



#1 Microsoft 365 Backup Guide by Veeam

Technical considerations for
Veeam Backup for Microsoft 365

Michele Domanico,
Edward Watson



Chapters

Understanding the Microsoft 365 backup market	3	How to back up and restore with Veeam	13
Planning your Microsoft 365 backup	4	Creating a backup job	14
Installation package	5	Selecting backup scope	15
Infrastructure components	6	Scheduling options	16
Simple versus advanced deployments	7	Veeam Explorers	17
Infrastructure planning	8	Exploring Microsoft 365 data	18
Deployment options	9	How to restore in 1-2-3	19
Supported storage	10	What should matter to you?	22
Retention policies	11	Key difference makers	23
Backup architecture	12	What are customers saying?	24
		Conclusion	25

Understanding the Microsoft 365 backup market

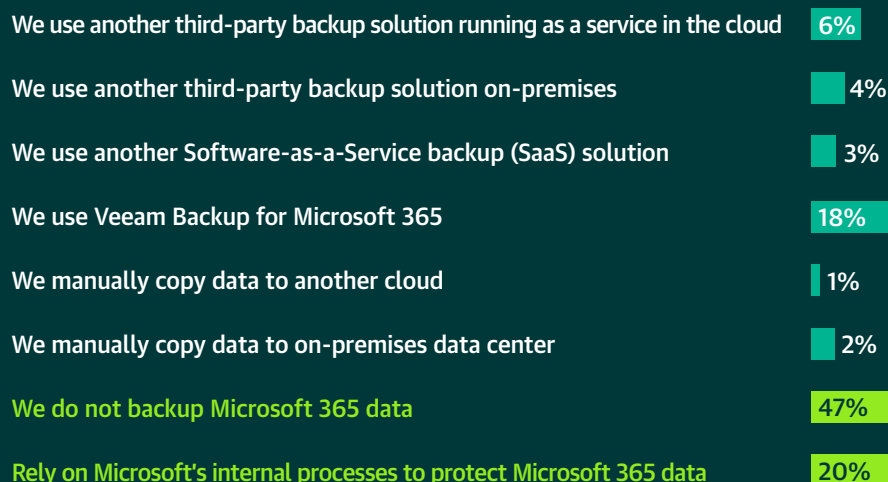
Microsoft 365 backup has become one of most commonly debated topics in the IT industry. The opinions are varied, with some IT professionals understanding why Microsoft 365 data is critical for their business and use a third-party backup, while others are on the fence but actively researching to discover the facts, and of course there are those that refuse to believe that a backup is necessary at all, believing strongly that Microsoft 365 mitigates any and all risks by itself.

Microsoft 365 backup has come a long way in the last four to five years. In survey data between 2017 and 2019 there were some amazing developments — people that formerly claimed “we rely on Microsoft’s native tools” was by far the majority and “we do not backup Microsoft 365” was a small percentage.

By 2019 however they had flip flopped, “we rely on Microsoft’s native tools” was down to 20% while “we do not backup Microsoft 365” had skyrocketed to 47%.

This shift can be explained by organizations previously thinking that Microsoft tools protected their data but realizing later on that native capabilities did not equate to a backup solution. They now acknowledge there is a gap in protection, and they are adopting a third-party backup solution to fulfill this need.

What is your organizations primary protection strategy for Microsoft 365?
(Please select one choice from the list below)



Planning your Microsoft 365 backup

- Installation package
- Infrastructure components
- Simple vs. advanced deployments
- Infrastructure planning
- Deployment options
- Supported storage
- Retention policies
- Backup architecture



Installation package

The Veeam® Backup *for Microsoft 365* installation image includes the following components:

1. Veeam Backup *for Microsoft 365*

Installs Veeam Backup *for Microsoft 365* with the following services:

- Control global configuration settings
- Manage backup proxy servers and repositories
- Process REST commands. (This component is disabled by default and can be enabled)
- Automate operations with PowerShell
- Restore backed up data via Veeam Explorers

2. Veeam Backup *for Microsoft 365* Console

Installs the following services:

- The user interface client for local and remote Veeam Backup *for Microsoft 365* servers
- Veeam Explorers for data restores

3. Veeam Backup *for Microsoft 365* PowerShell

Installs the PowerShell extension with sets of PowerShell cmdlets.

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

Installs the RESTful API plugin and the Restore Portal.

Infrastructure components

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. There are **three core components of this solution** – backup server, backup proxy and backup repository. Additionally, there are components such as RESTful API plug-in and PowerShell.



Backup server

The Veeam Backup *for Microsoft 365* server is the central configuration and control component. It is responsible for setting up and managing other components, job scheduling, task coordination and more.

