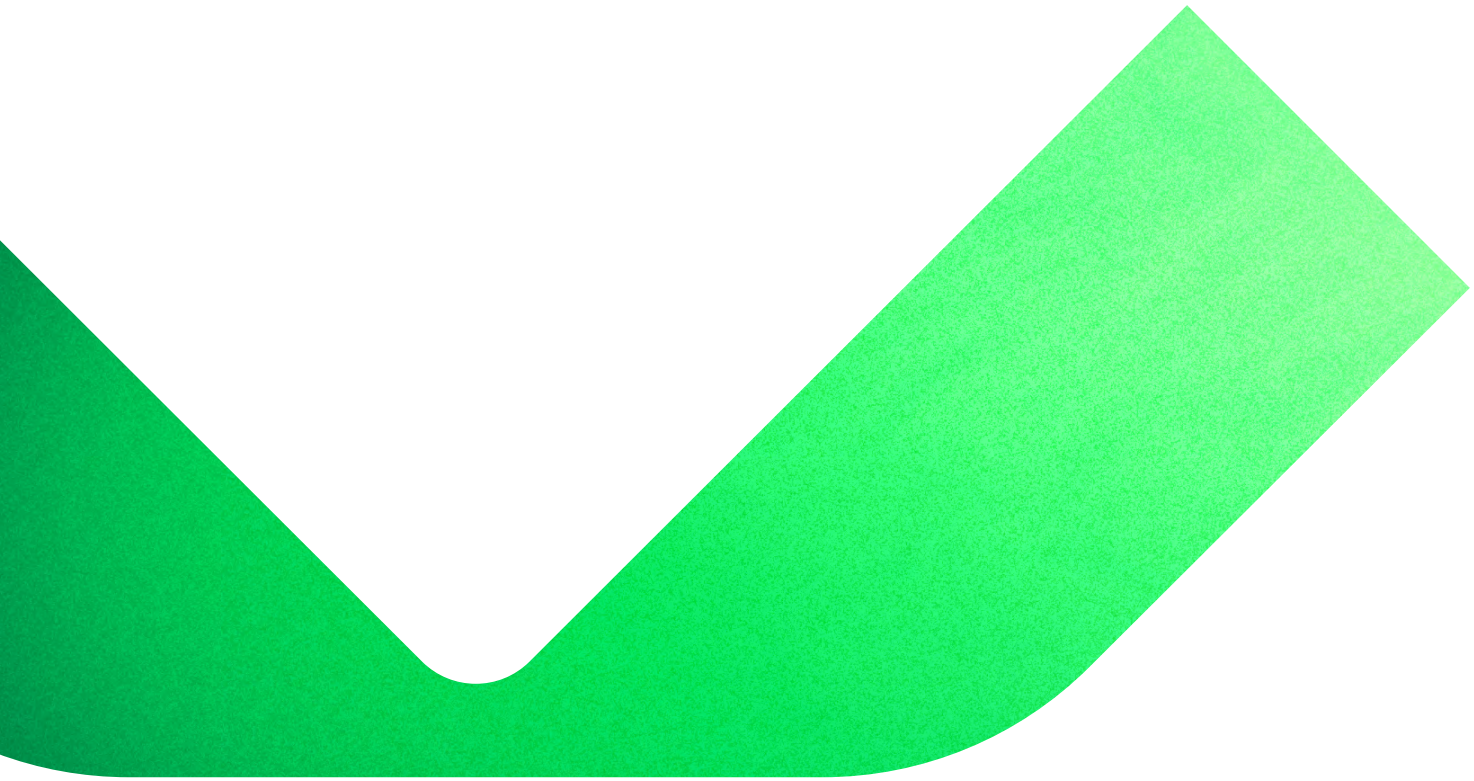
Veeam Agent *for Microsoft Windows* v6.3

What's New



Added in v6.3

Platform support

Upgrade to the latest Microsoft releases with confidence thanks to the official support for:

Microsoft Windows Server 2025 and Microsoft Windows 11 24H2 support — V6.3 adds full support for the latest Microsoft Windows operating systems. This includes support for recovery media creation and correct operating system version detection and handling in the UI.

