or IP address of the Veeam Backup for Microsoft 365 server.
   - A port number which is used to connect to the specified Veeam Backup for Microsoft 365 server.
   - Authentication credentials that you want to use to connect to the specified Veeam Backup for Microsoft 365 server.
     Mind that the account you are using must be a member of the Local Administrator group on the specified Veeam Backup for Microsoft 365 server. To use your current account, select Use Windows session authentication.
3. If you want to save a connection shortcut to the desktop, click Save shortcut in the lower-left corner.
4. Click Connect.

Launching with Command Line

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

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

For example:

C:\Program Files\Veeam\Backup365\Veeam.Archiver.Shell.exe /local=true
- `/host=<hostname> /port=<port> /usewincredentials=true`
  To connect to Veeam Backup for Microsoft 365 that is installed on a remote machine using the `/host` and `/port` parameters.
  For example:

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

- `/host=<host> /port=<port> /account=<domain\accountName>`
  To connect to Veeam Backup for Microsoft 365 that is installed on a remote machine using the `/host` and `/port` parameters.
  You can also provide an account that you want to use to launch Veeam Backup for Microsoft 365 using the `/account=<domain\accountName>` format.
  For example:

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

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

Main Menu

The main menu comprises the following:

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

• Exit. Closes the Veeam Backup for Microsoft 365 console window.

Main Application Window

The main application window can be divided into five categories:

• The views switch that allows you to switch among the following infrastructure views:
  o The Organizations view is intended to work with Microsoft organizations, as well as backup, backup copy and retrieval jobs. Also, it provides statistics for recently performed backup, backup copy and restore sessions.
  o The Backup Infrastructure view displays a list of backup infrastructure components: backup proxies, backup repositories and object storage repositories. You can use this view for backup infrastructure setup — here you can configure backup infrastructure components that will be used for data backup, backup copy and restore of backed-up data.
  o The History view displays statistics on backup, backup copy, retrieve and restore sessions performed with Veeam Backup for Microsoft 365.

• The inventory pane that displays a hierarchy or list of items relevant for a specific view. Lists are displayed in the preview pane.
  Items displayed in the inventory pane differ depending on the active view. For example, in the Organizations view, the inventory pane displays the following nodes:
    o The Organizations node that includes Microsoft organizations added to the scope and a list of backup and backup copy jobs configured for these organizations.
o The Data retrieval node with a list of retrieval jobs and their statuses.

o The Last 24 hours node with the list of backup, backup copy and restore sessions performed within the last 24 hours and their statuses.

In the Backup Infrastructure view, the inventory pane displays nodes for backup infrastructure components — backup proxies, backup repositories and object storage repositories.

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

On the ribbon, the following tabs are displayed:

- The Home tab provides quick access to the most common operations. It lets you manage organizations, create backup jobs, explore backed-up data, retrieve data from archives and configure reports. This tab is always available, no matter which view is currently active.

- Other tabs contain commands specific for certain items and appear when these items are selected in the inventory or preview pane.
  - The View tab allows you to switch between the compact and full view modes.
  - The Jobs tab contains commands specific for backup jobs.
  - The Backup Proxy tab contains commands specific for backup proxies.
  - The Backup Repository tab contains commands specific for backup repositories.
  - The Object Storage Repository tab contains commands specific for object storage repositories.
  - The Retrievals tab contains commands specific for retrieval jobs.
  - The Last 24 Hours tab allows you to stop backup, backup copy and restore sessions.

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

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

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

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

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

Consider the following:

- When closing the Veeam Backup for Microsoft 365 console, all running backup and backup copy sessions will continue to be executed in the background.

- Restore sessions (if any) will not be affected.
Configuration

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

You configure general settings for Veeam Backup for Microsoft 365. General settings are applied to all backup and backup copy jobs, backup infrastructure components and data restore using Restore Portal.
Folder Exclusions

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

To configure exclusions, do the following:

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

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

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

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

![Options](image-url)
Session History

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

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

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

4. Click OK.
REST API Settings

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

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

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

1. In the main menu, click General Options.
2. Open the REST API tab.
3. Select the Enable REST service check box.
4. In the Authentication token lifetime field, specify the lifetime value for an authentication token (in minutes).
   
   REST API authorization is based on the OAuth 2.0 Authorization Framework.

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

   Also, Restore Portal uses this port to communicate with the Veeam Backup for Microsoft 365 RESTful API Service. For more information, see Used Ports.

6. Click Install to specify an SSL certificate.

   You can generate a new certificate or select an existing certificate using the Select Certificate wizard. For more information, see Installing SSL Certificates.
7. Click OK.

![Options dialog box image]

- **Specify the port configuration and SSL certificate to be used by Veeam Backup for Microsoft 365 RESTful API Service.**
- **Enable REST service**
- **Authentication token lifetime (in minutes):** 60
- **HTTPS port:** 443
- **Installed certificate:**
  - **Issued to:** CN=Veeam Software, OU=Veeam Software, OU=Veeam Sc
  - **Issued by:** CN=Veeam Software, OU=Veeam Software, OU=Veeam Sc
  - **Friendly name:** Veeam Software Group GmbH certificate
  - **Expiration date:** 7/23/2023 12:44 PM
  - **Install...**
**Restore Portal Settings**

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

**NOTE**

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

To configure the Restore Portal settings, do the following:

1. In the main menu, click **General Options**.
2. Open the **Restore Portal** tab.
3. Select the **Enable Restore Portal** check box.
4. Do one of the following:
   - Register a new Azure AD application automatically
     To do this, click **Configure** and follow the steps of the **Configure Application** wizard. For more information, see Creating or Configuring Azure AD Application.
     Veeam Backup for Microsoft 365 automatically grants the required permissions to the Azure AD application that you create and generates an SSL certificate. For more information, see Registering New Azure AD Application.
   - Configure an existing Azure AD application
     To do this, click **Configure** and follow the steps of the **Configure Application** wizard. For more information, see Creating or Configuring Azure AD Application.
     Veeam Backup for Microsoft 365 checks the Azure AD application permissions, grants the missing permissions if needed and updates an SSL certificate. For more information, see Configuring Existing Azure AD Application.
     Mind that configuring an exiting Azure AD application is available starting from version 6a (build 6.1.0.222).
Creating or Configuring Azure AD Application

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

1. Launch the Configure Application wizard.
2. Configure connection to Restore Portal.
3. Register or configure Azure AD application.
4. Log in to Microsoft 365.
Step 1. Launch Configure Application Wizard

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

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

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

You can select one of the following options:

- **Register a new Azure AD application automatically**
  
  With this option selected, Veeam Backup for Microsoft 365 requires to provide an application name, a certificate to register a new Azure AD application in Azure Active Directory and specify web address of a computer with Veeam Backup for Microsoft 365 REST API component installed. For more information, see Registering New Azure AD Application.

- **Use an existing Azure AD application**
  
  With this option selected, Veeam Backup for Microsoft 365 requires to modify connection parameters of the existing Azure AD application. For more information, see Configuring Existing Azure AD Application.
Step 3. Register or Configure Azure AD Application

At this step of the wizard, you can create a new application in Azure Active Directory or configure an existing one.

- **Registering a new application**
  Use this method if you have selected the *Register a new Azure AD application automatically* option at the previous step of the wizard.

- **Configure an existing application**
  Use this method if you have selected the *Use an existing Azure AD application* option at the previous step of the wizard.

**NOTE**

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

### Registering New Azure AD Application

You can register a new Azure AD application in Azure Active Directory. Veeam Backup for Microsoft 365 will use this application to connect to Restore Portal. When registering a new Azure AD application, Veeam Backup for Microsoft 365 automatically grants the *required permissions* to this application.

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

1. From the **Region** drop-down list, select a Microsoft Azure region.
2. In the **Name** field, enter a name that you want to use to register a new Azure AD application in your Azure Active Directory.
3. Click **Install** to specify an SSL certificate that you want to use for data exchange between Restore Portal and the created Azure AD application.
4. In the **Select Certificate** wizard, select a certificate. For more information, see *Installing SSL Certificates*.
   You can generate a new self-signed certificate or use an existing one. Before using an existing certificate, make sure to register this certificate in Azure Active Directory. For more information, see *this Microsoft article*. When generating a new self-signed certificate, Veeam Backup for Microsoft 365 will register it automatically.
5. In the **Restore Portal web address** field, specify web address of a computer with Veeam Backup for Microsoft 365 REST API component installed. Restore operators and end users will use this web address to open Restore Portal in a web browser window.
Consider the following:

- The website is available over HTTPS protocol only.
- By default, port 4443 must be opened on the Veeam Backup for Microsoft 365 server or a computer with Veeam Backup for Microsoft 365 REST API component installed. For more information, see Used Ports.
- The web address must be specified in one of the following formats:
  - \texttt{https://<IPv4 address>:<port number>}, where \texttt{<IPv4 address>} is a public IPv4 address of a computer with Veeam Backup for Microsoft 365 REST API component installed. For example, \texttt{https://135.169.170.192:4443}.
  - \texttt{https://<DNS hostname>:<port number>}, where \texttt{<DNS hostname>} is DNS hostname of a computer with Veeam Backup for Microsoft 365 REST API component installed. For example, \texttt{https://portal.abc.com:4443}.

### Configuring Existing Azure AD Application

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

To configure an existing application, do the following:

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

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

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

   You can find this number in the application settings of your Azure Active Directory. For more information, see this Microsoft article.

3. Click **Install** to specify an SSL certificate that you want to use for data exchange between Restore Portal and the created Azure AD application.
4. In the **Select Certificate** wizard, select a certificate. For more information, see the [Installing SSL Certificates](#) article. You can generate a new self-signed certificate or use an existing one. Before using an existing certificate, make sure to register this certificate in Azure Active Directory. For more information, see the [Microsoft article](#). When generating a new self-signed certificate, Veeam Backup for Microsoft 365 will register it automatically.

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

Consider the following:

- The website is available over HTTPS protocol only.
- By default, port **4443** must be opened on the Veeam Backup for Microsoft 365 server or a computer with Veeam Backup for Microsoft 365 REST API component installed. For more information, see the [Used Ports](#) article.
- The web address must be specified in one of the following formats:
  - `https://<IPv4 address>:<port number>`, where `<IPv4 address>` is a public IPv4 address of a computer with Veeam Backup for Microsoft 365 REST API component installed. For example, `https://135.169.170.192:4443`.
  - `https://<DNS hostname>:<port number>`, where `<DNS hostname>` is DNS hostname of a computer with Veeam Backup for Microsoft 365 REST API component installed. For example, `https://portal.abc.com:4443`.

### Configure Application

**Region:**

- *Default*

**Application ID:**

- `D575e56a10e-46f9-1b90-2f6103aebc0`

**Certificate to authenticate with Azure AD:**

- `D1A093978959DD56AC7CE78DD6F022A5AFC1AA`

**Restore Portal web address:**

- `https://portal.abc.com:4443`
Step 4. Log In to Microsoft 365

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

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

1. Click **Copy code** to copy an authentication code.
   
   Mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.

2. Click the Microsoft authentication portal link.
   
   A web browser window opens.

3. On the **Sign in to your account** webpage, paste the code that you have copied and sign in to Microsoft Azure.
   
   Make sure to sign in with the user account that has the *Global Administrator* role. For more information about this role, see [this Microsoft article](#).

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

![Configure Application](image)
Notification Settings

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

**NOTE**
Consider the following:

- Only basic authentication on an SMTP server is supported. To authenticate MFA-enabled user accounts, Veeam Backup for Microsoft 365 needs an app password.
- Notifications about the backup job results are sent by a backup proxy server specified in the properties of the backup job. For more information, see Specify Backup Proxy and Repository.

To configure email notifications, do the following:

1. In the main menu, click **General Options**.
2. Open the **Notifications** tab.
3. Select the **Enable email notifications** check box.
4. Specify the address of a server that you want to use as an SMTP server.
5. To provide advanced settings, click **Advanced** and specify the following:
   - A port number of an SMTP server you want to use.
     - By default, Veeam Backup for Microsoft 365 establishes a connection to the `smtp.office365.com` server over port `587`. For more information, see this Microsoft article.
   - Select the **Connect Using SSL** check box to establish a secure connection.
   - Select the **The SMTP server requires authentication** check box and provide authentication credentials.
6. In the **From** field, specify the email address to be shown as a sender.
7. In the **To** field, specify the email address of a notification recipient.
   - To specify multiple email addresses, use semicolon.
8. Edit a notification subject, if needed.

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

   where:
   - \%JobResult\%. A backup job result (*Success*, *Warning*, *Failed*).
   - \%OrgName\%. A Microsoft 365 organization for which the job was configured.
   - \%JobName\%. The backup job name.
   - \%ObjectCount\%. The number of processed items.
   - \%Issues\%. The number of items with *Failed* or *Warning* states.
   - \%Time\%. Date and time of backup job completion.
9. From the **Attachment** drop-down list, select whether to include a detailed report as an attachment to the email notification. This setting applies to notifications about backup jobs that process more than 1000 objects.

   - Select **Include detailed report as an attachment** if you want to include a detailed report as an email attachment. If you select this option, Veeam Backup for Microsoft 365 will provide a summary about the backup job results in the notification body and a detailed report for each object processed by the job in the email attachment.
   
   - Select **Do not include detailed report** if you do not want to include a detailed report as an email attachment. If you select this option, email notifications will only contain a summary about the job results in the notification body.

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

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

   - **Notify on success**
   
   - **Notify on warning**
   
   - **Notify on failure**

11. [Optional] If a backup job is configured to perform retry attempts, select the **Suppress notifications until the last retry** check box to send email notifications only after the last attempt.

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

13. Click **OK**.
Security Settings

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

To configure security settings, do the following:

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

2. Open the **Security** tab.

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

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

4. Click OK.

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

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

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

- **Backup as a Service for Microsoft 365.** In this scenario, tenants authenticate to Veeam Backup for Microsoft 365 server with Microsoft organization credentials.
  
  Enabling tenant authentication is required for users from tenant organizations to view and restore backups that are located on the service provider side. For more information, see Enabling tenant authentication.

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

  Enabling restore operator authentication is required if you want to configure Restore Portal. For more information, see Enabling restore operator authentication.

**NOTE**

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

Enabling Tenant Authentication

To enable tenant authentication, do the following:

1. In the main menu, click General Options.
2. Open the Authentication tab.
3. Select the Enable tenants authentication with organization credentials check box.
4. Click Install to specify an SSL certificate.
   
   You can generate a new certificate or select an existing certificate using the Select Certificate wizard. For more information, see Installing SSL Certificates.

5. Click OK.

**TIP**

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

Enabling Restore Operator Authentication

To enable restore operator authentication, do the following:

1. In the main menu, click General Options.
2. Open the Authentication tab.
3. Select the **Enable restore operator authentication with Microsoft credentials** check box.

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

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

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

   **NOTE**

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

5. Click **OK**.
New Versions and Automatic Updates

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

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

1. In the main menu, click **General Options**.
2. Open the **Updates** tab.
3. Select the **Automatically check and notify me on available updates** check box.
   - If you select this check box, Veeam Backup for Microsoft 365 will notify you about available updates with a dialog message in the user interface.
4. Select the following check boxes:
   - **Allow for automatic updates**. If you select this check box, Veeam Backup for Microsoft 365 will regularly check Veeam servers for critical updates. If a new critical update is available, Veeam Backup for Microsoft 365 will notify you about available update with an email message, download this update in the background and install it to the backup infrastructure components.
   - **Send email notification on available updates**. If you select this check box, Veeam Backup for Microsoft 365 will notify you about available updates with an email message.
   - For sending email notifications, Veeam Backup for Microsoft 365 uses the recipient address and the SMTP server settings specified in the email notification settings. For more information, see **Notification Settings**.
5. Click **OK**.
For information on how to update Veeam Backup for Microsoft 365, see Updating Veeam Backup for Microsoft 365.

<table>
<thead>
<tr>
<th>Options</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Folders</td>
<td>History</td>
<td>REST API</td>
<td>Restore Portal</td>
<td>Updates</td>
<td>Internet Proxy</td>
</tr>
<tr>
<td>Security</td>
<td>Authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Automatically check and notify me on available updates
- Allow for automatic updates
- Send email notification on available updates

[Options]

[OK] [Cancel] [Apply]
Global Internet Proxy Server Settings

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

**NOTE**

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

To set an internet proxy server, do the following:

1. In the main menu, click **General Options**.
2. Open the **Internet Proxy** tab.
3. Select the **Use the following internet proxy settings** option.
4. In the **Host** field, specify a server that has access to the internet and which you want to use as your internet proxy.
   
   You can provide a DNS or IP address of a server.
5. In the **Port** field, provide a port number over which to connect to the specified server.
6. Select the **Use authentication** check box to provide authentication credentials to access the internet proxy server.
7. Click **OK**.
TIP

Also, you can configure an internet proxy server for each of your backup proxies. For more information, see Configuring Internet Proxy Server for Backup Proxies.
Configuring REST API and Restore Portal on Separate Computer

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

1. Open the Veeam Backup for Microsoft 365 REST API component installation folder.
   By default, Veeam Backup for Microsoft 365 REST API component is installed to the C:\Program Files\Veeam\Backup365 folder.

   The Veeam Backup for Microsoft 365 window opens.

3. Configure REST API settings. For more information, see Configuring REST API Settings.

4. Configure Restore Portal settings. For more information, see Configuring Restore Portal Settings.

5. Click Apply.

6. Click OK to close the Veeam Backup for Microsoft 365 window.

Configuring REST API Settings

On the REST API tab, do the following:

1. Select the Enable REST service check box.

2. In the Authentication token lifetime field, specify the lifetime value for an authentication token (in minutes).
   REST API authorization is based on the OAuth 2.0 Authorization Framework.

3. In the HTTPS port field, specify a port number which Veeam Backup for Microsoft 365 use to access the Veeam Backup for Microsoft 365 RESTful API Service.

4. In the Controller host field, specify a DNS name or IP address of the Veeam Backup for Microsoft 365 server.

5. Click Install to specify an SSL certificate.
   You can generate a new certificate or select an existing certificate using the Select Certificate wizard. For more information, see Installing SSL Certificates.
NOTE
If you have generated a new self-signed certificate for restore operators, you must import the certificate for restore operators to the Trusted Root Certification Authorities certificate store on the separate computer with REST API installed.

Configuring Restore Portal Settings

On the Restore Portal tab, do the following:

1. Select the Enable Restore Portal check box.

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

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

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

   You can find this identification number in the application settings of your Azure Active Directory. For more information, see this Microsoft article. Make sure to manually grant the required permissions to your Azure AD application.

4. In the Application certificate section, click Install to specify an SSL certificate that you want to use for data exchange between Restore Portal and the specified Azure AD application.

   You can generate a new certificate or select an existing certificate using the Select Certificate wizard. For more information, see Installing SSL Certificates.
NOTE

If you generated a new self-signed certificate for the specified Azure AD application, you must add this certificate in the application settings of your Azure Active Directory.
SSL Certificates Overview

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

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

<table>
<thead>
<tr>
<th>Usage Scenario</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Managing Microsoft 365 Organization</strong></td>
<td>Required to establish communication and data exchange between Veeam Backup for Microsoft 365 and Azure AD application when adding Microsoft 365 organizations.</td>
<td>For more information, see Microsoft 365 Organizations.</td>
</tr>
<tr>
<td></td>
<td>Required to establish communication and data exchange between Veeam Backup for Microsoft 365 and Azure AD application when configuring backup applications.</td>
<td>For more information, see Backup Applications.</td>
</tr>
<tr>
<td><strong>Communicating with Backup Proxy Server</strong></td>
<td>Required to establish communication and data exchange between the Veeam Backup for Microsoft 365 server and a backup proxy server deployed in a workgroup.</td>
<td>For more information, see Security Settings.</td>
</tr>
</tbody>
</table>
| **Communicating with REST API on Veeam Backup for Microsoft 365 server** | Required to establish communication and data exchange between the following:  
  - Veeam Backup for Microsoft 365 RESTful API Service and the Veeam Backup for Microsoft 365 server  
  - Restore Portal and Veeam Backup for Microsoft 365 | For more information, see REST API Settings. |
| **Communicating with REST API on Separate Computer** | Required to establish communication and data exchange between the following:  
  - Veeam Backup for Microsoft 365 RESTful API Service and the Veeam Backup for Microsoft 365 server  
  - Restore Portal and Veeam Backup for Microsoft 365 | For more information, see Configuring REST API and Restore Portal on Separate Computer. |
<table>
<thead>
<tr>
<th>Usage Scenario</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Communicating with Restore Portal</strong></td>
<td>Required to establish communication and data exchange between the Veeam Backup for Microsoft 365 server, Microsoft 365 organization, Azure AD application, the <em>Veeam Backup for Microsoft 365 RESTful API Service</em> and Restore Portal.</td>
<td>For more information, see <em>Restore Portal Settings</em>, Configuring REST API and Restore Portal on Separate Computer, How Restore Portal Works.</td>
</tr>
<tr>
<td><strong>Authenticating Restore Operators to Veeam Backup for Microsoft 365 server</strong></td>
<td>Required to authenticate restore operators to Veeam Backup for Microsoft 365 with Microsoft 365 credentials and encrypt network traffic between <em>Veeam Backup for Microsoft 365 Service</em> and <em>Veeam Backup for Microsoft 365 RESTful API Service</em>.</td>
<td>For more information, see <em>Authentication Settings</em>.</td>
</tr>
<tr>
<td><strong>Authenticating Tenants to Veeam Backup for Microsoft 365 in Service Provider Infrastructure</strong></td>
<td>Required to authenticate tenants to Veeam Backup for Microsoft 365 with Microsoft organization credentials.</td>
<td>For more information, see <em>Authentication Settings</em> and Backup as Service for Microsoft 365.</td>
</tr>
</tbody>
</table>
Installing SSL Certificates

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

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

![Select Certificate Wizard](image-url)
Generating New Certificate

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

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

To import a certificate, do the following:

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

![Select Certificate dialog](image)

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

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

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

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

- **Object storage repositories**
  Object storage repositories are cloud-based and on-premises storage systems that you can employ to keep your backup data. Also, you can use Azure Blob Storage Archive access tier, Amazon S3 Glacier and Amazon S3 Glacier Deep Archive storage classes as a target for backup copy jobs.
Backup Proxy Servers

A backup proxy server is an architecture component used to leverage network traffic when backing up or restoring data.

Consider the following:

- By default, the role of the backup proxy server is assigned to the machine where Veeam Backup for Microsoft 365 is installed. The default backup proxy server is displayed as Local backup proxy in Veeam Backup for Microsoft 365.
  
  After you install Veeam Backup for Microsoft 365, you should configure an additional set of backup proxy servers to manage your data in a more efficient manner.

- A backup proxy server can be a physical or virtual machine.

- Veeam Backup for Microsoft 365 automatically installs the Veeam Backup Proxy for Microsoft 365 Service on a computer that you want to use as a backup proxy server when you add a backup proxy server to the Veeam Backup for Microsoft 365 backup infrastructure. For more information, see Adding Backup Proxy Servers.

- Veeam Backup for Microsoft 365 allows you to deploy the following types of backup proxy servers:
  - Domain backup proxy
  - Workgroup backup proxy

  For more information, see Backup Proxy Deployment Scenarios.

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

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

- A backup proxy server is responsible for sending email notifications about backup job completion results.
  
  To send email notifications, backup proxy servers use an SMTP server. For more information about configuring an SMTP server, see Notification Settings.

Backup Proxy Deployment Scenarios

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

- **Scenario 1. Domain backup proxy**
  
  In this scenario, a machine used as a backup proxy server resides in the same domain as the Veeam Backup for Microsoft 365 server or in a trusted domain. To establish a connection with a domain backup proxy, Veeam Backup for Microsoft 365 uses credentials that you provide when you add a backup proxy server to the Veeam Backup for Microsoft 365 infrastructure.

- **Scenario 2. Workgroup backup proxy**
  
  In this scenario, a machine used as a backup proxy server resides in a workgroup. To establish a connection with a workgroup backup proxy, Veeam Backup for Microsoft 365 uses an SSL certificate. For more information, see Security Settings.
Adding Backup Proxy Servers

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

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

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

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

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

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

   If the specified computer does not have a direct access to the internet, you can **configure an internet proxy server** for such a computer.

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

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

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

   **NOTE**

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

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

![Backup Proxy Configuration](image-url)
Step 3. Specify Credentials

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

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

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

- For a domain backup proxy, Veeam Backup for Microsoft 365 uses credentials for entire communication with the backup proxy server.

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

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

Editing Backup Proxy Server Settings

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

To edit backup proxy server settings, do the following:

1. Open the Backup Infrastructure view.
2. In the inventory pane, select the Backup Proxies node.
3. In the preview pane, do one of the following:
   - Select a backup proxy server and on the Backup Proxy tab, click Edit Proxy on the ribbon.
   - Right-click a backup proxy server and select Edit.
4. Modify the required settings.
   You can change the following parameters:
   - The port number to access the backup proxy server computer.
   - Description.
   - User credentials to connect this backup proxy.

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

**Rescanning Backup Proxy Servers**

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

To rescan a backup proxy server, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Backup Proxies** node.
3. In the preview pane, do one of the following:
   - Select a backup proxy server and on the **Backup Proxy** tab, click **Rescan** on the ribbon.
   - Right-click a backup proxy server and select **Rescan**.
If you want to rescan all backup proxy servers in your environment, right-click the **Backup Proxies** node and select **Rescan**.

To upgrade backup proxy servers, do the following:

1. Launch the **Proxy Upgrade** wizard.
2. Select a backup proxy server to upgrade.
3. Specify credentials.
Step 1. Launch Proxy Upgrade Wizard

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

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

If you want to upgrade all backup proxy servers at the same time, right-click the **Backup Proxies** node and click **Upgrade**.
Step 2. Select Backup Proxy Server to Upgrade

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

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

![Proxy Upgrade Window](image)

Select proxy servers to upgrade

<table>
<thead>
<tr>
<th>Server</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ 172.17.55.105</td>
<td>Workgroup</td>
</tr>
</tbody>
</table>

[Back] [Next] [Cancel]
Step 3. Specify Credentials

At this step of the wizard, enter user credentials to connect to the backup proxy server. The account must be a member of the *Local Administrator* group.

![Proxy Upgrade](image)

- Specify credentials to connect to proxy servers:
  - Use current account (SRV01\Administrator)
  - Use the following account:
    - Username: SRV01\Administrator
    - Password: ************

Removing Backup Proxy Servers

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

Consider the following:

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

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

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

Modifying Backup Proxy Server Properties

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

To configure backup proxy server properties, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Backup Proxies** node.
3. In the preview pane, right-click a backup proxy server, select **Properties** and proceed to:
   - Configuring Threads and Network Bandwidth
   - Configuring Internet Proxy Server for Backup Proxies
NOTE
The Properties option is unavailable if a backup proxy server needs to be upgraded. For more information about upgrading backup proxy servers, see Upgrading Backup Proxy Servers.

Configuring Threads and Network Bandwidth

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

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

1. On the General tab, do the following:
   - In the Set the number of threads to field, specify the allowed number of threads.
     A thread defines the total number of proxy server threads that are responsible for handling data transfer to/from backup repositories. By default, 64 threads are used. Depending on your environment configuration and capacities (low CPU or RAM deficiency), running too many threads may significantly reduce the efficiency due to possible throttling errors or connection failures. As every production environment operates under different equipment capacity, Veeam Backup for Microsoft 365 allows you to explicitly define the number of threads that your infrastructure is potentially able to handle without losing performance.
   - Select the Throttle network traffic to check box and specify the average download speed.
     For example, if you have set this value to 10 Mbps and have downloaded 100 Mb in 8 seconds, Veeam Backup for Microsoft 365 will stop retrieving new data for approximately 2 minutes after which download will be resumed automatically. The exact time for which Veeam Backup for Microsoft 365 stops getting data is calculated by predefined algorithms and depends upon the value that you specify as traffic throttling, the amount of downloaded data and the amount of time it took to get this data.
2. Click **OK**.

