Veeam Backup & Replication 10 Release Notes

This document provides last-minute information about Veeam Backup & Replication 10, including system requirements, installation and upgrade procedure, as well as relevant information on technical support, documentation, online resources and so on.

The release version of Veeam Backup & Replication 10 is available for download at: veeam.com/backup-replication-download.html starting from February 18, 2020.

If you are upgrading to v10, please **review the upgrade checklist closely** prior to performing the upgrade.

See next:

System Requirements

We recommend that all 3rd party software and components are kept at the latest patch level, since these updates often address issues that can cause slow performance, backup failures and data corruptions.

VMware Infrastructure

Platforms

- vSphere
- vCloud Director
- VMware Cloud on AWS

Hosts

- ESXi 6.x (up to 6.7 U3)
- ESXi 5.5

Software

- vCenter Server or vCenter Server Appliance 6.x (up to 6.7 U3)
- vCenter Server or vCenter Server Appliance 5.x
- vCloud Director 10.0
- vCloud Director 9.x
- vCloud Director 8.20

Standalone ESXi hosts are fully supported, so vCenter Server and vCloud Director are optional. However, whenever they are present, we highly recommend that your register both with Veeam.

vSphere Virtual Machines

Virtual Hardware

- All types and versions of virtual hardware are supported.
- Virtual machines with virtual NVDIMM devices, with virtual disks engaged in SCSI bus sharing or residing on PMem datastores are not supported for host-based backup, because VMware does not support snapshotting such VMs. Please use agent-based backup to protect such VMs.
- RDM virtual disks in physical mode, independent disks and disks connected via in-guest iSCSI initiator are not supported for host-based backup. Such disks are skipped from processing automatically. If backing up these disks is required, please use agent-based backup.

OS

- All operating systems supported by VMware vSphere version in use.
- Microsoft VSS integration is supported for Microsoft Windows 2008 and later, except Nano Server (due to the absence of VSS framework).
- File level restore is supported for the following file systems, including Microsoft Windows Logical Disk Manager (LDM) dynamic disks and Linux Logical Volume Manager (LVM):

OS	Supported File Systems
Windows	FAT, FAT32 NTFS ReFS
Linux	ext2, ext3, ext4 ReiserFS JFS XFS Btrfs
BSD	UFS, UFS2
Mac	HFS, HFS+
OES	NSS
Solaris	UFS ZFS (except pool versions of Oracle Solaris)

Software

- VMware Tools (optional, recommended)

Microsoft Infrastructure

Hosts

- Windows Server Hyper-V 2019 (up to 1909 SAC release)
- Windows Server Hyper-V 2016 (including all SAC releases)
- Windows Server Hyper-V 2012 R2
- Windows Server Hyper-V 2012
- Windows Server Hyper-V 2008 R2 SP1
- Microsoft Hyper-V Server (free hypervisor) of supported Hyper-V versions

Depending on your Windows Server version, some additional hot fixes not included in the Windows Update distribution must be installed. Please refer to KB1838 for more information.

Microsoft Nano Server with Hyper-V role installed is not supported.

Software

- Microsoft PowerShell Engine 2.0 (optional, enables networkless guest processing)
- Microsoft System Center Virtual Machine Manager 2019
- Microsoft System Center Virtual Machine Manager 1807
- Microsoft System Center Virtual Machine Manager 1801
- Microsoft System Center Virtual Machine Manager 2016
- Microsoft System Center Virtual Machine Manager 2012 R2
- Microsoft System Center Virtual Machine Manager 2012 SP1
- Microsoft System Center Virtual Machine Manager 2008 R2 SP1

Standalone Hyper-V hosts and clusters are fully supported, so SCVMM is optional. However, whenever it is present, we highly recommend that your register one with Veeam.

Hyper-V Virtual Machines

Virtual Hardware

- Supported virtual hardware versions are 5.0 through 9.0.
- Both Generation 1 and 2 virtual machines are supported.
- Pass-through virtual disks and guest disks connected via in-guest FC or iSCSI initiators are not supported for host-based backup. Such disks are skipped from processing automatically. If backing up these disks is required, please use agent-based backup.

OS

- All operating systems supported by the Hyper-V version in use.
- Microsoft VSS integration is supported for Microsoft Windows 2008 and later, except Nano Server (due to the absence of VSS framework).
- File level restore is supported for the following file systems, including Microsoft Windows LDM dynamic disks and Linux LVM:

OS	Supported File Systems
Windows	FAT, FAT32 NTFS ReFS
Linux	ext2, ext3, ext4 ReiserFS JFS XFS Btrfs
BSD	UFS, UFS2
Mac	HFS, HFS+
Solaris	UFS ZFS (except pool versions of Oracle Solaris)

Software

- Hyper-V integration components (optional, recommended)

Veeam Backup & Replication Server

Hardware

CPU: x86-64 processor (minimum 4 cores recommended).

Memory: 4 GB RAM plus 500 MB RAM for each concurrent job.

Disk Space: 5 GB for product installation and 4.5 GB for Microsoft .NET Framework 4.7.2 installation. 10 GB per 100 VM for guest file system catalog folder (persistent data). Additional free disk space for Instant VM Recovery cache folder (non-persistent data, at least 10 GB recommended).

Network: 1 Gbps or faster for on-site backup and replication, and 1 Mbps or faster for off-site backup and replication. High latency and reasonably unstable WAN links are supported.

OS

Only 64-bit version of the following operating systems are supported:

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1
- Microsoft Windows 10 (version 1607 to 1909)
- Microsoft Windows 8.1
- Microsoft Windows 7 SP1

Software

- Microsoft SQL Server 2008 through 2019 (2016 SP1 Express is included)
- System Center Virtual Machine Manager 2008R2 through 1807 Admin UI (optional, to be able to register SCVMM server with Backup & Replication infrastructure)
- Microsoft .NET Framework 4.7.2 (included in the setup)
- Windows Installer 4.5 (included in the setup)
- Microsoft PowerShell 2.0 (included in the setup)
- Firefox, Google Chrome, Microsoft Edge or Microsoft Internet Explorer 11.0 or later

Veeam Backup & Replication Console

Hardware

CPU: x86-64 processor.

Memory: 2 GB RAM

Disk Space: 500 MB for product installation and 4.5 GB for Microsoft .NET Framework 4.7.2 installation.

Network: 1 Mbps connection to the backup server. High latency and low bandwidth impact user interface responsiveness.