Microsoft SharePoint SE 24 H2 support — V6.3 adds support for application-aware processing of the latest SharePoint version.

Restore

Automated Bare Metal Recovery — Automate the recovery process with support for answer files, streamlining the restoration of systems to the original or dissimilar hardware. By completely eliminating the need for manual input during recovery or limiting users to only basic settings like restore point selection, this capability eliminates the requirement for end-user training or detailed guidance during the recovery process while avoiding input errors. This makes bare metal recoveries effortless for backup admins and helps to get your end users back to being productive faster.

Bare Metal Recovery from manual copies — Due to popular demand, we are adding the ability to perform bare metal recovery from a locally attached storage device containing backups manually copied from a backup repository. This provides added flexibility and convenience by allowing you to restore systems without establishing a direct network connection to the backup repository, which may not always be feasible. Note: To enable this functionality, create recovery media once agent is upgraded.

General

Backup network detection — Optimize backup data flow and reduce backup window by creating the *AgentDirectConnectionPriority* (DWORD, 1) registry value under the *HKLM\SOFTWARE\Veeam\Veeam Endpoint Backup key* on the protected machine to instruct the backup agent to prioritize the backup repository IP address within the same subnet as the agent, optimizing network efficiency and improving backup performance through reduced latency and increased data transfer speeds. **Note:** This option is not enabled by default because it changes the current behavior, and we try to avoid such disruption in minor releases.

Hidden repository size for managed agents — We hid the repository size and remaining capacity from the backup job wizard and from the Control Panel on the managed backup agents. This should eliminate questions and concerns from end users about backup repository space which many Veeam backup administrators told us they struggle with.

Expanded GFS configuration — GFS settings now offer additional options, allowing you to specify the second, third, and fourth week for the monthly GFS setting. This helps backup administrators align long-term retention with business needs and organizational policies.

GFS restore point notification — The job action log will now specifically highlight the creation of a GFS restore point, providing better visibility into GFS restore point selection logic and facilitating troubleshooting of long-term retention policy behavior.

Added in v6.2

File-level recovery

File restore target selection — users can now leverage the new Restore To option during file-level recoveries to specify a different Windows machine as the restore target. This dramatically simplifies restore operations at the backup server when the original machine is no longer available and can facilitate complex migration scenarios by providing the flexibility to easily extract all data from backup to the desired destination.

ReFS support in cloud machines — file-level recovery is now supported from cloud-native agent backups of AWS EC2 instances and Microsoft Azure virtual machines with ReFS disks. Requires file-level recovery to be started at the backup server.

User interface

UI branding — in response to popular demand, we have introduced the ability to customize the Control Panel logo image and the tray icon. This feature allows you to align the user interface with your corporate aesthetics, reinforcing your brand's identity. To perform the customization, create the LogoIcon (DWORD, 1) registry value under the HKLM\SOFTWARE\Veeam\Veeam Endpoint Backup key on each endpoint and place your custom logo.png and logo.ico files into the %ProgramFiles%\Veeam Endpoint Backup\Resources folder.

Added in v6.1

Security

Malware detection — when backing up to a Veeam repository, standalone and self-managing agents include the suspicious file system activity detection functionality explained at the beginning of this document (Managed by Server agent-based backup jobs provide full malware detection capabilities).

Backup storage

Scale-out backup repositories from object storage support — starting from this version, standalone agent can store its backup in a scale-out repository with Performance Tier backed by a single object storage extent.

Backup mapping support for object storage repositories — standalone agents now support mapping of the existing backups stored in an object storage repository to a new backup job.

Platform support

Microsoft Windows 11 23H2 support — added full support for the latest version (23H2) of Microsoft Windows 11 operating system. This includes support for recovery media creation and correct operating system version detection.

Added in v6.0

General

Lower resource usage with SQLite — v6 now uses SQLite instead of Microsoft SQL Server LocalDB for its configuration database. This significantly reduces resource consumption, dramatically lowers agent redistributable size and helps you avoid possible conflicts with your existing SQL Server installations. When upgrading to V6, your existing configurations will automatically be migrated into a newly provisioned SQLite instance. The LocalDB can then be uninstalled manually if desired.