![Backup Proxy Properties dialog box](image)

Configuring Internet Proxy Server for Backup Proxies

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

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

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

2. Click **OK**.
**NOTE**

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

<table>
<thead>
<tr>
<th>General</th>
<th>Internet Proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Do not use internet proxy</td>
</tr>
<tr>
<td></td>
<td>Use internet proxy settings from the management server</td>
</tr>
<tr>
<td></td>
<td>Use the following internet proxy settings</td>
</tr>
<tr>
<td>Host</td>
<td>delta.tech.local</td>
</tr>
<tr>
<td>Port</td>
<td>3128</td>
</tr>
<tr>
<td></td>
<td>Use authentication:</td>
</tr>
<tr>
<td>Username</td>
<td>Administrator</td>
</tr>
<tr>
<td>Password</td>
<td>*************</td>
</tr>
</tbody>
</table>

![Backup Proxy Properties](#)
Backup Repositories

A backup repository is a storage system where you can keep backups created by your backup jobs. Veeam Backup for Microsoft 365 uses Extensible Storage Engine (ESE) databases, also known as JET Blue, to store backed-up data.

You can add the following types of backup repositories to the Veeam Backup for Microsoft 365 infrastructure:

- A local directory on a backup proxy server.
  A default backup repository is the `C:\VeeamRepository` directory on a computer with Veeam Backup for Microsoft 365.
- Direct Attached Storage (DAS) connected to the backup proxy server.
- Storage Area Network (SAN).
  A backup server must be connected to the SAN fabric using hardware, virtual HBA or software iSCSI initiator.
- Network Attached Storage (SMB shares version 3.0 or later).
  Experimental support.

**NOTE**
Consider the following:

- Veeam Backup for Microsoft 365 does not support encryption at-rest for these types of backup repositories.
- You can store your backups on volumes encrypted using the BitLocker technology if it applies to your system. After encryption, the I/O rate of the volume may change.

About Backup Repository Structure

In a backup repository, all backed-up items are stored in a way that each item belongs to a separate folder named after the year when the item has been modified.

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

**NOTE**
If a backup repository is extended with object storage, only cache will be saved to such an extended backup repository.
Consider the following example. A Microsoft organization owns a mailbox that contains 3 email items; each item has been modified on a different date (10:00 AM on 9/1/2016, 10:20 AM on 11/11/2017 and 3:20 PM on 12/21/2018). To protect these items, you configure a backup job that stores backed-up files in a specific backup repository. When running backup job sessions, Veeam Backup for Microsoft 365 adds items to the backup repository in the following way:

- **During the initial backup job session,** Veeam Backup for Microsoft 365 collects all data from the Microsoft organization and saves the data to folders in the backup repository.

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

- **During subsequent backup job sessions,** Veeam Backup for Microsoft 365 backs up only those email items that were changed since the last backup job session.

  This means that if the organization receives a new email item at 7:28 PM on 12/21/2018, and no other items change since the initial backup job session, Veeam Backup for Microsoft 365 will back up only the new item — and save the data to the `repository.adb` file in the 2018 repository folder.

**NOTE**

Although the example describes only Microsoft Exchange items, the same approach applies to Microsoft SharePoint items, Microsoft OneDrive for Business items and Microsoft Teams items.
About Retention Policy

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

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

- **Snapshot-Based Retention**
  Select this type if you want to keep an item until the restore point of an item's version is within the retention coverage.

- **Item-Level Retention**
  Select this type if you want to keep an item until its creation time or last modification time is within the retention coverage.

Item-Level Retention

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

The following is an example that demonstrates three backup files; each file contains Microsoft 365 items per year where each item has its own last modification time.

For example, your retention policy is said to be applied at 10:20 AM on September 1, 2018. In such a scenario, Veeam Backup for Microsoft 365 will remove the *Item 1* from the *Backup 1* repository because the *Item 1* exceeds the retention period (2 years in our example) by 20 minutes.

The next item to be removed is the *Item 2* because its last modifications were made at 10:20 AM on November 11, 2016. That said, when a retention policy is being applied, for example, at 10:30 AM on November 11, 2018, Veeam Backup for Microsoft 365 removes the *Item 2* because its age equals 2 years and 10 minutes which exceeds the specified threshold.

The same is repeated until no items left in a repository. After that, Veeam Backup for Microsoft 365 completely removes such a repository from the hard drive.

**NOTE**

Backup jobs do not process items the last modification time of which exceeds the specified retention period.
Snapshot-Based Retention

Each item in a backup file may have its own different versions. A different version means that the user could have changed any attribute of an item 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.

When a retention policy is applied in backup repositories with the snapshot-based retention type, Veeam Backup for Microsoft 365 removes versions of an item, but not an item itself. Data removal from backup occurs every time the restore point of an item's version in a backup file goes beyond the retention coverage. Eventually, if no more changes were made to an item, Veeam Backup for Microsoft 365 will remove all versions of an item except the latest one. The latest versions and items that were never changed stay in a backup repository with the snapshot-based retention type forever.

The following example represents two backup files consisting of three items each, where each item has its own backup date. Consider the Item 1 of Backup 1 storage to be an email message, the attributes of which have been modified three times in the production environment; each modification was made on different days (Mon, Tue, and Wed) and each modification was successfully backed up.

That said, there are three different versions of the Item 1 in a backup repository.

According to the example, if the retention policy is 1 year and said to be applied at 10:00 AM on September 12, 2018, then all the item versions that exceed the specified retention threshold will be removed from the backup repository. These versions are the Version 1 and Version 2.

The Version 3 is the latest and if no more versions will be created for the Item 1, it will be kept in Backup 1 storage along with initial versions of Item 2 and Item 3.

**NOTE**

Backup jobs process all available items regardless of their creation time or last modification time.

Removing Items After Unsuccessful Backup Attempts

If during the subsequent backup job sessions Veeam Backup for Microsoft 365 fails to back up organization mailboxes, Microsoft SharePoint items, Microsoft OneDrive for Business items, or Microsoft Teams items, the product preserves the latest backup state of such items until the next successful backup is created.
The following is an example that demonstrates a backup of the mailbox A which is followed by 6 consecutive unsuccessful attempts (B through G) of backing up that same mailbox during the subsequent backup job sessions. The mailbox A will not be removed until this mailbox is successfully backed up during the attempt H.

Removing Restore Points

Each version of an item can have its own restore point. The restore points of items are removed as soon as they are out of the retention coverage. Once the latest available restore point is removed, the parent item of such a restore point will be removed as well.

Consider the following example with four items (A through D) and two restore points (A1 and A2) both of which belong to the item A. The A1 restore point has already been removed since it was out of the retention scope, whereas the A2 restore point will only be removed after it goes out of the retention coverage (Example 1).

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

Backup Job Idleness

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

The following is an example in which the mailbox A has been removed because it was already out of the retention scope (Example 1), and the next mailbox to be removed is the mailbox B, the removal of which will happen once it goes beyond the retention coverage (Example 2).
The same is applicable to Microsoft SharePoint, Microsoft OneDrive for Business and Microsoft Teams.

### Direct Attached Storage (DAS)

In Veeam Backup for Microsoft 365, you can use the following Microsoft Windows and Linux-based storage types as backup repositories:

- A Windows-based server with local or directly attached storage.
  
  Such storage can be a local disk, directly attached disk-based storage (such as a USB hard drive), or iSCSI/FC SAN LUN in case the server is connected into the SAN fabric.

- Linux-based storage connected to the Veeam Backup for Microsoft 365 server.
  
  Such storage can be a local disk, directly attached disk-based storage (such as a USB hard drive), NFS share, or iSCSI/FC SAN LUN in case the server is connected into the SAN fabric. The storage must then be provisioned to the Windows-based server VM as a volume in the guest OS.

### Network Attached Storage (SMB Shares)

Veeam Backup for Microsoft 365 allows you to use network attached storage (NAS) as backup repositories. Such NAS can be a shared folder on your computer, or any other physical device that can be accessed using the Server Message Block (SMB) protocol.

Consider the following:

- Network share browsing is not supported; make sure to prove the path to the shared folder manually.
- A shared folder must be on a computer or device located within the same or a trusted domain.
- To use SMB 3.0 or later, make sure you are using Microsoft Windows 8 or later or Microsoft Windows Server 2012 or later. Mind that Network Attached Storage repository is on experimental support.

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

- Configure NTFS permissions.
- Configure share permissions.

For more information, see this Veeam article.

After you share a folder, you can access it using the SMB 3.0 protocol to read/write data to/from this folder.
To add a shared folder as a backup repository, in the Specify Backup Proxy Server step, in the Path field, specify the path to the shared folder using the following syntax: \\<FQDN_name> or <ip_address>\\<shared_folder_name>.

Adding Backup Repositories

To add a new backup repository, do the following:

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

To launch the New Backup Repository wizard, do the following:

1. Open the Backup Infrastructure view.
2. In the inventory pane, select the Backup Repositories node.
3. Do one of the following:
   - On the Backup Repository tab, click Add Repository on the ribbon.
   - Right-click the Backup Repositories node and select Add backup repository.
Step 2. Specify Backup Repository Name

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

1. In the **Name** field, enter a name for the backup repository.
2. In the **Description** field, enter optional description.

![Backup Repository Details](image)
Step 3. Specify Backup Proxy Server

At this step of the wizard, select a backup proxy server and specify a directory where you want to store backups.

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

1. From the Backup proxy drop-down list, select a backup proxy server. For more information, see Backup Proxy Servers.

2. In the Path field, specify a directory to store your backup data. Click Browse to select a directory.
   
   When planning to extend a backup repository with object storage, this directory will only be keeping cache consisting of required metadata. For more information, see About Cache. The actual data will be compressed and backed up directly to object storage that you specify at the next step.
   
   When specifying a directory that already contains cache, at the next step, make sure to select the same exact object storage repository for which this cache was created.

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

**NOTE**

To use a shared folder, provide the path manually. For more information about shared folders, see Network Attached Storage (SMB Shares).
Step 4. Specify Object Storage Repository

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

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

Consider the following:

- You cannot extend a backup repository with object storage which is already an extension to another backup repository.
- Extending an existing backup repository is not possible.
- If object storage that you select contains offloaded backup data, you will be offered to synchronize required metadata (cache) of such offloaded backups with the backup repository that is being added.
  
  If you skip synchronization, the backup repository will be added with the Out of Sync state. To use such a repository, make sure to synchronize it manually. For more information, see Synchronizing Repositories.
- If object storage that you select contains encrypted data, make sure to provide the same exact password with which this data was encrypted. Otherwise, the addition of object storage will not be possible.
- Removing object storage from the backup repository configuration is not possible after the backup repository was extended with object storage.

To extend a backup repository with object storage, do the following:

1. Select the **Offload backup data to object storage** check box.
2. From the drop-down list, select an object storage repository to which you want to offload your data.

   Make sure that an object storage repository has been added to your environment in advance. Otherwise, click Add and follow the steps of the wizard. For more information on how to add an object storage repository, see Adding Object Storage Repositories.
3. Select the **Encrypt data uploaded to object storage** check box to encrypt the offloaded data.
4. From the **Password** drop-down list, select an encryption password.

   If you already have a password record that was configured beforehand, select such a record from the drop-down list. Otherwise, click Add and add an encryption password. For more information, see Managing Encryption Passwords. You can also click Manage passwords to manage existing password records.

   A password can be changed at any time. A password change does not impose any restrictions on accessing existing backup data in object storage.
IMPORTANT
Make sure to remember your password because, if lost, it cannot be restored.

Object storage backup repository

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

- [ ] Offload backup data to object storage

- [x] Encrypt data uploaded to object storage

Password:

Add...
Step 5. Specify Retention Policy Settings

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

To specify retention settings, do the following:

1. From the Retention policy drop-down list, choose how long your data should be stored in a backup repository.

2. Select a retention type:
   - **Snapshot-based retention.**
     Select this type if you want to keep an item until the restore point of an item’s version is within the retention coverage.
   - **Item-level retention.**
     Select this type if you want to keep an item until its creation time or last modification time is within the retention coverage.

3. Click Advanced if you want to specify when to apply a retention policy. You can select the following options:
   - **Daily at**
     Select this option if you want a retention policy to be applied on a daily basis and choose the time and day.
   - **Monthly at**
     Select this option if you want a retention policy to be applied on a monthly basis and choose the time and day which can be the first, second, third, fourth or even the last one in the month.
Consider the following:

- The retention type of a backup repository cannot be changed once set.
- The retention type of a backup repository cannot be modified when extending a repository with object storage that contains offloaded backup data.

    In such a scenario, the retention type will be inherited from that of object storage that you have selected at the previous step of the wizard.
- A retention policy configured in this step removes outdated restore points located in object storage repositories.

**New Backup Repository**

Specify retention policy settings

Retention policy

3 years

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

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

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

Advanced

**Back**  **Finish**  **Cancel**

**Editing Backup Repository Settings**

Veeam Backup for Microsoft 365 allows you to edit backup repository settings.

Consider the following:

- Editing the **Backup proxy** and **Path** values is not possible after the repository was created.
- Extending a backup repository with object storage is not possible after the backup repository was added to the Veeam Backup for Microsoft 365 backup infrastructure.

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

- Removing object storage from the backup repository configuration is not possible after the backup repository was extended with object storage.
- The retention type of a backup repository cannot be changed once set.

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

    For information on how to upgrade a backup repository, see Upgrading Backup Repositories.
To edit backup repository settings, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Backup Repositories** node.
3. In the preview pane, do one of the following:
   - Select a backup repository and on the **Backup Repository** tab, click **Edit Repository** on the ribbon.
   - Right-click a backup repository and select **Edit**.
4. Modify the required settings.
   You can change the following parameters:
   - The backup repository name and description.
   - Frequency of applying the retention policy.

**Removing Backup Repositories**

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

Consider the following:

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

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

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Backup Repositories** node.
3. In the preview pane, do one of the following:
   - Select a backup repository and on the **Backup Repository** tab, click **Remove Repository** on the ribbon.
   - Right-click a backup repository and select **Remove**.

---

### Upgrading Backup Repositories

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

To upgrade backup repositories, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Backup Repositories > Out of Date** node.
3. In the preview pane, do one of the following:
   - Select a backup repository and on the **Backup Repository** tab, click **Upgrade Repository** on the ribbon.
   - Right-click a backup repository and select **Upgrade**.
Synchronizing Repositories

The **Synchronize Repository** option allows you to synchronize cache between object storage and extended backup repositories.

Such synchronization is required when an extended backup repository has the **Out of Sync** state. This state is assigned if you skip synchronization during **extension** of a backup repository with object storage.

Once cache is synchronized, you can do the following:

- Open and restore data from backups located in object storage.
  
  Backups located in object storage become available for browsing and restore. For more information, see [Exploring Single Organization](#) and [Exploring All Organizations](#).

- Create new backups and offload these backups to object storage. For more information, see [Data Backup and Backup Copy](#).

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

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Backup Repositories > Out of Sync** node.
3. In the preview pane, do one of the following:
   - Select a backup repository and on the **Backup Repository** tab, click **Synchronize Repository** on the ribbon.
   - Right-click a backup repository and select **Synchronize**.

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

If you want to stop synchronization, click **Stop Sync** on the ribbon.
About Invalid State

In Veeam Backup for Microsoft 365, a backup repository can be put into an *Invalid* state in any of the following cases:

- Local cache on an extended backup repository is different from that in object storage.
  
  A cache state is verified by comparing timestamps and an identification number of the associated backup and proxy repositories; these values must be identical to each other.

- A repository lock in object storage is missing.
  
  A repository lock is imposed by the backup proxy server and prevents such locked object storage from being added as an extension to any other backup repository configuration. A lock file is saved to the `RepositoryLock` directory. For more information, see *About Object Storage Repository Structure*.

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

- If any of the following is true for extended backup repositories:
  
  o A connection to object storage is missing.
  
  o A container/bucket is missing or has been renamed.
  
  o A repository folder is missing or has been renamed.

- A connection to DAS or NAS is missing.
  
  Such an invalid backup repository becomes available after your DAS or NAS is online.

Once a repository is put into an *Invalid* state, restore or backup from/to such a repository is impossible.
Invalid backup repositories can be found in the **Backup Infrastructure** view under the **Backup Repositories** > **Invalid** node.
Object Storage Repositories

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

- **S3 Compatible object storage**
  
  Any S3 Compatible object storage device fully compatible with the AWS S3 operations and AWS S3 Signature Version 4 standard.

- **Amazon S3 object storage**
  
  For more information about Amazon S3 object storage, see [this Amazon article](#). For more information about Amazon S3 storage classes that Veeam Backup for Microsoft 365 supports, see [Supported Amazon S3 Storage Classes](#). For more information about required permissions, see [Amazon S3 Storage Permissions](#).

- **Microsoft Azure Blob storage**
  
  For more information about Microsoft Azure Blob storage, see [this Microsoft article](#). For more information about Azure storage account types that Veeam Backup for Microsoft 365 supports, see [Supported Azure Storage Account Types](#). For more information about Azure archive storage permissions, see [Azure Archive Storage Permissions](#).

- **IBM Cloud Object Storage**
  
  For more information about IBM Cloud Object Storage, see [this IBM article](#).

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

About Object Storage Repository Structure

Veeam Backup for Microsoft 365 creates and maintains the different structures for object storage repositories of the following types:

- **Non-Archive Storage**

- **Archive Storage**
Non-Archive Storage

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

The following table lists the structure that is created and maintained by Veeam Backup for Microsoft 365 in object storage.

<table>
<thead>
<tr>
<th>Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;bucket_name/container_name&gt;</code></td>
<td>A bucket or container name. Buckets and containers must be created in advance using the cloud provider tools. Veeam Backup for Microsoft 365 does not support creating new buckets or containers.</td>
</tr>
<tr>
<td><code>&lt;bucket_name/container_name&gt;/Veeam/Backup365/</code></td>
<td>A set of mandatory folders created by Veeam Backup for Microsoft 365.</td>
</tr>
<tr>
<td><code>&lt;repository_folder_name&gt;</code></td>
<td>A repository folder that you create when adding a new object storage repository. For more information on how to add a new object storage repository, see Adding Object Storage Repositories.</td>
</tr>
</tbody>
</table>
| `<repository_folder_name>/CommonInfo` | Contains the following directories and blob files:  
  - `[Directory] WebRestorePoints`. Contains information about available restore points for Microsoft SharePoint and OneDrive for Business. Both directories keep a blob file that contains a list of available restore points. Each blob may store up to 100,000 records after which another blob file is created.  
  - `[Blob file] Organizations`. Contains a list of backed-up organizations.  
  - `[Blob file] RepositoryConfig`. Contains extended backup repository configuration such as the retention type and other auxiliary information. |
<table>
<thead>
<tr>
<th>Directory</th>
<th>Description</th>
</tr>
</thead>
</table>
| **<repository_folder_name>/CriticalDataBackup** | Contains identical copies of the following blob files:  
  - *[Blob file] Organizations*. Contains a list of backed-up organizations.  
  - *[Blob file] RepositoryConfig*. Contains extended backup repository configuration such as the retention type and other auxiliary information.  
  - *[Blob file] BackupKeys*. Contains information about the encryption keys that you set during extension of a backup repository with object storage. |
| **<repository_folder_name>/Encryption** | Contains the *BackupKeys* blob file that holds information about the encryption keys that you set during extension of a backup repository with object storage.  
For more information on how to extend a backup repository with object storage, see Specify Object Storage Repository. |
| **<repository_folder_name>/Organizations** | The root folder that contains backed-up Microsoft organizations. Each organization is kept in its own folder with a unique identification number. |
| **Organizations/<organization_Id>** | The *<organization_Id>* directory contains the following blob files:  
  - *AccountMailbox*. Contains information required to load the backup contents into the Veeam Explorer for Microsoft Exchange scope.  
  - *AccountWeb*. Contains information required to load the backup contents into the Veeam Explorer for Microsoft SharePoint scope. |
<table>
<thead>
<tr>
<th>Directory</th>
<th>Description</th>
</tr>
</thead>
</table>
| "<organization_id>/Mailboxes/<mailbox_id>" | The Mailboxes directory contains backed-up Exchange mailboxes. Each mailbox is saved under a unique identification number to the &lt;mailbox_id&gt; directory.

The &lt;mailbox_id&gt; directory contains the following directories:

- **Folders**. Contains backed-up Exchange folders such as *Inbox*, *Drafts*, *Sent Items*, and other.
- **FoldersHistory**. Contains folder changes.

For example, you may have renamed a folder. In such a scenario, after the subsequent backup session, Veeam Backup for Microsoft 365 will update information about the renamed folders and save each new folder version to the FoldersHistory directory.

- **ItemsChanges**. Contains incremental backup data.
- **ItemsData**. Contains blob data of the backed-up Exchange messages.

For example, attachments are saved to this folder.

- **ItemsPreview**. Contains required data to load the backup contents into the Veeam Explorer for Microsoft Exchange scope.
- **PostsPreview**. Contains required data to load the backup contents into the Veeam Explorer for Microsoft Teams scope. |
<p>| &quot;&lt;organization_id&gt;/RestorePointObjects&quot; | Contains blob files with a list of objects (mailboxes, sites, and other) that were backed up by Veeam Backup for Microsoft 365 per a particular restore point at the specified point in time. |
| &quot;&lt;organization_id&gt;/Sites&quot; | Contains a blob file with a list of backed-up SharePoint sites. |</p>
<table>
<thead>
<tr>
<th>Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;organization_id&gt;/Teams</td>
<td>Contains the following directories:</td>
</tr>
<tr>
<td></td>
<td>- <em>Accounts</em>. Contains names and descriptions of all users included in all teams at the moment of the latest backup.</td>
</tr>
<tr>
<td></td>
<td>- <code>&lt;team_id&gt;</code>. Contains backed-up Microsoft Teams data such as <em>Channels</em>, <em>Tabs</em> and <em>Users</em>.</td>
</tr>
<tr>
<td></td>
<td>- <em>TeamHistorySnapshots</em>. Contains blob files with team changes and information about team <em>Applications</em> at the specified point in time.</td>
</tr>
<tr>
<td></td>
<td>- <em>TeamInfos</em>. Contains blob files with unchanged information about teams.</td>
</tr>
<tr>
<td>&lt;organization_id&gt;/WebData</td>
<td>Contains data that is required to restore SharePoint or OneDrive items.</td>
</tr>
<tr>
<td>&lt;organization_id&gt;/WebBackups</td>
<td>Contains a list of SharePoint sites to be loaded into the Veeam Explorer for Microsoft SharePoint scope.</td>
</tr>
<tr>
<td>&lt;organization_id&gt;/WebPreview</td>
<td>Contains backup dates of SharePoint sites.</td>
</tr>
<tr>
<td></td>
<td>Required for a snapshot-based retention policy.</td>
</tr>
<tr>
<td>&lt;organization_id&gt;/Webs/&lt;web_id&gt;</td>
<td>A set of folders that contain backed-up SharePoint sites and OneDrive Items.</td>
</tr>
<tr>
<td></td>
<td>The <code>&lt;web_id&gt;</code> directory contains the following directories:</td>
</tr>
<tr>
<td></td>
<td>- <em>Files</em>. Contains files of the SharePoint site.</td>
</tr>
<tr>
<td></td>
<td>- <em>Items</em>. Contains items such as those located under the <em>Subsites</em> and <em>Content</em> folders for SharePoint, and users folders for OneDrive.</td>
</tr>
<tr>
<td></td>
<td>- <em>Lists</em>. Contains SharePoint lists.</td>
</tr>
<tr>
<td></td>
<td>- <em>ListsData</em>. Contains properties of SharePoint lists.</td>
</tr>
<tr>
<td></td>
<td>- <em>ListViews</em>. Contains SharePoint list views.</td>
</tr>
<tr>
<td>&lt;repository_folder_name&gt;/RepositoryLock</td>
<td>Contains a lock file that tells that this storage is already an extension to a backup repository.</td>
</tr>
<tr>
<td></td>
<td>Object storage can only be owned by one owner (a backup repository) at a time.</td>
</tr>
<tr>
<td></td>
<td>For more information on how to extend a backup repository with object storage, see <a href="#">Specify Object Storage Repository</a>.</td>
</tr>
</tbody>
</table>
**Archive Storage**

You can use Azure Blob Storage Archive access tier, Amazon S3 Glacier and Amazon S3 Glacier Deep Archive storage classes as a target for backup copy jobs and create an instance of your backups in these archive object storage.

The following table lists the structure that is created and maintained by Veeam Backup for Microsoft 365 in archive object storage.

<table>
<thead>
<tr>
<th>Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;bucket_name/container_name&gt;</code></td>
<td>A bucket or container name. Buckets and containers must be created in advance using the cloud provider tools. Veeam Backup for Microsoft 365 does not support creating new buckets or containers.</td>
</tr>
<tr>
<td><code>&lt;bucket_name/container_name&gt;/Veeam/Backup365/</code></td>
<td>A set of mandatory folders created by Veeam Backup for Microsoft 365.</td>
</tr>
<tr>
<td><code>&lt;repository_folder_name&gt;</code></td>
<td>A repository folder that you create when adding a new object storage repository. For more information on how to add a new object storage repository, see Adding Object Storage Repositories.</td>
</tr>
</tbody>
</table>
| `<repository_folder_name>/CommonInfo` | Contains the following blob files:  
  - [Blob file] StorageStatistics. Contains information on used space in archive object storage per organization.  
  - [Blob file] RepositoryConfig. Contains extended backup repository configuration such as the retention type and other auxiliary information, as well as version of the blob file. |
| `<repository_folder_name>/CriticalDataBackup` | Contains identical copies of the following blob files:  
  - [Blob file] RepositoryConfig. Contains extended backup repository configuration such as the retention type and other auxiliary information, as well as version of the blob file.  
  - [Blob file] BackupKeys. Contains information about the encryption keys that you set during extension of a backup repository with object storage, as well as version of the blob file. |
<p>| <code>&lt;repository_folder_name&gt;/DataRetrievalsMetadata</code> | Contains information about backed-up data retrievals. |</p>
<table>
<thead>
<tr>
<th>Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;repository_folder_name&gt;/Encryption</code></td>
<td>Contains the <em>BackupKeys</em> blob file that holds information about the encryption keys that you set during extension of a backup repository with object storage, as well as version of the blob file. For more information on how to extend a backup repository with object storage, see <a href="#">Specify Object Storage Repository</a>.</td>
</tr>
<tr>
<td><code>&lt;repository_folder_name&gt;/OrganizationInfos</code></td>
<td>Contains blob files with the information about archived Microsoft organizations.</td>
</tr>
<tr>
<td><code>&lt;repository_folder_name&gt;/Organizations</code></td>
<td>The root folder that contains archived Microsoft organizations. Each organization is kept in its own folder with a unique identification number.</td>
</tr>
<tr>
<td><code>&lt;organization_id&gt;/AccountMailboxes</code></td>
<td>Contains blob files with the information about account mailboxes.</td>
</tr>
<tr>
<td><code>&lt;organization_id&gt;/CopyObjects</code></td>
<td>Contains dates of the latest attempt of archiving backed-up data of objects per object.</td>
</tr>
</tbody>
</table>
| `<organization_id>/Mailboxes/<mailbox_Id>` | The *Mailboxes* directory contains archived Exchange mailboxes. Each mailbox is saved under a unique identification number to the `<mailbox_Id>` directory. The `<mailbox_Id>` directory contains the following directories:  
  - *Backups*. Contains archived Exchange data.
  - *Folders*. Contains a snapshot of Exchange folders at the specified point in time. |
<p>| <code>&lt;organization_id&gt;/MailboxInfos</code> | Contains blob files with the information about archived Exchange mailboxes. |
| <code>&lt;organization_id&gt;/RestorePoints</code> | Contains blob files with the information about restore points created by Veeam Backup for Microsoft 365 and a list of restore point objects per restore point. |
| <code>&lt;organization_id&gt;/Sites</code> | Contains a blob file with a list of archived SharePoint sites. |
| <code>&lt;organization_id&gt;/TeamInfos</code> | Contains blob files with the unchanged information about teams. |</p>
<table>
<thead>
<tr>
<th>Directory</th>
<th>Description</th>
</tr>
</thead>
</table>
| <organization_id>/Teams | Contains the following directories:  
  - *Accounts*. Contains names and descriptions of all users included in all teams.  
  - `<team_id>`. Contains archived Microsoft Teams data such as *Channels*, *Tabs*, *Applications* and *UsersMembership*. |
| <organization_id>/WebBackups | Contains a list of archived SharePoint sites. |
| <organization_id>/WebRestorePoints | Contains information on how web objects were backed up per restore point. |
| <organization_id>/Webs/<web_Id> | A set of folders that contain archived SharePoint sites and OneDrive Items.  
The `<web_Id>` directory contains the following directories:  
  - *Files*. Contains archived files of the SharePoint site.  
  - *WebParts*. Contains Web Parts of SharePoint sites.  
  - *Items*. Contains archived items such as those located under the *Subsites* and *Content* folders for SharePoint, and users folders for OneDrive.  
  - *Lists*. Contains archived SharePoint lists.  
  - *ListViews*. Contains archived SharePoint list views. |
| <repository_folder_name>/RepositoryLock | Contains a lock file that tells that this storage is already an extension to a backup repository.  
Object storage can only be owned by one owner (a backup repository) at a time.  
For more information on how to extend a backup repository with object storage, see Specify Object Storage Repository. |
About Cache

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

For example, when you use Veeam Explorers to open backups located in object storage, Veeam Backup for Microsoft 365 uses cache from which it retrieves the structure of the backed-up objects of your organizations. Such a structure is then loaded into the inventory pane of each of the Veeam Explorers so that you can navigate through it without actually downloading any data from object storage.
Consider the following about cache:

- Cache is metadata that holds information about backed-up objects.
- Cache is created (or updated) during each backup session.
- Cache is saved to the PersistentCache directory in an extended backup repository as a JET-based database and also replicated to the object storage repository.