OS

Only 64-bit version of the following operating systems are supported:

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1
- Microsoft Windows 10 (version 1607 to 1909)
- Microsoft Windows 8.1
- Microsoft Windows 7 SP1

Software

- Microsoft .NET Framework 4.7.2 (included in the setup)
- Microsoft PowerShell 2.0 (included in the setup)
- Windows Installer 4.5 (included in the setup)
- Firefox, Google Chrome, Microsoft Edge or Microsoft Internet Explorer 11.0 or later

Backup Proxy Server

Hardware

CPU: x86-64 processor (minimum 2 cores or vCPUs). Using multi-core processors improves data processing performance, and allows for more tasks to be processed concurrently.

Memory: 2 GB RAM plus 200MB for each concurrent task. Using faster memory improves data processing performance.

Disk Space: 300 MB.

Network: 1 Gbps or faster for on-site backup and replication, and 1 Mbps or faster for off-site backup and replication. High latency and reasonably unstable WAN links are supported.

OS

For VMware backup proxy server, 64-bit versions of the following Microsoft Windows operating systems are supported, including Core edition:

- Microsoft Windows Server 2019 (up to 1909 SAC release)
- Microsoft Windows Server 2016 (including all SAC releases)
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1
- Microsoft Windows 10 (version 1607 to 1909)
- Microsoft Windows 8.1
- Microsoft Windows 7 SP1

In addition, for hot add transport mode only, 64-bit versions of the following Linux distributions are supported:

- Debian 8 to 10
- Fedora 30, 31
- RHEL/CentOS 6.0 to 8.1
- openSUSE Leap 15.1
- Oracle Linux 6 (UEK3) to 8
- SLES 11 SP4, 12 SP1-SP5, 15 SP0-SP1
- Ubuntu 14.04 LTS, 16.04 LTS, 18.04 LTS, 19.10

Support for other distributions is experimental.

For Hyper-V off-host backup proxy server, the following operating systems are supported, including Core Edition (Hyper-V role enabled must be enabled on the server):

- Microsoft Windows Server 2019 (up to 1909 SAC release)
- Microsoft Windows Server 2016 (including all SAC releases)
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1

Software

For vSphere backup proxy server running on Microsoft Windows Server 2008 R2 or earlier:

- Microsoft Visual C++ 2008 SP1 Redistributable Package (x64). Installation package can be downloaded from https://vee.am/runtime

Backup Repository Server

These requirements also apply to mount servers (if separate from the repository server) and gateway servers for file share and deduplicating appliance-based repositories.

Hardware

CPU: x86 processor (x86-64 recommended).

Memory: 4 GB RAM, plus up to 2 GB RAM (32-bit OS) or up to 4 GB RAM (64-bit OS) for each concurrently processed machine (depending on machine size, number of disks and backup chain's length) or file share.

Network: 1 Gbps or faster for on-site backup and replication, and 1 Mbps or faster for off-site backup and replication. High latency and reasonably unstable WAN links are supported.

OS

Both 32-bit and 64-bit (recommended) versions of the following operating systems are supported, including Core edition:

- Microsoft Windows Server 2019 (up to 1909 SAC release)
- Microsoft Windows Server 2016 (including all SAC releases)
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1
- Microsoft Windows 10 (version 1607 to 1909)
- Microsoft Windows 8.1
- Microsoft Windows 7 SP1
- Linux (bash shell, SSH and Perl are required)

Tape Server

Hardware

CPU: x86 processor (x86-64 recommended).

Memory: 2 GB RAM plus 200MB for each concurrent task. Restoring VMs directly from tape requires 400MB of RAM per 1TB of the restored virtual disk size.

Disk Space: 300 MB, plus 10GB for temporary data storage for backup and restore operations.

Network: 1 Gbps or faster.

OS

Both 32-bit and 64-bit (recommended) versions of the following operating systems are supported, including Core edition:

- Microsoft Windows Server 2019 (up to 1909 SAC release)
- Microsoft Windows Server 2016 (including all SAC releases)
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1
- Microsoft Windows 10 (version 1607 to 1909)
- Microsoft Windows 8.1
- Microsoft Windows 7 SP1

WAN Accelerator Server

Hardware

CPU: x86-64 processor. Using multi-core processors improves data processing performance and is highly recommended on WAN links faster than 10 Mbps.

Memory: 8 GB RAM. Using faster memory improves data processing performance.

Disk Space: Disk space requirements depend on the WAN Accelerator role:

Source WAN Accelerator requires 20 GB per 1 TB of source data to store digests of data blocks of source VM disks. Disk space consumption is dynamic and changes as unique VMs are added to (or removed from) to jobs with WAN Acceleration enabled.

Target WAN Accelerator requires global cache size as defined by user (fixed amount). Disk space is reserved immediately upon selecting WAN Accelerators as a target one in any job.

Network: 1 Gbps or faster for on-site backup and replication, and 1 Mbps or faster for off-site backup and replication. High latency and reasonably unstable WAN links are supported.

> **TIP:**
>
> Global cache is not leveraged by source WAN Accelerators, or by WAN accelerators in high-bandwidth mode, so it does not need to be allocated and populated in such cases.

OS

Only 64-bit version of the following operating systems are supported, including Core edition:

- Microsoft Windows Server 2019 (up to 1909 SAC release)
- Microsoft Windows Server 2016 (including all SAC releases)
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1
- Microsoft Windows 10 (version 1607 to 1909)
- Microsoft Windows 8.1
- Microsoft Windows 7 SP1

Backup Enterprise Manager

Hardware

Processor: x86-64 processor.

Memory: 4 GB RAM.

Hard Disk Space: 2 GB for product installation plus sufficient disk space to store guest file system catalog from connected backup servers (according to data retention policy).

Network: 1 Mbps or faster connection to Veeam Backup & Replication servers.

OS

Only 64-bit version of the following operating systems is supported:

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1
- Microsoft Windows 10 (version 1607 to 1909)
- Microsoft Windows 8.1
- Microsoft Windows 7 SP1

Server Software

- Microsoft Internet Information Services 7.5 or later
- Microsoft SQL Server 2008 through 2019 (2016 SP1 Express is included)
- Microsoft .NET Framework 4.7.2 (included in the setup)
- Windows Installer 4.5 (included in the setup)

Client Software

- Firefox, Google Chrome, Microsoft Edge or Microsoft Internet Explorer 11.0 or later. The browser must have JavaScript and WebSocket protocol enabled.
- Microsoft Excel 2003 or later (to view reports exported to Microsoft Excel format).