Kerberos-only authentication — V6v can now be deployed in environments with NTLM authentication disabled for enhanced security. Kerberos-only authentication is supported out of the box as long as all the backup infrastructure components are using valid and resolvable DNS names (IP addresses are not supported by Kerberos).

IPv6 support — added support for IPv6 communication in both IPv6-only and dual-stack networks where the agent gives preference to IPv6 over IPv4 addresses when both are available. This flexibility allows you to set up your backup infrastructure in an IPv6-only network right away or gradually migrate to IPv6 by running it alongside your IPv4 infrastructure.

OAuth 2.0 support for email notifications — in addition to basic SMTP authentication, v6 now supports secure authorization and token-based authentication for Google Gmail and Microsoft 365 with the modern OAuth 2.0 protocol.

Backup engine

Changed Block Tracking (CBT) for Microsoft Windows workstations — in addition to Microsoft Windows servers, Veeam's® CBT driver can now be installed on workstations that run Windows 10 or Windows 11 operating systems when faster incremental backup is desired.

File-level backup enhancements — in addition to image-level backups, V6 is now able to leverage a CBT driver for file-level backups as well. Depending on the workload that runs on the protected machine, like when there are many large files that are constantly changing, the usage of a CBT driver can help you significantly accelerate incremental backup performance and reduce incremental backup size. Files smaller than 50MB are not tracked by the CBT driver to balance resource consumption during backup with achieved benefits.

Improved VPN connection detection — v6 adds support for detecting Palo Alto VPN connections for VPN-based backup restriction functionality.

Increased tolerance to Microsoft VSS issues — the backup job will no longer give up immediately in the case of a Microsoft VSS snapshot creation issue and will instead attempt to retry the snapshot creation operation a few times before failing. This should increase backup success rate for heavy-loaded application servers.

Backup storage

Direct backup to object storage — Take full advantage of the unlimited scalability, built-in reliability and resiliency of on-premises and cloud object storage without having to sacrifice backup and

restore performance. Back up directly to cloud or on-premises object storage or select an object-storage-based Veeam repository. Whenever this kind of repository is managed by a Veeam Backup & Replication™ server or Veeam Cloud Connect server, it also offers secure multi-tenant access to backups without the need to distribute individual access keys to all your agents or configure each agent to use a dedicated bucket.

Immutable backups — Ensure that your backups can always be restored after a cyberattack with comprehensive enterprise-grade immutability options that are provided by S3-compatible object storage, Amazon S3 and Microsoft Azure Blob storage and any S3 Compatible object storage that has Object Lock support. You can also now use immutable backups with a Veeam Hardened Repository and HPE StoreOnce repository that's managed by a Veeam Backup & Replication server.

Health check light — When backing up directly to an object storage repository as a target, storage-level data corruption guard scans will only check if all your required objects exist. This provides some balance considering the performance implications and cloud egress costs of full content verification.

Restore

Recovery tokens — V6 adds support for a simpler way to provide users who are performing Bare Metal Recovery with access to a particular backup that's stored in a Veeam repository. Veeam Backup & Replication v12 administrators are now able to generate time-limited access keys or recovery tokens to be shared with users and enable them to connect to a Veeam repository when performing Bare Metal Recovery.

User interface

Increased GFS restore point limit — You can now create weekly GFS retention policies of up to 9999 weeks long. Surprisingly, the previous UI limit of 999 weeks was not enough for some customers who face certain compliance requirements!

Platform support

Windows 10 22H2 and Windows 11 22H2 support — V6 adds full support for the latest version (22H2) of both Microsoft Windows 10 and Windows 11 operating systems. This includes support for recovery media creation and correct operating system version detection and handling in the UI.

Microsoft SQL Server 2022 support — V6 adds support for application-aware processing and transaction log backups for SQL Server 2022.

Microsoft SharePoint Server Subscription Edition support — V6 adds support for application-aware processing of the latest SharePoint Server version.