© 2022 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**

Read the End User Software License Agreement before using the accompanying software programs. Using any part of the software indicates that you accept the terms of the End User Software License Agreement.
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONTACTING VEEAM SOFTWARE</td>
<td>6</td>
</tr>
<tr>
<td>ABOUT THIS DOCUMENT</td>
<td>7</td>
</tr>
<tr>
<td>OVERVIEW</td>
<td>8</td>
</tr>
<tr>
<td>Solution Architecture</td>
<td>9</td>
</tr>
<tr>
<td>Standalone and Managed Operation Modes</td>
<td>10</td>
</tr>
<tr>
<td>Data Backup</td>
<td>11</td>
</tr>
<tr>
<td>Backup Policies and Jobs</td>
<td>12</td>
</tr>
<tr>
<td>File-Level Backup</td>
<td>14</td>
</tr>
<tr>
<td>How Backup Works</td>
<td>15</td>
</tr>
<tr>
<td>Backup Chain</td>
<td>16</td>
</tr>
<tr>
<td>Backup Repository</td>
<td>20</td>
</tr>
<tr>
<td>Data Encryption</td>
<td>21</td>
</tr>
<tr>
<td>Backup of External Drives</td>
<td>29</td>
</tr>
<tr>
<td>Data Restore</td>
<td>30</td>
</tr>
<tr>
<td>Integration with Veeam Backup &amp; Replication</td>
<td>31</td>
</tr>
<tr>
<td>Backup to Veeam Cloud Connect Repository</td>
<td>32</td>
</tr>
<tr>
<td>MANAGING VEEAM AGENT IN VEEAM BACKUP &amp; REPLICATION</td>
<td>33</td>
</tr>
<tr>
<td>PLANNING AND PREPARATION</td>
<td>34</td>
</tr>
<tr>
<td>System Requirements</td>
<td>35</td>
</tr>
<tr>
<td>Used Ports</td>
<td>37</td>
</tr>
<tr>
<td>GETTING STARTED</td>
<td>39</td>
</tr>
<tr>
<td>INSTALLATION AND CONFIGURATION</td>
<td>41</td>
</tr>
<tr>
<td>Before You Begin</td>
<td>42</td>
</tr>
<tr>
<td>Installing Veeam Agent</td>
<td>43</td>
</tr>
<tr>
<td>Granting Full Disk Access</td>
<td>44</td>
</tr>
<tr>
<td>Importing Connection Settings</td>
<td>45</td>
</tr>
<tr>
<td>Upgrading Veeam Agent</td>
<td>46</td>
</tr>
<tr>
<td>Uninstalling Veeam Agent</td>
<td>47</td>
</tr>
<tr>
<td>Granting Permissions to Users</td>
<td>48</td>
</tr>
<tr>
<td>Installation and Configuration with MDM Solution</td>
<td>49</td>
</tr>
<tr>
<td>Installation and Configuration with Command Line Interface</td>
<td>50</td>
</tr>
<tr>
<td>Installing Veeam Agent</td>
<td>51</td>
</tr>
<tr>
<td>Granting Permissions to Users</td>
<td>52</td>
</tr>
<tr>
<td>Managing Veeam Agent Operation Mode</td>
<td>53</td>
</tr>
<tr>
<td>Uninstalling Veeam Agent</td>
<td>56</td>
</tr>
<tr>
<td>GETTING TO KNOW USER INTERFACE</td>
<td>57</td>
</tr>
</tbody>
</table>
Contacting Veeam Software

At Veeam Software we value 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, visit the Veeam Customer Support Portal 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 office locations, visit the Veeam Contacts Webpage.

Online Support

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

- Full documentation set: veeam.com/documentation-guides-datasheets.html
- Veeam R&D Forums: forums.veeam.com
About This Document

This user guide provides information about main features of Veeam Agent for Mac 1.0.

Intended Audience

The user guide is intended for anyone who wants to use Veeam Agent for Mac 1.0 or later to protect their computer.
Overview

Veeam Agent for Mac is a data protection and disaster recovery solution for physical endpoints and virtual machines running macOS.

Veeam Agent can be used by IT administrators to protect different types of computers and devices: servers, desktops and laptops.

Veeam Agent offers a variety of features to protect your data. You can back up all user profiles or individual folders. Backups can be stored on a local hard drive, on an external hard drive, in a network shared folder, on a Veeam backup repository, or Veeam Cloud Connect repository.

In case of a disaster, you can restore individual files and folders from backups to its original location or a new location.

Veeam Agent for Mac is a part of Veeam Backup & Replication. Backup administrators who work with Veeam Backup & Replication can perform tasks with Veeam Agent backups: configure backup policies, manage backups created with backup policies, restore files and folders from backups.
Solution Architecture

Veeam Agent for Mac is set up on a macOS physical computer or virtual machine whose data you want to protect.

When you install the product, Veeam Agent deploys the following components:

- **Veeam Agent for Mac Service (veeamService)** is a service responsible for managing all tasks and resources in Veeam Agent. The veamService component is registered as a daemon in the macOS upon the product installation. The service is started automatically when you start the OS, and runs in the background.

- **Veeam Agent for Mac Job Manager (veeamjobman)** is a process started by Veeam Agent for Mac Service for every backup job session.

- **Veeam Agent** that communicates with the Veeam Agent for Mac Service and Veeam Agent for Mac Job Manager. Veeam Agent is started by Veeam Agent for Mac Manager to perform data transfer operations of any kind: copy data from the backed-up volume to the backup location during backup, from the backup location to the target volume during restore, perform data compression, and so on.

- **Veeam Agent for Mac Installer (veeaminstaller)** is a component responsible for Veeam Agent uninstallation process. To learn more, see Uninstalling Veeam Agent.

- **Veeam Agent for Mac GUI Application** is a component responsible for the Veeam Agent tray menu and the File Level Restore wizard.

- To store its configuration data, Veeam Agent uses the SQLite database engine. SQLite requires only few files to install and takes little resources to run on a macOS.

---

Mac computer with Veeam Agent

- Veeam Agent Service
- Veeam Agent Job Manager
- Veeam Agent
- Veeam Agent Installer
- Veeam Agent GUI
- SQLite Database Engine
Standalone and Managed Operation Modes

Veeam Agent for Mac can operate in two modes: managed mode and standalone mode. Features and limitations of Veeam Agent for Mac differ depending on the operating mode selected for the product.

- **Managed mode**

  In the managed mode, Veeam Agent for Mac operates under control from Veeam Backup & Replication. To use Veeam Agent operating in the managed mode, you must create protection group for pre-installed Veeam Agents, deploy Veeam Agent directly on the Mac computer you want to protect, and connect Veeam Agent to Veeam Backup & Replication. After that, you can configure managed backup jobs to protect data on the Mac computer. To learn more, see Getting Started.

- **Standalone mode**

  In the standalone mode, Veeam Agent for Mac operates as a standalone product. To use Veeam Agent operating in the standalone mode, you must create protection group for pre-installed Veeam Agents, deploy Veeam Agent directly on the Mac computer you want to protect, but you do not need to connect Veeam Agent to Veeam Backup & Replication. After that, you can configure standalone backup jobs to protect data on the Mac computer.

  You can still use Veeam Agent operating in the standalone mode with Veeam Backup & Replication. In this scenario, you can use a Veeam backup repository as a target location for Veeam Agent backups and use the Veeam Backup & Replication console to perform a number of tasks with Veeam Agent backups.

**IMPORTANT**

Veeam Agent selects the operation mode depending on the way you work with backup jobs. To learn more, see Backup Policies and Jobs.
Data Backup

It is recommended that you regularly back up data stored on your Mac computer. Backup creates a safety copy of your data. If any kind of disaster strikes, you can restore your data from the backup and be sure that you will not lose the necessary information.

You can set up Veeam Agent to perform automatic scheduled backups (triggered at specific time of the day), or you can choose to back up data manually when needed.

You can back up all user profiles or individual folders and files.

You can set up Veeam Agent to create multiple backups — with individual backup scope, upon individual schedule or in different locations. This functionality is available if Veeam Agent operates in the Workstation or Server edition. To learn more about editions, see Product Editions.

Backups created with Veeam Agent can be saved to the following locations:

- Removable storage device
- Local computer drive
- SMB (CIFS) network shared folder
- Backup repository managed by a Veeam backup server
- Veeam Cloud Connect repository
Backup Policies and Jobs

To back up data of the protected Mac computer, you must configure a Veeam Agent backup job. The Veeam Agent backup job defines what data to back up, how, where and when to back up data. In case of Veeam Agent for Mac, you can create Veeam Agent backup jobs on Mac computers using backup policies.

Backup policy

The backup policy describes configuration of individual Veeam Agent backup jobs that run on protected computers. Backup policy is configured in Veeam Backup & Replication. Veeam Backup & Replication uses the backup policy as a saved template and applies settings from the backup policy to Veeam Agents that run on computers specified in the backup policy. Veeam Agents use these settings from the backup policy to configure the backup jobs on Veeam Agent computers.

To learn how backup policy works in detail, see the Backup Policy section in the Veeam Agent Management Guide.

In Veeam Backup & Replication, you can configure several file-level backup policies with different settings. For example, you can configure one backup policy to back up the entire Users folder and another backup policy to back up specific files. You can configure backup policies targeted at different backup locations to keep several copies of your backed-up data. You can also configure several backup policies with individual schedule to fine-tune automatic backup creation process.

To learn more, see the Creating Agent Backup Policy for Mac Computers section in the Veeam Agent Management Guide.

NOTE

In Veeam Backup & Replication, you can create more than one backup policy only if Veeam Agent operates in the Workstation or Server edition. To learn more, see Product Editions.

Veeam Agent for Mac launches the backup policy according to the schedule you define. You can schedule the policy to start at specific time daily or on specific week days. You can also start a backup policy manually to perform backup on demand when needed.

Backup job

The backup job runs on the Veeam Agent computer. Veeam Agent uses settings from the backup policy configured in Veeam Backup & Replication to configure Veeam Agent backup job. You can use the backup job to create Veeam Agent backups in a target backup repository.

To learn how backup job works in detail, see How Backup Works.

In Veeam Agent for Mac, you can work with backup job in the following operation modes:

- Managed mode
  Veeam Agent for Mac can automatically create backup jobs based on backup policy settings configured using Veeam Backup & Replication. To learn more, see the Backup Policy section in the Veeam Agent Management Guide. If Veeam Agent creates a backup job using settings from the backup policy, Veeam Agent functions in the managed mode.

- Standalone Mode
  You can configure a backup job from scratch with the command line interface. In this case, Veeam Agent functions in the standalone mode and does not require a connection to Veeam Backup & Replication. You can also configure several file-level standalone backup jobs with different settings.
For example, you can configure backup jobs targeted at different backup locations to keep several copies of your backed-up data. You can also configure several backup policies with individual jobs to fine-tune automatic backup creation process.

To learn more, see Creating Standalone Backup Job.

**NOTE**

You can create more than one backup job only if Veeam Agent operates in the Workstation or Server edition. To learn more, see Product Editions.

To learn more about operation modes, see Standalone and Managed Operation Modes.
File-Level Backup

Veeam Agent for Mac copies backed-up data at the file level. The file-level backup captures data of individual folders and files on the machine. You can use the file-level backup to restore files and folders that you have added to the backup scope.

With Veeam Agent for Mac, you can specify which files and folders to back up:

- When you back up user profiles, Veeam Agent captures the content of the home folders of all users on your computer. When you recover from such backup, you will be able to restore all user profiles data or restore individual subfolders of home folders and files in these folders.

  **NOTE**
  - When you back up user profiles, Veeam Agent does not include guest user account in the backup scope.
  - If Veeam Agent operates in the standalone operation mode, you cannot back up user profiles. You can back up individual folders only. To learn more about operation modes, see Standalone and Managed Operation Modes.

- You can include individual folders in the backup. When you include a folder in the backup, its subfolders are automatically included in the backup too. When you recover from such backup, you will be able to restore folders that you have selected to back up, all subfolders of these folders and files in these folders.

- You can include or exclude files of a specific type in/from the backup. You can specify file names explicitly or use UNIX wildcard characters to define include and exclude file name masks. When you recover from such backup, you will be able to restore folders that you have selected to back up with files whose names match the specified include masks.
How Backup Works

During backup, Veeam Agent for Mac performs the following operations:

1. When a new job session starts, Veeam Agent creates a backup file in the target location.

2. In the backup file, Veeam Agent creates a virtual disk. The disk contains a volume with the ext4 file system.

3. Veeam Agent checks the file system of the volume which data you selected for backup. If data is located on the volume with the APFS file system, Veeam Agent commands macOS to create a APFS snapshot. The APFS snapshot helps make sure that the data on the volume is consistent and does not change at the moment of backup.

If data is located on the volume with any supported file system excluding APFS, Veeam Agent performs the backup operation in the snapshot-less mode. This mode allows you to back up data that resides in any supported file system mounted to the root file system of the Veeam Agent computer. However, Veeam Agent does not track whether source files have changed since the backup process start.

**IMPORTANT**

During backup in the snapshot-less mode, Veeam Agent does not track whether files and directories have changed in their original location since the time when the backup process started. To make sure that data in the backup is in the consistent state, you must not perform write operations in the file system that contains the backed-up data until the backup process completes.

4. [For incremental backup] To detect files that changed on the Veeam Agent computer since the previous backup session, Veeam Agent reads file metadata and compares last modification time of files in the original location and files in the backup created during the previous job session. If the file has modification time later than the previous job session start time, Veeam Agent considers the file as changed.

To learn about full and incremental backup, see Backup Chain.

5. Veeam Agent reads data from the created APFS snapshot or directly from the volume whose data you want to back up and copies data that you selected for backup to the target location.

After all backed-up data is transferred to the target location, Veeam Agent removes the APFS snapshot. In the target location, Veeam Agent stores copied data to the backup file.
Backup Chain

Every backup job session produces a new backup file in the target location. Backup files make up a backup chain. The backup chain can contain files of two types: full backups and incremental backups.

- During the first backup job session, Veeam Agent for Mac performs full backup. Veeam Agent copies all data that you have chosen to back up and stores the resulting full backup file (VBK) in the target location. The full backup takes significant time to complete and produces a large backup file: you have to copy the whole amount of data.

- During subsequent backup job sessions, Veeam Agent performs incremental backups. It copies only new or changed data relatively to the last backup job session and saves this data as an incremental backup file (VIB) in the target location. Incremental backups typically take less time than full backup: you have to copy only changes, not the whole amount of data.

After several backup cycles, you have a chain of backup files in the target location: the first full backup file and subsequent incremental backup files. Every backup file contains a restore point for backed up data. A restore point is a "snapshot" of your data at a specific point in time. You can use restore points to roll back your data to the necessary state.

To recover data to a specific restore point, you need a chain of backup files: a full backup file plus a set of incremental backup files following this full backup file. If some file from the backup chain is missing, you will not be able to roll back to the necessary state. For this reason, it is recommended that you do not delete separate backup files manually. To learn more, see Deleting Backups.

Types of Backup Files

Veeam Agent for Mac produces backup files of the following types:

- VBK — full backup file.
- VIB — incremental backup file.
- VBM — backup metadata file. The backup metadata file is updated with every backup job session. It contains information about the computer on which the backup was created, every restore point in the backup chain, how restore points are linked to each other and so on. The backup metadata file is required for performing file-level restore operations.
Backup Retention Policy

Restore points in the backup chain are not kept forever. They are removed according to the retention policy. The retention policy helps maintain the life cycle of restore points and make sure that backup files do not consume the whole disk space.

Veeam Agent for Mac retains the number of latest restore points defined by the user. During every backup policy session, Veeam Agent checks if there is any obsolete restore point in the backup chain. If some restore point is obsolete, it is removed from the chain.

When removing obsolete restore points, Veeam Agent for Mac does not simply delete backup files from disk. It transforms the backup chain so that the backup chain always contains a full backup file on which subsequent incremental backup files are dependent. To maintain the consistency of the backup chain, Veeam Agent uses the following rotation scheme:

1. During every backup policy session Veeam Agent adds a backup file to the backup chain and checks if there is an obsolete restore point.

2. If an obsolete restore point exists, Veeam Agent transforms the backup chain. As part of this process, it performs the following operations:
   a. Veeam Agent re-builds the full backup file to include in it data of the incremental backup file that follows the full backup file. To do this, Veeam Agent injects into the full backup file data blocks from the earliest incremental backup file in the chain. This way, a full backup ‘moves’ forward in the backup chain.
   b. The earliest incremental backup file is removed from the chain as redundant: its data has already been injected into the full backup file, and the full backup file includes data of this incremental backup file.
Active Full Backup

In some cases, you need to regularly create a full backup. For example, your corporate backup job may require that you create a full backup on weekend and run incremental backup on work days. To let you conform to these requirements, Veeam Agent for Mac lets you create active full backups.

When Veeam Agent performs active full backup, it produces a full backup file and adds this file to the backup chain.

The active full backup resets the backup chain. All incremental backup files use the latest active full backup file as a new starting point. A previously used full backup file and its subsequent incremental backup files remain on the disk. After the last incremental backup file created prior to the active full backup becomes outdated, Veeam Agent automatically deletes the previous backup chain. To learn more, see Retention Job for Active Full Backups.

You can schedule a backup job to create active full backups periodically. To do this, you can use the Veeam Backup & Replication console. To learn more, see the Backup Settings section in the Veeam Agent Management Guide

Retention Job for Active Full Backups

To be able to restore data from a Veeam Agent backup, you need to have a full backup file and a chain of subsequent incremental backup files on the disk. If you delete a full backup file, the whole chain of incremental backup files will become useless. In a similar manner, if you delete any incremental backup file before the point to which you want to roll back, you won’t be able to restore data (since later incremental backup files depend on earlier incremental backup files).

For this reason, if you create an active full backup, in some days there will be more restore points on the disk than specified by retention job settings. Veeam Agent will remove the full backup chain only after the last incremental backup file in the chain becomes outdated.

For example, the retention job is set to 3 restore points. A full backup file is created on Sunday, incremental backup files are created on Monday and Tuesday, and an active full backup is created on Wednesday. Although the backup chain now contains 4 restore points, Veeam Agent will not delete the previous backup chain. Veeam Agent will wait for the next 2 incremental backup files to be created, and only then will delete the whole previous chain, which will happen on Friday. As a result, although the retention job is set to 3 restore points, the actual number of backup files on the disk will be greater for some time.
Veeam Agent treats the active full backup in the same way as a regular full backup. If some restore point becomes obsolete, Veeam Agent will re-build the full backup file to include in it data of the incremental backup file that follows the full backup file. After that, Veeam Agent will remove the earliest incremental backup file from the chain as redundant.
Backup Repository

A backup job configured in Veeam Backup & Replication for Veeam Agent for Mac creates backup files in a backup repository. A backup repository is a folder on the storage where you want to keep backup files. You can use the following types of disk-based storage to create a backup repository:

- Local (internal) storage of the protected machine (not recommended).
- Direct attached storage (DAS), such as USB, eSATA or Firewire external drives.
- Network Attached Storage (NAS) able to represent itself as SMB (CIFS) share.
- Veeam Backup & Replication 11 or later backup repository.
- Veeam Backup & Replication 11 or later cloud repository.
Data Encryption

Data security is an important part of the backup strategy. You must protect your information from unauthorized access, especially if you back up sensitive data to remote locations. To keep your data safe, you can use data encryption.

