© 2019 Veeam Software.

All rights reserved. All trademarks are the property of their respective owners.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means, without written permission from Veeam Software (Veeam). The information contained in this document represents the current view of Veeam on the issue discussed as of the date of publication and is subject to change without notice. Veeam shall not be liable for technical or editorial errors or omissions contained herein. Veeam makes no warranties, express or implied, in this document. Veeam may have patents, patent applications, trademark, copyright, or other intellectual property rights covering the subject matter of this document. All other trademarks mentioned herein are the property of their respective owners. Except as expressly provided in any written license agreement from Veeam, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

**NOTE:**

Please read the End User Software License Agreement before using the accompanying software program(s). Using any part of the software indicates that you accept the terms of the End User Software License Agreement.
MANAGING VEEAM BACKUP & REPLICATION JOBS .................................................................................. 150
  Starting, Stopping and Retrying Jobs ........................................................................................... 151
  Disabling and Enabling Jobs ........................................................................................................ 152
  Downloading Job Logs and Session Report .................................................................................. 153
  Viewing and Exporting Veeam Backup & Replication Job Details ............................................... 154
  Viewing and Exporting Monitored Veeam Backup Agent Job Details ......................................... 156

MANAGING FAILOVER PLANS ............................................................................................................. 159
  Starting Failover Plans ................................................................................................................ 160
  Undoing Failover Plans ................................................................................................................. 161
  Viewing and Exporting Failover Plan Details ................................................................................ 162

MANAGING VEEAM AVAILABILITY CONSOLE AGENTS ................................................................... 164
  UPGRADING MANAGEMENT AGENTS .......................................................................................... 165
  SETTING MASTER AGENT FOR DISCOVERY .............................................................................. 166
  MODIFYING MANAGEMENT AGENT CONNECTION ACCOUNT .................................................... 168
  UNINSTALLING MANAGEMENT AGENTS .................................................................................... 169
  REBOOTING REMOTE COMPUTERS ............................................................................................ 170
  RESTARTING MANAGEMENT AGENT SERVICE .......................................................................... 171
  COLLECTING DATA .......................................................................................................................... 172

VIEWING INVOICES .......................................................................................................................... 173

RECEIVING BILLING NOTIFICATIONS .............................................................................................. 179

BACKUP REPORTING .......................................................................................................................... 180
  CONFIGURING BACKUP REPORTS ............................................................................................... 181
    Modifying Backup Report Configuration ...................................................................................... 186
    Deleting Backup Report Configuration ......................................................................................... 187
  RUNNING BACKUP REPORTS ........................................................................................................ 188
  VIEWING BACKUP REPORTS ......................................................................................................... 189
  SENDING BACKUP REPORTS ....................................................................................................... 193
  DELETING BACKUP REPORTS .................................................................................................... 195

WORKING WITH ALARMS .................................................................................................................. 196
  MANAGING ALARMS ...................................................................................................................... 197
    Modifying Alarm Settings ............................................................................................................. 198
    Changing Alarm Assignment Scope .......................................................................................... 203
    Enabling and Disabling Alarms ................................................................................................... 204
    Exporting Alarm Configuration ................................................................................................ 205
    Receiving Alarm Email Notifications ......................................................................................... 206
  WORKING WITH TRIGGERED ALARMS ......................................................................................... 207
    Resolving Alarms ......................................................................................................................... 208
    Deleting Alarms ........................................................................................................................... 209
    Viewing and Exporting Triggered Alarms .................................................................................. 210
MONITORING .......................................................................................................................... 212
  SUMMARY ............................................................................................................................. 213
  PROTECTED COMPUTERS ...................................................................................................... 218

MANAGING PORTAL USERS ................................................................................................. 221
  USER ROLES AND PERMISSIONS .......................................................................................... 222
  CREATING PORTAL USERS ................................................................................................... 224
    Creating Location Administrators ...................................................................................... 225
    Creating Location Users ....................................................................................................... 228
    Creating Subtenants ............................................................................................................. 231
    Creating Company Invoice Auditors .................................................................................. 235
  MODIFYING PORTAL USERS .................................................................................................. 237
  REMOVING PORTAL USERS .................................................................................................. 238
  DISABLING AND ENABLING PORTAL USERS ....................................................................... 239
  MODIFYING OWN USER PROFILE ....................................................................................... 241

MANAGING LOCATIONS ........................................................................................................ 243
  CREATING LOCATIONS .......................................................................................................... 244
  SETTING LOCATIONS ............................................................................................................ 245
  MODIFYING LOCATIONS ........................................................................................................ 247
  REMOVING LOCATIONS ........................................................................................................ 248

APPENDIX A. ADVANCED INSTALLATION AND CONFIGURATION PROCEDURES .............. 249
  HOW TO UPLOAD VEEAM BACKUP AGENT SETUP FILE TO CLIENT COMPUTERS WITH GPO ......................................................................................................................... 250

APPENDIX B. ALARMS ........................................................................................................... 252
Contacting Veeam Software

At Veeam Software we value the feedback from our customers. It is important not only to help you quickly with your technical issues, but it is our mission to listen to your input, and build products that incorporate your suggestions.

Customer Support

Should you have a technical concern, suggestion or question, please visit our Customer Center Portal at www.veeam.com/support.html to open a case, search our knowledge base, reference documentation, manage your license or obtain the latest product release.

Company Contacts

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

Online Support

If you have any questions about Veeam products, you can use the following resources:

- Full documentation set: www.veeam.com/documentation-guides-datasheets.html
- Community forum at forums.veeam.com
About This Document

This document describes how client companies that consume managed backup services can use Veeam Availability Console.

The document scope is limited to functionality available in the Client Portal and does not cover features available in the Administrator Portal and Reseller Portal. For details on Veeam Availability Console features available in the Administrator Portal, see Veeam Availability Console Guide for Service Providers. For details on Veeam Availability Console features available in the Reseller Portal, see Veeam Availability Console Guide for Resellers.

Intended Audience

The document is intended for users within client companies that want to automate deployment and configuration of Veeam backup agents and perform management of Veeam Backup & Replication installations with Veeam Availability Console.

Disclaimer

This document may include images that display names of companies, contact persons, address details and similar. Information of this type is fiction and provided for demonstration purposes only. Any resemblance to real companies or people is coincidental.

Document Revision History

<table>
<thead>
<tr>
<th>Revision #</th>
<th>Date</th>
<th>Change Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revision 2</td>
<td>04/10/2019</td>
<td>Updated section Viewing Backup Reports.</td>
</tr>
<tr>
<td>Revision 1</td>
<td>03/28/2019</td>
<td>Initial version of the document for Veeam Availability Console 3.0.</td>
</tr>
</tbody>
</table>
About Veeam Availability Console

Veeam Availability Console is a cloud-enabled platform for centralized management and monitoring of data protection operations and services. The solution is intended for physical and virtual environments protected with Veeam Agent for Microsoft Windows (further referred to as Veeam backup agent) and Veeam Backup & Replication. Veeam Availability Console allows service providers to deliver Veeam-powered Backup-as-a-Service (BaaS) and Disaster Recovery-as-a-Service (DRaaS) services to their customers.

For client companies that act as backup service consumers, Veeam Availability Console offers a Client Portal. The Client Portal is a private workspace for client company users where they can perform self-service tasks, without contacting the provider of backup services.

The Client Portal can be used by companies that:

- Have their Veeam backup agents managed in Veeam Availability Console
- Have their Veeam Backup & Replication installations managed in Veeam Availability Console
- Store backups and replicas created with Veeam backup agents and Veeam Backup & Replication in the cloud that is powered by Veeam Cloud Connect

Companies working with the Client Portal get access to the following services and tools:

- **Automated deployment, configuration and management of Veeam backup agents.** You can automate deployment and configuration of Veeam backup agents on machines in local and remote networks, manage backup jobs, and monitor the status of data protection operations for computers protected with Veeam backup agents.

- **Centralized monitoring and management of Veeam Backup & Replication.** You can manage Veeam Backup & Replication jobs configured to protect virtual machines, run failover plans, monitor and report on the status of data protection operations in virtual environments, or connect to backup servers remotely.

- **Resource monitoring for Veeam Cloud Connect.** You can monitor consumption of cloud repository and cloud host resources allocated for storing backups and replicas created with Veeam backup agents and Veeam Backup & Replication.

- **Self-service monitoring and backup reporting.** You can track the amount of consumed resources and provided services, view and download invoices generated by the service provider, and create backup reports showing whether you meet established RPO requirements.
System Requirements

The Veeam Availability Console Client Portal is a web-based console available through a web browser. To work with the Veeam Availability Console Client Portal, use one of the following browsers:

- Microsoft Internet Explorer 11 or later
- Microsoft Edge 35 or later
- Mozilla Firefox 50 or later
- Google Chrome 54 or later
Accessing Veeam Availability Console

To access Veeam Availability Console:

1. In a web browser, navigate to the Veeam Availability Console URL. Note that Veeam Availability Console is available over HTTPS.

   The Veeam Availability Console URL looks like the following one:
   
   https://vac.cloudprovider.com:1280

2. In the **Username** and **Password** fields, specify credentials of an authorized user.

   The user name must be provided in the **Company Name\User** format.

   If you are the only company user, and log in for the first time, use Company Owner credentials. Company Owner credentials are available in a welcome email notification that must be sent to you by the service provider. For details on users and privileges, see Managing Portal Users.

3. Select the **Remember me** check box to save the user name for future access.

4. Click **Login**.

   If Veeam Availability Console displays a list of Veeam Cloud Connect servers and asks you to specify the server you want to log in, contact your service provider for details on the necessary Veeam Cloud Connect server.

Logging Out

To log out of Veeam Availability Console, at the top right corner of the Veeam Availability Console window click your user name and choose **Log Out**.
Resetting Password

If you forget your password, you can reset it.

**NOTE:**

To be able to reset the password, you must have an email address and an answer to the security question specified in your user profile. Veeam Availability Console will use this information to reset the password. For details on working with user profile details, see Modifying Own User Profile.

To reset the password:

1. Navigate to the Veeam Availability Console **Login** page.
   For details, see Accessing Veeam Availability Console.
2. Click the **Forgot password** link.
   Veeam Availability Console will launch the **Reset Password** wizard.
3. At the **Reset User Password** step of the wizard, type your user name and an email address specified in your user profile.
   The user name must be provided in the **Company Name\User** format.

![Reset Password Wizard](image-url)
4. At the **Security Question** step of the wizard, type an answer to the security question specified in your user profile.

5. Check your inbox for an email message with instructions for resetting the password. The message will include a temporary password generated for you by Veeam Availability Console.

6. Click the **Login to Client Portal** link in the email message.

7. Log in to Veeam Availability Console with your user name and the temporary password. The user name must be provided in the **Company Name\User** format.

8. At the top right corner, click your user name and choose **Edit Profile**. Veeam Availability Console will launch the **Edit User** wizard.

9. Navigate to the **Login Info** step of the wizard.

10. In the **Current password** field, type the temporary password.
11. In the **New password** and **Confirm password** fields, type a new password.

![Edit User Interface]

12. Click **Finish**.

13. After you change the password, log in to Veeam Availability Console using your new password.

**Other Ways to Reset Password**

If you cannot obtain a temporary password by email for some reason (for example, you did not specify your email address or an answer to a security question in your user profile settings), contact the Administrator of the Client Portal. The Location Administrator can reset the password for you.
Getting Started

To quickly get started with Veeam Availability Console, keep to the following sequence of steps:

1. **Fill your company profile.**
   The company profile contains your company name, information about company address, contact details and so on. Company profile details will be used for invoices and email notifications, such as billing or alarm notifications.

2. **Create locations.**
   To differentiate backup services and cloud resources consumed by different offices or business units within your company, you can create multiple locations.

3. **Add systems to manage.**
   a. **Deploy Veeam Backup Agents and configure backup jobs.**
      Deploy Veeam backup agents on computers in your infrastructure and configure backup job settings.
   b. **Connect Veeam Backup & Replication servers.**
      Connect Veeam Backup & Replication servers that you plan to manage in Veeam Availability Console.

4. **Configure backup reports.**
   Configure and run backup reports to check the efficiency of data protection, and make sure that you meet established RPO requirements.

5. **Configure alarm settings.**
   Check alarm settings, alarm response actions, and configure alarm assignment.

6. **Create new portal users.**
   To provide access to Veeam Availability Console to other employees in your company, create new portal users and assign the necessary user roles for them.

**NOTE:**
To perform configuration tasks, a user must have the Location Administrator privileges in Veeam Availability Console. For details on users and privileges, see Managing Portal Users.
Filling Company Profile

Before you start working with Veeam Availability Console, you must fill out the company profile. The profile contains information about your company, such as the company name, address, contact person details and so on. Information specified in the company profile is included in invoices.

Some information in the company profile is populated by the Veeam Availability Console Portal Administrator, when a company account is registered. You must check provided details and fill the remaining information in the company profile.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Filling Company Profile

To fill the company profile:

1. Log in to Veeam Availability Console. For details, see Accessing Veeam Availability Console.
2. At the top right corner of the Veeam Availability Console window, click Configuration.
3. In the configuration menu on the left, click Company Info.
4. In the Tax ID field, specify the company tax identification number.
5. In the Country, State, City, Street, Phone, ZIP code, Web Site, Email fields, specify your company address and contact information.
6. Click Save.
Managing Veeam Backup Agents

Veeam Availability Console allows you to automate deployment and management of the Veeam Agent for Microsoft Windows software (or, in short, Veeam backup agents).

With Veeam Availability Console, you can install Veeam backup agents on remote computers that reside in managed company infrastructure, and perform various types of configuration and management operations, such as configuring backup job settings, starting and stopping backup jobs and so on.

To deploy and manage Veeam backup agents in Veeam Availability Console, keep to the following sequence of steps:

1. **Install Veeam backup agents.**
   Veeam Availability Console supports several methods for installing Veeam backup agents, including installation with discovery rules, installation using 3rd-party automation tools, and manual software installation.

2. **Configure Veeam backup agent job settings.**
   To automate Veeam backup agent job configuration for multiple computers, create and assign backup policies. Alternatively, you can perform configuration of backup job settings manually, on a per-computer basis.

3. **[Optional] Enable Read-Only access mode.**
   To prevent end users from changing Veeam backup agent job settings and performing restore operations, you can enable read-only access mode.

4. **Configure Veeam backup agent global settings.**
   Check and if necessary change Veeam backup agent global settings on managed computers.

5. **Manage Veeam backup agent jobs.**
   To administer data protection operations in company infrastructure, you can start, stop, enable and disable Veeam backup agent jobs on client computers. You can also monitor Veeam backup agent jobs that are managed by your Veeam Backup & Replication servers.

6. **Create backup reports.**
   To analyze the efficiency of data protection with Veeam backup agents, and make sure you can meet established RPO requirements for managed company infrastructure, you can configure and run backup reports.
Installing Veeam Backup Agents

To manage Veeam backup agents in Veeam Availability Console, you must deploy two software components on managed computers:

- **Veeam backup agent**
  
  This software component is responsible for all types of data protection and restore operations on a managed computer.

- **Veeam Availability Console management agent**
  
  This software component acts as a broker between Veeam backup agent and Veeam Availability Console. The management agent is responsible for transmitting commands from Veeam Availability Console to Veeam backup agent, performing management, software installation and configuration operations on a managed computer, collecting data from Veeam backup agent and communicating it back to Veeam Availability Console.

You can use one of the following methods to deploy Veeam backup agent and Veeam Availability Console management agent on computers in managed infrastructures:

- Install Veeam backup agents with discovery rules (recommended)
- Install Veeam backup agents with 3rd party automation tools
- Install Veeam backup agents manually
Installing Veeam Backup Agents with Discovery Rules (Recommended)

You can deploy Veeam backup agents and Veeam Availability Console management agents on managed computers using **discovery rules**. This is the recommended installation method. It allows you to run discovery and initiate the installation procedure in the Veeam Availability Console portal. Thus, you can minimize manual operations with the managed computers, or usage of any 3rd party tools during the installation process.

**How Installation with Discovery Rules is Performed**

For installation with discovery rules, Veeam Availability Console requires a **master agent**. A master agent is a Veeam Availability Console management agent that runs on a Windows machine in the managed infrastructure. This agent is responsible for performing various types of tasks during the discovery and installation procedures, such as collecting information about discovered computers, installing Veeam Availability Console management agents on managed computers, downloading the Veeam backup agent setup file, uploading it to managed computers, and so on.

Installation with discovery rules includes two processes that run one after another:

- Discovery of managed computers
- Installation of Veeam backup agents and Veeam Availability Console management agents on discovered computers

The following diagram provides a high-level pictorial overview of the discovery-based installation method.

---

**Discovery of Managed Computers**

Discovery of managed computers runs as follows:

1. A backup administrator sets up a master agent in a managed location, configures a discovery rule and initiates the discovery process.
The discovery rule describes settings required to perform discovery and (optionally) installation of Veeam backup agents on discovered computers. Discovery rule prescribes what master agent will be used for discovery, what managed computers must be scanned, what account will be used to connect to these computers, whether Veeam backup agents must be installed on discovered computers, and so on.

The discovery rule can use one of the following discovery methods: network-based discovery, Active Directory discovery or import-based discovery.

2. The master agent obtains from Veeam Availability Console discovery settings specified in the discovery rule. The agent connects to managed computers under the specified account, collects configuration information about each scanned computer through WMI, and communicates information about discovery results to Veeam Availability Console.

Information collected from discovered computers includes details on the computer type, platform, host name, guest OS, IP address, MAC address, available applications and information about Veeam backup agent (its presence on the machine, product version and license installed).

3. If the discovery rule is configured to install Veeam backup agents on discovered computers and set up a backup job, the master agent initiates these tasks after discovery.

For details on the installation process, see Installation of Veeam Backup Agents.

### Installation of Veeam Backup Agents

Installation of Veeam backup agents runs as follows:

1. A backup administrator initiates the installation process.
   - If a discovery rule is configured to install Veeam backup agents on discovered computers and set up a backup job, the installation process is initiated automatically after discovery. The backup administrator must only initiate the discovery process.
   - Otherwise, the backup administrator must instruct Veeam Availability Console to install Veeam backup agents on discovered computers.

2. The master agent downloads the Veeam backup agent setup file from the Veeam Installation Server (over the Internet), and uploads this file to discovered computers.

3. The master agent downloads the Veeam Availability Console management agent setup file from the Veeam Availability Console server, uploads this file to discovered computers, triggers management agent installation, and configures management agents to communicate with Veeam Availability Console.

4. Veeam Availability Console management agents on the discovered computers trigger installation of Veeam backup agents.

5. When installation completes, management agents activate Veeam backup agents.

6. If a backup job must be set up as part of the installation procedure, management agents apply a backup policy.

### How to Install Veeam Backup Agents with Discovery Rules

To install Veeam backup agents with discovery rules, perform the following steps:

1. **Install and configure a master agent.**
   - Install and configure a Veeam Availability Console master agent on a machine in the client infrastructure.

2. **Perform discovery of client computers.**
Configure discovery rules and run discovery to identify computers on which you plan to install Veeam backup agents.

3. **Initiate the installation procedure.**
   Initiate the installation procedure in Veeam Availability Console.

### Step 1. Install and Configure Master Agent

Before you start discovery and installation, you must install and configure a *master agent* on a Windows machine in the company infrastructure.

#### Prerequisites

Before you install and configure a master agent:

- Obtain the management agent setup file.
  For details, see [How to Obtain Management Agent Setup File](#).
- Make sure that the machine that will host the master agent has access to the Internet, and network access to all computers that you want to discover in the managed infrastructure.
- If you plan to discover computers using an Active Directory discovery method, make sure the machine that will host the master agent is part of a domain within which computers will be discovered.
- Make sure you have an account with local Administrator permissions on all computers that you want to discover.

#### Required Details

Obtain the following data from the service provider:

- FQDN or IP address of a cloud gateway
- Port on the cloud gateway used to transfer backup data to and from cloud repositories
- User credentials for connecting to the service provider (Company Owner credentials)
- Thumbprint of a certificate that is installed on the Veeam Availability Console and Veeam Cloud Connect servers

#### Installing and Configuring Master Agent

To install a master agent:

1. Copy the agent setup file to a location accessible from the machine where you want to install the master agent.
2. Log on to the machine as an Administrator.
3. Double-click the agent setup file to launch the [Veeam Availability Console Communication Agent](#) wizard.
4. Follow steps of the wizard.
5. At the last step of the wizard, click **Install**.
6. When installation completes, click Finish to close the wizard.

   The agent will be installed by the following path: %ProgramFiles%\Veeam\Availability
   Console\CommunicationAgent.

To configure a master agent:

1. In the icon tray, right-click the master agent icon and choose Agent Settings.

   If the icon is hidden, display hidden icons, find Veeam.MBP.Agent.Configurator in the list of
   notification area icons, and choose to show the icon and notifications for it.

2. In the Veeam Master Agent Settings window, specify settings that the agent must use to connect to
   Veeam Availability Console.

   a. In the Cloud Gateway field, type FQDN or IP address of a cloud gateway.

   b. In the Port field, specify the port on the cloud gateway that is used to transfer data to Veeam
      Availability Console.

   c. In the Username and Password fields, type user credentials of a Company Owner.

      The user name must be provided in the <Company Name\User> format.

3. In the Management Agent Settings window, click Apply.

   Management agent will connect to Veeam Availability Console server, download the security certificate
   and perform its verification.

   In case of errors during certificate verification you will be prompted the Security Certificate Preview
   window:

   • To view error details, at the top of the window, click the Learn more link.

   • To ignore the error and continue agent configuration, click Save.

4. In the Management Agent window, click Restart to restart the management agent and apply connection
   settings.

5. Wait for the agent to connect to Veeam Availability Console.

   When the agent connects to Veeam Availability Console, the status in the Management Agent Settings
   window will be displayed as Connected. The agent icon in the icon tray will turn blue.

6. [Optional] Specify an account that will be used for computer discovery and installation of Veeam backup
   agents.
If you do not specify an account at this stage, you will need to specify it when configuring discovery rules.

a. In the Veeam Master Agent Settings window, click the Remote computer discovery user account link.

b. In the Discovery Account window, select the Specify local administrator credentials for remote installation of backup agents check box.

c. In the Username and Password fields, specify credentials of an account that will be used to discover client computers and install Veeam backup agents.

The account must have local Administrator permissions on all computers that you want to discover in the client infrastructure.

d. Click OK.

7. In the Management Agent Settings window, click Close.

What You Can Do Next

If a company has more than one location, you must set a location for the master agent.

By default, all new master agents you install belong to the default company location. If the master agent belongs to a non-default location, you must explicitly set this location for the agent.

For details on setting locations, see Setting Locations.

How to Obtain Management Agent Setup File

To download the management agent setup file, you can use one of the following options.

Downloading Management Agent Setup File in Veeam Availability Console

You can download the management agent setup file in Veeam Availability Console:

1. Log in to Veeam Availability Console as a Company Owner or Location Administrator.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Managed Computers.
3. Open the Discovered Computers tab.
4. At the top of the computers list, click Download Agent.
The setup file `ManagementAgent.exe` will be saved to the default download location on your computer.

**Downloading Management Agent Setup File Using Link in Welcome Email**

Company users can download the management agent setup file using a link in the welcome email message that is sent to a Company Owner.

**Step 2. Perform Discovery of Client Computers**

To identify computers on which you can install Veeam backup agents, you must configure discovery rules and run discovery in the company infrastructure.

Veeam Availability Console supports the following discovery methods:

- **Network-based discovery**
  This method allows you to discover computers based on a range of IP addresses.

- **Active Directory discovery**
  This method allows you to discover computers being part of an AD domain.

- **Import-based discovery**
  This method allows you to discover computers by importing a list of IP addresses from a CSV file.

**Required Privileges**

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

**Configuring Network-Based Discovery Rules**

Network-based discovery rules allow you to discover computers based on a range of IP addresses you specify. This method is recommended for small environments, with no Active Directory domains.

**Prerequisites**

Before you configure a network-based discovery rule:

- Deploy a master agent on a machine in the company infrastructure.
  For details, see Step 1. Install and Configure Master Agent.

- Make sure you have an account with local Administrator permissions on all computers that you want to discover.
  This prerequisite is not required if you have specified a discovery account in the master agent configuration settings. For details, see Step 1. Install and Configure Master Agent.

- Make sure that remote computers are powered on and configured to allow discovery: the Remote Scheduled Tasks Management (RPC and RPC-EPMAP) firewall rules must allow inbound traffic.

- On remote computers that run a Windows desktop OS, the Windows Management Instrumentation
(WMI-In) firewall rule must be configured allow inbound traffic.

- If you plan to install Veeam backup agents as part of the discovery procedure, make sure that remote computers are configured to allow installation: the *File and Printer Sharing (SMB-In)* firewall rule must allow inbound traffic.

- If you plan to assign a backup policy as part of the discovery procedure, create a new backup policy or check and if necessary customize one of the predefined policies.

For details, see Configuring Backup Policies.

Configuring Network-Based Discovery Rule

To configure a network-based discovery rule:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click *Rules*.
3. On the *Rules* tab, click *New*.
   Veeam Availability Console will launch the *New Rule* wizard.
4. At the *Rule Name* step of the wizard, specify a discovery rule name.

![New Rule Wizard](image)
5. At the **Companies** step of the wizard, choose one or more companies for which the discovery rule is configured. Use the search field at the top of the list to find the necessary companies.

6. Click a link in the **Locations** column, then click a link in the **Master Agent** column, and select a management agent that will be used as the master agent for discovery in each company location.

   By default, discovery is performed in all company locations where you deployed a master agent. If you choose to perform discovery in multiple locations, after you complete the wizard steps, Veeam Availability Console will create a separate discovery rule for each location. If you do not want to perform discovery in some company locations, clear check boxes next to these locations.
For details on working with company locations, see Managing Locations.

7. **At the Discovery Method step of the wizard, select **Network-based discovery**.**

8. **At the Network Discovery step of the wizard, specify one or more networks and IP ranges that must be scanned to discover computers:**
   
   a. **Click Add.**
      
      Veeam Availability Console will open the **Network IP Range** window.
b. In **Network name** field, type an arbitrary name of the network that must be scanned.

c. In the **IP range** fields, type a range of IP addresses that must be scanned in the specified network.

d. Click **OK**.

e. Repeat steps a-d for each new IP range you want to include in the rule.

f. In the **Exclusion mask** field, specify a mask for names of computers that must be excluded from discovery.

   The mask can contain the asterisk (*) that stands for zero or more characters. You can specify multiple masks separated with commas.

9. At the **Access Account** step of the wizard, specify credentials of an account that the master agent will use to connect to computers within the discovery scope. The account must have local Administrator permissions on all discovered computers.

   If you have specified a discovery account in the master agent configuration settings, select the **Use credentials specified in the master management agent configuration** check box. For details on specifying master agent configuration settings, see Step 1. Install and Configure Master Agent.
Credentials specified in the master agent configuration take precedence over credentials specified in the discovery rule. For discovery, the master agent will use an account specified in its configuration settings. In case this account is not valid or not set, the master agent will use an account specified in the discovery rule.

10. At the Discovery Filters step of the wizard, choose what filters you want to enable for discovery.

- To filter computers by OS type, select By OS type in the list and click Edit. In the Operating System window, select the type of OS that must run on discovered computers (Server operating system, Client operating system). Click OK.

- To filter computers by application, select By application in the list and click Edit. In the Application window, select applications that must run on discovered computers (Microsoft Exchange Server, Microsoft SQL Server, Microsoft Active Directory, Microsoft SharePoint, Oracle, Other Applications). Click OK.

- To filter computers by platform, select By platform in the list and click Edit. In the Platform window, select platforms on which discovered computers must run (Microsoft Hyper-V and VMware vSphere, Physical computers, Microsoft Azure, Amazon Web Services, Other). Click OK.

- If you want to perform discovery among accessible computers only, select the Do not show inaccessible computers check box.
NOTE:

Different types of filter conditions are joined using Boolean AND operator. For example, if you enable filters *Server operating system, Microsoft SQL Server* and *VMware vSphere*, the list of discovered computers will include only VMware vSphere VMs that run Windows Server OS and Microsoft SQL Server.

11. At the **Email Notification** step of the wizard, you can enable notifications about discovery results by email.

   a. Select the **Send notifications** check box and specify a schedule according to which email notifications must be sent.
   
   b. In the **Subject** field, specify the subject of the notification.
   
   c. In the **To** field, specify an email address at which the email notification must be sent.
d. Select the **Send notification email after the first run** check box if a notification about discovery results must be sent after the first run of the discovery rule, regardless of the specified schedule.

12. At the **Backup Agent Deployment** step of the wizard, specify whether you want to install Veeam backup agents on discovered computers:

   a. If you do not want to install Veeam backup agents as part of the discovery process, leave the **Discover remote computer without installing backup agent** option selected.

   b. If after discovery Veeam backup agents must be installed automatically, select the **Discover remote computer, install backup agent and assign the selected backup policy** option.

      From the **Backup policy to apply** list, choose a backup policy that must be assigned immediately after installation. To view the selected policy details, click the **Show** link. If you do not want to assign any backup policy after installation, choose **No policy** from the list.

      If you do not have the necessary backup policy configured yet, you can click the **Create New** link to create a new policy, without exiting the **New Rule** wizard. For details on backup policies, see **Configuring Backup Policies**.

   c. By default, the read-only access mode is enabled for all Veeam backup agents installed as part of discovery. To disable the read-only access mode for Veeam backup agents on discovered computers, set the **Enable read only UI access for the backup agent** toggle to **Off**.
For details on the read-only access mode for Veeam backup agents, see Enabling Read-Only Access Mode.

13. At the Summary step of the wizard, review discovery rule settings.

   a. To start discovery after you save the rule, select the Launch the discovery rule when I click Finish check box.

   If you do not select this check box, you will need to launch discovery later. For details, see Running Discovery.
b. Click Finish.

Configuring Active Directory Discovery Rules

Active Directory discovery rules allow you to discover computers being part of an AD domain.

This method is recommended for client environments with Active Directory domains of any size. Active Directory discovery rules target AD containers, which helps perform dynamic discovery: if new computers join a domain, a new run of an AD-based rule will discover these computers.

Prerequisites

Before you configure an Active Directory discovery rule:

- Deploy a master agent on a machine in the company infrastructure. The machine must be included in a domain within which computers will be discovered.

  For details, see Step 1. Install and Configure Master Agent.

- Make sure you have an account with local Administrator permissions on all computers that you want to discover.

  This prerequisite is not required if you have specified a discovery account in the master agent configuration settings. For details, see Step 1. Install and Configure Master Agent.

- Make sure that remote computers are powered on and configured to allow discovery: the Remote Scheduled Tasks Management (RPC and RPC-EPMAP) firewall rules must allow inbound traffic.