Backup Target

Backups can be performed to the following disk-based storage:

- Local (internal) storage of the backup repository server.
- Direct Attached Storage (DAS) connected to the backup repository server, including external USB/eSATA drives and raw device mapping (RDM) volumes.
- Storage Area Network (SAN). Backup repository server must be connected into the SAN fabric via hardware or virtual HBA, or software iSCSI initiator.
- Network Attached Storage (NAS) able to present its capacity as NFS share (protocol version 3.0 and 4.1 only) or SMB/CIFS share (any protocol version). Using SMB protocol for non continuously available (CA) file shares is not recommended for reliability reasons. NFS shares are supported both for direct operation, and when mounted to a Linux repository server.
- Dell EMC DataDomain (DD OS version 5.6 or later) with DDBoost license. Both Ethernet and Fibre Channel (FC) connectivity is supported.
- ExaGrid (firmware version 5.0.0 or later).
- HPE StoreOnce (firmware version 3.15.1 or later) with Catalyst license. Both Ethernet and Fibre Channel (FC) connectivity is supported.
- Quantum and OEM partners (DXi software 3.4.0 or later). Supported Quantum DXi systems include DXi4700 (NAS configuration), DXi4700 (multi-protocol configuration), DXi 6900, DXi 6900-S.

Once backups are created, they can be copied (for redundancy) or offloaded (for long-term retention) to one of the following object storage types using scale-out backup repository functionality:

- Amazon S3
- IBM Cloud Object Storage
- Microsoft Azure Blob Storage (including Microsoft Azure Data Box)
- Any S3-compatible object storage (on-premises appliance, or cloud service provider)

Tape

LTO3 or later tape libraries (including VTL) and standalone drives are supported. Tape device must be directly attached to the backup server, to a tape server via SAS, FC or iSCSI interface. Note that VMware does not support connecting tape libraries to ESXi for VM pass-through.

Drivers

- Tape devices without device-specific, vendor-supplied OEM drivers for Windows installed will appear in Windows Device Manager as Unknown or Generic and require enabling native SCSI commands mode.
- If multiple driver installation modes are available for your tape device, use the one that allows for multiple open handles from a host to a drive to exist at the same time. Usually, such drivers are referred to as "non-exclusive".
- No other backup server must be interacting with the tape device.

Storage Snapshot Integrations

Storage snapshot integration is supported for pre-installed plug-ins and additional plug-ins that are available for download at: www.veeam.com/backup-replication-download.html.

Cisco HyperFlex (formerly HX-Series/SpringPath)

- NFS connectivity only
- HyperFlex 2.0 or later
- Basic authentication is not supported for SSO users in HyperFlex starting from version 3.0

DataCore

- Fibre Channel (FC) or iSCSI connectivity
- DataCore SANsymphony 10.0 PSP10 or later

Dell EMC SC Series (formerly Compellent)

- Fibre Channel (FC) or iSCSI connectivity
- Storage Center OS 7.4.2 or later
- FluidFS and Live Volumes are not supported

Dell EMC VNX, VNX2, VNXe and Unity

- NFS, Fibre Channel (FC) or iSCSI connectivity
- Dell EMC VNXe/Unity OE versions 3.x through 5.0

DDN (formerly Western Digital IntelliFlash, Tegile)

- NFS, Fibre Channel (FC) or iSCSI connectivity
- IntelliFlash 3.9.2 or later

Fujitsu ETERNUS AF and DX series

- Fibre Channel (FC) or iSCSI connectivity
- Software version V10L86-0000 or later

HPE Primera, 3PAR StoreServ

- Fibre Channel (FC) or iSCSI connectivity
- 3PAR OS versions 3.1.2 up to 3.3.1 MU3
- iSCSI VLAN tags are supported. Virtual Domains are supported.

HPE Nimble Storage AF-Series, HF-Series and CS-Series

- Fibre Channel (FC) or iSCSI connectivity
- Nimble OS 2.3 and later

HPE StoreVirtual (formerly LeftHand / P4000 series) and StoreVirtual VSA

- iSCSI connectivity only
- LeftHand OS versions 9.5 through 12.7
- HPE SV3200 (LeftHand OS version 13) is not supported

Huawei OceanStor

- NFS, Fibre Channel (FC) or iSCSI connectivity
- Huawei OceanStor V3 and F V3 Series (software version V300R006 and later)
- Huawei OceanStor Dorado V3 Series (software version V300R001 and later)
- Huawei OceanStor V5 and F V5 Series (software version V500R007 and later)
- Huawei OceanStor V6 (software version 6.0 and later)

IBM Spectrum Virtualize (includes IBM Storwize, IBM SVC)

- Fibre Channel (FC) or iSCSI connectivity
- Spectrum Virtualize 7.6 or later

INFINIDAT Infinibox F-series

- NFS, Fibre Channel (FC) or iSCSI connectivity
- InfiniBox version 3.0 and later

Lenovo Storage V series

- Fibre Channel (FC) or iSCSI connectivity
- Spectrum Virtualize 7.6 or later

NetApp SolidFire/HCI

- iSCSI connectivity
- NetApp SolidFire support requires Element OS version 9.0 or later
- NetApp HCI support requires Element OS version 10.0 or later

NetApp FAS/AFF, FlexArray (V-Series), ONTAP Edge/Select/Cloud VSA and IBM N series (FAS OEM)

- NFS, Fibre Channel (FC) or iSCSI connectivity
- Data ONTAP versions from 8.1 up to 9.7
- 7-mode or cDOT (cluster-mode)
- MetroCluster is supported
- ONTAP features application-aware data management and SVM-DR are not supported
- NetApp Synchronous SnapMirror is not supported

Pure Storage FlashArray

- NFS, Fibre Channel (FC) or iSCSI connectivity
- Purity version 4.8 and later
- Purity ActiveCluster is supported

Veeam Explorer for Microsoft Active Directory

Microsoft Active Directory Domain Controllers

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2008

Minimum supported domain and forest functional level is Windows 2008.

Veeam Explorer for Microsoft Exchange

Microsoft Exchange

- Microsoft Exchange 2019
- Microsoft Exchange 2016
- Microsoft Exchange 2013
- Microsoft Exchange 2010 SP1

Software

- Microsoft Outlook 2010 or later (64-bit) for PST exports (optional)

Veeam Explorer for Microsoft SharePoint

Microsoft SharePoint Server

- Microsoft SharePoint 2019
- Microsoft SharePoint 2016
- Microsoft SharePoint 2013
- Microsoft SharePoint 2010

The 3rd-party RBS providers are not supported.

