

Veeam Service Provider Console 7 Release Notes

This document provides last-minute information about Veeam Service Provider Console version 7, including system requirements and installation, as well as relevant information on technical support, documentation, online resources, and so on.

The release version of Veeam Service Provider Console 7 is available starting from January 30th, 2023.

See next:

- [System Requirements](#)
- [Sizing and Deployment Recommendations](#)
- [Installing Veeam Service Provider Console](#)
- [Uninstalling Veeam Service Provider Console](#)
- [Upgrading Veeam Service Provider Console](#)
- [Known Issues in Veeam Service Provider Console](#)
- [Licensing](#)
- [Contacting Veeam Software](#)

System Requirements

Unless otherwise stated, all 3rd party software must be at the latest update and patch level.

Veeam Service Provider Console

Hardware

- *CPU*: modern x64 processor (minimum 4 cores)
- *Memory*: 8GB RAM (recommended)

Network

- 1 Mbit/s

OS

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

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows 11
- Microsoft Windows 10 (starting from version 1909)
- Microsoft Windows 10 LTSC versions (1507, 1607, 1809)

NOTE:

You cannot install Veeam Service Provider Console on a machine running Microsoft Windows Server Core.

Software

- Microsoft SQL Server 2022/2019 CU4*/2017/2016/2014/2012 (SQL Server Express 2017 is included in the setup)
- Microsoft SQL Server 2012 Native Client (included in the setup)
- Microsoft SQL Server 2014 System CLR Types (included in the setup)
- Microsoft .NET Framework 4.7.2 (included in the setup)
- Microsoft Internet Information Services (IIS) 7.0 or later
- Windows Installer 5.0
- Microsoft ASP.NET Core 3.1.21 (included in the setup)
- Microsoft Visual C++ 2015 Redistributable Update 3 (included in the setup)
- Microsoft PowerShell 5 or later
- Microsoft Edge (latest version), Mozilla Firefox (latest version), Google Chrome (latest version)
- Microsoft Report Viewer 2015 (included in the setup)
- PDF viewer for viewing reports

*Microsoft SQL Server 2019 requires Cumulative Update package 4 (CU4). For details, see [this Microsoft KB article](#).

Veeam Cloud Connect

Platforms

- Veeam Backup & Replication
- VMware Cloud Director

Infrastructure

- Veeam Backup & Replication 12 (recommended)
- Veeam Backup & Replication 11a
- Veeam Backup & Replication 11
- VMware Cloud Director 10.x (up to 10.4)

Software

- Microsoft PowerShell 5 or later version

Plugins and Integrations

Veeam Service Provider Console integrates with the following Veeam and 3rd party products:

Platforms

- VCSP Pulse
- Veeam Backup & Replication
- Veeam Agent *for Microsoft Windows*
- Veeam Agent *for Linux*
- Veeam Agent *for Mac*
- Veeam Backup *for Microsoft 365*
- Veeam ONE
- ConnectWise Automate
- ConnectWise Manage
- Grafana

Infrastructure

- Veeam Backup & Replication 12 (recommended)
- Veeam Backup & Replication 11a
- Veeam Backup & Replication 11
- Veeam Backup & Replication 10a
- Veeam Agent for Microsoft Windows 6 (recommended)
- Veeam Agent for Microsoft Windows 5
- Veeam Agent for Linux 6 (recommended)
- Veeam Agent for Linux 5
- Veeam Agent for Mac 2 (recommended)
- Veeam Agent for Mac
- Veeam Backup for AWS 6 using Veeam Backup & Replication plugin (recommended)
- Veeam Backup for AWS 5a using Veeam Backup & Replication plugin
- Veeam Backup for AWS 5 using Veeam Backup & Replication plugin