Replication gives Veeam Backup for Microsoft 365 the ability to synchronize cache between object storage and the backup repository when:

- Creating a new backup repository and extending it with object storage that contains offloaded backup data.
  
  For more information on how to extend a backup repository, see Specify Object Storage Repository.
- Recovering lost cache.
  
  For example, you may have accidentally removed a directory with cache from the extended backup repository. In such a scenario, manual synchronization is required. For more information on how to synchronize data, see Synchronizing Repositories.

The location of the PersistentCache directory is specified at the Specify Backup Proxy Server step.

### About Compression

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

Compression works in the following way:

- All chunks of data that are larger than 512 bytes are subject to compression; each blob file that is created is compressed first and then saved to object storage.
  
  To compress data, Veeam Backup for Microsoft 365 uses the ZSTD algorithm. For more information about this algorithm, see this Zstandard article.
- Compression is done by the backup proxy server that you specify at the Specify Backup Proxy Server step.
- Certain types of data such as images or other media files cannot be compressed properly. Thereby an output compressed blob file becomes larger than it could be if it was not compressed at all. In such a scenario, the uncompressed version of the file will be saved.

### About Data Encryption

Data security is an important part of the backup strategy. You can use data encryption to protect your backups from unauthorized access in object storage repositories.

Before transferring your backed-up data to an object storage, Veeam Backup Proxy for Microsoft 365 Service encrypts data with the help of a cryptographic algorithm and a secret key. If encrypted data is intercepted, it cannot be unlocked and read by the eavesdropper. Only intended recipients who know the secret key can reverse encrypted information back to a readable format.

Veeam Backup for Microsoft 365 generates a secret key based on an encryption password that you create by yourself. For more information on how to configure encryption passwords, see Managing Encryption Passwords.

For data encryption, Veeam Backup for Microsoft 365 uses the 256-bit Advanced Encryption Standard (AES). For more information about AES, see this article.
Encryption Algorithm

To encrypt backed-up data, Veeam Backup for Microsoft 365 employs a symmetric-key encryption algorithm.

The symmetric, or single-key encryption algorithm, uses a single, common secret key to encrypt and decrypt data. Before data is sent to an object storage repository, it is encoded with a secret key. To restore encrypted data, you must have the same secret key. Users who do not have the secret key cannot decrypt data and get access to it.

Object Storage Retention

Obsolete restore points are removed from object storage automatically by Veeam Backup for Microsoft 365. Data removal is based on the retention policy settings that you configure when extending a backup repository with object storage.

Depending on how frequently your retention policy is configured to be executed, Veeam Backup for Microsoft 365 initiates a service task that calculates the age of offloaded restore points and if the age exceeds the specified retention period, this task purges obsolete restore points from object storage.

**IMPORTANT**

Do not remove anything from object storage manually, as this will irreversibly damage your backup structure to the point where you will be completely unable to read data from such corrupted backups.

Archive Object Storage Retention

Consider the following:

- The retention type of a backup repository extended with an archive object storage must match that of an extended backup repository where you keep your backups.

- If you increase the retention policy value for a backup repository extended with an archive object storage that has the item-level retention type and start a backup copy job without source backup job started prior to that, Veeam Backup for Microsoft 365 will not archive backed-up data of items whose last modification time fits the updated retention coverage of backup copy.

Adding Object Storage Repositories

You can add the following types of object storage repositories to the Veeam Backup for Microsoft 365 backup infrastructure:

- S3 Compatible Object Storage Repositories
- Amazon S3 Object Storage Repositories
- Microsoft Azure Blob Object Storage Repositories
- IBM Cloud Object Storage Repositories
Adding S3 Compatible Object Storage Repositories

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

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

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

1. Open the Backup Infrastructure view.
2. In the inventory pane, select the Object Storage Repositories node.
3. Do one of the following:
   - On the Object Storage Repository tab, click Add Object Storage on the ribbon.
   - Right-click the Object Storage Repositories node and select Add object storage.
Step 2. Specify Object Storage Repository Name

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

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

![New Object Storage Repository](image)
Step 3. Select Object Storage Type

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

**Object storage type**

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

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

- **Microsoft Azure Blob Storage**
  Adds Microsoft Azure cloud object storage. Microsoft Azure Blob Storage and Microsoft Azure Archive Storage are supported.

- **IBM Cloud Object Storage**
  Adds IBM Cloud object storage. S3 compatible versions of both on-premises and IBM Cloud storage offerings are supported.
Step 4. Specify Object Storage Service Point and Account

At this step of the wizard, specify a service point of your S3 Compatible device, select a datacenter region and specify account credentials.

1. In the Service point field, specify an endpoint address of your S3 Compatible device.
2. In the Data center region field, specify a region.
3. From the Specify account credentials to connect to S3 compatible storage bucket drop-down list, select user credentials to access your S3 Compatible object storage.

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

![New Object Storage Repository](Image)
Step 5. Specify Object Storage Bucket

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

1. From the **Bucket** drop-down list, select a bucket.
   
   Make sure that the bucket you want to use to store your data was created in advance; Veeam Backup for Microsoft 365 does not support creating new buckets.

2. In the **Folder** field, select a folder to which you want to map your object storage repository, and which will be used to store backups.
   
   To select a folder, click **Browse** and either select an existing folder or create a new one by clicking **New Folder**.
   
   For more information about how data is stored, see About Object Storage Repository Structure.

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

   ![Advanced settings](image)

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

      a. Select the **Limit object storage consumption** to check box and specify the limit value in GB, TB or PB.
         
         If you select this check box, Veeam Backup for Microsoft 365 limits the object storage capacity and prohibits running new jobs when the specified value is exceeded.
b. Click **OK**.

![Advanced Settings](image)

Adding Amazon S3 Object Storage Repositories

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

1. Launch the New Object Storage Repository wizard.
2. Specify an object storage repository name.
3. Select an object storage type.
4. Select Amazon S3 storage type.
5. Specify an object storage account.
7. Configure the Amazon archiver appliance.
Step 1. Launch New Object Storage Repository Wizard

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

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Object Storage Repositories** node.
3. Do one of the following:
   - On the **Object Storage Repository** tab, click **Add Object Storage** on the ribbon.
   - Right-click the **Object Storage Repositories** node and select **Add object storage**.
Step 2. Specify Object Storage Repository Name

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

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

![New Object Storage Repository](image_url)

Object storage repository name and description

<table>
<thead>
<tr>
<th>Name:</th>
<th>Veeam Object Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description:</td>
<td>Secondary Backup Storage</td>
</tr>
</tbody>
</table>

[Back][Next][Cancel]
Step 3. Select Object Storage Type

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

For more information about supported Amazon S3 storage classes, see Supported Amazon S3 Storage Classes.
Step 4. Select Amazon Storage Type

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

- **Amazon S3.** Select this option if you want to use this object storage as a target for backup jobs. Veeam Backup for Microsoft 365 supports Amazon S3 Standard and Amazon S3 Standard-Infrequent Access storage classes for this purpose.

- **Amazon S3 Glacier.** Select this option if you want to use this object storage as a target for backup copy jobs. Veeam Backup for Microsoft 365 supports Amazon S3 Glacier and Amazon S3 Glacier Deep Archive storage classes for this purpose.

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

<table>
<thead>
<tr>
<th>New Object Storage Repository</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Storage type</td>
</tr>
<tr>
<td><img src="Image" alt="Amazon S3" /></td>
</tr>
<tr>
<td>Adds Amazon S3 storage of Standard and Infrequent Access (IA) storage classes. Use this option for your primary backups.</td>
</tr>
<tr>
<td><img src="Image" alt="Amazon S3 Glacier" /></td>
</tr>
<tr>
<td>Adds Amazon S3 Glacier storage. Both Amazon S3 Glacier and Glacier Deep Archive are supported. Use this option for cost-efficient long-term storage of your backup copies.</td>
</tr>
</tbody>
</table>
Step 5. Specify Object Storage Account

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

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

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

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

![Image of the New Object Storage Repository page with options for Amazon AWS account and Region selection.]
Step 6. Specify Object Storage Settings

At this step of the wizard, select a location of your Amazon bucket, a bucket and folder where you want to keep backup data.

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

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

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

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

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

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

4. Click **Advanced** if you want to configure storage consumption limitations and select Amazon S3 storage class.

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

   a. Select the **Limit object storage consumption** check box and specify the limit value in GB, TB or PB.

      If you select this check box, Veeam Backup for Microsoft 365 limits the object storage capacity and prohibits running new jobs when the specified value is exceeded.

   b. Enable the S3 Standard-IA or S3 Glacier Deep Archive storage classes usage:
If you have selected the Amazon S3 option on the Select Amazon Storage Type step, select the Use infrequent access storage class check box if you plan to access your backup data in an infrequent manner and to mark each block as S3 Standard-IA (Amazon S3 Standard-Infrequent Access). For more information about infrequent access, see this Amazon article.

If you have selected the Amazon S3 Glacier option on the Select Amazon Storage Type step, select the Use Glacier Deep Archive check box if you plan to access your archived data rarely and to mark each block as S3 Glacier Deep Archive (Amazon S3 Glacier Deep Archive). For more information about data archiving, see this Amazon article.

c. Click OK.
Step 7. Configure Amazon Archiver Appliance

This step is only available if you have selected the **Amazon S3 Glacier** option at the **Select Amazon Storage Type** step of the wizard.

At this step of the wizard, you can optionally enable usage of the Amazon archiver appliance when Veeam Backup for Microsoft 365 creates a backup copy. Backed-up data is copied to different storage class: from general purpose (Amazon S3 Standard) or infrequent access (Amazon S3 Standard-Infrequent Access) storage class to archive storage class (Amazon S3 Glacier or Amazon S3 Glacier Deep Archive). If you use the archiver appliance, it usually speeds up the backup copy process and helps you reduce cost expensive operations. Also, using the archiver appliance, you protect your backups because all operations with backed-up data are performed within the Amazon cloud.

The Amazon archiver appliance is an auxiliary EC2 instance that is deployed and configured automatically by Veeam Backup for Microsoft 365 in Amazon EC2 only for the duration of a backup copy job. Veeam Backup for Microsoft 365 removes or reuses it after a backup copy job completes. By default, Veeam Backup for Microsoft 365 always keeps one archiver appliance for reuse.

If you do not want to use the Amazon archiver appliance, skip this step and click **Finish**.

To enable usage of the Amazon archiver appliance, do the following:

1. Select the **Use archiver appliance to copy data to an archive tier** check box.
2. Click **Customize** if you want to change the default settings of the archiver appliance.

3. In the **Cloud Archiver Appliance Settings** window, do the following:
   a. From the **EC2 instance type** drop-down list, select the instance type for the archiver appliance. For more information on instance types, see [this Amazon article](#).
   b. From the **Amazon Virtual Private Cloud (VPC)** drop-down list, select the Amazon VPC where Veeam Backup for Microsoft 365 will launch the target instance. For more information on the Amazon VPC, see [this Amazon article](#).
   c. From the **Subnet** drop-down list, select the subnet for the archiver appliance.
   d. From the **Security group** drop-down list, select a security group that will be associated with the archiver appliance. For more information on security groups for Amazon VPC, see [this Amazon article](#).
e. Specify the port that Veeam Backup for Microsoft 365 will use to route requests between the archiver appliance and backup infrastructure components.

f. Click OK.

Adding Microsoft Azure Blob Object Storage Repositories

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

1. Launch the New Object Storage Repository wizard.
2. Specify an object storage repository name.
3. Select an object storage type.
4. Select Microsoft Azure Blob Storage type.
5. Specify an object storage account.
7. Configure the Azure archiver appliance.
Step 1. Launch New Object Storage Repository Wizard

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

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Object Storage Repositories** node.
3. Do one of the following:
   - On the **Object Storage Repository** tab, click **Add Object Storage** on the ribbon.
   - Right-click the **Object Storage Repositories** node and select **Add object storage**.
Step 2. Specify Object Storage Repository Name

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

1. In the **Name** field, enter a name for the object storage repository.
2. In the **Description** field, enter optional description.
Step 3. Select Object Storage Type

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

<table>
<thead>
<tr>
<th>New Object Storage Repository</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Object storage type</strong></td>
</tr>
<tr>
<td>- <strong>S3 Compatible</strong></td>
</tr>
<tr>
<td>Adds a cloud object storage provider, or an on-premises object storage system.</td>
</tr>
<tr>
<td>- <strong>Amazon S3</strong></td>
</tr>
<tr>
<td>Adds Amazon S3 storage. Both Standard and Infrequent Access (IA) storage classes are supported.</td>
</tr>
<tr>
<td>- <strong>Microsoft Azure Blob Storage</strong></td>
</tr>
<tr>
<td>Adds Microsoft Azure cloud object storage, Microsoft Azure Blob Storage and Microsoft Azure Archive Storage are supported.</td>
</tr>
<tr>
<td>- <strong>IBM Cloud Object Storage</strong></td>
</tr>
<tr>
<td>Adds IBM Cloud object storage. S3 compatible versions of both on-premises and IBM Cloud storage offerings are supported.</td>
</tr>
</tbody>
</table>

For more information about supported Azure storage account types and supported access tiers for Azure Blob Storage, see [Supported Azure Storage Account Types](#).
Step 4. Select Microsoft Azure Blob Storage Type

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

- **Azure Blob Storage.** Select this option if you want to use this object storage as a target for backup jobs.
- **Azure Archive Storage.** Select this option if you want to use this object storage as a target for backup copy jobs.

For more information about supported Azure storage account types and supported access tiers for Azure Blob Storage, see Supported Azure Storage Account Types.
Step 5. Specify Object Storage Account

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

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

   If you already have a credentials record that was configured beforehand, select such a record from the drop-down list. Otherwise, click **Add** and provide your account and a shared key. For more information, see **Adding Microsoft Azure Blob Storage Account**. You can also click **Manage cloud accounts** to manage existing credentials records.

2. From the **Region** drop-down list, select a Microsoft Azure region.
Step 6. Specify Object Storage Settings

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

1. From the **Container** drop-down list, select an Azure container.
   
   Make sure that the container you want to use to store your data was created in advance; Veeam Backup for Microsoft 365 does not support creating new containers.

2. In the **Folder** field, select a cloud folder to which you want to map your object storage repository, and which will be used to store offloaded data.
   
   To select a folder, click **Browse** and either select an existing folder or create a new one by clicking **New Folder**.
   
   For more information about how data is stored, see About Object Storage Repository Structure.

3. Click **Advanced** if you want to configure storage consumption limitations.
4. In the **Advanced Settings** window, do the following:

   a. Select the **Limit object storage consumption to** check box and specify the limit value in GB, TB or PB.

      If you select this check box, Veeam Backup for Microsoft 365 limits the object storage capacity and prohibits running new jobs when the specified value is exceeded.

   b. Click **OK**.
Step 7. Configure Azure Archiver Appliance

This step is only available if you have selected the **Azure Archive Storage** option at the **Select Microsoft Azure Blob Storage Type** step of the wizard.

At this step of the wizard, you can optionally enable usage of the Azure archiver appliance when Veeam Backup for Microsoft 365 copies backed-up data from Azure Blob storage to Azure Archive storage. If you use the Azure archiver appliance, it usually speeds up the backup copy process and helps you reduce cost expensive operations.

The Azure archiver appliance is a small auxiliary machine in Microsoft Azure that is deployed and configured automatically by Veeam Backup for Microsoft 365. Veeam services that Veeam Backup for Microsoft 365 installs on the Azure archiver appliance compress data passed through. This helps reduce network traffic and increase the speed of backup copy.

The process of the Azure archiver appliance deployment takes a couple of minutes. If you enable usage of the Azure archiver appliance, Veeam Backup for Microsoft 365 will create the archiver appliance at the beginning of a backup copy job and remove or reuse it after a backup copy job completes. By default, Veeam Backup for Microsoft 365 always keeps one archiver appliance for reuse.

If you do not want to use the Azure archiver appliance, skip this step and click **Finish**.

To enable usage of the Azure archiver appliance, do the following:

1. Select the **Use archiver appliance to copy data to an archive tier** check box.
2. From the **Specify account credentials to connect to Microsoft Azure** drop-down list, select a service account credentials to access Microsoft Azure.
   
   If you already have a credentials record that was configured beforehand, select such a record from the drop-down list. Otherwise, click **Add** and configure a new Azure service account using the **Add Azure Service Account** wizard. For more information, see **Adding Microsoft Azure Service Account**. You can also click **Manage cloud accounts** to manage existing credentials records.
3. From the **Subscription** drop-down list, select Microsoft Azure subscription.
4. Click **Customize** if you want to change the default settings of the archiver appliance.
5. In the **Cloud Archiver Appliance Settings** window, do the following:
   a. From the **Size** drop-down list, select the size of the appliance.
   b. From the **Resource group** drop-down list, select a resource group that will be associated with the archiver appliance.
   c. From the **Virtual network** drop-down list, select a network to which the archiver appliance must be connected.
   d. From the **Subnet** drop-down list, select the subnet for the archiver appliance.
   e. Specify the port that Veeam Backup for Microsoft 365 will use to route requests between the archiver appliance and backup infrastructure components.
   f. Click **OK**.

![Cloud Archiver Appliance Settings](image)

### Adding IBM Cloud Object Storage Repositories

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

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

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

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Object Storage Repositories** node.
3. Do one of the following:
   - On the **Object Storage Repository** tab, click **Add Object Storage** on the ribbon.
   - Right-click the **Object Storage Repositories** node and select **Add object storage**.
Step 2. Specify Object Storage Repository Name

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

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

![New Object Storage Repository](image)

Object storage repository name and description

**Name:**

IBM Cloud Object Storage

**Description:**

Secondary Backup Storage
Step 3. Select Object Storage Type

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

Object storage type

- **S3 Compatible**
  Adds a cloud object storage provider, or an on-premises object storage system.
- **Amazon S3**
  Adds Amazon S3 storage. Both Standard and Infrequent Access (IA) storage classes are supported.
- **Microsoft Azure Blob Storage**
  Adds Microsoft Azure cloud object storage. Microsoft Azure Blob Storage and Microsoft Azure Archive Storage are supported.
- **IBM Cloud Object Storage**
  Adds IBM Cloud object storage. S3 compatible versions of both on-premises and IBM Cloud storage offerings are supported.
Step 4. Specify Object Storage Service Point and Account

At this step of the wizard, specify a service point of your IBM Cloud object storage, select a datacenter region and specify account credentials.

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

   If you already have a credentials record that was configured beforehand, select such a record from the drop-down list. Otherwise, click **Add** and provide your access and secret keys. For more information, see **Adding S3 Compatible and IBM Storage Access Key**. You can also click **Manage cloud accounts** to manage existing credentials records.
Step 5. Specify Object Storage Bucket

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

1. From the **Bucket** drop-down list, select a bucket.
   Make sure that the bucket you want to use to store your data was created in advance; Veeam Backup for Microsoft 365 does not support creating new buckets.

2. In the **Folder** field, select a folder to which you want to map your object storage repository, and which will be used to store backups.
   To select a folder, click **Browse** and either select an existing folder or create a new one by clicking **New Folder**.
   For more information about how data is stored, see **About Object Storage Repository Structure**.

3. Click **Advanced** if you want to configure storage consumption limitations.
4. In the **Advanced Settings** window, do the following:

   a. Select the **Limit object storage consumption** check box and specify the limit value in GB, TB or PB.

      If you select this check box, Veeam Backup for Microsoft 365 limits the object storage capacity and prohibits running new jobs when the specified value is exceeded.

   b. Click **OK**.

![Advanced Settings window](image)

### Editing Object Storage Settings

Veeam Backup for Microsoft 365 allows you to edit an object storage repository settings.

To edit an object storage repository settings, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Object Storage Repositories** node.
3. In the preview pane, do one of the following:
   
   - Select an object storage repository and on the **Object Storage Repository** tab, click **Edit Object Storage** on the ribbon.
   - Right-click an object storage repository and select **Edit**.
4. Modify the required settings.

You can change the following parameters:

- The name and description of an object storage repository.
- Its capacity to prohibit running new jobs when the specified value is exceeded.
- For archive object storage, you can enable or disable usage of the archiver appliance.

Removing Object Storage Repositories

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

Consider the following:

- You cannot remove an object storage repository that is in use by an extended backup repository.
  
  To remove such object storage, remove an extended backup repository and then remove object storage. For more information on how to remove a backup repository, see Removing Backup Repositories.

- When removing an object storage repository from the Veeam Backup for Microsoft 365 infrastructure, the backup data will not be removed from this storage.
To remove an object storage repository from the Veeam Backup for Microsoft 365 backup infrastructure, do the following:

1. Open the Backup Infrastructure view.
2. In the inventory pane, select the Object Storage Repositories node.
3. In the preview pane, do one of the following:
   - Select an object storage repository and on the Object Storage Repository tab, click Remove Object Storage on the ribbon.
   - Right-click an object storage repository and select Remove.
Credentials

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

- **Cloud credentials**
  You can use this type of credentials to work with object storage repositories.

- **Encryption passwords**
  You can use this type of credentials to encrypt data in object storage repositories.

Both cloud credentials and encryption passwords are stored in Veeam Backup for Microsoft 365 and encrypted using the Data Protection API (DPAPI) mechanisms. For more information, see this Microsoft article.
Managing Cloud Credentials

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

- S3 Compatible and IBM Cloud storage
- Amazon S3 storage
- Microsoft Azure Blob storage

If you want to use the Azure archiver appliance when Veeam Backup for Microsoft 365 copies backed-up data from Azure Blob storage to Azure Archive storage, you must add the Microsoft Azure service account.

Adding S3 Compatible and IBM Cloud Storage Access Key

You can add new credentials for S3 Compatible or IBM Cloud object storage.

To add credentials, do the following:

1. In the main menu, click Manage Cloud Credentials.
2. In the Cloud Credential Manager window, click Add > S3 Compatible access key.
3. In the Access key field, enter your access key.
4. In the Secret key field, enter your secret key.
5. In the Description field, enter optional description.
6. Click OK.
Adding Amazon AWS Access Key

You can add new credentials for Amazon S3 object storage.

To add credentials, do the following:

1. In the main menu, click Manage Cloud Credentials.
2. In the Cloud Credential Manager window, click Add > Amazon AWS access key.
3. In the Access key field, enter your access key.
4. In the Secret key field, enter your secret key.
5. In the Description field, enter optional description.
6. Click OK.
Adding Microsoft Azure Blob Storage Account

You can add new credentials for Microsoft Azure Blob storage.

To add credentials, do the following:

1. In the main menu, click Manage Cloud Credentials.
2. In the Cloud Credential Manager window, click Add > Microsoft Azure storage account.
3. In the Account field, enter your storage account name.
4. In the Shared key field, enter your shared key.
5. In the Description field, enter optional description.
6. Click OK.

Adding Microsoft Azure Service Account

You can add new credentials to use the Azure archiver appliance.

To add a new Microsoft Azure service account, do the following:

1. Launch the Add Azure Service Account wizard.
2. Configure connection to Microsoft Azure.
3. Register or select Azure AD Application.
4. Log in to Microsoft 365.
5. Select Microsoft Azure subscription.
Step 1. Launch Add Azure Service Account Wizard

To launch the Add Azure Service Account wizard, do the following:

1. In the main menu, click Manage Cloud Credentials.
2. In the Cloud Credential Manager window, click Add > Microsoft Azure service account.
Step 2. Configure Connection to Microsoft Azure

At this step of the wizard, select a Microsoft Azure region and choose whether you want to register a new Azure AD application to connect to Microsoft Azure or use an existing Azure AD application.

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

1. From the **Region** drop-down list, select a Microsoft Azure region.
2. Select one of the following options:
   - **Register a new Azure AD application automatically**
     With this option selected, Veeam Backup for Microsoft 365 requires to provide an application name and certificate to register a new Azure AD application in Azure Active Directory. For more information, see Registering New Azure AD Application.
   - **Use an existing Azure AD application**
     With this option selected, Veeam Backup for Microsoft 365 requires to provide connection parameters to the existing Azure AD application. For more information, see Using Existing Azure AD Application.
Step 3. Register or Select Azure AD Application

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

- **Registering a new application**
  
  Use this method if you have selected the *Register a new Azure AD application automatically* option at the previous step of the wizard.

- **Using an existing application**
  
  Use this method if you have selected the *Use an existing Azure AD application* option at the previous step of the wizard.

**Registering New Azure AD Application**

You can register a new Azure AD application in Azure Active Directory. Veeam Backup for Microsoft 365 will use this application for data exchange when transferring backed-up data from Azure Blob storage to Azure Archive storage during backup copy jobs.

When registering a new Azure AD application, Veeam Backup for Microsoft 365 automatically grants the required permissions to this application.

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

1. In the **Name** field, enter a name that you want to use to register a new Azure AD application in your Azure Active Directory.

2. Click **Install** to specify an SSL certificate that you want to use for data exchange between Veeam Backup for Microsoft 365 and an Azure AD application.

3. In the **Select Certificate** wizard, select a certificate. For more information, see [Installing SSL Certificates](#). You can generate a new self-signed certificate or use an existing one. Before using an existing certificate, make sure to register this certificate in Azure Active Directory. For more information, see [this Microsoft article](#). When generating a new self-signed certificate, Veeam Backup for Microsoft 365 will register it automatically.

4. In the **Specify Azure service account description** field, enter optional description.
Using Existing Azure AD Application

You can specify an existing Azure AD application in your Azure Active Directory. Veeam Backup for Microsoft 365 will use this application for data exchange when transferring backed-up data from Azure Blob storage to Azure Archive storage during backup copy jobs.