Data encryption transforms data to an unreadable, scrambled format with the help of a cryptographic algorithm and a secret key. If encrypted data is intercepted, it cannot be unlocked and read by the eavesdropper. Only intended recipients who know the secret key can reverse encrypted information back to a readable format.

In Veeam Agent for Mac, encryption works at the backup job level.

Veeam Agent uses the block cypher encryption algorithm. Encryption works at the source side. Veeam Agent reads backed-up data, encodes data blocks, transfers them to the target location in the encrypted format and stores the data to a backup file. Data decryption is also performed on the source side: Veeam Agent transfers encrypted data back to the source side and decrypts it there.

To create encrypted backups, you must enable the encryption option and specify a password that will be used for data encryption. To do this, you can use the Veeam Backup & Replication console. To learn more, see the Storage Settings section in the Veeam Agent Management Guide.
Encryption Algorithms

To encrypt data in backups and files, Veeam Agent employs a symmetric key encryption algorithm.

The symmetric, or single-key encryption algorithm, uses a single, common secret key to encrypt and decrypt data. Before data is sent to the target location, it is encoded with a secret key. To restore encrypted data, you must have the same secret key. Users who do not have the secret key cannot decrypt data and get access to it.

Veeam Agent for Mac relies on a hierarchical encryption scheme. Each layer in the hierarchy encrypts the layer below with a key of specific type.

In This Section

- Encryption Keys
- How Data Encryption Works
- How Data Decryption Works
Encryption Keys

An encryption key is a string of random characters that is used to bring data to a scrambled format and back to unscrambled. Encryption keys encode and decode initial data blocks or underlying keys in the key hierarchy.

Veeam Agent uses 4 types of keys:

- 3 service keys generated by Veeam Agent:
  - Session key
  - Metakey
  - Storage key
- 1 key generated based on a user password: a user key.

Session Keys and Metakeys

The session key is the lowest layer in the encryption key hierarchy. When Veeam Agent encrypts data, it first encodes every data block in a file with a session key. For session keys, Veeam Agent uses the AES algorithm with a 256-bit key length in the CBC-mode.

Veeam Agent generates a new session key for every backup job session. For example, if you have created an encrypted backup job and run 3 job sessions, Veeam Agent will produce 3 backup files that will be encrypted with 3 different session keys:

- Full backup file encrypted with session key 1
- Incremental backup file encrypted with session key 2
- Incremental backup file encrypted with session key 3

The session key is used to encrypt only data blocks in backup files. To encrypt backup metadata, Veeam Agent applies a separate key — metakey. Use of a metakey for metadata raises the security level of encrypted backups.
For every job session, Veeam Agent generates a new metakey. For example, if you have run 3 job sessions, Veeam Agent will encrypt metadata with 3 metakeys.

In the encryption process, session keys and metakeys are encrypted with keys of a higher layer — storage keys. Cryptograms of session keys and metakeys are stored to the resulting file next to encrypted data blocks. Metakeys are additionally kept in the Veeam Agent database.

**Storage Keys**

Backup files in the backup chain often need to be transformed, for example, when the earliest incremental backup file in the chain becomes obsolete and its data should be included into the full backup file. When Veeam Agent transforms a full backup file, it writes data blocks from several restore points to the full backup file. As a result, the full backup file contains data blocks that are encrypted in different job sessions with different session keys.

To restore data from such "composed" backup file, Veeam Agent would require a bunch of session keys. For example, if the backup chain contains restore points for 2 months, Veeam Agent would have to keep session keys for a 2-month period.

In such situation, storing and handling session keys would be resource consuming and complicated. To facilitate the encryption process, Veeam Agent uses another type of service key — a storage key.

For storage keys, Veeam Agent uses the AES algorithm with a 256-bit key length in the CBC-mode. A storage key is directly associated with one restore point in the backup chain. The storage key is used to encrypt the following keys in the encryption hierarchy:

- All session keys for all data blocks in one restore point
- Metakey encrypting backup metadata
During the restore process, Veeam Agent uses one storage key to decrypt all session keys for one restore point, no matter how many session keys were used to encrypt data blocks in this restore point. As a result, Veeam Agent does not need to keep the session keys history in the Veeam Agent database. Instead, it requires only one storage key to restore data from one file.

In the encryption process, storage keys are encrypted with a key of a higher layer — a user key. Cryptograms of storage keys are stored to the resulting file next to encrypted data blocks, and cryptograms of session keys and metakeys.

Storage keys are also kept in the Veeam Agent database. To maintain a set of valid storage keys in the database, Veeam Agent uses retention job settings specified for the job. When some restore point is removed from the backup chain by retention, the storage key corresponding to this restore point is also removed from the Veeam Agent database.

User Keys

When you enable encryption for a job, you must define a password to protect data processed by this job, and define a hint for the password. The password and the hint are saved in the job settings. Based on this password, Veeam Agent generates a user key.

The user key protects data at the job level. In the encryption hierarchy, the user key encrypts storage keys for all restore points in the backup chain.

Veeam Agent saves a hint for the password to its database and to the backup metadata file (VBM). When you decrypt a file, Veeam Agent displays a hint for the password that you must provide. After you enter a password, Veeam Agent derives a user key from the password and uses it to unlock the storage key for the encrypted file.

According to the security best practices, you should change passwords for encrypted jobs regularly. When you change a password for the job, Veeam Agent creates a new user key and uses it to encrypt new restore points in the backup chain. If you lose a password that was specified for encryption, you can change the password in the encryption settings. You can use the new password to restore data from all restore points in the backup chain, including those restore points that were encrypted with an old password.

How Data Encryption Works

Data encryption is performed as part of the backup process. Encryption works at the source side, before data is transported to the target location. As a result, encryption keys are not passed to the target side, which helps to avoid data interception.

The encryption process includes the following steps:

1. When you create a backup job, you enable the encryption option for the job and enter a password to protect data at the job level.
2. Veeam Agent generates a user key based on the entered password.
3. When you start an encrypted job, Veeam Agent creates a storage key and stores this key to its database.

4. Veeam Agent creates a session key and a metakey. The metakey is stored to the Veeam Agent database.

5. Veeam Agent processes job data in the following way:
   a. The session key encrypts data blocks in the backup file. The metakey encrypts backup metadata.
   b. The storage key encrypts the session key and the metakey.
   c. The user key encrypts the storage key.

6. Encrypted data blocks are passed to the target. The cryptograms of the user key, storage key, session key and metakey are stored to the resulting file next to encrypted data blocks.

How Data Decryption Works

When you restore data from an encrypted backup file, Veeam Agent for Mac performs data decryption automatically in the background or requires you to provide a password.

- If encryption keys required to unlock the backup file are available in the Veeam Agent database, you do not need to enter the password. Veeam Agent uses keys from the database to unlock the backup file. Data decryption is performed in the background, and data restore does not differ from that from an unencrypted one.

  Automatic data decryption can be performed if you encrypt and decrypt the backup file on the same Veeam Agent computer using the same Veeam Agent database.

- If encryption keys are not available in the Veeam Agent database, you need to provide a password to unlock the encrypted file.

Data decryption is performed at the source side, after data is transported back from the target side. As a result, encryption keys are not passed to the target side, which helps avoid data interception.

The decryption process includes the following steps. Keep in mind that steps 1 and 2 are required only if you decrypt the file on the Veeam Agent computer other than the computer where the file was encrypted.

1. You select the backup from which you want to restore data. Veeam Agent notifies you that one or more files in the backup chain are encrypted and requires a password.

2. You specify a password for the imported file. If the password has changed once or several times, you need to specify the latest password. In Veeam Agent, you can use the latest password to restore data from all restore points in the backup chain, including those restore points that were encrypted with an old password.
3. Veeam Agent reads the entered password and generates the user key based on this password. With the user key available, Veeam Agent performs decryption in the following way:
   a. Veeam Agent applies the user key to decrypt the storage key.
   b. The storage key, in its turn, unlocks underlying session keys and a metakey.
   c. Session keys decrypt data blocks in the encrypted file.

After the encrypted file is unlocked, you can work with it as usual.

![Diagram of encryption process]

**Backup Policy Encryption**

Encryption for the backup job is configured in the advanced job settings. You should enable the encryption option and specify a password to protect data in backup files produced by the backup job. To do this, use can use the Veeam Backup & Replication console. To learn more, see the Storage Settings section in the Veeam Agent Management Guide.

The backup job processing with encryption enabled includes the following steps:

1. You enable encryption for a backup job and specify a password.
2. Veeam Agent generates the necessary keys to protect backup data.
3. Veeam Agent encrypts data blocks and transfers them to the target location already encrypted.
4. On the target storage, encrypted data blocks are stored to a resulting backup file.

![Diagram of backup process]

Restore of an encrypted backup file includes the following steps:

1. You select an encrypted backup file and define a password to decrypt the backup file. If the password has changed once or several times, you need to specify the latest password that was used to encrypt files in the backup chain.
2. Veeam Agent uses the provided password to generate user key and unlock the subsequent keys for backup file decryption.
3. Veeam Agent retrieves data blocks from the backup file, sends them to the target volume and decrypts them on the target volume.

![Diagram showing Veeam Agent computer communicating with target storage](image.png)

**Encryption Best Practices**

To guarantee the flawless process of data encryption and decryption, consider the following advice.

**Password**

1. Use strong passwords that are hard to crack or guess. Consider the following recommendations:
   a. The password must be at least 8 characters long.
   b. The password must contain uppercase and lowercase characters.
   c. The password must be a mixture of alphabetic, numeric and punctuation characters.
   d. The password must significantly differ from the password you used previously.
   e. The password must not contain any real information related to you, for example, date of birth, your pet’s name, your logon name and so on.

2. Provide a meaningful hint for the password that will help you recall the password. The hint for the password must significantly differ from the password itself. The hint for the password is displayed when you select an encrypted backup server and attempt to unlock it.

3. Change passwords for encrypted policies regularly. Use of different passwords helps increase the encryption security level.

**Encryption for Existing Job**

If you enable encryption for an existing job, during the next job session Veeam 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 an existing backup job, Veeam Agent does not encrypt the previous backup chain created with this job. However, Veeam Agent encrypts backup metadata. As a result, you need to enter the password to restore data from unencrypted backup files in the backup chain as well as from encrypted backup files in this chain.
Backup of External Drives

You can use Veeam Agent for Mac to back up data that resides on external USB/eSATA or FireWire drives connected to the Veeam Agent computer.

You can include in the backup scope specific folders with files that reside on an external drive. To do this, you must use the Veeam Backup & Replication console. To learn more, see the Creating Agent Backup Policy for Mac Computers section in the Veeam Agent Management Guide.
Data Restore

Veeam Agent for Mac offers file-level restore to recover user profiles or individual folders and files. If you have lost or modified folders and files on your computer by mistake, you can restore a copy of the necessary objects from the backup.
Integration with Veeam Backup & Replication

To use Veeam Agent for Mac 1.0 with Veeam Backup & Replication, you must install Veeam Backup & Replication 11a on the Veeam backup server. Veeam Agent for Mac 1.0 supports integration with Veeam Backup & Replication 11 or later as well.

You can store backup files created with Veeam Agent for Mac on backup repositories managed by Veeam Backup & Replication. To do this, you must select a Veeam Backup & Replication backup repository as a target location in the properties of the backup policy.

**NOTE**

To configure and manage Veeam Agent backup policies, you must use the Veeam Backup & Replication console. To learn more, see the Creating Agent Backup Policy for Mac Computers section in the Veeam Agent Management Guide.

Veeam Agent for Mac works with the Veeam Backup & Replication backup repository as with any other backup repository. Backup files are stored to a separate folder; you can perform standard restore operations using these files.

Information about Veeam Agent backups stored on the Veeam Backup & Replication backup repositories, backup policies and sessions becomes available in the Veeam Backup & Replication console:

- The Veeam Agent for Mac backup policy is displayed in the list of policies in Veeam Backup & Replication.
- Backup files created with Veeam Agent for Mac are displayed in the list of backups, under the Agents node.
- Performed policy sessions are available in the History view of Veeam Backup & Replication.

Backup administrators working with Veeam Backup & Replication can perform a set of operations with Veeam Agent backups:

- Perform data protection operations: create and manage backup policies, copy Veeam Agent backups to secondary backup repositories and archive these backups to tape.
- Perform restore operations: restore individual files and directories from Veeam Agent backups.
- Perform administrative tasks: disable and delete Veeam Agent backup policies, remove Veeam Agent backups and so on.
Backup to Veeam Cloud Connect Repository

If you want to store your data in the cloud, you can connect to a Veeam Cloud Connect service provider (SP) and create Veeam Agent backups in a cloud repository. To do this, you must provide credentials of the tenant (or subtenant) account that you obtained from the SP, and select a cloud repository as a target for backup files in the properties of the backup job. To learn more, see the Cloud Repository Settings section in the Veeam Agent Management Guide.

**NOTE**
You can create Veeam Agent backups in a cloud repository only if the SP backup server runs Veeam Backup & Replication 11 or later.
Managing Veeam Agent in Veeam Backup & Replication

Veeam Backup & Replication lets you automate management of Veeam Agent on multiple computes in your infrastructure. You can configure Veeam Agent backup policies and perform other data protection and administration tasks on remote computers. To use the Veeam Agent management functionality in Veeam Backup & Replication, you must install Veeam Backup & Replication on the Veeam backup server.

To learn more, see Veeam Agent Management Guide.
Planning and Preparation

Before you install Veeam Agent for Mac, make sure that the target computer meets the system requirements and all required ports are open.
System Requirements

The protected Mac computer must meet requirements listed in the table below.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| **Hardware**  | The protected Mac computer must meet the following hardware requirements:  
- CPU: x64 or ARM Apple-branded hardware*  
- Disk Space: 200 MB free disk space for product installation  
- Network: 10 Mbps or faster network connection to a backup target  
* On a Mac computer with the ARM Apple-branded hardware, the product is running using the Rosetta Translation Environment. |
| **OS**        | Veeam Agent supports the following macOS versions:  
- Monterey 12.0 – 12.3.X  
- Big Sur 11.0 – 11.6.X  
- Catalina 10.15.X  
- High Sierra 10.13.6 |
| **File System** | Veeam Agent supports consistent data backup with snapshot for the APFS file system.  
The following file systems can be backed up in the snapshot-less mode:  
- HFS+  
- MS-DOS (FAT)  
- exFAT  
- NTFS  
- FAT32  
- SMB  
Consider the following:  
- Software RAID is not supported.  
- Total size of all file systems included in a file-level backup must not exceed 218 TB.  
- Size of a file in a backup must not exceed 16 TB.  
- Name of a file in a backup must not be larger than 254 bytes.  
Keep in mind that characters that you can use in the file name may be encoded in 2 bytes or more. |
Backup Target

Backup can be performed to the following types of storage:

- Local (internal) storage of the protected computer (not recommended).
- Direct attached storage (DAS), such as USB, eSATA or Firewire external drives.
- Network Attached Storage (NAS) able to represent itself as SMB (CIFS) share.
- Veeam Backup & Replication 11 or later backup repository (including deduplication appliances).
- Veeam Cloud Connect 11 or later cloud repository.

Network

Consider the following:

- If you back up to a repository managed by a Veeam backup server, Veeam Agent for Mac must be able to establish a direct IP connection to the Veeam Backup & Replication server. Veeam Agent for Mac cannot work with Veeam Backup & Replication that is located behind a NAT gateway.
- Domain names of the Veeam Agent for Mac computer, Veeam Backup & Replication server and other servers in the Veeam backup infrastructure must be resolvable into IPv4 addresses.
# Used Ports

Make sure that you open ports listed below to enable proper work of Veeam Agent for Mac.

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Protocol</th>
<th>Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veeam Agent computer</td>
<td>Veeam backup server</td>
<td>TCP</td>
<td>10006</td>
<td>Default port used for communication with the Veeam backup server. Data between the Veeam Agent for Mac computer and backup repositories is transferred directly, bypassing Veeam backup servers.</td>
</tr>
<tr>
<td></td>
<td>Shared folder SMB (CIFS) share</td>
<td>TCP/UDP</td>
<td>137 to 139, 445</td>
<td>Ports used as a transmission channel from the Veeam Agent for Mac computer to the target SMB (CIFS) share. Ports 137 to 139 are used by backup infrastructure components to communicate using NetBIOS.</td>
</tr>
<tr>
<td>Veeam Agent computer</td>
<td>TCP</td>
<td>10101</td>
<td></td>
<td>Port used to create a mount point on the computer. Veeam Agent uses this mount point when the restore process starts and allows you to browse and restore files.</td>
</tr>
<tr>
<td>TCP</td>
<td>2500 to 3300</td>
<td></td>
<td></td>
<td>Default range of ports used for communication between Veeam Agent for Mac components during data transmission. For every TCP connection that a backup job uses, one port from this range is assigned. Ports must be open for incoming and outgoing traffic. Established connections must be allowed.</td>
</tr>
</tbody>
</table>

### Communication with Veeam Backup & Replication Repositories

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Protocol</th>
<th>Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veeam Agent computer</td>
<td>Linux server performing the role of a backup repository</td>
<td>TCP</td>
<td>2500 to 3300</td>
<td>Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigned.</td>
</tr>
<tr>
<td>From</td>
<td>To</td>
<td>Protocol</td>
<td>Port</td>
<td>Notes</td>
</tr>
<tr>
<td>------</td>
<td>----</td>
<td>----------</td>
<td>------</td>
<td>-------</td>
</tr>
<tr>
<td>Microsoft Windows server performing the role of a backup repository</td>
<td>TCP</td>
<td>49152 to 65535 (for Microsoft Windows 2008 and newer)</td>
<td>Dynamic RPC port range. For more information, see this Microsoft KB article.</td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>2500 to 3300</td>
<td>Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigned.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Communication with Veeam Cloud Connect Repositories

| Veeam Agent computer | Cloud gateway | TCP | 6180 | Port on the cloud gateway used to transport Veeam Agent data to the Veeam Cloud Connect repository. |
| Certificate Revocation Lists | TCP | 80 or 443 (most popular) | Veeam Agent computer needs access to CRLs (Certificate Revocation Lists) of the CA (Certification Authority) who issued a certificate to the Veeam Cloud Connect service provider. Generally, information about CRL locations can be found on the CA website. |
Getting Started

To protect your computer from a disaster of any kind, you must perform the following operations in Veeam Backup & Replication and Veeam Agent for Mac:

1. **Create a protection group for pre-installed Veeam Agents using Veeam Backup & Replication.**
   During the protection group configuration process, the following setup files are generated:
   - 2 Veeam Agent for Mac packages
     You will need to select the package depending on the macOS version installed on your Mac computer. To learn more, see *Installing Veeam Agent*.
   - 2 configuration files
     You will need to select the configuration file depending on the way you plan to connect your Mac computer to Veeam backup server. To learn more, see *Importing Connection Settings*.
   - The *readme* file with installation instructions
     To learn more about protection groups for pre-installed Veeam Agents, see the Protection Group Types section in Agent Management Guide.