- Veeam Backup for AWS 4 using Veeam Backup & Replication plugin
- Veeam Backup for Microsoft Azure 5 using Veeam Backup & Replication plugin (recommended)
- Veeam Backup for Microsoft Azure 4 using Veeam Backup & Replication plugin
- Veeam Backup for Microsoft Azure 3 using Veeam Backup & Replication plugin
- Veeam Backup for Google Cloud 4 using Veeam Backup & Replication plugin (recommended)
- Veeam Backup for Nutanix AHV 4 using Veeam Backup & Replication plugin (recommended)
- Veeam Backup for Nutanix AHV 3 using Veeam Backup & Replication plugin
- Veeam Backup for Nutanix AHV 2.x using Veeam Backup & Replication plugin
- Veeam Backup for Microsoft 365 version 7 (recommended)
- Veeam Backup for Microsoft 365 version 6
- Veeam ONE 12
- Veeam ONE 11a
- ConnectWise Automate v7 or later
- ConnectWise Manage 2020.1 or later
- Grafana 6.5 or later

Veeam Management Agents

Machines running Veeam Service Provider Console management agents must meet the following requirements:

Hardware

- *CPU*: x86-64 processor architecture
- *Memory*: 2 GB RAM*

*memory sizing depends on managed products and managed workloads. See sizing recommendations in the [Deployment Guide](#) for more information.

Network

- 64 kbit/s when managing Veeam Agent *for Microsoft Windows*, Veeam Agent *for Linux*, Veeam Agent *for MAC*
- 128 kbit/s when managing Veeam Backup & Replication, Veeam ONE, Veeam Backup for Microsoft 365

Windows OS

Both 64-bit and 32-bit (where applicable) versions of the following operating systems are supported except Server Core installations for server OS:

- Microsoft Windows Server 2022
- 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 11
- Microsoft Windows 10 (starting from version 1909)
- Microsoft Windows 10 LTSC versions (1507, 1607, 1809)
- Microsoft Windows 8.1

- Microsoft Windows 7 SP1

Linux OS

Linux kernel versions 2.6.32 – 6.1 are supported if you use kernels supplied by your distribution.

Both 64-bit and 32-bit (where applicable) versions of the following operating systems are supported:

- Debian 10.13 – 11.x
- Ubuntu 16.04, 18.04, 20.04, 22.04, 22.10
- RHEL 6.3 – 9.1
- CentOS 7.x
- Oracle Linux 6.0 – 9.1 (RHCK)
- Oracle Linux 6 (starting from UEK R2) – Oracle Linux 9.1 (up to kernel version 5.15.0 – 6.80.3.1.el9uek)
- SLES 12 SP4, 12 SP5, 15 SP1 – SP4
- SLES for SAP 12 SP4, 12 SP5, 15 SP1 – 15 SP4
- Fedora 36, 37
- openSUSE Leap 15.3 – 15.4
- openSUSE Tumbleweed (experimental support)

Consider the following limitations:

- Linux kernel version 2.6.32 or later is supported as long as you use kernels supplied by your distribution.
- Fedora and openSUSE Tumbleweed are supported up to kernel 6.1.
- Linux kernel 2.6.32 - 754.6.3 in CentOS / RHEL and Oracle Linux (RHCK) is not supported.
- Automatic deployment from the Veeam Service Provider Console is not supported for the following distributions:
 - Fedora 36, 37
 - openSUSE Tumbleweed.

macOS

- Monterey 12.6.X
- Big Sur 11.7.X
- Catalina 10.15.X
- Mojave 10.14.X
- High Sierra 10.13.6
- Ventura 13.0.1

Software

- Microsoft .NET Framework 4.6 or later (Windows computers)

Managed Computers

Network

For remote network discovery rules based on the IP range option, discovered computers must have the following firewall rules enabled:

- File and Printer Sharing (SMB-In), TCP port 445
- Windows Management Instrumentation (WMI-In)

- Remote Scheduled Tasks Management (RPC and RPC-EPMAP). Incoming. TCP, RPC Dynamic Ports firewall rule
- TCP port 6180 (required for establishing the connection with cloud gateways)
- TCP port 22 (required for establishing the SSH connection with computers running Linux OS)

Software

- Veeam management agent

Sizing and Deployment Recommendations

Check the [Deployment Guide](#) document for achieving maximum performance of Veeam Service Provider Console in large-scale distributed environments.

