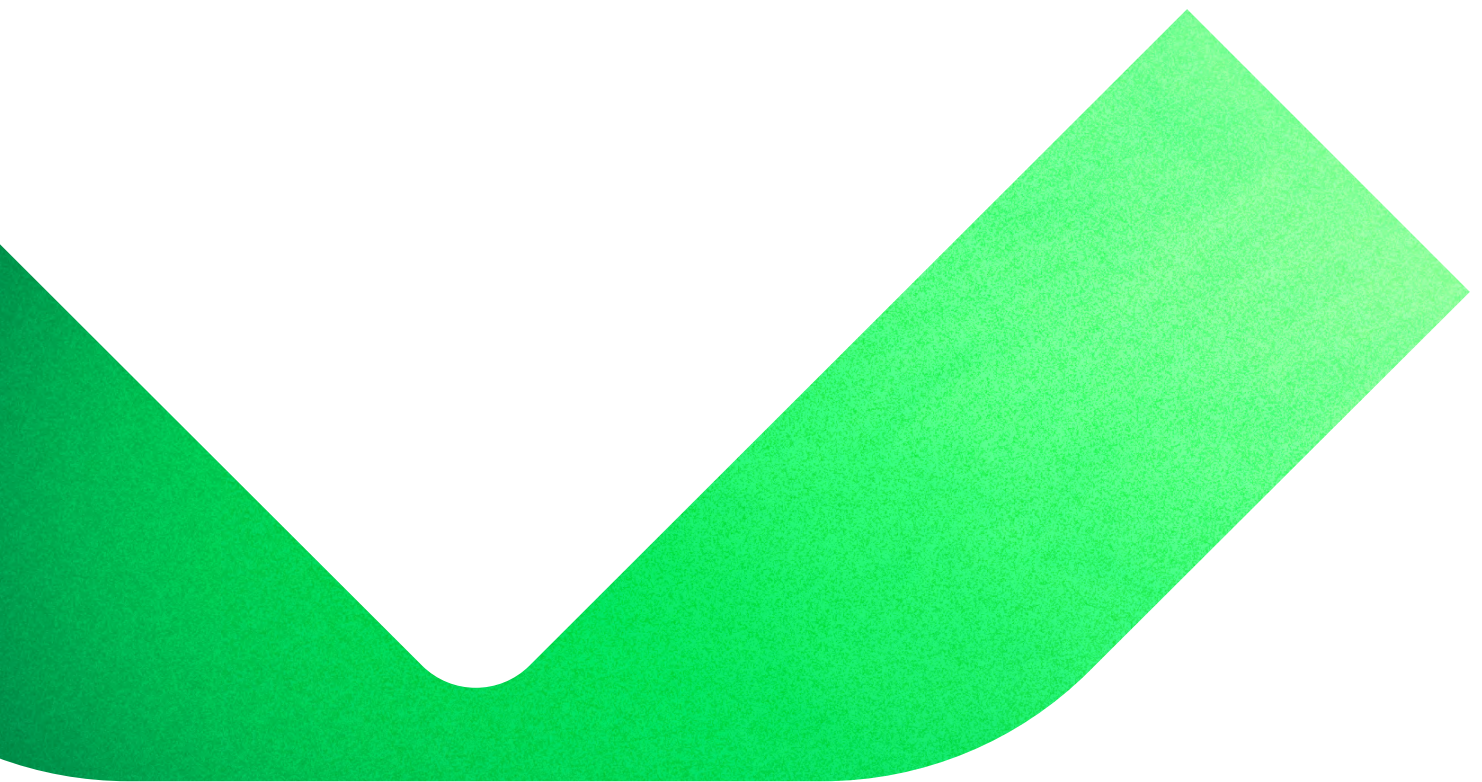




Veeam Backup *for Microsoft 365* v8.0

What's New



Introduction

Veeam Backup for Microsoft 365, the leader in protecting data in Exchange Online, SharePoint Online, OneDrive for Business and Teams now provides you with complete immutability, increased scalability and more. The following is the list of new features and enhancements you can now leverage in Veeam Backup for Microsoft 365 v8.

Complete immutability

Keep your Microsoft 365 backup data tamper-proof and protected against ransomware, accidental, or malicious deletion. With immutable backups introduced in version 8, alongside immutable backup copies, you can ensure comprehensive support for fully immutable backup data.

Gain flexibility and control by storing your immutable backups in the object storage of your choice, including Azure Blob Storage, Amazon S3 and Wasabi. Choose to make your backups immutable for a specific number of days or the entire duration of the repository retention period, tailoring your data protection strategies to your needs. Service providers can effortlessly manage exit strategies with the governance mode option, giving privileged storage administrators the ability to override lock settings when necessary.

Scalability and performance

Achieve enterprise-level scalability and enhance your backup and restore operations with Veeam Proxy Pools. Combine multiple (up to 150) backup proxies into a proxy pool to protect up to 1M objects and enable automated load balancing based on CPU and RAM consumption, as well as Microsoft 365 throttling. Each proxy pool can simultaneously work with multiple object storage repositories and include both Linux and Windows backup proxies. Easily scale up as needed by adding more backup proxies on the fly. Additionally, using proxy pools you can simplify regular maintenance and operating system upgrades on proxies—without interrupting your backup and restore operations.

