Veeam Service Provider Console 4.0 Release Notes

This document provides last-minute information about Veeam Service Provider Console version 4.0, 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 4.0 is available through Veeam Community Forums starting from March 31st, 2020.

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/or patch level.

Veeam Service Provider Console

Hardware

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

OS

Only the 64-bit version of the following operating system 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.x
- Microsoft Windows 7 SP1

**NOTE:**

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

Software

- Microsoft SQL Server 2019/2017/2016/2014/2012 (SQL Server Express 2012 SP4 and SQL Server Express 2016 SP2 are included in the setup)
- Microsoft SQL Server 2012 Native Client (included in the setup)
- Microsoft SQL Server 2014 System CLR Types
- Microsoft SQL Server 2014 Management Objects
- Microsoft .NET Framework 4.6.1 (included in the setup)
- Microsoft Internet Information Services (IIS) 7.0 or later
- Windows Installer 4.5
- Microsoft PowerShell 3.0 or later
- Microsoft Edge 80 or later, Mozilla Firefox 74 or later, Google Chrome 80 or later
- Microsoft Report Viewer 2015 (included in the setup)
- PDF viewer for viewing reports
Veeam Cloud Connect

Platforms
- Veeam Backup & Replication
- VMware vCloud Director

Software
- Microsoft PowerShell 3.0 or later

Infrastructure
- Veeam Backup & Replication 10 (recommended)
- Veeam Backup & Replication 9.5 Update 4.x
- VMware vCloud Director 10
- VMware vCloud Director 9.x
- VMware vCloud Director 8.20

Plugins

Platforms
- ConnectWise Automate
- ConnectWise Manage
- Grafana

Infrastructure
- ConnectWise Automate 12.0.237 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

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 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.x
• Microsoft Windows 7 SP1

Software
• Microsoft .NET Framework 4.6 or later

Network
• 32 kbit/s when managing Veeam Agent for Microsoft Windows
• 64 kbit/s when managing Veeam Backup & Replication

Managed Computers
Veeam Service Provider Console can manage the following Veeam products:

Platforms
• Veeam Agent for Microsoft Windows 4.0
• Veeam Agent for Microsoft Windows 3.0
• Veeam Backup & Replication 10
• Veeam Backup & Replication 9.5 Update 3 or later (compatible)

Software
• Veeam Management Agent

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.
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:

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 the 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 4.0 supports automated in-place upgrade from version 3.0 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 Availability Console 2.X and would like to upgrade your installation to version 4.0, please follow these steps:

1. Upgrade your Veeam Availability Console (VAC) server to version 3.0.
2. Update all management agents to version 3.0. The update procedure is initiated automatically upon the VAC server upgrade.
3. Make sure all management agents are updated, and only then upgrade your VAC server to version 4.0.
4. If you were using discovery rules to deploy backup agents, re-run these rules after upgrading your server to version 4.0. This will allow you to upgrade your Veeam backup agents to the latest version.
Known Issues in Veeam Service Provider Console

The following is a list of issues known to exist at the time of the Veeam Service Provider Console 4.0:

General

- Special characters are not supported in user login names.
- Selecting multiple data rows via 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 domain of the user.
- SQL Server using case sensitive collation is not supported.
- Updating management agent connection settings with a new company (tenant) name results in removing this management agent from the VSPC UI. To resolve that, no user action is required. The managed computer will re-register in the UI in one hour after the automatic data collection task is complete.
- Renaming tenant and company name in the VSCP at the same time will disconnect all management agents from the portal. To resolve it, reconfigure all management agents manually.

Security

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

Migration

- After migrating a Veeam Service Provider Console database to a new server, you must re-enter portal web address on the Configuration -> Portal Branding tab.

Client Management

- If tenant's or sub-tenant's password is changed using Veeam Cloud Connect console, then management agent connection settings will not be updated with the new settings. All agents need to be reconfigured manually. To work around this, update the tenant's password using Veeam Service Provider Console web UI. After you change the tenant name on the Cloud Connect server, all backups stored in a cloud repository will start a new backup chain.

Veeam Agent for Microsoft Windows

- Agent deployed using 3rd party applications is removed from all views after revoking the license key from the agent or uninstalling the agent. To start managing this agent again, re-install the management agent on the remote computer and register it in the backup portal.
- Veeam Agent for Microsoft Windows backup is considered as a cloud backup copy even after removing this agent from the backup copy job targeted to the cloud repository. As a workaround, change target of the Veeam Agent for Microsoft Windows backup job and let Veeam Service Provider Console collect the updated job config.
- After enabling or disabling usage of wake-up timers in the Veeam Agent settings, the target computer must be restarted to apply these changes.
• When tenant’s password is changed via console of a managed Veeam Backup & Replication server, all backup agents using the same credentials to connect to a cloud repository will not receive a new password. To resolve this, either upgrade the backup agent to the most recent version or adjust agent settings manually.