The recommended deployment configuration can be equally used for POC deployments and deployments in production.

Installing Veeam Service Provider Console

To install Veeam Service Provider Console server and Web UI:

1. Download the latest version of Veeam Service Provider Console ISO from <https://www.veeam.com/service-provider-availability-console.html>.
2. Mount the product ISO and use autorun or run the *Setup.exe* file.

Follow the installation procedure as described in [Veeam Service Provider Console Deployment Guide](#).

Uninstalling Veeam Service Provider Console

1. From the **Start** menu, select **Control Panel > Add or Remove Programs**.
2. In the programs list, select Veeam Service Provider Console and its components and click the **Remove** button.

For details on the uninstallation procedure, see [Veeam Service Provider Console Deployment Guide](#), section *Uninstalling Veeam Service Provider Console*.

Upgrading Veeam Service Provider Console

Veeam Service Provider Console version 7 supports automated in-place upgrade from version 6 that preserves all product settings and configuration.

Upgrade checklist:

1. Make sure all active Veeam Service Provider Console web UI sessions are closed before starting the update procedure.
2. Perform a backup of the SQL Server configuration database used by Veeam Service Provider Console, so that you can quickly go back to the previous version in case of issues with the update.

For a step-by-step update procedure, see [Veeam Service Provider Console Deployment Guide](#), section *Updating Veeam Service Provider Console*.

NOTE:

If you are running Veeam Service Provider Console 5 and would like to upgrade your installation to version 7, please follow these steps:

1. Upgrade your Veeam Service Provider Console server to version 6.
2. Update all management agents to version 6. The update procedure is initiated automatically upon the VSPC server upgrade.
3. Make sure all management agents are updated, and only then upgrade your VSPC server to version 7.

Known Issues in Veeam Service Provider Console

General

- Special characters are not supported in user login names.
- Selecting multiple data rows using *Shift+Click* operation is not supported.
- Logging in to the VSPC web site with domain user credentials is not supported when there is a managed company with the same name as the user's domain.
- Microsoft SQL Server with case sensitive collation is not supported.
- Veeam Backup & Replication servers using IP v6 are not supported by the backup portal.
- Site administrators do not have access to hosted Veeam Backup for Microsoft 365 servers data which includes protected data and managed jobs.

Security

- When updating a self-signed security certificate for the Veeam Service Provider Console server, you must manually reaccept the connection on all management agents. To resolve this, use trusted security certificates only.

Single Sign-On (SSO)

- Users that have the ";" character in the location name cannot be authenticated to the backup portal.

Veeam Agent *for Microsoft Windows* Integration

- Agent deployed using 3rd party applications is removed from all views after revoking the agent's license key or uninstalling the agent. To start managing this agent again, reinstall the management agent on the remote computer and register it in the backup portal.
- After enabling or disabling usage of wake-up timers in the backup agent settings, the target computer must be restarted to apply these changes.
- Changing tenant name under which backup agent is sending backups to a cloud repository or destination target leads to losing information about available restore points stored in the repository.
- If you configure a backup job with excluded volumes using the VSPC web UI and then edit this job using backup agent UI (running in the Full Admin Access mode), the excluded volumes selection will be discarded. To resolve that, reapply the backup policy in the VSPC web UI or run backup agents in the Read-only UI mode.
- Backup jobs that fail without any attempt to process the data (at the beginning of the processing cycle) are displayed in the running state in the VSPC UI until full data collection is performed for a backup agent.
- Custom variables configured in the backup policies cannot be edited using backup agent UI. To work around this, use backup policy edit options in the backup portal UI instead.
- Under certain conditions, the upgrade of Veeam backup agent to version 6 may fail with the "Failed to migrate the configuration" error message. To resolve this issue, restart the upgrade procedure using the backup portal UI.

Veeam Agent *for Linux* Integration

- After installation, the VSPC server needs up to 10 minutes to download all required agent packages. During this time backup agent installation using backup portal is not possible.