Veeam Explorer for Microsoft SQL Server

Microsoft SQL Server

- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2008
- Microsoft SQL Server 2005 SP4

Veeam Explorer for Oracle

OS

Both 32-bit and 64-bit versions of the following operating systems are supported, according to Oracle Database version compatibility matrix:

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2008
- CentOS 5 or later
- RedHat 5 or later
- Oracle Linux 5 or later
- SUSE Linux Enterprise 15
- SUSE Linux Enterprise 12
- SUSE Linux Enterprise 11

Oracle Database

- Oracle 19
- Oracle 18
- Oracle 12
- Oracle 11

Configuration

- Oracle Automatic Storage Management (optional, requires ASMlib present)

Known Issues

Backup infrastructure

- All registered server names must be resolvable into IPv4 address.
- NETBIOS names of backup servers must be resolvable on Enterprise Manager server.
- Linux servers registered with Veeam Backup & Replication infrastructure must use Password or Certificate-based authentication methods and bash shell.
- VeeamZIP operations do not respect backup repository I/O throttling settings.
- Backup proxy server cannot backup to a CIFS share based backup repository when CIFS share is located on the same server as the backup proxy server. To work around this, create regular Windows based backup repository on the proxy server instead.
- By default, storage infrastructure is rescanned every 10 minutes. Perform the "Rescan Storage" operation manually after storage infrastructure changes, otherwise backup proxies will not "see" the newly added volumes immediately.
- All sensitive information, such as user credentials or encryption keys are stored in the configuration database encrypted with machine-specific private key of backup server. Accordingly, a newly installed backup server will not be able to decrypt such information if attached to the existing database, so any encrypted information will have to be supplied manually. To work around this, use the configuration backup and restore functionality for backup server migrations.
- VM virtual disk file and configuration file names length must not exceed 128 symbols.

VMware

- Debian and Ubuntu based Linux backup proxies require that DNS names of vCenter Server and ESXi hosts are resolvable from the proxy server. Otherwise, jobs will be failing with the "NFC storage connection is unavailable" error.
- Linux backup proxies do not support processing of VMs with virtual disks without ddb.uuid unique IDs. Normally, such disks may only be created by certain P2V/V2V conversion tools.
- Linux backup proxies do not support CBT restores.
- NSX-T networking is not supported for Virtual Labs or Veeam Cloud Connect Replication.
- Virtual backup proxy server cannot be used to backup, replicate or copy itself in virtual appliance (hot add) mode. Jobs configured to do this will automatically failover to Network processing mode. CBT will be disabled for proxy VM.
- Virtual backup proxy server must have VMware Tools installed; otherwise it will be considered as not running, and will never be assigned any tasks.
- For populating replica disks during incremental replication passes and failback, Windows 7 and Windows 8 based backup proxy servers support "network" processing mode only. To work around this, install backup proxy servers on Windows Server OS.
- VMware vStorage API for Data Protection has some limitation preventing hot add process depending on VM configuration. For complete list of hot add limitations, refer to KB1054. With the default proxy settings, should hot add operation fail, the job will failover to the network mode for specific virtual disk.
- Processing of Fault-Tolerant VMs created on vSphere versions prior to vSphere 6 is not supported.
- Hard Disk restore may fail with the "*Restore job failed Error: A specified parameter was not correct: unitNumber*" error when restoring disk to a SCSI controller slot above 15. To work around this, add a paravirtual SCSI controller to the target VM by editing VM virtual hardware settings with vSphere Client.

- Disk mapping functionality is not supported for IDE, SATA and NVMe disks in the Hard Disk Restore wizard.
- Restore and replication of VMs between different ESX(i) versions requires that VM's virtual hardware version is compatible with the target host.
- Restoring VM with non-standard virtual disk layout (such as converted from VMware Workstation or VMware Server) as thin may fail. To work around this issue, restore these disks as thick.
- Instant recovery of non-VMware Linux machines to VMware is not supported for backups of machines with mkinitrd missing, or with mount points outside of /
- Virtual disk placement and type cannot be customized during full VM restore when restoring backups produced by version earlier than 6.1.
- Replication jobs may fail if source or target datastore has special symbols in its name.
- Networkless interaction with Microsoft Windows guests having UAC enabled (Vista or later) requires that Local Administrator (MACHINE\Administrator) or Domain Administrator (DOMAIN\Administrator) account is provided on Guest Processing step.
- Guest customization settings are not backed up and restored for vCloud Director VMs.
- The state of Standalone VM option of vCloud Director is not preserved with the full VM restore.
- Virtual appliance (hot add) processing mode does not support IDE disks. This is by design of VMware hot add functionality, which requires SCSI or SATA adaptors (SATA hot add support requires vSphere 6 or later).
- Direct NFS Access is not supported for VMs with existing snapshot, when VMware quiescence is enabled, or when Kerberos authentication is enabled on a storage device.
- Due to a change in ESXi 6.0 Update 1, replication and quick migration to VVol datastores is not possible with either Veeam or vSphere replication.
- RDM disks in virtual compatibility mode are skipped during Backup from Storage Snapshot.
- Pre-freeze and post-thaw scripts for Linux do not perform elevation to root (sudo) when networkless processing (VIX) is used.

VMware Cloud on AWS

- Only hot add transport mode is supported due to API limitation.
- All vPower NFS based functionality is not supported due to platform limitation.
- Networkless guest interaction is not supported due to API limitation.
- Re-IP addressing and file level recovery for replicas are not supported.
- Only cold switch is supported for Quick Migration.

Hyper-V 2016/2019

- Application-aware processing of VMs with Windows guest OS other than Windows Server 2016 and Windows 10 fails with the "Failed to take in-guest VSS snapshot COM error: Code: 0x80042308" error. This is a known Hyper-V 2016 compatibility issue that is fixed by updating Hyper-V integration components on the affected guests with KB3063109.
- Application-aware processing of Active Directory domain controllers running on guest OS other than Windows Server 2016 fails with the "*Failed to create VM recovery checkpoint*" error (32770). To resolve this issue, make sure the latest Windows Updates are installed for guest OS on the affected VMs.
- Backing up VMs from Hyper-V cluster in rolling upgrade is supported, however RCT will not be leveraged until the upgrade is completed for all nodes and cluster functional level is upgraded to

Windows Server 2016 or later. Keep in mind that VMs virtual hardware version must be upgraded to version 8.0 before RCT can be leveraged on the VM.