To use an existing application, do the following:

1. In the Tenant ID field, specify a name of your Microsoft 365 organization.
2. In the Application ID field, specify an identification number of your Azure AD application.
   You can find this number in an application settings in your Azure Active Directory. For more information, see this Microsoft article.
3. Select an Azure AD application authentication type. You can select either Application secret or Application certificate:
   a. To use a certificate, select the Application certificate option and click Install. For more information, see Installing SSL Certificates.
      Mind that you must upload a certificate file to the Azure portal beforehand. For more information, see this Microsoft article.
   b. To use a secret key, select the Application secret option and enter a secret key in the field nearby to access your custom application.
      To obtain a secret key, you will need to generate it first. For more information on how to generate a secret key, see this Microsoft article.
      Mind that a key will become hidden once you leave or refresh the page in the Azure portal. Consider saving the key to a secure location.
4. Select the Grant this application required permissions and register its certificate in Azure AD check box to automatically grant required permissions to Azure AD application.
   Veeam Backup for Microsoft 365 will also register the specified certificate in your Azure Active Directory.
   Mind that if this check box is not selected, Veeam Backup for Microsoft 365 skips the Log in to Microsoft 365 and Select Microsoft Azure Subscription steps and finishes the wizard.
5. In the **Specify Azure service account description** field, enter optional description.
Step 4. Log In to Microsoft 365

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

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

1. Click **Copy code** to copy an authentication code.
   Mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.

2. Click the Microsoft authentication portal link.
   A web browser window opens.

3. On the **Sign in to your account** webpage, paste the code that you have copied and sign in to Microsoft Azure.
   Make sure to sign in with the user account that has the **Global Administrator** role. For more information about this role, see [this Microsoft article](#).

4. Return to the **Add Azure Service Account** wizard and click **Next**.
Step 5. Select Microsoft Azure Subscription

At this step of the wizard, select check boxes next to Microsoft Azure subscriptions in the list. The subscription list contains all subscriptions associated with the user account that you have used to sign in to Microsoft Azure.

![Select Microsoft Azure Subscription](image)

Editing and Removing Cloud Credentials

Veeam Backup for Microsoft 365 allows you to edit and remove cloud credentials that you use to access object storage repositories.

Editing Credentials

To edit credentials, do the following:

1. In the main menu, click Manage Cloud Credentials.
2. In the Cloud Credential Manager window, select an account and click Edit.
3. Modify the selected credentials if needed.

**NOTE**

When editing Microsoft Azure storage accounts, you can change the shared key only.

Removing Credentials

To remove credentials, do the following:

1. In the main menu, click Manage Cloud Credentials.
2. In the Cloud Credential Manager window, select an account and click Remove.

**NOTE**

You cannot remove cloud credentials that are in use.
Managing Encryption Passwords

Veeam Backup for Microsoft 365 allows you to configure passwords that you can use to encrypt data in object storage repositories using the 256-bit Advanced Encryption Standard (AES).

To add an encryption password, do the following:

1. In the main menu, click Manage Passwords.
2. In the Password Manager window, click Add.
3. In the Password field, enter a new password.
4. In the Verify password field, re-enter the password.
5. In the Hint field, enter a hint that will help you to remember the password.

**IMPORTANT**

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

---

Editing and Removing Encryption Passwords

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

**Editing Encryption Passwords**

To edit an encryption password, do the following:

1. In the main menu, click Manage Passwords.
2. In the Password Manager window, select a password and click Edit.
3. In the Current password field, enter your current password.
4. In the New password field, enter a new password.
5. In the **Verify new password** field, re-enter the password.

6. In the **Hint** field, enter a hint that will help you to remember the password.

### Removing Encryption Passwords

To remove an encryption password, do the following:

1. In the main menu, click **Manage Passwords**.

2. In the **Password Manager** window, select a password and click **Remove**.

**NOTE**

You cannot remove passwords that are in use.
Organization Management

You can add the following types of Microsoft organizations to the Veeam Backup for Microsoft 365 environment:

- Microsoft 365 organizations
- On-Premises Microsoft organizations
- Hybrid organizations

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

- *Exchange Web Services* (EWS) and *PowerShell* to connect to Microsoft 365 and on-premises Microsoft Exchange organizations.
- *SharePoint Client Object Model* (CSOM) and *Windows Remote Management* to connect to on-premises Microsoft SharePoint organizations.
  
  For more information about Windows Remote Management, see [this Microsoft article](#).
- *Microsoft Graph API* to connect to Microsoft 365 organizations.
Microsoft 365 Organizations

You can add Microsoft 365 organizations to the Veeam Backup for Microsoft 365 infrastructure to back up data of these organizations and quickly restore it back to production servers in case of an unexpected disaster.

When you add Microsoft 365 organizations, you can use the following authentication methods:

- **Modern app-only authentication**
  When you use this method, Veeam Backup for Microsoft 365 uses only Azure AD application to authenticate to your Microsoft 365 organizations with enabled security defaults. You cannot use Veeam Backup account with the modern app-only authentication method.

- **Modern authentication with legacy protocols allowed**
  When you use this method, you can use both Veeam Backup account and Azure AD application to authenticate to your Microsoft 365 organizations with disabled security defaults. You use MFA-enabled Microsoft 365 user account as Veeam Backup account.

- **Basic authentication**
  When you use this method, you are required to provide a user account as Veeam Backup account to authenticate to your Microsoft 365 organization.

**NOTE**
Consider that backup and restore functionality of Veeam Backup for Microsoft 365 differs depending on authentication method that you use. For limitations in Veeam Backup for Microsoft 365 functionality when protecting organizations with modern app-only authentication, see this Veeam KB article.
Adding Organizations with Modern App-Only Authentication

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

With modern app-only authentication, you cannot use Veeam Backup account; only communications through Azure AD application is possible.

**NOTE**

Adding Microsoft 365 organizations using modern app-only authentication is not supported for Microsoft Azure Germany region. For limitations in Veeam Backup for Microsoft 365 functionality when protecting organizations with modern app-only authentication, see this Veeam KB article.

To add a new Microsoft 365 organization to Veeam Backup for Microsoft 365, do the following:

1. Launch the Add Organization wizard.
2. Select an organization deployment type.
3. Select Azure region and authentication method.
5. Register or select Azure AD Application.
7. Finish the wizard.
Step 1. Launch Add Organization Wizard

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

1. Open the **Organizations** view.
2. Do one of the following:
   - On the **Home** tab, click **Add Org** on the ribbon.
   - In the inventory pane, right-click the **Organizations** node and select **Add organization**.
Step 2. Select Organization Deployment Type

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

**NOTE**

Starting from version 6a (build 6.1.0.222), Veeam Backup for Microsoft 365 can back up Microsoft Teams messages using Microsoft Teams APIs in Microsoft Graph (Teams Export APIs). This method substitutes backup of the *TeamsMessagesData* folder that will be deprecated by Microsoft.

For more information on how to set up Veeam Backup for Microsoft 365 to use Teams Export APIs for team chats backup, see *Getting Started with Teams Export APIs*.

Depending on whether you enabled usage of Teams Export APIs for team chats backup, Veeam Backup for Microsoft 365 displays different settings at this step of the wizard. You can proceed to one of the following scenarios:

- **Backup of the TeamsMessagesData folder**

  Veeam Backup for Microsoft 365 displays these settings if you did not enable usage of Teams Export APIs for team chats backup.

- **Backup of team chats using Teams Export APIs**

  Veeam Backup for Microsoft 365 displays these settings if you enabled usage of Teams Export APIs for team chats backup.

**Backup of TeamsMessagesData Folder**

Veeam Backup for Microsoft 365 displays these settings if you did not enable usage of Teams Export APIs for team chats backup.

**NOTE**

For more information about team chats backup in Veeam Backup for Microsoft 365, see *Backup of Team Chats Using Teams Export APIs*.

To select an organization deployment type and Microsoft Online services whose data you want to protect, do the following:

1. From the **Select organization deployment type** drop-down list, select *Microsoft 365*.
2. If you want to back up Exchange Online data, select the **Exchange Online** check box.
3. If you want to back up SharePoint Online and OneDrive for Business data, select the **SharePoint Online and OneDrive for Business** check box.
4. If you want to back up Microsoft Teams data, select the **Microsoft Teams** check box.

   You can select this check box only if both **Exchange Online** and **SharePoint Online and OneDrive for Business** check boxes are selected.
NOTE
Microsoft Teams service is not supported for organizations in the Microsoft Azure China and Germany regions.

Backup of Team Chats Using Teams Export APIs

Veeam Backup for Microsoft 365 displays these settings if you enabled usage of Teams Export APIs for team chats backup.

To select an organization deployment type and Microsoft Online services whose data you want to protect, do the following:

1. From the Select organization deployment type drop-down list, select Microsoft 365.
2. If you want to back up Exchange Online data, select the Exchange Online check box.
3. If you want to back up SharePoint Online and OneDrive for Business data, select the SharePoint Online and OneDrive for Business check box.
4. If you want to back up Microsoft Teams data, select the Microsoft Teams check box.
   You can select this check box only if both Exchange Online and SharePoint Online and OneDrive for Business check boxes are selected.
5. If you want to back up team chats using Teams Export APIs, select the Teams chats check box.
   This check box is available only if the Microsoft Teams check box is selected. For more information on how to back up team chats, see Organization Object Types.
NOTE

Consider the following:

- Veeam Backup for Microsoft 365 backs up team chats using Teams Export APIs starting from version 6a (build 6.1.0.222).
- Microsoft Teams service is not supported for organizations in the Microsoft Azure China and Germany regions.
- Backup of team chats using Teams Export APIs is not supported for Microsoft organizations in the Microsoft Azure China, Germany, US Government GCC and US Government GCC High regions.
Step 3. Select Azure Region and Authentication Method

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

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

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

   Mind that you cannot select the Germany region for modern app-only authentication.

2. Select the Modern authentication option to use Azure AD application to connect to your Microsoft 365 organization with enabled security defaults.

   Make sure to leave the Allow for using legacy authentication protocols check box cleared. This check box allows you to add a Microsoft 365 organization with disabled security defaults. For more information, see Adding Organizations with Modern Authentication and Legacy Protocols.

   **NOTE**

   If you selected the Teams chats check box at the previous step of the wizard, the Modern authentication option is only available.
Step 4. Configure Connection to Microsoft 365

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

Backup of TeamsMessagesData Folder

You can select one of the following options:

- **Register a new Azure AD application automatically**
  
  With this option selected, Veeam Backup for Microsoft 365 requires to provide an application name and certificate to register a new Azure AD application in Azure Active Directory. For more information, see [Registering New Azure AD Application](#).

- **Use an existing Azure AD application**
  
  With this option selected, Veeam Backup for Microsoft 365 requires to provide connection parameters to the existing Azure AD application. For more information, see [Using Existing Azure AD Application](#).

<table>
<thead>
<tr>
<th>Add Organization</th>
<th>X</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Microsoft 365 connection settings</strong></td>
<td></td>
</tr>
<tr>
<td>Select how to connect to the Microsoft 365 organization:</td>
<td></td>
</tr>
<tr>
<td>☐ Register a new Azure AD application automatically</td>
<td></td>
</tr>
<tr>
<td>A new Veeam Backup for Microsoft 365 application will be registered in the specified Microsoft 365 organization and granted with required permissions.</td>
<td></td>
</tr>
<tr>
<td>☐ Use an existing Azure AD application</td>
<td></td>
</tr>
<tr>
<td>Use an existing pre-configured Azure AD application.</td>
<td></td>
</tr>
</tbody>
</table>
Backup of Team Chats Using Teams Export APIs

**NOTE**
If you selected the **Teams chats** check box at the **Select Organization Deployment Type** step of the wizard, registering a new Azure AD application is unavailable.

You can only select the **Use an existing Azure AD application** option. Veeam Backup for Microsoft 365 requires to provide connection parameters to the existing Azure AD application. For more information, see **Using Existing Azure AD Application**.

<table>
<thead>
<tr>
<th>Add Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Microsoft 365 connection settings</strong></td>
</tr>
<tr>
<td><strong>Select how to connect to the Microsoft 365 organization</strong>:</td>
</tr>
<tr>
<td>- Register a new Azure AD application automatically</td>
</tr>
<tr>
<td>- A new Veeam Backup for Microsoft 365 application will be registered in the specified Microsoft 365 organization and granted with the required permissions.</td>
</tr>
<tr>
<td>- Use an existing Azure AD application</td>
</tr>
<tr>
<td>- Use an existing pre-configured Azure AD application</td>
</tr>
</tbody>
</table>

| Back | Next | Cancel |
Step 5. Register or Select Azure AD Application

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

- **Registering a new application**
  Use this method if you have selected the *Register a new Azure AD application automatically* option at the previous step of the wizard.

- **Using an existing application**
  Use this method if you have selected the *Use an existing Azure AD application* option at the previous step of the wizard.

### Registering New Azure AD Application

**NOTE**

If you selected the *Teams chats* check box at the *Select Organization Deployment Type* step of the wizard, registering a new Azure AD application is unavailable.

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

When registering a new Azure AD application, Veeam Backup for Microsoft 365 automatically grants the required permissions to this application.

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

1. In the **Name** field, enter a name that you want to use to register a new Azure AD application in your Azure Active Directory.
2. Click **Install** to specify an SSL certificate that you want to use for data exchange between Veeam Backup for Microsoft 365 and an Azure AD application.
3. In the **Select Certificate** wizard, select a certificate. For more information, see *Installing SSL Certificates*.
   You can generate a new self-signed certificate or use an existing one. Before using an existing certificate, make sure to register this certificate in Azure Active Directory. For more information, see *this Microsoft article*. When generating a new self-signed certificate, Veeam Backup for Microsoft 365 will register it automatically.
4. Select the **Allow this application to enable export mode for SharePoint Web Parts** check box to allow Veeam Backup for Microsoft 365 to back up web parts of your Microsoft SharePoint websites. For more information about web parts, see *this Microsoft article*.

   By default, web parts of Microsoft SharePoint sites that belong to Microsoft 365 organization with enabled *security defaults* have the *allowexport* property set to *false* which prevents Veeam Backup for Microsoft 365 from having a direct access to such web parts.
If this check box is selected, Veeam Backup for Microsoft 365 automatically alters the `allowexport` property of each web part and sets this property to `true`. After the `allowexport` property is set to `true`, a web part can be backed up without any limitations.

### Using Existing Azure AD Application

You can specify an existing Azure AD application in your Azure Active Directory. Veeam Backup for Microsoft 365 will use this application for data exchange with your Microsoft 365 organizations during backup and restore sessions.

To use an existing application, do the following:

1. In the **Username** field, enter a user account that you want to use for impersonation. For more information about impersonation, see this Microsoft article.
   
   You can enter any account that belongs to your Microsoft 365 organization using the following format: `name@<domain_name>.<domain>`. For example, `user@abc.com`.

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

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

   You can find this number in the application settings of your Azure Active Directory. For more information, see this Microsoft article.

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

4. In the **Select Certificate** wizard, select a certificate. For more information, see Installing SSL Certificates.

   You can generate a new self-signed certificate or use an existing one. Before using an existing certificate, make sure to register this certificate in Azure Active Directory. For more information, see this Microsoft article. When generating a new self-signed certificate, Veeam Backup for Microsoft 365 will register it automatically.
5. Select the **Grant this application required permissions and register its certificate in Azure AD** check box to automatically grant **required permissions** to Azure AD application.

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

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

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

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

If this check box is selected, Veeam Backup for Microsoft 365 automatically alters the `allowexport` property of each web part and sets this property to `true`. After the `allowexport` property is set to `true`, a web part can be backed up without any limitations.
Step 6. Log In to Microsoft 365

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

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

1. Click **Copy code** to copy an authentication code.
   
   Mind that a code is valid for 15 minutes. You can click **Refresh** to request a new code from Microsoft.

2. Click the Microsoft authentication portal link.
   
   A web browser window opens.

3. On the **Sign in to your account** webpage, paste the code that you have copied and sign in to Microsoft Azure.
   
   Make sure to sign in with the user account that has the *Global Administrator* role. For more information about this role, see [this Microsoft article](#).

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

![Add Organization](image)

Log in to Microsoft 365

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

To sign in, authenticate with the below code at:

https://microsoft.com/dsaac/sign

[ ] Copy code

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

[Back] [Next] [Cancel]
Step 7. Finish Working with Wizard

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

The Microsoft 365 organization appears under the Organizations node in the inventory pane.
Adding Organizations with Modern Authentication and Legacy Protocols

When you add an organization using the modern authentication method with legacy protocols allowed, you use both Veeam Backup account and Azure AD application for authentication. Veeam Backup for Microsoft 365 uses Veeam Backup account and an application to establish a connection to your Microsoft 365 organizations with disabled security defaults and maintain data transfer during backup and restore sessions.

**NOTE**
Adding Microsoft 365 organizations using modern authentication with legacy protocols allowed is not supported for Microsoft Azure China region.

To add a new Microsoft 365 organization to Veeam Backup for Microsoft 365, check prerequisites and do the following:

1. Launch the Add Organization wizard.
2. Select an organization deployment type.
3. Select Azure region and authentication method.
4. Specify Azure AD application credentials.
5. Specify SharePoint Online, OneDrive for Business and Microsoft Teams credentials.
6. Finish the wizard.

**Before You Begin**

Before you start adding a new Microsoft 365 organization with enabled multi-factor authentication (MFA) and disabled security defaults, you must register a new Azure AD application in your Azure Active Directory.

You will be required to provide connection settings to this application at the Specify Azure AD Application Credentials step. Such an application is used for establishing and maintaining a connection to your Microsoft 365 organizations and to perform a backup and restore from/to such organizations.

Make sure to grant your Azure AD application required permissions.

Check the following:

- **Security defaults** are disabled in your Microsoft 365 organization.
- **Conditional Access policies are not blocking legacy authentication protocols** for Veeam Backup account.
Step 1. Launch Add Organization Wizard

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

1. Open the **Organizations** view.
2. Do one of the following:
   - On the **Home** tab, click **Add Org** on the ribbon.
   - In the inventory pane, right-click the **Organizations** node and select **Add organization**.
Step 2. Select Organization Deployment Type

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

To select an organization deployment type and Microsoft Online services whose data you want to protect, do the following:

1. From the Select organization deployment type drop-down list, select Microsoft 365.
2. If you want to back up Exchange Online data, select the Exchange Online check box.
3. If you want to back up SharePoint Online and OneDrive for Business data, select the SharePoint Online and OneDrive for Business check box.
4. If you want to back up Microsoft Teams data, select the Microsoft Teams check box.
   
   You can select this check box only if both Exchange Online and SharePoint Online and OneDrive for Business check boxes are selected.

NOTE
Microsoft Teams service is not supported for organizations in the Microsoft Azure China and Germany regions.
Step 3. Select Azure Region and Authentication Method

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

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

1. From the Region drop-down list, select a Microsoft Azure region your Microsoft 365 organization belongs to.
   Mind that you cannot select the China region for modern authentication with legacy protocols allowed.

2. Select the Modern authentication option and the Allow for using legacy authentication protocols check box to connect to your Microsoft 365 organization with disabled security defaults.
Step 4. Specify Azure AD Application Credentials

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

To specify Azure AD application credentials, do the following:

1. In the Application ID field, specify an identification number of your Azure AD application.
   
   You can find this number in an application settings in your Azure Active Directory. For more information, see this Microsoft article.

2. Select an Azure AD application authentication type. You can select either Application secret or Application certificate:
   
   o To use a secret key, select the Application secret option and enter a secret key in the field nearby to access your custom application.
     
     To obtain a secret key, you will need to generate it first. For more information on how to generate a secret key, see this Microsoft article.
     
     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.
   
   o To use a certificate, select the Application certificate option and click Install. For more information, see Installing SSL Certificates.
     
     Mind that you must upload a certificate file to the Azure portal beforehand. For more information, see this Microsoft article.

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

   You must provide a user account in one of the following formats: user@domain.com or user@domain.onmicrosoft.com. If you are using an ADFS account, you can only use a non-MFA enabled ADFS account.

4. Select the Grant this account required roles and permissions check box to automatically assign the ApplicationImpersonation role. This role is required to back up Microsoft 365 Exchange mailboxes.

   To assign the ApplicationImpersonation role, make sure the account that you use is a member of the Organization Management group and has been granted the Role Management role in advance.
5. Select the **Use the same credentials for SharePoint Online, OneDrive for Business and Microsoft Teams** check box if you want to use the same credentials to access your SharePoint Online, OneDrive for Business and Microsoft Teams organizations. This check box is only available if these organization types have been selected at the **Select Organization Deployment Type** step.

If the **Use the same credentials for SharePoint Online, OneDrive for Business and Microsoft Teams** check box is not selected, you will be offered to provide required credentials for the SharePoint Online, OneDrive for Business and Microsoft Teams organizations at the **Specify SharePoint Online, OneDrive for Business and Microsoft Teams Credentials** step.
Step 5. Specify SharePoint Online, OneDrive for Business and Microsoft Teams Credentials

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

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

To enter credentials, do the following:

1. In the **Application ID** field, specify an identification number of your Azure AD application.
   
   You can find this number in an application settings in your Azure Active Directory. For more information, see [this Microsoft article](#).

2. Select an Azure AD application authentication type. You can select either **Application secret** or **Application certificate**:
   
   o To use a secret key, select the **Application secret** option and enter a secret key in the field nearby to access your custom application.

   To obtain a secret key, you will need to generate it first. For more information on how to generate a secret key, see [this Microsoft article](#).

   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.

   o To use a certificate, select the **Application certificate** option and click **Install**. For more information, see [Installing SSL Certificates](#).

   Mind that you must upload a certificate file to the Azure portal beforehand. For more information, see [this Microsoft article](#).

3. In the **Username** and **App password** fields, specify a user account credentials to connect to your Microsoft 365 organization.

   You must provide a user account in one of the following formats: `user@domain.com` or `user@domain.onmicrosoft.com`. If you are using an ADFS account, you can only use a non-MFA enabled ADFS account.
4. Select the **Grant this account required roles and permissions** check box to automatically assign the *Site Collection Administrator* role that is required to back up Microsoft SharePoint Sites.
Step 6. Finish Working with Wizard

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

The Microsoft 365 organization appears under the Organizations node in the inventory pane.
Adding Organizations with Basic Authentication

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

To add a new Microsoft 365 organization to Veeam Backup for Microsoft 365, do the following:

1. **Launch the Add Organization wizard.**
2. **Select an organization deployment type.**
3. **Select Azure region and authentication method.**
4. **Specify Exchange Online credentials.**
5. **Specify SharePoint Online, OneDrive for Business and Microsoft Teams credentials.**
6. **Finish the wizard.**
Step 1. Launch Add Organization Wizard

To launch the Add Organization wizard, do the following:

1. Open the Organizations view.

2. Do one of the following:
   - On the Home tab, click Add Org on the ribbon.
   - In the inventory pane, right-click the Organizations node and select Add organization.
Step 2. Select Organization Deployment Type

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

To select an organization deployment type and Microsoft Online services whose data you want to protect, do the following:

1. From the Select organization deployment type drop-down list, select Microsoft 365.
2. If you want to back up Exchange Online data, select the Exchange Online check box.
3. If you want to back up SharePoint Online and OneDrive for Business data, select the SharePoint Online and OneDrive for Business check box.
4. If you want to back up Microsoft Teams data, select the Microsoft Teams check box.

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

NOTE
Microsoft Teams service is not supported for organizations in the Microsoft Azure China and Germany regions.

[Add Organization interface]

Select organization deployment type:
- Microsoft 365

Select the services you want to protect:
- [ ] Exchange Online
- [ ] SharePoint Online and OneDrive for Business
- [ ] Microsoft Teams

[Back, Next, Cancel buttons]
Step 3. Select Azure Region and Authentication Method

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

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

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

2. Select the **Basic authentication** option to connect to your Microsoft 365 organization using the basic authentication method.

**NOTE**

To connect to Microsoft 365 organizations that belong to *China* or *Germany* regions, Veeam Backup for Microsoft 365 requires an Azure AD application that is automatically deployed to your Azure Active Directory. To be able to deploy this application, Veeam Backup for Microsoft 365 requires the following roles to be granted to your Microsoft 365 account:

- *Application Administrator*
- *Cloud Application Administrator*
Step 4. Specify Exchange Online Credentials

At this step of the wizard, specify credentials to connect to your Exchange Online organization.

To specify credentials, do the following:

1. In the **Username** and **Password** fields, specify authentication credentials to connect to the Microsoft 365 organization.
   
   You must provide a user account in one of the following formats: *user@domain.com* or *user@domain.onmicrosoft.com*. If you are using an ADFS account, you can only use a non-MFA enabled ADFS account.

2. Select the **Grant this account required roles and permissions** check box to automatically assign the **ApplicationImpersonation** role. This role is required to back up Microsoft 365 Exchange mailboxes.
   
   To assign the **ApplicationImpersonation** role, make sure the account that you use is a member of the **Organization Management** group and has been granted the **Role Management** role in advance.

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

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

---

![Add Organization](image.png)
Step 5. Specify SharePoint Online, OneDrive for Business and Microsoft Teams Credentials

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

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

To enter credentials, do the following:

1. In the Username and Password fields, specify a user account credentials to connect to your Microsoft 365 organization.

   You must provide a user account in one of the following formats: user@domain.com or user@domain.onmicrosoft.com. If you are using an ADFS account, you can only use a non-MFA enabled ADFS account.

2. Select the Grant this account required roles and permissions check box to automatically assign the Site Collection Administrator role that is required to back up Microsoft SharePoint Sites.

   ![Add Organization](image-url)
Step 6. Finish Working with Wizard

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

The Microsoft 365 organization appears under the Organizations node in the inventory pane.
On-Premises Microsoft Organizations

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

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

To launch the Add Organization wizard, do the following:

1. Open the Organizations view.
2. Do one of the following:
   - On the Home tab, click Add Org on the ribbon.
   - In the inventory pane, right-click the Organizations node and select Add organization.
Step 2. Select Organization Deployment Type

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

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

1. From the **Select organization deployment type** drop-down list, select *On-premises*.
2. Select services that you want to protect:
   - **Microsoft Exchange Server**
     - Select this check box if you want to back up Microsoft Exchange data.
   - **Microsoft SharePoint Server**
     - Select this check box if you want to back up Microsoft SharePoint data.
Step 3. Specify Microsoft Exchange Connection Settings

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

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

1. **Server name** field, specify a Microsoft Exchange server to which you want to connect.
   
   You can use a DNS name of a server, NetBIOS name or its IP address. Make sure that the server has the Mailbox Server role.

2. In the **Username** and **Password** fields, specify authentication credentials to connect to the Microsoft Exchange server.
   
   You must provide a user account in one of the following formats: *domain\account* or *account@domain*. Consider that using ADFS accounts to add on-premises Microsoft organizations is not possible. Only Microsoft 365 organizations can be added with non-MFA enabled ADFS accounts.

3. Select the **Grant this account required roles and permissions** check box to automatically assign the *ApplicationImpersonation* role.
   
   Make sure the account that you use is a member of the *Organization Management* group and has been granted the *Role Management* role in advance. Otherwise, the automatic assignment of the *ApplicationImpersonation* role will fail; an organization will not be added.

   For more information about the required roles and permissions, see [Veeam Backup Account Permissions](#).

4. Select the **Configure throttling policy** check box to set the throttling policy for the account being used to *Unlimited*.
5. Click **Advanced** if you want to configure whether to connect to the Microsoft Exchange server using SSL and to skip one or more SSL verifications. To do this, select or clear any of the following check boxes:

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

![Advanced Settings](image)
Step 4. Specify Microsoft SharePoint Connection Settings

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

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

1. In the **Server name and port** field, specify a Microsoft SharePoint server name and the WinRM port number.
   
   You can use a DNS name of a server, NetBIOS name or its IP address.

2. In the **Username** and **Password** fields, specify authentication credentials to connect to the Microsoft SharePoint server.
   