- Cloud backup policies will be automatically reapplied to managed agents when the failover to available gateways option is enabled in the company properties.

Veeam Agent *for Mac* Integration

- Agents that are managed by Veeam Backup & Replication servers synchronize data once a day. To resolve this, manage these backup agents with Veeam Service Provider Console.

Veeam Backup & Replication Integration

- Support logs download from remote backup servers might fail with the following error message: "Failed to download log files. Please log in to the backup console and retrieve the required logs manually". To resolve this, upgrade the PowerShell framework to the most recent version. If this does not help, contact Veeam Customer Technical Support team.
- Job scheduling column does not display any data for Nutanix AHV jobs.
- Nutanix AHV jobs cannot be started when using Veeam Backup & Replication earlier than version 11a.
- Nutanix AHV workloads will always report "Backup" as protection type (ignoring snapshots) when using Veeam Backup & Replication earlier than version 11.
- Remote installation of hotfixes and cumulative patches might fail on highly loaded Veeam Backup & Replication servers. To resolve that, grant more resources to the backup server or install the required files manually.
- The list of processed VMs is missing for CDP (continuous data protection) policies running on Veeam Backup & Replication v11. To resolve this issue, upgrade your managed backup server to the most recent version.
- Some metadata on the Protected Data tab is missing for VMs protected with CDP policies. To resolve this issue, upgrade your managed backup server to the most recent version.
- Download traffic for backup agents managed by Veeam Backup & Replication server cannot be measured when agent jobs are targeted to an object storage repository.
- Minor warning messages for installation, upgrade and patching tasks for a Veeam Backup & Replication server do not affect the overall status of the main task and are only shown in the main task details.

Veeam Backup for Public Cloud Integration

- Information about available backup restore points is synchronized once a day for Veeam Backup & Replication servers running version 11 or earlier. To refresh data more frequently, initiate the external repository rescan procedure manually using the Veeam Backup & Replication console or upgrade your backup servers to version 11a or later.
- When a workload is added to multiple policies and one policy is manually started using the backup portal, the status of this backup policy will remain "Starting". To resolve this, restart the VSPC services.
- Opening a backup appliance UI when VSPC server is installed on Microsoft Windows Server 2012 is not supported.

Veeam Cloud Connect Integration

- Deleting backup restore points manually from a cloud repository leads to incorrect quota reporting. There is no workaround to this until the next update of Veeam Backup & Replication.
- Deleting backups from a cloud repository is not supported for renamed tenants. Backups that belonged to a tenant before the renaming are not deleted. To resolve this, delete these backup files manually.

VMware Cloud Director Integration

- After applying a cloud backup policy using Cloud Director tenants or sub-tenants, the user must specify tenant or sub-tenant credentials to start using a job.

Veeam ONE Integration

- License key cannot be remotely installed using the VSPC UI when Veeam ONE services are running under the *LocalSystem* account. To resolve this, use any other account to run Veeam ONE services.

Veeam Backup *for Microsoft 365* Integration

- Personal sites cannot be selected in backup jobs created using the Veeam Service Provider Console UI. To resolve this, configure backup jobs using the Veeam *Backup for Microsoft 365* server console.
- Cannot edit a backup job with objects newly created in Microsoft 365 and explicitly added to a job using the Veeam Backup for Microsoft 365 server console. To resolve this, wait for 24 hours and retry the operation.
- Number of objects can be different when selecting RPO and SLA filters on the RPO & SLA tab. This happens because the SLA filter treats personal sites and users as a single unit, while the RPO filter splits those objects into separate entities.
- Under a certain condition, the scheduled time for a backup job can in the backup portal UI can be different from an actual start of a backup job.
- Personal sites of users are not displayed in the SLA report and the SLA widget.
- On-premises and hybrid Microsoft 365 organizations are not supported by the backup portal.
- Restore points created with Veeam Backup for Microsoft 365 version 5 are not displayed in the backup portal.

Backup Policies

- A service provider cannot assign backup policies created by the managed client. To resolve that, the service provider needs to copy this backup policy first.