- Virtual machines with VMPmemController virtual hardware are skipped from processing due to a Hyper-V limitation around checkpointing of such VMs. Additionally, presence of such machines may cause restore operations to the same Hyper-V host to hang on Hyper-V 2016 versions earlier than 1803 SAC release due to a bug in Microsoft Hyper-V VSS Writer.
- VMs with pass-through virtual disks cannot be processed due to Hyper-V 2016 and later checkpoints limitation.

Hyper-V

- Virtual disks consisting of multiple files (such as from virtual machines originally created on Virtual Server 2005) are not supported for processing.
- CPU Type SCVMM parameter is not backed up and restored on Hyper-V VMs.
- When replicating from older to newer Hyper-V host version, failback is only supported to the original location if the original VM still exists.
- Backup of VMs with virtual disks located both on local and shared CSV/SMB storage is not supported due to Hyper-V limitation.
- Deleting Hyper-V replica from disk does not delete the replica VM from SCVMM.
- Offhost backup from deduplicated volume fails if the Data Deduplication feature is disabled on backup proxy server.
- Shared VHDX virtual disks can be backed up in crash-consistent mode only.
- Transaction log backup for Microsoft SQL Cluster running on shared VHDX is not supported due to a Microsoft limitation (no VSS support for Shared VHDX).
- Restoring a VM into the root folder of SMB share fails. To work around the issue, restore VM into a subfolder instead.

NAS Backup

- When files are backed up directly from Windows server, NTFS sparse files are handled as regular files, and thus are inflated during the restore.
- When files are backed up directly from Linux servers, maximum full file path length is limited to 4096.
- Symlinks within Linux-based SMB shares are not supported, and prevent the backups job from executing correctly.
- File filter dialog label incorrectly limits the include and exclude functionality to files and file masks only, however it is also supported to specify full folder paths as exclude filters.
- Force removal of SOBR extent (without backup evacuation) requires running the health check on impacted backups twice: after removing the extent, and after running the backup job for the first time.

Agent Management

- All protect computers names must be resolvable into IPv4 address.
- Universal and Domain local groups are not supported as containers for Microsoft Active Directory based protection groups. Use Global groups instead.
- Processing rate for agent backup jobs may show incorrect values (much higher than actual).
- On rare occasions, machines in Active Directory based Protection Group type may no respect an option to be automatically excluded after 30 days of being offline.

- When deleting the backup chain from disk GFS restore points are removed even if the option to keep those restore point has been selected.

Microsoft Windows Server Failover Cluster

- Workgroup clusters, multi-domain clusters and mixed OS version clusters are not supported for agent-based backup.
- Only failover clusters with shared disks are supported, CSV (Cluster Shared Volume) based clusters are not currently supported for agent-based backup.
- SQL Server AlwaysON Clusterless Availability Groups, and Availability Groups based on multiple SQL Server Failover Clusters are not supported for agent-based backup.
- NetBIOS and DNS names for all failover cluster nodes must be resolvable from the backup server.
- Failover clusters with the same NETBIOS names is not supported even when they are joined different domains.
- Adding a new node into the failover cluster will result in full backup performed for all shared disks.
- Bare Metal Recovery restore is not supported for shared disks. Such disks will be filtered out and not displayed in the corresponding wizard. To restore the content of such disks, use volume-level recovery or disk export functionality.
- Instant Restore to Hyper-V automatically skips clustered volumes during recovery.

Direct Restore to Amazon EC2

- Direct restore of disks larger than 5TB requires using proxy appliance, otherwise restore will fail with the "Object is too large" error.

Direct Restore to Microsoft Azure and Azure Stack

- Certain Linux computer configurations may require Azure VM configuration to be adjusted upon restore to Microsoft Azure. If your VM fails to boot, please contact Veeam Support for assistance.
- VM name, VM group name and VM size are not validated for compatibility with Microsoft Azure naming policy and storage account type and may cause the restore to fail.
- Microsoft Azure Stack subscription limits are not validated before the restore.

Secure Restore

- Microsoft Windows Defender does not support the option to stop antivirus scan after the first virus has been found, so the entire volume will always be scanned.

Windows File Level Restore

- Under rare unknown circumstances, file-level restore from ReFS 3.1 or later volumes may cause some Windows Server 2019 (or Windows 10 1809 or later) mount servers to BSOD, or FLR session to hang. The same applies to replica VM re-IP functionality for VMs with ReFS volumes. To work around this issue, create *ForceVhdMount* (DWORD) = 1 registry value under the *HKLM\SOFTWARE\Veeam\Veeam Backup and Replication* key on the backup server.
- File level restore may fail if a VM you are restoring from was lacking free disk space at the time of backup.
- Storage Spaces volumes are not supported for file level recovery. Consider using Instant VM Recovery to recover guest files from such VMs. Note that Microsoft does not support Storage Spaces within a VM.
- To restore files from deduplicated volumes, mount server and backup console must be installed on Windows Server with Data Deduplication feature enabled, and Windows Server version must be the

same or greater than one of the VM you are restoring from. Otherwise, deduplication driver incompatibility will cause file level recovery errors with false data corruption reports.

Multi-OS File Level Restore

- Legacy Logical Volume Manager version 1 (LVM1) volumes are not supported.
- Encrypted LVM volumes are not supported.
- Spanned, striped, mirrored and RAID-5 Windows dynamic disks are not supported. To work around, use Windows File Level Restore instead.
- Non-standard file system configurations support is limited (for example, configurations when file system journal is located on another volume, separately from actual file system are only supported for ext3 file system, but not for other file systems).
- Restoring files to the original location for Windows VMs is not supported. To work around, use Windows FLR instead.

Guest File System Indexing

- File ownership data is not collected for files on non-NTFS volumes.
- File ownership data is not collected for guest files of Hyper-V VMs.

Replica Failover

- Starting a replicated VM using means other than the product's user interface (including vSphere Client, Hyper-V Manager, SCVMM, PowerShell) disables advanced replication functionality such as Re-IP and failback.

Configuration backup and restore

- Under certain circumstances, some encrypted backups may get disconnected from the corresponding job and appear as Imported. To work around, use backup mapping functionality to reconnect the job to backup files.
- Immediately after configuration restore, Enterprise Manager may show duplicate jobs, and some jobs may be missing. The issue will go away by itself after some time.