• Changes of the backup agent settings may be displayed in VSPC web UI with a delay. This is caused by the scheduling settings of the data collection task.

• Job status of running backup jobs targeted to a cloud repository is not updated when all cloud gateways are disabled or unreachable.

• Changing tenant name under which backup agent is sending backups to a cloud repository leads to losing information about available restore points stored in the repository.

• If backup agent running on a computer with Windows 7 guest OS fails to upgrade to version 4.0, re-run a discovery rule which located this computer in the infrastructure.

Veeam Cloud Connect

• 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 belonging to a tenant before the renaming are not deleted. To resolve this, delete these backup files manually.

VMware vCloud Director

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

Backup Policies

• 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 the new company, re-install the management agent.

• The management agent doesn’t support connection through client proxy servers.

• If a master management agent uses custom user credentials to discover remote computers and install/patch Veeam Agent for Microsoft Windows, then after management agent failover operation (switching to the new management agent), custom credentials must be re-applied to the new master management agent.

• The master role cannot be manually assigned to the management agent from an External discovery rule. The management agent is selected automatically.

• When you unregister a service provider from the managed Veeam Backup & Replication server, management agent connection settings to the backup portal are also discarded. To resolve that, configure management agent connection settings manually.

• When changing tenant or sub-tenant password, make sure that all management agents using this tenant account are up-to-date, otherwise, the password will not be applied.
• The management agent will not collect any data when it is installed on a backup server manually without enabling the “Allow this Veeam Backup & Replication installation to be managed by the service provider” check box. To resolve this issue, enable the remote management check box in the Service Provider wizard on the backup server and restart the management agent service.

• The management agent may report a warning message that the security certificate of the backup portal has changed, even if it was not. To resolve this, connect the management agent to the backup portal in the same format as it was specified in the security certificate of the VSPC backup portal.

Remote Computer Discovery

• Users with administrator privileges on the remote computer must be used for computer discovery. Usage of other accounts will cause discovery rule failure.

• Microsoft Active Directory discovery process may take considerable time for domains with a large number of objects.

• Discovery of cloned machines with the same Bios UUID may fail. It is recommended to change Bios UUIDs for cloned machines before running discovery.

Alarms and Notifications

• Due to data collection engine scheduling, time stamps for triggered alarms might differ from the time of actual events.

• “VM without replica” alarm requires Veeam Backup & Replication 9.5 Update 3 or later to work.

• “VM without backup” alarm is not triggered for VMs contained in jobs that do not have any successful job sessions for the past period.

• Summary email notification setting is now global and cannot be selectively chosen for either discovery rules or alarms.

• Alarms tracking the number of stored agent backups in a cloud repository require Cloud Connect 9.5 Update 4 or later.

• All messages and alarms triggered on a Cloud Connect server will have a server time and date format. All other notifications will be using browser settings to display time and date information.

Monitoring and Reporting

• If you decrease the available cloud repository quota for the company using Veeam Backup & Replication console, cloud repository quotas for managed locations are not decreased. To resolve that, use the Veeam Service Provider Console web UI to change quotas.

• Managed VMs counter does not include VMs replicated to the cloud host. This issue is fixed in Veeam Backup & Replication 9.5 Update 3 or later.

• Backup to tape jobs do not display their destination in the Protected VMs report.

• 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, re-run the jobs and wait for the new data collection is complete.

• A computer is considered to have a cloud backup in the customer portal of VSPC, even if a cloud backup job never ran. To resolve this issue, run a backup job targeted to a cloud repository at least once.
• Overview dashboard will report agent backups transferred with a backup copy job of an unmanaged backup server to a cloud repository as local backups. To resolve this, install a management agent to that backup server.

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 target for the backup job is changed from a cloud repository to a non-cloud target repository.
• Billing dashboard of the service provider will show incorrect data if the service provider and a reseller are using different currencies in subscription plans.
• Used Storage Quota reports incorrect data when GFS restore point is removed manually.
• Data Transfer Out metric is not calculated for VM replicas from a backup server that is not managed by Veeam Service Provider Console.
• 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 manually.
• If an invoice is generated before an hourly sync-up task in VSPC is complete, all backup data will be aggregated into a default location. To resolve this, please re-generate the invoice in one hour.

Reseller Role

• When Cloud Connect is migrated to another server, all companies and resources that are hosted on that server and are managed by a reseller will be removed from that reseller. To resolve this, please re-add these companies to the reseller manually.