   You must provide a user account in one of the following formats: **domain\account** or **account@domain**. Consider that using ADFS accounts to add on-premises Microsoft organizations is not possible. Only Microsoft 365 organizations can be added with non-MFA enabled ADFS accounts.

3. Select the **Grant this account required roles and permissions** check box to automatically add a user account to the SharePoint **Site Collection Administrators** group and grant this user administrative privileges to access Microsoft SharePoint sites. This option also grants access to the **User Profile** service to work with OneDrive data.

   For more information about the required roles and permissions, see [Veeam Backup Account Permissions](#).

---

**Microsoft SharePoint Server connection settings**

**Server name and port:**

- **Server name and port**: [SharePoint](#) 5986

**User account to connect with:**

- **Username**: sharepointadministrator
- **Password**: ********

- [Grant this account required roles and permissions](#)

**Click Advanced to configure additional connection security settings**

[Advanced...](#)

[Back](#)  [Next](#)  [Cancel](#)
4. Click **Advanced** if you want to configure whether to connect to the Microsoft SharePoint server using SSL and to skip one or more SSL verifications. To do this, select or clear any of the following check boxes:

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

![Advanced Settings](image)
Step 5. Finish Working with Wizard

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

An on-premises Microsoft organization appears under the **Organizations** node in the inventory pane.
Hybrid Organizations

Veeam Backup for Microsoft 365 allows you to create hybrid configurations consisting of Microsoft 365 organizations and on-premises Microsoft Exchange/SharePoint organizations.

You can add hybrid organizations as per the following scenarios:

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

NOTE

Starting from version 6a (build 6.1.0.222), Veeam Backup for Microsoft 365 can back up Microsoft Teams messages using Microsoft Teams APIs in Microsoft Graph (Teams Export APIs). This method substitutes backup of the TeamsMessagesData folder that will be deprecated by Microsoft.

For more information on how to set up Veeam Backup for Microsoft 365 to use Teams Export APIs for team chats backup, see Getting Started with Teams Export APIs.

Depending on whether you enabled usage of Teams Export APIs for team chats backup, Veeam Backup for Microsoft 365 displays different settings at the Select Organization Deployment Type step of the wizard. You can proceed to one of the following scenarios:

- **Backup of the TeamsMessagesData folder**
  
  Veeam Backup for Microsoft 365 displays these settings if you did not enable usage of Teams Export APIs for team chats backup.

- **Backup of team chats using Teams Export APIs**
  
  Veeam Backup for Microsoft 365 displays these settings if you enabled usage of Teams Export APIs for team chats backup.
Backup of TeamsMessagesData Folder

Veeam Backup for Microsoft 365 displays these settings if you did not enable usage of Teams Export APIs for team chats backup.

**NOTE**

For more information about team chats backup in Veeam Backup for Microsoft 365, see Backup of Team Chats Using Teams Export APIs.

To specify Microsoft services that you want to protect in your hybrid organization, select the following check boxes based on the listed scenarios:

- **Exchange Online**
  To back up Exchange Online data.

- **Microsoft Exchange Server**
  To back up on-premises Microsoft Exchange data.

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

- **Microsoft SharePoint Server**
  To back up on-premises Microsoft SharePoint data.

- **Microsoft Teams**
  Select this check box if you want to back up Microsoft Teams data.
  You can select this check box only if both Exchange Online and SharePoint Online and OneDrive for Business check boxes are selected.

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

- Select Microsoft Azure region and authentication method for the Microsoft 365 organization. For more information, see Microsoft 365 Organizations.

- Specify connection settings to the on-premises Microsoft Exchange and Microsoft SharePoint servers. For more information, see On-Premises Microsoft Organizations.
**NOTE**

Consider the following:

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

![Add Organization](image-url)
Backup of Team Chats Using Teams Export APIs

Veeam Backup for Microsoft 365 displays these settings if you enabled usage of Teams Export APIs for team chats backup.

To specify Microsoft services that you want to protect in your hybrid organization, select the following check boxes based on the listed scenarios:

- **Exchange Online**
  To back up Exchange Online data.

- **Microsoft Exchange Server**
  To back up on-premises Microsoft Exchange data.

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

- **Microsoft SharePoint Server**
  To back up on-premises Microsoft SharePoint data.

- **Microsoft Teams**
  Select this check box if you want to back up Microsoft Teams data.
  You can select this check box only if both **Exchange Online** and **SharePoint Online and OneDrive for Business** check boxes are selected.

- **Teams chats**
  Select this check box if you want to back up team chats using Teams Export APIs. For more information, see Organization Object Types.
  This check box is available only if the **Microsoft Teams** check box is selected.

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

- Select Microsoft Azure region and authentication method for the Microsoft 365 organization. For more information, see Microsoft 365 Organizations.

- Specify connection settings to the on-premises Microsoft Exchange and Microsoft SharePoint servers. For more information, see On-Premises Microsoft Organizations.
NOTE
Consider the following:

- To create a hybrid organization, services that you select must belong to the same Microsoft 365 organization.
- You can use a non-MFA enabled ADFS account to add a Microsoft 365 organization. Using ADFS accounts to add on-premises Microsoft organizations is not possible.
- Backup of team chats using Teams Export APIs is only supported for Microsoft 365 organizations with modern app-only authentication starting from version 6a (build 6.1.0.222).
Backup Accounts

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

To configure backup accounts, you use Microsoft 365 user accounts. You do not need to grant them any permissions or assign roles to them. Veeam Backup for Microsoft 365 automatically assigns the required roles to configured backup accounts.

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

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

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

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

   Mind that the Manage backup accounts option is unavailable for organizations with modern app-only authentication. For organizations added using modern app-only authentication, you use the Manage backup applications option. For more information, see Adding Applications.

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

   Consider the following:

   o The entire security group will be granted the Site Collection Administrator role. If a user ceases to be a member of the selected group, the role is automatically revoked for this user.

   o You should not select the All Users security group. Instead, you can create a new security group and populate this group with user accounts that you want to use during a backup session of Microsoft SharePoint data. For more information on how to create a new security group, see this Microsoft article.

   o Mail-enabled security groups are not supported.

   o Veeam Backup for Microsoft 365 does not use an account under which you add your Microsoft 365 organization.

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

7. In the **Add Password** window, enter the password for the account and click **OK**. Make sure to specify an Azure AD application password instead of a user account password when adding MFA-enabled accounts.
Changing Password and Removing Accounts

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

Changing Password

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

1. Open the Organizations view.
2. In the inventory pane, right-click an organization and select Manage backup accounts.
3. In the Backup Accounts Manager window, in the Password column, click Configured next to the backup account whose password you want to change.
4. In the Edit Password window, modify the password.
5. Click OK.

Removing Account

To remove backup accounts from the backup configuration, do the following:

1. Open the Organizations view.
2. In the inventory pane, right-click an organization and select Manage backup accounts.
3. In the Backup Accounts Manager window, in the Account column, clear check boxes next to accounts that you no longer want to use.
4. Click OK.
Backup Applications

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

**NOTE**

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

For security purposes, data exchange between applications in Azure and Veeam Backup for Microsoft 365 is maintained using SSL certificates only; you cannot use an Azure AD application secret.

**NOTE**

For Microsoft 365 organizations added using either basic authentication or modern authentication with legacy protocols allowed, you use backup accounts instead. For more information, see Backup Accounts.
Adding Applications

When you add Azure AD applications to the backup configuration, Veeam Backup for Microsoft 365 retrieves a list of existing applications from your Azure Active Directory. From this list, you can select as many applications as you need. For more information about Azure AD applications, see this Microsoft article.

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

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

   Mind that the Manage backup applications option is available only for organizations added using modern app-only authentication. For organizations added using either basic authentication or modern authentication with legacy protocols allowed, you use the Manage backup accounts option. For more information, see Adding Accounts.
3. In the **Backup Applications Manager** window, click **Add**.

![Backup Applications Manager](image)

4. In the **Add Applications** window, select Azure AD applications that you want to add and click **Add**. Make sure to manually grant the **required permissions** to Azure AD applications in advance.

Also, mind that Veeam Backup for Microsoft 365 ignores an Azure AD application that you use when adding your Microsoft 365 organization.

![Add Applications](image)
5. Click **Not configured** next to each added application to configure an SSL certificate that you want to use for secure communications between Veeam Backup for Microsoft 365 and your Azure AD application.

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

Before selecting a certificate in Veeam Backup for Microsoft 365, you must upload a certificate file to the Microsoft Azure portal. For more information, see [this Microsoft article](#).
Creating Applications

When you create a new Azure AD application, Veeam Backup for Microsoft 365 automatically registers this application in Azure Active Directory of your Microsoft 365 organization. After you create an application, Veeam Backup for Microsoft 365 automatically adds this application to the backup configuration. For more information about Azure AD applications, see this Microsoft article.

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

1. Open the Organizations view.

2. In the inventory pane, right-click a Microsoft 365 organization with enabled security defaults and select Manage backup applications.

Mind that the Manage backup applications option is available only for organizations added using modern app-only authentication. For organizations added using either basic authentication or modern authentication with legacy protocols allowed, you use the Manage backup accounts option. For more information, see Adding Accounts.
3. In the **Backup Applications Manager** window, click **Create**.

![Backup Applications Manager](image)

The **Create Application** wizard runs.

4. Enter a name that you want to use for the Azure AD application and specify an SSL certificate for secure communications between Veeam Backup for Microsoft 365 and your application. For more information on how to install a certificate, see **Installing SSL Certificates**.

Veeam Backup for Microsoft 365 will automatically register the specified certificate in your Azure Active Directory and assign this certificate to the Azure AD application. In addition, Veeam Backup for Microsoft 365 automatically grants the **Sites.FullControl.All** permission to the application.
If you want to create more than one Azure AD application, select the **Use the same name and certificate to create Applications** check box and specify how many applications Veeam Backup for Microsoft 365 must create. Applications may have the same name, however, each application always has a unique identification number. You can create maximum 100 applications per wizard session. If you need to create more than 100 applications, you can click **Create** and repeat the steps.

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

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

6. Click the Microsoft authentication portal link.

A web browser window opens.

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

Make sure to sign in with the user account that has the **Global Administrator** role. For more information about this role, see [this Microsoft article](#).
8. Return to the **Create Application** wizard and click **Finish**.

Log in to Microsoft 365

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

To sign in, authenticate with the below code at:
https://login.microsoftonline.com/device/login

DAZC8AUF

You are authenticated to Microsoft 365 as administrator@tech.club
Updating Certificates and Removing Applications

You can update an SSL certificate of each configured Azure AD application or you can remove an application from the backup configuration if you no longer want to use it. For more information on how to configure backup applications, see Adding Applications and Creating Applications.

Updating Certificate

To update a certificate, do the following:

1. Open the Organizations view.
2. In the inventory pane, right-click an organization and select Manage backup applications.
3. In the Backup Applications Manager window, in the Certificate column, click Configured next to the Azure AD application whose certificate you want to update.
4. Update the certificate using the Select Certificate wizard. For more information about this wizard, see Installing SSL Certificates.

Removing Application

To remove an application, do the following:

1. Open the Organizations view.
2. In the inventory pane, right-click an organization and select Manage backup applications.
3. In the Backup Applications Manager window, select Azure AD application that you want to remove in the list and click Remove.
   You can select multiple applications using the [CTRL] key.
Editing Organization Settings

Veeam Backup for Microsoft 365 allows you to edit a Microsoft organization settings.

To edit a Microsoft organization settings, do the following:

1. Open the Organizations view.
2. In the inventory pane, select an organization.
3. Do one of the following:
   - On the Home tab, click Edit Org on the ribbon.
   - Right-click an organization and select Edit organization.
4. Modify the required settings.

You can edit the following organization settings:

- Organization deployment type.
  Consider that you cannot change the Microsoft 365 organization deployment type to the On-premises type.
- Services that you want to protect.
- Microsoft Azure region and authentication method.
- User name and password.
Renaming Organizations

You can rename your Microsoft 365 and on-premises Microsoft organizations. Mind that you change the organization name that is displayed only in the Veeam Backup for Microsoft 365 console.

To rename an organization, do the following:

1. Open the Organizations view.
2. In the inventory pane, right-click an organization and select Rename organization.
3. In the Rename Organization wizard, select one of the following options:
   - Use the default name. To continue using the default organization name.
   - Use the following name. To use a custom name.
     When selecting this option, provide a new name and click Rename.
Consider that when creating a Mailbox Protection Reports, organizations will be shown with their default names.

Specify organization name

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

- Use the default name (abc@micr0soft.com)
- Use the following name:

  On-Premises Microsoft SharePoint
Removing Organizations

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

Consider the following:

- Backup jobs configured for the organization that you are removing will be permanently deleted.
- When removing an organization, its backups will not be removed. For local backup repositories, you can open the backed-up data as a separated database in Veeam Explorers. For more information, see the following sections:
  - Veeam Explorer for Microsoft Exchange
  - Veeam Explorer for Microsoft SharePoint
  - Veeam Explorer for Microsoft OneDrive for Business
  - Veeam Explorer for Microsoft Teams

  If backups are stored in an object storage repository, you must re-add an organization to Veeam Backup for Microsoft 365 to access the backed-up data, or use the Get-VBORestorePoint cmdlet to get restore points for an object storage repository.

To remove an organization, do the following:

1. Open the Organizations view.
2. In the inventory pane, select an organization.
3. Do one of the following:
   - On the Home tab, click Remove Organization on the ribbon.
   - Right-click an organization and select Remove organization.
Data Backup and Backup Copy

Backup

To back up data of your Microsoft 365 and on-premises Microsoft organizations, you use backup jobs.

A backup job is a configuration unit of the backup activity. A backup job defines a list of users, groups, sites, teams, and organizations to back up, a location where to store backups, a schedule according to which new backups must be created. The first backup job session always produces a full backup of all objects added to a backup job scope. Subsequent backup job sessions are incremental — Veeam Backup for Microsoft 365 processes only those objects that have changed since the last backup job session.

Backup Copy

To enhance protection of your data against disasters, you can extend your backup jobs with backup copy capabilities. Backup copy allows you to create an instance of your backed-up data in the following cloud-based object storage: Azure Blob Storage Archive access tier, Amazon S3 Glacier storage class, or Amazon S3 Glacier Deep Archive storage class.

Data in backup copies has a different storage format as those created by backup jobs: blob files in backup copies are larger. Repacking of backed-up data is performed by either Veeam Backup for Microsoft 365 backup proxy or an auxiliary archiver appliance that Veeam Backup for Microsoft 365 can create in Microsoft Azure or Amazon EC2.

As well as backup, backup copy is a job-driven process. You can create a backup copy job right after configuring a backup job or later whenever you want. For more information, see Creating Backup Copy Job.

Getting Started with Backup Copy

Before you start creating a backup copy job to protect your backups, you must perform the following actions in the Veeam Backup for Microsoft 365 backup infrastructure:

1. Add an object storage where you want to keep your backups. For more information, see Adding Object Storage Repositories.
2. Add an object storage that you want to use as a target for backup copy jobs.
   Azure Blob Storage Archive access tier, Amazon S3 Glacier and Amazon S3 Glacier Deep Archive storage classes are supported only to store backup copies. For more information, see Adding Amazon S3 Object Storage Repositories and Adding Microsoft Azure Blob Object Storage Repositories.
3. Add a backup repository extended with an object storage where you want to keep your backups.
   You will use this backup repository as a target for your backup jobs. For more information, see Adding Backup Repositories.
4. Add a backup repository extended with an archive object storage to which you want to copy your backed-up data.
   You will use this backup repository as a target for your backup copy jobs. For more information, see Adding Backup Repositories.
NOTE
An extended backup repository where you keep your backups and a backup repository where you store backup copies must be located on the same backup proxy server and have the same retention type.

5. Create a backup job. When creating a backup job, map it to the extended backup repository where you want to keep your backups. For more information, see Specify Backup Proxy and Repository.

6. Create a backup copy job for the source backup job. When creating a backup copy job, select a backup repository extended with an archive object storage as a target repository where Veeam Backup for Microsoft 365 will copy your backed-up data. For more information, see Creating Backup Copy Job.

After Veeam Backup for Microsoft 365 has created backup copies, you can retrieve your data from a backup repository extended with an archive object storage when you need it. For more information, see Retrieving Backed-Up Data.

Backups that you have retrieved become available for explore and restore. For more information, see Exploring Retrieved Data and Data Restore. Mind that you cannot explore and restore the retrieved data using Restore Portal.
Organization Object Types

Veeam Backup for Microsoft 365 allows you to specify object types and their processing and exclusion options when creating and configuring backup jobs.

The following object types are available for backup and restore:

- **Organizations**
  Consists of organization objects and their processing options.

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

- **Users**
  Consists of shared mailboxes, public mailboxes and users.

- **Sites**
  Consists of Microsoft SharePoint sites and subsites.

- **Teams**
  Consists of Microsoft Teams teams.

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

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

![Edit Processing Options](image)

If you did not enable usage of Teams Export APIs for team chats backup.
Organizations

The following table lists processing/exclusion options available for Organization type:

<table>
<thead>
<tr>
<th>Options for Microsoft 365 Organizations</th>
<th>Options for On-premises Microsoft Exchange Organizations</th>
<th>Options for On-premises Microsoft SharePoint Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail, Archive, OneDrive, Sites, Teams and Teams chats</td>
<td>Mail and Archive</td>
<td>OneDrive and Sites</td>
</tr>
</tbody>
</table>

*If you enabled usage of Teams Export APIs for team chats backup.*

Groups

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

<table>
<thead>
<tr>
<th>Group Type</th>
<th>Options for Microsoft 365 Organizations</th>
<th>Options for On-premises Microsoft Exchange Organizations</th>
</tr>
</thead>
</table>
| M365 group (available only in Microsoft 365 organizations) | When configuring Microsoft 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 options | Members with Mail and Archive options |
| Distribution Group | | |
| Dynamic Distribution Group | | |

**NOTE**

Groups are not available in on-premises Microsoft SharePoint organizations.
## Users

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

<table>
<thead>
<tr>
<th>User Type</th>
<th>Options for Microsoft 365 Organizations</th>
<th>Options for On-premises Microsoft Exchange Organizations</th>
<th>Options for On-premises Microsoft SharePoint Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td><em>Mail, Archive, OneDrive and Site</em></td>
<td><em>Mail and Archive</em></td>
<td><em>OneDrive and Site</em></td>
</tr>
<tr>
<td>Shared Mailbox (available only in Microsoft 365 and Exchange organizations)</td>
<td><em>Note</em>: Veeam Backup for Microsoft 365 backs up SharePoint sites and OneDrive accounts content that belongs to a user account added to a backup job.</td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>Public Mailbox (available only in Microsoft 365 and Exchange organizations)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Sites

Consider the following:

- Objects of the *Site* type do not have any processing/exclusion options.
- Objects of this type are not available in on-premises Microsoft SharePoint organizations.
- You can select either the *root* site, or any of its *subsites*.

In the following example, you can select either the root *Development* site which automatically selects all of its subsites, or you can select, for example, *Builds* and *Releases*. In the latter case, the root *Development* site will not be selected.
Teams

Consider the following:

- Objects of this type are available in Microsoft 365 organizations only.
- When you add an object of this type to a backup job, Veeam Backup for Microsoft 365 backs up the following objects:
  - Team chats.
    To back up team chats, Veeam Backup for Microsoft 365 does one of the following:
    - Backs up the TeamChat and TeamsMessagesData folders of the group mailbox that belongs to the Microsoft 365 group associated with the backed-up team. This is the default scenario for team chats backup in Veeam Backup for Microsoft 365.
    - Uses Teams Export APIs. You can use Teams Export APIs for team chats backup only for Microsoft 365 organizations with modern app-only authentication. To proceed to this scenario, you must set up Veeam Backup for Microsoft 365 to use Teams Export APIs for team chats backup. For more information, see Backup of Team Chats Using Teams Export APIs.
  - Document library of the SharePoint team site.
  - Team metadata, for example, settings of the team, information about team members, channels, tabs, applications.
- You can edit processing options for the Team type objects only if you enable usage of Teams Export APIs for team chats backup. For more information, see Getting Started with Teams Export APIs.

The following table lists processing options available for objects of the Team type:

<table>
<thead>
<tr>
<th>Options for Microsoft 365 Organizations with Modern App-Only Authentication</th>
<th>Options for Microsoft 365 Organizations with Modern Authentication and Legacy Protocols</th>
<th>Options for Microsoft 365 Organizations with Basic Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chats and Channels, tabs, files, membership</td>
<td>Channels, tabs, files, membership</td>
<td>Channels, tabs, files, membership</td>
</tr>
</tbody>
</table>

**Note:** Channels, tabs, files, membership of a team are always processed.

Backup of Team Chats Using Teams Export APIs

Starting from version 6a (build 6.1.0.222), Veeam Backup for Microsoft 365 can back up Microsoft Teams messages using Microsoft Teams APIs in Microsoft Graph (Teams Export APIs). This method substitutes backup of the TeamsMessagesData folder that will be deprecated by Microsoft.

Teams Export APIs allow Veeam Backup for Microsoft 365 to access sensitive data of team chats, including channel messages. As a result, Veeam Backup for Microsoft 365 can back up such objects.
Because Teams Export APIs provide access to sensitive data, they are considered protected APIs. This is a reason that before starting to use Teams Export APIs in Veeam Backup for Microsoft 365, you must pass additional validation and grant permissions. For more information, see Getting Started with Teams Export APIs.

Consider the following:

- Microsoft applies an additional cost for using Microsoft Teams APIs in Microsoft Graph. Veeam Backup for Microsoft 365 API requests will be qualified as Model B.
- Backup of team chats using the Teams Export APIs is only supported for Microsoft 365 organizations with modern app-only authentication.
- Backup of team chats using Teams Export APIs is not supported for Microsoft organizations in the Microsoft Azure China, Germany, US Government GCC and US Government GCC High regions.

For more information about Teams Export APIs, see this Microsoft article.

Getting Started with Teams Export APIs

To set up Veeam Backup for Microsoft 365 to use Teams Export APIs for team chats backup, do the following:

1. In Microsoft Forms, fill out the request form required by Microsoft.
   Mind that processing your request to access Teams Export APIs may take up to 2 weeks. For more information on how to fill out the request form, see this Veeam KB article.

2. Enable usage of Teams Export APIs for team chats backup. Do the following:
   a. Run the `Set-VBOServer` cmdlet.
   b. Run the `Set-VBOProxy` cmdlet with the `EnableTeamsGraphAPIBackup` parameter.

   **NOTE**
   If you enabled usage of Teams Export APIs for team chats backup in PowerShell, you can not revert this action.
   For more information, see this Veeam KB article.

3. In the Add Organization or Edit Organization wizard, select the Teams chats check box when adding a new Microsoft 365 organization with modern app-only authentication or editing an existing one. If you do not select this check box, Veeam Backup for Microsoft 365 will not back up team chats.

4. Do one of the following to enable access for an existing Azure AD application to all Teams public channel messages:
   - In the Add Organization or Edit Organization wizard, allow Veeam Backup for Microsoft 365 to grant automatically the `ChannelMessage.Read.All` Microsoft Graph API permission to an existing Azure AD application when adding a new Microsoft 365 organization with modern app-only authentication or editing an existing one. For more information, see Adding Organizations with Modern App-Only Authentication.
   - In the Microsoft Azure portal, grant manually the `ChannelMessage.Read.All` Microsoft Graph API permission to this Azure AD application. For more information, see Permissions for Modern App-Only Authentication.

For more information on how to set up Veeam Backup for Microsoft 365 to use Teams Export APIs, see this Veeam KB article.
Creating Backup Job

To create a backup job, do the following:

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

To launch the New Backup Job wizard, do the following:

1. Open the Organizations view.

2. In the inventory pane, select an organization for which you want to create a backup job.

3. Do one of the following:
   - On the Home tab, click Backup on the ribbon.
   - Right-click an organization and select Add to backup job.
Step 2. Specify Backup Job Name

At this step of the wizard, enter a name for the backup job and provide optional description:

1. In the **Name** field, enter a name for the backup job.
2. In the **Description** field, enter optional description.
Step 3. Select Objects to Back Up

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

In Veeam Backup for Microsoft 365, you can select to back up the entire organization or choose specific users, groups, sites, teams, and organizations.

Consider the following:

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

To select objects to back up, do the following:

1. Select one of the following options:
   - Back up entire organization to back up all objects within the selected Microsoft organization.
   - Back up the following objects to back up specific users, groups, sites, teams, and organizations.

2. If you selected the Back up the following objects option, click Add and select one of the following options: Users, Groups, Sites, Teams, or Organization.

**NOTE**

If you select a group, site or team as an individual object for backup (and not as a part of a user account, group or organization), this object does not consume a unit in the Veeam license.
### Configuring Users Backup

**TIP**

Mind the following:
- To switch between objects of different types, you can click the buttons in the upper-right corner.
- To refresh the objects list, you can click **Refresh**.
- To quickly find necessary objects, you can use the search field at the bottom.

To configure *Users* backup, do the following:

1. In the **Add Objects** window, select check boxes next to the users that you want to back up.

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
<th>Office</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SharedMBL_6</td>
<td>SharedMBL_6@ci</td>
<td></td>
<td>User</td>
</tr>
<tr>
<td>SharedMBL_7</td>
<td>SharedMBL_7@ci</td>
<td></td>
<td>User</td>
</tr>
<tr>
<td>SharedMBL_70</td>
<td>SharedMBL_70@ci</td>
<td></td>
<td>User</td>
</tr>
<tr>
<td>SharedMBL_71</td>
<td>SharedMBL_71@ci</td>
<td></td>
<td>User</td>
</tr>
<tr>
<td>SharedMBL_72</td>
<td>SharedMBL_72@ci</td>
<td></td>
<td>User</td>
</tr>
<tr>
<td>SharedMBL_73</td>
<td>SharedMBL_73@ci</td>
<td></td>
<td>User</td>
</tr>
<tr>
<td>SharedMBL_74</td>
<td>SharedMBL_74@ci</td>
<td></td>
<td>User</td>
</tr>
<tr>
<td>SharedMBL_75</td>
<td>SharedMBL_75@ci</td>
<td></td>
<td>User</td>
</tr>
<tr>
<td>SharedMBL_76</td>
<td>SharedMBL_76@ci</td>
<td></td>
<td>User</td>
</tr>
<tr>
<td>SharedMBL_77</td>
<td>SharedMBL_77@ci</td>
<td></td>
<td>User</td>
</tr>
<tr>
<td>SharedMBL_78</td>
<td>SharedMBL_78@ci</td>
<td></td>
<td>User</td>
</tr>
<tr>
<td>SharedMBL_79</td>
<td>SharedMBL_79@ci</td>
<td></td>
<td>User</td>
</tr>
<tr>
<td>SharedMBL_80</td>
<td>SharedMBL_80@ci</td>
<td></td>
<td>User</td>
</tr>
<tr>
<td>SharedMBL_81</td>
<td>SharedMBL_81@ci</td>
<td></td>
<td>User</td>
</tr>
</tbody>
</table>

   *1 user selected*

   [Type in an object name to search for]

   Add   Cancel

2. Click **Add**.

The selected objects appear in the list of objects to back up.
3. If you want to specify processing options, select the necessary User type object and click **Edit**.
   Mind that you cannot edit processing options for the **Public Mailbox** objects.

4. In the **Edit Processing Options** window, select check boxes next to the processing options that you want to apply, and click **OK**.
   For more information about available User types and their processing options, see **Organization Object Types**.


# Configuring Groups Backup

## TIP

Mind the following:

- To switch between objects of different types, you can click the buttons in the upper-right corner.
- To refresh the objects list, you can click **Refresh**.
- To quickly find necessary objects, you can use the search field at the bottom.