Enterprise Manager

- Saving newly created or edited self-service portal tenant quotas to 9.5 Update 4 backup servers from Enterprise Manager 10 appears to hang, and eventually times out. However, in reality new quota settings will be saved correctly and immediately.
- Reverse DNS lookup on Enterprise Manager server must be functional for setting up self-service recovery delegation scope.
- The presence of .NET 3.5.1 WCF HTTP Activation Windows component prevents Enterprise Manager from functioning. To work around the issue, uninstall this component.

SureBackup

- After upgrading from Update 3a or earlier, SureBackup jobs for Hyper-V VMs will no longer work with Virtual Labs created prior to the upgrade. To work around this issue, click through Edit Virtual Lab wizard on the existing Virtual Labs.
- Automatic virtual lab configuration is not supported for networks with non-private network addresses.
- Automatic virtual lab networking configuration process may fail with the "*Unable to resolve default network settings*" error. To work around this issue, go back in the wizard and try again.

- Automatic virtual lab networking configuration may fail in some case when DVS are present in virtual environment. In such cases, use advanced configuration mode to configure virtual lab networking manually.
- SureBackup job fails on VM with unsupported or excluded virtual disks which were not explicitly set to be removed from configuration (as a part of disk exclusion settings in the backup job), because test VM cannot find its disks and is unable to start.
- Automatic physical mode RDM disk exclusion in the backup job may lead to situation when test VM is able to connect RDM disk, and produce irreversible changes on the disk. To avoid this, always exclude physical RDM disk from backup job explicitly, selecting the option to remove the excluded disks from configuration.
- Some antivirus applications are known to cause BSOD on backup repository server when SureBackup job is started. To prevent this, exclude backup folders from monitoring.

Cloud Connect Backup

- Microsoft SQL Server and Oracle transaction log backup to a cloud repository is not supported. However, Backup Copy jobs in the immediate copy mode are supported for copying transaction logs backups to a cloud repository.

Cloud Connect Replication

- Cloud replicas status is not refreshed in real-time, but rather periodically. You can press F5 to retrieve the most current state.
- vApp-level networks are not supported for network mapping functionality (only org-level networks).
- For non-Windows VMs, guest network settings cannot be detected automatically. Because of that, network mapping in the replication job wizard must be performed manually. Additionally, if you are replicating non-Windows VMs only, you need to manually specify the default gateways for each production network using Manage Default Gateways dialog on the Service providers node of the Backup infrastructure tab of the management tree.
- Network extension functionality requires static IP addresses assigned on the processed VMs. Dynamic IP addressing via DHCP is not supported, and DHCP must be disabled.
- Failover plans session cannot be viewed once failover has been performed.
- Enabling VM auto import in vCloud Director settings may impact replication functionality.
- Using move functionality of vCloud Director to move cloud replicas may cause virtual disk loss.
- Remote Console and Remote Desktop functionality is not supported for vCloud Director based tenants.

Backup Copy

- Backup Copy job in the immediate copy mode processes only the latest backup files chain. To make such jobs copy all existing backups, create *BackupCopyMirrorAll* (REG_MULTI_SZ) registry value under the *HKLM\SOFTWARE\Veeam\Veeam Backup and Replication* key on the backup server. This value should be populated with Backup Copy job names.

Object Storage

- When enabling Object Lock on an S3 bucket, use "None" option for the object lock configuration mode. Otherwise, you will not be able to register the bucket with Veeam. Note that we will automatically use Compliance object lock mode for each uploaded object.
- Using immutability feature with the existing S3 bucket containing backups created by 9.5 Update 4 requires that both Versioning and Object Lock are enabled on the bucket at the same time, before the

immutability feature is enabled. Any other approach will lead to backup offload failures and inability to correctly interact with backups in the bucket.
- Data in object storage bucket/container must be managed solely by Veeam, including retention and data management. Enabling lifecycle rules is not supported, and may result in backup and restore failures.

Tape

- Direct restore from tape is supported from backups created by version 9.0 or later.
- File to Tape job fails building a list of files to process, if catalog contains files with certain Unicode symbols.
- Backup to Tape job will perform full backup during each run if the source forever forward incremental backup job, or backup copy job in the immediate copy mode has retention of less than 3 restore points, or if the source backup copy job in the periodic copy mode has retention of less than 4 restore points.
- SQL transaction log backup to tape is not supported.
- If you manage several tape libraries with the same Veeam backup server and use barcodes to identify tapes in these libraries, all barcodes must be unique across all tape libraries.

Veeam Explorer for Microsoft Exchange

- Restoring public folder items from system "In-Place Hold Items" folder to original location restores them to the newly created folder with the same name, instead of actual system folder.

Veeam Explorer for Oracle

- Database export functionality may fail for databases large than 1TB in size due to SSH command limit. If you have such databases in your environment, please contact support to enable the work around.
- Database restore may fail if backed up Oracle server version and target server version have different patch levels.
- Database restore for Oracle Data Guard with tnsnames.ora and listener.ora located in non-default paths is not supported.
- Oracle Real Application Clusters (RAC) and Oracle Data Guard deployments with snapshot standby option enabled are not supported with OCI-based integration. To work around this issue, use Veeam Plug-in for Oracle RMAN.
- Restore from imported Veeam Plug-in for Oracle RMAN backups is not supported.
- Oracle XE on Linux is not supported.
- 32-bit Oracle application running on 64-bit operating systems is not supported.
- Configuration with multiple Oracle versions on the same machine is not supported.
- ASM-based Oracle deployments running in virtual machines with Open-VM-Tools installed is not supported.

Veeam Explorer for Microsoft SharePoint

- Modified By field of restored documents is updated with the account performing restore.
- Restored Issue list items are assigned new Issue ID.
- Restore of Time Card list is not supported.
- Versioning settings of SharePoint lists are not preserved on restore.
- Restoring Generic List and Pages Library may fail with the "*No content type 'XXX' found in web YYY*" error.
- Importing Picture Library export may result in IDs changed for some items.

- Importing Project Tasks list export does not preserve column order.
- Importing SharePoint list export does not preserve Validation Settings.
- Some Rating Settings of Discussion lists values are not restored.

Veeam Explorer for Microsoft SQL Server

- Point in time restore with fine tuning requires that all nodes of the same AlwaysOn availability group are located in the same time zone.
- Transaction log backup requires that at least one image-level backup of SQL Server VM is performed. This particularly means that transaction log backup will not function after full SQL Server VM restore is performed, or for newly appearing databases, until first image-level VM backup is performed.
- Transaction log backups is not supported for Windows Server 2008 or earlier guests on Hyper-V 2012 R2.
- SQL Server 2017 Graph Tables are not currently supported.