The server can be installed on a physical or virtual Windows-based machine. The server includes access to Console UI.



Backup proxy

The Veeam Backup *for Microsoft 365* proxy is the workhorse behind the scenes which conducts all the read and write activities, and intelligently converts objects to smaller, manageable items.

Backup proxies provide an optimal route for backup traffic and enables data transfers to happen efficiently.



Backup repository

The Veeam Backup *for Microsoft 365* repository is the location where Microsoft 365 data is stored. Repositories can also store important metadata used during backup and recovery operations.

Backup repositories are supported on the following types of storage: object storage (on-premises and cloud), directly attached storage (DAS), SAN, SMB (Server Message Block 3.0).

Simple versus advanced deployments

With Veeam Backup *for Microsoft 365*, you can use both simple and advanced deployment options. Find out which one will work best for you.



Simple deployment includes the installation of all components onto a single server. This machine can be either virtual or physical. Specs should follow configuration maximums. In this scenario, all the major components (i.e., the server, proxy and repository) are installed on the same machine.

A simple deployment scales out by adding multiple repositories that are operated by the same built-in proxy server. Simple deployments are suitable for small-to-medium-sized businesses (SMBs) that want to have a local backup copy of their Microsoft 365 data on-premises. This applies to public cloud deployments like Azure Cloud, AWS and other offerings too. In this case, backup data can be stored on disk/file-based repositories attached to the servers, as well as object storage repositories sitting in the public cloud and on-premises.



Advanced deployment gives the option to scale out installations by adding proxy and repository components to meet demanding business requirements. The process of adding these components is handled by the main server. When scaling out to an advanced deployment, the server installs the necessary components onto the required servers. It works by deploying the main veeam.archiver, proxy service along with a copy of the infrastructure configuration.

This newly added proxy benefits from the view of the entire infrastructure and provides the option to configure backup jobs by using additional repository targets. This entire process is wizard driven. Full automation is also possible using native PowerShell commands and RESTful APIs. Servers and proxies can be part of the same domain, a separate domain (with trust relationship) and even part of workgroups.

Infrastructure planning

Typically, the size of an environment dictates the deployment model. The size of an environment is not necessarily related to the number of Microsoft 365 users to protect. Instead, it's based on the number of objects to protect. The following objects are supported:



**Microsoft
Exchange**

- Primary mailboxes
- Archive mailboxes
- Shared mailboxes
- Public folders
- Resource mailboxes



**Microsoft
SharePoint**

- Collaboration sites
- Communication sites
- Personal sites



**Microsoft OneDrive
for Business**

- OneDrive for Business account



**Microsoft
Teams**

- Team (including channels and tabs)

Recommended configuration maximums

Max objects per instance	Max objects per proxy	Max users per job	Max proxies per deployment	Max users per proxy	Max users per deployment	CPU/ RAM per proxy	Max size per repository
1,000,000	20,000	5,000	50	5,000	250,000	8x CPU/ 32GB	Unlimited

Deployment options

Your Veeam Backup *for Microsoft 365* deployment can run on-premises, private, public and hybrid cloud environments. The prerequisites and how these components work for each environment are very similar. IT organizations have the flexibility to choose from different designs based on their current requirements.

On-premises deployments

For customers who want to have a local backup copy of Microsoft 365 data, an on-premises deployment is the best option because it has the ability to easily scale out from simple to advanced installations. This kind of deployment provides the flexibility required by an organization that uses Microsoft 365 hybrid deployments where the protected data resides within any combination of online and on-premises infrastructures.

Service providers deployments

Veeam Backup *for Microsoft 365* is employed by service providers who offer BaaS for Microsoft 365 data to their customers. The infrastructure is flexible and can be leveraged for “exclusive” access to single tenants and in “shared mode” where the same service can cover several organizations spread over separate repositories to maintain multi-tenancy.

Azure and AWS deployments

In the case of Microsoft Azure, there is a certified and pre-installed application available in the Azure Marketplace. Azure Marketplace requires the customer to enter the details of the Microsoft 365 tenants. Likewise, in the case of Amazon AWS, the application is certified and available from the AWS Marketplace. It comes preinstalled into an AWS EC2 instance and it is a matter of choosing the instance type based upon requirements.

Other public cloud providers

Veeam Backup *for Microsoft 365* allows the deployment on other preferred cloud providers. In fact, Veeam Backup *for Microsoft 365* can virtually run from any cloud. If the minimum requirements for the deployment are satisfied, any public cloud provider is a suitable candidate. This still provides the option to store the data into a separate location when desired.