- On remote computers that run a Windows desktop OS, the Windows Management Instrumentation (WMI-In) firewall rule must be configured allow inbound traffic.

- If you plan to install Veeam backup agents as part of the discovery procedure, make sure that remote computers are configured to allow installation: the File and Printer Sharing (SMB-In) firewall rule must allow inbound traffic.
If you plan to assign a backup policy as part of the discovery procedure, create a new backup policy or check and if necessary customize one of the predefined policies.

For details, see Configuring Backup Policies.

Configuring Active Directory Discovery Rule

To configure an Active Directory discovery rule:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Rules.
   Veeam Availability Console will launch the New Rule wizard.
4. At the Rule Name step of the wizard, specify a discovery rule name.
5. **At the Companies step of the wizard**, choose one or more companies for which the discovery rule is configured. Use the search field at the top of the list to find the necessary companies.

<table>
<thead>
<tr>
<th>Company</th>
<th>Slice</th>
<th>Locations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beta</td>
<td>Atlanta</td>
<td>Main Office</td>
</tr>
</tbody>
</table>

6. **Click a link in the Locations column**, then **click a link in the Master Agent column**, and select a management agent that will be used as the master agent for discovery in each company location.

   By default, discovery is performed in all company locations where you deployed a master agent. If you choose to perform discovery in multiple locations, after you complete the wizard steps, Veeam Availability Console will create a separate discovery rule for each location. If you do not want to perform discovery in some company locations, clear check boxes next to these locations.
For details on working with company locations, see Managing Locations.

7. At the Discovery Method step of the wizard, select Microsoft Active Directory discovery.

8. At the Active Directory Discovery step of the wizard, select the necessary method for Active Directory discovery:
   - Select Search through all Active Directory containers to discover all computers that are included in the Domain Controllers and Computers organizational units.
- Select **Select from organizational units** to discover computers that are included in selected organizational units only.

  If this option is selected, the **Organizational Units** step will become available in the wizard.

- Select **Run custom query** to discover computers based on results of a custom query. In the text field at the bottom, specify a LDAP query that must return a list of computers to scan.

In the **Exclusion mask** field, specify a mask for names of computers that must be excluded from discovery. The mask can contain an asterisk (*) that stands for zero or more characters. You can specify multiple masks separated with commas.

Select the **Ignore offline computers** check box to exclude from discovery computers that did not contact a domain controlled for 30 days or longer.

9. At the **Access Account** step of the wizard, specify credentials of an account that the master agent will use to connect to computers within the discovery scope. The account must have local Administrator permissions on all discovered computers.

If you have specified a discovery account in the master agent configuration settings, select the **Use credentials specified in the master agent configuration** check box. For details on specifying master agent configuration settings, see **Step 1. Install and Configure Master Agent**.
Credentials specified in the master agent configuration take precedence over credentials specified in the discovery rule. For discovery, the master agent will use an account specified in its configuration settings. In case this account is not valid or not set, the master agent will use an account specified in the discovery rule.

10. At the Organizational Units step of the wizard, select organizational units that must be scanned for discovered computers.

   This step of the wizard is available if at the Active Directory Discovery step you have selected the Select from organizational units option.

   a. Click a link in the Locations column for the necessary company.

   b. In the Locations window, click an organizational unit link for the necessary company location.

   c. In the Organizational Units window, select check boxes next to units that must be included to the discovery scope.

   d. In the Organizational Units window, click OK.
11. At the **Discovery Filters** step of the wizard, choose what filters you want to enable for discovery.

- To filter computers by OS type, select **By OS type** in the list and click **Edit**. In the **Operating System** window, select the type of OS that must run on discovered computers (**Server operating system**, **Client operating system**). Click **OK**.

- To filter computers by application, select **By application** in the list and click **Edit**. In the **Application** window, select applications that must run on discovered computers (**Microsoft Exchange Server**, **Microsoft SQL Server**, **Microsoft Active Directory**, **Microsoft SharePoint**, **Oracle**, **Other Applications**). Click **OK**.

- To filter computers by platform, select **By platform** in the list and click **Edit**. In the **Platform** window, select platforms on which discovered computers must run (**Microsoft Hyper-V and VMware vSphere**, **Physical computers**, **Microsoft Azure**, **Amazon Web Services**, **Other**). Click **OK**.

- If you want to perform discovery among accessible computers only, select the **Do not show inaccessible computers** check box.
NOTE:

Different types of filter conditions are joined using Boolean AND operator. For example, if you enable filters *Server operating system, Microsoft SQL Server* and *VMware vSphere*, the list of discovered computers will include only VMware vSphere VMs that run Windows Server OS and Microsoft SQL Server.

12. At the **Email Notification** step of the wizard, you can enable notifications about discovery results by email.

   a. Select the **Send notifications** check box and specify a schedule according to which email notifications must be sent.

   b. In the **Subject** field, specify the subject of the notification.

   c. In the **To** field, specify an email address at which the email notification must be sent.
d. Select the **Send notification email after the first run** check box if a notification about discovery results must be sent after the first run of the discovery rule, regardless of the specified schedule.

13. At the **Backup Agent Deployment** step of the wizard, specify whether you want to install Veeam backup agents on discovered computers:

   a. If you do not want to install Veeam backup agents as part of the discovery process, leave the **Discover remote computer without installing backup agent** option selected.

   b. If after discovery Veeam backup agents must be installed automatically, select the **Discover remote computer, install backup agent and assign the selected backup policy** option.

      From the **Backup policy to apply** list, choose a backup policy that must be assigned immediately after installation. To view the selected policy details, click the **Show** link. If you do not want to assign any backup policy after installation, choose **No policy** from the list.

      If you do not have the necessary backup policy configured yet, you can click the **Create New** link to create a new policy, without exiting the **New Rule** wizard. For details on backup policies, see **Configuring Backup Policies**.

   c. By default, the read-only access mode is enabled for all Veeam backup agents installed as part of discovery. To disable the read-only access mode for Veeam backup agents on discovered computers, set the **Enable read only UI access for the backup agent** toggle to **Off**.
For details on the read-only access mode for Veeam backup agents, see Enabling Read-Only Access Mode.

14. At the Summary step of the wizard, review discovery rule settings.

   a. To start discovery after you save the rule, select the Launch the discovery rule when I click Finish check box.

      If you do not select this check box, you will need to launch discovery later. For details, see Running Discovery.
b. Click **Finish**.

### Configuring Import-Based Discovery Rules

Import-based discovery rules allow you to discover computers using a list of computer IP addresses or DNS names imported from a CSV file.

### Prerequisites

Before you configure an import-based discovery rule:

- Deploy a master agent on a machine in the company infrastructure.
  
  For details, see **Step 1. Install and Configure Master Agent**.

- Make sure you have an account with local Administrator permissions on all computers that you want to discover.
  
  This prerequisite is not required if you have specified a discovery account in the master agent configuration settings. For details, see **Step 1. Install and Configure Master Agent**.

- Make sure that remote computers are powered on and configured to allow discovery: the *Remote Scheduled Tasks Management (RPC and RPC-EPMAP)* firewall rules must allow inbound traffic.

- On remote computers that run a Windows desktop OS, the *Windows Management Instrumentation (WMI-In)* firewall rule must be configured allow inbound traffic.

- Prepare a properly formed CSV file with the list of computer IP addresses or DNS names to scan.
  
  For details, see **Preparing CSV File for Import**.

- If you plan to install Veeam backup agents as part of the discovery procedure, make sure that remote computers are configured to allow installation: the *File and Printer Sharing (SMB-In)* firewall rule must allow inbound traffic.
If you plan to assign a backup policy as part of the discovery procedure, create a new backup policy or check and if necessary customize one of the predefined policies. For details, see Configuring Backup Policies.

Preparing CSV File for Import

To perform import-based discovery, you must create a CSV file with a list of computer IP addresses or DNS names to scan during discovery.

Delimit IP addresses and DNS names in the list with commas:

```
172.17.53.10,srv10,172.17.53.12,win2012r2,172.17.53.22
```

Alternatively, form a file where each new IP address or DNS name is on a new line:

```
172.17.53.10
srv10
172.17.53.12
win2012r2
172.17.53.22
```

Configuring Import-Based Discovery Rule

To configure an import-based discovery rule:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Rules.
   Veeam Availability Console will launch the New Rule wizard.
4. **At the Rule Name** step of the wizard, specify a discovery rule name.

![New Rule screenshot](image1)

5. **At the Companies** step of the wizard, choose one or more companies for which the discovery rule is configured. Use the search field at the top of the list to find the necessary companies.

![New Rule screenshot](image2)

6. **Click a link in the Locations column, then click a link in the Master Agent column, and select a management agent that will be used as the master agent for discovery in each company location.**

   By default, discovery is performed in all company locations where you deployed a master agent. If you
choose to perform discovery in multiple locations, after you complete the wizard steps, Veeam Availability Console will create a separate discovery rule for each location. If you do not want to perform discovery in some company locations, clear check boxes next to these locations.

For details on working with company locations, see Managing Locations.

7. At the **Discovery Method** step of the wizard, select *Computers from CSV file.*

8. At the **CSV File** step of the wizard, click **Browse** and specify a path to a CSV file that contains a list of IP
addresses or DNS names of computers that must be scanned.

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Companies</th>
<th>Discovery Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSV File</td>
<td>Access Account</td>
<td>Discovery Filters</td>
</tr>
<tr>
<td></td>
<td>Email Notification</td>
<td>Backup Agent Deployment</td>
</tr>
<tr>
<td></td>
<td>Summary</td>
<td></td>
</tr>
</tbody>
</table>

9. **At the Access Account** step of the wizard, specify credentials of an account that the master agent will use to connect to computers within the discovery scope. The account must have local Administrator permissions on all discovered computers.

If you have specified a discovery account in the master agent configuration settings, select the **Use credentials specified in the master agent configuration** check box. For details on specifying master agent configuration settings, see *Step 1. Install and Configure Master Agent*. 

For information on supported files format, please open the link.

For more details on the CSV file format, please refer to the Veeam Availability Console User Guide.
Credentials specified in the master agent configuration take precedence over credentials specified in the discovery rule. For discovery, the master agent will use an account specified in its configuration settings. In case this account is not valid or not set, the master agent will use an account specified in the discovery rule.

10. At the **Discovery Filters** step of the wizard, choose what filters you want to enable for discovery.

   - To filter computers by OS type, select **By OS type** in the list and click **Edit**. In the **Operating System** window, select the type of OS that must run on discovered computers (*Server operating system, Client operating system*). Click **OK**.

   - To filter computers by application, select **By application** in the list and click **Edit**. In the **Application** window, select applications that must run on discovered computers (*Microsoft Exchange Server, Microsoft SQL Server, Microsoft Active Directory, Microsoft SharePoint, Oracle, Other Applications*). Click **OK**.

   - To filter computers by platform, select **By platform** in the list and click **Edit**. In the **Platform** window, select platforms on which discovered computers must run (*Microsoft Hyper-V and VMware vSphere, Physical computers, Microsoft Azure, Amazon Web Services, Other*). Click **OK**.

   - If you want to perform discovery among accessible computers only, select the **Do not show inaccessible computers** check box.
NOTE:

Different types of filter conditions are joined using Boolean AND operator. For example, if you enable filters *Server operating system, Microsoft SQL Server* and *VMware vSphere*, the list of discovered computers will include only VMware vSphere VMs that run Windows Server OS and Microsoft SQL Server.

11. At the **Email Notification** step of the wizard, you can enable notifications about discovery results by email.
   
   a. Select the **Send notifications** check box and specify a schedule according to which email notifications must be sent.
   
   b. In the **Subject** field, specify the subject of the notification.
   
   c. In the **To** field, specify an email address at which the email notification must be sent.
d. Select the **Send notification email after the first run** check box if a notification about discovery results must be sent after the first run of the discovery rule, regardless of the specified schedule.

12. At the **Backup Agent Deployment** step of the wizard, specify whether you want to install Veeam backup agents on discovered computers:

   a. If you do not want to install Veeam backup agents as part of the discovery process, leave the **Discover remote computer without installing backup agent** option selected.

   b. If after discovery Veeam backup agents must be installed automatically, select the **Discover remote computer, install backup agent and assign the selected backup policy** option.

      From the **Backup policy to apply** list, choose a backup policy that must be assigned immediately after installation. To view the selected policy details, click the **Show** link. If you do not want to assign any backup policy after installation, choose **No policy** from the list.

      If you do not have the necessary backup policy configured yet, you can click the **Create New** link to create a new policy, without exiting the **New Rule** wizard. For details on backup policies, see **Configuring Backup Policies**.

   c. By default, the read-only access mode is enabled for all Veeam backup agents installed as part of discovery. To disable the read-only access mode for Veeam backup agents on discovered computers, set the **Enable read only UI access for the backup agent** toggle to **Off**.
For details on the read-only access mode for Veeam backup agents, see Enabling Read-Only Access Mode.

13. At the **Summary** step of the wizard, review discovery rule settings.

   a. To start discovery after you save the rule, select the **Launch the discovery rule when I click Finish** check box.

   If you do not select this check box, you will need to launch discovery later. For details, see **Running Discovery**.
b. Click Finish.

Running Discovery

After you configure discovery rules, you must run them to perform discovery. You can run discovery manually or schedule automatic discovery.

Running Discovery Manually

To run discovery manually:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Rules.
3. Select one or more discovery rules in the list.
4. At the top of the discovery rules list, click Run.
5. Wait until the discovery rule state changes its value from Running to Success.

Scheduling Discovery

Instead of running discovery manually, you can configure a schedule according to which discovery must be performed. In this case, discovery will run with a specified periodicity. If new computers complying with a discovery rule appear in the company network, Veeam Availability Console will add them to the list of discovered computers (and optionally, install Veeam backup agents and assign a backup policy, if the discovery rule is configured to perform these tasks).

To schedule automatic discovery:
1. Log in to Veeam Availability Console.  
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Rules.
3. Select the necessary discovery rule in the list.
4. At the top of the discovery rules list, click Schedule.
5. In the Discovery Rule Schedule window, select Daily at and specify a schedule according to which discovery must be performed:
   - To schedule daily discovery, select Everyday. In the Daily at list, choose the time of the day when discovery must run.
   - To schedule discovery on specific week days, select Selected days, click Days and specify week days on which discovery must run, and click OK. In the Daily at list, choose the time of the day when discovery must run.
6. Click Apply.

### Resetting Discovered Computers

To remove from the Discovered Computers list computers that were found with a discovery rule, you can reset discovery results. For example, this can be required if you improperly configured a discovery rule, discovery results display more computers than expected, or discovery results include computers that must not be protected with Veeam backup agents.

When you perform reset for a discovery rule, computers discovered with this rule are removed from the discovered computers list. However, computers on which Veeam Availability Console management agents are already installed and configured to communicate with Veeam Availability Console will be moved to the list of computers discovered by the External Discovery rule.

To reset discovery results:
1. Log in to Veeam Availability Console.  
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Rules.
3. Select one or more discovery rules in the list.
4. At the top of the discovery rules list, click **Reset Discovered Computers**.

The number of computers discovered with a rule will be set to zero, and computers that do not run management agents will be removed from the list of discovered computers.

**Viewing and Exporting Discovery Results**

You can view results of a performed discovery and export the list of discovered computers to a CSV or XML file.

**Viewing Discovered Computers**

To view the list of discovered computers:

1. Log in to Veeam Availability Console. For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click **Rules**.
3. Do one of the following:
   - Click the **Total Computers** link to view computers discovered by a specific discovery rule.
   - Select a rule in the list and click **View Discovered Computers**.
4. On the **Discovered Computers** tab of the **Managed Computers** section, you can apply the following filters to narrow down the list of discovered computers:
   - **Rule** — limit the list of computers by discovery rule.
     Choose **External Discovery** to display computers that were not discovered with discovery rules, but rather with the help of Veeam Availability Console management agents running on these computers.
   - **Hostname** — search discovered computers by host name.
   - **Connection status** — limit the list of computers by its connection status (**Online**, **Not Accessible**, **Rejected**).
   - **Agent status** — limit the list of computers by the Veeam Availability Console management agent connection status (**Installed**, **Warning**, **Inaccessible**, **Not Installed**).
   - **Platform type** — limit the list of computers by platform type (**vSphere and Hyper-V**, **Physical computers**, **Other**, **N/A**).
   - **OS type** — limit the list of computers by OS type supported by Veeam Availability Console (**Supported**, **Unsupported**, **Undefined**).
- **Agent version** — limit the list of computers by agent version *(Up-to-date, N/A, Out-of-date, Patch available)*.

Each computer in the list is described with a set of properties. By default, some properties in the list are hidden. To display additional properties, click the ellipsis on the right of the list header and choose properties that must be displayed.

- **Company** — company to which a computer belongs.
- **Site** — name of the Veeam Cloud Connect site on which the company is registered.
- **Location** — location to which a computer belongs.
- **Rule Name** — name of a discovery rule that was used to discover a computer.
  
  *External Discovery* means that a computer was not discovered with a discovery rule, but rather with the help of a Veeam Availability Console management agent running on these computers.

- **Platform** — computer platform type *(vSphere, Hyper-V, Physical, Other, N/A)*.
- **Hostname** — computer name.
- **Type** — computer type *(Server, Workstation, N/A)*.
- **Guest OS** — guest OS installed on a computer.
- **Application** — applications installed on a computer *(Microsoft Exchange Server, Microsoft SQL Server, Microsoft Active Directory, Microsoft SharePoint, Oracle, Other, N/A)*.
- **Computer Connection** — computer connection status *(Online, Not Accessible, Rejected)*.
- **Agent Deployment** — status of the Veeam backup agent deployment *(Success, Failed, Warning)*.
- **Deployment Progress** — progress of the Veeam backup agent deployment, in percent.
- **Agent Status** — Veeam Availability Console management agent connection status *(Installed, Warning, Inaccessible, Not Installed)*.
- **Agent Version** — version of a Veeam Availability Console management agent *(Up-to-date, N/A, Not installed, Out-of-date, Patch available)*.
- **Backup Policy** — name of a backup policy assigned to a Veeam backup agent.
- **IP Address** — computer IP address.
- **MAC Address** — computer MAC address.
- **Discovery Time** — date and time when a computer was discovered.
- **Agent Role** — role of a Veeam Availability Console management agent (Master, Client, N/A).
- **Connection Account** — account under which a Veeam Availability Console management agent connects to Veeam Availability Console.
- **Last Heartbeat** — time period since a Veeam Availability Console management agent sent the latest heartbeat to Veeam Availability Console.
- **Reboot Required** — indicates whether computer reboot is required.

### Exporting Discovered Computers

You can export discovered computer details to a **CSV** or **XML** file:

1. Log in to Veeam Availability Console. For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click **Managed Computers**.
3. Open the **Discovered Computers** tab.
4. Apply the necessary filters.
5. Click **Export** and choose a format of the exported data:
   - **Export CSV** — choose this option to structure exported data as a **CSV** file.
   - **Export XML** — choose this option to structure exported data as an **XML** file.

The file with exported data will be saved to the default download location on your computer.

### Step 3. Initiate Installation Procedure

Install Veeam backup agents and Veeam Availability Console management agents on discovered computers.

**NOTE:**

This step is not required if you configured discovery rules to install Veeam backup agents. In this case, installation of Veeam backup agents and management agents will be initiated automatically after discovery.

### Prerequisites

Before you install Veeam backup agents:

- Make sure that remote computers are configured to allow installation: the **File and Printer Sharing (SMB-In)** firewall rule must allow inbound traffic.
- Make sure that the machine that hosts the master agent is powered on, has connection to the Internet, and can access discovered computers.
- Make sure you have an account with local Administrator permissions on all client computers.
This account will be used to upload Veeam backup agent setup files to client computers and perform installation.

- If you plan to assign a backup policy as part of the installation procedure, create a new backup policy or check and if necessary customize one of the predefined policies.

For details, see Configuring Backup Policies.

### Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

### Installing Veeam Backup Agents

To install Veeam backup agents and Veeam Availability Console management agents on discovered computers:

1. Log in to Veeam Availability Console.
   
   For details, see Accessing Veeam Availability Console.

2. In the menu on the left, click Managed Computers.

3. Open the Discovered Computers tab.

4. Select check boxes next to the necessary computers.

5. At the top of the list, click Install Backup Agent.

   The Install Backup Agent window will be displayed.

6. In the Use guest OS credentials from section, select an account that will be used to upload setup files to remote computers and start installation.

   The account must have local Administrator permissions on computers where you want to install Veeam backup agents.

   - Select Account specified in the discovery rule or in the management agent settings if you want to use for installation the same account that you specified for discovery of client computers, either in the master agent configuration or in the discovery rule settings.

   - Select The following user account if you want to specify an account different from the one that you used for discovery. You can select an account from the list or click Create New to specify credentials for a new account.

7. In the Backup policy to apply list, choose a backup policy that must be applied as part of the installation process.

   The chosen backup policy will be used to configure backup job settings after installing Veeam backup agents. You can select No policy if you do not want to configure backup job settings as part of installation.

   To configure a new backup policy, click Create New and configure a new backup policy. For details, see Configuring Backup Policies.

8. By default, the read-only access mode is enabled for all Veeam backup agents. To disable the read-only access mode for Veeam backup agents, set the Enable read only UI access for the backup agent toggle to Off.

   For details on the read-only access mode for Veeam backup agents, see Enabling Read-Only Access Mode.
9. Click **Apply**.

10. Wait for the installation process to complete.
   The installation process may take up to several minutes.

Checking Installation Results

To make sure that installation of Veeam backup agents has completed successfully, complete the following steps:

1. Log in to Veeam Availability Console.
   For details, see [Accessing Veeam Availability Console](#).

2. In the menu on the left, click **Managed Computers**.

3. Open the **Discovered Computers** tab and find the necessary computers in the list.

4. Check the value in the **Agent Deployment** and **Deployment Progress** columns.
   If installation was successful, the **Agent Deployment** status must be **Success**, and the **Deployment Progress** must be **100%**.

5. Click a link in the **Agent Deployment** column to display session details of the installation procedure.
   In some cases, after installation you might need to perform additional operations. For example, if the setup detects a pending computer reboot, the list of installation session details, will display a warning notifying that reboot is required. To complete the installation, you can initiate computer reboot in Veeam Availability Console. For details, see [Rebooting Remote Computers](#).
Installing Veeam Backup Agents with 3rd Party Automation Tools (GPO Example)

You can use 3rd party automation tools to streamline deployment of Veeam backup agents and Veeam Availability Console management agents. This section provides guidelines on how to automate deployment using Windows Group Policies.

This method does not require you to perform preliminary discovery of remote computers in Veeam Availability Console.

Prerequisites

Before you install Veeam backup agents, check the following prerequisites:

- Make sure you have an account with local Administrator permissions on all computers.
- If you plan to apply a backup policy as part of the installation procedure, create a new backup policy or check and if necessary customize one of the predefined policies.
  
  For details, see Configuring Backup Policies.

Required Details

Obtain the following data from the service provider:

- FQDN or IP address of a cloud gateway
- Port on the cloud gateway used to transfer backup data to and from cloud repositories
- User credentials for connecting to the service provider (Company Owner credentials)
- Thumbprint of a certificate that is installed on the Veeam Availability Console and Veeam Cloud Connect servers

Installing Veeam Backup Agents

To install Veeam backup agents with 3rd party automation tools, perform the following steps:

1. **Deploy management agents.**
   
   Deploy and configure Veeam Availability Console management agents on client computers using Group Policies.

2. **Install Veeam Backup Agents.**
   
   Install Veeam backup agents on client computers.

Step 1. Deploy Management Agents Using Group Policy

You must create an MST file with custom configuration parameters and use this MST file to deploy the Veeam Availability Console management agents on client computers. The management agents will use parameters specified in the MST file to connect to a cloud gateway on the service provider side.
Step 1.1. Unpack Management Agent Setup Files

Unpack the content of the management agent setup file:

1. Obtain the necessary version of the Veeam Availability Console management agent setup file.
   
   The management agent setup files reside in the C:\Program Files\Veeam\Availability Console\ApplicationServer\AgentPackage folder on the machine where Veeam Availability Console is installed. If you installed Veeam Availability Console using a distributed installation scenario, check this folder on a machine where the Veeam Availability Console Server component runs.

2. Perform installation of the management agent in the administrator mode to unpack the content of the setup file:
   
   a. In the command prompt, run a command to start the Veeam Availability Console Communication Agent wizard.
      
      For example, for the 64-bit version of the management agent, the command must be:
      
      msiexec /a VAC.CommunicationAgent.x64.msi
   
   b. At the Network Location step of the wizard, specify a directory to which setup files must be unpacked.
   
   c. Click Install.

3. Check the output directory and make sure it includes the following items:
   
   - Setup file VAC.CommunicationAgent.x<bit>.msi
   - Folder RealProgramFiles

4. Copy the unpacked files to a network share.

   The network share must be accessible from all client computers on which you want to deploy the management agent.

   Make sure you set at least Read permissions on the files.
Step 1.2. Create MST Configuration File

Create an **MST** configuration file with installation parameters that point to the necessary cloud gateway:

1. In the directory with unpacked setup files, locate the management agent setup file and open it for edit with Orca.
   
   For details on Orca, see Windows Dev Center.

2. In the menu, choose **Transform > New Transform**.

3. In the **Tables** pane, click **Property**.

4. Add the following properties to the table:
   - **ACCEPT_THIRDPARTY_LICENSES** — specifies if you want to accept the terms of the license agreement for the 3rd party components.
     
     Specify 1 if you want to accept the terms and proceed with installation.
   - **ACCEPT_EULA** — specifies if you want to accept the terms of the Veeam license agreement.
     
     Specify 1 if you want to accept the terms and proceed with installation.
   - **CC_GATEWAY** — FQDN or IP address of a cloud gateway.
   - **VAC_TENANT** — user name for connecting to the service provider.
   - **VAC_TENANT_PASSWORD** — password for connecting to the service provider.
     
     You must specify credentials of the Company Owner.
   - **VAC_CERT_THUMBPRINT** — thumbprint of a certificate that is installed on the Veeam Cloud Connect and Veeam Availability Console servers, and used to secure traffic between the service provider and clients.
     
     The thumbprint is used to verify the authenticity of the certificate. Although this property is optional, it is recommended that you specify it.

5. If you have changed the default port number when deploying the cloud gateway, locate the **CC_GATEWAY_PORT** property and change the port value.
   
   For details on the gateway port configuration, see Veeam Cloud Connect Administrator Guide, section **Adding Cloud Gateways**.

6. In the menu, choose **Transform > Generate Transform**.

7. Save the **MST** file with configuration details.

8. Close Orca.

9. Copy the **MST** to a network share.

The network share must be accessible from all client computers on which you want to deploy the management agent.
Make sure you set at least Read permissions on the file.

**Step 1.3. Create Group Policies**

Create a Group Policy that will install and configure the management agent on client computers:

1. Log on to a domain controller.
2. Open the Group Policy Management Console.
3. Right-click the OU which includes computers on which management agents must be deployed, and choose to create a new Group Policy Object.
4. Right-click the Group Policy Object and choose Edit.
5. In the left pane of the Group Policy Management Editor, expand Computer Configuration > Policies > Software Settings.
7. In the Open window, point to the management agent setup file located on the network share. This must be the setup file obtained as a result of installation in the administrator mode, as described at Step 1.1.
8. In the Deploy Software window, choose the Advanced deployment method.
9. Open the Modifications tab, click Add and choose the MST file located on the network share.
10. Click OK.
12. Right-click the Always wait for the network at computer startup and logon policy setting and choose Edit.
13. In the policy setting window, select **Enabled** and click **OK**.

14. Close the Group Policy Management Editor.

---

**Step 1.4. Apply Group Policies to Client Computers**

Apply the created Group Policy to client computers.

**Step 2. Install Veeam Backup Agents**

Install Veeam backup agents on client computers. You can use one of the following installation methods.

**Initiating Installation in Veeam Availability Console**

You can initiate installation of Veeam backup agents in Veeam Availability Console. After you initiate installation, Veeam Availability Console management agents on remote computers will download the Veeam backup agent setup file from the Veeam Installation Server over the Internet, install Veeam backup agents and assign a backup policy.
NOTE:

To ensure that Veeam backup agents can be installed on client computers, make sure that:

- Remote computers are powered on.
- Remote computers on which you plan to install Veeam backup agents have access to the Internet.
- Remote computers are configured to allow installation: the File and Printer Sharing (SMB-In) firewall rule must allow inbound traffic.

If for some reason, you cannot download the Veeam backup agent setup file from the Veeam Installation Server, you can obtain the supported version of the setup file and place it by the \C:\ProgramData\Veeam\Veeam Availability Console\AgentPackage\VeeamAgentWindows.exe path on a remote computer. When you initiate installation in Veeam Availability Console, this setup file will be used to install Veeam backup agent on a remote computer. To automate upload of setup files, you can use 3rd party tools, like GPO. For details on how to upload the Veeam backup agent setup file using GPO, see How to Upload Veeam Backup Agent Setup File to Client Computers with GPO.

To initiate Veeam backup agent installation:

1. Log in to Veeam Availability Console as a Company Owner or Location Administrator. For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Managed Computers.
3. Open the Discovered Computers tab.
4. Select check boxes next to the necessary computers.
5. Click Install Backup Agent. The Install Backup Agent window will be displayed.
6. In the Backup policy to apply list, choose a backup policy that must be applied as part of the installation process.
   The chosen backup policy will be used to configure backup job settings after installing Veeam backup agents. You can select No policy if you do not want to configure backup job settings as part of installation.
   To configure a new backup policy, click Create New and configure a new backup policy. For details, see Configuring Backup Policies.
7. By default, the read-only access mode is enabled for all Veeam backup agents. To disable the read-only access mode for Veeam backup agents, set the Enable read only UI access for the backup agent toggle to Off.
   For details on the read-only access mode for Veeam backup agents, see Enabling Read-Only Access Mode.
8. Click Apply.
9. Wait for the installation process to complete.
The installation process may take up to several minutes.

Installing Veeam Backup Agents Outside Veeam Availability Console

You can install Veeam backup agents outside Veeam Availability Console:

1. **Install Veeam backup agents on computers you want to protect.**
   - You can use the installation wizard or install the software in the unattended mode.
   - For details, see Veeam Agent for Microsoft Windows User Guide, sections Installing Veeam Agent for Microsoft Windows and Installing Veeam Agent for Microsoft Windows in the Unattended Mode.

2. **Activate Veeam backup agents in Veeam Availability Console.**
   - For details, see Activating Veeam Backup Agents.
Installing Veeam Backup Agents Manually

You can deploy Veeam backup agents and Veeam Availability Console management agents on client computers manually.

Prerequisites

Before you install Veeam backup agents, check the following prerequisites:

- Obtain the management agent setup file.
  For details, see How to Obtain Management Agent Setup File.
- Make sure you have an account with local Administrator permissions on all computers.
- If you plan to apply a backup policy as part of the installation procedure, create a new backup policy or check and if necessary customize one of the predefined policies.
  For details, see Configuring Backup Policies.