2. **Using external tools, transfer the Veeam Agent setup files to the Mac computer you want to protect.**

3. **Install and connect Veeam Agent to Veeam backup server with a configuration file.**
   To learn more, see *Installation and Configuration*.

4. **Define what data you want to back up and configure a backup policy using Veeam Backup & Replication.**
   Before you configure the backup policy, you should decide on the following backup details:
   - Backup destination: where you want to store your backed-up data.
   - Backup scope: all user profiles or individual folders and files.
   - Backup schedule: how often you want to back up your data.
   After that, you can configure one or several backup policies. The backup policy captures the data that you have added to the backup scope and creates a chain of restore points in the target location. If your data gets lost or corrupted, you can restore it from the necessary restore point.
   You can configure the backup policy with the *Backup Job* wizard on the Veeam Backup & Replication side. To learn more, see the Creating Agent Backup Policy for Mac Computers section in the Veeam Agent Management Guide.

5. **Create a backup job.**
   To create a backup job on the Veeam Agent computer, you must apply the backup policy to the Veeam Agent computer. To learn more, see the Applying Backup Policy to Protected Computers section in the Veeam Agent Management Guide.
   Veeam Agent installed on the computer included in a protection group for pre-installed Veeam Agents connects to Veeam Backup & Replication every 6 hours and gets updated backup policy settings. Using these backup policy settings, Veeam Agent creates a backup job.
   Alternatively, you can configure a backup job manually with the command line interface. In this case, Veeam Agent for Mac functions in the standalone mode and does not require connection to Veeam Backup & Replication.
5. **Start the backup job.**
   
   You can set the backup policy to start automatically according to the defined schedule or start the backup policy manually from your Mac computer. To learn more, see *Starting Backup Policies*.  

6. **Monitor backup task performance using Veeam Backup & Replication.**
   
   You can use the Veeam Backup & Replication to check how backup tasks are being performed, what errors have occurred during backup policy sessions and so on.  

7. In case of a disaster, **you can restore your data**. You can perform data recovery operations in several ways:
   
   - You can restore all user profiles.
   - You can restore individual files and folders.

   To learn more, see *Performing Restore*.  

Installation and Configuration

You can install Veeam Agent for Mac on any macOS-based endpoint whose data you plan to protect — virtual machine or physical device (server, desktop or laptop).

Keep in mind that Veeam Agent for Mac 1.0 is a part of Veeam Backup & Replication 11a. To get the Veeam Agent installation package, you must generate the package using Veeam Backup & Replication 11a and install the package on the Mac computer.
Before You Begin

Before you start the installation process, check the following prerequisites:

1. You must obtain Veeam Agent for Mac setup files from your System Administrator. To learn more, see the Deploying Veeam Agents Using Generated Setup Files section in the Veeam Agent Management Guide.

2. The computer on which you plan to install Veeam Agent must satisfy system requirements specified in this document.

3. To install the Veeam Agent package, you must use the Administrator account on the computer where you plan to install the product.

4. If you have used the Beta version of Veeam Agent for Mac, you must remove Veeam Agent software packages prior to installing the release version of the product. To learn more, see Uninstalling Veeam Agent.
Installing Veeam Agent

To install Veeam Agent for Mac with the Installation wizard:

1. Save Veeam Agent setup files on the Mac computer where you plan to install the product.

2. Select the Veeam Agent for Mac package depending on the macOS version running on your Mac computer:
   - If the macOS version 10.13 (High Sierra) is installed, select the Veeam Agent for Mac-1.0.1.822-macos10.13.6 package.
   - If the macOS version 10.14 (Mojave) or later is installed, select the Veeam Agent for Mac-1.0.1.822 package.

3. Double-click the package.

4. Follow the installation instructions.
   - During the installation process, you must do the following:
     a. Accept the Veeam End User License Agreement.
     b. Accept the 3rd Party Components License Agreements.

**IMPORTANT**

Do not change Veeam Agent for Mac installation location. Veeam Agent must be installed in the Applications folder of the volume from which your Mac started up.

After the installation process is complete, you must enable full disk access for Veeam Agent. To learn more, see Granting Full Disk Access.

Keep in mind that during the installation process, Veeam Agent will prompt you to enter the Administrator password.

Alternatively, you can install Veeam Agent for Mac with the MDM solution or command line interface.
Granting Full Disk Access

After installation, Veeam Agent requires permission to access folders and files on the Veeam Agent computer.

NOTE

If you are using macOS High Sierra (version10.13.6), the access to files and folders is granted automatically at the moment of installation. Starting from macOS Mojave (10.14.X), you must grant access manually.

To grant full disk access:

1. In the upper-left corner of the screen, click the Apple menu > System Preferences.
2. In System Preferences, click the Security & Privacy pane and select the Privacy tab.
3. In the bottom-left corner, click the lock icon and enter the Administrator password to allow preferences editing.
4. In the list of services, select Full Disk Access.
5. In the list of apps, select the check box next to Veeam Agent for Mac.
   
   If the Veeam Agent for Mac check box is not available, click the plus button, and find and add Veeam Agent for Mac to the list of applications.
6. Close the window.

Alternatively, you can grant full disk access to Veeam Agent with the MDM solution.

After an access to the disk is provided, you can connect your Veeam Agent computer to the Veeam backup server.
Importing Connection Settings

To use Veeam Agent for Mac together with Veeam Backup & Replication, you must connect your Mac computer to the Veeam backup server. To do this, you must import the configuration file. The configuration file is one of the Veeam Agent for Mac setup files that you must obtain from your System Administrator. To learn more, see the Deploying Veeam Agents Using Generated Setup Files section in the Veeam Agent Management Guide.

To import the Veeam Agent for Mac configuration file:

1. Start Veeam Agent with Launchpad.
2. In the upper-right corner of the menu bar, click the Veeam Agent icon.
3. Select Import > Configuration.
4. In the Finder, select the XML file with the configuration and click Open.

When the configuration file is imported, Veeam Agent immediately connects to the Veeam backup server. After that, your Veeam Agent computer will be displayed as a member of the protection group in the Veeam Backup & Replication console.

If your Veeam Agent computer is connected to the Veeam backup server, and the backup policy is already configured on the Veeam Backup & Replication side, you can back up data on your Veeam Agent computer. To learn more, see Starting Backup Policy.

To learn more about backup policy configuration, see the Creating Agent Backup Policy for Mac Computers section in the Veeam Agent Management Guide.

Alternatively, you can import the Veeam Agent for Mac configuration with the MDM solution or command line interface.
Upgrading Veeam Agent

If a newer version is available, you can upgrade Veeam Agent without uninstallation of the previous version. During the upgrade process, configuration and backup files that were created with the previous version of Veeam Agent are not impacted in any way.

**IMPORTANT**

Before starting the upgrade process, make sure that there are no backup jobs running on the Veeam Agent computer.

To upgrade Veeam Agent for Mac with the Installation wizard:

1. Save setup files for the Veeam Agent newer version on the Mac computer where you plan to upgrade the product.

2. Select the Veeam Agent for Mac package depending on the macOS version running on the Mac computer:
   - If the macOS version 10.13 (High Sierra) is installed, select the Veeam Agent for Mac-1.0.1.822-macos10.13.6 package.
   - If the macOS version 10.14 (Mojave) or later is installed, select the Veeam Agent for Mac-1.0.1.822 package.

3. Double-click the package.

4. Click OK to accept an upgrade of Veeam Agent that is currently installed on the Mac computer.

5. Follow the installation instructions.

   During the installation process, you must do the following:
   - Accept the Veeam End User License Agreement.
   - Accept the 3rd Party Components License Agreements.

**IMPORTANT**

Do not change Veeam Agent for Mac installation location. Veeam Agent must be installed in the Applications folder of the volume from which your Mac started up.

Keep in mind that during the upgrade process, Veeam Agent will prompt you to enter the Administrator password.
Uninstalling Veeam Agent

To uninstall Veeam Agent for Mac:

1. Open the Finder, then click Applications in the sidebar of the Finder window.
2. Open the Veeam folder.
3. Double-click the Uninstall Agent for Mac application. After that, Veeam Agent for Mac and Uninstall Agent for Mac applications will be uninstalled.

Keep in mind that during the uninstallation process, Veeam Agent will prompt you to enter the Administrator password.

**IMPORTANT**

Do not move Veeam Agent for Mac and Uninstall Agent for Mac applications to Trash.

Alternatively, you can uninstall Veeam Agent with the command line interface. This may be useful if you want to delete a local Veeam Agent database together with Veeam Agent for Mac. For details, see Uninstalling Veeam Agent with Command Line Interface.
Granting Permissions to Users

When you install Veeam Agent for Mac, the product program files are placed to the folders on the system volume. For full access to Veeam Agent files, the administrator account is required. Rights to execute product files and run commands are also granted to users that belong to the veeam group.

The veeam group is automatically created by Veeam Agent at the process of the product installation. To let regular users work with Veeam Agent without the need to gain root privileges, you can add the necessary users to this group. Users in the veeam group will be able to execute Veeam Agent commands and perform backup and restore tasks under regular user account.

**IMPORTANT**

Consider the following:

- To add a user to the veeam group, you must have the administrator account in the macOS.
- Administrator can restore all user profiles that are available in the backup file, standard user can restore only one's user profile.

To add a user to the veeam group:

1. In the upper-left corner of the screen, click the Apple menu > System Preferences.
2. In System Preferences, click the Users & Groups pane.
3. In the bottom-left corner, click the lock icon and enter the administrator password to allow editing.
4. In the list of services, expand the Groups pane.
5. In the list of users, select the check box next to the user you want to add to the group.
6. Close the window.

Alternatively, you can add a user to the veeam group with the command line interface.
Installation and Configuration with MDM Solution

You can install and configure Veeam Agent for Mac with the Mobile Device Management (MDM) solution. Veeam Agent for Mac provides setup files for the following MDM solutions:

- Microsoft Intune
- SimpleMDM

Veeam Agent for Mac installation and configuration includes the following operations:

1. Veeam Agent installation.
   
   Only the Veeam Agent for Mac installation package is required.
   
   For details how to deploy a .pkg package, refer to the documentation of your MDM solution.

2. Granting full disk access to Veeam Agent.
   
   To grant full disk access and perform other configuration tasks, you need to use the following Veeam Agent parameters:
   
   o Application ID: \textit{NX3JU8SRVL}
   
   o Bundle ID: \textit{com.veeam.Agent}
   
   For other details, refer to the documentation of your MDM solution.

3. Veeam Agent configuration.
   
   The configuration process is required to connect Veeam Agent to Veeam backup server and include Veeam Agent computer in the protection group. Veeam Agent configuration is performed by deploying device profile on the Veeam Agent computer.
   
   If you use Microsoft Intune or SimpleMDM, see detailed instructions in Appendix A. Deploying Device Profile with MDM Solution. If you use another MDM solution, instructions may differ, refer to the documentation of your MDM solution.
Installation and Configuration with Command Line Interface

You can install and configure Veeam Agent for Mac with the command line interface.
Installing Veeam Agent

To install Veeam Agent for Mac with the command line Interface:

1. Save the downloaded package on the computer where you plan to install the product.
2. Install the package with the following command:

   ```bash
   installer -pkg </path/package.pkg> -target <volume>
   ```

   where:
   - `</path/package.pkg>` — full path to the downloaded package on the computer.
   - `<volume>` — name of the volume where you want to install Veeam Agent. To install Veeam Agent on the volume from which your Mac computer started up, specify the ’/’ (slash) character.

   For example:
   ```bash
   user@wrk01:~$ installer -pkg /Users/User/Desktop/Veeam?Agent?for?Mac-1.0.1.822.pkg -target /
   ```

3. After the installation process is complete, grant full disk access for Veeam Agent. To learn more, see Granting Full Disk Access.
Granting Permissions to Users

To add a user to the `veeam` group, use the following command:

```
deditgroup -o edit -a <username> veeam
```

where:

`<username>` — name of the account to which you want to grant access to Veeam Agent.

For example:

```
user@wrk01:~$ dseditgroup -o edit -a user veeam
```

To check whether the user is added to the `veeam` group, you can use the following command:

```
groups
```

For example:

```
user@wrk01:~$ groups
current groups:
staff adm everyone dip plugdev lpadmin veeam
```
Managing Veeam Agent Operation Mode

Veeam Agent for Mac can operate in two different modes. Depending on the selected mode, Veeam Agent has different features and limitations. To learn more, see Standalone and Managed Operation Modes.

Veeam Agent allows you to perform the following actions to manage the operation mode:

- View operation mode details.
- Reset to the standalone operation mode.
- Connect to Veeam backup server.
- Synchronize with Veeam backup server.
- Export logs to Veeam backup server.

Viewing Operation Mode

To view the current Veeam Agent operation mode, use the following command:

```
veeamconfig mode info
```

Veeam Agent displays the operation mode details:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Owner</strong></td>
<td>Name of the backup repository that manages Veeam Agent. If Veeam Agent operates in the standalone mode, Veeam Agent displays the <em>Not set</em> value.</td>
</tr>
</tbody>
</table>
| **Mode**  | Current Veeam Agent operating mode. Possible values:  
  - *Standalone* — Veeam Agent operates in the standalone mode.  
  - *Pre-installed agent* — Veeam Agent operates in the managed mode as member of a protection group for pre-installed Veeam Agents.  
  
  Keep in mind that features and limitations of Veeam Agent operating in the managed mode are different from those in the standalone mode. To learn more about managed mode, see the Veeam Agent Management Guide. |

For example:

```
user@wrk01:~$ veeamconfig mode info
Owner: Backup server (backupserver001.tech.local)
Mode: Pre-installed agent
```

If Veeam Agent operates in the managed mode, you can reset it to the standalone mode at any time. To learn more, see Resetting to Standalone Operation Mode.
Resetting to Standalone Operation Mode

If Veeam Agent operates in the managed mode, you can manually reset it to the standalone mode from the Veeam Agent side. To learn more about operation modes, see Standalone and Managed Operation Modes.

Before you reset Veeam Agent to the standalone mode, consider the following:

- Veeam Agent computer will be automatically removed from the protection group in Veeam Backup & Replication.
- All backup jobs configured on Veeam Agent computer will be deleted. If you plan to protect this computer with a standalone Veeam Agent, you will need to create new backup jobs.
- Veeam backup server settings including protection group configuration settings will be deleted.
- Previously created backup files will remain in the target backup repository. If the target repository is managed by the Veeam backup server, in the Veeam Backup & Replication console, they will be marked as Orphaned.

To reset Veeam Agent to the standalone operating mode, run the following command:

```
veeamconfig mode reset
```

You can use the `--force` option to override additional input prompts and error messages:

```
veeamconfig mode reset --force
```

Connecting to Veeam Backup & Replication

If you want to connect a Veeam Agent computer to the Veeam backup server as a member of a protection group for pre-installed Veeam Agents, you must apply connection settings from the configuration file. The configuration file is one of the Veeam Agent for Mac setup files that you must obtain from your System Administrator. To learn more about deployment using external tools, see the Deploying Veeam Agent for Mac section in the Veeam Agent Management Guide.

To connect Veeam Agent to Veeam backup server:

1. Get the configuration file from your System Administrator and upload this file to the Veeam Agent computer.
2. Navigate to the directory where you have saved the configuration file and run the following command:

```
veeamconfig mode setvbrsettings --cfg <file_name>.xml --force
```

where:

- `<file_name>` — a configuration file name.
- `--force` — with this option enabled, Veeam Agent will override additional input prompts and error messages. This parameter is optional.

Alternatively, you can specify the full path to the configuration file with the `--cfg` option.
For example:

```
user@wrk01:~$ veeamconfig mode setvbrsettings --cfg /Users/user/Mac\ Workstations\ Dists/Mac/Mac\ Workstations.xml
```

**Synchronizing with Veeam Backup Server**

After you connected Veeam Agent to the Veeam backup server, you may need to synchronize them. The reason is that the connection between the Veeam backup server and Veeam Agent computer added as a member of the protection group for pre-installed Veeam Agents is not persistent. Veeam Agent synchronizes with Veeam Backup & Replication every 6 hours. During the synchronization, Veeam Agent gets updated backup policies and configuration settings from the Veeam backup server, the Veeam backup server gets certificate details and session logs from Veeam Agent.

Keep in mind that this command is available only for Veeam Agent connected to the Veeam backup server as a member of the protection group for pre-installed Veeam Agents. To learn more, see the Protection Group Types section in the Veeam Agent Management Guide.

To synchronize Veeam Agent immediately, run the following command:

```
veeamconfig mode syncnow
```

**Exporting Logs to Veeam Backup Server**

If Veeam Agent is connected to the Veeam backup server as a member of the protection group for pre-installed Veeam Agents, Veeam Agent can collect product logs, export them to an archive file and send to the Veeam backup server. This operation may be required if you want to report an issue and need to attach log files to the support case.

Keep in mind that this command is available only for Veeam Agent connected to the Veeam backup server as a member of the protection group for pre-installed Veeam Agents. To learn more, see the Protection Group Types section in the Veeam Agent Management Guide.

To export logs, use the following command:

```
veeamconfig mode exportdebuglogs
```

Veeam Agent will collect logs, export them to an archive file with the name `veeam_logs_<date>_<time>.tar.gz` and save the archive to the following folder on the Veeam backup server:

```
C:\ProgramData\Veeam\Backup\Endpoint\Other\AgentLogs\<computer_name>
```

where `<computer_name>` — name of the computer with Veeam Agent installed.

**TIP**

You can also export logs to a local directory on the Veeam Agent computer. To learn more, see Exporting Product Logs.
Uninstalling Veeam Agent

To uninstall Veeam Agent for Mac, use the following command:

```
sudo </path/application.app>/Contents/MacOS/veeaminstaller uninstall-agent --purge
```

where:

`</path/application.app>` — full path to the application on the computer.

The `--purge` option is optional. Use this option to delete a local Veeam Agent database together with Veeam Agent for Mac.

For example:

```
user@wrk01:-$ % sudo /Applications/Veeam/Veeam\ Agent\ for\ Mac.app/Contents/MacOS/veeaminstaller uninstall-agent --purge
```
Getting to Know User Interface

With Veeam Agent for Mac, you can perform backup, restore and configuration tasks in the following ways:

- **With the Veeam Backup & Replication console**, you can perform data protection and administration tasks. You can collect Veeam Agent computers in groups, configure backup policies, and monitor performance and status of any backup. To learn more, see the Veeam Agent Management Guide.

- **With the Veeam Agent control panel**, you can perform basic data recovery tasks. You can import configurations and backup policies, start and stop backup policies, and recover files and folders.