Management Agent

- Migrating management agents between companies is not supported. To start managing a computer from a new company, reinstall the management agent.
- The management agent does not support connection through client proxy servers.
- If a master management agent uses custom user credentials to discover remote computers and to install Veeam Agent for Microsoft Windows, then after management agent failover operation (switching to the new management agent), custom credentials must be reapplied to the new master management agent.
- Management agents cannot be reassigned using the Set Company action from the client's company to the service provider company ("My Company"). As a workaround, reinstall the management agent and pre-select the required company in the agent installation package options.

Discovery Rules

- Microsoft Active Directory discovery process may take a considerable time for domains with a large number of objects.
- The Discovery of cloned machines with the same Bios UUID may fail. It is recommended to change Bios UUIDs for cloned machines before running discovery.
- Discovery rules exclude computers running Veeam Cloud Connect from the discovery results.

Alarms and Notifications

- Due to data collection engine scheduling, time stamps for triggered alarms might differ from the time of actual events.
- "VM without backup" alarm is not triggered for VMs contained in jobs that do not have any successful job sessions for the past period.

Monitoring and Reporting

- When you start a File to Tape job twice, the job state will be reported as failed until the first job run is complete. Some jobs collected from the managed Veeam Backup & Replication servers for the first time might show "-" as their job status. To resolve that, rerun the jobs and wait until the new data collection is complete.
- Information about jobs and restore points for backup agents managed by Veeam Backup & Replication is based on the agent time zone.
- "Unsupported license deployment. Shared license key usage" alarm is not triggered for the VSPC server. To stay compliant with licensing rules, use unique keys for every server.
- RPO & SLA widgets do not contain any data for objects that were added to a job but were never processed (have no restore points created).
- Session States tab does not display any data about CDP policies.

Billing

- Hardware plans with unlimited RAM resources are excluded from the quota usage dashboard.
- Rejected computers are ignored in the billing reports.
- Billing reports stop tracking backups created by Veeam Agent *for Microsoft Windows* pointed to the cloud repository if the target for the backup job is changed from a cloud repository to a non-cloud repository.
- Used Storage Quota reports incorrect data when GFS restore point is removed manually.
- Data Transfer Out metric is not calculated for VM replicas from backup servers that are not managed in Veeam Service Provider Console.
- A subscription plan created by a reseller will not be preserved in the managed company configuration if this company is removed from the reseller. To resolve this, please assign a new subscription plan to the company manually.
- Computers that were added to protection groups in Veeam Backup & Replication and never had successful job runs are treated as servers in invoices and billing data.
- Total sums on the widgets will display incorrect values if subscription plans with different currencies are used within the same VSPC server.
- Download traffic (data transfer out counter) is not measured for full health check operations triggered by Veeam backup agent jobs.
- Download traffic (data transfer out counter) is not measured when running volume-level restores for a Veeam backup agent.
- Correct billing on public cloud backup appliances requires Veeam Backup & Replication v12 or later.

Reseller Role

- When Veeam Cloud Connect is migrated to another server, all companies and resources hosted on that server and are managed by a reseller will be removed from that reseller. To resolve this, please readd these companies to the reseller manually.
- When management agent is reinstalled on the Veeam Cloud Connect server, all companies managed by a reseller will lose their references to the managing account. To resolve that, reassign all managed companies to resellers using the VSPC UI.

Licensing and Usage Reporting

- Backup servers deleted during a reporting month are not tracked in the usage reports and license usage statistics. To resolve that, calculate usage for these servers manually.
- Any non-approved usage adjustments are discarded during the upgrade of the backup portal. To resolve this, approve all adjustments before upgrading the backup portal to a new major version.

Plugin Library

- Site administrators do not have access to the VSPC plugin library. To resolve this, use backup portal administrator accounts when logging in to the portal.