Required Details

Obtain the following data from the service provider:

- FQDN or IP address of a cloud gateway
- Port on the cloud gateway used to transfer backup data to and from cloud repositories
- User credentials for connecting to the service provider (Company Owner credentials)
- Thumbprint of a certificate that is installed on the Veeam Availability Console and Veeam Cloud Connect servers

Installing Veeam Backup Agents

To install Veeam backup agents manually, perform the following steps:

1. **Deploy management agents.**
   Manually deploy and configure Veeam Availability Console management agents on client computers.

2. **Install Veeam backup agents.**
   Install Veeam backup agents on client computers.

Step 1. Deploy Management Agents

Deploy Veeam Availability Console management agents on managed computers, and configure these agents to communicate with Veeam Availability Console:

To install a management agent on a managed computer:

1. Copy the agent setup file to a location accessible from the machine where you want to install the management agent.
2. Log on to the machine as an Administrator.
3. Double-click the agent setup file to launch the Veeam Availability Console Communication Agent wizard.

4. Follow steps of the wizard.

5. At the last step of the wizard, click Install.

6. When installation completes, click Finish to close the wizard.

   The agent will be installed by the following path: %ProgramFiles%\Veeam\Availability Console\CommunicationAgent.

To configure a management agent:

1. In the icon tray, right-click the management agent icon and choose Agent Settings.

   If the icon is hidden, display hidden icons, find Veeam.MBP.Agent.Configurator in the list of notification area icons, and choose to show the icon and notifications for it.

2. In the Management Agent Settings window, specify settings that the agent must use to connect to Veeam Availability Console.

   a. In the Cloud Gateway field, type FQDN or IP address of a cloud gateway.

   b. In the Port field, specify the port on the cloud gateway that is used to transfer data to Veeam Availability Console.

   c. In the Username and Password fields, type user credentials of a Company Owner.

      The user name must be provided in the <Company Name>User> format.

3. In the Management Agent Settings window, click Apply.

   Management agent will connect to Veeam Availability Console server, download the security certificate and perform its verification.

   In case of errors during certificate verification you will be prompted the Security Certificate Preview window:

   • To view error details, at the top of the window, click the Learn more link.

   • To ignore the error and continue agent configuration, click Save.

4. In the Management Agent window, click Restart to restart the management agent and apply connection settings.
5. Wait for the agent to connect to Veeam Availability Console.
   When the agent connects to Veeam Availability Console, the status in the Veeam Master Agent Settings window will be displayed as Connected. The agent icon in the icon tray will turn blue.

6. In the Management Agent Settings window, click Close.

Step 2. Install Veeam Backup Agents

Install Veeam backup agents on client computers. You can use one of the following installation methods.

Initiating Installation in Veeam Availability Console

You can initiate installation of Veeam backup agents in Veeam Availability Console. After you initiate installation, Veeam Availability Console management agents on remote computers will download the Veeam backup agent setup file from the Veeam Installation Server over the Internet, install Veeam backup agents and assign a backup policy.

NOTE:

To ensure that Veeam backup agents can be installed on client computers, make sure that:

- Remote computers are powered on.
- Remote computers on which you plan to install Veeam backup agents have access to the Internet.
- Remote computers are configured to allow installation: the File and Printer Sharing (SMB-In) firewall rule must allow inbound traffic.

If for some reason, you cannot download the Veeam backup agent setup file from the Veeam Installation Server, you can obtain the supported version of the setup file and place it by the C:\ProgramData\Veeam\Veeam Availability Console\AgentPackage\VeeamAgentWindows.exe path on a remote computer. When you initiate installation in Veeam Availability Console, this setup file will be used to install Veeam backup agent on a remote computer. To automate upload of setup files, you can use 3rd party tools, like GPO. For details on how to upload the Veeam backup agent setup file using GPO, see How to Upload Veeam Backup Agent Setup File to Client Computers with GPO.

To initiate Veeam backup agent installation:

1. Log in to Veeam Availability Console as a Company Owner or Location Administrator.
   For details, see Accessing Veeam Availability Console.

2. In the menu on the left, click Managed Computers.

3. Open the Discovered Computers tab.

4. Select check boxes next to the necessary computers.

5. Click Install Backup Agent.
   The Install Backup Agent window will be displayed.

6. In the Backup policy to apply list, choose a backup policy that must be applied as part of the installation process.
   The chosen backup policy will be used to configure backup job settings after installing Veeam backup agents. You can select No policy if you do not want to configure backup job settings as part of installation.
To configure a new backup policy, click Create New and configure a new backup policy. For details, see Configuring Backup Policies.

7. By default, the read-only access mode is enabled for all Veeam backup agents. To disable the read-only access mode for Veeam backup agents, set the Enable read only UI access for the backup agent toggle to Off.

   For details on the read-only access mode for Veeam backup agents, see Enabling Read-Only Access Mode.

8. Click Apply.

9. Wait for the installation process to complete.

   The installation process may take up to several minutes.

Installing Veeam Backup Agents Outside Veeam Availability Console

You can install Veeam backup agents outside Veeam Availability Console:

1. Install Veeam backup agents on computers you want to protect.

   You can use the installation wizard or install the software in the unattended mode.

   For details, see Veeam Agent for Microsoft Windows User Guide, sections Installing Veeam Agent for Microsoft Windows and Installing Veeam Agent for Microsoft Windows in the Unattended Mode.


   For details, see Activating Veeam Backup Agents.
Activating Veeam Backup Agents

Veeam backup agents can operate in two modes: *unmanaged* and *managed*.

- **Unmanaged** — in this mode, Veeam backup agents cannot be managed in Veeam Availability Console. Unmanaged Veeam backup agents include:
  - Standalone Veeam backup agents that run either a free or a paid product version.
  - Veeam backup agents managed by client Veeam Backup & Replication servers.

  End users working with Veeam backup agents directly can access all available functions, update the product and submit support cases to Veeam Software in the Control Panel.

- **Managed** — in this mode, Veeam backup agents can be managed in Veeam Availability Console. You can configure backup job settings, start and stop backup, change global settings, update and uninstall Veeam backup agents, and collect Veeam backup agent data for monitoring and billing.

  End users working with managed Veeam backup agents directly can perform most operations, with the following exceptions:
  - Users cannot submit a support case to Veeam Software in the Veeam backup agent Control Panel. To obtain support, users must contact their backup administrator.
  - Users cannot update Veeam backup agents in the Control Panel. Automatic updates are also disabled. To update Veeam backup agents, users must contact their backup administrator.
  - Users cannot install or change a license, and cannot switch Veeam backup agent to another edition.

  The role of the backup administrator can be performed by the service provider or by a backup administrator in the managed company.

  In the managed mode, Veeam backup agent Control Panel displays the name of the service provider company at the top left corner. The *About* section in the Control Panel displays a notification saying that the license and edition are managed by administrator.

To manage Veeam backup agents in Veeam Availability Console and monitor the state of computer data protection, you must activate Veeam backup agents. Every activated Veeam backup agent requires one or more Veeam Availability Console licenses, depending on the computer platform and the backup job mode.
NOTE:

- When you install Veeam backup agents using discovery rules, or initiate Veeam backup agent installation in Veeam Availability Console, Veeam backup agents are activated automatically. You must manually activate Veeam backup agents only if Veeam backup agents were installed outside Veeam Availability Console (for example, using GPO), and therefore were not registered in Veeam Availability Console.
- To activate Veeam backup agents managed by client Veeam Backup & Replication servers, you must remove these agents from Veeam Backup & Replication console first. For details, see Veeam Agent Management Guide.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Activating Veeam Backup Agents

To activate Veeam backup agents on client computers:

1. Log in to Veeam Availability Console. For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Managed Computers.
3. Open the Discovered Backup Agents tab.
4. Select the necessary Veeam backup agents in the list.
   - To display all unmanaged Veeam backup agents in the list, click Filter, and in the Filter by installed license section select Not activated (Unmanaged) and click Apply.
5. Click Activation and choose Switch to Managed Mode.

After you activate a Veeam backup agent, Veeam Availability Console will assign one or more licenses to it. The Veeam backup agent license status will be set to Managed. The number of used and total licenses in the Veeam Availability Console license pool will be updated.

Switching Veeam Backup Agents to Unmanaged Mode

To switch Veeam backup agents to the unmanaged mode:

1. Log in to Veeam Availability Console. For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Managed Computers.
3. Open the Discovered Backup Agents tab.
4. Select the necessary Veeam backup agents in the list.
   - To display all managed Veeam backup agents in the list, click Filter, in the Filter by installed license section select Activated (Managed) and click Apply.
5. Click Activation and choose Switch to Unmanaged Mode.
After you switch Veeam backup agents to the unmanaged mode, Veeam Availability Console will revoke licenses from it. The number of used and total licenses in the Veeam Availability Console license pool will be updated.
Configuring Backup Job Settings

In Veeam Availability Console, you can configure Veeam backup agent job settings on computers you want to protect.

There are two methods to configure Veeam backup agent job settings:

- **Configure and assign backup policies**
  
  Backup policies are saved templates that describe backup job configuration and can be assigned to one or more Veeam backup agents. You can use this method if Veeam backup agent jobs have not been configured on managed computers yet, or if you want to change settings of previously configured jobs on multiple computers.

- **Configure backup job settings on individual computers**
  
  You can use this method if you need to configure a backup job on a single computer. You can configure backup job from predefined template or from scratch. You cannot use this method to configure backup job settings on multiple computers.
Configuring Backup Policies

To configure Veeam backup agent job settings on a managed computer from scratch, you must assign a backup policy to it. A backup policy describes configuration of a Veeam backup agent job and can be used as a saved template. Backup policies speed up the process of configuring backup job settings on managed computers: instead of specifying backup job settings manually, you can apply settings from a preconfigured backup policy to a group of computers. For details, see Assigning Backup Policies.

By default, Veeam Availability Console includes two predefined backup policies:


In addition to predefined backup policies, you can create multiple custom backup policies with different configuration settings and assign them to different groups of computers. For example, you can configure backup policies for different machine types, applications, companies and so on.

Backup policies can be configured in the Veeam Availability Console Administrator Portal, Reseller Portal and Client Portal. Predefined backup policies and public policies configured by the Portal Administrator are available to all resellers in the Reseller Portal and all companies in the Client Portal. Public backup policies configured by Service Provider Administrator in the Reseller Portal are available to all companies managed by this reseller. Backup policies configured by Company Owner or Location Administrators and private policies configured by the Portal Administrator or Service Provider Global Administrator for a company are available to this company only, but can be managed in the Administrator Portal and Reseller Portal.

Creating Backup Policies

You can create custom backup policies with Veeam backup agent job settings that will suit your data protection requirements for managed computers.

Before you create a backup policy, check prerequisites described in Before You Begin.

To create a backup policy, complete the following steps:

1. Launch the New Backup Policy wizard.
2. Specify the job template name and description.
3. Choose the backup agent operation mode.
4. Choose the backup mode.
5. Choose volumes to back up.
6. Choose folders to back up.
7. Choose backup destination.
8. Specify local storage settings.
10. Specify backup server settings.
11. Specify backup repository settings.
12. Specify cloud backup settings.
13. Specify cloud repository quota.
15. Choose backup cache location.
16. Specify guest OS processing options.
17. Configure backup schedule.
18. Review backup job settings.

Before You Begin

Before you configure a backup policy, check the following prerequisites:

- The target location where you plan to store backup files must have enough free space.
- The number of jobs that you can assign to a Veeam backup agent depends on the product edition. For details on the limitation of the number of jobs, see Veeam Agent for Microsoft Windows User Guide, section Backup Job.
- [For Veeam Backup & Replication repository targets] You can store created backups in a backup repository only if the backup server runs Veeam Backup & Replication 9.5 Update 3 or later.
- [For Veeam Backup & Replication repository targets] If you plan to use a Veeam Backup & Replication repository as a target for backups, you must pre-configure user access permissions on this backup repository. For details, see Veeam Agent for Microsoft Windows User Guide, section Setting Up User Permissions on Backup Repositories.

Backup has the following limitations:

- You cannot save the backup of entire computer on the local computer disk. Use an external hard drive or USB drive, network shared folder or backup repository as a target location.
- Veeam Agent for Microsoft Windows does not back up data to which symbolic links are targeted. It only backs up the path information that the symbolic links contain. After restore, identical symbolic links are created in the restore destination.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Step 1. Launch New Backup Policy Wizard

To launch the New Backup Policy wizard:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. At the top right corner of the Veeam Availability Console window, click Configuration.
3. In the configuration menu on the left, click Backup Policies.
4. At the top of the list, click New.
   Veeam Availability Console will launch the New Backup Policy wizard.
Step 2. Specify Backup Policy Name and Description

At the **Backup Policy Name** step of the wizard, specify name and description of the backup policy.

![Backup Policy Name](image)

**Operation Mode**
- **Server** — choose this mode for computers running a server OS version.
  
  This mode supports application-aware processing, files indexing and flexible backup job schedule, and is designed to protect application servers.

Step 3. Choose Backup Agent Operation Mode

At the **Operation Mode** step of the wizard, select the operation mode:

- **Server** — choose this mode for computers running a server OS version.
  
  This mode supports application-aware processing, files indexing and flexible backup job schedule, and is designed to protect application servers.
**Workstation** — choose this mode for end users’ computers running a workstation OS version.

This mode provides user-friendly job schedule, and is designed to protect end user computers.

### Step 4. Choose Backup Mode

At the **Backup Mode** step of the wizard, select the mode in which you want to create a backup:

- **Entire computer** — select this option if you want to create a backup of the entire computer image. When you restore data from such backup, you will be able to recover the entire computer image as well as data on specific computer volumes: files, folders, application data and so on. With this option selected, you will pass to the **Destination** step of the wizard.

  If you want to include in the backup one or more external USB drives, select the Include external USB drives check box. With this option selected, Veeam backup agent will include in the backup all supported external drives that are connected to the managed computer at the time when the backup job starts. Veeam backup agent supports backup of external drives that support Microsoft VSS: HDD, SSD, and so on. USB flash drives (USB sticks) are not supported. For details, see [Veeam Agent for Microsoft Windows User Guide](#), section *Backup of External Drives*.

- **Volume level backup** — select this option if you want to create a backup of specific computer volumes, for example, all volumes except the system one. When you restore data from such backup, you will be able to recover data on these volumes only: files, folders, application data and so on. With this option selected, you will pass to the **Volumes** step of the wizard.

- **File level backup** — select this option if you want to create a backup of individual folders on your computer. With this option selected, you will pass to the **Files** step of the wizard.
**TIP:**

File-level backup is typically slower than volume-level backup. Depending on the performance capabilities of your computer and backup environment, the difference between file-level and volume-level backup job performance may increase significantly. If you plan to back up all folders with files on a specific volume or back up large amount of data, it is recommended that you configure volume-level backup instead of file-level backup.

---

**Step 5. Choose Volumes to Back Up**

The **Volumes** step of the wizard is available if at the **Backup Mode** step you have chosen to create a volume-level backup.

In the **Objects to backup** list, specify volumes that you want to include in the backup scope:

1. In the text field, type a drive letter and click **Add**.
   
   The drive letter must be specified in the following format: **C:**

2. Repeat step 1 for all volumes that you want to add to the backup scope.
NOTE:

1. When you include a system volume in the backup, Veeam backup agent automatically includes the System Reserved/UEFI or other system partitions in the backup too.

2. Veeam backup agent automatically adds to the list of exclusions the following Microsoft Windows objects for all computer users: temporary files folder, Recycle Bin, Microsoft Windows pagefile, hibernate file and VSS snapshot files from the System Volume Information folder.

---

**Step 6. Choose Folders to Back Up**

The **Files** step of the wizard is available if at the **Backup Mode** step you have chosen to create a file-level backup.

In the file-level backup mode, you can create two types of backups:

- File-level backup that includes individual folders on the computer.
- Hybrid backup that contains individual folders and specific volumes of the computer.

In the **Objects to backup** list, specify folders that you want to include in the backup scope:

1. In the **Objects to backup** field, type a folder path and click **Add**.
   
   You can specify a drive letter at this step. In this case, Veeam backup agent will add the whole volume to the backup.
   
   Repeat this step for all folders that you want to add to the backup.

2. Select the **Operating system** check box to include in the backup data pertaining to the OS installed on the computer.
3. Select the **Personal files** check box to include in the backup the user profile folder, including all user settings and data. Typically, the user profile data is stored in the **Users** folder on the system disk, for example, `C:\Users`.

---

### Configuring Filters

To include or exclude files of a specific type in/from the backup scope, you can configure filters:

1. At the **Files** step of the wizard, click **Advanced**.

2. Specify include and exclude filters for files you want to back up:
   - In the **Include masks** field, specify file names and/or masks for file types that you want to back up, for example, `MyMovie.avi`, `*filename*`, `*.docx`, `*.mp3`. Veeam backup agent will create a backup only for selected files. Other files will not be backed up.
   - In the **Exclude masks** field, specify file names and/or masks for file types that you do not want to back up, for example, `OldPhotos.rar`, `*.tmp`, `*.back`. Veeam backup agent will back up all files except files of the specified type.

3. Click **Add**.

4. Repeat steps 2–3 for each mask that you want to add.

You can use a combination of include and exclude masks. Note that exclude masks have a higher priority than include masks. For example, you can specify masks in the following way:

- **Include mask**: `*.avi`
- **Exclude mask**: `*movie*`
Veeam backup agent will include in the backup all files of the AVI format that do not contain 'movie' in their names.

**NOTE:**

Veeam backup agent automatically adds to the list of exclusions the following Microsoft Windows objects for all computer users: temporary files folder, Recycle Bin, Microsoft Windows pagefile, hibernate file and VSS snapshot files from the System Volume Information folder.

**Step 7. Choose Backup Destination**

At the **Destination** step of the wizard, select a target location for the created backup:

- **Local storage** — select this option if you want to save the backup on a removable storage device attached to the endpoint, or on a local drive of the endpoint. With this option selected, you will pass to the **Local Storage** step of the wizard.

- **Shared folder** — select this option if you want to save the backup in a network shared folder. With this option selected, you will pass to the **Shared Folder** step of the wizard.

- **Veeam Backup & Replication repository** — select this option if you want to save the backup on a backup repository managed by a Veeam Backup & Replication server. With this option selected, you will pass to the **Backup Server** step of the wizard.

- **Cloud Connect Repository** — select this option if you want to save the backup on a cloud repository exposed by the Veeam Cloud Connect service provider. With this option selected, you will pass to the **Cloud Repository** step of the wizard.
1. It is strongly recommended that you store backups in the external location like USB storage device, shared network folder or in the cloud. You can also keep your backup files on a separate non-system local drive.

2. If you choose to store the backup on a Veeam Backup & Replication repository, you must pre-configure user access permissions on this backup repository. For details, see Veeam Agent for Microsoft Windows User Guide, section Setting Up User Permissions on Backup Repositories.

---

**Step 8. Specify Local Storage Settings**

The **Local Storage** step of the wizard is available if at the **Destination** step you have chosen to save the backup on a local drive of the computer.

Specify local storage settings:

1. In the **Destination target** field, specify a path to the folder where backup files must be stored.
   
   If the folder does not exist, Veeam backup agent will create it during backup.
   
   Do not specify the root drive directory, like `C:` or `D:`.

2. Specify backup retention policy settings:
   
   - [For Workstation operation mode] In the **Keep backups for the past <N> days when computer was running** field, specify the number of days for which you want to store backup files in the target location. By default, Veeam backup agent keeps backup files for 14 days. After this period is over, Veeam backup agent will remove the earliest restore points from the backup chain.
For details, see Veeam Agent for Microsoft Windows User Guide, section Backup Retention Policy in Free and Workstation Editions.

- [For Server operation mode] In the Restore points to keep on disk field, specify the number of restore points you want to keep in the target location. By default, Veeam backup agent keeps 14 latest restore points. After this number is exceeded, Veeam backup agent will remove the earliest restore points from the backup chain.


3. Click Advanced Settings to specify advanced settings for the backup job.

For details, see Specify Advanced Job Settings.

**IMPORTANT!**

1. If you choose to store the backup on a local folder included in the backup scope, Veeam Agent for Microsoft Windows will automatically exclude this folder from the backup.

2. USB storage devices formatted as FAT32 do not allow storing files larger than 4 GB in size. For this reason, it is recommended that you do not use such USB storage devices as a backup target.

---

### Step 9. Specify Shared Folder Settings

The **Shared Folder** step of the wizard is available if at the Destination step you have chosen to save the backup in a network shared folder.

Specify shared folder settings:

1. In the **Shared folder** field, type a UNC name of the network shared folder in which you want to store
backup files.

The UNC name must start with two back slashes (\\).

2. In the **Connection account** fields, specify a user name and password of the account that has access permissions on this shared folder.

   The user name must be specified in the **DOMAIN\USERNAME** format.

   To view the specified password, click and hold the eye icon on the right of the **Password** field.

3. Select the **Use the specified account to create individual sub-folders for each managed backup agent** check box if backup of each managed computer must be stored in its own subfolder of the shared folder.

   If this check box selected, each managed Veeam backup agent that writes data to the network share will create a separate subfolder and store backups to this subfolder. The machine account of the managed computer will be set as the subfolder owner. As a result, the machine account of each managed computer will have access to the subfolder where its backups are stored, and will not be able to access content of other subfolders on the network share.

   If the check box is selected, make sure that the following prerequisites are completed:

   - Managed computers protected with Veeam backup agents are members of an Active Directory domain.
   - The shared folder is included in the same Active Directory domain as the managed computers.
   - **Everyone** has **Read** and **Write** permissions on the shared folder.
   - Child objects (subfolders) do not inherit permissions from the shared folder.

   If the check box is not selected, backups for all managed computers will be stored in the shared folder.

4. Specify backup retention policy settings:

   - [For Workstation operation mode] In the **Keep backups for the past <N> days when computer was running** field, specify the number of days for which you want to store backup files in the target location. By default, Veeam backup agent keeps backup files for 14 days. After this period is over, Veeam backup agent will remove the earliest restore points from the backup chain.

     For details, see Veeam Agent for Microsoft Windows User Guide, section **Backup Retention Policy in Free and Workstation Editions**.

   - [For Server operation mode] In the **Restore points to keep on disk** field, specify the number of restore points you want to keep in the target location. By default, Veeam backup agent keeps 14 latest restore points. After this number is exceeded, Veeam backup agent will remove the earliest restore points from the backup chain.

     For details, see Veeam Agent for Microsoft Windows User Guide, section **Backup Retention Policy in Server Edition**.

5. Click **Advanced Settings** to specify advanced settings for the backup job.
For details, see Specify Advanced Job Settings.

Step 10. Specify Backup Server Settings

The Backup Server step of the wizard is available if at the Destination step you have chosen to store backup files on a Veeam Backup & Replication repository.

Specify settings for the Veeam backup server that manages the target backup repository:

1. In the Veeam backup server name or IP address field, specify a DNS name or IP address of the Veeam backup server.

2. In the Port field, specify a number of the port over which Veeam backup agent must communicate with the backup repository.

   By default, Veeam backup agent uses port 10001.
IMPORTANT!

If you specify a DNS name of the Veeam backup server, make sure that the Veeam backup server name is resolved into IPv4 address on the machine where Veeam backup agent is installed. The Veeam Backup Service in Veeam Backup & Replication listens on IPv4 addresses only. If the Veeam backup server name is resolved into IPv6 address, Veeam backup agent will fail to connect to the Veeam backup server.

**Step 11. Specify Backup Repository Settings**

The **Backup Repository** step of the wizard is available if at the **Destination** step you have chosen to save backup files on a Veeam Backup & Replication repository.

Specify settings for the target backup repository:

1. In the **Specify backup repository name** field, type the name of a backup repository where you want to store created backups.

   To store backups, you can use a simple backup repository or a scale-out backup repository.

2. Select the **Specify user credentials to access the selected Veeam Backup & Replication server and its backup repository** check box. In the **Username** and **Password** fields, specify a user name and password of the account that has access to this backup repository.

   Permissions on the backup repository managed by the target Veeam backup server must be granted beforehand. For details, see Veeam Agent for Microsoft Windows User Guide, section **Setting Up User Permissions on Backup Repositories**.

   If you do not select the **Specify user credentials to access the selected Veeam Backup & Replication server and its backup repository** check box, Veeam Agent for Microsoft Windows will connect to the
backup repository using the **NT AUTHORITY\SYSTEM** account of the computer where the product is installed. You can use this scenario if the computer is joined to the Active Directory domain. In this case, you can simply add the computer account (**DOMAIN\COMPUTERNAME$**) to an Active Directory group and grant access rights on the backup repository to this group.

Setting access permissions on the backup repository to **Everyone** is equal to granting access rights to the **Everyone** Microsoft Windows group (Anonymous users are excluded). If you have set such permissions on the backup repository, you can omit specifying credentials. However, this scenario is recommended for demo environments only.

3. Specify backup retention policy settings:
   - [For Workstation operation mode] In the **Keep backups for the past <N> days when computer was running** field, specify the number of days for which you want to store backup files in the target location. By default, Veeam backup agent keeps backup files for 14 days. After this period is over, Veeam backup agent will remove the earliest restore points from the backup chain.

   For details, see Veeam Agent for Microsoft Windows User Guide, section *Backup Retention Policy in Free and Workstation Editions*.

   - [For Server operation mode] In the **Restore points to keep on disk** field, specify the number of restore points you want to keep in the target location. By default, Veeam backup agent keeps 14 latest restore points. After this number is exceeded, Veeam backup agent will remove the earliest restore points from the backup chain.


4. Click **Advanced Settings** to specify advanced settings for the backup job.

   For details, see Specify Advanced Job Settings.
Step 12. Specify Cloud Backup Settings

The **Cloud Repository** step of the wizard is available if at the **Destination** step you have chosen to save backup files on a cloud repository.

1. Specify backup retention policy settings:
   - [For Workstation operation mode] In the **Keep backups for the past <N> days when computer was running** field, specify the number of days for which you want to store backup files in the target location. By default, Veeam backup agent keeps backup files for 14 days. After this period is over, Veeam backup agent will remove the earliest restore points from the backup chain.
     
     For details, see *Veeam Agent for Microsoft Windows User Guide*, section *Backup Retention Policy in Free and Workstation Editions*.
   
   - [For Server operation mode] In the **Restore points to keep on disk** field, specify the number of restore points you want to keep in the target location. By default, Veeam backup agent keeps 14 latest restore points. After this number is exceeded, Veeam backup agent will remove the earliest restore points from the backup chain.
     
     For details, see *Veeam Agent for Microsoft Windows User Guide*, section *Backup Retention Policy in Server Edition*.

2. Click **Advanced Settings** to specify advanced settings for the backup job.
   
   For details, see *Specify Advanced Job Settings*. 
NOTE:

The cloud repository on which backups will be stored will be selected automatically. If you want to store backups on a specific backup repository, you can choose this repository in backup job settings for specific computers. For details, see Configuring Backup Job Settings for Individual Computers.

Step 13. Specify Cloud Repository Quota

The Backup Quota step of the wizard is available if at the Destination step you have chosen to save backup files on a cloud repository.

You can select one of the following options:

- Use sub-tenant accounts for each managed backup agent automatically with the following user quota.

  If you select this option, Veeam Availability Console will create a subtenant account for each protected computer of a corresponding company. Veeam backup agent will use this account to write data to the cloud repository. The name of the subtenant account is formed according to the following pattern: `{company_name}_<{computer_name>}`.

  The subtenant quota will be set to the amount specified in the User quota field. If you do not want to limit the amount of space allocated to a subtenant, select the Unlimited quota check box.

  For details on subtenant accounts, see Veeam Cloud Connect Administrator Guide, section Subtenants.

- Use single tenant account for all computers managed by the company (not recommended).
If you select this option, Veeam Availability Console will store backups on a cloud repository using an account of a company to which protected computers belong.

Step 14. Specify Advanced Job Settings

In the Advanced Settings window, specify advanced settings for the backup job:

- Backup settings
- Maintenance settings
- Storage settings

You can access the Advanced Settings window from the following steps of the wizard:

- Local Storage — if you have chosen to store backups in the local storage.
- Shared Folder — if you have chosen to store backups in a shared folder.
- Backup Repository — if you have chosen to store backups on a Veeam Backup & Replication repository.
- Cloud Repository — if you have chosen to store backups in the Veeam Cloud Connect repository.

Backup Settings

On the Backup tab of the Advanced Settings window, specify settings for a backup chain created with the backup job:

1. If you want to periodically create synthetic full backups, select the Create synthetic full backups periodically check box and click Days to schedule synthetic full backups on the necessary week days.
For details on synthetic full backup, see Veeam Agent for Microsoft Windows User Guide, section Synthetic Full Backup.

2. If you want to periodically create active full backups, select the Create active full backups periodically check box. Use the Monthly on or Weekly on selected days options to define scheduling settings.

For details on active full backup, see Veeam Agent for Microsoft Windows User Guide, section Active Full Backup.

**NOTE:**
- Before scheduling periodic full backups, you must make sure that you have enough free space on the target location. As an alternative, you can create active full backups manually when needed.
- If you schedule the active full backup and synthetic full backup on the same day, Veeam backup agent will perform only active full backup. Synthetic full backup will be skipped.

### Maintenance Settings

On the **Maintenance** tab of the **Advanced Settings** window, specify maintenance settings for the backup chain created with the backup job:

1. To periodically perform a health check for the latest restore point in the backup chain, in the Storage-level corruption guard section, select the Perform backup files health check check box and specify the schedule for the health check.
Use the **Monthly on** or **Weekly on selected days** options to define scheduling settings.

2. [For Veeam backup repository and cloud repository targets] Select the **Remove deleted items data after** check box and specify the number of days for which you want to keep the backup created with the backup job in the target location.

3. To periodically compact a full backup, select the **Defragment and compact full backup file** check box.

   Use the **Monthly on** or **Weekly on selected days** options to define scheduling settings.

For details on health check for backup files, see Veeam Agent for Microsoft Windows User Guide, section *Health Check for Backup Files*.

### Storage Settings

On the **Storage** tab of the **Advanced Settings** window, specify storage settings for the backup job:

1. In the **Compression** level list, select a compression level for the backup: **None**, **Dedupe-friendly**, **Optimal**, **High** or **Extreme**.

2. In the **Storage optimization** section, select what type of backup target you plan to use: Local target (16 TB + backup files), Local target, LAN target or WAN target.

   Depending on the chosen storage type, Veeam backup agent will use data blocks of different size to optimize the size of backup files and job performance.

3. If you want to encrypt the content of backup files, in the **Encryption** section, specify encryption settings
for the backup job:

a. Select the **Enable backup file encryption** check box.

b. In the **Password** field, type a password that you want to use for encryption.

c. In the **Hint** field, type a hint for the password.