- **With the command line interface**, in addition to operations that can be performed with the Veeam Agent control panel, you can perform a set of advanced tasks. For example, you can:
  - Synchronize Veeam Agent with Veeam backup server.
  - Configure standalone backup jobs.
  - Perform operations with backup repositories.
  - Monitor performance and status of any backup, restore and other data transfer session that was started in Veeam Agent.
  - View detailed information on every backup that was created with Veeam Agent.
  - Export/import Veeam Agent configuration database to/from a configuration file.
Veeam Agent control panel is a GUI-like user interface that lets users perform main backup and restore tasks in an easy way. With Veeam Agent control panel, you do not need to work with the Terminal application and remember numerous commands. However, some advanced Veeam Agent operations are not supported by the control panel and can be performed with the command line interface only.

To launch the Veeam Agent control panel, go to Launchpad and click the Veeam Agent for Mac icon.

When you launch the Veeam Agent control panel for the first time, Veeam Agent offers you to grant Veeam Agent full access to the computer disk. To learn more, see Granting Full Disk Access.

After you perform initial product setup, you can use the Veeam Agent control panel to perform the following operations:

- Import a configuration file to connect to the Veeam Backup & Replication.
- Import a previously configured backup.
- Export Veeam Agent logs.
- Open the current Veeam Agent for Mac User Guide.
- Restore files and folders from existing backups.

After you import one or several backup policies, you can also use the control panel to start a backup policy.
Command Line Interface

Veeam Agent command line interface is a powerful tool that lets users perform advanced operations that are not supported by the Veeam Agent control panel.

To work with Veeam Agent using command line interface, you can use a terminal console or a terminal emulator of your choice. All tasks in Veeam Agent are performed with the `veeamconfig` command-line utility. To perform tasks with Veeam Agent, you should construct the necessary command and type it in the terminal prompt.

You can view short help information on every Veeam Agent command at any time you need. To learn more, see Viewing Help.

You should construct a command in the following format:

```
veeamconfig <command_1> <command_2> --<parameter_1> --<parameter_2> --<parameter_n>
```

where:

- `<command_1>` — command that defines a type of an object with which you want to perform a task. Currently, the following commands are available in Veeam Agent:
  - agreement
  - backup
  - cloud
  - config
  - grablogs
  - help
  - job
  - license
  - mode
  - point
  - repository
  - schedule
  - session
  - version
  - vbrserver

- `<command_2>` — command that defines a task that you want to perform with an object of the specified type. For example, you can perform the following commands with backup repositories:
  - create
  - delete
  - edit
- help
- list
- rescan

- `<parameter_1>, <parameter_2>, <parameter_n>` — parameters for the command that you want to execute. Commands may require one or several mandatory or optional parameters. Some commands, for example, `veeamconfig ui` and `veeamconfig [command] help` do not require parameters.

The following example shows the command that displays a list of backup repositories configured in Veeam Agent and the output of this command:

```
user@wrk01:~$ veeamconfig repository list
Name          ID                                      Location            Type      Accessible   Backup server
Repository_1  {818e3a0f-8155-4a51-9430-248a203a43d1}  /home/backups       local     true
Repository_2  {2155a2e7-a1e9-4347-9d8b-cf8f3a6f3fcb}  172.17.53.47/veeam     cifs      true
```
Viewing Help

You can view short help information on the specific Veeam Agent command. To view help, use the following command:

```
veeamconfig <command> help
```

where:

<command> – name of the command for which you want to view help information.

For example:

```
user@wrk01:~$ veeamconfig help
```

or

```
user@wrk01:~$ veeamconfig job help
```

or

```
user@wrk01:~$ veeamconfig job create help
```
Licensing

To work with Veeam Agent, you must accept terms of the product license agreement and license agreements for third-party components operating as part of the product.

If you want to use a commercial version of Veeam Agent, you must obtain a license and install it on the protected computer. If you do not install a license, the product will operate in the Free edition.

Depending on the Veeam Agent operation mode, you can manage licenses in the following ways:

- If Veeam Agent operates in the managed mode, you can manage product licenses and editions from the Veeam Backup & Replication console. To learn more, see Managing License with Veeam Backup & Replication.

- If Veeam Agent operates in the standalone mode, you can manage product licenses with the command line interface. To learn more, see Managing License with Command Line Interface.

To learn more about operation modes, see Standalone and Managed Operation Modes.
Product Editions

Veeam Agent for Mac offers three product editions that define product functionality and operation modes:

- **Server** — a commercial edition that provides access to all product functions and is intended for performing data protection tasks on servers that run macOS.
- **Workstation** — a commercial edition that offers limited capabilities that are sufficient for performing data protection tasks on desktop computers and laptops that run macOS.
- **Free** — a free edition that offers the same capabilities as the Workstation edition but does not come with a commercial support program. In contrast to the workstation and server editions, the Free edition does not require a license.

After the license expires, Veeam Agent for Mac automatically switches to the Free edition. To learn more, see License Expiration.

Limitations for Free and Workstation Editions

Compared to the Server edition of Veeam Agent for Mac, Free and Workstation editions have the following limitations:

For the Free edition

1. The number of backup policies that you can configure in Veeam Agent for Mac is limited to one.
2. If Veeam Agent operates in the managed mode, you cannot use a Veeam backup repository and Veeam Cloud Connect repository as target locations for backup files.
3. If Veeam Agent operates in the standalone mode, you cannot use a Veeam Cloud Connect repository as target locations for backup files.

For the Workstation edition

4. The number of backup jobs that you can configure in Veeam Agent for Mac is limited to one backup job targeted at a local drive, network shared folder, or Veeam backup repository plus unlimited number of backup jobs targeted at a Veeam Cloud Connect repository.
License Agreement

After you install Veeam Agent for Mac, you must accept terms of the product license agreement and license agreements for third-party components operating as part of the product. Until you accept the license agreements, you will not be able to perform backup and data recovery tasks with the Veeam Agent control panel and command line interface.
License Expiration

30 days before the license expiration date, Veeam Agent for Mac will display a warning at the top of the control panel. After the license expires, Veeam Agent for Mac will switch to the Free edition.

If Veeam Agent for Mac operated in the Server or Workstation edition and multiple backup jobs were configured, after switching to the Free edition, all backup jobs will be failing.
Managing License with Command Line Interface

If Veeam Agent operates in the standalone mode, you can manage product licenses with the command line interface.

You can perform the following operations with the license:

- Accept license agreements for the product itself and its third-party components.
- Install a license on the protected computer.
- View information about the license.
- Remove the license.

**TIP**

If Veeam Agent operates in the managed mode, you can manage product licenses only from the Veeam Backup & Replication console. To learn more, see Managing License with Veeam Backup & Replication.
Accepting License Agreements

To work with Veeam Agent for Mac, you must accept terms of the product license agreement and license agreements for third-party components operating as part of the product. Until you accept license agreements, you can use the `veeamconfig` utility to run the following commands only:

- `veeamconfig agreement show`
- `veeamconfig help` (or `veeamconfig -h` and `veeamconfig --help`)
- `veeamconfig mode info`
- `veeamconfig mode reset`
- `veeamconfig version` (or `veeamconfig -v` and `veeamconfig --version`)

To accept license agreements, use the following command:

```
veeamconfig agreement accepteula && veeamconfig agreement acceptthirdpartylicences
```

**TIP**

To check whether license agreements are accepted, use the following command: `veeamconfig agreement show`. 
Installing License

To install a license, use the following command:

```
veeamconfig license install --path <path> --workstation
```

or

```
veeamconfig license install --path <path> --server
```

where:

- `<path>` — path to the license key file in the local file system of your computer.
- `workstation` or `server` — edition in which Veeam Agent will operate. To learn more about editions, see Product Editions.

Veeam Agent for Mac will install the license and display information about the license. You can also view this information later at any time. To learn more, see Viewing License Information.

For example:

```
user@wrk01:~$ veeamconfig license install --path /Users/user/Desktop/veeam.lic --server
License was installed successfully.
License information:
  License source: Local license
  Mode: Server
  Support expiration: 2019/09/20 (649 days left)
  Status: License is valid.
  Issued to: TechCompany
  E-mail: administrators@tech.com
```

TIP

If you work with Veeam Agent operating in the managed mode, you can manage a license only from the Veeam Backup & Replication console. To learn more, see Managing Instance Consumption by Veeam Agents.
Viewing License Information

You can view information about the installed license. Use the following command:

```
veeamconfig license show
```

Veeam Agent for Mac will display information about the license. For example:

```
user@wrk01:~$ veeamconfig license show
License information:
   License source: Veeam Backup & Replication
   Mode: Worstation
```
Removing License

You can remove a license with the following command:

```
veeamconfig license remove
```

After you remove the license, Veeam Agent for Mac will continue to operate in the Free edition. If Veeam Agent operated in the Server edition and multiple backup jobs were configured, after switching to the Free edition, all backup jobs will be failing.
Performing Backup

You can back up your data to protect the user profiles, individual folders and files on your Mac computer. To back up your data, you must configure a backup policy in the Veeam Backup & Replication console. Depending on the product edition, Veeam Agent lets you configure one or several backup policies targeted at the same or different backup repositories.

You can configure a backup policy that will automatically back up your data by the defined schedule. You can also start a backup policy manually at any time.
Importing Backups

You can import a backup file created by Veeam Agent for Mac into the Veeam Agent database. For example, you may want to import a previously deleted backup or backup that was created by Veeam Agent installed on another computer.

Veeam Agent lets you to import backup files from one of the following sources:

- Local or network drive
- Veeam backup server
- Veeam cloud repository

Alternatively, you can import the backup with the command line interface.
Importing Backup from Local Storage

To import the backup file from the local or network drive:

1. In the **Type** field, select the **Local or Network drive** option.
2. Click **Browse** and select the necessary folder that contains the VBM file in the **Finder** window.
   Alternatively, you can type a path to the folder that contains the VBM file in the **Location** field.
3. Click **OK**.

**NOTE**

If you want to import the backup file from the network drive, you must connect your computer to the network storage beforehand.
Importing Backup from Veeam Backup Repository

To import the backup file from the Veeam backup server:

1. In the **Type** field, select the **Veeam Backup Server** option.
2. In the **Server** field, specify a DNS name or IP address of the Veeam backup server.
3. In the **Port** field, specify a number of the port over which Veeam Agent must communicate with the backup repository. By default, Veeam Agent uses port 10006.
4. In the **Login** field, type a name of the account that has access to the Veeam backup repository.
5. In the **Password** field, type a password of the account that has access to the Veeam backup repository. Permissions on the backup repository managed by the target Veeam backup server must be granted beforehand. To learn more, see Setting Up User Permissions on Backup Repositories.
6. Click **OK**.
Importing Backup from Veeam Cloud Repository

To import the backup file from the Veeam cloud repository:

1. In the **Type** field, select the **Veeam Cloud Connect** option.
2. In the **Server** field, enter a full DNS name or IP address of the cloud gateway.
3. In the **Port** field, specify the port over which Veeam Agent will communicate with the cloud gateway. By default, port 6180 is used.
4. In the **Login** field, enter the name of the tenant or subtenant account that the SP or your backup administrator has provided to you. The name of the subtenant account must be specified in the TENANT\SUBTENANT format.
5. In the **Password** field, provide a password for the tenant or subtenant account.
6. Click **OK**.

![Form for importing backup from Veeam Cloud Repository](https://example.com/form)
Creating Managed Backup Job

To back up files and directories of your machine, you must configure a backup policy in the Veeam Backup & Replication console. The backup policy settings define what data to back up as well as where and how to back up data.

To learn more about backup policy configuration, see the Creating Agent Backup Policy for Mac Computers section in the Veeam Agent Management Guide.

You can configure one or several backup policies to back up your data. Configuring several backup policies may be useful in the following situations:

- You can configure backup policies targeted at different backup repositories to keep several copies of your backed-up data at different locations.
- You can configure several backup policies and define individual schedule for every policy to back up necessary data at the desired time.

Alternatively, you can configure a standalone backup job on the Veeam Agent computer side. To do this, use the command line interface.
Starting Backup Job

You can start a backup job manually at any time you need, for example, if you want to create an additional restore point for Veeam Agent backup and do not want to change the policy schedule. You can also stop the running backup job before the policy session completes, if necessary.

You can start a backup job with the Veeam Agent control panel.

To start a backup job:

1. Start Veeam Agent with Launchpad.
2. In the upper-right corner of the menu bar, click the Veeam Agent icon.
3. Select **Start Backup Job**.
   
   If two or more backup jobs are configured, select **Jobs > Start Backup Job "<Name>"**, where `<Name>` is a backup job name.

Veeam Agent will immediately start the backup job.

**NOTE**

Consider the following:

- The **Start Backup Job** option is available only if at least one backup job is configured.
- Veeam Agent can perform only one backup job at a time. If you start a backup job when another backup job is already running, the job that you have started will fail.

Alternatively, you can start the backup job with the command line interface.
Stopping Backup Job

You can stop the running backup job before the job session completes, for example, if the backup process is about to take long, and you do not want the job to produce workload on the production environment during business hours.

When you stop a backup job, the job session will finish immediately. Veeam Agent will not produce a new restore point during the session, and the session will finish with the Failed status.

To stop a backup job:

1. In the upper-right corner of the menu bar, click the Veeam Agent icon.
2. Select Stop Backup Job.
   - If two or more backup jobs are configured, select Jobs > Stop Backup Job "<Name>", where <Name> is a backup job name.

Veeam Agent will immediately stop the backup job.

Alternatively, you can stop the backup job with the command line interface.
Performing Backup with Command Line Interface

Veeam Agent command line interface is a powerful tool that lets users perform advanced operations that are not supported by the Veeam Agent control panel.
Importing Backups

To import a backup using the command line interface:

1. Start the import process with the following command:

   ```
   veeamconfig backup import --path <path>
   ```

   where:

   `<path>` — path to the VBM file of the backup that you want to import.

   For example:

   ```
   user@wrk01:~$ veeamconfig backup import --path /home/share/BackupJob/BackupJob.vbm
   Backup has been imported successfully.
   Session ID: [4031f058-766c-4f2c-a7ae-7257adb2929f].
   Logs stored in: [/var/log/veeam/Import/Session_{4031f058-766c-4f2c-a7ae-7257adb2929f}].
   ```

2. You can monitor the import process and result by viewing the import session log with the following command:

   ```
   veeamconfig session log --id <session_id>
   ```

   where:

   `<session_id>` — ID of the import session.

   For example:

   ```
   user@wrk01:~$ veeamconfig session log --id 4031f058-766c-4f2c-a7ae-7257adb2929f
   2016-11-19 13:21:33 UTC {6ae2922d-454b-4a8d-a11b-2b5c7a85029d} [info] Importing backup
   2016-11-19 13:21:33 UTC {783f40a7-ea7e-4555-9c35-545d875990ee} [info] Backup has been imported.
   ```

3. Imported backup will be displayed in the list of backups. To view the list of backups, use the following command:

   ```
   veeamconfig backup list
   ```
For example:

```bash
user@wrk01:~$ veeamconfig backup list
```

<table>
<thead>
<tr>
<th>Job name</th>
<th>Backup ID</th>
<th>Repository</th>
</tr>
</thead>
<tbody>
<tr>
<td>wrk01 SystemBackup</td>
<td>{45f074d2-d2d9-423d-84e9-8f1798b08d4c}</td>
<td>Repository_1</td>
</tr>
<tr>
<td></td>
<td>1  2016-11-11 17:37</td>
<td></td>
</tr>
<tr>
<td>wrk01 DocsBackup</td>
<td>{ea64a7e5-038a-4c86-970a-6d59d4cf3968}</td>
<td>Repository_1</td>
</tr>
<tr>
<td></td>
<td>1  2016-11-11 18:30</td>
<td></td>
</tr>
<tr>
<td>wrk01 HomeBackup</td>
<td>{4f75bb20-a6b6-4323-9287-1c6c8cecc6b}</td>
<td>Repository_2</td>
</tr>
<tr>
<td></td>
<td>2  2016-11-15 11:28</td>
<td></td>
</tr>
<tr>
<td>BackupJob</td>
<td>{64957b1d-d219-456c-a9cd-9598292c10cd}</td>
<td>Imported</td>
</tr>
<tr>
<td></td>
<td>2016-11-19 19:12</td>
<td></td>
</tr>
</tbody>
</table>
Creating Backup Jobs

You can configure the standalone backup job with the command line interface. Using Veeam Agent for Mac commands, you can create a backup job, specify advanced settings for the created backup job, define backup schedule and enable backup encryption.

Creating Standalone Backup Job

To create a standalone backup job, use the following command:

```bash
veeamconfig job create filelevel --name <job_name> --reponame <repository_name> <objects> <advanced_options> <schedule_options> <active_full_backup_options> --nosnap
```

where:

- `<job_name>` — name for the created backup policy.
- `<repository_name>` — name of the backup repository that should be used as a target location for the backup policy. The backup repository must be created in advance. To learn more, see Creating Backup Repository.
  
  If you want to create Veeam Agent backups in the Veeam backup repository, you should connect to the Veeam backup server in advance, before configuring the backup policy. To learn more, see Connecting to Veeam Backup Server.
- `<objects>` — files and directories inclusion/exclusion options. To learn more, see File Inclusion Options.
- `<advanced_options>` — advanced options for the backup policy. To learn more, see Advanced Backup Policy Settings.
- `<schedule_options>` — schedule options for the backup policy. To learn more, see Schedule Settings.
- `<active_full_backup_options>` — active full backup schedule options for the backup policy. To learn more, see Active Full Backup Schedule Settings.

For example:

```bash
user@wrk01:~$ veeamconfig job create filelevel --name HomeFolderBackup --reponame NetworkRepository --includedirs /home/user --excludedirs /home/user/temp --excludemasks *.pdf
```

TIP

Consider the following:

- You can also specify backup schedule for the backup policy after your create the backup policy. For details, see Configuring Backup Schedule.
- You can also specify active full backup schedule for the backup policy after your create the backup policy. For details, see Configuring Active Full Backup Schedule.
File Inclusion Options

When you create a backup policy, you must specify at least one folder that should be included in backup. If you do not want to back up some files and directories in the specified folder, you can exclude specific files and directories from backup.