To configure *Groups* backup, do the following:

1. In the **Add Objects** window, select check boxes next to the groups that you want to back up.

2. Click **Add**.

   The selected objects appear in the list of objects to back up.
3. If you want to specify processing options, select the necessary Group type object and click **Edit**.

4. In the **Edit Processing Options** window, select check boxes next to the processing options that you want to apply, and click **OK**.

For more information about available Group types and their processing options, see **Organization Object Types**.
Configuring Sites Backup

TIP

Mind the following:

- To switch between objects of different types, you can click the buttons in the upper-right corner.
- To refresh the objects list, you can click **Refresh**.
- To quickly find necessary objects, you can use the search field at the bottom. Search is available only for personal sites and subsites displayed in the objects tree.

To configure Sites backup, do the following:

1. In the **Add Objects** window, select check boxes next to the sites or subsites that you want to back up. Mind that you need to expand the **Personal Sites** node or a node of a parent site to view all personal sites or subsites.

2. Click **Add**.

   The selected objects appear in the list of objects to back up. Mind that you cannot edit processing options for the **Site** type objects. For more information about the **Site** type, see **Organization Object Types**.
Configuring Teams Backup

**TIP**

Mind the following:
- To switch between objects of different types, you can click the buttons in the upper-right corner.
- To refresh the objects list, you can click **Refresh**.
- To quickly find necessary objects, you can use the search field at the bottom.

To configure *Teams* backup, do the following:

1. In the **Add Objects** window, select check boxes next to the teams that you want to back up.

   ![Add Objects Window](image)

   - Click **Add**.
     - The selected objects appear in the list of objects to back up.
   - If you want to specify processing options, select the necessary *Team* type object and click **Edit**.
NOTE
You can edit processing options for the Team type objects only if you set up Veeam Backup for Microsoft 365 to use Teams Export APIs for team chats backup.
For more information, see Getting Started with Teams Export APIs.

4. In the Edit Processing Options window, select check boxes next to the processing options that you want to apply, and click OK.

For more information about the Team type and its processing options, see Organization Object Types.

Mind that the Chats check box is available for editing only if you selected the Teams chats check box when adding a Microsoft 365 organization with modern app-only authentication.
Configuring Organization Backup

TIP
Mind the following:

- To switch between objects of different types, you can click the buttons in the upper-right corner.
- To refresh the objects list, you can click Refresh.
- To quickly find necessary objects, you can use the search field at the bottom.

To configure Organization backup, do the following:

1. In the Add Objects window, select check boxes next to the organizations that you want to back up.

   ![Add Objects Window](image)

2. Click Add.

   The selected objects appear in the list of objects to back up.
3. If you want to specify processing options, select the necessary *Organization* type object and click **Edit**.

4. In the **Edit Processing Options** window, select check boxes next to the processing options that you want to apply, and click **OK**.

For more information about the *Organization* type and its processing options, see [Organization Object Types](#).

Mind that the **Teams chats** check box is displayed only if you set up Veeam Backup for Microsoft 365 to use Teams Export APIs for team chats backup. This check box is available for editing only if you selected the **Teams chats** check box when adding a Microsoft 365 organization with modern app-only authentication.
Step 4. Select Objects to Exclude

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

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

**NOTE**

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

If you want to specify exclusion options, select an object in the list, click **Edit** and in the **Edit Exclusions** window, select exclusion options that you want to apply.

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

**NOTE**

You cannot edit exclusion options for the **Sites**, **Teams** and **Public Mailbox** objects.
The following is an example where the *Mail*, *Archive* and *Site* are excluded from the backup for the *Administrator* user. Veeam Backup for Microsoft 365 will only back up *OneDrive* data for this user.

To see what Veeam Backup for Microsoft 365 will exclude for the selected object to exclude, refer to the *Exclude* column. In this example, Veeam Backup for Microsoft 365 will exclude *Mail*, *Archive* and *Site*. 
Step 5. Specify Backup Proxy and Repository

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

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

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

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

You can select a standard backup repository or backup repository that was extended with object storage. When selecting an extended backup repository, all data will be compressed and backed up directly to object storage; Veeam Backup for Microsoft 365 saves only cache to the extended backup repository.

**NOTE**

If you want to extend a backup job with backup copy capabilities, you must specify an extended backup repository.
Step 6. Specify Scheduling Options

At this step of the wizard, configure a schedule for your backup job and actions that will be performed after completion of the wizard.

To configure a schedule, do the following:

1. If you want Veeam Backup for Microsoft 365 to run your backup job automatically in accordance with the schedule, select the Run the job automatically check box and customize a schedule. You can select one of the following options:
   - **Daily at this time.** Select this option if you want to run the job on the specified days at the specified hours.
   - **Periodically every.** Select this option if you want to run the job every \( N \) minutes or hours. If you select the period in hours, click Schedule and specify allowed and prohibited hours for the backup job to run. For more information, see Selecting Time Periods.

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

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

4. In the When I click Create section, do the following:
   a. Select the Start the job check box if you want to start a backup job right after completion of the wizard.
      If you do not want to start the job immediately, you can start it later. For more information, see Starting Backup Job.
   b. Select the Create a backup copy for this job check box if you want to configure archiving of backups created by Veeam Backup for Microsoft 365.
      Right after you click Create, you will be taken to the Select Target Backup Repository step of the New Backup Copy Job wizard.
      Mind that this check box is available only if the following conditions are met:
       - You have specified a backup repository that was extended with object storage to keep your backups.
You have added backup repositories extended with the Azure Blob Storage Archive access tier, Amazon S3 Glacier or Amazon S3 Glacier Deep Archive storage to the Veeam Backup for Microsoft 365 backup infrastructure.

If you do not want to configure a backup copy job immediately, you can launch the **New Backup Copy Job** wizard later. For more information, see Launch New Backup Copy Job Wizard.

### Selecting Time Periods

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

- Set the **Permitted** execution time frame for the backup job.
- Set the **Denied** execution time frame for the backup job.
- [In the **Schedule** window only] Specify a number of minutes for which you want to shift starting of the backup job within an hour if several backup jobs are scheduled to be started simultaneously. Using this option allows you to decrease the load on the Veeam Backup for Microsoft 365 backup infrastructure.

The main area of the dialog is divided into two axes:

- The vertical axis represents days of the week from Sunday to Saturday.
- The horizontal axis represents time intervals from 12 AM to 11:59 PM.

Within these axes a matrix is placed consisting of blocks. Each block represents a 59 minutes interval for each day of the week. The total number of blocks is 168 (24 blocks per each day of the week).
To set up an execution frame for the backup job, do the following:

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

   In addition, you can:
   a. Select multiple blocks simultaneously by clicking and holding the mouse pointer on the first block and dragging it until the last one that you want to use, including different days of the week.
   b. Click a day of the week in the vertical axis to select all the blocks of the day.
   c. Click All in the vertical axis to select all the blocks of the entire week.

2. On the right-hand side, select either the **Permitted** or **Denied** option to set up the execution rule for the selected blocks.

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

- Monday from 03:00 AM up until 09:59 AM.
- Thursday from 02:00 PM up until 08:59 PM.
Creating Backup Copy Job

To create a backup copy job, do the following:

1. **Launch the New Backup Copy Job wizard.**
2. **Select a target backup repository.**
3. **Specify scheduling options.**
Step 1. Launch New Backup Copy Job Wizard

**NOTE**

Backup copy capabilities are only available if you have specified an extended backup repository as a target for your backup jobs. For more information, see Specify Backup Proxy and Repository.

To launch the New Backup Copy Job wizard, do the following:

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

**TIP**

You can also select the root Organizations node to see all backup and backup copy jobs created for all organizations added to the scope.

3. In the preview pane, do one of the following:
   - Select a backup job for which you want to create a backup copy and on the Jobs tab, click Backup Copy on the ribbon.
   - Right-click a backup job and select Add to backup copy job.

Mind that you can create only one backup copy job per backup job.
Step 2. Select Target Backup Repository

At this step of the wizard, specify a backup repository that you want to use as a target for the backup copy job.

Consider the following:

- You can use only backup repositories extended with the Azure Blob Storage Archive access tier, Amazon S3 Glacier or Amazon S3 Glacier Deep Archive storage as a target for backup copy jobs.
- An extended backup repository where you keep your backups and a target backup repository must be located on the same backup proxy server and have the same retention type.

To specify a target backup repository, do the following:

1. In the **Backup job containing objects to process** field, check the backup job name.
2. From the **Target backup repository** drop-down list, select a backup repository extended with an archive object storage to which you want to copy your backed-up data.

![New Backup Copy Job](image)

Specify backup copy options

- **Backup job containing objects to process**: Full Backup
- **Target backup repository**: Amazon Archive (Created by SR\007\Administrator at 22:16 PM)
  - 97.4 GB free of 129.4 GB

*Only repositories of the same proxy and the same retention type as the source backup repository are shown.*
Step 3. Specify Scheduling Options

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

To configure a schedule, do the following:

1. In the Run backup copy job section, select one of the following options:
   - **Immediate**. Select this option if you want to run the backup copy job right after the latest restore point appears in the source backup repository. Veeam Backup for Microsoft 365 copies each restore point created by the source backup job (backup job for which you create a backup copy job).
   - **Daily at this time**. Select this option if you want to run the backup copy job on the specified days at the specified hours.
   - **Periodically every**. Select this option if you want to run the backup copy job every N minutes or hours. Mind that if you run your backup copy job daily or periodically, Veeam Backup for Microsoft 365 copies only the latest restore point that appeared in the source backup repository since the last run of this backup copy job.

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

Selecting Time Periods

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

- Set the **Permitted** execution time frame for the backup copy job.
- Set the **Denied** execution time frame for the backup copy job.

The main area of the dialog is divided into two axes:

- The vertical axis represents days of the week from Sunday to Saturday.
- The horizontal axis represents time intervals from 12 AM to 11:59 PM.
Within these axes a matrix is placed consisting of blocks. Each block represents a 59 minutes interval for each day of the week. The total number of blocks is 168 (24 blocks per each day of the week).

To set up an execution frame for the backup copy job, do the following:

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

   In addition, you can:
   a. Select multiple blocks simultaneously by clicking and holding the mouse pointer on the first block and dragging it until the last one that you want to use, including different days of the week.
   b. Click a day of the week in the vertical axis to select all the blocks of the day.
   c. Click All in the vertical axis to select all the blocks of the entire week.

2. On the right-hand side, select either the **Permitted** or **Denied** option to set up the execution rule for the selected blocks.

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

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

You can manage backup jobs that you created in Veeam Backup for Microsoft 365. For example, you can edit the settings of a backup job, start, stop, disable, remove backup jobs, explore backups created by backup jobs.
Starting Backup Job

To start a backup job, do the following:

1. Open the **Organizations** view.

2. In the inventory pane, select an organization.

   **TIP**
   
   You can also select the root **Organizations** node to see all backup and backup copy jobs that created for all organizations added to the scope.

3. In the preview pane, do one of the following:
   
   o Select a backup job and on the **Jobs** tab, click **Start** on the ribbon.
   
   o Right-click a backup job and select **Start**.
Stopping Backup Job

When Veeam Backup for Microsoft 365 stops a backup job, it preserves the data that has already been backed up. If you want to continue, use the **Start** command. For more information, see [Starting Backup Job](#).

Mind that when you restart the backup job, Veeam Backup for Microsoft 365 starts data processing from the beginning and may need additional time to re-identify the state of the backed-up data. After that Veeam Backup for Microsoft 365 continues with the remaining data to back up.

To stop a backup job, do the following:

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

   **TIP**
   
   You can also select the root **Organizations** node to see all backup and backup copy jobs that created for all organizations added to the scope.

3. In the preview pane, do one of the following:
   - Select a backup job and on the **Jobs** tab, click **Stop** on the ribbon.
   - Right-click a backup job and select **Stop**.

   ![Backup Job stops](image)
Enabling or Disabling Backup Job

You can enable or disable a backup job.

Consider the following:

- If a backup job is enabled, it can be executed on schedule.
- If a backup job is disabled, it cannot be executed on schedule but you can run it manually using the Start command. For more information, see Starting Backup Job.

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

1. Open the Organizations view.
2. In the inventory pane, select an organization.
   
   **TIP**
   
   You can also select the root Organizations node to see all backup and backup copy jobs that were created for all organizations added to the scope.

3. In the preview pane, do one of the following:
   - Select a backup job and on the Jobs tab, click Enable or Disable on the ribbon.
   - Right-click a backup job and select Enable or Disable.
Editing Backup Job Settings

Veeam Backup for Microsoft 365 allows you to edit a backup job settings.

To edit settings of a backup job, do the following:

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

   **TIP**
   
   You can also select the root **Organizations** node to see all backup and backup copy jobs that created for all organizations added to the scope.

3. In the preview pane, do one of the following:
   - Select a backup job and on the **Jobs** tab, click **Edit** on the ribbon.
   - Right-click a backup job and select **Edit**.
4. Modify the required settings.

   You can change the following parameters:
   - The name and description of a backup job.
   - The list of objects to back up and their processing options.
   - The list of objects to exclude and their exclusion options.

   Also, you can select another backup proxy server and backup repository, and reconfigure a backup job scheduling options.

   **NOTE**

   You cannot select another backup proxy server and backup repository with a different retention type if you edit a backup job for which a backup copy job is already created.
Removing Backup Job

You can remove a backup job from the Veeam Backup for Microsoft 365 configuration.

**NOTE**
Consider the following:

- When you remove a backup job, Veeam Backup for Microsoft 365 keeps the backup data in the backup location.
- When you remove a backup job, Veeam Backup for Microsoft 365 removes a backup copy job as well if such job was created for a backup job.

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

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

**TIP**
You can also select the root **Organizations** node to see all backup and backup copy jobs that created for all organizations added to the scope.

3. In the preview pane, do one of the following:
   - Select a backup job and on the **Jobs** tab, click **Delete** on the ribbon.
   - Right-click a backup job and select **Delete**.
Exploring Backup Job

You can open backups created by a backup job.

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

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

   **TIP**
   
   You can also select the root **Organizations** node to see all backup and backup copy jobs that created for all organizations added to the scope.

3. In the preview pane, do one of the following:
   - Select a backup job and on the **Jobs** tab, click **Explore** on the ribbon and select **Explore latest <product> state of <date_and_time>** or **Explore <product> point-in-time state**.
   - Right-click a backup job and select **Explore latest <product> state of <date_and_time>** or **Explore <product> point-in-time state**.

4. Proceed to **Data Restore**.
Upgrading Backup Job

After you upgrade Veeam Backup for Microsoft 365 to version 6.0, the existing backup jobs that were created with an earlier version of the product must be upgraded manually. This applies to the backup jobs created with Veeam Backup for Microsoft 365 versions 4.0, 4a and 4b that contain Office 365 group objects.

To upgrade backup jobs, do the following:

1. Open the Organizations view.
2. In the inventory pane, select an organization and then the Out of Date node.
3. In the preview pane, do one of the following:
   - Select a backup job and on the Jobs tab, click Upgrade on the ribbon.
   - Right-click a backup job and select Upgrade.
Managing Backup Copy Jobs

You can manage backup copy jobs that you created for your backup jobs in Veeam Backup for Microsoft 365. For example, you can edit the settings of a backup copy job, start, stop, disable, remove backup copy jobs.
Starting Backup Copy Job

By default, a backup copy job starts automatically either right after appearing of the latest restore point in the source backup repository or if you configure to run your backup copy job periodically – right after its creation and then in the specified time interval.

You can start your backup copy job manually. Manual start can be helpful if the backup copy job was disabled for some time or if a new restore point has already appeared in the source backup repository but the backup copy job was configured to run daily or periodically.

NOTE
Consider the following:

- Veeam Backup for Microsoft 365 processes only the latest restore point that appeared in the source backup repository since this backup copy job was created.
- Restore points created by the previous versions of Veeam Backup for Microsoft 365 are not processed.

To start a backup copy job manually, do the following:

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

TIP
You can also select the root Organizations node to see all backup and backup copy jobs that created for all organizations added to the scope.
3. In the preview pane, do one of the following:

   - Select a backup copy job and on the Jobs tab, click **Start** on the ribbon.
   - Right-click a backup copy job and select **Start**.

   A backup copy job name consists of a backup job name for which a backup copy job is created and the *copy job postfix*. 
Stopping Backup Copy Job

To stop a backup copy job, do the following:

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

   **TIP**

   You can also select the root **Organizations** node to see all backup and backup copy jobs that created for all organizations added to the scope.

3. In the preview pane, do one of the following:
   
   - Select a backup copy job and on the **Jobs** tab, click **Stop** on the ribbon.
   - Right-click a backup copy job and select **Stop**.

   A backup copy job name consists of a backup job name for which a backup copy job is created and the **copy job postfix**.
Enabling or Disabling Backup Copy Job

You can enable or disable a backup copy job.

Consider the following:

- If a backup copy job is enabled, it can be executed on schedule.
- If a backup copy job is disabled, it cannot be executed on schedule but you can run it manually using the Start command. For more information, see Starting Backup Copy Job.

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

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

   **TIP**
   
   You can also select the root Organizations node to see all backup and backup copy jobs that created for all organizations added to the scope.

3. In the preview pane, do one of the following:
   
   - Select a backup copy job and on the Jobs tab, click **Enable** or **Disable** on the ribbon.
   - Right-click a backup copy job and select **Enable** or **Disable**.

   A backup copy job name consists of a backup job name for which a backup copy job is created and the *copy job* postfix.
Editing Backup Copy Job Settings

Veeam Backup for Microsoft 365 allows you to edit a backup copy job settings.

To edit settings of a backup copy job, do the following:

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

**TIP**
You can also select the root **Organizations** node to see all backup and backup copy jobs that created for all organizations added to the scope.

3. In the preview pane, do one of the following:
   - Select a backup copy job and on the **Jobs** tab, click **Edit** on the ribbon.
   - Right-click a backup copy job and select **Edit**.

A backup copy job name consists of a backup job name for which a backup copy job is created and the **copy job** postfix.

4. Modify the required settings.
   You can change a **target backup repository** and reconfigure a backup copy job scheduling options.
Removing Backup Copy Job

You can remove a backup copy job from the Veeam Backup for Microsoft 365 configuration.

**NOTE**
When you remove a backup copy job, Veeam Backup for Microsoft 365 keeps the backed-up files in the target backup repository extended with an archive object storage. You can retrieve your backed-up data from the target backup repository. For more information, see Retrieving Backed-Up Data.

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

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

**TIP**
You can also select the root Organizations node to see all backup and backup copy jobs that created for all organizations added to the scope.

3. In the preview pane, do one of the following:
   - Select a backup copy job and on the Jobs tab, click **Delete** on the ribbon.
   - Right-click a backup copy job and select **Delete**.

A backup copy job name consists of a backup job name for which a backup copy job is created and the copy job postfix.
Retrieving Backed-Up Data

Data retrieval is the process of receiving temporary access to archived data, so that it can be explored.

As well as data backup and backup copy, data retrieval is a job-driven process. When you want to access your data in backup copies, you create a retrieval job. For more information, see Creating Retrieval Job.

**NOTE**

If you want to view the created retrieval jobs and their statuses, in the inventory pane, open the Organizations view, select the Data retrieval node and view the list in the preview pane.

When the retrieval job is complete, the retrieved data will be available for a specified period of time, during which you can explore and restore your data using Veeam Explorers. You can extend the availability period for data that Veeam Backup for Microsoft 365 has retrieved. For more information, see Editing Retrieval Job Settings and Extending Availability of Retrieved Data.

Data retrieval cost varies depending on the desired speed of the process. You can select an option that you prefer at the Select Retrieval Mode step of the Retrieve Backup Copy wizard. Mind that options differ for Azure Blob Storage Archive, Amazon S3 Glacier and Amazon S3 Glacier Deep Archive.
Creating Retrieval Job

To create a retrieval job, do the following:

1. Launch the Retrieve Backup Copy wizard.
2. Specify a retrieval job name.
3. Specify point in time.
4. Select an organization.
5. Select objects.
6. Select a retrieval mode.
7. Specify data availability period.
Step 1. Launch Retrieve Backup Copy Wizard

To launch the Retrieve Backup Copy wizard, do the following:

1. Open the Backup Infrastructure view.
2. In the inventory pane, select the Backup Repositories node.
3. In the preview pane, do one of the following:
   - Select a backup repository extended with an archive object storage and on the Backup Repository tab, click Retrieve Data on the ribbon and select Retrieve <product> data.
   - Right-click a backup repository extended with an archive object storage and select Retrieve <product> data.

**NOTE**

The Retrieve <product> data option is one of the following:

- **Retrieve Exchange data.** Use this option to create a retrieval job for the subsequent explore and restore of the retrieved data using Veeam Explorer for Microsoft Exchange.
- **Retrieve SharePoint data.** Use this option to create a retrieval job for the subsequent explore and restore of the retrieved data using Veeam Explorer for Microsoft SharePoint.
- **Retrieve OneDrive data.** Use this option to create a retrieval job for the subsequent explore and restore of the retrieved data using Veeam Explorer for Microsoft OneDrive for Business.
- **Retrieve Teams data.** Use this option to create a retrieval job for the subsequent explore and restore of the retrieved data using Veeam Explorer for Microsoft Teams.
Step 2. Specify Retrieval Job Name

At this step of the wizard, edit the suggested name for the retrieval job if needed and provide optional description:

1. In the **Name** field, edit the retrieval job name that Veeam Backup for Microsoft 365 suggests.
2. In the **Description** field, enter optional description.

![Retrieve Backup Copy](image)

Specify data retrieval name and description

<table>
<thead>
<tr>
<th>Name:</th>
<th>Exchange data retrieval</th>
</tr>
</thead>
</table>

| Description: | Created by (SPV01D)\Administrator at 11:40:40 PM |

[Previous] [Next] [Cancel]
**Step 3. Specify Point In Time**

At this step of the wizard, select a backup state of the archived data that you want to retrieve from archive:

1. Select one of the following options:
   - **Use the latest available state.** Select this option to retrieve the latest state of the archived data.
   - **Use the following point in time.** Select this option to retrieve the archived data of the selected date.

2. If you want to view historic data, select the following check boxes:
   - **Show items that have been deleted by user.** Select this option to show items that have been removed by the user before the specified date.
   - **Show all versions of items that have been modified by user.** Select this option to show all versions of items that have been modified by the user before the specified date.

---

**Specify point in time**

Specify point in time you want to retrieve from an archive repository:

- [ ] Use the latest available state
- [x] Use the following point in time:

  Thursday, February 24, 2022 12:19:39 AM

Use these eDiscovery settings to find mailbox items which are no longer present in the selected state. Enabling these options may significantly increase the amount of data returned by queries.

- [x] Show items that have been deleted by user
- [x] Show all versions of items that have been modified by user

[Back] [Next] [Cancel]
Step 4. Select Organization

At this step of the wizard, select an organization. Veeam Backup for Microsoft 365 will retrieve from the archive backed-up data of objects that are belong to the selected organization.
Step 5. Select Objects

At this step of the wizard, select check boxes next to the objects (mailboxes, OneDrives, teams) whose backed-up data you want to retrieve from the archive.

Selecting SharePoint Sites

If you want to retrieve backed-up data of the SharePoint sites, do the following:

1. Click Add.
2. In the **Add Objects** window, select check boxes next to the sites or subsites whose backed-up data you want to retrieve from the archive.

3. Click **Add**.

   The selected objects appear in the list of SharePoint sites whose backed-up data you want to retrieve from the archive.
Step 6. Select Retrieval Mode

At this step of the wizard, select a retrieval mode that you want to use. Data retrieval cost varies depending on the desired speed of the process. Options differ for Azure Blob Storage Archive, Amazon S3 Glacier and Amazon S3 Glacier Deep Archive.

Amazon S3 Glacier / Amazon S3 Glacier Deep Archive

Select one of the following options:

- **Expedited (most expensive)**
  Use this option to access your backed-up data within several minutes.

- **Standard**
  Use this option to access your backed-up data within several hours.

- **Bulk (lowest cost)**
  Use this option to access your backed-up data within the longer time period.

Azure Blob Storage Archive

Select one of the following options:

- **High Priority (most expensive)**
  Use this option to access your backed-up data within 1 hour.
- **Standard Priority (lowest cost)**
  
  Use this option to access your backed-up data within several hours.

Select retrieval mode

- **High Priority (most expensive)**
  
  High Priority retrievals allow you to quickly access archived backup files. Data accessed using High Priority retrievals are typically made available within less than one hour.

- **Standard Priority (lowest cost)**
  
  Standard Priority retrievals allow you to access archived backups within several hours. Standard Priority retrievals typically complete within up to 15 hours.
Step 7. Specify Availability Period

At this step of the wizard, specify the availability period that you want to apply for the retrieved backed-up data. During this period you will be able to explore and restore your data using Veeam Explorers. For more information, see Exploring Retrieved Data.

If you want to receive a notification that the availability period is about to end, select the Send a notification email N hours before the retrieved data expires check box and specify the time for the notification.

**NOTE**

You can extend the availability period if necessary. For more information, see Editing Retrieval Job Settings and Extending Availability of Retrieved Data.

<table>
<thead>
<tr>
<th>Retrieve Backup Copy</th>
<th>X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify availability period</td>
<td></td>
</tr>
<tr>
<td>Keep retrieved data available for</td>
<td>days</td>
</tr>
<tr>
<td>Controls how long to keep the retrieved data in the hot tier for. You will be able to prolong data availability manually. If a restore process is still running when the data expires, the availability period will be automatically prolonged for the remaining duration of the restore process.</td>
<td></td>
</tr>
<tr>
<td>Send a notification email</td>
<td>hours before the retrieved data expires</td>
</tr>
</tbody>
</table>

| Back | Finish | Cancel |
Editing Retrieval Job Settings

Veeam Backup for Microsoft 365 allows you to edit a retrieval job settings.

To edit settings of a retrieval job, do the following:

1. Open the Organizations view.

2. In the inventory pane, select the Data retrieval node.

3. In the preview pane, do one of the following:
   - Select a retrieval job and on the Retrievals tab, click Edit on the ribbon.
   - Right-click a retrieval job and select Edit.

4. Modify the required settings.
   
   You can change the following parameters:
   - The name and description of a retrieval job.
   - The availability period of the retrieved backed-up data.
Extending Availability of Retrieved Data

You can extend the availability period of the retrieved backed-up data.

To extend the availability period of the retrieved backed-up data, do the following:

1. Open the Organizations view.
2. In the inventory pane, select the Data retrieval node.
3. In the preview pane, do one of the following:
   - Select a retrieval job with backed-up data which availability period you want to extend and on the Retrievals tab, click Extend Availability on the ribbon.
   - Right-click a retrieval job and select Extend Availability.
4. In the wizard window that opens, specify number of days during which the retrieved backed-up data will be available to explore and restore using Veeam Explorers.
5. If you want to receive a notification that the availability period is about to end, select the Send a notification email N hours before the retrieved data expires check box and specify the time for the notification.
Data Restore

To restore Microsoft organization data, you can use Veeam Explorers and Restore Portal:

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

- **Veeam Explorer for Microsoft SharePoint**
  To explore and restore Microsoft SharePoint sites, libraries and items.

- **Veeam Explorer for Microsoft OneDrive for Business**
  To explore and restore Microsoft OneDrive for Business items and folders.

- **Veeam Explorer for Microsoft Teams**
  To explore and restore Microsoft Teams teams, channels, tabs, posts and files.

- **Restore Portal**
  To explore and restore Microsoft Exchange, Microsoft SharePoint and Microsoft OneDrive for Business data using Restore Portal. Restore Portal allows users to perform self-service restore.

To launch Veeam Explorers, you use the **Explore** option. For more information, see the following sections:

- **Exploring Backup Jobs**
  To open backups created by the selected backup job.

- **Exploring Single Organization**
  To open backups created by all backup jobs of a specific organization.

- **Exploring All Organizations**
  To open backups of all organizations.