   In case you lose the password, the specified hint will help you to remember the lost password.

For details on encryption, see *Veeam Agent for Microsoft Windows User Guide*, section *Data Encryption*. 
NOTE:

- You cannot specify encryption options for the backup job if you have chosen to save backup files on a Veeam backup repository. Encryption options for Veeam backup agent jobs targeted at a Veeam Backup & Replication repository are managed by a backup administrator working with Veeam Backup & Replication. For details, refer to the Veeam Backup & Replication documentation at https://www.veeam.com/documentation-guides-datasheets.html.

- If you lose a password that was specified for encryption, you can change the password in the encryption settings. After the backup job creates a new restore point encrypted with the new password, you will be able to use this password to restore data from all restore points in the backup chain, including those restore points that were encrypted with an old password.

- If you enable encryption for the existing backup job that has already created one or more restore points, during the next job session, Veeam backup agent will create active full backup. The created full backup file and subsequent incremental backup files in the backup chain will be encrypted with the specified password.

- Encryption is not retroactive. If you enable encryption for the existing backup job, Veeam backup agent does not encrypt the previous backup chain created with this job.

Step 15. Choose Local Backup Cache Location

The **Backup Cache** step of the wizard is available if you have chosen to save backup files on a remote storage: in a network shared folder, on a Veeam Backup & Replication repository or cloud repository.
Specify backup cache settings:

1. Select the **Enable backup cache** check box.
2. In the **Location** field, specify a path to the folder on the protected computer in which backup cache files must be stored.
3. In the **Maximum size** field, specify the size for the backup cache.

When defining the size of the backup cache, consider the following:

- Each full backup file may consume about 50% of the backed-up data size.
- Each incremental backup file may consume about 10% of the backed-up data size.

**TIP:**

For the backup cache, you can use a dedicated removable storage device, for example, a USB key or an SD card. In this case, the backup cache will not consume disk space on the local drive of the managed computer.

For details on backup cache, see Veeam Agent for Microsoft Windows User Guide, section *Backup Cache*.

---

**Step 16. Specify Guest OS Processing Options**

The **Guest Processing** step of the wizard is available if at the **Backup Mode** step you have chosen the **Server** operation mode.

At this step, you can enable the following settings for guest OS processing:

- **Application-aware processing**
- Transaction log handling for Microsoft SQL Server
- Archived log handling for Oracle databases
- Microsoft SharePoint account settings
- Use of pre-freeze and post-thaw scripts
- File indexing

**Application-Aware Processing**

If the computer runs VSS-aware applications, you can enable application-aware processing to create a transactionally consistent backup. The transactionally consistent backup guarantees proper recovery of applications without data loss.

To enable application-aware processing:

1. At the **Guest Processing** step of the wizard, select the **Enable application-aware processing** check box.
2. Click the **Customize application handing options for individual applications** link.
3. In the **Processing Settings** window, on the **General** tab, specify if Veeam backup agent must process transaction logs or copy-only backups must be created.
   a. Select **Process transaction logs with this job** if Veeam backup agent must process transaction logs.
      [For Microsoft Exchange] With this option selected, Veeam backup agent will wait for backup to complete successfully and then trigger truncation of transaction logs. If the backup job fails, logs will remain unaltered until the next backup job session.
      [For Microsoft SQL Server and Oracle] You will need to specify additional settings for transaction log handling on the **SQL** and **Oracle** tabs of the **Processing Settings** window. For details, see Transaction Log Handling for Microsoft SQL Server and Transaction Log Handling for Oracle Databases.
   b. Select the **Perform copy only** option if you use another tool to maintain consistency of the database state. Veeam backup agent will create a copy-only backup. The copy only backup preserves the chain of full/differential backup files and transaction logs. For details, see http://msdn.microsoft.com/en-us/library/ms191495.aspx.

**IMPORTANT!**

If both Microsoft SQL Server and Oracle Server are installed on the same server, and log backup is enabled for both applications, Veeam backup agent will back up only Oracle transaction logs. Microsoft SQL Server transaction logs will not be processed.
For details on transaction log truncation, see Veeam Agent for Microsoft Windows User Guide, section Transaction Log Truncation.

Transaction Log Handling for Microsoft SQL Server

If you back up Microsoft SQL Server, you can specify how Veeam backup agent must process database transaction logs:

1. At the Guest Processing step of the wizard, select the Enable application-aware processing check box.
2. Click the Customize application handing options for individual applications link.
3. In the Processing Settings window, on the General tab, select Process transaction logs with this job.
4. In the Processing Settings window, open the SQL tab.
5. To specify a user account that Veeam backup agent must use to connect to the Microsoft SQL Server, select the Specify Microsoft SQL Server account with database admin privileges check box and specify a user name and password for the user account.

   To connect to the Microsoft SQL Server, you must use a Microsoft Windows user account that has sysadmin privileges on the Microsoft SQL Server. You cannot use Microsoft SQL Server accounts (for example, the SA account) to connect to the database.

6. Specify how transaction logs must be processed. You can select one of the following options:
   - Select Truncate logs to truncate transaction logs after successful backup. Veeam backup agent will wait for backup to complete successfully and then truncate transaction logs. If the backup job fails, the logs will remain unaltered until the next backup job session.
Select **Do not truncate logs** to preserve transaction logs. When the backup job completes, Veeam backup agent will not truncate transaction logs.

It is recommended that you enable this option for databases that use the **Simple recovery** model. If you enable this option for databases that use the **Full or Bulk-logged recovery** model, transaction logs may grow large and consume all disk space. In this case, the database administrator must take care of transaction logs.

Select **Backup logs periodically** to back up transaction logs with Veeam backup agent. Veeam backup agent will periodically copy transaction logs to the backup location and store them together with the image-level backup. During the backup job session, transaction logs will be truncated.

For details on log handling, see Veeam Agent for Microsoft Windows User Guide, section *Microsoft SQL Server and Oracle Logs Backup*.

If you have chosen to back up transaction logs with Veeam backup agent, you must specify settings for transaction logs backup:

1. In the **Backup logs every** \(<N>\) minutes field, specify the frequency for transaction logs backup.
   
   By default, transaction logs are backed up every 15 minutes. The maximum log backup interval is 480 minutes.

2. In the **Retain log backups** section, specify retention policy for transaction logs stored in the backup location.
   
   - Select **Until the corresponding image-level backup is deleted** to apply the same retention policy for image-level backups and transaction log backups.
   
   - Select **Keep only last** \(<N>\) **days of log backups** to keep transaction logs for a specific number of days. By default, transaction logs are kept for 15 days. If you select this option, you must make sure that retention for transaction logs is not greater than retention for the image-level backup. For details, see Veeam Agent for Microsoft Windows User Guide, section *Retention for Database Log Backups*. 


IMPORTANT!

Veeam backup agent automatically excludes its configuration database from application-aware processing during backup. Transaction logs for the configuration database are not backed up.

Archived Log Handling for Oracle Databases

If you back up a server that hosts an Oracle database, you can specify how Veeam backup agent must process archived logs:

1. At the Guest Processing step of the wizard, select the Enable application-aware processing check box.
2. Click the Customize application handing options for individual applications link.
3. In the Processing Settings window, on the General tab, select Process transaction logs with this job.
4. In the Processing Settings window, open the Oracle tab.
5. Specify a user account that Veeam Agent for Microsoft Windows must use to connect to the Oracle database:
   a. Select the Specify Oracle account with SYSDBA privileges check box.
   b. In the Account field, select what type of user account you plan to use: Windows account.
   c. In the Username and Password fields, type a username and password for the account.
      The specified account must have SYSDBA permissions on the Oracle database.
6. In the **Archived logs** section, specify if Veeam backup agent must delete archived logs on the Oracle database:

- **Select Do not delete archived logs** if you want Veeam backup agent to preserve archived logs. When the backup job completes, Veeam Agent for Microsoft Windows will not delete archived logs.

  It is recommended that you select this option for databases for which the **ARCHIVELOG** mode is turned off. If the **ARCHIVELOG** mode is turned on, archived logs may grow large and consume all disk space. In this case, the database administrator must take care of archived logs.

- **Select Delete logs older than <N> hours or Delete logs over <N> GB** if you want Veeam Agent for Microsoft Windows to delete archived logs that are older than <N> hours or larger than <N> GB. Veeam backup agent will wait for the backup to complete successfully and then trigger archived logs deletion using Oracle Call Interface (OCI). If the backup job fails, the logs will remain unaltered until the next backup job session.

7. To back up Oracle archived logs with Veeam backup agent, select the **Backup log every <N> minutes** check box and specify the frequency for archived logs backup.

   By default, archived logs are backed up every 15 minutes. The maximum log backup interval is 480 minutes.

8. In the **Retain log backups** section, specify retention policy for archived logs stored in the backup location:

   - **Select Until the corresponding image-level backup is deleted** to apply the same retention policy for image-level backups and archived log backups.

   - **Select Keep only last <n> days of log backups** to keep archived logs for a specific number of days.
By default, archived logs are kept for 15 days. If you select this option, you must make sure that retention for archived logs is not greater than retention for the image-level backups. For details, see Veeam Agent for Microsoft Windows User Guide, section Retention for Database Log Backups.

Microsoft SharePoint Account Settings

If you back up a server that hosts Microsoft SharePoint, you must specify a user account that has enough permissions on the application:

1. At the Guest Processing step of the wizard, select the Enable application-aware processing check box.
2. Click the Customize application handing options for individual applications link.
3. In the Processing Settings window, open the SharePoint tab.
4. Select the Specify Microsoft SharePoint admin account check box.
5. In the **Username** and **Password** fields, type credentials of the account.

**Use of Pre-Freeze and Post-Thaw Scripts**

If you plan to back up data of applications that do not support VSS, you can specify what scripts Veeam backup agent must use to help quiesce the OS and applications on the protected computer. The pre-freeze script quiesces the file system and application data to bring the OS to a consistent state before Veeam backup agent creates a VSS snapshot. After the VSS snapshot is created, the post-thaw script brings the file system and applications to their initial state.

To specify pre-freeze and post-thaw scripts for the job:

1. At the **Guest Processing** step of the wizard, select the **Enable application-aware processing** check box.
2. Click the **Customize application handing options for individual applications** link.
3. In the **Processing Settings** window, open the **Scripts** tab.
4. In the **Script processing mode** section, specify the scenario for scripts execution:
   - Select **Require successful script execution** if Veeam backup agent must stop the backup process if the script fails.
   - Select **Ignore script execution failures** if the backup process must continue even if script errors occur.
   - Select **Disable script execution** if you do not want to run scripts.
5. In the **Scripts** section, specify paths to pre-freeze and post-thaw scripts.
Veeam backup agent supports scripts in the EXE, BAT and CMD format.

6. By default, Veeam backup agent performs guest processing activities under the Local System account. To specify a user account that Veeam backup agent must use to run pre-freeze and post-thaw scripts, select the Specify admin account for script execution check box and enter a user name and password for the user account.

For details on scripts, see Veeam Agent for Microsoft Windows User Guide, section Pre-Freeze and Post-Thaw Scripts.

File Indexing

To specify guest OS indexing options:

1. At the Guest Processing step of the wizard, select the Enable guest file system indexing check box.
2. Click the Customize advanced guest file system indexing options link.
3. In the Indexing Settings window, specify the indexing scope:
   - Select Index everything to index all files within the backup scope. Veeam backup agent will index all files that reside on your computer OS (for entire computer backup), on the volumes that you have selected for backup (for volume-level backup), in the directories that you have selected for backup (for file-level backup).
   - Select Index everything except to index all files on your computer OS except those defined in the list.

By default, system folders are excluded from indexing. You can add or delete folders using the
Add and Remove buttons on the right. You can use system environment variables to form the list, for example: %windir%, %Program Files% and %Temp%.

- Select Index only following folders to define folders that you want to index. You can add or delete folders to index using the Add and Remove buttons on the right. You can use system environment variables to form the list, for example: %windir%, %Program Files% and %Temp%.

For details on file system indexing, see Veeam Agent for Microsoft Windows User Guide, section File System Indexing.

Step 17. Configure Backup Schedule

At the Schedule step of the wizard, specify the schedule according to which backup must run. Backup job scheduling options depend on the application mode in which Veeam backup agent operates:

- Workstation Backup Schedule
- Server Backup Schedule

Workstation Backup Schedule

At the Schedule step of the wizard, specify the schedule according to which backup must be performed.

1. Select the Daily at check box and use the fields on the right to specify time and days when the backup job must start:
   - Everyday — select this option to start the job at the specified time daily.
   - On week-days — select this option to start the job at the specified time on week-days.
   - On these days — select this option to start the job at the specified time on selected days.

You can leave the Daily at check box cleared to configure the backup job without daily schedule. In this
case, you will be able to use the configured backup job to perform backup automatically at specific events. You can also use the configured backup job to create ad-hoc incremental and standalone full backups. For details, see Veeam Agent for Microsoft Windows User Guide, section Performing Ad-Hoc Backups.

2. If you have selected the **On these days** option, click the **Days** button and clear check boxes for the days when the job must not start.

3. Select the action that Veeam backup agent must perform in case your computer is powered off at the time when the scheduled backup job must start:
   - **Backup once powered on** — select this option if Veeam backup agent must start the scheduled backup job when you power on the computer.
   - **Skip backup** — select this option if Veeam backup agent must not to start the scheduled backup job when the computer is powered on. Veeam backup agent will perform backup at the next scheduled time.

4. If Veeam backup agent must perform a finalizing action after the backup job completes successfully, select the necessary action:
   - **Keep running** — select this option if the computer must keep on working.
   - **Sleep** — select this option if Veeam backup agent must bring the computer to the standby mode.
   - **Shutdown** — select this option if Veeam backup agent must shut down the computer.
   - **Hibernate** — select this option if Veeam backup agent must bring the computer to the hibernate mode. This option is available if the hibernate mode is enabled on the computer. For details, see [https://support.microsoft.com/en-us/kb/920730](https://support.microsoft.com/en-us/kb/920730).

   Veeam backup agent applies this setting only to scheduled backups. If you start standalone full backup or incremental backup manually, Veeam backup agent will ignore this setting, and the computer will not be shut down or brought to the standby mode when the backup job completes.

   When the backup job completes, Veeam backup agent will prompt a dialog with a countdown to the selected post-job action. You can select to proceed to the action immediately or to cancel the action. For details, see Veeam Agent for Microsoft Windows User Guide, section Controlling Backup Post-Job Action.

5. In the **At the following events** section, specify settings for events that trigger the backup job launch:
   - Select the **Lock** check box if the scheduled backup job must when the user locks the computer.
   - Select the **Log off** check box if the scheduled backup job must start when the user working with the computer performs a logout operation.
   - Select the **When backup target is connected** check box if the scheduled backup job must start when the backup storage becomes available (for example, when the computer connects to a local network and the target shared folder is accessible).
   - Select the **Eject removable storage once backup is completed** check box if Veeam backup agent must unmount the storage device after the backup job completes successfully. With this option selected, backup files on the removable storage will be protected from encrypting ransomware, such as CryptoLocker.
   - Use the **Back up no more often than every <N> <time units>** field to restrict the frequency of backup job sessions. Specify a minutely, hourly or daily interval between the backup job sessions.

   The **Back up no more often than every <N> <time units>** option is applied only to job sessions started at
specific events. Daily backups are performed according to defined schedule regardless of the time interval specified for this setting.

**IMPORTANT!**

If the power scheme on the endpoint does not allow using wake up timers, you can manually change the power scheme settings on the endpoint. To do this, navigate to Control Panel > **All Control Panel Items** > **Power Options** > **Edit Plan Settings**.

### Server Backup Schedule

At the **Schedule** step of the wizard, select to run the backup job manually or schedule the job to run on a regular basis.

To specify the job schedule:

1. Select the **Run the job automatically** check box.
   
   If this check box is not selected, you will have to start the backup job manually to create backup.

2. Define scheduling settings for the job:

   - To run the job at specific time daily, on defined week days or with specific periodicity, select **Daily at this time**. Use the fields on the right to configure the necessary schedule.

   - To run the job once a month on specific days, select **Monthly at this time**. Use the fields on the right to configure the necessary schedule.

   - To run the job repeatedly throughout a day with a specific time interval, select **Periodically every**. In the field on the right, select the necessary time unit: **Hours** or **Minutes**. Click **Schedule**.
and use the time table to define the permitted time window for the job.

A repeatedly run job is started by the following rules:

- Veeam backup agent always starts counting defined intervals from 12:00 AM. For example, if you configure to run a job with a 4-hour interval, the job will start at 12:00 AM, 4:00 AM, 8:00 AM, 12:00 PM, 4:00 PM and so on.

- If you define permitted hours for the job, after the denied interval is over, Veeam backup agent will immediately start the job and then run the job by the defined schedule.

For example, you have configured a job to run with a 2-hour interval and defined permitted hours from 9:00 AM to 5:00 PM. According to the rules above, the job will first run at 9:00 AM, when the denied period is over. After that, the job will run at 10:00 AM, 12:00 PM, 2:00 PM and 4:00 PM.

- To run the job continuously, select the **Periodically every** option and choose **Continuously** from the list on the right. A new backup job session will start as soon as the previous backup job session finishes.

3. In the **Automatic retry** section, define whether Veeam backup agent must attempt to run the backup job again if the job fails for some reason. Type the number of attempts to run the job and define time intervals between them. If you select continuous backup, Veeam backup agent will retry the job for the defined number of times without any time intervals between the job runs.

4. In the **Backup window** section, define the time interval within which the backup job must complete. The backup window prevents the job from overlapping with production hours and ensures that the job does not impact performance of your server.

   To set up a backup window for the job:

   a. Select the **Terminate job if it exceeds allowed backup window** check box and click **Window**.

   b. In the **Select time periods** window, define the allowed hours and prohibited hours for backup.
If the job exceeds the allowed window, it will be automatically terminated.

<table>
<thead>
<tr>
<th>Schedule</th>
<th>Choose when you want backup job to be started automatically.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run the job automatically</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Daily at this time: 12:36 AM Everyday Days...</td>
<td></td>
</tr>
<tr>
<td>Monthly at this time: 10:08 AM First Sunday Months...</td>
<td></td>
</tr>
<tr>
<td>Periodically every: 1 Hours Schedule...</td>
<td></td>
</tr>
<tr>
<td>Automate retry</td>
<td></td>
</tr>
<tr>
<td>Retry failed job: 2 times</td>
<td></td>
</tr>
<tr>
<td>Wait before each retry for: 10 minutes</td>
<td></td>
</tr>
<tr>
<td>Terminate job if it exceeds allowed backup window...</td>
<td></td>
</tr>
</tbody>
</table>

If the job does not complete within allocated backup window, it will be terminated to prevent snapshot commit during production hours.
Step 18. Review Backup Policy Settings

At the **Summary** step of the wizard, review settings of the configured backup job and click **Finish**.

### Assigning Backup Policies

To configure Veeam backup agent job settings on one or more managed computers, you can assign a saved backup policy to these computers. You can assign any backup policy, including predefined policies, policies created by your company users, and policies created by your service provider.

### Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

### Assigning Backup Policies

To assign a backup policy to one or more managed computers:

1. Log in to Veeam Availability Console.  
   For details, see [Accessing Veeam Availability Console](#).
2. In the menu on the left, click **Managed Computers**.
3. Open the **Discovered Backup Agents** tab.
4. Select the necessary computers in the list.
5. At the top of the list, click the Assign link.
6. In the Backup Policies window, select the necessary policy and click Assign.
7. Check the status of the policy assignment in the Backup Policy column.
   If the policy was assigned successfully, the Name column will display the policy name. If there was a problem assigning the policy, the column will display the Failed to apply error message. Click the message to review possible causes.

Other Ways to Assign Backup Policies

You can also assign backup policies:

- As part of the discovery process, in the discovery rule settings.
  For details, see Step 2. Perform Discovery of Client Computers.
- As part of Veeam backup agent installation process.
  For details, see Step 3. Initiate Installation Procedure.

Modifying Backup Policies

You can modify settings of all saved backup policies, including predefined policies, policies that you created and policies created by Location Administrators in the Client Portal.

NOTE:
Predefined backup policies and policies configured by your service provider cannot be modified directly in the Client Portal. When you choose to edit a predefined backup policy or a policy configured by your service provider, Veeam Availability Console will create a copy of this policy. You can modify settings of this copy and assign it to Veeam backup agents. For details on working with backup policy copies, see Copying Backup Policies.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Modifying Backup Policies

To modify settings of a backup policy:
1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. At the top right corner of the Veeam Availability Console window, click Configuration.
3. In the configuration menu on the left, click Backup Policies.
4. Select the necessary policy in the list.
   To find a backup policy, you can use the following controls:
- Use the search field to find a backup policy by name.
- Use the **Type** filter to show backup policies for workstations or servers only.
- Use the **Policy Type** filter to show only policies created by your service provider or policies created in the Client Portal.
- Use the **Policy Access Type** filter to show only public or private policies.

5. At the top of the policies list, click **Edit**.
6. Modify backup policy settings as described in Creating Backup Policies.
7. Save changes.
8. If a backup policy is already assigned to one or more Veeam backup agents, the backup policy wizard will display a notification window prompting to apply changes to agents. Click **OK** to close the notification window, then click **Propagate Changes**.

   If you do not apply the modified settings, you can do it later, as described in section **Updating Backup Job Configuration**.

### Updating Backup Job Configuration

When you modify settings of a backup policy, you can immediately apply them to Veeam backup agents that have this policy assigned. If you do not apply modified settings, the status of a backup policy for Veeam backup agents will be set to **Outdated**. To put Veeam backup agent job settings in sync with the updated backup policy, you must get the latest job configuration.

### Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

### Updating Veeam Backup Agent Job Configuration

To update Veeam backup agent job configuration and synchronize it with the backup policy:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click **Managed Computers**.
3. Open the **Discovered Backup Agents** tab.
4. Click **Filter**. In the **Filter backup agents by assigned policy** section, select the **Outdated** check box only. Click **Apply**.
   The list of Veeam backup agents will display backup agents whose backup job settings were not updated in accordance with the new backup policy settings.
5. Select the necessary Veeam backup agents in the list.
6. Click a link in the **Backup Policy** column.
   The **Assigned Backup Policies** window will open.
7. From the list of backup policies, select one or more policies whose setting you want to propagate to Veeam backup agents.
8. At the top of the list, click **Update Config**.

**Other Ways to Update Backup Job Configuration**

Alternatively, you can update backup job configuration in the list of Veeam backup agent jobs:

1. Log in to Veeam Availability Console.  
   For details, see [Accessing Veeam Availability Console](#).
2. In the menu on the left, click **Backup Jobs**.
3. Open the **Managed Backup Agents** tab.
4. Select the necessary computer in the list and click a link in the **Successful Jobs** column.
5. In the **Agent Jobs** window, click **Filter**. In the **Filter agents backup jobs by assigned policy** section, select the **Outdated** check box only. Click **Apply**.  
   The list of backup jobs will display jobs whose settings were not updated in accordance with the new backup policy settings.
6. Select the necessary jobs in the list.
7. At the top of the list, click **Update Config**.

**Copying Backup Policies**

Instead of creating a new backup policy from scratch, you can create a copy of an existing backup policy and modify its settings. This can be useful if you need to create a set of similar backup policies with only a few settings that differ.

**Required Privileges**

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

**Copying Backup Policies**

To create a copy of a backup policy:

1. Log in to Veeam Availability Console.  
   For details, see [Accessing Veeam Availability Console](#).
2. At the top right corner of the Veeam Availability Console window, click **Configuration**.
3. In the configuration menu on the left, click **Backup Policies**.
4. Select the necessary policy in the list.  
   To find a backup policy, you can use the following controls:
   - Use the search field to find a backup policy by name.
   - Use the **Type** filter to show backup policies for workstations or servers only.
   - Use the **Policy Type** filter to show only policies created by your service provider or policies created in the Client Portal.
5. At the top of the list, click **Copy**.
6. Modify the necessary policy settings as described in **Creating Backup Policies**.
7. Save changes.

### Removing Backup Policies

You can remove backup policies configured by your company users in the Client Portal.

**NOTE:**

When removing backup policies, note the following limitations:

- You cannot remove a backup policy if it is assigned to one or more managed Veeam backup agents. Before you remove such backup policy, assign to managed Veeam backup agents another policy, instead of the one you want to remove. For details, see **Assigning Backup Policies**.
- You cannot remove predefined backup policies and policies configured by your service provider.

### Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

### Removing Backup Policies

To remove a backup policy:

1. Log in to Veeam Availability Console.
   
   For details, see **Accessing Veeam Availability Console**.

2. At the top right corner of the Veeam Availability Console window, click **Configuration**.

3. In the configuration menu on the left, click **Backup Policies**.

4. Select the necessary policy in the list.
   
   To find a backup policy, you can use the following controls:
   - Use the search field to find a backup policy by name.
   - Use the **Type** filter to show backup policies for workstations or servers only.
   - Use the **Policy Type** filter to show only policies created by your service provider or policies created in the Client Portal.
   - Use the **Policy Access Type** filter to show only public or private policies.

5. At the top of the policies list, click **Remove**.

6. In the displayed window, click **Yes** to confirm removal.
Changing Backup Job Settings for Individual Computers

Instead of assigning backup policies, you can configure Veeam backup agent job settings for individual managed computers.

Before You Begin

Before you configure a backup job, check the following prerequisites:

- The target location where you plan to store backup files must have enough free space.
- The number of jobs that you can assign to a Veeam backup agent depends on the product edition. For details on the limitation of the number of jobs, see Veeam Agent for Microsoft Windows User Guide, section Backup Job.
- [For Veeam Backup & Replication repository targets] You can store created backups in a backup repository only if the backup server runs Veeam Backup & Replication 9.5 Update 3 or later.
- [For Veeam Backup & Replication repository targets] If you plan to use a Veeam Backup & Replication repository as a target for backups, you must pre-configure user access permissions on this backup repository. For details, see Veeam Agent for Microsoft Windows User Guide, section Setting Up User Permissions on Backup Repositories.

Backup has the following limitations:

- You cannot save the backup of entire computer on the local computer disk. Use an external hard drive or USB drive, network shared folder or backup repository as a target location.
- Veeam Agent for Microsoft Windows does not back up data to which symbolic links are targeted. It only backs up the path information that the symbolic links contain. After restore, identical symbolic links are created in the restore destination.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Configuring Backup Job Settings

To configure Veeam backup agent job settings:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Backup Jobs.
3. Open the Managed Backup Agents tab.
4. Do one of the following:
   - Choose the necessary computers in the list and click Create Job at the top of the list.
Choose the necessary computers in the list and click a link in the **Successful Jobs** column. In the **Agent Jobs** window, click **Create Job**.

5. At the **Create Job** step of the **New Backup Job** wizard, select one of the following options:

- **Create a new job**
  
  Select this option to create a job configuration from scratch. Configure Veeam backup agent job settings as described in **Creating Backup Policies**.

- **Use a job template**
  
  Select this option to use an existing policy as a template for job configuration. At the **Backup Policies** step of the wizard, select a backup policy on which the backup job will be based. Veeam Availability Console will assign the policy to the selected managed computers.

**NOTE:**

When you create backup job configuration from scratch, some configuration steps may differ from steps available for backup policies. For example, at the **Cloud Repository** step, you can choose a specific cloud repository as a backup target. In backup policy settings, this possibility is not available.

**Modifying Veeam Backup Agent Jobs**

You can modify Veeam backup agent job settings on a single managed computer without affecting job configuration applied to other Veeam backup agents.
Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Modifying Veeam Backup Agent Job

To modify Veeam backup agent job settings:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Backup Jobs.
3. Open the Managed Backup Agents tab.
4. Choose the necessary computer in the list and click a link in the Successful Jobs column.
5. In the Agent Jobs window, select the job that you want to modify and click Edit.
6. In the Edit Job wizard, modify Veeam backup agent job settings.
   For details on backup job settings, see Creating Backup Policies.
7. Save changes.

Other Ways to Modify Veeam Backup Agent Job Settings

You can configure Veeam backup agent job settings in the list of discovered computers:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Managed Computers.
3. Open the Discovered Backup Agents tab.
4. Choose the necessary computer in the list and click a link in the Backup Policy column.
5. In the Assigned Backup Policies window, select the job that you want to modify and click Edit.
6. In the Edit Job wizard, modify Veeam backup agent job settings.
   For details on backup job settings, see Creating Backup Policies.
7. Save changes.

Removing Veeam Backup Agent Jobs

If you no longer want to protect data of a managed computer, you can remove a backup job configuration.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.
Removing Veeam Backup Agent Job

To remove a job configuration from Veeam backup agent:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Backup Jobs.
3. Open the Managed Backup Agents tab.
4. Choose the necessary computer in the list and click a link in the Successful Jobs column.
5. In the Agent Jobs window, select one or more jobs that you want to remove and click Delete Job.
6. In the Delete Backup Job window, click Delete to confirm removal.
   [For Veeam backup agents version 3.0 or later] If the backup job is pointed to a cloud repository, you can select if you want to remove backup files, created by this job:
   - To delete the backup job and all backup files, in the Delete Backup Job window, click Delete All.
   - To delete only the backup job and keep the backup files in the cloud, in the Delete Backup Job window, click Delete Job.

Other Ways to Remove Veeam Backup Agent Job Settings

You can configure Veeam backup agent job settings in the list of discovered computers:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Managed Computers.
3. Open the Discovered Backup Agents tab.
4. Choose the necessary computer in the list and click a link in the Backup Policy column.
5. In the Assigned Backup Policies window, select one of more jobs that you want to remove and click Delete Job.
6. In the Delete Backup Job window, click Delete to confirm removal.
   [For Veeam backup agents version 3.0 or later] If the backup job is pointed to a cloud repository, you can select if you want to remove backup files, created by this job:
   - To delete the backup job and all backup files, in the Delete Backup Job window, click Delete All.
   - To delete only the backup job and keep the backup files in the cloud, in the Delete Backup Job window, click Delete Job.
Enabling Read-Only Access Mode

To prevent end users from changing Veeam backup agent job settings, and performing restore, you can enable read-only access mode.

In the read-only access mode, Veeam backup agents can be managed only in Veeam Availability Console. The Veeam backup agent Control Panel section displays a notification saying that the product is managed by a system administrator.

End users working directly with Veeam backup agent in the read-only access mode can perform a limited set of operations, including:

- Running the backup job manually
- Viewing backup session statistics
- Creating Veeam Recovery Media
- Restoring individual files

Other operations are not available for end users.

**NOTE:**

When you install Veeam backup agents using discovery rules, or initiate Veeam backup agent installation in Veeam Availability Console, the read-only access mode is enabled by default. You might need to manually enable the read-only access mode only if Veeam backup agents were installed outside Veeam Availability Console (for example, using GPO), or if for some reason you chose not to keep the default access mode settings when installing Veeam backup agents.