Architectural changes

- **Centralized PostgreSQL database** — PostgreSQL is now a mandatory component that hosts all product databases, including the product's configuration database, organization's cache databases, and repository persistent caches. You can use your existing PostgreSQL server or install a new instance that comes as part of the Veeam Backup for Microsoft 365 deployment.
- **NATS Server** — NATS Server with the JetStream engine is now a mandatory component required for Veeam Backup for Microsoft 365. This high-performance messaging system forms the basis for backup proxy pool operations, providing scalability and streaming for distributed data processing.

Other new features and enhancements

General

- **Shared and private teams channels backup and restore** — ensure complete protection of your Microsoft Teams, including private and shared team channels, its tabs, files, messages, settings, and membership.
- **Linux backup proxies** — simplify your backup infrastructure management and reduce TCO by using Linux hosts as remote backup proxies, with support for both Red Hat and Ubuntu.
- **Ready-to-use object storage repositories** — set up a ready-to-use object storage repository with a single wizard that guides you through all the required steps and settings — from naming to immutability and retention settings.
- **Microsoft Educational SKUs** — easily identify the Microsoft SKU type and assigned Microsoft 365 licenses for your protected users, including educational plans.
- **S3 One Zone-Infrequent Access** — meet your restore time objectives and storage budget with the flexibility to store your backups in the S3 One Zone-Infrequent Access storage class.
- **Retention period settings at a glance** — instantly see retention period settings for each of your repositories in the Backup Infrastructure view and simplify your daily administrative routine.
- **Last cache update at a glance** — instantly see the time of updating the cached list of your organization's objects when you fill in your backup job with users, groups, teams, and sites to protect.
- **Distributed tracing** — ensure faster troubleshooting in a distributed Veeam Backup for Microsoft 365 infrastructure and track internal product requests to background services and databases with distributed tracing.
- **Install license along with the product installation** — install your Veeam license file during Veeam Backup for Microsoft 365 deployment and save time on post-deployment product administration.

Management and security enhancements

- **RBAC to the backup console and Veeam Explorers** — keep backups management under control by granting specific users and groups permissions to access Veeam Backup for Microsoft 365 console and Veeam Explorers. Enable multi-factor authentication (MFA) logon for backup administrators to strengthen access security.
- **Custom service account for a proxy service** — improve security by using a dedicated custom user account for running a backup proxy service.
- **OAuth 2.0 support for email notifications in Veeam Explorers** — secure authorization and access-token-based authentication for Google Gmail and Microsoft 365 through the modern OAuth 2.0 protocol.
- **Cookie headers in REST APIs requests** — for meeting security best practices and simplified authentication, incoming REST API requests can now authorize via cookie headers.

- **REST APIs tokens invalidated on logout** — both access and refresh tokens are invalidated on user logout to ensure a secure termination of the user session and prevent any unauthorized access to protected resources.
- **Control available REST API endpoints** — harden security by keeping the availability of REST API endpoints under control. Restrict the availability of the Swagger UI and endpoints that are not required for the Restore Portal.

REST APIs

- **Optimized restores via REST APIs** — we optimized data restores initiated via REST APIs and made backup proxies responsible for executing data restores to the initial or new locations, thus reducing the number of product components involved and connections required.
- **Relationship between a restore event and organization objects** — the (GET) /v8/restoreSessions/{restoreSessionId}/events/{eventId} request now returns the following parameters in the response: "organizationId", "backedUpOrganizationId", "userId", "groupId", "siteId", "teamId".
- **Restore sessions filtering** — (GET) /v8/RestoreSessions requests now allow for filtering restore sessions by their from/to completion time.

Data processing and operational improvements

- **Resuming SharePoint backups** — interrupted full and incremental SharePoint Online backups are restarted from the point of interruption to save on repetitive data processing from scratch.
- **Faster enumeration of SharePoint sites** — we improved the speed of listing SharePoint sites in various scenarios, including backup job configuration and defining a scope for restore operators.
- **More stable restore sessions connections** — we made the connection between Veeam Explorers and the Veeam Backup for Microsoft 365 controller more resistant to unexpected glitches to handle mass restores and avoid any restore interruptions.
- **Consolidation of data in S3-compatible repositories** — on-demand consolidation of smaller data objects in S3-compatible object storage repositories allows fitting the storage system limits on the maximum number of objects in a bucket.

Important changes

- **Paid APIs for Teams channel messages backup** — protection of teams channel messages is now only possible via the protected paid Teams Export APIs, which becomes the default and only setting. For more information see [KB4453](#), [KB4340](#), [KB4322](#).
- **Deprecation of Basic authentication** — modern app-only authentication is the default and only connection method for new Microsoft 365 organizations that you want to protect with Veeam.