- **Exploring Retrieved Data**
  To open backups that you have retrieved from archives located in backup repositories extended with the Azure Blob Storage Archive access tier, Amazon S3 Glacier or Amazon S3 Glacier Deep Archive storage.

You can also restore Microsoft organization data from backups created for the Veeam Backup for Microsoft 365 server by Veeam Backup & Replication. For more information, see the **Application Items Restore** section of the Veeam Backup & Replication User Guide.
Exploring Backup Jobs

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

The following is an example of exploring the Backup Job 2 from the Repository 2. This job has three restore points created on January 20, January 27 and February 4. In such a scenario, Veeam Backup for Microsoft 365 loads only the latest restore point (created on February 4) into the Veeam Explorers scope.

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

1. Open the Organizations view.
2. In the inventory pane, select an organization.
3. In the preview pane, select a backup job that contains backups that you want to open.
4. On the Jobs tab, click Explore on the ribbon, or right-click a backup job and select one of the following options:
   - Explore latest <product> state of <date_and_time>. To explore the latest backup state.
   - Explore <product> point-in-time state. To select a point-in-time state. For more information, see Exploring Point In Time.
Exploring Single Organization

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

The following is an example of exploring a single organization with backups that are stored in three different backup repositories. In such a scenario, the following restore points will be merged and loaded into the Veeam Explorers scope:

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

**NOTE**

If you remove a backup job from the Veeam Backup for Microsoft 365 configuration, the backup data created by this job remains in a backup repository and is also loaded into the Veeam Explorers scope.
To open backups created by all backup jobs of a specific organization, do the following:

1. Open the Organizations view.

2. In the inventory pane, right-click an organization and select one of the following options:
   - **Explore latest <product> state of <date_and_time>**. To explore the latest backup state.
   - **Explore <product> point-in-time state**. To select a point-in-time state. For more information, see Exploring Point In Time.
Exploring All Organizations

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

The following is an example of exploring two organizations: \( A \) and \( B \). The organization \( A \) has three backup jobs and the organization \( B \) has two backup jobs.

When exploring the organization \( A \), the following restore points will be merged and loaded into the Veeam Explorers scope:

- For \( 	ext{Repository 1} \), only the restore point created on February 3.
- For \( 	ext{Repository 2} \), only the restore point created on February 4.
- For \( 	ext{Repository 3} \), only the restore point created on February 3.

When exploring the organization \( B \), the following restore points will be merged and loaded into the Veeam Explorers scope:

- For \( 	ext{Repository 2} \), only the restore point created on February 3.
- For \( 	ext{Repository 2} \), only the restore point created on January 24.

NOTE

If you remove a backup job from the Veeam Backup for Microsoft 365 configuration, the backup data created by this job remains in a backup repository and is also loaded into the Veeam Explorers scope.
To open backups of all organizations, do the following:

1. Open the **Organizations** view.

2. Right-click the root **Organizations** node and select one of the following options:
   - **Explore latest <product> state of <date_and_time>**. To explore the latest backup state.
   - **Explore <product> point-in-time state**. To select a point-in-time state. For more information, see **Exploring Point In Time**.
Exploring Point In Time

When exploring a point-in-time state, Veeam Backup for Microsoft 365 runs the **Explore Backup** wizard.

At the **Specify point in time** step of the wizard, select a backup state that you want to open:

1. Select one of the following options:
   - **Use the latest available state**. Select this option to load the latest state of items in the backup file.
   - **Use the following point in time**. Select this option to load a backup as of the selected date.

2. If you want to view historic data, select the following check boxes:
   - **Show items that have been deleted by user**. Select this option to show items that have been removed by the user before the specified date.
   - **Show all versions of items that have been modified by user**. Select this option to show all versions of items that have been modified by the user before the specified date.

![Specify point in time](Exploring_Point_In_Time.png)
Exploring Retrieved Data

NOTE

By default, the retrieved data is available for explore during 1 day. You can specify the availability period at the Specify Availability Period step of the Retrieve Backup Copy wizard.

If the retrieved data are restored by Veeam Explorers, the availability period is prolonged automatically for the remaining duration of the restore process. You can extend the availability period. For more information, see Editing Retrieval Job Settings and Extending Availability of Retrieved Data.

To open backups that you have retrieved from an archive, do the following:

1. Open the Organizations view.
2. In the inventory pane, select the Data retrieval node.
3. In the preview pane, do one of the following:
   - Select a retrieval job that contains backed-up data that you want to open and on the Retrievals tab, click Explore on the ribbon.
   - Right-click a retrieval job and select Explore retrieved <product> state.
Backup, Backup Copy, Retrieve and Restore Statistics

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

To review backup, backup copy, retrieve and restore sessions, open the History view and select one of the following nodes:

- **Jobs.** To see all backup and backup copy sessions.
  - **Backup.** To see both completed and running backup sessions.
  - **Copy.** To see both completed and running backup copy sessions.
- **Retrieve.** To see both completed and running retrieve sessions.
- **Restore.** To see Veeam Explorers restore sessions.

To stop a running session, select it in the preview pane and click Stop on the ribbon. For more information, see Stopping Backup Job and Stopping Backup Copy Job.

To review a specific session results of only particular type, use the Success, Warnings or Errors check boxes at the bottom.
Viewing Backup and Backup Copy Session Metrics

You can view a backup and backup copy session metrics in one of the following ways:

- Open the **Organizations** view and in the inventory pane, select an organization and then select a backup or backup copy job in the preview pane.

- Open the **History** view and in the inventory pane, select the **Jobs > Backup** or **Jobs > Copy** node and then select a backup or backup copy session in the preview pane.

### Metrics of a backup or backup copy session consist of the following sections:

- **The Status** section that shows the following fields:
  - **Session status**. The current state of the selected session.
  - **Bottleneck**. A bottleneck value.
    
    This value may be: **Detecting**, **Source**, **Target** and **N/A**.
    
    - **The Detecting** state is displayed when a backup or backup copy job is started and Veeam Backup for Microsoft 365 has not calculated the bottleneck value.
    
    - **The Source** state is displayed when a bottleneck occurs during download.
      
      For example, if you have a slow connection or problems occur on the internet provider side and your connection speed drops significantly, the bottleneck value will typically be shown as **Source**.
      
    - **The Target** state is displayed when a bottleneck occurs during writing data to disk.
      
      For example, if you are using a hard drive that is fragmented or an old type of the hard drive, the bottleneck value will typically be shown as **Target**.
      
    - **The N/A state is displayed when no bottleneck occurs.**
  
  - **Last Backup**. The date and time of the last backup or backup session.

- **The Data** section that shows the following fields:
  - **Processing rate**. Shows the processing rate.
  - **Read rate**. Shows the download speed.
  - **Write rate**. Shows the writing speed.
• The **Summary** section that shows the following fields:
  
  o **Duration.** The duration of the backup or backup copy session.
  
  o **Objects.** Shows how many objects have been backed up or copied during the session.
    
    An object is an OneDrive account, SharePoint site, Microsoft Teams team, mailbox and archive mailbox, including group mailboxes, public folders and discovery search mailboxes.
  
  o **Transferred.** Shows how many bytes have been downloaded.
Viewing Retrieve Session Metrics

You can view a retrieve session metrics in one of the following ways:

- Open the Organizations view and in the inventory pane, select the Data retrieval node and then select a retrieval job in the preview pane.
- Open the History view and in the inventory pane, select the Retrieve node and then select a retrieve session in the preview pane.

<table>
<thead>
<tr>
<th>Info</th>
<th>Status</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: Exchange data retrieval</td>
<td>Status: Success</td>
<td>Objects: 3 of 3</td>
</tr>
<tr>
<td>Operations: Retrieve</td>
<td>Start Time: 8/16/2021 2:15 AM</td>
<td>Processed: 1 blobs</td>
</tr>
<tr>
<td></td>
<td>End Time: 8/16/2021 2:19 AM</td>
<td></td>
</tr>
</tbody>
</table>

Metrics of a retrieve session consist of the following sections:

- The **Info** section that shows the following fields:
  - **Name.** The name of the retrieve session.
  - **Operation.** The name of the operation.
    
    Can be *Retrieve* or *Remove*.

- The **Status** section that shows the following fields:
  - **Status.** The status of the session.
    
    Can be *Running*, *Success*, *Warning*, or *Error*.
  - **Start Time.** The start time of the session.
  - **End Time.** The end time of the session.

- The **Summary** section that shows the following fields:
  - **Objects.** Shows how many objects have been selected for retrieval of their backed-up data.
    
    An object is an OneDrive account, SharePoint site, Microsoft Teams team, mailbox and archive mailbox, including group mailboxes, public folders and discovery search mailboxes.
  - **Processed.** Shows how many blob files have been downloaded.
Viewing Restore Session Metrics

To view a restore session metrics, do the following:

1. Open the History view.
2. In the inventory pane, select the Restore node.
3. In the preview pane, select a restore session.

<table>
<thead>
<tr>
<th>Info</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: Exchange restore Job: Full Backup - 9/16/2021 12:00:45 AM</td>
<td>Status: Success</td>
</tr>
<tr>
<td>Session type: Restore</td>
<td>Start Time: 9/16/2021 2:02 AM</td>
</tr>
<tr>
<td>Initiated by: SRV0101\Administrator</td>
<td>End Time: 9/16/2021 2:03 AM</td>
</tr>
</tbody>
</table>

Metrics of a restore session consist of the following sections:

- The **Info** section that shows the following fields:
  - **Name**. The name of the restore session.
  - **Session type**. The session type.
  - **Initiated by**. The user name under which the session has been executed or is still in progress.

- The **Status** section that shows the following fields:
  - **Status**. The status of the session.
    - Can be *Running, Success, Warning, or Error*.
  - **Start Time**. The start time of the session.
  - **End Time**. The end time of the session.
Reporting

Veeam Backup for Microsoft 365 allows you to create the following data protection reports:

- Mailbox Protection Reports
- Storage Consumption Reports
- License Overview Reports
- User Protection Reports
Creating Mailbox Protection Reports

The Mailbox Protection reports show statistical information on protected and unprotected mailboxes of your Microsoft 365 and on-premises Microsoft Exchange organizations.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Shows a description of the report.</td>
</tr>
<tr>
<td>Reporting Date</td>
<td>Shows the date when the report was created.</td>
</tr>
<tr>
<td>License Information</td>
<td>Shows the following:</td>
</tr>
<tr>
<td></td>
<td>• Product name</td>
</tr>
<tr>
<td></td>
<td>• Company name</td>
</tr>
<tr>
<td></td>
<td>• License type</td>
</tr>
<tr>
<td></td>
<td>• License expiration date</td>
</tr>
<tr>
<td></td>
<td>• Support identification number</td>
</tr>
<tr>
<td>Summary</td>
<td>Shows the total number of protected and unprotected mailboxes per each organization added to the scope:</td>
</tr>
<tr>
<td></td>
<td>• A mailbox is considered protected if it was backed up at least once within the last 31 days.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>The following types of mailboxes are included in the report:</td>
</tr>
<tr>
<td></td>
<td>• Group mailbox</td>
</tr>
<tr>
<td></td>
<td>• Public mailbox</td>
</tr>
<tr>
<td></td>
<td>• Shared mailbox</td>
</tr>
<tr>
<td></td>
<td>• Resource (Equipment and Room) mailbox</td>
</tr>
</tbody>
</table>

Renamed organizations will be shown with their original names. For more information about renaming organizations, see Renaming Organizations.

To generate a report, do the following:

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

**TIP**
You can also select the root Organizations node to generate a report for all organizations added to the scope.
3. On the **Home** tab, click **Reports > Mailbox Protection**.
   The **Generate Report** wizard runs.

4. Click **Browse** to specify a location to save the report.
   Use the **Save as type** drop-down list in the **Save As** dialog to select PDF or CSV format in which you want to save the report.

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

6. Click **Finish**.

![Generate Report dialog](image)
Creating Storage Consumption Reports

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Shows a description of the report.</td>
</tr>
<tr>
<td>Reporting Interval</td>
<td>Shows the time interval for which the report was generated.</td>
</tr>
<tr>
<td>License Information</td>
<td>Shows the following:</td>
</tr>
<tr>
<td></td>
<td>• Product name</td>
</tr>
<tr>
<td></td>
<td>• Company name</td>
</tr>
<tr>
<td></td>
<td>• License type</td>
</tr>
<tr>
<td></td>
<td>• License expiration date</td>
</tr>
<tr>
<td></td>
<td>• Support identification number</td>
</tr>
<tr>
<td>Summary</td>
<td>Shows occupied storage space of all backup repositories added to the scope.</td>
</tr>
<tr>
<td>Top 5 Repositories by Storage Usage</td>
<td>Shows top 5 repositories in which data in backups or backup copies occupies the most disk space.</td>
</tr>
<tr>
<td>Top 5 Repositories by Growth</td>
<td>Shows top 5 repositories in which the space is occupied most frequently.</td>
</tr>
<tr>
<td>Daily Change (GB)</td>
<td>Information is shown per standalone backup repositories and backup repositories that were extended with object storage. For extended backup repositories, Veeam Backup for Microsoft 365 shows the following statistical information:</td>
</tr>
<tr>
<td></td>
<td>• Used space that is occupied by cache.</td>
</tr>
<tr>
<td></td>
<td>• Used space that is occupied by data in backups or backup copies that stored in object storage.</td>
</tr>
<tr>
<td>Repository Growth (GB)</td>
<td></td>
</tr>
</tbody>
</table>

Consider the following:

- Repositories that have no statistical information are not included in the report. No information is available when you added a new backup repository. For more information on how to add a new backup repository, see Adding Backup Repositories.

  Since nothing has been placed to a backup repository after it was added, no statistical information is available, therefore, this repository is not included in the report.
Repositories whose **Daily Change** and **Total Size** values are less than 10 MB are not included in the report.

For example, a report is said to be built starting from 09/01/2021 to 09/30/2021 and the period from 09/01/2021 to 09/09/2021 is empty (both the **Daily Change** and **Total Size** values are less than 10 MB). In this scenario, such a report will only show statistical information starting from 09/10/2021.

To generate a report, do the following:

1. Open the **Organizations** view.
2. In the inventory pane, select an organization.
   
   **TIP**
   
   You can also select the root **Organizations** node to generate a report for backup and object storage repositories of all organizations added to the scope.

3. On the **Home** tab, click **Reports > Storage Consumption**.
   
   The **Generate Report** wizard runs.
4. Specify a time interval for reporting.
5. Click **Browse** to specify a location to save the report.
   
   Use the **Save as type** drop-down list in the **Save As** dialog to select PDF or CSV format in which you want to save the report.
6. Select the **Open report after publishing** check box to open the generated report using the default application.
7. Click **Finish**.
Creating License Overview Reports

The **License Overview** reports show statistical information on how many licenses are in use and by which organization.

Each report consists of the following fields and shows information per organization consuming the license.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Shows a description of the report.</td>
</tr>
<tr>
<td>Reporting Interval</td>
<td>Shows the time interval for which the report is generated.</td>
</tr>
<tr>
<td><strong>Note</strong>: By default, the report is generated for 30 days. If the reporting interval that you set is more than 1 day, the report includes all organizations that consumed the license within the specified period. Even if an organization license expired within the specified period, such organization is included in the report as well.</td>
<td></td>
</tr>
<tr>
<td>License Information</td>
<td>Shows the following:</td>
</tr>
<tr>
<td></td>
<td>• Product name</td>
</tr>
<tr>
<td></td>
<td>• Company name</td>
</tr>
<tr>
<td></td>
<td>• License type</td>
</tr>
<tr>
<td></td>
<td>• License expiration date</td>
</tr>
<tr>
<td></td>
<td>• Support identification number</td>
</tr>
<tr>
<td>Summary</td>
<td>Shows how many licenses are in use, including licenses for user accounts whose status is <strong>new user</strong>.</td>
</tr>
<tr>
<td>Top 5 Organizations by License Usage</td>
<td>Shows top 5 organizations that consume the license the most.</td>
</tr>
</tbody>
</table>

**NOTE**

When using a rental license, the **License Overview** report also shows a number of **new user** accounts per each organization. For more information, see **Rental License**.

To generate a report, do the following:

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

**TIP**

You can also select the root **Organizations** node to generate a report for all organizations added to the scope.
3. On the **Home** tab, click **Reports > License Overview**.

   The **Generate Report** wizard runs.

4. Specify a time interval for reporting.

5. Click **Browse** to specify a location to save the report.

   Use the **Save as type** drop-down list in the **Save As** dialog to select PDF or CSV format in which you want to save the report.

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

7. Click **Finish**.
Creating User Protection Reports

Starting from version 6a (build 6.1.0.222), Veeam Backup for Microsoft 365 allows you to create the User Protection reports. These reports show statistical information on protected and unprotected user accounts of your Microsoft 365 and on-premises Microsoft organizations.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Shows a description of the report.</td>
</tr>
<tr>
<td>Reporting Date</td>
<td>Shows the date when the report was created.</td>
</tr>
<tr>
<td>License Information</td>
<td>Shows the following:</td>
</tr>
<tr>
<td></td>
<td>- Product name</td>
</tr>
<tr>
<td></td>
<td>- Company name</td>
</tr>
<tr>
<td></td>
<td>- License type</td>
</tr>
<tr>
<td></td>
<td>- License expiration date</td>
</tr>
<tr>
<td></td>
<td>- Support identification number</td>
</tr>
<tr>
<td>Summary</td>
<td>Shows the total number of protected and unprotected users per each organization added to the scope:</td>
</tr>
<tr>
<td></td>
<td>- A user is considered protected if both a user is currently added to a backup job and restore points are available for a user data in Veeam Backup for Microsoft 365.</td>
</tr>
<tr>
<td></td>
<td>- A user is considered unprotected if a user is not added to a backup job and there are no restore points for a user data in Veeam Backup for Microsoft 365.</td>
</tr>
<tr>
<td></td>
<td>- A user is considered unprotected with restore points if a user is not added to a backup job, but restore points are available for a user data in Veeam Backup for Microsoft 365.</td>
</tr>
</tbody>
</table>

Only user accounts are included in the report; group accounts are not included.

If an organization was removed from Veeam Backup for Microsoft 365, the report shows information only about users whose data was backed up.

Renamed organizations will be shown with their original names. For more information about renaming organizations, see Renaming Organizations.

To generate a report, do the following:

1. Open the Organizations view.
2. In the inventory pane, select an organization for which you want to create a report.
3. On the **Home** tab, click **Reports > User Protection**.

   The **Generate Report** wizard runs.

4. Click **Browse** to specify a location to save the report.

   Use the **Save as type** drop-down list in the **Save As** dialog to select PDF or CSV format in which you want to save the report.

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

6. Click **Finish**.
Managing Log Files

Veeam Backup for Microsoft 365 allows you to collect log files generated by default and enable the extended logging mode. Log files help you and Veeam Customer Support specialists to troubleshoot product operation issues when working with Veeam Backup for Microsoft 365 and Veeam Explorers.

Logs for Veeam Backup for Microsoft 365 Components

Veeam Backup for Microsoft 365 creates a separate log file for each of its components and saves them in the %ProgramData%\Veeam\Backup365\Logs folder.

Logs for Veeam Backup for Microsoft 365 PowerShell

For PowerShell modules, Veeam Backup for Microsoft 365 saves log files in the %ProgramData%\Veeam\Backup365\Logs\PowerShell folder.

If you move a Microsoft organization data from one backup repository to another using the Move-VBOEntityData cmdlet, Veeam Backup for Microsoft 365 saves log files in the %ProgramData%\Veeam\Backup365\Logs\Move folder.

If you remove a Microsoft organization data from a backup repository using the Remove-VBOEntityData cmdlet, Veeam Backup for Microsoft 365 saves log files in the %ProgramData%\Veeam\Backup365\Logs\Remove folder.

Logs for Backup and Backup Copy Jobs

For each backup or backup copy job, Veeam Backup for Microsoft 365 saves log files in the %ProgramData%\Veeam\Backup365\Logs\<organization_name>\<job_name> folder.

This folder includes the following log files:

- A separate log file for each job session.
- A separate log file for each performed task.
- A summary report file in the HTML format with information about all job sessions and all objects that were processed during each job session.
- An archiver appliance log file if Veeam Backup for Microsoft 365 uses archiver appliance when performing a backup copy job.

Logs for Data Retrieve

Veeam Backup for Microsoft 365 creates a separate log file for each retrieval job. Depending on type of the retrieved data, Veeam Backup for Microsoft 365 saves log files in the following subfolders of the %ProgramData%\Veeam\Backup365\Logs\<organization_name> folder:

- Exchange data retrieval
- SharePoint data retrieval
- OneDrive data retrieval
- Teams data retrieval
Logs for Restore Portal

For each restore session that is performed on Restore Portal, Veeam Backup for Microsoft 365 saves logs to the Veeam.Archiver.Service_<timestamp> and Veeam.Archiver.REST_<timestamp> files located in the %ProgramData%\Veeam\Backup365\Logs folder.

Logs for Veeam Explorers

Log files for Veeam Explorers are saved separately in the %ProgramData%\Veeam\Backup\<Veeam_Explorer_Name>\Logs folder.
Collecting Log Files

To collect log files, do the following:

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

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

4. Specify a time period for log export:
   - Select the **Collect logs for the last N days** option to specify the number of days for which to export your log files.
   - Select the **Collect logs for the specified time period** option to set up a period for log files export.
Select the **Collect all logs** option to export all existing log files regardless of the time period.

5. Specify the path.

6. Click **Finish**.
Enabling Extended Logging Mode

Extended logging mode augments log records generated during the Veeam Backup for Microsoft 365 operation. In comparison to log records generated by default, extended log records contain additional information such as more detailed description of operations performed during the backup and restore processes, as well as more detailed description of items processed during backup and restore.

Veeam Customer Support specialists use log files generated in the extended logging mode to troubleshoot product operation issues and may ask you to enable this mode after you report a problem to Veeam Customer Support.

To enable extended logging mode, do the following:

1. In the main menu, click **Help and Support > Support information**.
2. Select the **Configure extended logging** option.

![Support Information](image-url)
3. Select components (local or remote) to which you want to apply the extended logging mode.

4. Click **Finish**.

After you enable extended logging mode, you need to go back to the main application window and perform actions for which you want to collect additional information. Then you can collect logs. For more information, see **Collecting Log Files**.
Backup as Service for Microsoft 365

You can configure *Backup as a Service for Microsoft 365* for service providers and tenants.
For Service Providers

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

1. Install Veeam Backup for Microsoft 365 on a server with Veeam Backup & Replication with the enabled *Cloud Connect* feature.
   
   For more information, see the *Deployment* section of this guide and the *Installing Veeam Backup & Replication* section of the Veeam Backup & Replication User Guide.

2. Install Veeam Backup for Microsoft 365 and Veeam Backup & Replication licenses.
   
   For more information, see the *Licensing and License Types* of this guide and the *Licensing for Service Providers* section of the Veeam Cloud Connect Guide.

3. Configure a TLS certificate. For more information, see the *Managing TLS Certificates* section of the Veeam Cloud Connect Guide.
   
   Without a certificate, you will not be able to add a *Cloud Gateway* component.

4. Configure a cloud gateway. For more information, see the *Adding Cloud Gateways* section of the Veeam Cloud Connect Guide.

5. Add new tenants. For more information, see the *Registering Tenant Accounts* section of the Veeam Cloud Connect Guide.

6. Configure your Veeam Backup for Microsoft 365 environment. For more information, see *Configuring Veeam Backup for Microsoft 365*.

A service provider can use Veeam Backup for Microsoft 365 REST API to build a web portal that will allow tenants to browse and restore their backups without using Veeam Explorers. For more information, see *REST API Reference*.

**NOTE**

Consider the following:

- Make sure to install Veeam Explorer for Microsoft Exchange, Veeam Explorer for Microsoft SharePoint, Veeam Explorer for Microsoft OneDrive for Business and Veeam Explorer for Microsoft Teams that come as part of the Veeam Backup for Microsoft 365 6.0 installation package. For more information, see *Installing Veeam Backup for Microsoft 365 and Veeam Explorers*.

- Make sure to install Veeam Backup for Microsoft 365 on a server with Veeam Backup & Replication 10 or later.
Configuring Veeam Backup for Microsoft 365

To configure Veeam Backup for Microsoft 365 on a service provider side, the following actions must be performed:

1. Configure the Veeam Backup for Microsoft 365 environment. For more information on how to configure Veeam Backup for Microsoft 365 settings, see General Settings.

2. Enable tenant authentication to the Veeam Backup for Microsoft 365 server to perform self-restore procedures. For more information, see Authentication Settings.

3. Configure backup proxy servers. For more information, see Backup Proxy Servers.

4. Configure backup repositories. For more information, see Backup Repositories.

5. Add tenant organizations to the Veeam Backup for Microsoft 365 scope. For more information, see Organization Management.

6. Configure backup and backup copy for data in tenant organizations. For more information, see Data Backup and Backup Copy.

7. Configure data restore using Restore Portal for end users and restore operators from tenant organizations. For more information, see Configuring Restore Portal for Multiple Tenants.

**NOTE**

As a service provider, you must obtain Microsoft organization credentials of your tenants. The same credentials will be used by tenants to connect to the Veeam Backup for Microsoft 365 server on a service provider side for self-restore procedures using Veeam Explorers.
For Tenants

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

1. Add a service provider in Veeam Backup & Replication. For more information, see the [Connecting to Service Providers](#) section of the Veeam Cloud Connect Guide.

2. Add backups to the Veeam Explorer scope. For more information, see [Exploring Backups in Veeam Explorers](#).

**NOTE**

Mind the following:

- Make sure to install Veeam Explorer for Microsoft Exchange, Veeam Explorer for Microsoft SharePoint, Veeam Explorer for Microsoft OneDrive for Business and Veeam Explorer for Microsoft Teams that come as part of the Veeam Backup for Microsoft 365 6.0 installation package. For more information, see [Installing Veeam Explorers for Tenants](#).
- By default, tenants cannot restore anything without the service provider assistance. To be able to perform self-restore procedures, a service provider must configure authentication settings for tenants. For more information, see [Authentication Settings](#).
- Tenants must provide service providers with their Microsoft organization credentials. Tenants can use the same credentials when adding a Veeam Backup for Microsoft 365 service provider server to the Veeam Explorers scope. For more information, see [Exploring Backups in Veeam Explorers](#).
Exploring Backups in Veeam Explorers

To explore backups located on the service provider side, add such backups in Veeam Explorers. For more information, see the following sections of the Veeam Explorers User Guide:

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

NOTE

Consider the following:

- Make sure to have access to the service provider server to be able to explore your backups. For more information on how to grant access, see Authentication Settings.
- [For connection to a service provider using the modern app-only authentication method] The account that you plan to use to log in to Microsoft 365 must be assigned the Global Administrator role.
Data Restore Using Restore Portal

Restore Portal is a web-based solution that allows users to perform self-service restore of backed-up data. They can explore and restore Microsoft Exchange, Microsoft SharePoint and Microsoft OneDrive for Business data from backups created by Veeam Backup for Microsoft 365.

Restore Portal offers two scenarios for data restore: self-service restore and operator restore. For more information about available usage scenarios, see Restore Portal Usage Scenarios.

Veeam Backup for Microsoft 365 users who take part in the Restore Portal usage scenarios can be divided into three groups:

- **Veeam Backup for Microsoft 365 administrators** — IT specialists who use Veeam Backup for Microsoft 365 to protect data in Microsoft organizations. They maintain the Veeam Backup for Microsoft 365 backup infrastructure, configure general application settings including the REST API, Authentication Settings and Restore Portal settings, and assign permissions to users who act as restore operators.

- **Restore operators** — a service provider representatives or other users who restore data from backups created by Veeam Backup for Microsoft 365 for other users.

- **End users** — users of a Microsoft 365 organization who perform self-service restore of their own backed-up data.