To define the backup scope for the backup policy, you can use the following command-line options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description and values</th>
</tr>
</thead>
<tbody>
<tr>
<td>--includedirs</td>
<td>Full path to a folder that should be included in backup, for example: /home/user. You can specify one or several paths to directories in the computer file system. To separate several paths, use the ',' (comma) character. For example: /home/user/Documents,/home/user/reports. Tip: If you want to back up the root directory and specify the '/' (slash) character, Veeam Agent does not automatically include mount points in the backup scope. To include mount points, you need to specify paths to these mount points manually. For example, you have a file system mounted to the /home/media directory. If you add / as an object to the backup scope, Veeam Agent will not back up the mounted file system. To back up the root directory and the mounted file system, add the following objects to the backup scope: /, /home/media.</td>
</tr>
<tr>
<td>--excludedirs</td>
<td>Full path to a folder that should be excluded from backup. The folder specified with this option must be a subfolder of the folder specified with the --includedirs option. To separate several paths, use the ',' (comma) character. For example, /home/user/Documents,/home/user/reports.</td>
</tr>
</tbody>
</table>
| --includemasks | Mask for file name or path that should be included in backup. You can use the following UNIX wildcard characters for file name masks:
  - '*' — a substitution for one or more characters in the file name or path. Can be used for any sequence of characters (including no characters). For example, *.pdf.
  - '?' — a substitution of one character in the file name or path. For example, report?.pdf.
  - '[]' — a substitution of one character in the file name or path with any of the characters enclosed in square brackets (or a range of characters defined with the '-' character). For example: report_201[3456].pdf or report_201[3-6].pdf.
  Keep in mind that you must specify all names with masks in double quotation marks (""). For example: --includemasks "*.bak". If you want to use several file name masks, you must specify them in double quotation marks (""" and separated with a comma (,). For example: --includemasks "*.bak,*.pdf". File inclusion option is applied to all directories that are specified with the --includedirs option. For example, if you include in backup the /home/user/Documents folder and files that match the report?.pdf file name... |
Option | Description and values
--- | ---
mask, Veeam Agent will back up the /home/user/Documents/report.pdf file and will not back up the /home/user/reports/report.pdf file.

---excludemasks

Mask for file name or path that should be excluded from backup. You can use the followingUNIX wildcard characters for file name masks:

- ‘*’ — a substitution for one or more characters in the file name or path. Can be used for any sequence of characters (including no characters). For example, *.pdf.
- ‘?’ — a substitution of one character in the file name or path. For example, repor?.pdf.
- ‘[]’ — a substitution of one character in the file name or path with any of the characters enclosed in square brackets (or a range of characters defined with the ‘-’ character). For example: report_201[3456].pdf or report_201[3-6].pdf.

Keep in mind that you must specify all names with masks in double quotation marks (""). For example: --excludemasks "*.bak".

If you want to use several file name masks, you must specify them in double quotation marks ("" ) and separated with a comma (,). For example: --excludemasks *.bak,*.pdf.

File exclusion option is applied to all directories that are specified with the --includedirs option and files that match file name masks specified with the --includemasks option. For example, you may want to specify the following backup scope for the backup policy:

- Include in backup the /home/user/Documents folder
- Include files that match the report.* file name mask
- Exclude files that match the *.odt file name mask.

In this case, Veeam Agent will back up the /home/user/Documents/report.pdf file and will not back up /home/user/Documents/report.odt and /home/user/reports/report.pdf files.
Advanced Backup Policy Settings

You can specify the following advanced options for the backup policy:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description and values</th>
</tr>
</thead>
</table>
| **--compressionlevel** | Data compression level. Possible values are:  
  - 0 — No compression  
  - 1 — Rle  
  - 2 — Lz4  
  - 3 — ZlibLow  
  - 4 — ZlibHigh |
| **--blocksize** | Data block size in kilobytes. Possible values are 256, 512, 1024, 4096 or 8192.  
  The default value is 1024. |
| **--maxpoints** | The number of restore points that you want to store in the backup location. By default, Veeam Agent keeps 7 latest restore points. When the new restore point that exceeds the specified number is created, Veeam Agent will remove the earliest restore point from the backup chain. |
| **--setencryption** | Defines that data encryption option is enabled for the policy. When you use the veeamconfig job create command with the --setencryption option, Veeam Agent will prompt you to specify a password for data encryption and hint for the password. |
| **--deleteold** | The number of days to keep the backup created with the backup job in the target location. If Veeam Agent does not create new restore points for the backup, the backup will remain in the target location for the specified number of days. When this period is over, the backup will be removed from the target location. Possible values are: 1–999.  
  If you do not specify the --deleteold option, Veeam Agent will not apply this setting. As a result, backup will be stored in the target location until you delete it manually. |

Schedule Settings

You can specify schedule options for the backup policy to create backups daily or on specific weekdays at specific time:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description and values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>--daily</strong></td>
<td>Defines that the backup policy must start daily at specific time.</td>
</tr>
</tbody>
</table>
### Option Description and values

<table>
<thead>
<tr>
<th>Option</th>
<th>Description and values</th>
</tr>
</thead>
</table>
| --weekdays | Weekdays when the backup policy must start separated by a comma (','). Possible values are:  
  - *Mon* — Monday  
  - *Tue* — Tuesday  
  - *Wed* — Wednesday  
  - *Thu* — Thursday  
  - *Fri* — Friday  
  - *Sat* — Saturday  
  - *Sun* — Sunday |
| --at      | Time of day when the backup policy must start specified in the *HH:MM* format. For example: 20:00. |

After the backup policy is created, Veeam Agent automatically enables backup schedule. To learn about how to configure backup schedule for an existing backup policy, see [Configuring Backup Schedule](#).

### Active Full Backup Schedule Settings

You can specify schedule options for the backup policy to create active full backups on specific weekdays or days of the month:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description and values</th>
</tr>
</thead>
</table>
| --weekdays-full | Weekdays when the backup policy must create an active full backup separated by a comma (','). Possible values are:  
  - *Mon* — Monday  
  - *Tue* — Tuesday  
  - *Wed* — Wednesday  
  - *Thu* — Thursday  
  - *Fri* — Friday  
  - *Sat* — Saturday  
  - *Sun* — Sunday |
| --thisday-full | Days of the month when the backup policy must create an active full backup separated by a comma (','). Possible values are: 1-30 (or 1-31, depending on the month length). |

After the backup policy is created, Veeam Agent automatically enables active full backup schedule. To learn about how to configure active full backup schedule for an existing backup policy, see [Configuring Active Full Backup Schedule](#).
Creating Active Full Backup

You can create an ad-hoc full backup — active full backup, and add it to the backup chain on the target storage. The active full backup resets the backup chain. All subsequent incremental backups use the active full backup as a starting point. The previously used full backup will remain on the target storage until it is removed from the backup chain according to the retention policy.

Before you create an active full backup, check the following prerequisites:

- The backup policy must be configured.
- You cannot create an active full backup if a backup task of any type is currently running.

To perform active full backup, use the following command:

```
veeamconfig job start --name <job_name> --activefull
```

or

```
veeamconfig job start --id <job_id> --activefull
```

where:

- `<job_name>` — name of the backup policy that you want to start to create an active full backup.
- `<job_id>` — ID of the backup policy that you want to start to create an active full backup.

For example:

```
user@wrk01:~$ veeamconfig job start --name SystemBackup --activefull
Backup job has been started.
Session ID: [{ce864e24-8211-4df7-973a-741adce96fe7}].
Logs stored in: [/var/log/veeam/Backup/SystemBackup/Session_20180611_150046_{ce864e24-8211-4df7-973a-741adce96fe7}].
```

You can view the progress for the active full backup session in the same way as for any other backup policy session. In particular, you can check the backup policy session status or view the backup policy session log using the Veeam Agent command line interface. You can also monitor the backup policy performance in the Veeam Backup & Replication console. To learn more, see Reporting with Veeam Backup & Replication Console.
Configuring Backup Schedule

To run a backup job periodically without user intervention, you can schedule it to start automatically. You can specify schedule settings individually for every policy created in Veeam Agent for Mac. You can perform the following actions with the backup policy schedule via the command-line interface:

- Specify schedule settings for the backup job.
- Enable schedule for the backup job.
- View the schedule defined for the backup job.
- Disable schedule for the backup job.

Specifying Backup Schedule

You can schedule a backup policy to start at a specific time daily or on specific week days.

Specifying Daily Schedule

To specify daily schedule settings for the backup policy, use the following command:

```
veeamconfig schedule set --jobid <job_id> --daily --at <time>
```

or

```
veeamconfig schedule set --jobname <job_name> --daily --at <time>
```

where:

- `<job_id>` — ID of the backup policy for which you want to configure the schedule. You should look up the policy ID in advance, before configuring the schedule, for example, with the `veeamconfig job list` command. To learn more, see Viewing List of Backup Policies.

- `<job_name>` — name of the backup policy for which you want to configure the schedule.

- `<time>` — time of day when the backup policy must start specified in the `HH:MM` format. For example: 20:00.

For example:

```
user@wrk01:~$ veeamconfig schedule set --jobid 4849a3ae-1935-4969-98a3-d8ac2f6c73f --daily --at 20:00
```

Specifying Schedule on Specific Days

To specify schedule settings for the backup policy, use the following command:

```
veeamconfig schedule set --jobid <job_id> --weekdays <days> --at <time>
```
or

```bash
veeamconfig schedule set --jobname <job_name> --weekdays <days> --at <time>
```

where:

- `<job_id>` — ID of the backup policy for which you want to configure the schedule. You should look up the policy ID in advance, before configuring the schedule, for example, with the `veeamconfig job list` command. To learn more, see Viewing List of Backup Policies.

- `<job_name>` — name of the backup policy for which you want to configure the schedule.

- `<days>` — days when the backup policy must start separated by a comma (','). For example: Monday, Tuesday, Wednesday, Thursday, Friday.

- `<time>` — time of day when the backup policy must start specified in the `HH:MM` format. For example: 20:00.

For example:

```bash
user@wrk01:~$ veeamconfig schedule set --jobname DailyBackup --weekdays Monday, Tuesday, Wednesday, Thursday, Friday --at 20:00
```

### Enabling Backup Schedule

To run a backup policy automatically upon the defined schedule, you must enable the schedule for the policy. Use the following command:

```bash
veeamconfig schedule enable --jobid <job_id>
```

or

```bash
veeamconfig schedule enable --jobname <job_name>
```

where:

- `<job_id>` — ID of the backup policy for which you want to enable the schedule. You should look up the policy ID in advance, for example, with the `veeamconfig job list` command. To learn more, see Viewing List of Backup Policies.

- `<job_name>` — name of the backup policy for which you want to enable the schedule.

For example:

```bash
user@wrk01:~$ veeamconfig schedule enable --jobid 4849a3ae-1935-4969-98a3-d8acd2f6c73f
```

You can disable the schedule for the policy at any time. To learn more, see Disabling Backup Schedule.
Viewing Backup Schedule

To view the schedule defined for the backup policy, use the following command:

```
veeamconfig schedule show --jobid <job_id>
```

or

```
veeamconfig schedule show --jobname <job_name>
```

where:

- `<job_id>` — ID of the backup policy for which you want to view the schedule.
- `<job_name>` — name of the backup policy for which you want to view the schedule.

Veeam Agent for Mac displays the following information about the backup policy schedule:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Days</td>
<td>Days on which the backup policy runs automatically.</td>
</tr>
<tr>
<td>At</td>
<td>Time of day when the backup policy starts automatically.</td>
</tr>
<tr>
<td>Run automatically</td>
<td>State of backup schedule. Possible values:</td>
</tr>
<tr>
<td></td>
<td>• Enabled</td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
</tr>
</tbody>
</table>

For example:

```
user@wrk01:~$ veeamconfig schedule show --jobid 4849a3ae-1935-4969-98a3-d8acd2f6c73f
Days: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday
At: 20:00
Run automatically: enabled
```

Disabling Backup Schedule

To disable the schedule for the backup policy, use the following command:

```
veeamconfig schedule disable --jobid <job_id>
```

or

```
veeamconfig schedule disable --jobname <job_name>
```
where:

- `<job_id>` — ID of the backup policy for which you want to disable the schedule.
- `<job_name>` — name of the backup policy for which you want to disable the schedule.

For example:

```
user@wrk01:~$ veeamconfig schedule disable --jobid 4849a3ae-1935-4969-98a3-d8ac d2f6c73f
```

### Configuring Active Full Backup Schedule

You can schedule a backup policy to create active full backups periodically. You can specify active full schedule settings individually for every policy created in Veeam Agent for Mac. You can perform the following actions with the active full backup schedule via the command-line interface:

- Specify active full backup schedule.
- Enable active full backup schedule.
- View active full backup schedule.
- Disable active full backup schedule.

**TIP**

You can also specify active full backup schedule for the backup policy when you create the policy. For details, see [Creating Backup Policy](#).

### Specifying Active Full Backup Schedule

You can schedule a backup policy to create active full backups on a specific day of the month or on specific weekdays.

#### Specifying Monthly Active Full Backup Schedule

To instruct Veeam Agent to perform active full backup on a specific day on the month, use the following command:

```
veeamconfig schedule activefull set --jobid <job_id> --thisday <day>
```

or

```
veeamconfig schedule activefull set --jobname <job_name> --thisday <day>
```

where:

- `<job_id>` — ID of the backup policy for which you want to configure the active full backup schedule. You should look up the policy ID in advance, before configuring the schedule, for example, with the `veeamconfig job list` command. To learn more, see [Viewing List of Backup Policies](#).
• `<job_name>` — name of the backup policy for which you want to configure the active full backup schedule.

• `<day>` — number of the day of the month when Veeam Agent must perform active full backup.

For example:

```bash
user@wrk01:~$ veeamconfig schedule activefull set --jobname DailyBackup --thisday 1
```

### Specifying Weekly Active Full Backup Schedule

To instruct Veeam Agent to perform active full backup on specific week days, use the following command:

```bash
veeamconfig schedule activefull set --jobid <job_id> --weekdays <days>
```

or

```bash
veeamconfig schedule activefull set --jobname <job_name> --weekdays <days>
```

where:

• `<job_id>` — ID of the backup policy for which you want to configure the active full backup schedule. You should look up the policy ID in advance, before configuring the schedule, for example, with the `veeamconfig job list` command. To learn more, see Viewing List of Backup Policies.

• `<job_name>` — name of the backup policy for which you want to configure the active full backup schedule.

• `<days>` — days when the backup policy must create an active full backup separated by a comma (','). For example: Monday,Friday. The backup policy will create an active full backup on the specified days at the time specified in the backup policy schedule settings.

For example:

```bash
user@wrk01:~$ veeamconfig schedule activefull set --jobname DailyBackup --weekdays Monday,Friday
```

### Enabling Active Full Backup Schedule

After you specify active full backup schedule settings for the backup policy, Veeam Agent automatically enables active full backup schedule for the policy. You can also enable active full backup schedule manually, for example, if you previously disabled it for the backup policy. To enable active full backup schedule, use the following command:

```bash
veeamconfig schedule activefull enable --jobid <job_id>
```

or
veeamconfig schedule activefull enable --jobname <job_name>

where:

- `<job_id>` — ID of the backup policy for which you want to enable the active full backup schedule. You should look up the policy ID in advance, for example, with the veeamconfig policy list command. To learn more, see Viewing List of Backup Policies.
- `<job_name>` — name of the backup policy for which you want to enable the active full backup schedule.

For example:

```
user@wrk01:-$ veeamconfig schedule activefull enable --jobname DailyBackup
```

You can disable the schedule for the policy at any time. To learn more, see Disabling Backup Schedule.

### Viewing Active Full Backup Schedule

To view the active full backup schedule defined for the backup policy, use the following command:

```
veeamconfig schedule activefull show --jobid <job_id>
```

or

```
veeamconfig schedule activefull show --jobname <job_name>
```

where:

- `<job_id>` — ID of the backup policy for which you want to view the active full backup schedule.
- `<job_name>` — name of the backup policy for which you want to view the active full backup schedule.

Veeam Agent for Mac displays the following information about the active full backup schedule:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Every <code>&lt;value&gt;</code></td>
<td>Days on which the backup policy creates active full backups. For example: Every Monday or Every 1 day of every month.</td>
</tr>
<tr>
<td>Run automatically</td>
<td>State of the active full backup schedule. Possible values:</td>
</tr>
<tr>
<td></td>
<td>• Enabled</td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
</tr>
</tbody>
</table>

For example:

```
user@wrk01:-$ veeamconfig schedule activefull show --jobname DailyBackup
Every Monday
Run automatically: enabled
```
Disabling Active Full Backup Schedule

To disable the active full backup schedule for the backup policy, use the following command:

```
veeamconfig schedule activefull disable --jobid <job_id>
```

or

```
veeamconfig schedule activefull disable --jobname <job_name>
```

where:

- `<job_id>` — ID of the backup policy for which you want to disable the active full backup schedule.
- `<job_name>` — name of the backup policy for which you want to disable the active full backup schedule.

For example:

```
user@wrk01:~$ veeamconfig schedule activefull disable --jobname DailyBackup
```
Starting Backup Job

You can start a backup job with the command line interface. When you start a backup job, Veeam Agent initiates a new backup job session and provides you with a Session ID. You can monitor the progress of the backup job session or view the session status.

**NOTE**
Veeam Agent can currently perform only one backup job at a time. You cannot start a backup job when another backup job is already running.

To start a backup job, use the following command:

```
veeamconfig job start --name <job_name>
```

or

```
veeamconfig job start --id <job_id>
```

where:

- `<job_name>` — name of the backup job that you want to start.
- `<job_id>` — ID of the backup job that you want to start.

**TIP**
You can use the `veeamconfig job start` command with the `--activefull` option to create active full backups. To learn more, see Creating Active Full Backups.

For example:

```
user@wrk01:~$ veeamconfig job start --name SystemBackup
Backup job has been started.
Session ID: [381532f7-426a-4e89-b9fc-43d98942c71a].
Logs stored in: [/var/log/veeam/Backup/SystemBackup/Session_20161207_162608_{381532f7-426a-4e89-b9fc-43d98942c71a}].
```

You can check the backup job session status or view the backup job session log using the Veeam Agent command line interface.
Stopping Backup Job

To stop a backup job, use the following command:

```
veeamconfig session stop --id <session_id>
```

or

```
veeamconfig session stop --force --id <session_id>
```

where:

- `<session_id>` — ID of the currently running backup job session that you want to stop.
- `--force` — with this option enabled, Veeam Agent will immediately stop the backup session even if it is unable to stop the `veeamjobman` process for some reason.

For example:

```
user@wrk01:~$ veeamconfig session stop --id 381532f7-426a-4e89-b9fc-43d98942c71a
Session has stopped.
```
Managing Backup Jobs

You can perform the following actions with backup policies configured in Veeam Agent for Mac:

- View the list of configured backup jobs.
- View information about the backup job settings.
- Edit the backup job settings.
- Delete a backup job.
Viewing List of Backup Jobs

To view a list of backup jobs configured in Veeam Agent, use the following command:

```bash
veeamconfig job list
```

In the list of backup jobs, Veeam Agent displays the following information:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the backup job.</td>
</tr>
<tr>
<td>ID</td>
<td>ID of the backup job.</td>
</tr>
<tr>
<td>Repository</td>
<td>Name of the backup repository that is specified as a backup storage for the backup job.</td>
</tr>
</tbody>
</table>

For example:

```bash
user@wrk01:~$ veeamconfig job list
Name               ID                                      Repository
SystemBackup       {2495911e-58db-4452-b4d1-f53dcfbc600e}  Repository_1
DocumentsBackup    {bcf821e6-b35f-4d57-b1c3-d3a477605cb9}  Repository_1
HomePartitionBackup {2aaa8c71-2434-4f12-a168-3d8e225fa416}  Repository_2
```
Viewing Backup Job Settings

To view detailed information about the backup job settings, use the following command:

```
veeamconfig job info --name <job_name>
```

or

```
veeamconfig job info --id <job_id>
```

where:
- `<job_name>` — name of the backup job for which you want to view settings.
- `<job_id>` — ID of the backup job for which you want to view settings.