**Required Privileges**

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

**Enabling Read-Only Access Mode**

To enable read-only access mode for Veeam backup agents:
1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Backup Jobs.
3. Open the Managed Backup Agents tab.
4. Select one or more Veeam backup agent jobs in the list.
   To display all Veeam backup agents running in the full access mode, click Filter, in the Filter backup agents by UI mode section select Full and click Apply.
5. At the top of the list, click Agent UI Mode and choose Switch to read-only UI.

Disabling Read-Only Access Mode

To disable read-only access for Veeam backup agents:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Backup Jobs.
3. Open the Managed Backup Agents tab.
4. Select one or more Veeam backup agent jobs in the list.
   To display all Veeam backup agents running in the read-only access mode, click Filter, in the Filter backup agents by UI mode mode to display section select Read-Only and click Apply.
5. At the top of the list, click Agent UI Mode and choose Switch to full admin access.
Configuring Veeam Backup Agent Global Settings

In Veeam Availability Console, you can configure Veeam backup agent global settings for one or more managed computers.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Configuring Veeam Backup Agent Global Settings

To configure Veeam backup agent global settings:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Backup Jobs.
3. Open the Managed Backup Agents tab.
4. Select one or more Veeam backup agent jobs in the list.
5. At the top of the list, click Settings.
6. In the Settings window, specify the required global settings:
   - **Disable scheduled backups** — select this option if you do not want to run automatic backups for some period of time. For example, you may want to put backup activities on hold if you plan to perform resource consuming operations on the endpoint at the time when the backup job is scheduled.
     For details, see Veeam Agent for Microsoft Windows User Guide, section Disabling and Enabling Scheduled Backups.
   - **Disable Control Panel notifications** — select this option if you want to disable Veeam backup agent warning and information messages on the notification bar in the Control Panel.
     For details, see Veeam Agent for Microsoft Windows User Guide, section Disabling Control Panel Notifications.
   - **Disable backup over metered connection** — select this option if you want to disable backup over metered Internet connection to avoid extra costs. Veeam backup agents can automatically detect metered connections. If this option is enabled, Veeam backup agents will not perform backup when the endpoint is on such connection.
     For details, see Veeam Agent for Microsoft Windows User Guide, section Disabling Backup over Metered Connections.
   - **Throttle backup activity when system is busy** — select this option if during backup Veeam backup agents must set low priority for its components engaged in the backup process.
     For details, see Veeam Agent for Microsoft Windows User Guide, section Throttling Backup Activities.
   - **Use wake up timers to start jobs** — select this option if Veeam backup agents must automatically wake up a managed computer from sleep at the time when the backup job is
scheduled to start.

This option is supported for computers running Veeam Agent for Microsoft Windows version 2.2 or later.

For details, see Veeam Agent for Microsoft Windows User Guide, section Computer Wake Up from Sleep.

- **Require local admin privileges for FLR operation** — select this option if you want to disallow to perform file-level restore under an account that does not have administrative privileges on the computer with Veeam backup agent.

  This option is supported for computers running Veeam Agent for Microsoft Windows version 3.0 or later.

  For details file-level restore, see Veeam Agent Management Guide, section Restoring Files and Folders.

- **Restrict VPN connection usage for backup** — select this option if you want to disable backup over VPN connections.

  This option is supported for computers running Veeam Agent for Microsoft Windows version 3.0 or later.

  For details, see Veeam Agent for Microsoft Windows User Guide, section Disabling Backup over VPN Connections.

- **Limit bandwidth consumption to** — select this option if you want to limit bandwidth consumption for Veeam backup agent jobs and specify the maximum speed for transferring data from Veeam backup agent to the target location.

  This option is supported for computers running Veeam Agent for Microsoft Windows version 3.0 or later.

  For details, see Veeam Agent for Microsoft Windows User Guide, section Limiting Bandwidth Consumption.

7. Click **Apply**.

   After you save changes, the specified global settings will be propagated to selected Veeam backup agents.
Managing Veeam Backup Agent Jobs

You can manage Veeam backup agent jobs configured on client computers. Job management operations include starting and stopping backup jobs, disabling and enabling backup jobs, deleting jobs and downloading Veeam backup agent logs.
Starting and Stopping Veeam Backup Agent Jobs

You can start and stop Veeam backup agent jobs without accessing the Veeam backup agent Control Panel on managed computers. For example, if a backup job has failed, you can start this job again in Veeam Availability Console to avoid client data loss.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Starting Jobs

To start Veeam backup agent jobs:

1. Log in to Veeam Availability Console. For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Backup Jobs.
3. Open the Managed Backup Agents tab.
4. Find the necessary Veeam backup agent in the list and click a link in the Successful Jobs column.
5. In the Agent Jobs window, select one or more backup jobs.
6. At the top of the list, click Start.

Stopping Jobs

To stop Veeam backup agent jobs:

1. Log in to Veeam Availability Console. For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Backup Jobs.
3. Open the Managed Backup Agents tab.
4. Find the necessary Veeam backup agent in the list and click a link in the Successful Jobs column.
5. In the Agent Jobs window, select one or more backup jobs.
6. At the top of the list, click Stop.
Disabling and Enabling Veeam Backup Agent Jobs

You can disable and enable scheduled Veeam backup agent jobs without accessing the Veeam backup agent Control Panel on managed computers. For example, to prevent a backup job from writing data to a cloud repository by a configured schedule, you can temporarily disable this job.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Disabling Jobs

To prevent Veeam backup agent jobs start by the schedule, you can disable them:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Backup Jobs.
3. Open the Managed Backup Agents tab.
4. Select one or more Veeam backup agents in the list.
5. At the top of the list, click Disable.

Veeam Availability Console will disable all scheduled backup jobs on selected Veeam backup agents.

Enabling Jobs

To enabled previously disabled Veeam backup agent jobs:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Backup Jobs.
3. Open the Managed Backup Agents tab.
4. Select one or more backup jobs in the list.
5. At the top of the list, click Enable.

Veeam Availability Console will enable all scheduled backup jobs on selected Veeam backup agents.
Downloading Veeam Backup Agent Job Logs

You can export job logs for Veeam backup agent installed on managed computers. Exported data is saved in a ZIP archive.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Downloading Veeam Backup Agent Job Logs

To download Veeam backup agent job logs:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Backup Jobs.
3. Open the Managed Backup Agents tab.
4. Select the necessary agent in the list.
5. Click a link in the Successful Jobs column.
   The Backup Agent Jobs window will pop up.
6. In the Backup Agent Jobs window, select one or more backup jobs in the list.
7. At the top of the jobs list, click Download Logs.
8. In the Download Logs dialog box, specify a time interval for which logs must be collected:
   - Collect logs for the last ... days — choose this option to collect data for a specific number of days in the past.
   - Collect logs for the specified time period — choose this option to collect data for a specific time interval in the past.
9. Click OK.
10. Wait until Veeam Availability Console collects log data.

The file with exported data will be saved to the default download location on your computer.
**Viewing and Exporting Veeam Backup Agent Job Details**

You can view Veeam backup agent job details and export them to a **CSV** or **XML** file.

**Required Privileges**

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator, Location User.

Location User can only view job details but cannot perform export.

**Viewing and Exporting Managed Veeam Backup Agent Job Details**

To view and export Veeam backup agent job details:

1. Log in to Veeam Availability Console.
   
   For details, see [Accessing Veeam Availability Console](#).

2. In the menu on the left, click **Backup Jobs**.

3. Open the **Managed Backup Agents** tab.

   Veeam Availability Console will display a list of managed Veeam backup agents.

4. To narrow down the list of Veeam backup agents, you can apply the following filters:

   - **Computer name** — limit the list of Veeam backup agents by the name of a protected computer.
   - **Operation mode** — limit the list of Veeam backup agents by operation mode (*Servers, Workstations*).
   - **Platform type** — limit the list of Veeam backup agents by platform type (*Physical, Cloud*).
   - **Backup mode** — limit the list of Veeam backup agents by backup operation mode (*Entire Computer, FLR, Volume Level*).
   - **Cloud copy** — limit the list of jobs by cloud copy existence (*Yes, No*).
   - **UI mode** — limit the list of Veeam backup agents by mode (*Read-Only, Full*).
   - **Location** — limit the list of jobs by location to which jobs belong. To limit the list of jobs by location, use filters at the top left corner of the Veeam Availability Console window.

5. To export summary details of all jobs on selected Veeam backup agents, click **Export** and choose a format of the exported data:

   - **Export CSV** — choose this option to structure exported data as a **CSV** file.
   - **Export XML** — choose this option to structure exported data as an **XML** file.

   The file with exported data will be saved to the default download location on your computer.

6. To export details of one or more jobs on a particular Veeam backup agent:

   a. Select the necessary Veeam backup agent in the list and click a link in the **Successful Jobs**
column.

b. In the Agent Jobs window, select the necessary Veeam backup agent jobs.

To narrow down the list of jobs, you can apply the following filters:

- **Policy** — limit the list of jobs by the name of a backup policy assigned to Veeam backup agent.
- **Job Status** — limit the list of jobs by status of the latest job session (Success, Warning, Failed, Running, Info).
- **Operation mode** — limit the list of jobs by operation mode (Servers, Workstations).
- **Assigned policy** — limit the list of jobs by the status of a backup policy assigned to Veeam backup agent (Assigned, Not assigned, Custom, Outdated).
- **Backup target** — limit the list of jobs by the location where backup files for a managed computer reside (Local, Offsite).

c. Click **Export** and choose a format of the exported data:

- **Export CSV** — choose this option to structure exported data as a CSV file.
- **Export XML** — choose this option to structure exported data as an XML file.

The file with exported data will be saved to the default download location on your computer.

Each Veeam backup agent job in the list is described with a set of properties. By default, some properties in the list are hidden. To display additional properties, click the ellipsis on the right of the list header and choose properties that must be displayed.

- **Backup Status** — status of the latest job session (Success, Warning, Failed, Running).
- **Name** — name of the backup job.
- **Backup Policy** — backup policy assigned to Veeam backup agent.
- **Operation Mode** — backup job operation mode (Workstation, Server).
- **Destination** — location where backup files for a managed computer reside.
- **Restore Points** — number of restore points available in the backup chain for a managed computer.
- **Backup Size** — total size of all restore points for a managed computer.
- **Scheduling** — job scheduling settings.
- **Last Run** — date and time when the latest backup job session started.
- **Last Modified** — date and time when settings of the backup job were last modified.
- **Modified By** — user who last modified job settings.
- **Next Run** — date and time of the next backup job session according to the backup schedule.
- **Repository Free Space** — amount of free space available on the target repository (repository where backup files for a managed computer reside).
- **Avg. Duration** — average time it took to complete the job session (total job duration time for the previous month divided by the number of times the job ran).
- **Duration** — duration of the latest job session.
- **Backup Mode** — backup operation mode (*Entire Computer, File level, Volume Level*).
Updating Veeam Backup Agents

In Veeam Availability Console, you can initiate update of Veeam backup agents on protected computers.

For example, you may need to perform the update procedure if computers in the client infrastructure already have Veeam backup agents installed, but the software version is not supported by Veeam Availability Console. To be able to manage Veeam backup agents in Veeam Availability Console, you must update the software to the supported version.

The update procedure works as follows:

1. Veeam Availability Console periodically connects to the Veeam Installation Server (over the Internet), and checks whether a new version of the Veeam backup agent software is available.
2. If a new software version is available for managed Veeam backup agents, Veeam Availability Console displays warnings next to these Veeam backup agent saying that the backup agent version is outdated.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Checking Whether New Veeam Backup Agent Version is Available

To check whether a newer software version is available for managed Veeam backup agents:

1. Log in to Veeam Availability Console. For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Managed Computers.
3. Open the Discovered Backup Agents tab.
4. To display all Veeam backup agents that you can update, click Filter, in the Agent version section select Out-of-date, and click Apply.

Otherwise, you can sort Veeam backup agents in the list by values in the Backup Agent Version column. For Veeam backup agents that can be updated, the column displays a warning icon with the Out-of-date value.

Veeam Availability Console offers the following methods for updating Veeam backup agents:
- You can update Veeam backup agents from the Veeam Installation Server
- You can update Veeam backup agents in the offline mode
Updating Veeam Backup Agents from Veeam Installation Server

The procedure of updating Veeam backup agents from Veeam Installation Server is performed with the help of a master agent. The master agent downloads the Veeam backup agent setup file from the Veeam Installation Server (over the Internet), uploads this setup file to client computers within the update scope, and initiates the software update.

The update procedure depends on the method that you used to install Veeam backup agents:

- If you installed Veeam backup agents with a discovery rule, you must update them as described in Updating Veeam Backup Agents Installed with Discovery Rules.
- If you installed Veeam backup agents with 3rd party tools, like GPO, or installed Veeam backup agents manually, you must update them as described in Updating Veeam Backup Agents Installed with 3rd Party Tools or Manually.

Before You Begin

Before you start the update procedure, make sure that:

- Computers on which you plan to update Veeam backup agents are powered on.
- The computer that hosts the master agent has access to the Internet.
- Computers are configured to allow upload of a Veeam backup agent setup file: the File and Printer Sharing (SMB-In) firewall rule must allow inbound traffic.

Updating Veeam Backup Agents Installed with Discovery Rules

To update Veeam backup agents installed with a discovery rule:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Managed Computers.
3. Open the Discovered Backup Agents tab.
4. Select one or more Veeam backup agents in the list.
5. At the top of the list, click Backup Agent and choose Update.
   After you initiate the update procedure, the value in the Backup Agent Version column will change to Updating. You can click the Updating link to track the progress of the update procedure.
6. Check the value in the Backup Agent Version column.
   After the update procedure completes, the value in this column will be set to Up-to-date.

In some cases, after update you might need to perform additional operations. For example, if the setup detects a pending computer reboot, the Backup Agent Version column will display a warning notifying that reboot is required. To complete the update procedure, you can initiate computer reboot in Veeam Availability Console. For details, see Rebooting Remote Computers.
Updating Veeam Backup Agents Installed with 3rd Party Tools or Manually

To update Veeam backup agents installed using 3rd party automation tools (like GPO) or manually, you will require to include in the update scope a computer that runs a master agent. The role of a master agent is normally assigned to a computer in a company location whose management agent was the first one to register in Veeam Availability Console. To learn how to check what computer runs a master agent, see Checking Management Agent Role.

To update Veeam backup agents installed using 3rd party automation tools (like GPO) or manually:

1. In the master agent settings, specify credentials of an account that will be used to upload the setup file to client computers.
   a. Log on to a computer that hosts the master agent.
   b. In the icon tray, right-click the master agent icon and choose Agent Settings.
   c. In the Veeam Master Agent Settings window, click the Remote computer discovery user account link.
   d. In the Discovery Account window, select the Specify local administrator credentials for remote installation of backup agents check box.
   e. In the Username and Password fields, specify credentials of an account that will be used to upload the Veeam backup agent setup file to client computers.

      The account must have local Administrator permissions on all computers in the update scope – that is, computers that run Veeam backup agents that must be updated.

   f. Click OK.
   g. In the Veeam Master Agent Settings window, click Close.

2. Log in to Veeam Availability Console.

   For details, see Accessing Veeam Availability Console.

3. In the menu on the left, click Managed Computers.

4. Open the Discovered Backup Agents tab.

5. Select one or more Veeam backup agents in the list.
6. At the top of the list, click **Backup Agent** and choose **Update**.

   After you initiate the update procedure, the value in the **Backup Agent Version** column will change to **Updating**. You can click the **Updating** link to track the progress of the update procedure.

7. Check the value in the **Backup Agent Version** column.

   After the update procedure completes, the value in this column will be set to **Up-to-date**.

   In some cases, after update you might need to perform additional operations. For example, if the setup detects a pending computer reboot, the **Backup Agent Version** column will display a warning notifying that reboot is required. To complete the update procedure, you can initiate computer reboot in Veeam Availability Console. For details, see [Rebooting Remote Computers](#).
Updating Veeam Backup Agents in Offline Mode

If none of the computers that host Veeam backup agents has connection to the Internet, or you do not want to fetch the Veeam backup agent setup file from the Veeam Installation Server, you can perform offline update. In this update scenario, the Veeam backup agent setup file is placed to a folder on a computer that hosts the master agent, or to a network share. During update, the master agent uploads this setup file to client computers, and initiates the software update.

The update procedure depends on the method that you used to install Veeam backup agents:

- If you installed Veeam backup agents with a discovery rule, you must update them as described in Updating Veeam Backup Agents Installed with Discovery Rules.
- If you installed Veeam backup agents with 3rd party tools, like GPO, or installed Veeam backup agents manually, you must update them as described in Updating Veeam Backup Agents Installed with 3rd Party Tools or Manually.

Before You Begin

Before you start the update procedure, make sure that:

- Computers on which you plan to update Veeam backup agents are powered on.
- Computers are configured to allow upload of a Veeam backup agent setup file: the File and Printer Sharing (SMB-In) firewall rule must allow inbound traffic.

Updating Veeam Backup Agents Installed with Discovery Rules

To update Veeam backup agents installed with a discovery rule:

1. Download a new version of the Veeam backup agent setup file.
2. Place the Veeam backup agent setup file to a folder on a computer that hosts the master agent, or to a network share.

   The master agent must have access to this folder. Make sure that the account under which the master agent service runs has Read/Write permissions on the folder.
3. Log on to a computer that hosts the master agent and specify the path to the Veeam backup agent setup file:
   a. Open the Registry Editor.
   b. In the Registry Editor, navigate to the `HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\VAC\Agent` path.
   c. Create a new registry key value with the following settings:
      - **Type**: String value
      - **Value name**: VawLink
- **Value data**: path to the Veeam backup agent setup file

4. Open the Services console, and restart *Veeam Management Agent Service*.

4. Log in to Veeam Availability Console. For details, see Accessing Veeam Availability Console.

5. In the menu on the left, click *Managed Computers*.

6. Open the *Discovered Backup Agents* tab.

7. Select one or more Veeam backup agents in the list.

8. At the top of the list, click *Backup Agent* and choose *Update*.

   After you initiate the update procedure, the value in the *Backup Agent Version* column will change to *Updating*. You can click the *Updating* link to track the progress of the update procedure.
9. Check the value in the **Backup Agent Version** column.

After the update procedure completes, the value in this column will be set to *Up-to-date*.

In some cases, after update you might need to perform additional operations. For example, if the setup detects a pending computer reboot, the **Backup Agent Version** column will display a warning notifying that reboot is required. To complete the update procedure, you can initiate computer reboot in Veeam Availability Console. For details, see [Rebooting Remote Computers](#).

### Updating Veeam Backup Agents Installed with 3rd Party Tools or Manually

To update Veeam backup agents installed using 3rd party automation tools (like GPO) or manually, you will require to include in the update scope a computer that runs a master agent. The role of a master agent is normally assigned to a computer in a company location whose management agent was the first one to register in Veeam Availability Console. To learn how to check what computer runs a master agent, see [Checking Management Agent Role](#).

To update Veeam backup agents installed using 3rd party automation tools (like GPO) or manually:

1. Download a new version of the Veeam backup agent setup file.
2. Place the Veeam backup agent setup file to a folder on a computer that hosts the master agent, or to a network share.
   - The master agent must have access to this folder. Make sure that the account under which the master agent service runs has at least *Read/Write* permissions on the folder.
3. Log on to a computer that hosts the master agent and specify the path to the Veeam backup agent setup file:

   a. Open the Registry Editor.
   b. In the Registry Editor, navigate to the `HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\VAC\Agent` path.
   c. Create a new registry key value with the following settings:
      - **Type**: String value
      - **Value name**: VawLink
- **Value data**: path to the Veeam backup agent setup file

4. In the master agent settings, specify credentials of an account that will be used to upload the setup file to client computers.
   a. Log on to a computer that hosts the master agent.
   b. In the icon tray, right-click the master agent icon and choose **Agent Settings**.
   c. In the **Veeam Master Agent Settings** window, click the **Remote computer discovery user account** link.
   d. In the **Discovery Account** window, select the **Specify local administrator credentials for remote installation of backup agents** check box.
e. In the **Username** and **Password** fields, specify credentials of an account that will be used to upload the Veeam backup agent setup file to client computers.

The account must have local Administrator permissions on all computers in the update scope – that is, computers that run Veeam backup agents that must be updated.

f. Click **OK**.

  g. In the **Veeam Master Agent Settings** window, click **Close**.

5. Log in to Veeam Availability Console.
   
   For details, see Accessing Veeam Availability Console.

6. In the menu on the left, click **Managed Computers**.

7. Open the **Discovered Backup Agents** tab.

8. Select one or more Veeam backup agents in the list.

9. At the top of the list, click **Backup Agent** and choose **Update**.

   After you initiate the update procedure, the value in the **Backup Agent Version** column will change to **Updating**. You can click the **Updating** link to track the progress of the update procedure.

10. Check the value in the **Backup Agent Version** column.

    After the update procedure completes, the value in this column will be set to **Up-to-date**.

    In some cases, after update you might need to perform additional operations. For example, if the setup detects a pending computer reboot, the **Backup Agent Version** column will display a warning notifying that reboot is required. To complete the update procedure, you can initiate computer reboot in Veeam Availability Console. For details, see Rebooting Remote Computers.
Managing CBT Driver

To increase the speed and efficiency of incremental backups of managed servers, you might need to install the CBT driver. The driver is installed on every server machine protected with Veeam backup agent.

The CBT driver keeps track of data blocks that changed since the latest backup session. Information about changed data blocks is registered, and when a backup job runs, Veeam backup agent uses this information to find out what data blocks have changed since the last run of the job, and then copies only changed data blocks from the disk.

NOTE:

You can install the CBT driver on managed computers that meet all of the following requirements:

- Computers must run Microsoft Windows Server OS.
- Computers must have Veeam backup agent 2.1 or later installed.
- Veeam backup agent must be configured to run in the Server operation mode. For details, see Selecting Product Edition.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Installing CBT Driver

To install the CBT driver for one or more Veeam backup agents:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Managed Computers.
3. Open the Discovered Backup Agents tab.
4. Click Filter. In the Operation mode section, select the Server check box only. Click Apply.
   The list of discovered computers will display Veeam backup agents running in the Server operation mode.
5. Select one or more Veeam backup agents in the list.
6. At the top of the list, click Backup Agent and choose Install CBT Driver.
7. Check the value in the CBT Driver column.
   When installation completes, it must display Installed (Reboot required) status.
8. Reboot computers on which you installed the CBT driver.
   You can reboot the remote computer in Veeam Availability Console, as described in Rebooting Remote Computers.

Uninstalling CBT Driver

To uninstall the CBT driver from one or more Veeam backup agents:
1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Managed Computers.
3. Open the Discovered Backup Agents tab.
4. Click Filter. In the Operation mode section, select the Server check box only. Click Apply.
   The list of discovered computers will display Veeam backup agents running in the Server operation mode.
5. Select one or more Veeam backup agents in the list.
6. At the top of the list, click Backup Agent and choose Uninstall CBT Driver.
7. Reboot computers on which you uninstalled the CBT driver.
   You can reboot the remote computer in Veeam Availability Console, as described in Rebooting Remote Computers.
Restarting Veeam Backup Agents

You can restart Veeam backup agents on remote computers.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Restarting Veeam Backup Agents

To restart Veeam backup agents on one or more remote computers:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Managed Computers.
3. Open the Discovered Backup Agents tab.
4. Select the necessary Veeam backup agents in the list.
5. At the top of the list, click Backup Agent and choose Restart.
Uninstalling Veeam Backup Agents

You can uninstall Veeam backup agents on managed computers. During the uninstall procedure, both Veeam backup agents and Veeam Availability Console management agents are removed from client machines. After you uninstall Veeam backup agents, the number of used and total licenses in the Veeam Availability Console license pool will be updated.

**NOTE:**

If a managed computer runs Veeam Backup & Replication or Veeam Backup Enterprise Manager together with Veeam backup agent, a Veeam Availability Console management agent is not removed as part of the uninstall procedure.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Uninstalling Veeam Backup Agents

To uninstall Veeam backup agents from one or more managed computers:

1. Log in to Veeam Availability Console. For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Managed Computers.
3. Open the Discovered Backup Agents tab.
4. Select the necessary Veeam backup agents in the list.
5. At the top of the list, click Backup Agent and choose Delete.
6. In the displayed window, click Yes to confirm removal.
Downloading Veeam Backup Agent Logs

You can export logs for Veeam backup agent installed on managed computers. Exported data is saved in a ZIP archive.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Downloading Veeam Backup Agent Logs

To download Veeam backup agent logs:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Backup Jobs.
3. Open the Managed Backup Agents tab.
4. Select the necessary agents in the list.
5. At the top of the agents list, click Download Logs.
6. In the Download Logs dialog box, specify a time interval for which logs must be collected:
   - Collect logs for the last ... days — choose this option to collect data for a specific number of days in the past.
   - Collect logs for the specified time period — choose this option to collect data for a specific time interval in the past.
7. Click OK.
8. Wait until Veeam Availability Console collects log data.

The file with exported data will be saved to the default download location on your computer.

Other Ways to Download Veeam Backup Agent Logs

You can download Veeam backup agent logs in the list of managed Veeam backup agents:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Managed Computers.
3. Open the Discovered Backup Agents tab.
4. Select the necessary Veeam backup agents in the list.
5. At the top of the list, click Backup Agent and select Download Logs.
6. In the Download Logs window, specify a time interval for which logs must be collected:
   - Last ... days — choose this option to collect data for a specific number of days in the past.
- **Period** — choose this option to collect data for a specific time interval in the past.

7. Click **Apply**.

   Veeam Availability Console will display a window with message notifying that the download process started. Click **OK** to close the window.

8. Wait until Veeam Availability Console collects log data.

The file with exported data will be saved to the default download location on your computer.
Viewing and Exporting Veeam Backup Agent Details

You can view details on managed Veeam backup agents and export them to a CSV or XML file.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator, Location User.

Viewing and Exporting Veeam Backup Agents Details

To view and export Veeam backup agents details:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Managed Computers.
3. Open the Discovered Backup Agents tab.
4. To narrow down the list of managed Veeam backup agents, you can apply the following filters:
   - **Hostname** — limit the list of Veeam backup agents by the name of protected computer.
   - **Backup Policy** — limit the list of Veeam backup agents by the name of a backup policy.
   - **Agent Status** — limit the list of Veeam backup agents by the Veeam Availability Console management agent status *(Healthy, Warning, Error, Info)*.
   - **Assigned policy** — limit the list of Veeam backup agents by the backup policy assignment status *(Assigned, Not assigned, Custom, Outdated)*.
   - **Operation mode** — limit the list of Veeam backup agents by operation mode *(Servers, Workstations)*.
   - **Platform type** — limit the list of Veeam backup agents by platform type *(Physical, Cloud)*.
   - **Activation** — limit the list of Veeam backup agents by mode *(Activated, Not activated)*.
   - **Agent version** — limit the list of Veeam backup agents by version *(Up-to-date, Out-of-date, Attention required)*.
   - **Location** — limit the list of jobs by location to which jobs belong. To limit the list of jobs by location, use filters at the top left corner of the Veeam Availability Console window.
5. To export Veeam backup agent details, click Export and choose a format of the exported data:
   - **Export CSV** — choose this option to structure exported data as a CSV file.
   - **Export XML** — choose this option to structure exported data as an XML file.
The file with exported data will be saved to the default download location on your computer.

Each Veeam backup agent in the list is described with a set of properties. By default, some properties in the list are hidden. To display additional properties, click the ellipsis on the right of the list header and choose properties that must be displayed.

- **Agent Status** — Veeam Availability Console management agent status (*Healthy, Warning, Error, Unknown*).

- **Company** — name of a company to which Veeam backup agent belongs.

- **Site** — name of a Veeam Cloud Connect site on which the company is registered.

- **Location** — name of a location to which Veeam backup agent belongs.

- **Platform** — computer platform on which Veeam backup agent is deployed (*Physical, Cloud*).

- **Hostname** — name of a managed computer on which Veeam backup agent is deployed.

- **Operation Mode** — backup job operation mode (*Workstation, Server*).

- **Backup Policy** — backup policy assigned to Veeam backup agent.

- **Activation** — date and time when Veeam backup agent was activated.

- **Last Heartbeat** — date and time when a management agent on a managed computer sent the latest heartbeat to Veeam Availability Console.

- **Guest OS** — guest OS on a managed computer.

- **Backup Agent Version** — version of Veeam backup agent deployed on a managed computer.

- **Connection Account** — company owner user name that is used to connect Veeam Availability Console management agent to a cloud gateway.

- **Backup Agent License** — license mode (*Activated, Free, Paid (Standalone)*).

- **Reboot Required** — indicates whether computer reboot is required (normally, computer reboot is required after installation procedures).

- **CBT Driver** — indicates whether CBT driver is installed.

- **Patch Level** — level of Veeam backup agent patch.
Managing Veeam Backup & Replication

Veeam Availability Console allows you to manage Veeam Backup & Replication servers on behalf of companies that act as consumers of backup services. In the Client Portal, you can manage jobs and run failover plans configured on managed Veeam Backup & Replication servers, as well as monitor and manage Veeam Backup & Replication infrastructures.

To manage Veeam Backup & Replication servers, you must complete the following steps:

1. **Connect Veeam Backup & Replication servers.**
   To manage Veeam Backup & Replication servers, you must first connect them to Veeam Availability Console.

2. **Connect to Veeam Backup & Replication servers with the Remote Backup Console.**
   To perform on-going management and troubleshooting, you can connect to managed Veeam Backup & Replication servers using the Remote Backup Console.

3. **Manage Veeam Backup & Replication jobs.**
   To administer data protection operations in managed virtual infrastructures, you can start, stop, enable and disable jobs configured on managed Veeam Backup & Replication servers.

4. **Manage failover plans.**
   To prevent data loss in case of an accident or a major failure, you can manage failover plans configured on managed Veeam Backup & Replication servers.
Connecting Veeam Backup & Replication Servers

To manage Veeam Backup & Replication or Veeam Backup Enterprise Manager servers in Veeam Availability Console, you must first connect these servers to Veeam Availability Console.

When you connect a Veeam Backup & Replication or Veeam Backup Enterprise Manager server to Veeam Availability Console, a Veeam Availability Console management agent is deployed on this server. The management agent is responsible for transmitting commands from Veeam Availability Console to the backup server, performing management operations, collecting data from Veeam Backup & Replication and communicating it back to Veeam Availability Console.

Before You Begin

Before you connect Veeam Backup & Replication, obtain the following data from the service provider:

- FQDN or IP address of a cloud gateway.
- Port on the cloud gateway used to transfer backup data to and from cloud repositories. The management agent will use this port for communication with Veeam Availability Console.
- User credentials for connecting to the service provider (Company Owner credentials).