ConnectWise Manage Plugin

- Companies with the "Not Approved" or "Credit Hold" states are not displayed in the plugin UI.
- ConnectWise Manage tickets created based on the "Computer without backup" and "VM without backup" alarms contain the missed RPO information as of the time when the alarm threshold was breached. To see the actual data of the missed RPO event, please use the VSPC web UI.
- The default data synchronization interval between Veeam Service Provider Console and plugin for ConnectWise Manage is 5 minutes. This affects all configuration settings, including SMTP server configuration. To change this interval, please contact the Veeam Customer Technical Support team.
- Monitoring services that are part of the backup portal subscription plan are not synchronized with ConnectWise Manage billing system.

ConnectWise Automate Plugin

- Companies created in the ConnectWise Automate Control Center fail to apply cloud backup policies to managed backup agents. To resolve it, add cloud repository resources to newly created companies using Veeam Service Provider Console web UI.
- If you change the VSPC web UI security certificate to an untrusted certificate, the connection from the plugin to the VSPC server will fail. To resolve this, reconnect the plugin manually in the plugin configuration settings.
- Activation status, agent version, location settings, and other properties for the backup agent are updated only by the synchronization task scheduled to run periodically.
- After activating a retired company in the Automate Control Center, click the **Resend Everything** button to populate the Veeam Service Provider Console plugin with new data.
- Backup agents moved between different companies in the Control Center must be reactivated in the Veeam Service Provider Console. Otherwise, company mapping will be incorrect.
- To complete the deletion of the Veeam Service Provider Console plugin, all Control Centers must be relaunched.

- Computers with operating systems unsupported by Veeam backup agent are not displayed in the Control Center plugin UI.
- Installation of a backup agent is not supported when either Veeam Service Provider Console or ConnectWise Automate server is not connected to the internet.

Upgrade

- Upgrade is not supported when the Veeam Service Provider Console configuration database and the SQL Server Instance hosting its database have different collation settings.
- All management agents will report inaccessible state during the upgrade until agents deployed on Veeam Cloud Connect servers are upgraded.
- After the upgrade, custom settings from service and web UI config files (*Veeam.MBP.Service.exe.config*; *Veeam.Portal.ConnectionHub.exe.config*; *Web.config*) are reset to default values. This does not apply to custom ports and security certificates used by the backup portal.

REST API

- Under certain conditions, the REST API swagger page might not load when using the Mozilla Firefox browser.

Licensing

To start using Veeam Service Provider Console, you must first obtain a Veeam Universal License (VUL) and deploy Veeam Cloud Connect infrastructure.

- For VCSP users, you may use an existing Veeam Cloud Connect infrastructure. If you do not yet have Veeam Cloud Connect installed, then provision the infrastructure and generate the required license keys using the VCSP Pulse portal.
- For Enterprise users, you may use an existing Veeam Cloud Connect infrastructure. If you do not yet have Veeam Cloud Connect installed, contact your Veeam representative.

To deploy Veeam Service Provider Console use any unused VUL key generated using the VCSP Pulse portal.

Technical Documentation References

If you have any questions about Veeam Service Provider Console, you may use the following resources:

- Product web page: <https://www.veeam.com/service-provider-availability-console.html>
- User guides: <https://www.veeam.com/documentation-guides-datasheets.html>
- Veeam Cloud & Service Provider (VCSP) private community forum (registration is required): <https://forums.veeam.com/veeam-cloud-service-providers-forum-f34>

Technical Support

We offer email and phone technical support for customers on maintenance and during the official evaluation period. For a 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 submit your support ticket or obtain additional information, please visit www.veeam.com/support.html.

TIP:

BEFORE CONTACTING TECHNICAL SUPPORT, CONSIDER SEARCHING FOR A RESOLUTION ON VEEAM COMMUNITY FORUMS AT www.veeam.com/forums.

Contacting Veeam Software

At Veeam Software we pay close attention to comments from our customers. It is important to us not only to quickly help you with your technical support issues – we make it our mission to listen to your input, and to build our products with your suggestions in mind.

Should you have a Customer Support issue or question, please feel free to contact us. 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 www.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 office locations, please visit www.veeam.com/contacts.