Veeam Agent for Mac displays the following information about the backup job:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>ID of the backup job.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the backup job.</td>
</tr>
<tr>
<td>Repository ID</td>
<td>ID of the backup repository that is specified as a backup storage for the backup job.</td>
</tr>
<tr>
<td>Repository name</td>
<td>Name of the backup repository that is specified as a backup storage for the backup job.</td>
</tr>
<tr>
<td>Creation time</td>
<td>Date and time of the backup job creation.</td>
</tr>
<tr>
<td>Compression</td>
<td>Data compression level. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• 0 — No compression</td>
</tr>
<tr>
<td></td>
<td>• 1 — Rle</td>
</tr>
<tr>
<td></td>
<td>• 2 — Lz4</td>
</tr>
<tr>
<td></td>
<td>• 3 — ZlibLow</td>
</tr>
<tr>
<td></td>
<td>• 4 — ZlibHigh</td>
</tr>
<tr>
<td>Max Points</td>
<td>Number of restore points to keep on disk. By default, Veeam Agent for Mac keeps 7 latest restore points. When the new restore point that exceeds the specified number is created, Veeam Agent for Mac will remove the earliest restore point from the backup chain.</td>
</tr>
<tr>
<td>Block size</td>
<td>Size of data blocks that Veeam Agent uses to process data.</td>
</tr>
<tr>
<td>Retry count</td>
<td>Number of retries specified for the backup job.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------</td>
</tr>
<tr>
<td>Objects for backup</td>
<td>Backup scope specified for the backup job.</td>
</tr>
<tr>
<td>Schedule</td>
<td>Schedule specified for the backup job.</td>
</tr>
</tbody>
</table>

For example:

```
user@wrk01:~$ veeamconfig job info --name SystemBackup
Backup job
  ID: {2495911e-58db-4452-b4d1-f53dcfbc600e}
  Name: SystemBackup
  Repository ID: {4557ef7a-9c44-4f28-b8d0-44d78e5dd5d}
  Repository name: Repository_1
  Creation time: 2017-04-06 13:29:03
  Options:
    Compression: Lz4
    Max Points: 7
    Block size: 1024 KB
    Retry count: 3
    Snapshot required
  Objects for backup:
    Include User profiles: all
  Schedule:
    Every day
    At: 12:00
```
Editing Backup Job Settings

If you want to change settings of the backup job, you can edit it at any time. For example, you may want to edit the backup job to add a new folder to the backup scope or change the target location.

To edit a backup job, use the following command:

```
veeamconfig job edit filelevel <option> for --name <job_name>
```

or

```
veeamconfig job edit filelevel <option> for --id <job_id>
```

where:

- `<option>` — option that you want to edit for the job. You can specify one or several options at a time. To learn more, see Backup Job Options.
- `<job_name>` — name of the backup job that you want to edit.
- `<job_id>` — ID of the backup job that you want to edit.

For example:

```
user@wrk01:~$ veeamconfig job edit filelevel --name SystemVolumeBackup for --name SystemVolume
```

Backup Job Options

You can use the following options to edit parameters for the backup job:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description and values</th>
</tr>
</thead>
<tbody>
<tr>
<td>--compressionlevel</td>
<td>Data compression level. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• 0 — No compression</td>
</tr>
<tr>
<td></td>
<td>• 1 — Rle</td>
</tr>
<tr>
<td></td>
<td>• 2 — Lz4</td>
</tr>
<tr>
<td></td>
<td>• 3 — ZlibLow</td>
</tr>
<tr>
<td></td>
<td>• 4 — ZlibHigh</td>
</tr>
<tr>
<td>--blocksize</td>
<td>Data block size in kilobytes. Possible values are 256, 512, 1024, 4096 or 8192.</td>
</tr>
<tr>
<td></td>
<td>The default value is 1024.</td>
</tr>
<tr>
<td>--maxpoints</td>
<td>Number of restore points that you want to store in the backup location. By default,</td>
</tr>
<tr>
<td></td>
<td>Veeam Agent keeps 7 latest restore points. When the new restore point that exceeds the</td>
</tr>
<tr>
<td></td>
<td>specified number is created, Veeam Agent will remove the earliest restore point from</td>
</tr>
<tr>
<td></td>
<td>the backup chain.</td>
</tr>
<tr>
<td>Option</td>
<td>Description and values</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>--includedirs</td>
<td>Full path to a folder that should be included in backup, for example: /home/user. You can specify one or several paths to directories in the computer file system. To separate several paths, use a ',' (comma) character, for example: /home/user/Documents,/home/user/reports.</td>
</tr>
<tr>
<td>--excludedirs</td>
<td>Full path to a folder that should be excluded from backup. The folder specified with this option must be a subfolder of the folder specified with the --includedirs option. To separate several paths, use a ',' (comma) character, for example, /home/user/Documents,/home/user/reports.</td>
</tr>
</tbody>
</table>
| --includemasks| Mask for file name or path that should be included in backup. You can use the following UNIX wildcard characters for file name masks:  
- '('* — a substitution for one or more characters in the file name or path. Can be used for any sequence of characters (including no characters). For example, *.pdf.  
- '?(' — a substitution of one character in the file name or path. For example, repor?.pdf.  
- '[[](' — a substitution of one character in the file name or path with any of the characters enclosed in square brackets (or a range of characters defined with the '-' character). For example: report_201[3456].pdf or report_201[3-6].pdf.  
To separate several masks, use a ',' (comma) character, for example, report.*,reports.*.  
File inclusion option is applied to all directories that are specified with the --includedirs option. For example, if you include in backup the /home/user/Documents folder and files that match the repor?.pdf file name mask, Veeam Agent will back up the /home/user/Documents/report.pdf file and will not back up the /home/user/reports/report.pdf file. |
| --excludemasks| Mask for file name or path that should be excluded from backup. You can use the following UNIX wildcard characters for file name masks:  
- '('* — a substitution for one or more characters in the file name or path. Can be used for any sequence of characters (including no characters). For example, *.pdf.  
- '?(' — a substitution of one character in the file name or path. For example, repor?.pdf.  
- '[[](' — a substitution of one character in the file name or path with any of the characters enclosed in square brackets (or a range of characters defined with the '-' character). For example: report_201[3456].pdf or report_201[3-6].pdf. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description and values</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To separate several masks, use a ',' (comma) character, for example, report.<em>,reports.</em>.</td>
</tr>
<tr>
<td></td>
<td>File exclusion option is applied to all directories that are specified with the --includedirs option and files that match file name masks specified with the --includemasks option. For example, you may want to specify the following backup scope for the backup job:</td>
</tr>
<tr>
<td></td>
<td>- Include in backup the /home/user/Documents folder</td>
</tr>
<tr>
<td></td>
<td>- Include files that match the report.* file name mask</td>
</tr>
<tr>
<td></td>
<td>- Exclude files that match the *.odt file name mask.</td>
</tr>
<tr>
<td></td>
<td>In this case, Veeam Agent will back up the /home/user/Documents/report.pdf file and will not back up /home/user/Documents/report.odt and /home/user/reports/report.pdf files.</td>
</tr>
<tr>
<td></td>
<td>If you want to use several name masks, you must specify them in double quotation marks, for example: veeamconfig job create filelevel --name BackupJob1 --reponame vault13 --includedirs /home --includemasks &quot;<em>.bak,</em>.pdf&quot;.</td>
</tr>
<tr>
<td>--setencryption</td>
<td>Defines that data encryption option is enabled for the job. You can use this option to enable encryption for the existing backup job or change a password used for encryption for the backup job. When you use the veeamconfig job edit command with the --setencryption option, Veeam Agent for Mac will prompt you to specify a password for data encryption and hint for the password.</td>
</tr>
<tr>
<td>--resetencryption</td>
<td>Defines that data encryption option is disabled for the job. You can use this option to disable encryption for the existing backup job.</td>
</tr>
<tr>
<td>--deleteold</td>
<td>The number of days to keep the backup created with the backup job in the target location. If Veeam Agent does not create new restore points for the backup, the backup will remain in the target location for the specified number of days. When this period is over, the backup will be removed from the target location. Possible values are: 1–999.</td>
</tr>
<tr>
<td></td>
<td>If the --deleteold option is not specified, Veeam Agent does not apply this setting. As a result, backup will be stored in the target location until you delete it manually.</td>
</tr>
<tr>
<td></td>
<td>If you specified the value earlier and want to disable this setting, specify the false value for the option: --deleteold false. After the next successful backup session, this setting will be disabled for the backup in the target location.</td>
</tr>
</tbody>
</table>
NOTE

Consider the following:

- If you change the target location for the backup job, during the next backup job session Veeam Agent for Mac will perform full data backup. All subsequent backup sessions will produce incremental backups — Veeam Agent for Mac will copy only changed data to the target location and add a new incremental backup file to the backup chain.

- If you change the backup scope for the backup job, during the next backup job session Veeam Agent for Mac will create a new incremental backup. The backup will contain all data blocks pertaining to new data added to the backup scope and changed data blocks pertaining to original data in the backup scope (data that was processed by the job at the time before you changed the backup scope).

- Full backup takes much more time than incremental backup. If you change the target location, you can copy an existing backup chain to the new location manually. In this case, the new backup job session will produce an incremental backup file and add it to the backup chain.
Deleting Backup Job

You can delete a backup job with the Veeam Agent command line interface. To delete a backup job, use the following command:

```
veeamconfig job delete --name <job_name>
```

or

```
veeamconfig job delete --id <job_id>
```

where:

- `<job_name>` — name of the backup job that you want to delete.
- `<job_id>` — ID of the backup job that you want to delete.

For example:

```
user@wrk01:~$ veeamconfig job delete --name SystemBackup
```
Managing Backups

You can perform the following operations with backups created by backup jobs configured in Veeam Agent for Mac:

- View backups
- View backup details
- View restore points in backup
- Delete backup
Viewing Backups

To view a list of backups created by a backup job configured in Veeam Agent for Mac, use the following command:

```
veeamconfig backup list
```

In the list of backups, Veeam Agent for Mac displays the following information:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Job name</strong></td>
<td>Name of the backup job by which the backup was created.</td>
</tr>
<tr>
<td><strong>Backup ID</strong></td>
<td>ID of the backup.</td>
</tr>
<tr>
<td><strong>Repository</strong></td>
<td>Name of the backup repository in which the backup was created.</td>
</tr>
<tr>
<td></td>
<td>Imported backups are marked as <em>Imported</em> in the <strong>Repository</strong> column.</td>
</tr>
<tr>
<td></td>
<td>For information about the import procedure, see <a href="#">Importing Backups</a>.</td>
</tr>
<tr>
<td><strong>Created at</strong></td>
<td>Date and time of the backup creation.</td>
</tr>
</tbody>
</table>

For example:

```
user@wrk01:~$ veeamconfig backup list
Job name            Backup ID                               Repository    Created at
wrk01 SystemBackup  {45f074d2-d2d9-423d-84e9-8f1798b08d4c}  Repository_1  2016-11-11 17:37
wrk01 DocsBackup    {ea64a7e5-038a-4c86-970a-6d59d4cf3968}  Repository_1  2016-11-11 18:30
wrk01 HomeBackup    {4f75bb20-a6b6-4323-9287-1c6c8cecb6b}  Repository_2  2016-11-15 11:28
```
Viewing Backup Details

You can view detailed information about specific backup. To view backup details, use the following command:

```
veeamconfig backup show --id <backup_id>
```

where:

- `<backup_id>` — ID of the backup for which you want to view detailed information.

Veeam Agent for Mac displays the following information:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine name</td>
<td>Host name of the machine on which the backup job is configured and the name of the job.</td>
</tr>
<tr>
<td>Backed up</td>
<td>Backup scope for the file-level backup job.</td>
</tr>
</tbody>
</table>

For example:

```
user@wrk01:$ veeamconfig backup show --id ea64a7e5-038a-4c86-970a-6d59d4cf3968
  Machine name: wrk01 DocsBackup
  File-level backup
  Backed up:
  /home/user/Documents
```
Viewing Restore Points in Backup

To view information about restore points in the backup, you can use one of the following commands:

```
veeamconfig backup info --id <backup_id>
```

or

```
veeamconfig point list --backupid <backup_id>
```

where:

- `<backup_id>` — ID of the backup for which you want to view information on restore points.

For example:

```
user@wrk01:~$ veeamconfig backup info --id 4f75bb20-a6b6-4323-9287-1c6c8ceccb6b
```

or

```
user@wrk01:~$ veeamconfig point list --backupid 4f75bb20-a6b6-4323-9287-1c6c8ceccb6b
```

Veeam Agent for Mac displays the following information about restore points in the backup:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job name</td>
<td>Name of the backup job by which the backup was created.</td>
</tr>
<tr>
<td>OIB ID</td>
<td>ID of the restore point in the backup.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of the restore point. Possible values:</td>
</tr>
<tr>
<td></td>
<td>• Full</td>
</tr>
<tr>
<td></td>
<td>• Increment</td>
</tr>
<tr>
<td>Created at</td>
<td>Date and time of the restore point creation.</td>
</tr>
<tr>
<td>Is corrupt</td>
<td>Indicates whether restore point in the backup is corrupted. Possible values:</td>
</tr>
<tr>
<td></td>
<td>• True</td>
</tr>
<tr>
<td></td>
<td>• False</td>
</tr>
</tbody>
</table>
Deleting Backups

Backup files created with Veeam Agent are removed automatically according to the retention job settings. You can also remove backups from the target location and/or Veeam Agent configuration database manually if necessary.

Removing Backup from Configuration

To remove a backup from the Veeam Agent configuration database, use the following command:

```
veeamconfig backup delete --id <backup_id>
```

where:

- `<backup_id>` — ID of the backup that you want to delete.

Veeam Agent for Mac will remove records about the deleted backup from the Veeam Agent database. Backup files themselves (VBK, VIB, VBM) remain in the backup repository. You can import the removed backup later to Veeam Agent for Mac and perform restore operations with the imported backup.

Deleting Backup Files

To delete backup files from the target location and Veeam Agent database, use the following command:

```
veeamconfig backup delete --id <backup_id> --purge
```

where:

- `<backup_id>` — ID of the backup that you want to delete.

Veeam Agent for Mac will remove records about the deleted backup from the Veeam Agent database and, additionally, delete backup files themselves from the destination storage.
Managing Service Providers

You can store backup files created with Veeam Agent for Mac on a cloud repository exposed to you by a Veeam Cloud Connect service provider. To do this, you must connect to a service provider. After that, you can specify a cloud repository as a target location for backup files in the properties of the backup job.
Connecting to Service Provider

To create Veeam Agent backups on a cloud repository, you must connect to a Veeam Cloud Connect service provider.

To connect Veeam Agent for Mac to a service provider, use the following command:

```sh
toolkit config cloud add --name <sp_name> --address <sp_address> --port <sp_port>

--login <username> --password <password> --fingerprint <sp_thumbprint>
```

where:

- `<sp_name>` — name of the service provider to which you want to connect.
- `<sp_address>` — IP address or full DNS name of the cloud gateway that the SP or your backup administrator has provided to you.
- `<sp_port>` — port over which Veeam Agent must communicate with the cloud gateway. The default port used for communication with the cloud gateway is 6180.
- `<username>` — name of the tenant or subtenant account that the SP or your backup administrator has provided to you. The name of the subtenant account must be specified in the `TENANT/SUBTENANT` format.
- `<password>` — password of the tenant or subtenant account used to connect to the service provider.
- `<sp_thumbprint>` — thumbprint used to verify the TLS certificate that the SP has provided to you.

For example:

```sh
user@wrk01:~$ veeamconfig cloud add --name SP --address 172.17.53.15 --port 6180

--login TechCompany/User01 --password P@ssw0rd --fingerprint 92FA988A3D9E80EE095DDAB75BF06B05DF6F205B
```

**NOTE**

When you enter the `veeamconfig cloud add` command, Veeam Agent will display information about the TLS certificate obtained from the SP. To accept the certificate, type `yes` in the command prompt and press **Enter**.

When Veeam Agent connects to the service provider, Veeam Agent retrieves information about cloud repositories available to the tenant or subtenant and displays them in the list of available backup repositories. You can then specify a cloud repository as a target for a backup job.

**TIP**

To view the list of available cloud repositories, use the `veeamconfig repository list` command. To learn more, see [Viewing List of Backup Repositories](#).
Viewing List of Service Providers

To view a list of service providers to which Veeam Agent is connected, use the following command:

```
veeamconfig cloud list
```

Veeam Agent will display the list service providers.

For the service provider in the list, Veeam Agent for Mac displays the following information:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the service provider.</td>
</tr>
<tr>
<td>ID</td>
<td>ID of the service provider in the Veeam Agent database.</td>
</tr>
<tr>
<td>Address</td>
<td>IP address of the cloud gateway and port over which Veeam Agent communicates with the cloud gateway.</td>
</tr>
<tr>
<td>Gate servers</td>
<td>IP address of the cloud gateway and port over which Veeam Agent communicates with the cloud gateway.</td>
</tr>
<tr>
<td>Username</td>
<td>Name of the tenant or subtenant account used for connection to the service provider.</td>
</tr>
</tbody>
</table>

For example:

```
user@wrk01:~$ veeamconfig cloud list
Name        ID                                      Address                Gate servers  Username
SP          {0840f770-354d-426a-b5ce-1aa80f56cc08}  172.17.53.15:6180       TechCompany
```
Editing Connection to Service Provider

You can edit the following parameters for a connection to a Veeam Cloud Connect service provider:

- Display name of the Veeam Cloud Connect service provider
- IP address and port used to connect to the cloud gateway
- Account to connect to the service provider
- Thumbprint to connect to the service provider

Changing SP Name

To change a name for the SP, use the following command:

```
veeamconfig cloud edit --name <new_sp_name> for --name <old_sp_name>
```

or

```
veeamconfig cloud edit --name <new_sp_name> for --id <sp_id>
```

where:

- `<old_sp_name>` — current name of the SP.
- `<new_sp_name>` — desired name for the SP.
- `<sp_id>` — ID of the SP.

For example:

```
user@wrk01:~$ veeamconfig cloud edit --name SP for --id 7d3022de-4f4d-4c70-85eb-e8a946a555cd
```

Changing IP Address and Port for Cloud Gateway

To change the IP address and port of the cloud gateway provided by the SP, use the following command:

```
veeamconfig cloud edit --address <sp_address> --port <sp_port> for --name <sp_name>
```

or

```
veeamconfig cloud edit --address <sp_address> --port <sp_port> for --id <sp_id>
```

where:

- `<sp_address>` — IP address or full DNS name of the cloud gateway that the SP or your backup administrator has provided to you.
- `<sp_port>` — port over which Veeam Agent must communicate with the cloud gateway. The default port used for communication with the cloud gateway is 6180.

