Veeam Service Provider Console
What's new in v5?

Veeam® remains focused on developing integrated **cloud and managed service operation** capabilities, so a service provider like you can be the hero to organizations of all sizes. NEW Veeam Service Provider Console v5 expands even further on its purpose-built capabilities to fulfill these needs.

In addition, **enterprises with distributed environments** can also take advantage of these latest enhancements including expanded support for remote management of Linux and Mac.

Veeam Agent *for Linux* and Veeam Agent *for Mac* support

NEW Veeam Service Provider Console v5 introduces full support of Veeam Agent *for Linux* and the NEW Veeam Agent *for Mac*. Now you can build on centralized backup management for Microsoft Windows by extending physical server and remote workstation protection of Linux and Mac devices.

The unique benefits of Veeam Agent *for Linux* and Veeam Agent *for Mac* support include:

Linux machine discovery. You can now automatically discover Linux machines via scanning your clients' remote networks and applying various filters such as OS distros or installed packages to discover workloads that need to be protected.

Automatic deployment. After running remote discovery rules, you can automatically push the Veeam Agent *for Linux* package to remote computers and apply backup policies to start protecting critical data.

In the case of Veeam Agent *for Mac*, both packages (management agent and backup agent) are now combined to a single package that should make the installation via JAMF and other MDM tools process much easier.

Remote job management. Not only can you apply backup policies, but you can also make changes to the existing backup jobs on backup agents.

Monitoring and alerting. To better control SLAs and RPOs agreed with your client, you can use our predefined job status and computers with no backup alarms.

Backup status reporting. Predefined protected computers report now includes Linux and macOS workloads and can be used for detecting unprotected computers based on the defined SLA.

Billing and invoicing. Predefined subscription plan options now include Linux and Mac agents. This allows you to send invoices to your customers with all the details on protected workloads.

NEW Veeam Service Provider Console v5

Be the hero your customers need by delivering Backup as a Service (BaaS) and Disaster Recovery as a Service (DRaaS) powered by NEW Veeam Service Provider Console v5. This FREE solution, seamlessly integrated with v11 and purpose-built for service providers, offers an expanded capability set including:

- Centralized management for **Windows, Linux** and now **Mac Agents**
- Extended monitoring and reporting reach into cloud-native workloads running in **AWS** and **Azure**
- Line of sight into **lower-cost object storage utilization**
- Enhanced **billing and invoicing capabilities**

And more!

Eliminate data loss and ransomware with a centralized management platform that makes it easy to remotely monitor and manage your customers' Veeam environments at scale and at cost.

Supported environments

For a detailed list of supported environments, reference the product Release Notes.

Veeam Backup *for AWS* and Veeam Backup *for Microsoft Azure* support

NEW Veeam Service Provider Console v5 extends into the protection of cloud-native workloads with the support of Veeam Backup & Replication™ plug-ins for AWS and Microsoft Azure. Now service providers can build managed services around the protection of customers' workloads running in the public cloud.

The unique benefits of Veeam Backup *for AWS* and Veeam Backup *for Microsoft Azure* support include:

Monitoring and alerting. As a service provider, you can now monitor backup and snapshot job status via predefined alarms and notifications.

Backup status reporting. Predefined protected VMs report now includes VMs hosted in AWS or Microsoft Azure public clouds so that you can verify protection status for each discovered VM based on the agreed SLA.

Billing and invoicing. In addition to reporting, you can now charge for management and data protection services for VMs hosted in AWS or Microsoft Azure public cloud and automatically send invoices to your customers.

License usage reporting. The monthly usage report now includes all protected workload types discovered by Veeam plug-ins for AWS and Microsoft Azure via Veeam Backup & Replication servers.

Enhanced support for Veeam Agents managed by Veeam Backup & Replication

No matter how you deploy and manage Veeam Agents, we got you covered! Based on your feedback and requests for additional capabilities for Agents managed by Veeam Backup & Replication, we have made the following enhancements in this most recent release, including:

Backup status reporting. Starting from v5, you can now report on RPO status for agents managed by Veeam Backup & Replication. This also includes seeing these agents on the Protected Data tab in the main UI.

Billing and invoicing. In addition to creating reports for protected computers and viewing the latest restore points data, you can now create invoices that include Agents managed by Veeam Backup & Replication.