Licensing

• 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.
• Changing a license key during a reporting period (from 1st to 10th day of the month) will reset all usage data for the reported month.

ConnectWise Manage Plugin

• Companies with “Not Approved” or “Credit Hold” states are not displayed in the plugin UI.
• Subscription plan selection cannot be saved until at least one product is mapped or created in the ConnectWise Manage product catalog.
• 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 Veeam Service Provider Console web UI.
• The default data synchronization interval between Veeam Service Provider Console and its plugin for ConnectWise Manage is 5 minutes. This affects all configuration settings, including SMTP server
configuration, etc. To change this interval, please contact Veeam Customer Technical Support team.

ConnectWise Automate Plugin

- Companies created from 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 UI.
- If you change the security certificate for the VSPC web UI to an untrusted certificate, the connection from plugin to the VSPC server will fail. To resolve it, 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 that is scheduled to run periodically.
- After activating a retired company in the Automate Control Center, click the Resend Everything button to populate Veeam Service Provider Console plugin with new data.
- Backup policies created by a managed company (tenant) are not available to resellers and service providers for assignments in the plugin. To resolve it, use Veeam Server Provider Console UI to assign these policies.
- Backup agents moved between different companies in the Control Center must be re-activated 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 need to be relaunched.
- Computers with operating systems unsupported by a Veeam backup agent are not displayed in the plugin UI in the Control Center.

Upgrade

- Unresolved alarms for connection state issues are triggered again after upgrading the Veeam Service Provider Console server.
- The size of the SQL Server transaction log may grow dramatically after the upgrade. To resolve it, please shrink the transaction logs manually using the built-in functionality of Microsoft SQL Server Management Studio.
- If you are using a custom port for the Veeam Service Provider Console web site, then make sure you specify this port both in IIS settings and in the web.config file before starting the upgrade procedure.
- After the update, all objects in the /computers resource in the VSPC API will receive new IDs. If you are using these objects in the integration, then re-query these objects to get the list of new IDs.
- The automatic upgrade of the management agent installed on the Cloud Connect server cannot be performed when Veeam Service Provider Console had other Cloud Connect servers previously registered in the infrastructure. To resolve this issue, edit connection settings to the Cloud Connect server and retry the upgrade of the management agent.
- Managed computers not running Microsoft .NET Framework 4.6 will require a reboot upon upgrading the Veeam Service Provider Console server and its management agents.
- Cloud Connect servers must be switched to the maintenance mode before starting an upgrade procedure. Otherwise, Veeam Service Provider Console will collect inconsistent data from these servers.
- The predefined group of portal administrators is enabled by default regardless of the previous condition.

- Upgrade is not supported when Veeam Service Provider Console configuration database and the SQL Server Instance hosting its database have different collation settings.

**RESTful APIs**

- File to tape jobs are only returned for Veeam Backup & Replication v10 servers when using this endpoint: `/infrastructure/backupServers/jobs/fileTapeJobs/objects`

- NAS backup jobs report a zero total backup size when using this endpoint: `/infrastructure/backupServers/jobs`
Licensing

To start using Veeam Service Provider Console, you must first obtain a Veeam Universal License 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, a free 1 Instance license has been made available to all partners on the License Management Portal (my.veeam.com).
- 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.

Then, deploy Veeam Service Provider Console and install the same license that is used for the Veeam Cloud Connect infrastructure.

Managing Veeam Backup & Replication

To manage Veeam Backup & Replication, enable the remote management check box on the client backup server. The client backup server may be licensed with any Veeam key (Subscription, Perpetual or Rental) with any paid Edition enabled.

**NOTE:**

You cannot use Veeam Service Provider Console to manage Veeam Backup & Replication Community and Starter editions.

Managing Veeam Agent *for Microsoft Windows* (Standalone)

You can use Veeam Service Provider Console as a management portal for Veeam Agent *for Microsoft Windows*, instead of using Veeam Backup & Replication.

Install any VCSP Rental Veeam Instance License with the desired number of Instances (matching to the number of Servers and Workstations under management). A VCSP Rental license can be obtained from Veeam Sales.

Managing Veeam Cloud Connect Only

To manage Veeam Cloud Connect servers, add them to the Veeam Service Provider Console. Licensing for this scenario is covered by your initial deployment.

For more information about using Veeam Service Provider Console to manage VCSP Rental licenses and usage reports, see the VCSP Rental Usage Reporting Guide.
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/availability-console.html
- User guides: https://www.veeam.com/documentation-guides-datasheets.html
- Veeam Cloud & Service Provider (VCSP) private community forum (pre-registration is required): https://forums.veeam.com/veeam-cloud-service-providers-forum-f34

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 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 offices location, please visit www.veeam.com/contacts.