Connecting Veeam Backup & Replication Servers

To connect a Veeam Backup & Replication server to Veeam Availability Console:

1. Log on to a machine that runs Veeam Backup & Replication.
   
   A user account under which you log on must have local Administrator privileges or the Veeam Backup Administrator role assigned in Veeam Backup & Replication.

2. Launch the Veeam Backup & Replication console.

3. Open the Backup Infrastructure view.

4. In the inventory pane on the left, select Service Providers.

5. Click Add Service Provider on the ribbon.

   Alternatively, you can right-click the Service providers node in the inventory pane and choose Add service provider, or click Add service provider in the main area on the right.

6. At the Service Provider step of the wizard, configure the following settings:
   
   a. In the DNS name or IP address field, specify DNS name or IP address of a cloud gateway.
      
      This can be any cloud gateway deployed on the service provider side.
   
   b. In the Description field, specify description of the service provider.
   
   c. In the Port field, specify the port on the cloud gateway that is used to transfer backup data to the cloud.
      
      The default port number is 6180, and can be customized when a cloud gateway is deployed.
   
   d. Select the Allow this Veeam Backup & Replication installation to be managed by the service provider check box.
When this check box is selected, Veeam Backup & Replication deploys a Veeam Availability Console management agent on a backup server. The management agent is downloaded from Veeam Availability Console.

7. At the **Credentials** step of the wizard, specify user credentials for connecting to the service provider. You must specify credentials of the Company Owner communicated to you by the service provider.

8. Follow the other steps of the wizard. At the last wizard step, click **Finish**.

For details on connecting to service providers, see *Veeam Cloud Connect Administrator Guide*, section *Connecting to Service Providers*.

**IMPORTANT!**

To connect a Veeam Backup & Replication server to Veeam Availability Console, you must always use the **Service Provider** wizard in Veeam Backup & Replication. Do not use other methods to deploy Veeam Availability Console management agents on Veeam Backup & Replication servers, as these methods do not guarantee proper communication between backup servers and Veeam Availability Console.

### Connecting Veeam Backup Enterprise Manager Servers

If Veeam Backup Enterprise Manager is present in the backup infrastructure, you can install the management agent on a machine running Veeam Backup Enterprise Manager. When the agent is installed on a Veeam Backup Enterprise Manager server, Veeam Availability Console can obtain data from this server and monitor its health state.

The management agent on the Veeam Backup Enterprise Manager server must be deployed manually. For details, see *Deploy Management Agents*.

**NOTE:**

You must deploy the management agent manually only if Veeam Backup Enterprise Manager runs on a dedicated machine — that is, if it is not co-installed with Veeam Backup & Replication.
Remote Connection to Veeam Backup & Replication Servers

To perform on-going management and troubleshooting, you can connect to Veeam Backup & Replication servers using the Remote Backup Console.

The Remote Backup Console is a client-side component that provides access to a remote backup server. The console allows you to log in to Veeam Backup & Replication and perform all kinds of data protection and disaster recovery operations as if you work on the local backup server.

For details on Remote Backup Console, see Veeam Backup & Replication User Guide, section Backup & Replication Console.

**NOTE:**
The remote connection using Remote Backup Console is available if the Veeam Cloud Connect server and client Veeam Backup & Replication servers run Veeam Backup & Replication 9.5 Update 2 or later.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Installing Remote Backup Console

To install Remote Backup Console:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Backup Jobs and open the Managed Backup Servers tab.
3. At the top of the list, click Download Remote Backup Console.
   Save the Remote Backup Console setup file to a location that is accessible from a machine where you plan to install the console.
4. Log on to a machine where you plan to install the Remote Backup Console as a local Administrator.
5. Launch the Remote Backup Console setup file and follow the steps of the setup wizard.
6. At the last step of the wizard, click Finish.

Working with Remote Backup Console

For details on working with Remote Backup Console, see Veeam Backup & Replication User Guide, section Backup & Replication Console.
Managing Veeam Backup & Replication Jobs

You can manage Veeam Backup & Replication jobs configured on client backup servers, including:

- Backup jobs
- Replication jobs
- SureBackup jobs
- Backup copy jobs
- File to tape jobs
- Backup to tape jobs
- File and VM copy jobs
- SQL log backup jobs
- Oracle log backup jobs

You can start, stop and retry jobs, enable and disable jobs, view and export job details, download job logs and session reports.
Starting, Stopping and Retrying Jobs

You can start, stop and retry jobs without accessing the Veeam Backup & Replication console on managed backup servers. For example, if a backup job failed, you can manually retry or start this job in Veeam Availability Console to avoid data loss.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator, Location User.

Starting Jobs

To start one or more Veeam Backup & Replication jobs:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Backup Jobs.
3. Open the Managed Backup Servers tab.
4. Select the necessary jobs in the list.
5. At the top of the list, click Start.

Stopping Jobs

To stop one or more running Veeam Backup & Replication jobs:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Backup Jobs.
3. Open the Managed Backup Servers tab.
4. Select the necessary jobs in the list.
5. At the top of the list, click Stop.

Retrying Jobs

To restart one or more failed Veeam Backup & Replication jobs:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Backup Jobs.
3. Open the Managed Backup Servers tab.
4. Select the necessary jobs in the list.
5. At the top of the list, click Retry.
Disabling and Enabling Jobs

You can disable and enable scheduled jobs without accessing the Veeam Backup & Replication console on managed backup servers. For example, to prevent a backup job from writing data to a cloud repository, you can temporarily disable this job.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator, Location User.

Disabling Jobs

A disabled job will not start by the schedule. If you disable a job that has a child job (such as a SQL log backup or Oracle log backup), both the parent and the child jobs will be disabled.

To disable one or more scheduled jobs:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Backup Jobs.
3. Open the Managed Backup Servers tab.
4. Select the necessary jobs in the list.
5. At the top of the list, click Disable.

Enabling Jobs

To enable one or more previously disabled jobs:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Backup Jobs.
3. Open the Managed Backup Servers tab.
4. Select the necessary jobs in the list.
5. At the top of the list, click Enable.
Downloading Job Logs and Session Report

You can export a job session report and job logs for Veeam Backup & Replication jobs configured on managed backup servers. Exported data is saved in a ZIP archive.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator, Location User.

Downloading Job Logs and Session Report

To download a job session report and job logs:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Backup Jobs.
3. Open the Managed Backup Servers tab.
4. Select the necessary jobs in the list.
5. At the top of the jobs list, click Download Logs.
6. In the Download Logs window, specify a time interval for which job statistics and logs must be collected:
   - Last ... days — choose this option to collect data for a specific number of days in the past.
   - Period — choose this option to collect data for a specific time interval in the past.
7. Click Apply.
8. Wait until Veeam Availability Console collects session and log data.

The file with exported data will be saved to the default download location on your computer.
Viewing and Exporting Veeam Backup & Replication Job Details

You can view details on Veeam Backup & Replication jobs configured on managed backup servers and export them to a CSV or XML file.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator, Location User.

Viewing and Exporting Veeam Backup & Replication Job

To view and export Veeam Backup & Replication job details:

1. Log in to Veeam Availability Console. For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Backup Jobs.
3. Open the Managed Backup Servers tab.
   Veeam Availability Console will display a list of all Veeam Backup & Replication jobs configured on managed backup servers.
   To narrow down the list of jobs, you can apply the following filters:
   - **Job** — search jobs by job name.
   - **Status** — limit the list of jobs by the result of the latest job session (Success, Warning, Failed, Running, Information).
   - **Backup Target** — limit the list of jobs by target backup location (Local backup, Offsite backup).
   - **Type** — limit the list of jobs by type (Backup, Replication, SureBackup, Backup Copy, File to Tape, Backup to Tape, Copy, SQL Log Backup, Oracle Log Backup).
   - **Location** — limit the list of jobs by location to which jobs belong. To limit the list of jobs by location, use filters at the top left corner of the Veeam Availability Console window.
4. To export job details, click Export and choose a format of the exported data:
   - **Export CSV** — choose this option to structure exported data as a CSV file.
   - **Export XML** — choose this option to structure exported data as an XML file.
The file with exported data will be saved to the default download location on your computer.

### Managed Backup Agents
- **Job** — name of a data protection job.
- **Company** — name of a company to which a job belongs.
- **Site** — name of the Veeam Cloud Connect site on which the company is registered.
- **Location** — name of a location to which a job belongs.
- **Server** — name of a backup server on which a job is configured.
- **Job Status** — status of the latest job session (Success, Warning, Failed, Running, No Info).
- **Type** — job type (Backup, Replication, SureBackup, Backup copy, File to tape, Backup to tape, Copy, SQL log backup, Oracle log backup).
- **Last Run** — date and time when the latest job session started.
- **End Time** — date and time when the latest job session ended.
- **Duration** — time taken to complete the latest job session.
- **Avg. Duration** — average time a job session takes to complete (total duration of job sessions for the previous month divided by the number of job sessions for the previous month).
- **Target** — name of a target backup location.
- **Processing Rate** — rate at which VM data was processed during the latest job session.
- **Transferred Data** — total amount of data that was transferred to target during the latest job session.
- **Bottleneck** — bottleneck in the process of transferring the data from source to target (source, proxy, network, target, source WAN accelerator, target WAN accelerator).
- **Scheduling** — job schedule (Daily, Monthly, Periodically, Chained, Not scheduled, Disabled, Continuously).
- **Protected VMs** — number of processed by a job VMs that have backup or replica restore points.

### Example

<table>
<thead>
<tr>
<th>Job</th>
<th>Server</th>
<th>Job Status</th>
<th>Type</th>
<th>Last Run</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online Daily Apache</td>
<td>BACKURO2</td>
<td>Failed</td>
<td>Backup</td>
<td>10/17/2017 16:50 AM</td>
<td>2 minutes 16 seconds</td>
</tr>
<tr>
<td>Local Backup</td>
<td>BACKURO2</td>
<td>Running</td>
<td>Replication</td>
<td>10/17/2017 16:59 AM</td>
<td>3 seconds</td>
</tr>
<tr>
<td>Weekly VDI Backup</td>
<td>BACKURO1</td>
<td>Success</td>
<td>Backup</td>
<td>10/16/2017 4:37 PM</td>
<td>6 minutes 15 seconds</td>
</tr>
<tr>
<td>MediaServer Backup to Cloud</td>
<td>BACKURO1</td>
<td>Success</td>
<td>Backup Copy</td>
<td>10/17/2017 2:08 AM</td>
<td>16 minutes 34 seconds</td>
</tr>
</tbody>
</table>

---

Each job in the list is described with a set of properties. By default, some properties in the list are hidden. To display additional properties, click the ellipsis on the right of the list header and choose job properties that must be displayed.
Viewing and Exporting Monitored Veeam Backup Agent Job Details

You can view job details of Veeam backup agents managed by client Veeam Backup & Replication servers. You can also export these details to a CSV or XML file.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator, Location User.

Viewing and Exporting Monitored Veeam Backup & Replication Job

To view and export monitored Veeam Backup & Replication job details:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Backup Jobs.
3. Open the Monitored Backup Agents tab.
   Veeam Availability Console will display a list of jobs for Veeam backup agents managed by client Veeam Backup & Replication servers.
4. To narrow down the list of backup jobs, you can apply the following filters:
   - Computer — limit the list of jobs by the name of a protected computer.
   - Policy or Job — limit the list of jobs by the name of a backup policy.
   - Backup Server — limit the list of jobs by the name of a backup server that manages Veeam backup agent.
   - Status — limit the list of jobs by the result of the latest job session (Success, Warning, Failed, Running, Info).
   - Job mode — limit the list of jobs by job mode (Managed by backup server, Managed by Agent).
   - OS type — limit the list of jobs by operation system (Linux, Windows).
   - Operation mode — limit the list of jobs by operation mode (Servers, Workstations).
5. To export job details, click Export and choose a format of the exported data:
   - Export CSV — choose this option to structure exported data as a CSV file.
   - Export XML — choose this option to structure exported data as an XML file.
The file with exported data will be saved to the default download location on your computer.

Each monitored Veeam backup agent job in the list is described with a set of properties. By default, some properties in the list are hidden. To display additional properties, click the ellipsis on the right of the list header and choose properties that must be displayed.

- **Backup Status** — status of the latest job session (Success, Warning, Failed, Running).
- **Company** — name of a company to which a monitored computer belongs.
- **Site** — name of the Veeam Cloud Connect site on which the company is registered.
- **Location** — name of a location to which a monitored computer belongs.
- **Backup Server** — name of a Veeam Backup & Replication server on which the backup job is managed.
- **Job** — name of Veeam backup agent job.
- **Job Mode** — type of Veeam backup agent job (Job, Policy).
- **Scheduling** — job scheduling settings.
- **Backed up Computers** — number of computers backed up by a job.

You can click this property, to view and export details of computers included in a job.

The following additional details are available for a computer:

- **Backup Source** — source files and folders used to create a backup.
- **Computer** — name of a computer included in a job.
- **Destination** — name of a backup repository, shared folder, or storage to which backup files are stored.
- **Restore Points** — number of restore points available in the backup chain for a managed computer.

- **Transferred data** — amount of data transferred during the latest job session.
- **Duration** — duration of the latest job session.
- **Last Run** — shows how long ago the latest backup job session started.
- **Last Run Time** — date and time when the latest backup job session started.
- **OS Type** — type of computer operation system (Linux, Windows).
- **Operation Mode** — Veeam backup agent operation mode (Workstation, Server).
For details on Veeam backup agents jobs managed by Veeam Backup & Replication, see Veeam Agent Management Guide, section Creating Veeam Agent Backup Jobs.
Managing Failover Plans

You can manage failover plans configured on managed Veeam Backup & Replication servers, including:

- Local failover plans that include regular VM replicas.
  For details on local failover plans, see Veeam Backup & Replication User Guide, section Failover Plan.
- Cloud failover plans that include cloud VM replicas.
  For details on cloud failover plans, see Veeam Cloud Connect Guide, section Cloud Failover Plan.

You can start and undo failover plans, view and export failover plan details.
Starting Failover Plans

You can start a failover plan without accessing the Veeam Backup & Replication console on a managed backup server.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Starting Failover Plans

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Failover Plans.
3. Select the necessary plan in the list.
4. At the top of the list, click Start.
Undoing Failover Plans

You can undo a failover plan without accessing the Veeam Backup & Replication console on a managed backup server.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Undoing Failover Plans

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Failover Plans.
3. Select the necessary plan in the list.
4. At the top of the list, click Undo.
Viewing and Exporting Failover Plan Details

You can view details on failover plans configured on managed backup servers and export them to a CSV or XML file.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Viewing and Exporting Failover Plan Details

To view and export failover plan details:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Failover Plans.
   Veeam Availability Console will display a list of all failover plans configured on managed backup servers.
   To narrow down the list of failover plans, you can apply the following filters:
   - **Failover Plan** — search failover plans by plan name.
   - **Type** — limit the list of failover plans by type (Local, Cloud).
   - **Location** — limit the list of jobs by location to which jobs belong. To limit the list of jobs by location, use filters at the top left corner of the Veeam Availability Console window.
3. To export failover plan details, click Export and choose a format of the exported data:
   - **Export CSV** — choose this option to structure exported data as a CSV file.
   - **Export XML** — choose this option to structure exported data as an XML file.
   The file with exported data will be saved to the default download location on your computer.

Each failover plan in the list is described with a set of properties.
- **Failover Plan** — failover plan name.
- **Server** — name of a backup server on which the failover plan is configured.
- **Company** — name of a company for which a failover plan is configured.
- **Site** — name of the Veeam Cloud Connect site on which the company is registered.
- **Location** — name of a company location to which the failover plan belongs.
- **VMs** — number of VMs included in the failover plan.
  To view the list of VMs in the plan, click the link in the **VMs** column.
- **State** — status of the failover plan (*Ready, In Progress, Undo in Progress, Completed*).
- **Type** — type of the failover plan (*Local, Cloud*).
Managing Veeam Availability Console Agents

In some situations, you might need to administer Veeam Availability Console management agents:

- Management agents installed on computers protected with Veeam backup agent
- Management agents installed on Veeam Backup & Replication servers

In Veeam Availability Console, you can perform the following tasks with management agents:

- Upgrade management agents
- Set a master agent for discovery
- Modify connection account for a management agent
- Reboot computers on which management agents run
- Restart management agent service
- Collect data from machines hosting management agents
- Uninstall management agents
Upgrading Management Agents

Veeam Availability Console and its management agents must run the same software version. Otherwise, they cannot properly communicate with each other. When you upgrade or migrate to a new version of Veeam Availability Console, or install an update, you also need to upgrade management agents running on client computers.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Upgrading Management Agents

To upgrade Veeam Availability Console management agents:

1. Log in to Veeam Availability Console. For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Managed Computers.
3. Open the Discovered Computers tab.
4. Click Filter. In the Filter by agent version section, select the Out-of-date check box only. Click Apply.
   The list of discovered computers will display management agents whose software version does not coincide with the Veeam Availability Console version.
5. Select the necessary management agents in the list.
6. At the top of the list, click Management Agent and choose Upgrade.
7. In the displayed window, check the result of the upgrade and click OK.
Setting Master Agent for Discovery

A Veeam Availability Console management agent can act as a client agent or as a master agent.

- **Client management agent** is used to interact with Veeam backup agent or Veeam Backup & Replication on a client computer.
- **Master management agent** is used to perform discovery of computers in the client infrastructure, and automate installation and update of Veeam backup agents.

For details, see Installing Veeam Backup Agents with Discovery Rules (Recommended) and Updating Veeam Backup Agents.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Checking Management Agent Role

You can check what role is currently assigned to a management agent:

1. Log in to Veeam Availability Console.
   
   For details, see Accessing Veeam Availability Console.

2. In the menu on the left, click **Managed Computers**.

3. Open the **Discovered Computers** tab.

4. [For management agents deployed with a discovery rule] Do the following:
   
   a. In the **Rule** list at the top, select the necessary discovery rule.
   
   b. To limit the scope of discovered computers, use the company and location filters at the top left corner of the Veeam Availability Console window.
      
      For example, this can be required if you want to find a computer that runs a master agent in a specific company location.
   
   c. On the right of the computers list header, click the ellipsis and choose to display the **Agent Role** column.
   
   d. Check the value in the **Agent Role** column.
      
      For a client management agent, the value is set to **Client**. For a master agent, the value is set to **Master**.

5. [For management agents deployed outside Veeam Availability Console] Do the following:
   
   a. In the **Rule** list at the top, select **External Discovery**.
   
   b. To limit the scope of discovered computers, use the company and location filters at the top left corner of the Veeam Availability Console window.
      
      For example, this can be required if you want to find a computer that runs a master agent in a specific company location.
   
   c. On the right of the computers list header, click the ellipsis and choose to display the **Agent Role** column.
d. Check the value in the **Agent Role** column.

For a client management agent, the value is set to *Client*. For a master agent, the value is set to *Master*.

### Setting New Master Agent

You can assign the role of a master agent to a client management agent. Thus, you can change a master agent for a discovery rule: the role of a master agent will be moved from one management agent to another one. Note that when you move the master agent role from one management agent to another, both management agents must belong to scope of the same discovery rule.

To set a new master agent for a discovery rule:

1. Log in to Veeam Availability Console.
   For details, see *Accessing Veeam Availability Console*.
2. In the menu on the left, click **Managed Computers**.
3. Open the **Discovered Computers** tab.
4. In the **Rule** list, select the necessary discovery rule.
5. Click **Filter**. In the **Select agent status to display** section, select the **Installed** check box only. Click **Apply**.
   The list of discovered computers will display computers with management agents installed.
6. Select the necessary computer in the list.
7. At the top of the list, click **Management Agent** and choose **Set as Master**.
8. In the list of discovered computers, make sure that the **Agent Role** value for the selected computer changed to *Master*. 
Modifying Management Agent Connection Account

As a rule, when a Veeam Availability Console management agent is deployed, it is configured to use a Company Owner account to connect to Veeam Availability Console. However, management agents that run together with Veeam backup agents can connect to Veeam Availability Console under a subtenant account, instead of the Company Owner account.

You can modify an account under which a management agent connects to Veeam Availability Console.

- If an agent uses a Company Owner account, you may need to change it to a subtenant account.
- If an agent uses a subtenant account, you can change it to the company Owner account.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Changing Management Agent Connection Account

To change a connection account for a management agent:

1. Log in to Veeam Availability Console.
   
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Managed Computers.
3. Open the Discovered Computers tab.
4. Click Filter. In the Select agent status to display section, select the Installed, Warning or Inaccessible check boxes. Click Apply.
   
   The list of discovered computers will display computers with management agents installed.
5. Select the necessary computers in the list.
6. At the top of the list, click Management Agent and choose Edit Connection.
7. In the Veeam Management Agent Connection Settings window, specify a user name and password for a new connection account.
   
   - A Company Owner user name must be specified in the following format: <company_name>.
   - A subtenant user name must be specified in the following format: <company_name>\<subtenant_username>.
8. Click Apply.
   
   The management agent on a client computer will be restarted using the new connection account settings.
Uninstalling Management Agents

You can uninstall Veeam Availability Console management agents from managed computers. After you uninstall management agents from managed computers, you will no longer be able to manage backup software on these computers:

- Veeam Backup & Replication and Veeam Backup Enterprise Manager on Veeam backup servers.
- Veeam backup agents on managed computers.

When you uninstall a management agent from a computer protected with Veeam backup agent, the Veeam backup agent will be switched to the Unmanaged mode. The number of used and total licenses in the Veeam Availability Console license pool will be updated.

**NOTE:**
You cannot uninstall management agents with the Rejected status.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Uninstalling Management Agents

To uninstall Veeam Availability Console management agents from one or more managed computers:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Managed Computers.
3. Open the Discovered Computers tab.
4. Select the necessary computers in the list.
5. At the top of the list, click Management Agent and choose Delete.
6. In the displayed window, click Yes to confirm management agent removal.
Rebooting Remote Computers

In some cases, you might need to reboot computers that run Veeam Availability Console management agents. The most often cases when you need to perform computer reboot are:

- Installation of Veeam backup agents: if a pending computer reboot is detected during Veeam backup agent installation, you must reboot a computer to complete the installation process.
- Installation of the CBT Driver: after you install the CBT driver, you must reboot a computer.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Rebooting Remote Computers

To send a command to Veeam Availability Console management agents to initiate reboot of remote computers:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Managed Computers.
3. Open the Discovered Computers tab.
4. Select the necessary computers in the list.
5. At the top of the list, click Management Agent and choose Reboot Remote Computer.
6. In the displayed window, click Yes to confirm computer reboot.
Restarting Management Agent Service

Veeam Availability Console is implemented as a Veeam Management Agent Service that runs on a managed computer. If something goes wrong with this service, you might try to restart it on a managed computer.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Restarting Management Agent Service

To restart the management agent service on one or more managed computers:

1. Log in to Veeam Availability Console. For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Managed Computers.
3. Open the Discovered Computers tab.
4. Select the necessary computers in the list.
5. At the top of the list, click Management Agent and choose Restart Agent Service.
Collecting Data

By default, Veeam Availability Console management agents send data to Veeam Availability Console every hour, or when specific events, such as backup job failure, occur. If required, you can initiate unscheduled data collection from machines that run management agents. These can be machines hosting Veeam backup agents, Veeam Backup & Replication and Veeam Backup Enterprise Manager.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Collecting Data from Veeam Backup Agents

To initiate data collection from Veeam backup agents:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Managed Computers.
3. Open the Discovered Backup Agents tab.
4. Select one or more Veeam backup agents in the list.
5. Click Collect Data.

Collecting Data from Veeam Backup & Replication

To initiate data collection from Veeam Backup & Replication and Veeam Backup Enterprise Manager servers:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Managed Computers.
3. Open the Discovered Backup Servers tab.
4. Select one or more backup servers in the list.
5. Click Collect Data.
Viewing Invoices

In the Client Portal, you can view details of invoices that the Portal Administrator or Service Provider Administrator generated for your company. Invoices are available as PDF documents that you can view or download.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Company Invoice Auditor.

Viewing Invoices

To view invoice details:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Invoices.
   Veeam Availability Console will display a list of invoices. To narrow down the list of invoices, you can use the following filters:
   - **Status** — limit the list of invoices by payment status (Paid, Unpaid, Overdue, Information).
   - **Time period** — limit the list of invoices by generation date.
3. Select the necessary invoice in the list and click a link in the Invoice column.
   The invoice PDF file will be saved to the default download location on your computer.

Each invoice in the list is described with a set of properties. By default, some properties in the list are hidden. To display additional properties, click the ellipsis on the right of the list header and choose properties that must be displayed.

- **Invoice** — link to download an invoice.
- **Site** — name of a Veeam Cloud Connect site on which the company is registered.
- **Generated On** — date and time when an invoice was generated.
- **Due Date** — date by which a client company must make a payment.
• **Status** — invoice status.

• **Paid Date** — date when an invoice was marked as paid.

• **Total Sum** — total cost of consumed backup services calculated for an invoice.

• **Invoice ID** — number that uniquely identifies an invoice.

• **Subscription Plan** — name of a subscription plan which was used to charge a company in Veeam Availability Console.

### Types of Invoices

Information available in an invoice depends on the invoice type.

Veeam Availability Console offers three types of invoices:

• **Summary invoice** provides information about consumed services and their cost.

• **Detailed invoice** provides information about consumed services and their cost. In addition, a detailed invoice provides information about services consumed by each company location on each day of a specified period.

• **Quota usage report** provides information about services consumed by each company location on each day of a specified period. A quota usage report does not include cost details.

### Summary Invoice

A summary invoice provides information about consumed services and their cost.
An example of a summary invoice is shown below.

A summary invoice includes the following information:

- **Invoice ID** — number that uniquely identifies an invoice.
- **Generation date** — date when an invoice was generated, in the M/D/YYYY format.
- **Company quota usage** — billing period.
- **Payment due by** — date by which a company must make a payment. The payment date is one month after the invoice generation date. If an invoice is not paid by the due date, its status is changed to *Overdue*.
- **From** — name and contact details of the service provider.
- **To** — name and contact details of a managed company.
- **Summary** — charge rate information specified in the subscription plan, total gross cost, total tax and discount, as well as the invoice total. This section also includes the cost breakdown for all types of provided services.
Detailed Invoice

A detailed invoice provides information about consumed services and their cost. In addition, a detailed invoice provides information about services consumed by each company location on each day of a specified period.

An example of a detailed invoice is shown below.

A detailed invoice includes the following information:

- **Invoice ID** – number that uniquely identifies an invoice.
- **Generation date** – date when an invoice was generated, in the M/D/YYYY format.
- **Company resource usage** – billing period.
- **Payment due by** — date by which a company must make a payment. The payment date is one month after an invoice generation date. If an invoice is not paid by the due date, its status is changed to *Overdue*.

- **From** — name and contact details of the service provider.

- **To** — name and contact details of a managed company.

- **Summary** — charge rate information specified in the subscription plan, total gross cost, total tax and discount, as well as the invoice total. This section also includes the cost breakdown for all types of provided services.

- **Details** — information about services consumed by each company location on each day of the quota usage period.

**Quota Usage Report**

A quota usage report provides information about services consumed by each company location on each day of a specified period. A quota usage report does not include service cost details.
An example of a quota usage report is shown below.

A quota usage report includes the following information:

- **Generation date** — date when a report was generated, in the M/D/YYYY format.
- **Company quota usage** — period for which quota usage details are provided.
- **From** — name and contact details of the service provider.
- **To** — name and contact details of a managed company.
- **Details** — information about services consumed by each company location on each day of the quota usage period.
Receiving Billing Notifications

A billing notification is an email message with an attached invoice sent to a client. The following image illustrates what a billing notification looks like.

![Billing Notification](image)

Only the Company Owner can receive billing notifications. The Company Owner in the user profile can specify an email address at which billing notifications must be sent. For details, see Modifying Own User Profile.
Backup Reporting

To track the efficiency of data protection, you can create backup reports:

- **Protected Computers** report analyzes the efficiency of computer data protection with Veeam backup agents.
- **Protected VMs** report analyzes the efficiency of VM data protection with Veeam Backup & Replication.

Backup reports examine whether managed computers and VMs have backup or replica restore points created within the specified time range (RPO period), and provide information on the completion status of recent backup or replication job sessions. The reports can help you identify computers and VMs that function without a proper protection, and make sure the existing backups or replicas meet established RPO requirements.

In Veeam Availability Console, you can generate backup reports and send them by email to the Company Owner. Reports are sent as **PDF** files attached to report notifications. To automate reporting, you can configure a schedule according to which backup reports will be generated and report notifications will be sent.

To get started with backup reports, keep to the following sequence of steps:

1. **Configure backup report settings.**
   Specify settings of backup reports. When you configure a backup report, you can create a schedule according to which the report must be generated and sent. If you do not schedule backup reports, you will need to generate and send them manually.

2. **View backup reports.**
   View reports, generated manually or by the configured schedule.
Configuring Backup Reports

Before you run a backup report, you must create and save a report configuration. A report configuration stores custom report settings, such as the scope of the report, scheduling settings and so on. You can create multiple report configurations with different report settings for different locations.

Report configuration can be defined both in the Veeam Availability Console Administrator Portal and Client Portal. Report configurations created by the Portal Administrator for your company are available in your Client Portal. And vice versa, report configurations created in your Client Portal can be managed by the Portal Administrator.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Configuring Backup Reports

To create a report configuration:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Reports.
3. Open the Report Configuration tab.
4. At the top of the list, click New.
   Veeam Availability Console will launch the New Report wizard.
5. At the Report Template step of the wizard, select the report type:
   - Protected Computers — choose this option to create a report that will analyze computer data protection with Veeam backup agents.
- **Protected VMs** – choose this option to create a report that will analyze VM data protection with Veeam Backup & Replication.

6. **At the Name steps of the wizard, specify the report name and description.**

   The report name and description will be displayed in reports generated based on this report configuration.

   - Name: Beta Main Office
   - Description: Check daily backups for mission-critical computers in the main office.

7. **At the Locations step of the wizard, select one or more company locations. Use the search field at the top to find the necessary location.**
By choosing a location you can limit the scope of the report: only computers or VMs belonging to the chosen locations will be included in the report.

8. At the **Parameters** step of the wizard, specify report settings:

   a. In the **Select RPO** section, specify a period for which protected computers or VMs must have backup or replica restore points.

      RPO defines a period between backup sessions, or, in other words, a period for which you can afford to lose data. For example, if protected computers must have daily backups, specify 1 day or 24 hours as the RPO value.

   b. [For Protected Computers report] In the **Select operation mode** list, choose what type of OSes must be analyzed in the report (*All, Servers, Workstations*).

   c. [For Protected VMs report] In the **Select job type** list, choose what type of Veeam Backup & Replication jobs must be analyzed in the report (*All, Backup, Replication, Backup Copy, Backup to Tape*).

   d. In the **Exclusion mask names** field, specify a mask for excluding computers or VMs from the report scope.