Supported storage

Veeam Backup *for Microsoft 365* support a variety of different storage options. Backup repositories are supported on the following types of storage:



DAS

Directly attached storage (DAS) is supported, which includes DAS, USB/external serial advanced technology attachments (eSATA) and raw device mapping (RDM).



SAN

The server and proxy can be connected to the storage area network (SAN) fabric via hardware, a virtual host bus adapter (HBA) or software internet small computer system (iSCSI) initiators. This provides direct access to the repository. For simple deployments, the SAN is presented to the server. With advanced deployments, SAN storage is presented to the proxy directly. The latter proves useful when delegating the execution of jobs to proxies for larger environments.



Object storage

For organizations that have a cloud first strategy, Veeam supports object storage. These include AWS S3, Microsoft Azure Blob Storage, IBM Cloud, S3-compatible (cloud and on-premises) and more. You can also store a backup copy in lower cost, long-term object storage including Amazon S3 Glacier, Glacier Deep Archive and Azure Archive.



SMB

SMB: (Server Message Block 3.0 and higher) is supported. Since the server and the proxy run under a local system account, the server's computer account must have the corresponding permissions on the network share. Windows 7 SP1 and Windows 2008 R2 SP1 do not support SMB (3.0) shares.

Retention policies

The retention policy is a configuration that applies to repositories directly, not to jobs. This is a global setting and it affects all backup jobs that use the same repository. There are two types of retention policies – item-level and snapshot-based.



Item-level retention policies operate in two ways:

1. During the first backup, objects that are included within the retention policy period are evaluated based on their last modification date. For example, by setting a retention policy of three years, the backup job will automatically include all the items in which this value is below three years. This will leave out anything older than three years.
2. Based on the age of the data and according to the last modification date, all data that's older than three years will be automatically purged from the repository. At any point in time, the repository will only include a rolling time window based on the retention policy set for the specified period.



Snapshot-based retention policies operate in two ways:

1. During the first backup, all available objects are included in the backup job, regardless of their creation, deletion or modification time. The first backup is a full backup. This is followed by incremental backups, which only add changes like new, deleted and updated items from the previous job.
2. At selected intervals and based on a schedule, the repository will then apply the retention policy based on their last backup date. This provides a point-in-time (PIT) approach.

Edit 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 repository.