Veeam Explorer for Storage Snapshots

- VMs with virtual disk files located on different storage volumes are supported only for snapshots created by Veeam Backup & Replication 9.5 Update 4 or later jobs. For other storage snapshots, only disks residing on the same datastore with the VMX file will be available for all restore types.
- Storage snapshots and volumes with name starting with "VeeamAUX_" are automatically excluded from processing.

Cisco HyperFlex

- Scenarios where several Cisco HyperFlex systems are registered under different VMware vCenter Servers are not currently supported. It is recommended to back up VMs of each VMware vCenter Server instance using a separate Veeam backup server.

Dell EMC VNX(e)

- Legacy SnapView snapshot technology is not supported in favor of VNX Snapshot.
- Concurrent operations from the same LUN (such as backup and restore) is not supported due to EMC VNXe limitation.

IBM SVC and StorWize

- Storage snapshots created by backup jobs with versions prior to 9.5 Update 4a will be skipped by the retention policy, and have to be removed manually.

NetApp ONTAP

- Infinite volumes are not supported.
- vFiler DR units are not supported, and are automatically hidden by the UI.
- Configurations with VM stored on a non-default vFiler based on qtree (instead of volume) is not supported.

Globalization

- Non-ASCII characters are not supported in the: product's installation path; source or destination path of SSH-enabled file copy operations; VM file and folder names for multi-OS file level recovery to the original location.

- Some user interface (UI) controls may appear misplaced when non-standard diplay's DPI setting is set. To work around the issue, change DPI setting to 100% or 125% using Display settings of the Windows Control Panel.

User Interface

- Job filter functionality includes unmanaged Windows and Linux agent jobs under both Server and Workstation workload types.

PowerShell

- Restores from imported backups residing on a CIFS share are not supported through PowerShell.

Upgrade

- First Hyper-V backup and replication job run after upgrade will not use the changed block tracking information, and thus may take longer than expected (applies to Windows Server Hyper-V 2008 R2 – 2012 R2).

Installing Veeam Backup & Replication

Veeam Backup & Replication Server

To install Veeam Backup & Replication 10 server and management console:

1. Download the latest version of Veeam Backup & Replication ISO from: veeam.com/backup-replication-download.html.
2. Mount the product ISO and use autorun, or run the *Setup.exe* file.
3. Click the Veeam Backup & Replication tile.
4. Accept the terms of Veeam Backup & Replication and 3rd party components license agreements to install the product. You can find a copy at veeam.com/eula.html
5. Provide setup program with your license file.
6. Review the default installation settings. To change the defaults, select the **Let me specify different settings** and go through additional wizard steps.
7. Click **Install** to start the installation and follow the setup wizard steps.
8. Once the installation is complete, download and install the latest available update from veeam.com/updates.html.
9. Launch the Veeam Backup product by clicking the **Veeam Backup & Replication** product icon on your desktop, and specifying localhost as the backup server.

Veeam Backup Enterprise Manager

If you want to manage one or more Veeam Backup servers with centralized management web UI, install Veeam Backup Enterprise Manager. You only need one Enterprise Manager installation per environment.

To install Veeam Backup Enterprise Manager:

1. Mount the product ISO and use autorun, or run the *Setup.exe* file.
2. Click the Veeam Backup Enterprise Manager tile.
3. Accept the terms of License Agreement to install the product.
4. Provide setup program with your license file.
5. Review the default installation settings. To change the defaults, select the **Let me specify different settings** and go through additional wizard steps.
6. Click **Install** to start the installation and follow the setup wizard steps.
7. Once the installation is complete, download and install the latest available update from veeam.com/updates.html
8. Once the installation is complete, access the Veeam Backup Enterprise Manager web UI by clicking the **Veeam Backup Enterprise Manager** product icon on your desktop.

Uninstalling Veeam Backup & Replication

1. From the Start menu, select **Control Panel > Add or Remove Programs**.
2. In the programs list, select **Veeam Backup & Replication** and click the **Remove** button.
3. In the programs list, select and remove any additional remaining Veeam components.

Upgrading Veeam Backup & Replication

Veeam Backup & Replication 10 supports automated in-place upgrade from version 9.5 Update 3 or later which preserves all products settings and configuration. To upgrade from earlier versions, please contact our Customer Support.

Upgrade checklist:

1. Review the Licensing section of the What's New in Veeam Backup & Replication 10 document for any changes that may affect you and consider postponing the upgrade until they are resolved.
2. Are you using an Instance license to protect some of your vSphere or Hyper-V VMs with agent-based backup jobs in presence of a Socket license? As an enforcement of the existing licensing policy, hosts where such VMs are running will require and consume Socket licenses with v10. This may result in your agent-based backup jobs failing after the upgrade due to insufficient Socket licenses.
3. Are you using Veeam Availability for Nutanix AHV 1.0? Veeam Backup & Replication 10 is not compatible with this version. Please wait until Veeam Availability for Nutanix AHV 2.0 is generally available before upgrading.
4. Are you using Veeam Availability Orchestrator 1.0 or 2.0 ? Veeam Backup & Replication 10 is not compatible with these versions. Please wait until Veeam Availability Orchestrator 3.0 is generally available before upgrading.
5. v10 uses the new license file format. The setup wizard will offer to download your v10 license automatically. This requires uploading your currently installed license to Veeam servers. If your backup server has no Internet connection, or if you prefer not to have your license uploaded, or in case of license upgrade issues – please download your v10 license from the Veeam Customer Portal manually. Note that you must have an active maintenance agreement at the time when you access the portal.
6. Are you using Veeam Backup Enterprise Manager? If yes, start the upgrade procedure from this component. Note that Enterprise Manager 10 supports backup servers version 9.5 Update 3 or later, so you can potentially run both old and new versions of backup server side by side, if required.
7. Are you using Veeam ONE to monitor your backup infrastructure? If yes, upgrade it next. Veeam ONE 10 supports monitoring of backup servers with version 9.5 Update 3 or later.
8. Is the backup server to be upgraded installed on the supported operating system? If not, you must migrate the server to the supported OS first, before performing the upgrade. Refer to the Veeam support KB article KB1803 for more information on how to perform such migration.
9. Are you using Cloud Connect? If yes, check with your Cloud Connect service provider if they have already upgraded their system to at least the version you are upgrading to.
10. Ensure there is no active processes, such as any running jobs and restore sessions. We recommend that you do not stop running jobs and let them complete successfully instead. Disable any periodic and Backup Copy jobs, so that they do not start during the upgrade.