      The mask will be evaluated against the computer or VM names. You can use the ‘*’ (asterisk) and ‘?’ (question mark) wildcards in the mask. The ‘*’ (asterisk) character stands for zero or more characters. The ‘?’ (question mark) stands for a single character. For example, if you want to exclude from the report VM replicas with default names created with Veeam Backup & Replication, you can specify a mask with the ‘*_replica’ name query.

      You can specify more than one mask in the field. Separate multiple masks with commas.
e. [For Protected Computers report] In the **Group By** list, choose how analyzed data must be grouped in the report (by *Agent* or *Backup Policy*).

### New Report

<table>
<thead>
<tr>
<th>Report Template</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td></td>
</tr>
<tr>
<td>Locations</td>
<td></td>
</tr>
<tr>
<td>Parameters</td>
<td></td>
</tr>
<tr>
<td>Schedule</td>
<td></td>
</tr>
<tr>
<td>Summary</td>
<td></td>
</tr>
</tbody>
</table>

**Parameters**

Specify parameters for this backup report.

- **Select RPX**: 10
- **Select job type**: All
- **Exclusion mask [names]**: ^_qa, _support

9. At the **Schedule** step of the wizard, specify a schedule according to which the report must be generated and sent to companies:

   - If you do not want to generate the report automatically, leave the **No schedule** option selected.

   In this case, you will need to generate and send the report manually. For details, see *Running Backup Reports* and *Sending Backup Reports*
To generate and send the report to the Company Owner automatically, in accordance with a specific schedule, select the **Daily at** option and specify when and how often the report must be generated and sent.

10. At the **Summary** step of the wizard, review the report configuration and click **Finish**.
Modifying Backup Report Configuration

You can modify settings of a saved backup report configuration. These can be report configurations created both in the Veeam Availability Console Client Portal, and configurations created by the Administrator Portal users.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Modifying Backup Report Configuration

To modify report configuration:

1. Log in to Veeam Availability Console. For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Reports.
3. Open the Report Configuration tab.
4. Select the necessary report configuration and click Edit at the top of the list.
5. Modify settings of the report configuration as described in Configuring Backup Reports. You can modify all report configuration settings except the report type.
6. Save changes.
Deleting Backup Report Configuration

You can delete saved backup report configurations that you no longer need. These can be report configurations created both in the Veeam Availability Console Client Portal, and configurations created by the Administrator Portal users.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Deleting Backup Report Configuration

To delete one or more backup report configurations:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Reports.
3. Open the Report Configuration tab.
4. Select the necessary report configurations and click Remove at the top of the list.
5. In the displayed window, click Yes to confirm removal.
Running Backup Reports

You can manually create backup reports based on saved report configurations. These can be report configurations created both in the Veeam Availability Console Client Portal, and configurations created by the Administrator Portal users.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Running Backup Reports

To create backup reports based on saved report configurations:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Reports.
3. Open the Report Configuration tab.
4. Select the necessary report configurations in the list.
5. At the top of the list, click Run.

Veeam Availability Console will save a manually created backup report in the report list but will not send a report notification to the Company Owner. To learn how to view details of generated reports, see Viewing Backup Reports.
Viewing Backup Reports

Backup reports that were generated manually or automatically, according to a specified schedule, are saved in the All Reports list. Backup reports are available as PDF documents that you can download and view.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator, Location User.

Viewing Backup Report

To view a backup report:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Reports.
   Veeam Availability Console will display a list of all generated backup reports. To narrow down the list of reports, you can use the following filters:
   - Name — search backup reports by report configuration name.
   - Type — limit the list of reports by type (VM Backup Reports, Backup Agent Reports).
   - Time period — limit the list of backup reports by generation date.
   - Location — limit the list of reports by location to which jobs belong. To limit the list of reports by location, use filters at the top left corner of the Veeam Availability Console window.
3. Select the necessary backup report in the list and click View at the top of the list.
   Alternatively, you can click a link in the Report column.
   The backup report PDF file will be saved to the default download location on your computer.

Protected Computers Backup Report

The Protected Computers report analyzes the efficiency of computer data protection with Veeam backup agents.

- The Report Parameters section provides information about company locations, RPO period and OS type of computers in the report scope, mask for the computers excluded from the report scope, and the way Veeam backup agent jobs are grouped in the report.
- The Summary section provides information about the number of company locations in the report scope and the number of discovered, protected and unprotected computers in each location.
- The report charts display information about protected and unprotected computers, the type and platform of computers protected with Veeam backup agents, the latest backup status of each job on protected computers and reasons for a failure to meet RPO requirements.
- The Details section provides information about all protected and unprotected computers including host name, backup policy name, backup source and target, number of available restore points and date and time of the latest backup.
The **Protected Agents** subsection displays a list of client computers that have at least one backup or replica restore point that meets RPO requirements specified in the report configuration. Information on protected computers in each company location is grouped by Veeam backup agent or backup policy, as configured in the report parameters.

The **Unprotected Agents** subsection displays a list of client computers that do not have valid backup or replica restore points within the configured RPO period. Information on unprotected computers in each company location is grouped by the age of the latest backup files.
Protected VMs Backup Report

The Protected VMs report analyzes the efficiency of VM data protection with Veeam Backup & Replication.

- The Report Parameters section provides information about company locations, RPO period and job type, type of VMs in the report scope and mask for the VMs excluded from the report scope.
- The Summary section provides information about the total number of VMs and the number of protected and unprotected VMs in each company location.
- The report charts display information about the number of VMs protected with Veeam Backup & Replication, and the latest backup status.
- The Details section provides information about all protected and unprotected VMs including VM name, backup job name and destination, backup type, number of available restore points and date and time of the latest backup.
- The Protected VMs subsection displays a list of VMs that have at least one backup or replica restore point that meets RPO requirements specified in the report configuration. Information on protected VMs in each company location is grouped by last backup state.
The **Unprotected VMs** subsection displays a list of VMs that have outdated or missing backup or replica restore points. Information on unprotected VMs in each company location is grouped by the age of the latest backup files.
Sending Backup Reports

If you specify a schedule in the backup report configuration, Veeam Availability Console will automatically send to the Company Owner report notifications with generated backup reports.

The following image illustrates what a backup report notification looks like.

You can also manually send backup reports to the Company Owner. You may need to send a backup report manually if the Company Owner did not receive a scheduled backup report for some reason, or if you want to send a manually generated backup report.

Before you send a backup report to the Company Owner, make sure that an email address is specified in the Company Owner user profile. For details, see Modifying Own User Profile.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Sending Backup Reports

To send one or more backup reports manually:

1. Log in to Veeam Availability Console.
For details, see Accessing Veeam Availability Console.

2. In the menu on the left, click Reports.
3. Select the necessary reports in the list.
4. Click Send.
5. In the displayed message box, click Yes to confirm sending.
Deleting Backup Reports

You can delete generated backup reports if you no longer need them. These can be report configurations created both in the Veeam Availability Console Client Portal, and configurations created by the Portal Administrator.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Deleting Backup Reports

To delete one or more generated backup reports:

1. Log in to Veeam Availability Console.
   
   For details, see Accessing Veeam Availability Console.

2. In the menu on the left, click Reports.

3. Select the necessary reports in the list.

4. Click Remove.

5. In the displayed window, click Yes to confirm removal.
Working with Alarms

Veeam Availability Console comes with a set of predefined alarms that notify about important events, state changes and potential problems in managed client backup infrastructures, and inform about issues with Veeam Availability Console. All alarms include detailed knowledge base articles. If a problem occurs, you will have all necessary information for troubleshooting and finding the root cause of an issue. For a list of predefined alarms, see Appendix B. Alarms.

Depending on your requirements, you can customize predefined alarms, modify alarm rules and change alarm response actions.

Alarm Rules

Alarms can be triggered in response to:

- Changed state of backup infrastructure objects
- Specific events
- Resource usage values exceeding or falling below thresholds

Conditions under which alarms must be triggered are described with alarm rules. You can customize alarm rules in accordance with your requirements.

Alarm Severity

Every triggered alarm has its own status, or alarm severity. Alarm severity defines how serious the state change or event is, and how badly it can affect a backup infrastructure object or hinder data protection.

There are four alarm severity levels, color-coded as follows:

- **Error** (red) indicates a critical situation or major problem that requires immediate action.
- **Warning** (yellow) indicates a potential problem or non-critical issue that needs your attention. If the issue is left without attention, it can potentially cause a major problem.
- **Resolved** (green) indicates that the issue was eliminated because the condition has changed, or shows that an alarm was resolved manually.
- **Information** (blue) indicates general information about a specific condition, or health state of a backup infrastructure object.

Alarm Response Actions

When an alarm is triggered, it becomes available in the **Active Alarms** dashboard in Veeam Availability Console. You can view alarms in Veeam Availability Console or can configure Veeam Availability Console to perform additional actions in response to triggered alarms or alarm status changes:

- Send an email notification with alarm details
- Run a custom script
- Perform both these actions at once

By default, all alarms are configured to send email notifications to Administrator when a new alarm is triggered or when the alarm status changes. If necessary, you can change alarm response actions in alarm settings.
Managing Alarms

Veeam Availability Console includes a set of predefined alarms that you can use to monitor client backup infrastructures. Depending on your requirements, you can customize alarms to meet specific monitoring conditions, change alarm assignment scope, enable and disable alarms, and export alarms configuration.

**NOTE:**

The following users can manage alarms in Veeam Availability Console: Portal Administrator, Location Administrator, Company Owner, Service Provider Global Administrator, Service Provider Administrator. Although all of these users can work with the same set of alarms, alarm configuration is not synchronized between the Administrator, Reseller and Client Portals. When you modify, enable or disable alarms as a Portal Administrator, these changes are not applied to alarms managed by a Company Owner or Location Administrator in the Client Portal.

A similar rule applies to alarm notifications: notifications about alarms configured in the Administrator Portal will be sent to Portal Administrators, while notifications about alarms configured in the Client Portal will be sent to Company Owners and Location Administrators.
Modifying Alarm Settings

You can modify alarm rules and response actions in accordance with your requirements.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Modifying Alarm Settings

To modify alarm settings, perform the following steps.

Step 1. Launch the Edit Alarm Wizard

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. At the top right corner of the Veeam Availability Console window, click Configuration.
3. In the configuration menu on the left, click Alarms Management.
4. Select an alarm you want to modify.
5. At the top of the list, click Edit.
   Alternatively, you can click a link in the Alarm Name column.

Veeam Availability Console will launch the Edit Alarm wizard.
Step 2. Specify Alarm Rules

At the **Rules** step of the wizard, specify conditions according to which the alarm must be triggered. Options available for alarm rules vary for different alarms. Depending on the alarm type, you may need to modify alarm thresholds, alarm tolerance, alarm severity and so on.

**TIP:**
You can use the following characters for masks:

- (*) — a substitution for one or more characters in the object name or path. Can be used for any sequence of characters (including no characters).
- (?) — a substitution of one character in the object name or path.

Step 3. Specify Alarm Response Actions

At the **Actions** step of the wizard, specify actions that must be performed when a new alarm is triggered, or when the status of an existing alarm changes.

Veeam Availability Console supports three types of response actions:

- You can send an email notification to Company Owner and Location Administrator, and at the email address that is specified in global notification settings
- You can send an email notification at a specified email address
- You can run a custom script

By default, all alarms are configured to send an email notification to Company Owner and Location Administrators and at the email address that is specified in global notification settings. Alarm notifications are sent each time when a new alarm is triggered, or when the status of an existing alarm changes. This response action is called *Use global notification settings*. You can modify the default alarm response action, or add new actions.
Sending Alarm Notifications by Email

You can add an alarm action that will send an email notification when a new alarm is triggered, or when the alarm status changes:

1. At the top right corner of the wizard, click Add.
2. In the Action field, choose Send email notification.
3. In the Value field, type an email address at which a notification must be sent.
4. In the Condition field, choose an alarm state that must trigger the response action:
   - Any state — select this option if a notification must be sent every time when the alarm status changes to Error, Warning or Info, or when a new alarm with one of these statuses is triggered.
   - Errors and warnings — select this option if a notification must be sent every time when the alarm status changes to Error or Warning, or when a new alarm with one of these statuses is triggered.
   - Errors only — select this option if a notification must be sent every time when the alarm status changes to Error, or when a new alarm with this status is triggered.

Running Custom Script

You can add an alarm action that will run a custom script when a new alarm is triggered, or when the alarm status changes. This can be a BAT, CMD, EXE or PS1 script.

By running a script, you can automate routine tasks that are normally performed when specific alarms fire. For example, if a critical system is affected, you may need to immediately open a ticket with the in-house support or perform actions that will eliminate the problem.

1. At the top right corner of the wizard, click Add.
2. In the Action field, choose Execute script.
3. In the Value field, type a path to the script file.
As a general rule, the script must reside on the machine for which the alarm was triggered.

On the client side, these can be machines that run Veeam Availability Console management agents:

- If an alarm targets the *Company* object, the script file can reside on managed Veeam backup agents or Veeam backup servers. When the alarm is triggered or when the alarm status changes, the script will run on all managed Veeam backup agents and Veeam backup servers of the company, provided that the script file is present on these machines. Note that the path to the script on all managed machines must be the same.

- If an alarm targets the *Location* object, the script file can reside on managed Veeam backup agents or Veeam backup servers. When the alarm is triggered for a specific location or when the alarm status changes, the script will run on all managed Veeam backup agents and Veeam backup servers that belong to the affected location, provided that the script file is present on these machines. Note that the path to the script on all managed machines must be the same.

- If an alarm targets a specific backup infrastructure component (Veeam backup agent, backup proxy, backup repository, WAN accelerator and so on), the script file must reside on the Veeam backup server that manages this component.

On the service provider side, this can be the Veeam Cloud Connect server, or the machine where Veeam Availability Console is installed. If you used a distributed deployment scenario, place the script on the machine where the Veeam Availability Console Server component runs.

4. In the **Condition** field, choose an alarm state that must trigger the response action:

- **Any state** — select this option if the script must run every time when the alarm status changes to *Error*, *Warning* or *Info*, or when a new alarm with one of these statuses is triggered.

- **Errors and warnings** — select this option if the script must run every time when the alarm status changes to *Error* or *Warning*, or when a new alarm with one of these statuses is triggered.

- **Errors only** — select this option if the script must run every time when the alarm status changes to *Error*, or when a new alarm with this status is triggered.
Step 4. Save Alarm Settings
At the Knowledge Base step of the wizard, click Finish to save alarm settings.

Modifying Multiple Alarms
Veeam Availability Console supports batch alarm editing. In the batch editing mode, you can change only alarm response actions.

Required Privileges
To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Modifying Multiple Alarms
To modify response actions of several alarms in batch:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.

2. At the top right corner of the Veeam Availability Console window, click Configuration.

3. In the configuration menu on the left, click Alarms Management.

4. Select alarms you want to modify.

5. At the top of the list, click Edit.

6. At the Actions step of the wizard, modify alarm response actions.
   For details, see Step 3. Specify Alarm Response Actions.

7. At the Knowledge Base step of the wizard, click Finish to save alarm settings.
Changing Alarm Assignment Scope

By default, alarms aimed to monitor client backup infrastructures are assigned to all companies and locations. If you do not want to check alarm conditions for a specific company or location, you can exclude this company or location from the alarm assignment scope. As a result, the alarm will never be triggered for the excluded company or location, even if the alarm conditions are met.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Changing Alarm Assignment Scope

To change the assignment scope for one or more alarms:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. At the top right corner of the Veeam Availability Console window, click Configuration.
3. In the configuration menu on the left, click Alarms Management.
4. Select one or more alarms in the list.
5. At the top of the list, click Assign.
6. In the Assign Alarm window, clear check boxes next to locations that must be excluded from the alarm assignment scope.
7. Clear the All new locations check box if all new locations you create in future must be excluded from the alarm assignment scope.
8. Click Apply.

After you exclude a company or location from the alarm assignment scope, you can check the excluded objects. To do so, find the necessary alarm in the list and click the Review link in the Exclusions column. In the Assign Alarm window, you can check and modify the alarm assignment scope if required.
Enabling and Disabling Alarms

You can enable and disable alarms.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Enabling Alarms

Out of the box, the most critical alarms are enabled. However, some alarms are disabled by default. These are non-critical alarms and alarms requiring that you review and customize alarm rules or assignment scope in accordance with your needs.

To enable one or more alarms:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. At the top right corner of the Veeam Availability Console window, click Configuration.
3. In the configuration menu on the left, click Alarms Management.
4. Select the necessary alarms in the list.
5. At the top of the list, click Enable.

Disabling Alarms

You can disable alarms that you do not use for monitoring. Disabled items will not trigger alarms for any companies and locations, even if the alarm conditions are met.

To disable one or more alarms:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. At the top right corner of the Veeam Availability Console window, click Configuration.
3. In the configuration menu on the left, click Alarms Management.
4. Select the necessary alarms in the list.
5. At the top of the alarm list, click Disable.

NOTE:

After you disable an alarm, all unresolved Warning or Error notifications that were triggered by this alarm will change their status to Resolved.
Exporting Alarm Configuration

You can export information about configured alarms to a CSV or XML file.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Exporting Alarm Configuration

To export alarm configuration to a CSV or XML file:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. At the top right corner of the Veeam Availability Console window, click Configuration.
3. In the configuration menu on the left, click Alarms Management.
4. Click Export and choose a format of the exported data:
   - Click Export CSV to structure exported data as a CSV file.
   - Click Export XML to structure exported data as an XML file.

The file with exported data will be saved to the default download location on your computer.
Receiving Alarm Email Notifications

To stay informed about potential problems in the managed backup infrastructure and get notified when you are approaching quota limits for allocated cloud resources, you can configure Veeam Availability Console to send email notifications about alarms.

To configure Veeam Availability Console to send email notifications with alarm details:

1. Specify email notification recipients.
   a. Specify email addresses of Location Administrators and Company Owner.
      By default, all alarms are configured to send email notifications to Location Administrators. When you create a new portal user, you must specify user's email address. If you assign the Location Administrator role to the portal user, Veeam Availability Console will send alarm notifications at the user's email address.
      If you are the Company Owner, and want to receive alarm notifications, make sure you have an email address specified in your user profile. For details on working with user profile details, see Modifying Own User Profile.
   b. Specify additional email notification recipients.
      You can configure Veeam Availability Console to send email notifications to users other than Location Administrators and Company Owner. To do so, you can add an alarm response action that will send an email to the necessary recipient.

2. Specify when email notifications must be sent.
   By default, Veeam Availability Console sends email notifications every time when a new alarm is triggered, or when the status of an existing alarm changes to Error or Warning. You can configure alarm response actions to send email notifications when an alarm acquires a specific status only. For example, you can choose to receive email notifications about errors and warnings only, and skip notifications about informational and resolved alarms.

The following image illustrates an email notification with alarm details.
Working with Triggered Alarms

Triggered alarms are available in the **Active Alarms** section of Veeam Availability Console. You can view the list of triggered alarms, check alarm details, resolve alarms, delete alarms you no longer need, and export triggered alarms to a file.
Resolving Alarms

Triggered alarms can be resolved automatically or manually.

Alarms are resolved automatically in the following cases:

- When an alarm is disabled. For details, see Enabling and Disabling Alarms.
- When conditions that caused the alarm are eliminated.

You can also resolve alarms manually if the state of the monitored object is back to normal, or if the alarm requires no further investigation, and no corrective actions must be taken.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Resolving Alarms

To manually resolve one or more alarms:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Active Alarms.
3. Select the necessary alarms in the list.
4. At the top of the alarm list, click Resolve.
5. In the Resolve Alarm window, specify a comment about resolving the alarm.
6. Click OK.

The specified alarm resolution comment will be available in the list of alarm status changes. To view the comment, click the N. of Repeats link for the triggered alarm, and then click the Comment link for the necessary status change. For details on viewing alarms, see Viewing and Exporting Triggered Alarms.
Deleting Alarms

You can delete triggered alarms if you no longer need to keep them in Veeam Availability Console.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Deleting Alarms

To delete one or more triggered alarms:

1. Log in to Veeam Availability Console. For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Active Alarms.
3. Select the necessary alarms in the list.
4. At the top of the alarm list, click Delete Alarm.
5. In the displayed window, click Yes to confirm removal.
Viewing and Exporting Triggered Alarms

You can view triggered alarms and export alarm details to a CSV or XML file.

Required Privileges

To perform this task, a user must have one of the following roles assigned: Company Owner, Location Administrator, Location User.

Viewing and Exporting Triggered Alarms

To view and export triggered alarm details:

1. Log in to Veeam Availability Console. For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Active Alarms. Veeam Availability Console will display a list of all triggered alarms.
   To narrow down the list of alarms, you can apply the following filters:
   - **Alarm** — search triggered alarms by name.
   - **Status** — limit the list of alarms by the alarm status (Resolved, Warning, Error, Info).
   - **Time Period** — limit the list of alarms by the time when alarms were triggered.
   - **Location** — limit the list of alarms by location for which alarms were triggered. To limit the list of alarms by location, use filters at the top left corner of the Veeam Availability Console window.
3. To view information about triggered alarms:
   - To view alarm details, click the alarm Status link.
   - To view an alarm cause and resolution steps, click the Alarm link.
   - To view the history of alarm status changes, click the N of Repeats link. In the displayed window, click Rules to view a condition that caused the alarm status change, or click the Comment link to view information on resolving the alarm.
4. To export alarm details, click Export and choose a format of the exported data:
   - **Export CSV** — choose this option to structure exported data as a CSV file.
   - **Export XML** — choose this option to structure exported data as an XML file.
The file with exported data will be saved to the default download location on your computer.

**Alarm Details**

Each alarm in the list is described with the following properties. By default, some properties in the list are hidden. To display additional properties, click the ellipsis on the right of the list header and choose properties that must be displayed.

- **Status** — alarm status (Resolved, Warning, Error, Info). Click the alarm status link to view alarm details.
- **Location** — name of a location for which the alarm was triggered.
- **Computer** — name of a machine where the alarm was registered (for example, client backup server, Veeam Availability Console server).
- **Time** — date and time when the alarm was triggered.
- **Alarm** — alarm name. Click the alarm name link to view a knowledge base article for the alarm.
- **Object** — name of an object that caused the alarm.
- **N. of Repeats** — number of times that the alarm changed its status. Click the alarm repeats link to view the alarm history.
Monitoring

Veeam Availability Console includes a set of dashboards that provide information about managed Veeam backup agents and VMs, as well as details about cloud resources.

- **Summary**
  This dashboard consolidates information about on computers protected with Veeam backup agents, VMs protected with Veeam Backup & Replication, as well as details on the amount of cloud resources consumed by the company.

- **Protected Computers**
  This dashboard shows the list of computers protected with Veeam backup agents, and VMs protected with Veeam Backup & Replication.
Summary

The Summary dashboard consolidates information about computers protected with Veeam backup agents, VMs protected with Veeam Backup & Replication, as well as details on the amount of cloud resources consumed by the company.

Required Privileges

To access this dashboard, a user must have one of the following roles assigned: Company Owner, Location Administrator, Location User.

Accessing Summary Dashboard

To access the Summary dashboard:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Summary.
3. Use tabs at the top to open the necessary dashboard view:
   - Agent Backup
   - VM Backup
   - Cloud Backup Quota
   - Cloud Replication Quota
Agent Backup

The **Agent Backup** dashboard view provides summary information about computers protected with Veeam backup agents. A protected computer is a computer that has at least one backup restore point.

The dashboard view includes the following widgets:

- **Protected Servers** widget shows the number of computers that run Veeam backup agents in the **Server** mode and have at least one backup restore point. The widget details the status of the latest Veeam backup agent job session, and shows how many job sessions completed successfully, or ended up with warnings or errors.

- **Protected Workstations** widget shows the number of computers that run Veeam backup agents in the **Workstation** mode and have at least one backup restore point. The widget shows the status of the latest Veeam backup agent job session, and shows how many job sessions completed successfully, or ended up with warnings or errors.

- **Protected Computers by Backup Target** widget shows types of target locations on which backups of protected computers are stored. The widget details how many Veeam backup agents store their backups locally, on cloud repositories, on a network share or on a Veeam Backup & Replication repository.

- **Protected Computers by Job Status** widget shows number of job sessions finished with different results. The widget details how many jobs finished successfully, finished with warning or failed.
VM Backup

The **VM Backup** dashboard view provides summary information about VMs protected with Veeam Backup & Replication. A protected VM is a VM that has a backup or replica restore point.

The dashboard view includes the following widgets:

- **Protected VMs** widget shows the number of protected VMs. The widget details the status of the latest Veeam Backup & Replication job session that protects the VMs, and shows how many job sessions completed successfully, or ended up with warnings or errors.

- **VMs by Backup Type** widget shows how many VMs are protected with backup and replication jobs.

- **VMs by Backup Copies** widget shows how many protected VMs have backup copies. The widget chart details the number of protected VMs that have backup copies stored offsite (in the cloud), locally on the client side, and the number of protected VMs without backup copies.
Cloud Backup Quota

The **Cloud Backup Quota** dashboard view provides information about cloud repository resources allocated for the company, used and remaining cloud resources.

The dashboard view includes the following widgets:

- **Used Storage** widget shows the amount of space allocated for the company on all cloud repositories, the amount of used and remaining space.

- **VMs Stored in Cloud Repository** widget shows the VM quota set for the company by the service provider, the number of VMs already stored in cloud repositories, and the remaining VM quota.

- **Workstations Stored in Cloud Repository** widget shows the workstation quota set for the company by the service provider, the number of workstations already stored in cloud repositories, and the remaining workstation quota.

- **Servers Stored in Cloud Repository** widget shows the server quota set for the company by the service provider, the number of servers already stored in cloud repositories, and the remaining server quota.
- **Data Transfer Out** widget shows the data transfer out quota set for the company by the service provider, the amount of data already downloaded from cloud repositories during the current billing period (length of time between two successive invoices), and the remaining data transfer out quota.

## Cloud Replication Quota

The **Cloud Backup Quota** dashboard view provides information about cloud host resources allocated for the company, used and remaining cloud resources.

The dashboard view includes the following widgets:

- **Used CPU Resources** widget shows the number of configured vCPUs, and the number of cloud VM replicas on which these vCPUs are configured.
  
  By default, the widget shows information for all hardware plans by which the company is subscribed. To choose a specific hardware plan, use the list at the top of the widget.

- **User Cloud Memory** widget shows the amount of memory allocated for cloud VM replicas, the amount of already used memory, and the remaining memory.

- **Used Cloud Storage** widget shows the amount of cloud storage space allocated for the company cloud VM replicas, the amount of used and remaining space.
Protected Computers

The Protected VMs view shows the list of computers protected with Veeam backup agents, and VMs protected with Veeam Backup & Replication.

Required Privileges

To access this dashboard, a user must have one of the following roles assigned: Company Owner, Location Administrator, Location User.

Accessing Summary Dashboard

To access the Protected Computers dashboard:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Protected Computers.
3. Use tabs at the top to open the necessary dashboard view:
   - Computers
   - Virtual Machines

Computers

The Computers dashboard view shows the list of computers protected with Veeam backup agents. A protected computer is a computer that has at least one backup restore point.

You can use the following filters to narrow down the list of protected computers:

- **Name** — search the list of computers by name.
- **Operation mode** — limit the list of computers by operation mode (Server, Workstation).
- **Cloud copy** — limit the list of computers by cloud copy existence (Yes, No).
- **Backup type** – limit the list of computers by backup type (*Entire OS, Volume-level, File-level*).

Each computer in the list is described with a set of properties.

- **Name** – name of a managed computer on which Veeam backup agent is deployed.
- **N. of Jobs** – number of finished backup jobs.

You can click this property to view details of backup job sessions in which the managed computer is included.

The following additional details are available for a job:

- **Backup Policy** – name of a backup policy assigned to Veeam backup agent.
- **Operation Mode** – backup job operation mode (*Workstation, Server*).
- **Backup Type** – type of backup (*Entire OS, Volume-level, File-level*).
- **Restore Points** – number of restore points available in the backup chain for a managed computer.
- **Latest Restore Point** – date and time when the latest restore point was created.
- **Backup Size** – total size of all restore points for a managed computer.
- **Destination** – location where backup files for a managed computer reside.
- **Next Job Run** – date and time of the next backup job session according to the backup schedule.

- **Guest OS** – guest OS on a managed computer.
- **Latest Restore Point** – shows how long ago the latest restore point was created.
- **Cloud Copy** – existence of cloud copy (*Yes, No*).
- **Site** – name of Veeam Cloud Connect repository whose resources are allocated to a protected computer.
- **Location** – location to which a protected computer belongs.
Virtual Machines

The **Virtual Machines** dashboard view shows the list of computers protected with Veeam Backup & Replication. A protected VM is a VM that has at least one backup or replica restore point.

You can use the following filters to narrow down the list of protected computers:

- **VM Name** — search the list of VMs by name.
- **Type** — limit the list of VMs by job type (*Backup, Replication, Backup copy*).
- **Backup location** — limit the list of VMs by backup target (*Offsite copy, Local copy*).

Each VM in the list is described with a set of properties.

- **VM** — VM name.
- **Backup Server** — name of a backup server on which a protecting job is configured.
- **Backup Job** — name of a job that protects a VM.
- **Backup Type** — type of job that protects a VM (*Backup, Backup Copy, Replication*).
- **Restore Points** — number of restore points created for a VM by a protecting job.
- **Latest Restore Point** — date and time when the latest restore point was created for a VM.
- **Destination** — repository where VM backup is located (for backup and backup copy jobs) or repository where VM metadata is stored (for replication jobs).
- **Location** — location to which a backup server belongs.
Managing Portal Users

By default, the only user that can access the Client Portal is the Company Owner. To allow other employees in your company work with the Veeam Availability Console Client Portal, you can create new portal users with the necessary user permissions.
User Roles and Permissions

When you create a new user that can work with the Veeam Availability Console Client Portal, you must assign a role to this user. A user role defines permissions for a user, that is, what operations a user can perform, and what scope of data is available to a user in Veeam Availability Console.

Veeam Availability Console supports the following user roles for client companies:

- Company Owner
- Location Administrator
- Location User
- Subtenant
- Company Invoice Auditor

Company Owner

Company Owner is the primary user acting on behalf of a company that consumes provided backup services. The Company Owner user is created when a company account is registered in Veeam Availability Console. For each company, there can be only one Company Owner.

You can think of the Company Owner as of a super user at the company level. In the Client Portal, the Company Owner has access to all monitoring and billing data for all company locations, and can perform all types of available configuration and management operations.

Location Administrator

Location Administrator has a similar set of privileges as the Company Owner, with a number of limitations:

- Location Administrator does not have access to billing information
- The scope of data available to a Location Administrator can be limited to one or more company locations

Location User

Location User has access to company monitoring data, but cannot perform most configuration and management tasks. This user can only work with the functionality available in the Veeam Availability Console Client Portal. Data available to a Location User can be limited to one or more company locations, and the user can access data pertaining to all managed Veeam backup agents, Veeam Backup & Replication or Veeam Backup Enterprise Manager servers in these locations.