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

Advanced

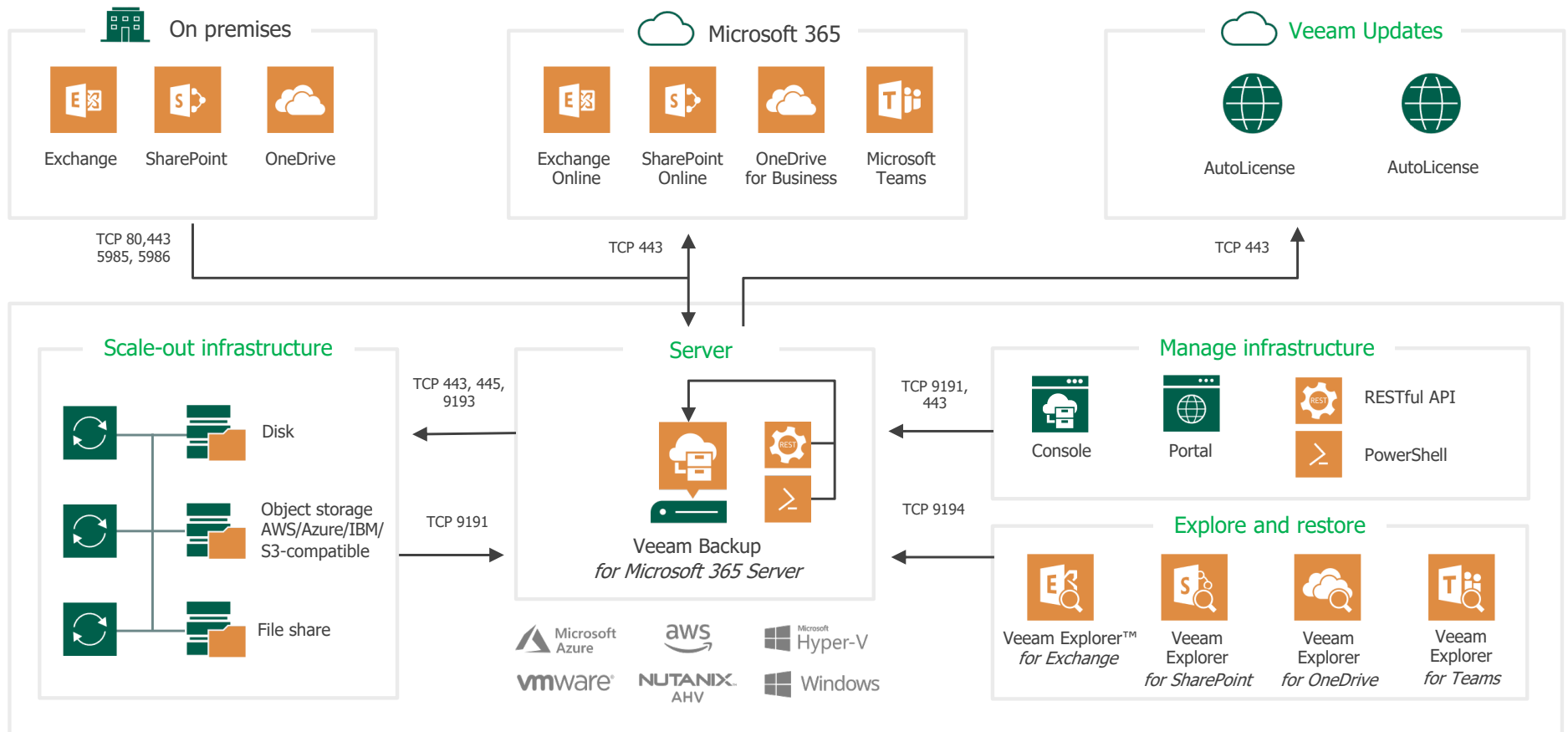
Back

Finish

Cancel

Backup architecture

Veeam Backup for Microsoft 365



How to back up and restore with Veeam

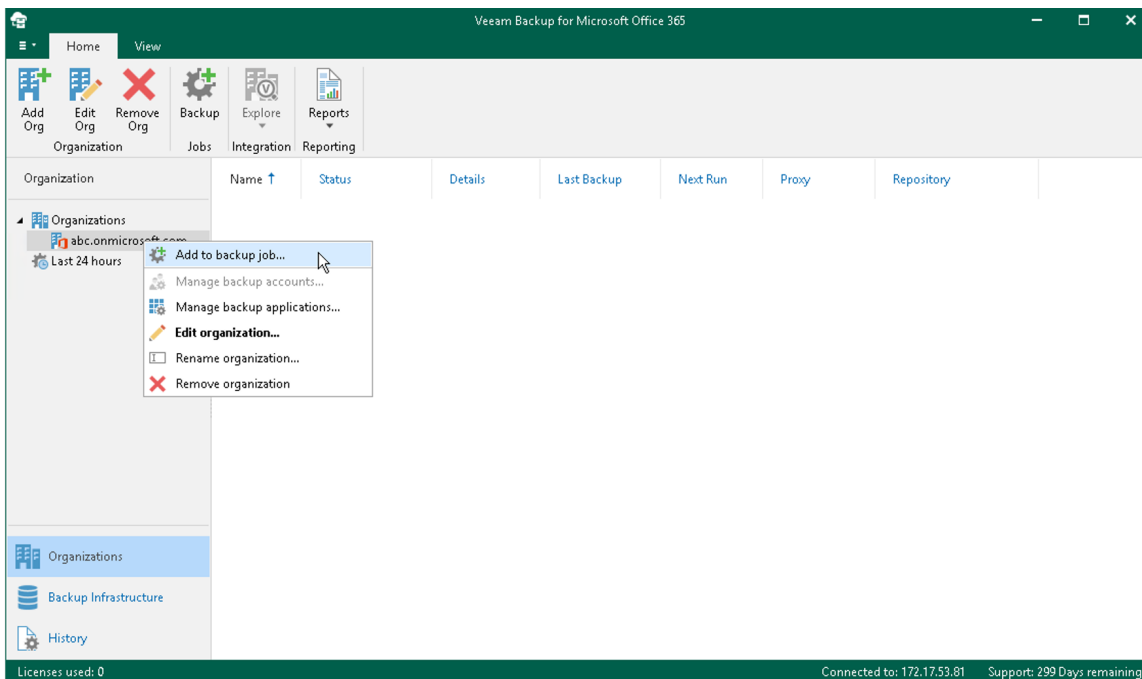
- Creating a backup job
- Selecting backup scope
- Scheduling options
- Veeam Explorers
- Exploring Microsoft 365 data
- How to restore in 1-2-3



Creating a backup job

To back up data of your Microsoft 365 and on-premises organizations, you use backup jobs.