- `<sp_name>` — name of the SP.

- `<sp_id>` — ID of the SP.

For example:

```
user@wrk01:~$ veeamconfig cloud edit --address 172.17.53.67 --port 6180 for --name SP
```

### Changing Account to Connect to SP

To change an account whose credentials will be used to connect to the SP, use the following command:

```
veeamconfig cloud edit --login <username> --password <password> for --name <sp_name>
```

or

```
veeamconfig cloud edit --login <username> --password <password> for --id <sp_id>
```

where:

- `<username>` — name of the tenant or subtenant account that the SP or your backup administrator has provided to you. The name of the subtenant account must be specified in the `TENANT/SUBTENANT` format.

- `<password>` — password of the tenant or subtenant account used to connect to the service provider.

- `<sp_name>` — name of the SP.

- `<sp_id>` — ID of the SP.

For example:

```
user@wrk01:~$ veeamconfig cloud edit --login ABC_Compan/User01 --password P@ssw0rd for --name SP
```
Changing Thumbprint to Connect to SP

To change a thumbprint that will be used to connect to the SP, use the following command:

```bash
veeamconfig cloud edit --fingerprint <sp_thumbprint> --login <username> --password <password> for --name <sp_name>
```

or

```bash
veeamconfig cloud edit --fingerprint <sp_thumbprint> --login <username> --password <password> for --id <sp_id>
```

where:
- `<sp_thumbprint>` — thumbprint used to verify the TLS certificate and connect to the service provider.
- `<username>` — name of the tenant or subtenant account that the SP or your backup administrator has provided to you. The name of the subtenant account must be specified in the TENANT/SUBTENANT format.
- `<password>` — password of the tenant or subtenant account used to connect to the service provider.
- `<sp_name>` — name of the SP.
- `<sp_id>` — ID of the SP.

For example:

```bash
user@wrk01:$ veeamconfig cloud edit --fingerprint 92FA988A3D9E80EE095DDAB75BF06B05DF6F205B --login ABC_Compan/User01 --password P@ssw0rd for --name SP
```
Updating List of Cloud Repositories

When you connect to the Veeam Cloud Connect service provider, Veeam Agent for Mac retrieves and saves to the database information about cloud repositories available to the tenant or subtenant whose account you use to connect to the SP. You can refresh information about available cloud repositories manually at any time. This may be useful, for example, after the SP changes backup resource settings for the tenant.

To update the list of cloud repositories, use the following command:

```bash
veeamconfig cloud resync
```

If the cloud repository currently used as a target location for Veeam Agent backups becomes unavailable, and Veeam Agent fails to reflect this change in its database for some reason, the `veeamconfig cloud resync` command may finish with errors. In this case, you can use the `--force` option to refresh information about available cloud repositories. For example:

```bash
veeamconfig cloud resync --force
```

With the `--force` option, Veeam Agent will retrieve the list of available cloud repositories from the service provider and save the new information about cloud repositories in the Veeam Agent database.

**TIP**

To view updated list of available cloud repositories after resync, use the `veeamconfig cloud list` command. To learn more, see Viewing List of Service Providers.
Deleting Connection to Service Provider

You can delete a connection to the service provider to which Veeam Agent for Mac is currently connected. When you delete a connection to a service provider, Veeam Agent removes the record on the deleted service provider from the database. Cloud repositories managed by the deleted service provider are removed from the list of available backup repositories. Backup files created by backup jobs targeted at these repositories remain intact on the cloud repository.

You cannot delete a connection to the service provider if a cloud repository managed by this service provider is used by a backup job. To remove such connection to a service provider, you first need to delete a reference to the cloud repository in the job settings.

To delete a connection to the service provider, use the following command:

```bash
veeamconfig cloud delete --name <sp_name>
```

or

```bash
veeamconfig cloud delete --id <sp_id>
```

where:

- `<sp_name>` — name of the service provider.
- `<sp_id>` — ID of the service provider.

For example:

```bash
user@wrk01:~$ veeamconfig cloud delete --name SP
```
Managing Veeam Backup & Replication Servers

You can store backup files created with Veeam Agent for Mac on backup repositories managed by Veeam Backup & Replication. To do this, you must connect to a Veeam backup server. After that, you can specify a Veeam backup repository as a target location for backup files in the properties of the backup job.
Connecting to Veeam Backup Server

To create Veeam Agent backups on a backup repository managed by Veeam Backup & Replication, you must connect to a Veeam backup server.

**IMPORTANT**
Currently, Veeam Agent for Mac can be connected to one Veeam Backup & Replication server only. If you want to create backups on the backup repository managed by another Veeam backup server, you need to delete currently used backup server and all jobs targeted at backup repositories managed by this backup server. To learn more, see Deleting Connection to Veeam Backup Server.

If you add a connection to another backup server, backup jobs targeted at the original backup server will fail, and backups created on the Veeam backup repository will become unavailable in Veeam Agent. To continue using the original backup server, you need to delete the connection to the new backup server and re-create all backup jobs that use the original backup server.

If you change an account to connect to the Veeam backup server and then start a backup job targeted at the backup repository managed by this backup server, Veeam Agent will start a new backup chain on the backup repository.

To connect Veeam Agent for Mac to a Veeam backup server, use the following command:

```
veeamconfig vbrserver add --name <vbr_name> --address <vbr_address> --port <vbr_port> --login <username> --domain <domain> --password <password>
```

where:

- `<vbr_name>` — name of the Veeam backup server that manages the backup repository.
- `<vbr_address>` — IP address of the Veeam backup server.
- `<vbr_port>` — port over which Veeam Agent must communicate with Veeam Backup & Replication. The default port used for communication with the Veeam backup server is 10006.
- `<username>` — a name of the account that has access to the Veeam backup repository.
- `<domain>` — a name of the domain in which the account that has access to the Veeam backup repository is registered.
- `<password>` — password of the account that has access to the Veeam backup repository. Permissions on the backup repository managed by the target Veeam backup server must be granted beforehand. To learn more, see Setting Up User Permissions on Backup Repositories.

For example:

```
user@wrk01:~$ veeamconfig vbrserver add --name vbr01 --address 172.17.53.1 --port 10006 --login veeam --domain tech --password P@ssw0rd
```

When Veeam Agent for Mac connects to a Veeam Backup & Replication server, Veeam Agent retrieves information about backup repositories managed by this Veeam backup server and displays them in the list of available backup repositories. You can then specify a Veeam backup repository as a target for a backup job.

To view the list of backup repositories, use the `veeamconfig repository list` command. To learn more, see Viewing List of Backup Repositories.
Viewing List of Veeam Backup Servers

To view a list of Veeam backup servers to which Veeam Agent for Mac is connected, use the following command:

```
veeamconfig vbrserver list
```

Veeam Agent will display the list of Veeam backup servers.

For the Veeam backup server in the list, Veeam Agent for Mac displays the following information:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the Veeam backup server.</td>
</tr>
<tr>
<td>ID</td>
<td>ID of the Veeam backup server in the Veeam Agent database.</td>
</tr>
<tr>
<td>Endpoint</td>
<td>IP address of the Veeam backup server and port over which Veeam Agent for Mac communicates with Veeam Backup &amp; Replication.</td>
</tr>
</tbody>
</table>

For example:

```
user@wrk01:~$ veeamconfig vbrserver list
Name        ID                                      Endpoint
vbr01       {0fc87c11-6a8d-48c1-8aeb-7f7655738796} 172.17.53.1:10006
```
Viewing Backup Server Details

You can view detailed information about the Veeam backup server to which Veeam Agent for Mac is connected. Use the following command:

```
veeamconfig vbrserver info --name <vbr_name>
```

or

```
veeamconfig vbrserver info --id <vbr_id>
```

where:

- `<vbr_name>` — name of the Veeam backup server.
- `<vbr_id>` — ID of the Veeam backup server in the Veeam Agent database.

Veeam Agent for Mac displays the following information about the Veeam backup server:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>ID of the Veeam backup server in the Veeam Agent database.</td>
</tr>
<tr>
<td>Name</td>
<td>Display name of the Veeam backup server.</td>
</tr>
<tr>
<td>Endpoint</td>
<td>IP address of the Veeam backup server and port over which Veeam Agent for Mac communicates with Veeam Backup &amp; Replication.</td>
</tr>
<tr>
<td>Login</td>
<td>Name of the account that has access to the Veeam backup repository.</td>
</tr>
<tr>
<td>Domain</td>
<td>Name of the domain in which the account that has access to the Veeam backup repository is registered.</td>
</tr>
</tbody>
</table>

For example:

```
user@wrk01:~$ veeamconfig vbrserver info --name vbr01
VBR server
  ID: {0fc87c11-6a8d-48c1-8aeb-7f7655738796}
  Name: vbr01
  Endpoint: 172.17.53.1:10006
  Login: veeam
  Domain: tech
```
Editing Connection to Veeam Backup Server

You can edit the following parameters for a connection to a Veeam backup server:

- Display name of the Veeam backup server
- IP address and port used to connect to the Veeam backup server
- Account to connect to the Veeam backup server

Changing Veeam Backup Server Name

To change a name for the Veeam backup server, use the following command:

```
veeamconfig vbrserver edit --name <new_vbr_name>
```

where:

- `<new_vbr_name>` — desired name for the backup server.

For example:

```
user@wrk01:$ veeamconfig vbrserver edit --name vbr01
```

Changing IP Address and Port for Veeam Backup Server

To change the IP address and port used to connect to the Veeam backup server, use the following command:

```
veeamconfig vbrserver edit --address <vbr_address> --port <vbr_port>
```

where:

- `<vbr_address>` — IP address of the Veeam backup server.
- `<vbr_port>` — port over which Veeam Agent for Mac must communicate with Veeam Backup & Replication.

For example:

```
user@wrk01:$ veeamconfig vbrserver edit --address 172.17.53.1 --port 10006
```

Changing Account to Connect to Veeam Backup Server

**NOTE**

If you change an account to connect to the Veeam backup server and then start a backup job targeted at the backup repository managed by this backup server, Veeam Agent will start a new backup chain on the backup repository.
To change an account whose credentials will be used to connect to the Veeam backup server, use the following command:

```bash
veeamconfig vbrserver edit --login <username> --domain <domain> --password <password>
```

where:

- `<username>` — name of the account that has access to the Veeam backup repository.
- `<domain>` — name of the domain in which the account that has access to the Veeam backup repository is registered.
- `<password>` — password of the account that has access to the Veeam backup repository.

For example:

```bash
user@wrk01:$ veeamconfig vbrserver edit --login veeam --domain tech --password P@ssw0rd2
```

### Changing Several Backup Server Parameters

You can change several parameters for the connection to the Veeam backup server simultaneously. For example, the following command changes the name and connection settings for the Veeam backup server:

```bash
user@wrk01:$ veeamconfig vbrserver edit --name vbr02 --address 172.17.53.2 --port 10006
```

### Updating List of Veeam Backup Repositories

When you connect to a Veeam backup server, Veeam Agent for Mac retrieves information about backup repositories managed by this Veeam backup server and displays them in the list of available backup repositories. You can refresh information about available Veeam backup repositories manually at any time. This may be useful, for example, after a new backup repository was added on the Veeam backup server.

To update the list of backup repositories managed by the Veeam backup server, use the following command:

```bash
veeamconfig vbrserver resync
```

**TIP**

To view updated list of available Veeam backup repositories after resync, use the `veeamconfig repository list` command. To learn more, see Viewing List of Backup Repositories.
Deleting Connection to Veeam Backup Server

You can delete a connection to the Veeam backup server to which Veeam Agent is currently connected. When you delete a connection to a Veeam backup server, Veeam Agent removes record on the deleted backup server from its database. Veeam backup repositories managed by the deleted backup server are removed from the list of available backup repositories. Backup files created by backup jobs targeted these repositories remain intact on the backup storage.

You cannot delete a connection to the Veeam backup server in the following situations:

- Veeam Agent operates in the managed mode. To delete connection to the Veeam backup server, reset Veeam Agent to the standalone mode. For details, see Resetting to Standalone Operation Mode.

- Veeam Agent has a backup job that saves backup files to a repository managed by this backup server. To remove such connection to the Veeam backup server, you first need to delete reference to the Veeam backup repository in the job settings.

To delete a connection to the Veeam backup server, use the following command:

```
veeamconfig vbrserver delete --name <vbr_name>
```

or

```
veeamconfig vbrserver delete --id <vbr_id>
```

where:

- `<vbr_name>` — name of the Veeam backup server.
- `<vbr_id>` — ID of the Veeam backup server.

For example:

```
user@wrk01:$ veeamconfig vbrserver delete --name vbr01
```
Managing Backup Repositories

A backup repository is a storage location where Veeam Agent for Mac keeps backup files. You can use the following types of disk-based storage as a target location for a backup job:

- Local (internal) storage of the protected machine (not recommended).
- Direct attached storage (DAS), such as USB, eSATA or Firewire external drives.
- Network Attached Storage (NAS) able to represent itself as SMB (CIFS) share.
- Veeam Backup & Replication 11 or later backup repository.
- Veeam Backup & Replication 11 or later cloud repository.
Creating Backup Repository

Veeam Agent for Mac creates backup files in a backup repository. When you create a backup policy in Veeam Backup & Replication or a backup job using command line interface of the Veeam Agent computer, you must specify a target location for the backup. Veeam Agent will create a backup repository in the specified location and save information about this repository in the database.

**IMPORTANT**

A backup repository must be created on a separate volume from a volume whose data you plan to back up.

If you want to create backups in local or network shared folder, you must create a repository. To learn more, see the following sections:

- Creating a repository in a local folder
- Creating a repository in an SMB network shared folder

If you want to create Veeam Agent backups in a Veeam backup repository of cloud repository, you do not need to create repositories. Before configuring the backup job, you need to connect to the Veeam backup server or Veeam Cloud Connect service provider. To learn more, see the following sections:

- Connecting to Veeam Backup Server
- Connecting to Service Provider

Creating Repository in Local Folder

To create a repository in a local folder, use the following command:

```bash
veeamconfig repository create --name <repository_name> --location <path_to_repository>
```

where:

- `<repository_name>` — name of the repository.
- `<path_to_repository>` — path to the folder in which backup files will be stored.

For example:

```
user@wrk01:~$ veeamconfig repository create --name VeeamBackup --location /home/backups
```
Creating Repository in SMB Share

To create a repository in an SMB share, use the following command:

```
veeamconfig repository create --name <repository_name> --type smb --location <path_to_repository>
-username <user_name> --password --domain <domain>
```

where:

- `<repository_name>` — name for the backup repository.
- `<path_to_repository>` — path to the network shared folder where backup files will be stored in the //SERVER/FOLDER format.
- `<user_name>` — account name that Veeam Agent will use to access the SMB network shared folder.
- `<domain>` — domain in which the account that has access permissions on the shared folder is registered.

Mind that if you specify `--password` parameter, Veeam Agent will prompt you to specify a password for the SMB network shared folder.

Examples

Command with `--username`, `--password`, `--domain` parameters:

```
user@wrk01:~$ veeamconfig repository create --name VeeamBackup --type smb --location //srv02/VeeamRepository --username Administrator --password --domain srv02
```

**TIP**

- If you mount a network shared folder to a folder in the Veeam Agent machine file system in advance, you can create the backup repository in the same way as in a local folder. For details, see Creating Repository in Local Folder.
- macOS may save CIFS/SMB credentials in a cache. As a result, if credentials have been changed, Veeam Agent for Mac uses obsolete credentials and fails to connect to shared folders. To refresh cached credentials, reboot the Veeam Agent computer.
Viewing List of Backup Repositories

To view backup repositories configured in Veeam Agent for Mac, use the following command:

```
veeamconfig repository list
```

Veeam Agent will display a list of backup repositories.

You can view the following information about backup repositories:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the backup repository.</td>
</tr>
<tr>
<td>ID</td>
<td>ID of the backup repository.</td>
</tr>
<tr>
<td>Location</td>
<td>Folder in the local file system specified as a target location for backup files.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of the backup repository. Possible values:</td>
</tr>
<tr>
<td></td>
<td>• Local</td>
</tr>
<tr>
<td></td>
<td>• Backup server</td>
</tr>
<tr>
<td>Backup server</td>
<td>Backup server on which Veeam backup repository added to Veeam Agent is configured.</td>
</tr>
</tbody>
</table>

For example:

```
user@wrk01:~$ veeamconfig repository list
Name          ID                                      Location        Type   Backup server
BackupVol01   {818e3a0f-8155-4a51-9430-248a203a43d1}  /home/backups   local
BackupVol02   {2155a2e7-a1e9-4347-9d8b-cf8f3a6f3fcb}  /home/backups2  local
```
Editing Backup Repository

You can edit settings for a backup repository created with Veeam Agent for Mac.

You can edit the following parameters for the backup repository:

- Name of the backup repository
- Location of the backup repository

**NOTE**

Consider the following:

- If you change location for the backup repository that is already used by a backup job and contains backup files, during the next backup job run, Veeam Agent will create a new backup chain in the new repository location.
- You can temporarily change backup repository location if you want to create an ad hoc full backup in addition to the backup chain created by the backup job in the original repository location.

Changing Backup Repository Name

To change a name for the backup repository, use the following command:

```
veeamconfig repository edit --name <new_name> for --name <old_name>
```

or

```
veeamconfig repository edit --name <new_name> for --id <id>
```

where:

- `<old_name>` — current name of the backup repository.
- `<new_name>` — desired name for the backup repository.
- `<id>` — ID of the backup repository.

For example:

```
user@wrk01:~$ veeamconfig repository edit --name LocalRepository for --name Repository_1
```

Changing Backup Repository Location

To change location for the backup repository, use the following command:

```
veeamconfig repository edit --location <path> for --name <name>
```

or
veeamconfig repository edit --location <path> for --id <id>

where:

- `<path>` — desired path for the backup repository.
- `<name>` — current name of the backup repository.
- `<id>` — ID of the backup repository.

For example:

```
user@wrk01:~$ veeamconfig repository edit --location /home/veeam for --id 3458797-3ffe-45bc-870e-c5628643bbb3
```

### Changing Backup Repository Name and Location

You can change a name and location for the backup repository at the same time, for example:

```
user@wrk01:~$ veeamconfig repository edit --name LocalRepository --location /home/veeam for --name Repository_1
```
Rescanning Veeam Backup Repository

If Veeam Agent for Mac fails to display backups stored in the Veeam Backup & Replication backup repository for some reason, you can rescan the Veeam backup repository. Veeam Agent will try to reconnect to the Veeam backup server and refresh the list of backups in the backup repository.

To rescan a Veeam backup repository, use the following command:

```
veeamconfig repository rescan --id <repository_id>
```

or

```
veeamconfig repository rescan --name <repository_name>
```

where:
- `<repository_id>` — ID of the backup repository that you want to rescan.
- `<repository_name>` — name of the backup repository that you want to rescan.