RESTful APIs support. Starting from v5, we have exposed data about these to all related endpoints.

Enhanced billing and invoicing

Visibility into storage usage has always been critical for billing and invoicing, especially with the incredible adoption of Capacity Tier for storing backups in the cloud repository. With Archive Tier's introduction in Veeam Backup & Replication v11, we have expanded our billing capabilities for more granular per-tenant usage reporting.

The unique benefits of enhanced billing and invoicing include:

New invoice layout. The predefined invoice template has been dramatically simplified with the removal of no-cost services.

Capacity and archive tiers support. You can now create invoices based on cloud repository usage, including detailed per-tenant information on storage consumption for capacity and archive tiers in a Scale-out-Backup Repository™.

"Insider protection" reporting. Now you have the ability to bill for consumed storage when customers enable the "insider protection" feature for their cloud repositories.

Allocated quota billing. You now have an option to charge either for allocated or consumed space of a cloud repository.

"Free of charge" resources. Starting from this release, you can now include "free of charge" resources to subscription plans.

Guest OS billing. You can now charge extra for the guest OS of managed computers.

Usage reporting for billing of capacity tier, archive tier and the insider protection feature can be captured through subscription plans configured in Veeam Service Provider Console UI. Alternatively, you can query usage reporting through the use of APIs into your established billing platforms.

NEW RESTful APIs v3

In the previous release, Veeam Service Provider Console introduced NEW RESTful APIs in a preview mode. With this release, the RESTful APIs v3 interface is production-ready and offers simplified integration and automation with third-party apps and platforms for powerful, effective BaaS and DRaaS service delivery. It is highly recommended to migrate your integrations to this API version, as RESTful APIs v2 will be deprecated in the next major release.

The unique benefits of RESTful APIs v3 include:

Detailed information for billing and backup reporting. With this release, Veeam Service Provider Console introduces detailed information about managed workloads that can help you build your own billing systems or integrate backup status data into existing management portals.

More actions and endpoints. You can now use RESTful APIs to integrate Veeam Service Provider Console into your existing tenant management workflows and portals.

Detailed changelog. To make the transition from v2 APIs to v3 smoother, we have included the detailed log of new endpoints, breaking changes in the RESTful APIs user guide.

Other enhancements

In addition to the above-mentioned major areas of improvement, v5 includes other enhancements, which respond to customer feedback and on-going R&D learnings, the most significant of which are listed below.

Alarms

Acknowledged state. Starting from v5, monitoring engineers can switch triggered alarms that require more time for troubleshooting to the acknowledged state. This allows them to react more quickly to the new triggered alarms.

"Computer and VM with no backup/replica" alarm enhancements. Monitoring engineers can now set tolerance periods for more flexible RPO threshold configurations. This should decrease the number of false positives when monitoring the data protection state.

Disabled companies monitoring. Disabled or "expired" companies no longer trigger alerts within the service provider portal. This should allow a monitoring engineer to be laser-focused on active clients.

Email notification enhancements. You can now access additional parameters when configuring alarm notification settings. For example, monitoring engineers can specify the service provider company name in notification recipients and include managed tenants and users to this list.

Post-alarm action enhancements. Monitoring engineers can now pass parameters to the scripts triggered as a post-alarm action. This gives them more options and actions when remediating triggered alarms.

Alarm rules enhancements. Monitoring engineers can now reset alarm rules to the default state. This should help to resolve any potential issues with incorrect or misconfigured thresholds.

Veeam Agent *for Microsoft Windows*

Granular backup exclusion options. You can now easily create backup policies with more flexible exclusion rules for volume and file-level backed backup jobs. This feature requires the latest version of Veeam Agent *for Microsoft Windows.*

GFS retention policy support. You can now leverage the new version of Veeam Agent *for Microsoft Windows* to configure a GFS retention policy setting for a standalone agent.

Daily retention support. Starting from v5, you can use the backup portal UI to configure a daily retention policy for managed server agents.

Veeam Backup *& Replication*

Remote patching. You now have an option to install hotfixes and cumulative patches to managed backup servers remotely. No need to go onsite or use RDP for that!

VMware Cloud Director replication jobs support. Veeam Service Provide Console can now display job state for VMware Cloud Director replication jobs. This enables a single pane of glass view for monitoring engineers.