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



Backup job steps

Creating a backup job in Veeam Backup for Microsoft 365 is an easy, wizard-driven process. There are six steps you will need to follow for the backup job setup:

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

Selecting backup scope

In Veeam Backup *for Microsoft 365*, you can select to **back up an entire organization or specify users, groups, sites, teams and organizations**. You can also select objects to exclude that you do not want to backup. You have the following options:

Create scope

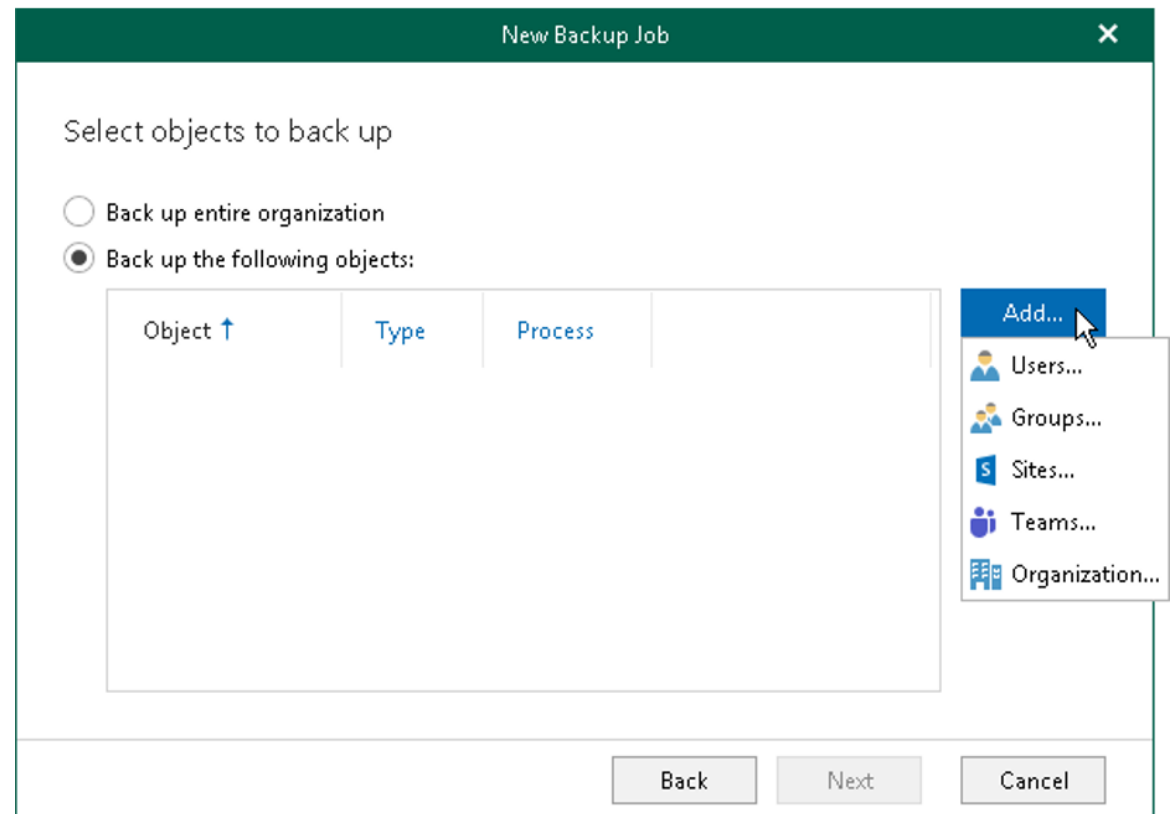
- Add entire organization applications
- Add Teams, users, sites
- Dynamically add with Microsoft 365 groups

Exclude scope

- Exclude sites, Teams or users
- Dynamically exclude with Microsoft 365 groups

Some considerations:

- You can create only one entire organization backup job per organization.
- Objects that are already processed by any of your backup jobs will be skipped from the entire organization processing list.
- When you add an organization object, [processing options](#) are applied to all users, groups and sites in the selected organization.



Scheduling options

Veeam Backup for Microsoft 365 allows you to tailor your backups to your exact specifications. You can select one of the following options:

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

The 'New Backup Job' dialog box has a title bar with a close button. The main content area is titled 'Select scheduling options'. It contains several checkboxes and input fields:

- ☒ Run the job automatically
 - ☒ Daily at this time: 1:00 AM (dropdown: Everyday)
 - ☐ Periodically every: 5 minutes (dropdown: Schedule...)
- ☒ Retry failed objects processing: 3 (dropdown: times)
 - Wait before each retry attempt for: 10 (dropdown: minutes)
- ☒ Terminate the job if it exceeds allowed backup window (button: Window...)
- ☒ Start the job when I click Create

At the bottom are three buttons: Back, Create, and Cancel.

- Time periods can be selected in the dialog, in which you can:
- Set the **Permitted** execution time frame for the backup job.
 - Set the **Denied** execution time frame for the backup job.

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

- Monday from 3 a.m. up until 9:59 a.m.
- Thursday from 2 p.m. up until 8:59 p.m.