If the Veeam Backup for Microsoft 365 administrator in a Microsoft 365 organization has configured the REST API and Restore Portal settings in Veeam Backup for Microsoft 365, restore operators and end users access Restore Portal from any computer and perform all operations in a web browser window. For more information, see Launching Restore Portal and Performing Restore.
Restore Portal Usage Scenarios

Restore Portal offers users two scenarios for data restore:

- **Self-service restore.** In this scenario, users explore and restore their own data from backups created by Veeam Backup for Microsoft 365. After a user logs in to Restore Portal, only data that Veeam Backup for Microsoft 365 has backed up for this user account is available to explore and restore.

- **Operator restore.** In this scenario, the Veeam Backup for Microsoft 365 administrator specifies a user (or a group in which this user is included) as a restore operator.

  Restore operators have permissions to explore and restore data from backups for specific organization object types: users, groups (group members only), sites, or the entire Microsoft 365 organization. Permissions are assigned to restore operators when the Veeam Backup for Microsoft 365 administrator adds a *restore operator role*. For more information on how to add a restore operator role, see [Adding Restore Operator Role](#).

  After a restore operator logs in to Restore Portal, the product shows backed-up data for objects that the restore operator is allowed to manage — that is, to explore and restore data from backups created by Veeam Backup for Microsoft 365 for these objects.

  Restore operators can work separately with data of the managed objects. Restore Portal allows them to switch between the managed objects. For more information on how to select an object whose backed-up data a restore operator will explore and restore, see [Changing Restore Operator Scope](#).

Restore operations that end users and restore operators can perform with the backed-up data are the same in both usage scenarios.
How Restore Portal Works

The following components are involved in the Restore Portal operation:

- Veeam Backup for Microsoft 365 server
- *Veeam Backup for Microsoft 365 RESTful API Service*
- Microsoft 365 organization
- Restore Portal
- *Veeam Backup Proxy for Microsoft 365 Service*

Veeam Backup for Microsoft 365 uses REST API and Azure AD application when authenticating users to Restore Portal with their Microsoft 365 user account credentials. REST API authorization is based on the OAuth 2.0 Authorization Framework. For more information on how to create and configure Azure AD application to access Restore Portal, see Creating or Configuring Azure AD Application.

Restore Portal uses REST API to communicate with the Veeam Backup for Microsoft 365 server. For more information on how to configure REST API, see REST API Settings.

Data exchange between the Veeam Backup for Microsoft 365 server, Microsoft 365 organization, Azure AD application, the Veeam Backup for Microsoft 365 RESTful API Service and Restore Portal is performed using SSL certificates. For more information, see Installing SSL Certificates.
Considerations and Limitations

This section lists considerations and known limitations of Restore Portal.

- Restore Portal is supported only for organizations added to Veeam Backup for Microsoft 365 using the modern app-only authentication method. Azure AD application that you have used to add your Microsoft 365 organization must have permissions for data restore using an application certificate.

- Backups created for on-premises Microsoft organizations cannot be restored using Restore Portal. For hybrid organizations, Restore Portal allows you to restore only data from backups created for Microsoft 365 organizations.

- Microsoft Teams data is not supported for explore and restore using Restore Portal. If a restore operator is allowed to manage the entire Microsoft 365 organization, only Microsoft Exchange, Microsoft SharePoint and Microsoft OneDrive for Business data will be available for explore and restore.

- Group mailboxes data is not supported for explore and restore using Restore Portal.

- Restore Portal allows you to restore data from the latest restore point that available in a backup repository.

- Items of different types that you added to the restore list (for example, mailbox items, OneDrive and SharePoint files) will not be restored simultaneously. You must configure and run different restore operations for Exchange, SharePoint and OneDrive items.

- Backups that were retrieved from backup copies cannot be restored using Restore Portal.

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

Restore Portal is deployed automatically along with Veeam Backup for Microsoft 365 REST API component installation.

The Veeam Backup for Microsoft 365 administrator can configure Restore Portal for the following backup infrastructures:

- Single Microsoft 365 Organization
- Multiple Tenants on Service Provider Side

Configuring Restore Portal for Single Microsoft 365 Organization

If the Veeam Backup for Microsoft 365 administrator wants to allow end users and restore operators in a Microsoft 365 organization to explore and restore data from backups using Restore Portal, the following actions must be performed before users start using the web application:

1. Check that Veeam Backup for Microsoft 365 REST API component is installed either on the Veeam Backup for Microsoft 365 server or on a separate computer.
   
   Installing REST API separately from a Veeam Backup for Microsoft 365 server allows you to decrease the load on infrastructure when exploring and restoring data from backups using the Restore Portal. For more information, see Installing Veeam Backup for Microsoft 365 and Veeam Explorers to deploy the solution to the Veeam Backup for Microsoft 365 server and Installing REST API on Separate Computer to deploy Veeam Backup for Microsoft 365 REST API component separately.

2. Enable the Veeam Backup for Microsoft 365 RESTful API Service.
   
   This service processes REST API commands and allows Restore Portal to communicate with Veeam Backup for Microsoft 365. For more information, see REST API Settings if you have deployed the solution on the Veeam Backup for Microsoft 365 server and Configuring REST API and Restore Portal on Separate Computer if you have installed REST API separately.

3. Enable restore operator authentication to the Veeam Backup for Microsoft 365 server. For more information, see Authentication Settings.

4. Enable Restore Portal and configure access to it. For more information, see Restore Portal Settings if you have deployed the solution on the Veeam Backup for Microsoft 365 server and Configuring REST API and Restore Portal on Separate Computer if you have installed REST API separately.

5. Add restore operator roles to assign permissions to users who act as restore operators. For more information, see Adding Restore Operator Role.

6. Provide end users and restore operators with the Restore Portal web address.

Configuring Restore Portal for Multiple Tenants

**NOTE**

Follow these steps as a part of Backup as a Service for Microsoft 365 usage scenario. For more information, see Backup as Service for Microsoft 365.
To configure access for end users and restore operators from tenant organizations to Restore Portal, the following actions must be performed on a service provider side before users start using the web application:

1. Check that Veeam Backup for Microsoft 365 REST API component is installed either on the Veeam Backup for Microsoft 365 server or on a separate computer.

   Installing REST API separately from a Veeam Backup for Microsoft 365 server allows you to decrease the load on infrastructure when exploring and restoring data from backups using the Restore Portal. For more information, see Installing Veeam Backup for Microsoft 365 and Veeam Explorers to deploy the solution to the Veeam Backup for Microsoft 365 server and Installing REST API on Separate Computer to deploy Veeam Backup for Microsoft 365 REST API component separately.

2. Enable the **Veeam Backup for Microsoft 365 RESTful API Service**.

   This service processes REST API commands and allows Restore Portal to communicate with Veeam Backup for Microsoft 365. For more information, see REST API Settings if you have deployed the solution on the Veeam Backup for Microsoft 365 server and Configuring REST API and Restore Portal on Separate Computer if you have installed REST API separately.

3. Enable tenant and restore operator authentication to the Veeam Backup for Microsoft 365 server. For more information, see Authentication Settings.

4. Enable Restore Portal and configure access to it. For more information, see Restore Portal Settings if you have deployed the solution on the Veeam Backup for Microsoft 365 server and Configuring REST API and Restore Portal on Separate Computer if you have installed REST API separately.

   **IMPORTANT**
   Azure AD application that you want to use to access Restore Portal must be created for a Microsoft 365 organization on a service provider side.

5. Run the **Install-Module** cmdlet to install the Azure Active Directory PowerShell for Graph module. For more information, see this Microsoft article.

6. Share the configured Azure AD application with all tenant organizations. To do this, perform the following steps:
   a. Run the **New-AzureADServicePrincipal** cmdlet. Specify an application ID of Azure AD application configured for authentication to Restore Portal as the **AppId** parameter value.

      ```powershell
      $Credential = Get-Credential
      Connect-AzureAD -Credential $Credential
      New-AzureADServicePrincipal -AppId "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXXX X"
      ```
   b. Sign in to the tenant organization Azure portal.
   c. Go to **Azure Active Directory > Enterprise applications**.
   d. Search for Azure AD application configured for authentication to Restore Portal by the application name or object ID, or use filters with the **Application type** search criteria removed.
   e. Go to the application permissions and grant admin consent to this application on behalf of all users in the tenant organization. For more information, see this Microsoft article, Permissions for Authentication to Restore Portal and contact Veeam Customer Support.

7. Add restore operator roles to assign permissions to users who act as restore operators. For more information, see Adding Restore Operator Role.

8. Provide end users and restore operators with the Restore Portal web address.
Adding Restore Operator Role

In the operator restore scenario, Veeam Backup for Microsoft 365 administrators must add restore operator roles.

When adding a restore operator role, they select organization users or groups and assign permissions to them. Such users or groups become restore operators. Restore operators are allowed to explore and restore data from backups created by Veeam Backup for Microsoft 365 for specific organization object types: users, groups (group members only), sites, or the entire Microsoft 365 organization.

To add a restore operator role, check prerequisites and do the following:

1. Launch the New Restore Operator Role wizard.
2. Specify a role name.
3. Select Microsoft organization.
4. Select restore operators.
5. Select objects to manage.
6. Select objects to exclude.

Before You Begin

Before you add a restore operator role, check the following prerequisites:

- You can add restore operator roles for users and groups of Microsoft 365 organizations and hybrid organizations.
- The organization for which you want to add a restore operator role must be added to Veeam Backup for Microsoft 365 using the modern app-only authentication method.
Step 1. Launch New Restore Operator Role Wizard

To launch the New Restore Operator Role wizard, do the following:

1. In the main menu, click Restore Operator Roles.
2. In the Restore Operator Roles window, click Add.
Step 2. Specify Role Name

At this step of the wizard, enter a name for the restore operator role and provide optional description:

1. In the Name field, enter a name for the restore operator role.
2. In the Description field, enter optional description.
Step 3. Select Organization

At this step of the wizard, from the Organization drop-down list, select an organization whose users or groups will act as restore operators.

Mind the following:

- You can add restore operator roles only for Microsoft 365 organizations and hybrid organizations.
- The organization for which you want to add a restore operator role must be added to Veeam Backup for Microsoft 365 using the modern app-only authentication method.

![New Restore Operator Role](image)

Specify organization

**Organization:**

![sbc.onmicrosoft.com]

(restore operator roles are only supported for Microsoft 365 organizations that are using modern app-only authentication.)
Step 4. Select Restore Operators

At this step of the wizard, select users or groups that you want to act as restore operators.

To select restore operators, do the following:

1. Click **Add** and select either **Users** or **Groups**.

2. In the **Add Objects** window, select check boxes next to the users or groups that you want to act as restore operators.
MIND THE FOLLOWING:

- To switch between objects of different types, you can click the buttons in the upper-right corner.
- To refresh the objects list, you can click **Refresh**.
- To quickly find necessary objects, you can use the search field at the bottom.

3. Click **Add**.

The selected objects appear in the list of restore operators.
Step 5. Select Objects to Manage

At this step of the wizard, select objects to manage. Restore operators will be able to explore and restore backed-up data of these objects using Restore Portal.

You can select either the entire organization or specific users, groups, and sites.

To select objects to manage, do the following:

1. Select one of the following options:
   - **Manage entire organization** to allow restore operators to explore and restore data from backups created by Veeam Backup for Microsoft 365 for all objects (except teams) within the selected Microsoft 365 organization.
     - Mind that if a restore operator is allowed to explore and restore data from backups created by Veeam Backup for Microsoft 365 for the entire Microsoft 365 organization, changing a restore operator scope may take a considerable time.
   - **Manage the following objects** to allow restore operators to explore and restore data from backups created by Veeam Backup for Microsoft 365 for specific users, groups, or sites.

2. If you selected the **Manage the following objects** option, click Add and select one of the following options: **Users**, **Groups**, or **Sites**.

3. In the **Add Objects** window, select check boxes next to the users, groups, or sites whose backed-up data the restore operators will be able to explore and restore using Restore Portal.
TIP
Mind the following:

- To switch between objects of different types, you can click the buttons in the upper-right corner.
- To refresh the objects list, you can click Refresh.
- To quickly find necessary objects, you can use the search field at the bottom.

4. Click Add.

The selected objects appear in the list of objects to manage.
Step 6. Select Objects to Exclude

At this step of the wizard, select objects to exclude. Restore operators will be prohibited to explore and restore backed-up data of these objects using Restore Portal.

To exclude objects, do the following:

1. Click **Add** and select one of the following options: *Users, Groups, or Sites*.

2. In the **Add Objects** window, select check boxes next to the users, groups, or sites whose backed-up data the restore operators will be prohibited to explore and restore using Restore Portal.

**TIP**

Mind the following:

- To switch between objects of different types, you can click the buttons in the upper-right corner.
- To refresh the objects list, you can click **Refresh**.
- To quickly find necessary objects, you can use the search field at the bottom.
3. Click **Add**.

The selected objects appear in the list of objects to exclude.

<table>
<thead>
<tr>
<th>Object</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>bscc_group</td>
<td>Security Group</td>
</tr>
<tr>
<td>SharedMBK_1</td>
<td>User</td>
</tr>
<tr>
<td>SharedMBK_10</td>
<td>User</td>
</tr>
<tr>
<td>SharedMBK_2</td>
<td>User</td>
</tr>
<tr>
<td>SharedMBK_3</td>
<td>User</td>
</tr>
<tr>
<td>SharedMBK_4</td>
<td>User</td>
</tr>
<tr>
<td>SharedMBK_5</td>
<td>User</td>
</tr>
</tbody>
</table>
Editing Restore Operator Role Settings

Veeam Backup for Microsoft 365 allows you to edit restore operator role settings.

To edit settings of a restore operator role, do the following:

1. In the main menu, click Restore Operator Roles.
2. In the Restore Operator Roles window, select a restore operator role and click Edit.
3. Modify the required settings.
   You can change the following parameters:
   - The name and description of a restore operator role.
   - The list of restore operators.
   - The lists of objects whose backed-up data the restore operators will and will not be able to explore and restore using Restore Portal.
Removing Restore Operator Role

You can remove a restore operator role from the Veeam Backup for Microsoft 365 configuration if you no longer need it.

To remove a restore operator role, do the following:

1. In the main menu, click **Restore Operator Roles**.
2. In the **Restore Operator Roles** window, select a restore operator role and click **Remove**.

![Restore Operator Roles window](image-url)
Launching Restore Portal

To launch Restore Portal, do the following:

1. Open a web browser on any computer and navigate to the Restore Portal web address.

   Consider the following:
   
   o The web address must be specified in one of the following formats:
     
     ▪ https://<IPv4 address>:<port number>, where <IPv4 address> is a public IPv4 address of a computer with Veeam Backup for Microsoft 365 REST API component installed. For example, https://135.169.170.192:4443.
     
     ▪ https://<DNS hostname>:<port number>, where <DNS hostname> is DNS hostname of a computer with Veeam Backup for Microsoft 365 REST API component installed. For example, https://portal.abc.com:4443.
   
   o The Restore Portal web address must be provided by the Veeam Backup for Microsoft 365 administrator.

   NOTE
   
   You can access Restore Portal using the only URI that was specified by the Veeam Backup for Microsoft 365 administrator when registering a new Azure AD application for authentication to Restore Portal. To add another URI or edit the application, the Veeam Backup for Microsoft 365 administrator must configure the application settings in the Azure Active Directory. For more information on how to configure the Restore Portal web address, see Creating or Configuring Azure AD Application.

   o You do not need any Veeam Backup for Microsoft 365 components or Veeam Explorers installed on a computer that you use to access Restore Portal.
   
   o Internet Explorer is not supported. To access Restore Portal, use Microsoft Edge (version 79 or later), Mozilla Firefox (version 21 or later) or Google Chrome (version 24 or later).

2. On the welcome page, enter a user account that you use to connect to the Microsoft 365 organization.

   You must provide a user account in one of the following formats: user@domain.com or user@domain.onmicrosoft.com.

3. Click Log In.

   Restore Portal will redirect you to the Microsoft authentication portal where you will be prompted to enter your Microsoft 365 user account password.
NOTE
If multi-factor authentication (MFA) is enabled in the Microsoft 365 organization, the Microsoft authentication portal also will prompt the user to verify the user identity using an additional verification method.

Logging Out

To log out of Restore Portal, in the upper-right corner of the Restore Portal window, click the user name and click Log Out.

After you log out, all sessions that were opened by Veeam Backup for Microsoft 365 to explore backed-up data are stopped. Restore sessions with restore operations that are running on Restore Portal will continue in the background till data restore completes.
User Interface

The web-based user interface of Restore Portal is designed to let you quickly explore backed-up Microsoft Exchange, Microsoft SharePoint, and Microsoft OneDrive for Business data in one window. Also, it allows you to perform restore operations without using Veeam Explorers and view details about restore sessions progress and results and the restore sessions history.

The main window consists of the Explore, Restore Sessions, and Restore List tabs.

Explore Tab

This tab contains two panes:

- The navigation pane allows you to browse through the hierarchy of folders with backed-up data. Nodes with Microsoft Exchange, Microsoft OneDrive for Business, and Microsoft SharePoint data are displayed in the navigation pane separately. Availability of nodes differs depending on backups created by Veeam Backup for Microsoft 365 for an object whose backed-up data is explored at the moment. For example, for a user object the following data can be displayed:
  - Exchange Online mailbox
  - Archive mailbox
  - OneDrive for Business
  - Personal Site (available only for restore operators)

For restore operators, Restore Portal displays data for user objects and SharePoint sites that restore operators are allowed to explore.

- The preview pane allows you to view details about items that are contained in a folder you have selected in the navigation pane. You can search items and select items that you want to restore or add to the restore list.
NOTE

Consider the following:

- Restore Portal displays up to 2000 items, so search for specific items.
- You can narrow your search results by specifying various search criteria using the `criteria:value` format. For more information about search parameters, see this section of REST API Reference.
- You can also use logical upper-cased operators such as `AND`, `OR` and `NOT` along with wildcard characters such as `*` and `?`.
- To search items by a specific date/time, specify the time in the UTC format. You can hover over the date in the `Received` column to view the UTC value.
Restore Sessions Tab

On this tab, you view details about restore session progress and results.

You can do the following:

- Stop a restore session.
- Search and filter restore sessions by type, status and time period.
- View the list of events that occurred during a restore session, search and filter events by their status.
Restore List Tab

On this tab, you view and edit the content of the restore list. This tab appears only if a restore list is not empty.

You can do the following:

- Select items that you want to restore.
- Remove items from the restore list.
- Search and filter items by their restore status.

Notification Pane

Notification pane is hidden in the upper-right corner of the Restore Portal window under the notification icon shaped like a bell.

To expand the notification pane, click the notification icon.

For more information, see Managing Notifications.
Managing Notifications

Restore Portal notifies you about restore sessions results. Notifications appear in the notification pane.

Each notification includes a restore session name, a status icon, and a status link. If you click the restore session status link, Restore Portal opens the Restore Sessions tab and navigates you directly to the restore session record.

If you want the notification pane to expand automatically when a new notification appears, do the following:

1. Click the notification icon to expand the notification pane.
2. Enable the Auto-display new messages option.
Changing Restore Operator Scope

After logging in to Restore Portal, restore operators can view the list of objects available to them to manage — that is, to explore and restore data from backups created by Veeam Backup for Microsoft 365 for these objects. For more information on how assign permissions to a restore operator, see Adding Restore Operator Role.

Restore operators can manage data of organization objects separately. Thus, they must switch between the managed objects: users, groups (group members only), sites, or the entire Microsoft 365 organization. In terms of Veeam Backup for Microsoft 365, this operation is called Changing restore operator scope.

NOTE
If a restore operator is allowed to explore and restore data from backups created by Veeam Backup for Microsoft 365 for all objects (except teams) within a Microsoft 365 organization, loading of available objects may take a considerable time. To avoid this, the Veeam Backup for Microsoft 365 administrator can edit the restore operator role settings and select not the entire organization, but specific users, groups, or sites as objects to manage. For more information, see Editing Restore Operator Role Settings and Select Objects to Manage.

To select an object whose backed-up data a restore operator will explore and restore, do the following:

1. In the upper-right corner of the Restore Portal window, click the user name and select Change Scope.
2. In the Change scope window, select an object that you want to manage. You can search objects and filter them by their organization object type.
3. Click Change scope.

The name of the selected object will appear in the upper-right corner of the Restore Portal window under the restore operator user name. The Explore tab will be displayed, on which you can browse through the hierarchy of folders with backed-up data of the selected object.
Performing Restore

After logging in to Restore Portal, you can explore and restore data from backups created by Veeam Backup for Microsoft 365. If you act as an end user, you perform self-service restore of your own data. If you have a restore operator permissions, you explore and restore backed-up data for those objects that you are allowed to manage. For more information about Restore Portal usage scenarios, see Restore Portal Usage Scenarios. For more information on how to assign permissions to a restore operator, see Adding Restore Operator Role.

To select items that you want to restore, do the following:

1. Open the Explore tab.
2. In the navigation pane, browse through the hierarchy of folders with backed-up data.
3. Select a folder that contains data you want to restore.
4. In the preview pane, select check boxes next to the necessary items.
   For documents and files, you can select which version of an item you want to restore. To do this, in the Version column, click the most recent version number, and in the displayed window, select the earlier version to restore.

**NOTE**

Consider the following:

- Restore Portal displays up to 2000 items, so search for specific items.
- You can narrow your search results by specifying various search criteria using the criteria:value format. For more information about search parameters, see this section of REST API Reference.
- You can also use logical upper-cased operators such as AND, OR and NOT along with wildcard characters such as * and ?.
- To search items by a specific date/time, specify the time in the UTC format. You can hover over the date in the Received column to view the UTC value.

5. Click Restore.
6. Configure restore operation options. Depending on the type of items that you selected to restore, Restore Portal runs one of the following wizards:
   - Exchange Restore
   - SharePoint Restore
   - OneDrive Restore
Using Restore List

If you want to select items located in different folders in the hierarchy of folders with backed-up data displayed in the navigation pane, you can add them to the restore list. For example, you can add to the restore list one by one items of different types: mailbox items, OneDrive and SharePoint files, and proceed to their restore.

To add items to the restore list, do the following:

1. Open the Explore tab.
2. In the navigation pane, browse through the hierarchy of folders with backed-up data.
3. Select a folder that contains data you want to restore.
4. In the preview pane, select check boxes next to the necessary items.
   
   For documents and files, you can select which version of an item you want to restore. To do this, in the Version column, click the most recent version number, and in the displayed window, select the earlier version to restore.

   
   **NOTE**

   Consider the following:
   
   • Restore Portal displays up to 2000 items, so search for specific items.
   • You can narrow your search results by specifying various search criteria using the criteria:value format. For more information about search parameters, see this section of REST API Reference.
   • You can also use logical upper-cased operators such as AND, OR and NOT along with wildcard characters such as * and ?.
   • To search items by a specific date/time, specify the time in the UTC format. You can hover over the date in the Received column to view the UTC value.

5. Click Add to Restore List.
6. Repeat steps 2–5 to add more items to the restore list.
7. On the Restore List tab, review the list of items that you added to the restore list.
8. To restore items, select check boxes next to the necessary items and click Restore and then select one of the following options:
   
   • **Restore Exchange Items.** This option runs the Exchange Restore wizard.
   • **Restore OneDrive Items.** This option runs the OneDrive Restore wizard.
   • **Restore SharePoint Items.** This option runs the SharePoint Restore wizard.
   • **Restore SharePoint Documents.** This option runs the SharePoint Restore wizard.

   **TIP**

   To remove items from the restore list, select check boxes next to the necessary items and click Remove from Restore List.
9. Follow the steps of the wizard that you ran and configure restore operation options. Mind that you must run wizards manually one after another.
Exchange Restore

The Exchange Restore wizard allows you to configure options that Veeam Backup for Microsoft 365 will apply when restoring the selected Microsoft Exchange items.

To configure Exchange restore, do the following:

1. At the **Items** step, specify items that you want to restore. If you no longer want to restore an item, select it and click **Remove**.

2. At the **Restore mode** step, select where you want to restore the selected items:
   - **Restore to the original location**. Select this option if you want to restore the selected items to their original location. Then proceed to step 5.
   - **Restore to a new location**. Select this option if you want to restore the selected items to another location and specify the folder name in the **Restore to the following folder** field. If the specified folder does not exist, it will be created automatically.

3. Click **Advanced options** to open the **Restore options** dialog.
4. In the **Restore options** dialog, select check boxes next to the additional options that you want to apply during the restore operation and then click **Apply**:

   - **Restore changed items.** Select this check box if you want to restore items that have been changed.
   - **Restore missing items.** Select this check box if you want to restore items that are missing in the target folder.
   - **Mark restored items as unread.** Select this check box if you want to mark each restored item as unread.

5. **[Optional]** At the **Reason** step, specify a restore reason. This information will be available in the **Reason** column on the **Restore Sessions** tab and you will be able to reference it later.

6. At the **Summary** step, review details of the restore operation and click **Finish**.

   Restore Portal runs the restore operation immediately and opens the **Restore Sessions** tab, where you view details about restore session progress and results.
SharePoint Restore

The SharePoint Restore wizard allows you to configure options that Veeam Backup for Microsoft 365 will apply when restoring the selected Microsoft SharePoint items.

To configure SharePoint restore, do the following:

1. At the **Items** step, specify items that you want to restore. If you no longer want to restore an item, select it and click **Remove**.

2. At the **Restore mode** step, select where you want to restore the selected items:
   - **Restore to the original location**. Select this option if you want to restore the selected items to their original location. Then proceed to step 5.
   - **Restore to a new location**. Select this option if you want to restore the selected items to another location and specify the list name in the **Restore to the following list** field.

   Mind that if you restore document libraries, lists or documents and the specified list does not exist, it will be created automatically. If you restore list items, make sure to specify a list that exists in the original SharePoint site.
3. Click **Advanced options** to open the **Restore options** dialog.

4. In the **Restore options** dialog, select check boxes next to the additional options that you want to apply during the restore operation and then click **Apply**:
   - **Changed items**: Select this check box if you want to restore data that has been modified in the production environment.
   - **Missing items**: Select this check box if you want to restore missing items.
   - **Restore permissions**: Select this check box if you want to restore permissions.
   - **Send a notification by email to the users with permissions to the file**: Select this check box if you want to notify users about items restore.
   - **Restore only the latest version**: Select this check box if you want to restore only the latest version of items.
   - **Overwrite**: Select this option to overwrite data in the production environment.
   - **Merge**: Select this option to merge an existing and a backup version of items.

5. [Optional] At the **Reason** step, specify a restore reason. This information will be available in the **Reason** column on the **Restore Sessions** tab and you will be able to reference it later.

6. At the **Summary** step, review details of the restore operation and click **Finish**.

Restore Portal runs the restore operation immediately and opens the **Restore Sessions** tab, where you view details about restore session progress and results.
OneDrive Restore

The **OneDrive Restore** wizard allows you to configure options that Veeam Backup for Microsoft 365 will apply when restoring the selected Microsoft OneDrive for Business items.

To configure OneDrive restore, do the following:

1. **At the Items step**, specify items that you want to restore. If you no longer want to restore an item, select it and click **Remove**.

2. **At the Restore mode step**, choose whether you want to overwrite the file or document in the original location or keep the restored one along with the original.

3. **[Optional] At the Reason step**, specify a restore reason. This information will be available in the **Reason** column on the **Restore Sessions** tab and you will be able to reference it later.

4. **At the Summary step**, review details of the restore operation and click **Finish**.

*Restore Portal* runs the restore operation immediately and opens the **Restore Sessions** tab, where you view details about restore session progress and results.
Data Restore Using Veeam Explorers

Veeam Explorers extend the functionality of Veeam Backup for Microsoft 365 and allow you to explore and restore data from backups.

For more information on how to use Veeam Explorers, see the Veeam Explorers User Guide for Veeam Backup for Microsoft 365.