Veeam Cloud Connect

Performance enhancements for VMware Cloud Director company creation. The process of creating companies in large VMware Cloud Director (VCD) infrastructures has been dramatically enhanced. Now, you don't need to wait for the entire VCD infrastructure to be scanned before creating a new tenant.

Backup reporting

Protected VMs report update. This report now includes filtering options for job and platform type.

Protected computers report update. This report now includes filtering options for guest OS and agent management type.

Protected data tab update. This tab now contains information about the source and backup sizes for most of the protected workloads. This data is also exposed via APIs, which can be used to create invoices for your clients.

Company management

No billing option. Service providers who are using in-house billing systems now have an option not to assign any subscription plan to managed companies. This will disable the default invoice generation process.

No alarms option. You can now turn off additional self-monitoring capabilities via alarms for managed companies via editing their company profiles. This is a recommended option when managed clients do not use the self-service backup portal.

Discovery rules

Backup agent deployment enhancements. The backup agent deployment process now has a retry option for unexcepted errors during the installation process. This helps when managing a highly mobile environment with computers that frequently go offline or online.

Scheduling enhancements. Discovery rules can now be scheduled, allowing you better time-management and prioritization of when discoveries must be performed.

Reseller

Automatic deployment settings. Resellers can now define their parameters for the automated deployment settings. Previously these settings were shared with the "hosting service" provider.

Backup infrastructure dashboard. Resellers now have access to the high-level overview of the backup infrastructure health state of managed companies.

Security

Multi-factor authentication. With this release, you can now enable multi-factor authentication (TOTP-based) for internal and external users when logging in to the backup portal.

Password reset operation enhancement. With this release, users who forgot their password no longer need to use secret questions to restore access to the backup portal. Starting from v5, the password reset operation uses time-based URLs sent out to an email address for ease of use.

UI

Job sessions overview dashboard. This dashboard provides an at-a-glance day-by-day view across all jobs and all workloads.

Management agents

Gateway pool update enhancements. When updating a gateway pool configuration, management agents will automatically pick it up without any manual steps required from the service provider.

Troubleshooting options enhancements. You can now initiate a full resync of data collection job for managed Veeam Agents and Veeam Backup & Replication servers. This option is useful as a first troubleshooting step when there is no data collected from remote computers.

Usability enhancements

Login enhancements. You can now create aliases for names of managed companies, making the login process more user-friendly.

Simplified backup jobs and protected data views. Veeam Service Provider Console v5 now groups all workloads based on their types, avoiding "tabs sprawl" in the UI.

Backup policy creation. You can now create predefined backup policies from already configured backup agents.

Tags. You can now assign tags to managed computers. This should allow you to quickly identify the "owner" of the remote computer and take measures if needed accordingly.

Failover plans update. Users initiating a VM failover operation can now see an assigned IP address to establish a network connection to the VM.

Subscription plan updates. Now you can review all companies assigned to a specific subscription plan.

Default cloud repository option. In the case of multiple cloud repositories assigned to a managed company, you can now select a default repository when creating a cloud backup job.

Advanced log configuration. You can now select a home folder for debug logs.

Export to CSV and XML. The data format has been improved when using the export to CSV or XML option for UI data tables.

Inactive or disabled objects. All inactive or disabled items are now greyed out for better distinction in the UI data tables.

Retries for backup policy. The backup policy configuration process now has a retry option for unexcepted errors. This helps when you're managing a highly mobile environment with computers that frequently go offline or online.

Usage reporting

Rental workloads reporting. Starting from v5, you can see a breakdown by rental and total workloads on the summary dashboard.

License usage dashboard updates. You can now view usage trends per workload type in the summary dashboard.

New workloads support. You can now report usage for all new workloads in Veeam Backup & Replication v11, including Veeam Backup *for AWS* and Veeam Backup *for Microsoft Azure*.

Historical reporting. You can now review usage reports generated for previous months right from the service provider console UI.

ConnectWise Manage plug-in

New billing options. You can now leverage all-new subscription plan options in integration with the ConnectWise Manage billing system.

ConnectWise Automate plug-in

Support for Veeam Service Provider Console v5. You can now use new versions of Veeam backup agents to protect workloads of your customers. To do that, please update your existing plug-in via ConnectWise Automate Solutions Center to the most recent version.

Learn more
www.veeam.com

Download free trial
vee.am/vspc