The 'Time Periods' dialog box has a title bar with a close button. It displays a calendar grid for the days of the week (Sunday to Saturday). The grid shows time slots from 12 to 12. A legend on the right indicates that a blue square represents 'Permitted' and a white square represents 'Denied'.

The grid shows the following denied periods:

- Monday: 3:00 AM to 9:59 AM
- Thursday: 2:00 PM to 8:59 PM

At the bottom are two buttons: OK and Cancel.

Veeam Explorers

Veeam Explorers for *Microsoft Exchange*, *Microsoft SharePoint*, *OneDrive for Business* and *Microsoft Teams* are designed to search and recover data between online, on-premises and hybrid Microsoft 365 deployments.

There are [40 total restore options available](#).



Veeam Explorer for Microsoft Exchange

To explore and recover Microsoft Exchange mailboxes, folders, messages, tasks, contacts and items.



Veeam Explorer for Microsoft SharePoint

To explore and recover Microsoft SharePoint sites, libraries and items.



Veeam Explorer for Microsoft OneDrive for Business

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



Veeam Explorer for Microsoft Teams

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

Veeam Explorers assist the architecture with the following tasks and use cases:

- **In-place and out-of-place restores:** by default, these restores provide the capability to recover data to the original location. This is known as an in-place restore. Where required, the ability to perform restores to a different location is also supported. In this case, it performs an out-of-place restore.
- **Browse content:** once Microsoft 365 organization data (both online and on-premises) is stored in a repository, the Veeam Explorer component directly reads these backup files to present the entire content in a hierarchical format. For each object, the built-in browsers offer a context-sensitive option to send, restore and export.
- **Search for content:** the Veeam Explorer components include an "Advanced Find" capability to perform sophisticated eDiscovery searches by using different criteria based on data and metadata. The table below shows the current field groups. Searches can include multiple criteria.

Exploring Microsoft 365 data

You can explore your Microsoft 365 data four key ways:

1. Exploring backup jobs

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

2. Exploring single organizations

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.

3. 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.

4. Exploring point-in-time

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

Use the latest available state.

Select this option to load the latest state of items in the backup file.

Use the following point in time.

Select this option to load a backup as of the selected date.

Specify point in time

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

☐ Use the latest available state

☒ Use the following point in time:

Friday, November 27, 2020 5:02:51 AM

Use these eDiscovery settings to find mailbox items which are no longer present in the selected state. Enabling these options may significantly increase the amount of data returned by queries.

☒ Show items that have been deleted by user

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

Back Finish Cancel

How to restore in 1-2-3: step 1

There are three major steps for restoring Microsoft 365 data with Veeam. The first step to setup restores is to launch the restore wizard. In this example we'll show how to restore data from OneDrive for Business.

Launch the Restore wizard.

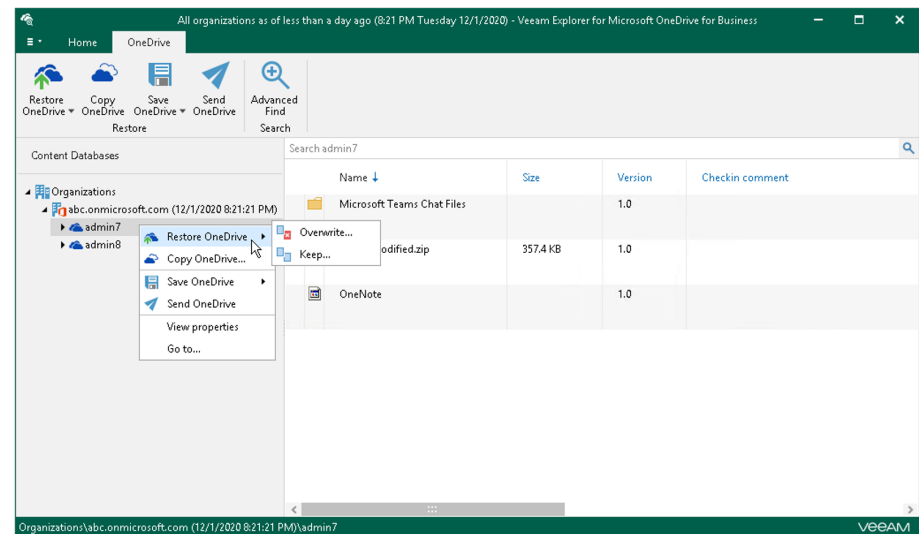
To launch the **Restore wizard**, you will do the following:

1. Select an object that you want to restore:

- To restore a OneDrive for Business account, select the necessary account in the inventory pane.
- To restore a folder, select the necessary folder in the inventory pane.
- To restore a document, select a folder that contains the document in the inventory pane and select the document in the preview pane.