Veeam Backup Enterprise Manager

To perform upgrade of Veeam Backup Enterprise Manager to version 10, you must be running version 9.5 Update 3 or later on the supported operating system (refer to the System Requirements section of this document). To upgrade from previous versions, contact Veeam Technical Support.

1. Perform a backup of the corresponding SQL Server configuration databases used by Enterprise Manager server, so that you can go back to previous version in case of issues with the upgrade.
2. Mount the product ISO and use autorun, or run the *Setup.exe* file.
3. Click the Veeam Backup Enterprise Manager tile.
4. Follow the setup wizard steps as outlined in the installation procedure above. Be sure to select the same SQL database and instance that was used by the previous Veeam Backup Enterprise Manager version.
5. If you have Veeam Backup & Replication server installed on the server, upgrade it immediately after completing the upgrade of Veeam Backup Enterprise Manager server, otherwise this local backup server will not be able to run jobs.
6. Once the installation is complete, download and install the latest available update from veeam.com/updates.html.

Please note that immediately after upgrade, Enterprise Manager performance may be impacted due to configuration database being optimized by the maintenance job. This can take up to an hour depending on the database size.

Veeam Backup & Replication Server

To perform upgrade of Veeam Backup & Replication server to version 10, you must be running version 9.5 Update 3 on the supported operating system (refer to the System Requirements section of this document). To upgrade from previous versions, contact Veeam Technical Support.

1. Download the latest version of Veeam Backup & Replication ISO from: veeam.com/backup-replication-download.html.
2. Ensure there is no active processes, such as any running jobs and restore sessions. We recommend that you do not stop running jobs and let them complete successfully instead. Disable any periodic and Backup Copy jobs, so that they do not start during the upgrade.
3. Perform a backup of the corresponding SQL Server configuration databases used by the backup server, so that you can easily go back to previous version in case of issues with the upgrade. You can also use built-in configuration backup functionality.
4. Mount the product ISO and use autorun, or run the *Setup.exe* file.
5. Click the Veeam Backup & Replication tile.
6. Follow the upgrade wizard steps as outlined in the installation procedure above. Be sure to select the same SQL database and instance that was used by the previous product version.
7. If you are using remote backup consoles, upgrade them manually using the product ISO file. Unfortunately, automatic upgrade is not supported this time due to the major version number change.
8. Download and install the latest available update from veeam.com/updates.html.
9. Open the Veeam Backup & Replication user interface. If necessary, the automated upgrade wizard will automatically appear, prompting you to upgrade product components running on remote servers. Follow the wizard to complete the upgrade process.
10. If some remote servers are unavailable at the time of upgrade, you can run the Upgrade wizard at any time later from the main product menu. Note that out-of-date product components cannot be used by jobs until they are updated to the backup server version.

11. If you are using Virtual Labs functionality, please open each Virtual Lab settings, and click through the wizard to redeploy each virtual lab with the new proxy appliance version.
12. Enable any scheduled jobs that you have disabled before the upgrade.

Please note that immediately after upgrade, backup server performance may be impacted due to configuration database being optimized by the maintenance job. This can take up to an hour depending on the database size.

Licensing

Veeam Backup & Replication can be licensed per protected workload, or per CPU Socket of underlying hypervisor host (for vSphere or Hyper-V VMs protection only). For more information, see Veeam Licensing Policy at veeam.com/licensing-policy.html

The trial license key is sent to you automatically after downloading the product. The trial license is valid for 30 days from that moment, and includes Basic technical support.

To obtain a full license key, please refer to veeam.com/buy-veeam-products-pricing.html

Subscription licenses include maintenance plan with Premium support. The perpetual license includes a one-year maintenance plan with Basic support. To renew or upgrade your maintenance plan, please contact Veeam Renewals at veeam.com/renewal.html

Updating Veeam Backup & Replication License

Veeam Backup & Replication server license is managed centrally by Enterprise Manager server. If you are using Enterprise Manager, do not update license on individual backup servers directly, as Enterprise Manager will force its license to all connected backup servers.

To install the new license file to a backup server connected to Enterprise Manager server:

1. Open **Configuration > Licensing** tab in Enterprise Manager UI, and click **Install License.**
2. Browse to the license file (**.lic**) that was sent to you after registration to install the license. To learn more, see the Licensing section.
3. The provided license file will be automatically propagated and applied to all Veeam Backup servers connected to this Enterprise Manager server.

To install the new license file to a standalone backup server that is not managed by Enterprise Manager server:

1. Select **License** from the main menu.
2. Click the **Install** license button to browse to the license file (**.lic**) that was sent to you after registration to install the license. To learn more, see the Licensing section.

Technical Documentation References

If you have any questions about Veeam Backup & Replication, you may use the following resources:

- Product web page: www.veeam.com/vm-backup-recovery-replication-software.html
- User guides: www.veeam.com/documentation-guides-datasheets.html
- Community forums: www.veeam.com/forums

To view the product help, press the **F1** key or select **Help > Online Help** from the main menu.

Technical Support

We offer email and phone technical support for customers with active maintenance agreement and during the official evaluation period. For better experience, please provide the following when contacting our technical support:

- Version information for the product and all infrastructure components.
- Error message and/or accurate description of the problem you are having.
- Log files. To export the log files, select **Help > Support Information** from the main menu, and follow the wizard to export the relevant set of log files.

To submit your support ticket or obtain additional information, please visit veeam.com/support.html.

> **TIP:**
>
> Before contacting technical support, consider searching for a resolution on Veeam Community Forums at veeam.com/forums

Contacting Veeam Software

At Veeam Software, we pay close attention to comments from our customers — and make it our mission to listen to your input, and to build our products with your suggestions in mind. We encourage all customers to join Veeam Community Forums at veeam.com/forums and share their feedback directly with the R&D team.

Should you have a technical or licensing issue or question, please feel free to contact our Customer Support organization directly. We have qualified technical and customer support staff available 24 hours a day, 7 days a week who will help you with any inquiry that you may have.

Customer Support

For the most up to date information about our support practices, business hours and contact details, please visit veeam.com/support.html. You can also use this page to submit a support ticket and download the support policy guide.

Company Contacts

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