Subtenant

A Subtenant is a user who has cloud repository resources allocated and acts as a subtenant in Veeam Cloud Connect. This user can store backups created with Veeam backup agent, using own credentials. In addition, a Subtenant has access to the Client Portal. The scope of monitoring data available to a Subtenant in the Client Portal is limited to a computer (or computers) that is protected with Veeam backup agent, and whose data is stored on a cloud repository.

For details on Veeam Cloud Connect subtenants, see Veeam Cloud Connect Administrator Guide, section Subtenants.
Company Invoice Auditor

Company Invoice Auditor has access to billing details pertaining to a company. This user can view invoices and receive billing notifications.

User Permissions

The following table describes what functionality is available to company users in the Client Portal in accordance with their user role.

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Company Owner</th>
<th>Location Administrator</th>
<th>Location User</th>
<th>Subtenant</th>
<th>Company Invoice Auditor</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuration tasks</strong></td>
<td>Full</td>
<td>Full</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>(locations, portal users, backup policies, alarms, company info)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Veeam Backup &amp; Replication jobs</strong></td>
<td>Full</td>
<td>Full</td>
<td>Read</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Veeam backup agent jobs</strong></td>
<td>Full</td>
<td>Full</td>
<td>Read</td>
<td>Read*</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Failover plans</strong></td>
<td>Full</td>
<td>Full</td>
<td>Read</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Discovery rules</strong></td>
<td>Full</td>
<td>Full</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Managed computers</strong></td>
<td>Full</td>
<td>Full</td>
<td>Read</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Invoices</strong></td>
<td>Read</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Read</td>
</tr>
<tr>
<td><strong>Backup reports</strong></td>
<td>Full</td>
<td>Full</td>
<td>Read</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Summary</strong></td>
<td>Read</td>
<td>Read</td>
<td>Read</td>
<td>Read*</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Active alarms</strong></td>
<td>Full</td>
<td>Full</td>
<td>Read</td>
<td>Read*</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Protected computers</strong></td>
<td>Read</td>
<td>Read</td>
<td>Read</td>
<td>Read*</td>
<td>N/A</td>
</tr>
</tbody>
</table>

* Limited to computers protected with Veeam backup agents, with backups stored on a cloud repository under the account of a Subtenant User.
Creating Portal Users

To allow employees in the company work with the Client Portal, you can create new portal users:

- Location Administrators
- Location Users
- Subtenants
- Company Invoice Auditors
Creating Location Administrators

You can create new users with the Location Administrator role.

Required Privileges

To perform the task, a user must have one of the following roles assigned: Company Owner.

Creating Location Administrators

To create a new Location Administrator in Veeam Availability Console:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. At the top right corner of the Veeam Availability Console window, click Configuration.
3. In the configuration menu on the left, click Portal Users.
4. At the top of the user list, click New.
   Veeam Availability Console will launch the New User wizard.
5. At the User Info step of the wizard, specify user’s title, first name, last name and email address.
   Veeam Availability Console can use this address to send email notifications to the user, such as password reset notifications and so on.
6. At the Login Info step of the wizard, specify user credentials and choose a user role:
   a. In the Username, Password and Confirm Password fields, type a user name and password.
      The password must contain characters from at least 3 of the following categories: uppercase characters, lowercase characters, base 10 digits (0 through 9), non-alphanumeric characters. The password length must be at least 6 characters.
b. In the **Role** field, choose *Location Administrator*.

7. At the **Locations** step of the wizard, select company locations whose data must be available for the user in the Client Portal.
8. At the **Summary** step of the wizard, review user details and click **Finish**.

![User details summary](image-url)
Creating Location Users

You can create new users with the Location User role.

Required Privileges

To perform the task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Creating Location Users

To create a new Location User in Veeam Availability Console:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. At the top right corner of the Veeam Availability Console window, click Configuration.
3. In the configuration menu on the left, click Portal Users.
4. At the top of the user list, click New.
   Veeam Availability Console will launch the New User wizard.
5. At the User Info step of the wizard, specify user’s title, first name, last name and email address.
   Veeam Availability Console can use this address to send email notifications to the user, such as password reset notifications.

   ![New User Wizard Screenshot]

6. At the Login Info step of the wizard, specify user credentials and choose a user role:
   a. In the Username, Password and Confirm Password fields, type a user name and password.
      The password must contain characters from at least 3 of the following categories: uppercase characters, lowercase characters, base 10 digits (0 through 9), non-alphanumeric characters.
b. In the Role field, choose Location User.

7. At the Locations step of the wizard, select company locations whose data must be available for the user in the Client Portal.
8. At the **Summary** step of the wizard, review user details and click **Finish**.
Creating Subtenants

You can create a new portal user with the Subtenant role and allocate to this user cloud repository space, or user quota. A user quota is an amount of storage space allocated for specific user within the company quota on a cloud repository.

A Subtenant can consume storage resources provided through the user quota for storing Veeam agent backups in the cloud. When pointing a Veeam backup agent job to a cloud repository, you can specify credentials of a Subtenant. Backup files created by the Veeam backup agent job will consume cloud space within the Subtenant quota only.

In addition to storing backups on a cloud repository, a Subtenant can access the Veeam Availability Console Client Portal. The scope of monitoring data available to a Subtenant in the Client Portal is limited to a computer (or computers) protected with Veeam backup agents whose data is stored on a cloud repository under the account of the Subtenant. That is, a Subtenant can view details only about those Veeam backup agents that are configured to store backup data to the cloud under credentials of this user.

Required Privileges

To perform the task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Creating Subtenants

To create a new Subtenant in Veeam Availability Console:

1. Log in to Veeam Availability Console. For details, see Accessing Veeam Availability Console.
2. At the top right corner of the Veeam Availability Console window, click Configuration.
3. In the configuration menu on the left, click Portal Users.
4. At the top of the user list, click New.
   Veeam Availability Console will launch the New User wizard.
5. At the User Info step of the wizard, specify user’s title, first name, last name and email address.
Veeam Availability Console can use this address to send email notifications to the user, such as password reset notifications.

6. At the Login Info step of the wizard, specify user credentials and choose a user role:
   
a. In the Username, Password and Confirm Password fields, type a user name and password. The password must contain characters from at least 3 of the following categories: uppercase characters, lowercase characters, base 10 digits (0 through 9), non-alphanumeric characters. The password length must be at least 6 characters.

   b. In the Role field, choose Subtenant.
7. At the **Locations** step of the wizard, select company locations whose data must be available for the user in the Client Portal.

8. At the **Quota** step of the wizard, allocate cloud repository resources to the user.

   You can specify the size of the user quota or create an unlimited user quota. With an unlimited user quota, the Subtenant can consume all storage space within the company quota on a cloud repository.
9. At the **Summary** step of the wizard, review user details and click **Finish**.

### Automatic Creation of Subtenants

Veeam Availability Console can automatically create Subtenants. This normally happens if you use a backup policy that is configured to store backup data on a cloud repository and to create subtenant accounts for each managed Veeam backup agent automatically. When such backup policy is assigned to Veeam backup agents, Veeam Availability Console creates a Subtenant account for each Veeam backup agent to which the backup policy is assigned. For details, see Step 14. Specify Cloud Repository Quota.

Veeam backup agents use these Subtenant accounts to write data to a cloud repository. The name of each Subtenant account is formed according to the following pattern: `<company_name>_<computer_name>`. 
Creating Company Invoice Auditors

You can create new users with the Company Invoice Auditor role.

Required Privileges

To perform the task, a user must have one of the following roles assigned: Company Owner.

Creating Company Invoice Auditors

To create a new Invoice Auditor in Veeam Availability Console:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. At the top right corner of the Veeam Availability Console window, click Configuration.
3. In the configuration menu on the left, click Portal Users.
4. At the top of the user list, click New.
   Veeam Availability Console will launch the New User wizard.
5. At the User Info step of the wizard, specify user's title, first name, last name and email address.
   Veeam Availability Console can use this address to send email notifications to the user, such as backup report notifications, password reset notifications and so on.
6. At the Login Info step of the wizard, specify user credentials and choose a user role:
   a. In the Username, Password and Confirm Password fields, type a user name and password.
      The password must contain characters from at least 3 of the following categories: uppercase characters, lowercase characters, base 10 digits (0 through 9), non-alphanumeric characters. The password length must be at least 6 characters.
b. In the **Role** field, choose *Company Invoice Auditor*.

![New User form](image)

7. At the **Summary** step of the wizard, review user details.

   If you want to send to the user all company invoices, select the **Enable automatic delivery of invoices for this user** check box. Veeam Availability Console will send the invoices automatically after generation.

![New User form](image)

8. Click **Finish**.
Modifying Portal Users

You can modify settings of Veeam Availability Console portal users.

Required Privileges

To perform the task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

- Company Owner can modify settings for users having any role assigned
- Location Administrator can modify settings for any users except Company Owner.

Modifying Portal User Settings

To modify settings of portal users:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. At the top right corner of the Veeam Availability Console window, click Configuration.
3. In the configuration menu on the left, click Portal Users.
4. Select the necessary user in the list.
5. At the top of the user list, click Edit.
6. Modify user settings as described in Creating Portal Users.
   You can modify all settings except the user name.
7. Save changes.

NOTE:

When modifying Company Owner details, especially the password for this user, mind the following:

- After you modify the password, the client will need to reconnect to the service provider.
  Connection settings must be reconfigured for all machines that run Veeam Availability Console management agents, such as Veeam Backup & Replication servers and Veeam backup agents — provided that management agents connect to Veeam Availability Console under the Company Owner account.
- The password change is applied immediately, without waiting for any running tasks to complete. If you modify the password while client's backup to cloud, backup copy to cloud or replication to cloud jobs are still running, these jobs will fail because of lost connection to cloud repositories and hosts.
Removing Portal Users

You can remove portal users that you previously created for your company.

**NOTE:**

When removing portal users, mind the following limitations:

- You cannot remove the Company Owner user. This user can be removed by the Portal Administrator only.
- You cannot remove a Subtenant if credentials of this user are specified in a Veeam backup agent job settings. This situation is possible if you configured a backup job to write data to a cloud repository under an account of the Subtenant you plan to remove. Before you can remove the user, you must specify another account in the Veeam backup agent job settings. For details on changing Veeam backup agent job settings, see Configuring Backup Job Settings for Individual Computers.

**Required Privileges**

To perform the task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

- Company Owner can delete users having any role assigned
- Location Administrator can delete any users except Company Owner.

**Removing Portal Users**

To remove one or more portal users:

1. Log in to Veeam Availability Console. For details, see Accessing Veeam Availability Console.
2. At the top right corner of the Veeam Availability Console window, click **Configuration**.
3. In the configuration menu on the left, click **Portal Users**.
4. Select the necessary users in the list.
5. At the top of the user list, click **Remove**.
6. In the **Remove User** window click **Yes**.
Disabling and Enabling Portal Users

To control access to the Veeam Availability Console Client Portal, you can enable and disable users.

Required Privileges

To perform the task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

- Company Owner can disable and enable users having any role assigned
- Location Administrator can disable and enable Location Users only

Disabling Portal Users

To prevent a user from accessing the Veeam Availability Console Client Portal, you can disable this user.

**NOTE:**

You cannot disable a Subtenant if credentials of this user are specified in a Veeam backup agent job settings. This situation is possible if you configured a backup job to write data to a cloud repository under an account of the Subtenant you plan to disable. Before you can disable the user, you must specify another account in the Veeam backup agent job settings. For details on changing Veeam backup agent job settings, see Configuring Backup Job Settings for Individual Computers.

To disable a portal user:
1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. At the top right corner of the Veeam Availability Console window, click Configuration.
3. In the configuration menu on the left, click Portal Users.
4. Select the necessary users in the list.
5. At the top of the user list, click Disable.
6. In the Change Users Status window, click Yes.

Enabling Portal Users

To enable a portal user you previously disabled:
1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. At the top right corner of the Veeam Availability Console window, click Configuration.
3. In the configuration menu on the left, click Portal Users.
4. Select the necessary users in the list.
5. At the top of the user list, click Enable.
6. In the **Change Users Status** window, click **Yes**.
Modifying Own User Profile

All portal users working with the Veeam Availability Console Client Portal can modify their user profile to update contact information and password:

1. Log in to Veeam Availability Console.  
   For details, see Accessing Veeam Availability Console.

2. At the top right corner, click your user name and choose Edit Profile.  
   Veeam Availability Console will open the Edit User wizard.

3. At the User Info step of the wizard, you can modify your title, first name, last name and email address.  
   Veeam Availability Console will use this address to send you email notifications, such as billing notifications, backup report notifications, password reset notifications and so on.

4. At the Login Info step of the wizard, you can change your password details:
   a. In the Current Password field, type your current password.
   b. In the New Password and Confirm Password fields, type a new password.
      The password must contain characters from at least 3 of the following categories: uppercase characters, lowercase characters, base 10 digits (0 through 9), non-alphanumeric characters. The password length must be at least 6 characters.
   c. In the Security Question and Answer fields, choose a question and specify an answer that will be used for resetting the user password.
For details on user roles, see Resetting Password.

5. At the Summary step of the wizard, review the specified details.

   [For Company Owner, Company Invoice Auditor] Select the **Enable automatic delivery of invoices for this user** check box if you want to receive a billing notification by email each time when a new invoice for the company is generated and sent. For details, see Receiving Billing Notifications.

6. Click Finish.
Managing Locations

Your company may run multiple Veeam backup agents, Veeam Backup & Replication and Veeam Backup Enterprise Manager servers located in different remote offices and branch offices (ROBO). To differentiate backup services and cloud resources consumed by each office, you can use locations.

A **location** is a logical group that can include one or more managed Veeam backup agents, Veeam Backup & Replication and Veeam Backup Enterprise Manager servers. By default, all managed machines are grouped into a pre-configured system location — **Default location**. In addition to the system location, you can create locations for remote and branch offices where you have managed Veeam backup agents, Veeam Backup & Replication and Veeam Backup Enterprise Manager servers, and move managed machines to these locations.

Locations are leveraged in different areas of Veeam Availability Console, and can be very useful when it comes to controlling the scope of information about managed objects.

### Tracking Consumed Services in Invoices

You can use locations to keep track of the type and amount of backup services and cloud resources consumed by different offices or business units in your company. If you configure multiple locations for your company, invoices will provide a breakdown of costs by location. Thus, you can track the cost of backup services provided for specific locations.

For details on details available in invoices, see [Viewing Invoices](#).

### Limiting Data Scope in the Client Portal

Locations can serve as an instrument of controlling the scope of data that must be available to company users in the Client Portal. When you create a new Location Administrator or Location User, you can choose locations that must be available to this user. By assigning specific locations to a user, you limit the scope of managed Veeam backup agents, Veeam Backup & Replication and Veeam Backup Enterprise Manager servers whose details will be available to the user in the Client Portal.

For details on working with portal users, see [Managing Portal Users](#).

### Filtering Data in Monitoring Dashboards and Alarms

You can use locations to filter the scope of monitoring data.

Monitoring dashboards in the Client Portal allow you either to filter or sort monitoring data by location, so that you could concentrate on details pertaining to specific offices or business units within your company.

For details on monitoring dashboards, see [Monitoring](#).

Monitoring alarms also come with support for locations. Veeam Availability Console includes predefined alarms that allow you to track the amount of cloud repository space consumed by each location, and alert on unprotected VMs in company offices. To fine-tune alerting, you can also customize alarms to suit the needs of different offices, and assign these alarms to specific locations.

For details on alarms, see [Working with Alarms](#).
Creating Locations

You can create new company locations to differentiate backup services and cloud resources consumed by offices or business units in your company.

Required Privileges

To perform the task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Creating Locations

To create a new company location:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. At the top right corner of the Veeam Availability Console window, click Configuration.
3. In the configuration menu on the left, click Locations.
4. At the top of the location list, click New.
5. In the New Location window, specify location settings:
   a. In the Name field, specify a location name.
   b. In the Cloud repository storage quota field, specify the maximum amount of cloud repository space that must be available for this location. This amount cannot be greater that the total cloud repository storage quota for your company.

   The specified cloud repository storage quota is used as a threshold for the Summary dashboard and for the Company cloud storage quota alarm. It does not limit the actual amount of data that can be uploaded from the location to cloud repositories.

6. Click OK.

When you create a new location, the cloud repository storage quota of the Default location is decreased by the amount of the cloud repository storage quota set for the new location.

What to Do Next

After you create new locations, you can define what machines and what users will be associated with the new location. For details, see Setting Locations.
Setting Locations

You can set locations for managed machines running Veeam Backup & Replication, Veeam Backup Enterprise Manager and Veeam backup agents. By default, all managed Veeam backup agents, Veeam Backup & Replication and Veeam Backup Enterprise Manager servers reside in the Default location. By setting a new location, you 'move' a managed machine to a new logical group.

You can also set locations for company users to control the scope of data that must be available to these users in the Client Portal. A user working with the Client Portal can only work with details of managed machines that are included in the scope of a location, or locations, to which this user is subscribed.

Required Privileges

To perform the task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Setting Locations for Veeam Backup & Replication Servers

To set a location for one or more Veeam Backup & Replication or Veeam Backup Enterprise Manager servers:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Managed Computers.
3. Open the Discovered Backup Servers tab.
4. Select the necessary backup servers in the list.
5. At the top of the list, click Set Location.
6. In the Set Location window, choose a location to which selected backup servers must be moved.
7. Click OK.

Setting Locations for Discovered Computers

To set a location for one or more discovered computers:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Managed Computers.
3. Open the Discovered Computers tab.
4. Select the necessary Veeam backup agents in the list.
5. At the top of the list, click Management Agent and select Set Location.
6. In the Set Location window, choose a location to which selected Veeam backup agents must be moved.
7. Click OK.
Setting Locations for Discovered Veeam Backup Agents

To set a location for one or more managed discovered Veeam backup agents:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. In the menu on the left, click Managed Computers.
3. Open the Discovered Backup Agents tab.
4. Select the necessary agents in the list.
5. At the top of the list, click Backup Agent and select Set Location.
6. In the Set Location window, choose a location to which selected Veeam backup agents must be moved.
7. Click OK.

Setting Locations for Portal Users

To restrict the scope of data that must be available to company users in Veeam Availability Console, you can choose locations for these users. You can set locations for Location Administrators and Location Users.

To set a location for one or more company users:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. At the top right corner of the Veeam Availability Console window, click Configuration.
3. In the configuration menu on the left, click Portal Users.
4. Select the necessary company users in the list and click Set Location.
5. In the Edit User window, choose a location to which selected users must have access.
6. Click OK.
Modifying Locations
You can modify settings of previously created locations.

Required Privileges
To perform the task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Modifying Location Settings
To modify location settings:

1. Log in to Veeam Availability Console.
   For details, see Accessing Veeam Availability Console.
2. At the top right corner of the Veeam Availability Console window, click Configuration.
3. In the configuration menu on the left, click Locations.
4. Select the necessary location in the list.
5. At the top of the location list, click Edit.
6. Modify location settings as described in Creating Locations.
7. Click OK.

NOTE:
- You cannot change cloud repository storage quota for the Default location. Quota for this location is managed by Veeam Availability Console.
- If you change the cloud repository storage quota, the quota of the Default location will be updated as well. If the cloud repository storage quota is increased, the quota of the Default location will be decreased by the increase amount, and if the cloud repository storage quota is decreased, the quota of the Default location will be increased.
Removing Locations

If you no longer need a location, you can remove it. After you remove a location, all Veeam backup agents, Veeam Backup & Replication and Veeam Backup Enterprise Manager servers associated with this location will be moved to the Default location. The cloud repository storage quota of the removed location will be added to the quota of the Default location.

NOTE:
- You cannot remove the Default location.
- You cannot remove a location if this location includes managed Veeam Backup & Replication, Veeam Backup Enterprise Manager servers or Veeam backup agents. Before you remove such a location, move managed machines to a new location. For details, see Setting Locations.
- You cannot remove a location if this location has associated portal users, except the Company Owner. Before you remove such a location, modify settings of portal users to remove from the visibility scope a location you plan to remove. For details, see Modifying Portal Users.

Required Privileges

To perform the task, a user must have one of the following roles assigned: Company Owner, Location Administrator.

Removing Locations

To remove a location:

1. Log in to Veeam Availability Console. For details, see Accessing Veeam Availability Console.
2. At the top right corner of the Veeam Availability Console window, click Configuration.
3. In the configuration menu on the left, click Locations.
4. Select the necessary location in the list.
5. At the top of the location list, click Remove.
Appendix A. Advanced Installation and Configuration Procedures

This section describes advanced procedures that you might need to perform when installing and configuring Veeam Availability Console software components. Each topic in this section describes a specific use case, and provides instructions that you must follow to achieve the result.
How to Upload Veeam Backup Agent Setup File to Client Computers with GPO

This topic describes how you can upload the Veeam backup agent setup file to client computers using GPO. The procedure can be required if you do not want or cannot download the Veeam backup agent setup file from the Veeam Installation Server (over the Internet) during installation. For details, see Initiating Installation in Veeam Availability Console.

To create a Group Policy that will copy the Veeam backup agent setup file to client computers:

1. Download a setup file for the supported version of Veeam backup agent, and place its setup file it to a network share.
   The network share must be accessible from all computers on which you want to install Veeam backup agents.
   Make sure you set at least Read permissions on the file.
2. Log on to a domain controller.
3. Open the Group Policy Management Console.
4. Right-click the OU that includes computers that must be protected with Veeam Agent for Microsoft Windows, and choose to create a new Group Policy Object.
5. Right-click the Group Policy Object and choose Edit.
6. In the left pane of the Group Policy Management Editor, expand Computer Configuration > Preferences > Windows Settings.
7. Right-click Files and select New > File.
8. In the New File Properties window, specify the following settings:
   a. In the Action list, choose Create.
   b. In the Source file(s) field, specify the path to the Veeam backup agent setup file located on a network share.
   c. In the Destination File field, specify a path to the Veeam backup agent setup file on a client computer.
      You must specify the following path to the file, including the file name:
      C:\ProgramData\Veeam\Veeam Availability Console\AgentPackage\VeeamAgentWindows.exe.
9. Click OK.
10. Close the Group Policy Management Editor.
Appendix B. Alarms

Veeam Availability Console includes a set of predefined alarms described in the following table.

<table>
<thead>
<tr>
<th>Alarm Name</th>
<th>Alarm Description</th>
<th>Object</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup agent connection state</td>
<td>This alarm checks whether a Veeam backup agent is running or can be contacted.</td>
<td>Backup agent</td>
<td>Yes</td>
</tr>
<tr>
<td>Backup agent job state</td>
<td>This alarm checks whether a Veeam backup agent job session failed or finished with a warning.</td>
<td>Backup agent job</td>
<td>Yes</td>
</tr>
<tr>
<td>Backup agent job state (managed by backup server)</td>
<td>This alarm checks whether a Veeam backup agent job session configured on a Veeam Backup &amp; Replication server failed or finished with a warning.</td>
<td>Backup agent job</td>
<td>Yes</td>
</tr>
<tr>
<td>Backup Enterprise Manager connection state</td>
<td>This alarm checks whether the Veeam Backup Enterprise Manager service is running.</td>
<td>Enterprise Manager</td>
<td>Yes</td>
</tr>
<tr>
<td>Backup proxy connection state</td>
<td>This alarm checks the connection status between a Veeam backup server and backup proxy.</td>
<td>Backup proxy</td>
<td>Yes</td>
</tr>
<tr>
<td>Backup proxy version is out-of-date</td>
<td>This alarm checks whether the version of a backup proxy matches the version of Veeam Backup &amp; Replication installed on a backup server.</td>
<td>Backup proxy</td>
<td>Yes</td>
</tr>
<tr>
<td>Backup repository connection state</td>
<td>This alarm checks the connection status between a Veeam backup server and backup repository.</td>
<td>Backup repository</td>
<td>Yes</td>
</tr>
<tr>
<td>Backup repository version is out-of-date</td>
<td>This alarm checks whether the version of a backup repository matches the version of Veeam Backup &amp; Replication installed on a backup server.</td>
<td>Backup repository</td>
<td>Yes</td>
</tr>
<tr>
<td>Backup server connection state</td>
<td>This alarm checks whether the Veeam Backup Service is running on a backup server.</td>
<td>Backup server</td>
<td>Yes</td>
</tr>
<tr>
<td>Backup server license exceeded</td>
<td>This alarm checks whether the Veeam Backup &amp; Replication product license has been exceeded.</td>
<td>Backup server</td>
<td>Yes</td>
</tr>
<tr>
<td>Backup server license expiration</td>
<td>This alarm checks whether the Veeam Backup &amp; Replication product license has expired.</td>
<td>Backup server</td>
<td>Yes</td>
</tr>
<tr>
<td>Backup server support contract expiration</td>
<td>This alarm checks whether the Veeam Backup &amp; Replication support contract has expired.</td>
<td>Backup server</td>
<td>Yes</td>
</tr>
<tr>
<td>Alarm Description</td>
<td>Description</td>
<td>Category</td>
<td>Status</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>--------</td>
</tr>
<tr>
<td>Company cloud host memory quota</td>
<td>This alarm tracks whether the total amount of configured memory for cloud replicas has breached the configured threshold.</td>
<td>Company</td>
<td>Yes</td>
</tr>
<tr>
<td>Company cloud host storage quota</td>
<td>This alarm tracks whether storage quota assigned to a company as a part of the hardware plan has been exceeded.</td>
<td>Company</td>
<td>Yes</td>
</tr>
<tr>
<td>Company cloud storage quota</td>
<td>This alarm checks whether a company is running out of space on a cloud repository.</td>
<td>Company</td>
<td>Yes</td>
</tr>
<tr>
<td>Company data download quota</td>
<td>This alarm checks whether a company is running out of the data transfer out quota on cloud repositories.</td>
<td>Company</td>
<td>No</td>
</tr>
<tr>
<td>Company location cloud storage quota</td>
<td>This alarm checks whether a location is running out of space on a cloud repository.</td>
<td>Location</td>
<td>No</td>
</tr>
<tr>
<td>Computer without backup</td>
<td>This alarm checks whether computers running Veeam Backup Agents have been backed up within the defined RPO (Recovery Point Objective) interval.</td>
<td>Backup agent</td>
<td>Yes</td>
</tr>
<tr>
<td>Discovery rule state</td>
<td>This alarm checks whether a discovery rule failed.</td>
<td>Discovery rule</td>
<td>Yes</td>
</tr>
<tr>
<td>Failover Plan session state</td>
<td>This alarm checks whether one or more VMs in a failover plan failed to start.</td>
<td>VM failover plan</td>
<td>Yes</td>
</tr>
<tr>
<td>Job session state</td>
<td>This alarm checks whether a job session failed or finished with a warning.</td>
<td>VM backup job</td>
<td>Yes</td>
</tr>
<tr>
<td>Job state</td>
<td>This alarm checks whether a job was in a disabled state for more than an allowed time period.</td>
<td>VM backup job</td>
<td>Yes</td>
</tr>
<tr>
<td>Management agent connection state</td>
<td>This alarm checks the connection status between Veeam Availability Console and a management agent running on a Veeam Backup &amp; Replication server, Veeam Backup Enterprise Manager server or a computer protected with Veeam backup agent.</td>
<td>Management agent</td>
<td>No</td>
</tr>
<tr>
<td>Management agent version is out-of-date</td>
<td>This alarm checks whether the version of a management agent running on a Veeam Backup &amp; Replication server, Veeam Backup Enterprise Manager server or a computer protected with Veeam backup agent matches the version of Veeam Availability Console.</td>
<td>Management agent</td>
<td>No</td>
</tr>
<tr>
<td>Max allowed backup agent job duration</td>
<td>This alarm checks whether a Veeam backup agent job session has exceeded the maximum allowed session duration.</td>
<td>Backup agent job</td>
<td>No</td>
</tr>
<tr>
<td>Alarm Name</td>
<td>Description</td>
<td>Target</td>
<td>Result</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>Max allowed job duration</td>
<td>This alarm checks whether a Veeam Backup &amp; Replication job session has exceeded the maximum allowed session duration.</td>
<td>VM backup job</td>
<td>No</td>
</tr>
<tr>
<td>Repository free space</td>
<td>This alarm checks whether a backup repository is running out of space.</td>
<td>Backup repository</td>
<td>Yes</td>
</tr>
<tr>
<td>Server agent backups stored in cloud repository</td>
<td>This alarm checks whether the number of server agent backups stored in a cloud repository exceeds the maximum allowed limit.</td>
<td>Cloud repository</td>
<td>Yes</td>
</tr>
<tr>
<td>SureBackup job session state</td>
<td>This alarm checks whether one or more verification checks specified in the SureBackup job failed.</td>
<td>VM job (SureBackup)</td>
<td>Yes</td>
</tr>
<tr>
<td>User cloud storage quota</td>
<td>This alarm tracks whether a user is running out of space on a cloud repository.</td>
<td>User</td>
<td>Yes</td>
</tr>
<tr>
<td>VM without backup</td>
<td>This alarm checks whether VMs managed with Veeam Backup &amp; Replication have been backed up within the defined RPO (Recovery Point Objective) interval.</td>
<td>Backup server</td>
<td>Yes</td>
</tr>
<tr>
<td>VM without replica</td>
<td>This alarm checks whether VMs managed with Veeam Backup &amp; Replication have been replicated within the defined RPO (Recovery Point Objective) interval.</td>
<td>Backup server</td>
<td>Yes</td>
</tr>
<tr>
<td>VMs in the backup repository</td>
<td>This alarm checks whether the number of VMs stored in a backup repository exceeds the maximum allowed limit.</td>
<td>Backup repository</td>
<td>No</td>
</tr>
<tr>
<td>VMs stored in cloud repository</td>
<td>This alarm checks whether the number of VMs stored in a cloud repository exceeds the maximum allowed limit.</td>
<td>Cloud repository</td>
<td>Yes</td>
</tr>
<tr>
<td>WAN accelerator connection state</td>
<td>This alarm checks the connection status between a Veeam backup server and WAN accelerator.</td>
<td>WAN accelerator</td>
<td>Yes</td>
</tr>
<tr>
<td>WAN accelerator version is out-of-date</td>
<td>This alarm checks whether the version of a WAN accelerator matches the version of Veeam Backup &amp; Replication installed on a backup server.</td>
<td>WAN accelerator</td>
<td>Yes</td>
</tr>
<tr>
<td>Workstation agent backups stored in cloud repository</td>
<td>This alarm checks whether the number of workstation agent backups stored in a cloud repository exceeds the maximum allowed limit.</td>
<td>Cloud repository</td>
<td>Yes</td>
</tr>
</tbody>
</table>