2. On the **OneDrive/Folder/Document** tab, click **Restore OneDrive/Restore Folder/Restore Document** and select one of the following options:

- **Overwrite** — to completely overwrite existing OneDrive data.
- **Keep** — to preserve existing data and recover items with the **RESTORED** prefix (RESTORED-`<file_name>.ext`).



Alternatively, right-click an object that you want to restore and select **Restore OneDrive/Restore folder/Restore document > Overwrite** or **Restore OneDrive/Restore folder/Restore document > Keep**.

How to restore in 1-2-3: step 2

At this step of the wizard, choose whether you want to use modern or basic authentication.

Modern authentication

To use modern authentication, do the following:

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

This will allow Veeam Backup for Microsoft 365 to use an Azure AD application for a restore. For more information, see [Microsoft 365 Organizations](#).

2. In the **Application ID** field, enter an identification number of the Azure AD application that you want to use for a restore. By default, Veeam Explorer for Microsoft OneDrive for Business populates this field with the identification number of the application that was used during a backup session. If you want to use another application, make sure to grant this application required permissions. For more information, see [Permissions for Modern App-Only Authentication](#).

Basic authentication

Basic authentication can only be used by organizations that still support legacy auth protocols. To use basic authentication, do the following:

1. From the **Specify the authentication method** drop-down list, select **Basic authentication**.
2. Enter credentials to connect to the SharePoint organization.

Restore Wizard

Office 365 connection settings

Specify the authentication method:

Basic authentication

Specify user account to connect with:

Username: administrator@abc.onmicrosoft.com

Password:

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

Back Next Cancel

How to restore in 1-2-3: step 3

This step is only available if you have selected the **Modern authentication** option at the previous step of the wizard.

At this step of the wizard, sign into your Microsoft 365 organization.

To sign into 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.

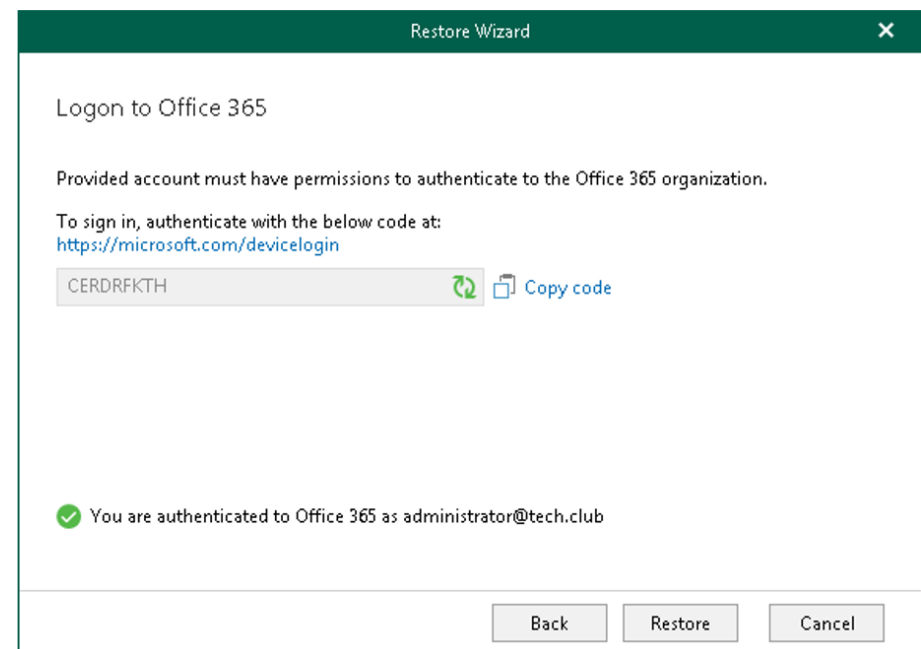
2. Click the link to the Microsoft portal.

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

Make sure to log in with the user account that has required permissions assigned. For Veeam Explorer *for Microsoft OneDrive for Business*, required permissions are the same as for Veeam Explorer *for Microsoft SharePoint*. For more information, see [Required Permissions](#).

Make sure that the required settings are specified for the Azure AD application used for restore. For more information, see [Configuring Azure AD Application Settings](#).

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



Keep in mind, there are additional steps needed to restore certain applications.

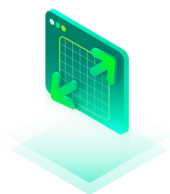
What should matter to you?

- Key difference makers
- What are customers saying?
- Conclusion



Key difference makers

There are some key benefits that Veeam Backup *for Microsoft 365* can provide over other vendors. Many backup vendors do not offer the flexibility or functionality necessary to tailor data protection to specific business needs.



Complete flexibility

Maintain ownership of data by choosing any infrastructure that fits your business need and change it whenever required with support for nearly any cloud or hardware platform.

SaaS vendors typically limit the cloud options and may force customers to use their cloud. Changes are rarely possible after setup.



Customizable backup

Maintain control by delivering the appropriate level of protection to different users according to the business value of their data.

Backup frequency is rarely flexible with SaaS vendors, preventing organizations from delivering the right level of protection to their different users.



Many recovery options

Minimize business downtime by recovering data in the way that makes the most sense, no matter the kind of data loss.

Other backup vendors provide limited ability to minimize downtime after data loss, as data may not be recoverable exactly as needed by an organization.

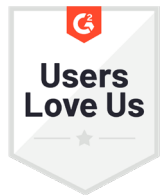
What are customers saying?

Most customers that use Veeam Backup *for Microsoft 365* think that it is a great product, but don't take our word for it – see for yourself! Luckily, there are a few third-party review platforms where you can find completely raw and unfiltered reviews and opinions of the product, including [TrustRadius](#), [G2 Crowd](#) and [Reddit Forums](#).

Get Veeam Backup for MS 365 – your boss will love you!

"Cloud services have flaws, and it is ultimately the sys admin's responsibility to ensure data is safe. Veeam Backup for MS 365 does exactly what it says on the box, by allowing the administrator to take control of their data."

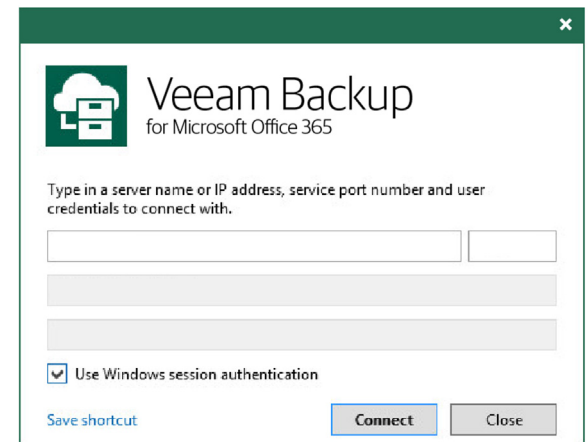
— **IT Administrator**
Staffing & Recruiting
1001-5000 employees



Veeam Backup for M365 keeps your data protected how you choose!

"It allows us to address a major concern with Microsoft 365, and that's being in control of our data. With M365, you often don't know where your data is stored and if there's an issue, how you will recover from it. With Backup for M365, we're in charge of making sure our data is protected."

— **Systems Administrator**
Moses Lake Industries
Semiconductors |
201-500 employees

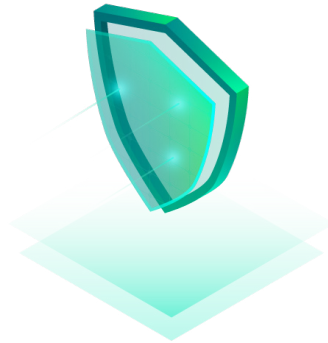


Conclusion

With Microsoft 365, it's your data — you control it — and it is your responsibility to protect it.

Veeam Backup *for Microsoft 365* eliminates the risk of losing access to your Microsoft 365 data including Exchange Online, SharePoint Online, OneDrive for Business and Microsoft Teams. It ensures that you remain in complete control and that your data is always protected and accessible.

With Veeam, you can securely back up Microsoft 365 to any location including on-premises, Azure, AWS or a service provider and:



Protect your Microsoft 365 data from accidental deletion, security threats and retention policy gaps



Quickly restore individual Microsoft 365 items and files with industry-leading recovery flexibility



Meet legal and compliance requirements with efficient eDiscovery of Microsoft 365 backup archives



To learn more about Logicalis + Veeam,
please: [Contact us!](#)



Gold
Microsoft Partner



#1 Microsoft 365 Backup

More control. Effortless recovery.

NEW Veeam® Backup *for Microsoft 365 v6* has added the **Self-Service Restore Portal** for Microsoft 365 environments, empowering IT administrators to securely delegate restores to their users. **V6** also includes **backup copy to Amazon S3 Glacier, Glacier Deep Archive and Azure Archive**.

Version 6 of Veeam Backup *for Microsoft 365* provides:

- **Automation and scalability** for enterprise organizations
- **Time savings** through handling restores for Microsoft 365 users
- **Enhanced security** with multi-factor authentication (MFA)
- **Recovery confidence** with a backup copy in low-cost object storage