For example:

```
user@wrk01:~$ veeamconfig repository rescan --name [vbr01]BackupVol01
```

You can also rescan all Veeam backup repositories managed by the backup server to which Veeam Agent is connected with the following command:

```
veeamconfig repository rescan --all
```
Deleting Backup Repository

You can delete a backup repository configured with Veeam Agent for Mac. When you delete a backup repository, Veeam Agent removes record on the deleted repository from its database. Backup files created by a backup job targeted at the deleted backup repository remain intact on the backup storage.

To delete a backup repository, use the following command:

```
veeamconfig repository delete --id <repository_id>
```

or

```
veeamconfig repository delete --name <repository_name>
```

where:

- `<repository_id>` – ID of the backup repository that you want to delete.
- `<repository_name>` – name of the backup repository that you want to delete.

For example:

```
user@wrk01:~$ veeamconfig repository delete --name Repository_1
```

**NOTE**

You cannot delete a backup repository that is specified as a backup storage location in the backup job settings.
Performing Restore

If you experience a problem with your computer, your data gets lost or corrupted, you can use one of the following options to recover your data or bring the computer back to work:

- Restore user profiles
- Restore individual files and folders
- Restore data from encrypted backups
Restore Users

You can restore user profiles that contain data of all protected computer users.

When you restore user profiles, Veeam Agent restores the Home folders of all users that were set on the Veeam Agent computer at the moment of backup. If the computer, where you plan to restore, contains users with the same name as in the backup, these users will be overwritten.

**NOTE**

- Administrator can restore all user profiles that are available in the backup file, standard user can restore only one's user profile.
- Veeam Agent does not back up profiles of network users that do not have local accounts.
Before You Begin

Before you begin the restore process, check the following prerequisites:

- The backup from which you plan to restore data must be successfully created at least once.

- The backup from which you plan to restore data must created by a backup policy in the User data mode. To learn more, see Backup Mode.

- [For backups stored in network shared folders, on Veeam backup repositories and Veeam Cloud Connect repositories] You must have access to the target location where the backup file resides.

- [For Veeam backup repository targets] If you plan to restore data from a backup stored on a backup repository, you must have access permissions on this backup repository. To learn more, see Setting Up User Permissions on Backup Repositories.
Restoring User Profiles

To restore user profiles:

1. Start the Veeam Agent control panel with Launchpad. Veeam Agent will immediately display the File Level Restore wizard.

2. Select the backup in the left pane. Then select the restore point from which you want to recover data in the right pane.

3. Click Restore Users and confirm the restore in the window.

Veeam Agent will copy the content of the backup file to the Users folder in the computer file system and display a notification window with the corresponding message.
Restoring Files and Folders

If some files and folders on your computer get lost or corrupted, you can restore them from backups.

When you perform file-level restore, Veeam Agent publishes the backup content directly into the computer file system. You can browse to files and folders in the backup, restore files and folders to their initial location, copy files and folders to a new location or simply target applications to restored files and work with them as usual.
Before You Begin

Before you begin the restore process, check the following prerequisites:

- The backup from which you plan to restore data must be successfully created at least once.

- [For backups stored in network shared folders, on Veeam backup repositories and Veeam Cloud Connect repositories] You must have access to the target location where the backup file resides.

- [For Veeam backup repository targets] If you plan to restore data from a backup stored on a backup repository, you must have access permissions on this backup repository. To learn more, see Setting Up User Permissions on Backup Repositories.
Restoring Files and Folders

To restore individual files and folders:

1. Start the Veeam Agent control panel with Launchpad. Veeam Agent will immediately display the **File Level Restore** wizard.

2. Select the backup in the left pane. Then select the restore point from which you want to recover data in the right pane.

3. Click **Open Backup**.

4. In the **Finder** window, select file or folder that you want to restore and do one of the following operations:
   - Restore data to the original location and overwrite the original object.
   - Restore data to the original location but keep the original object too.
     - In this case, Veeam Agent adds the **Restored_** or **Restored_%timestamp%** prefix to the name of the restored version of the object. As a result, if you restore a hidden file, this file becomes visible.
   - Copy data to a new location.
Restoring Data from Encrypted Backups

When you restore data from an encrypted backup, Veeam Agent performs data decryption automatically in the background or requires you to specify a password.

- If encryption keys required to unlock the backup file are available in the Veeam Agent database, that is, if you encrypt and decrypt the backup file on the same Veeam Agent computer, you do not need to specify the password. Veeam Agent uses keys from the database to unlock the backup file. Data decryption is performed in the background, and data restore from the encrypted backup does not differ from that from an unencrypted one.

- If encryption keys are not available in the Veeam Agent database, you need to provide a password to unlock the encrypted file. The password must be the same as the password that was used to encrypt the backup file. If the password has changed once or several times, you need to specify the latest password. In Veeam Agent, you can use the latest password to restore data form all restore points in the backup chain, including restore points that were encrypted with an old password and restore points that were created before you have enabled the encryption option for the job.

Restoring Data from Encrypted Backups

To restore data from an encrypted backup using the Veeam Agent graphical user interface:

1. If you want to perform file-level restore from an encrypted backup that was created on another Veeam Agent computer, launch the Veeam Agent control panel with Launchpad.
2. Select the encrypted backup and restore point from which you want to restore data.
3. Veeam Agent will display the Encryption window. Enter the password for the backup file.

   In the Hint field of the Encryption window, Veeam Agent displays a hint for the password that was used to encrypt the backup file. Use the hint to recall the password.

   If you changed the password one or several times while the backup chain was created, you need to specify the latest password. In Veeam Agent, you can use the latest password to restore data form all restore points in the backup chain, including those restore points that were encrypted with an old password.

   If you enter correct password, Veeam Agent will decrypt the backup metadata. You will be able to continue the restore operation in a regular manner.
Reporting

Veeam Agent for Mac provides several ways to get information about performed operations with the Veeam Agent command line interface.

For every data transfer operation, for example data backup and restore, backup import and export, Veeam Agent starts a new session. You can monitor performance of sessions started by Veeam Agent in the following ways:

- In Veeam Backup & Replication.
- On Veeam Agent computer.
Reporting with Veeam Backup & Replication Console

Veeam Backup & Replication provides several ways to get information about backup policies and backups:

- You can view statistics for Veeam Agent backup policies configured in Veeam Backup & Replication.
- You can view summary information about backups created on the backup repository.
- You can generate reports with statistics data for performed backup policy sessions.
- You can set up Veeam Backup & Replication to send reports automatically by email.
Reporting with Veeam Agent Computer

Veeam Agent for Mac provides several ways to get information about performed backups:

- You can get information about Veeam Agent events using Mac Notification Center.
- Viewing the job session result using the command line interface.
- View the session status using the command line interface.
- View session logs using the command line interface.
Viewing Events with Mac Notification Center

Veeam Agent can inform you about its events using the Mac Notification Center. Once an event occurs, a message notifying about this event will appear on the desktop. This lets you view the notification without the need to open the Veeam Agent Control Panel and take the necessary actions immediately.

The notification closes automatically in a few seconds. To close the notification manually, click the message.

To disable desktop notifications:

1. In **System Preferences**, click the **Notifications** pane.
2. Select **Veeam Agent for Mac** in the list and disable the **Allow Notifications from Veeam Agent for Mac** option.
Viewing All Sessions

You can view detailed statistics on all backup job sessions performed by Veeam Agent for Mac. To view the list of job sessions, use the following command:

```
veeamconfig session list
```

Veeam Agent displays the following information all job sessions:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>ID of the session.</td>
</tr>
<tr>
<td>Job name</td>
<td>Name of the backup job that is parent to the session. Veeam Agent displays value for this parameter only for backup job sessions.</td>
</tr>
<tr>
<td>Job ID</td>
<td>ID of the backup job that is parent to the session. Veeam Agent displays value for this parameter only for backup job sessions.</td>
</tr>
<tr>
<td>State</td>
<td>Current status of the session.</td>
</tr>
<tr>
<td>Start time</td>
<td>Date and time of the session start.</td>
</tr>
<tr>
<td>End time</td>
<td>Date and time of the session completion. Veeam Agent displays value for this parameter only for completed sessions.</td>
</tr>
</tbody>
</table>

For example:

```
user@wrk001 ~ % veeamconfig session list

Daily Backup                 Backup  {404b6874-884c-4735-b19d-42b1d46e961d}  Success  2021-02-19 14:12  2021-02-19 14:12
Daily Backup                 Backup  {3968c2d4-9672-4049-aec0-f7cd63520828}  Success  2021-02-19 14:22  2021-02-19 14:22
Daily Backup                 Backup  {bc64e783-5703-48b9-8e5e-80b88a336f99}  Success  2021-02-19 14:32  2021-02-19 14:32
Daily Backup                 Backup  {49691302-74f3-4edc-891e-f95f55eba47f}  Failed   2021-02-19 14:42  2021-02-19 14:42
Mac Workstations             Backup  {51ba3622-dd83-4ef3-b381-175ad1181d1a}  Success  2021-02-19 22:05  2021-02-19 22:06
Mac Workstations             Backup  {42a01b26-de71-4a2f-9093-fc4a5361d73e}  Success  2021-02-19 22:07  2021-02-19 22:08
```
Viewing Session Information

You can view status of every session that was started by Veeam Agent for Mac. To view the session status, use the following command:

```
veeamconfig session info --id <session_id>
```

where:

`<session_id>` — ID of the session for which you want to check status.

Veeam Agent displays the following information about sessions:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>ID of the session.</td>
</tr>
<tr>
<td>Job name</td>
<td>Name of the backup job that is parent to the session. Veeam Agent displays value for this parameter only for backup job sessions.</td>
</tr>
<tr>
<td>Job ID</td>
<td>ID of the backup job that is parent to the session. Veeam Agent displays value for this parameter only for backup job sessions.</td>
</tr>
<tr>
<td>State</td>
<td>Current status of the session.</td>
</tr>
<tr>
<td>Start time</td>
<td>Date and time of the session start.</td>
</tr>
<tr>
<td>End time</td>
<td>Date and time of the session completion. Veeam Agent displays value for this parameter only for completed sessions.</td>
</tr>
</tbody>
</table>

The following example shows status information on the completed backup policy session:

```
user@wrk01:~$ veeamconfig session info --id 1592755d-3a2b-40a9-a036-5c81853b369e
Backup session
  ID: {1592755d-3a2b-40a9-a036-5c81853b369e}
  Job name: SystemBackup
  Job ID: {2495911e-58db-4452-b4d1-f53dfbc600e}
  State: Success
  Start time: 2016-11-11 14:37:21 UTC
  End time: 2016-11-11 14:40:02 UTC
```
Viewing Session Logs

You can monitor the backup and restore process by viewing the backup job session and restore session logs in the Veeam Agent command line interface.

To view Veeam Agent session log, use the following command:

```bash
veeamconfig session log --id <session_id>
```

where:

- `<session_id>` — ID of the backup job or restore session.

For example:

```
user@wrk001 ~ % veeamconfig session log --id ff19ce06-7c54-4b07-96b6-15014992c00c

2021-02-26 12:19:52 UTC [info] Job Daily Backup started at 2021-02-26 12:19:52 UTC
2021-02-26 12:19:56 UTC [info] Preparing to backup
2021-02-26 12:20:16 UTC [info] Waiting for backup infrastructure resources availability
2021-02-26 12:20:18 UTC [info] Creating volume snapshot
2021-02-26 12:20:53 UTC [info] Starting full backup to [backupserver001.tech.local] Default Backup Repository
2021-02-26 12:20:57 UTC [info] Backing up files /Users/commonuser, /Users/administrator
2021-02-26 12:21:23 UTC [info] Backing up summary.xml
2021-02-26 12:21:42 UTC [info] Releasing snapshot
2021-02-26 12:21:45 UTC [info] Processing finished at 2021-02-26 12:21:45 UTC
```
Managing Configuration Database

Veeam Agent configuration database includes Veeam Agent for Mac settings, backup job configurations, and statistics information. You can perform the following operations with the Veeam Agent configuration database:

- Exports the current Veeam Agent configuration database to the output XML file.
- Imports Veeam Agent configuration database from the input XML file.
Exporting Configuration Database

You can export the Veeam Agent configuration database to a configuration file in the XML format. This may be useful, for example, if you want to change Veeam Agent settings by editing a configuration file or copy the Veeam Agent configuration to another computer.

To export the Veeam Agent configuration database, use the following command:

```bash
veeamconfig config export --file <path>
```

where:

- `<path>` – path to a configuration file to which you want to import configuration.

For example:

```bash
user@wrk01:~$ veeamconfig config export --file veeam/config.xml
```

**NOTE**

A folder in which you want to save the configuration file must exist in the file system.
Importing Configuration Database

You import the Veeam Agent configuration from a file in the XML format to the configuration database. This may be useful, for example, if you have changed Veeam Agent for Mac settings by editing a configuration file or want to apply configuration of another instance of Veeam Agent to Veeam Agent installed on your computer.

To import the Veeam Agent configuration database, use the following command:

```
veeamconfig config import --file <path>
```

where:

`<path>` — path to a configuration file to which you want to import configuration.

For example:

```
user@srv01:~$ veeamconfig config import --file veeam/config.xml
```
Exporting Product Logs

Veeam Agent offers a simple and convenient way to collect product logs and export them to an archive file. This operation may be required if you want to report an issue and need to attach log files to the support case.

When you export logs, Veeam Agent collects its log files and configuration files, exports them to an archive file in the `tar.gz` format and saves this archive file to a folder on the Veeam Agent computer.

You can perform the export logs operation in one of the following ways:

- **With the Veeam Agent control panel** — in this case, Veeam Agent will save the log archive on the Veeam backup server.

- **With the command line interface** — in this case, Veeam Agent will save the log archive to the current working folder.
Exporting Logs with Control Panel

You can use the Veeam Agent control panel to collect and export product logs. When you export logs with the control panel, you can choose where Veeam Agent should save the resulting log archive.

To export logs:

1. Launch the Veeam Agent control panel with Launchpad.
2. In the upper-right corner of the menu bar, click the Veeam Agent icon.
3. Select Export Logs.

Veeam Agent saves logs to the following folder on the Veeam backup server:

```
C:\ProgramData\Veeam\Backup\Endpoint\Other\AgentLogs\<computer_name>
```

where `<computer_name>` is a name of the computer with Veeam Agent installed.

If Veeam Agent computer is not connected to the Veeam backup server, Veeam Agent exports logs to the folder that you specify in the Finder window.
Exporting Logs with Command Line Interface

You can use the Veeam Agent command line interface to collect and export product logs. To export logs, use the following command:

```bash
veeamconfig grablogs
```

Veeam Agent will collect logs, export them to an archive file with the name `veeam_logs_<date>_<time>.tar.gz`, and save the archive to the current working folder.

For example:

```bash
user@wrk01:~$ veeamconfig grablogs
Logs have been exported successfully.
```
Getting Support

If you have any questions or want to share your feedback about Veeam Agent, you can use one of the following options:

- You can search for the information on the necessary subject in the current Veeam Agent for Mac User Guide.

- You can visit Veeam R&D Forums and share your opinion or ask a question.

- If you use Veeam Agent with an active license installed, you can visit Veeam Customer Support Portal and submit a support case to the Veeam Customer Support Team.
Using with Veeam Backup & Replication

To get full functionality of Veeam Agent for Mac, you must use Veeam Agent together with Veeam Backup & Replication.

**IMPORTANT**

If you plan to use Veeam Agent for Mac 1.0 with Veeam Backup & Replication, you must install Veeam Backup & Replication 11a on the Veeam backup server. Veeam Agent for Mac 1.0 supports integration with Veeam Backup & Replication 11 or later as well.

Veeam Backup & Replication lets you perform a number of additional administrative actions for Veeam Agent for Mac:

- Set up user permissions on backup repositories
- Manage licenses and editions of Veeam Agents

To learn more about tasks performed with the Veeam Backup & Replication console, see the Veeam Agent Management Guide.
Setting Up User Permissions on Backup Repositories

To be able to store backups on a backup repository managed by a Veeam backup server, the user must have access permissions on this backup repository.

NOTE

If you plan to create backups on a Veeam backup repository with Veeam Agent backup jobs configured in Veeam Backup & Replication, you do not need to grant access permissions on the backup repository to users. In the Veeam Agent management scenario, to establish a connection between the backup server and protected computers, Veeam Backup & Replication uses a TLS certificate. To learn more, see the Configuring Security Settings section in the Veeam Agent Management Guide.

Access permissions are granted to security principals such as users and AD groups by the backup administrator working with Veeam Backup & Replication. Users with granted access permissions can target Veeam Agent backup jobs at this backup repository and perform restore from backups located on this backup repository.

Right after installation, access permissions on the default backup repository are set to Allow to everyone for testing and evaluation purposes. If necessary, you can change these settings.

After you create a new backup repository, access permissions on this repository are set to Deny to everyone. To allow users to store backups on the backup repository, you must grant users with access permissions to this repository.

To grant access permissions to a security principal:

1. In Veeam Backup & Replication, open the Backup Infrastructure view.
2. In the inventory pane, click one of the following nodes:
   - The Backup Repositories node — if you want to grant access permissions on a regular backup repository to Veeam Agent users.
   - The Scale-out Repositories node — if you want to grant access permissions on a scale-out backup repository to Veeam Agent users.
3. In the working area, select the necessary backup repository and click **Set Access Permissions** on the ribbon or right-click the backup repository and select **Access permissions**. If you do not see the **Set Access Permissions** button on the ribbon or the **Access permissions** command is not available in the shortcut menu, press and hold the Ctrl key, right-click the backup repository and select **Access permissions**.

4. In the **Access Permissions** window, specify to whom you want to grant access permissions on this backup repository:

   - **Allow to everyone** — select this option if you want all users to be able to store backups on this backup repository. Setting access permissions to *Everyone* is equal to granting access rights to the *Everyone* Microsoft Windows group (*Anonymous* users are excluded). Note, however, this scenario is recommended for demo environments only.

   - **Allow to the following accounts or groups only** — select this option if you want only specific users to be able to store backups on this backup repository. Click **Add** to add the necessary users and groups to the list.

5. If you want to encrypt Veeam Agent backup files stored on the backup repository, select the **Encrypt backups stored in this repository** check box and choose the necessary password from the field below. If you have not specified a password beforehand, click **Add** on the right or the **Manage passwords** link to add a new password. Veeam Backup & Replication will encrypt files on the backup repository side using its built-in encryption mechanism. To learn more, see the **Encryption Algorithms** section in the Veeam Backup & Replication User Guide.
Managing License

If you plan to use Veeam Agent for Mac with Veeam Backup & Replication, you must have a license installed in Veeam Backup & Replication. The license must have a total number of instances that is sufficient to protect macOS-based machines (workstations and servers) on which you plan to install Veeam Agent. The number of backup jobs configured in Veeam Agent does not consume the license. To learn more about instance licensing in Veeam Backup & Replication, see the Licensing section in the Veeam Backup & Replication User Guide.

After Veeam Agent for Mac connects to Veeam Backup & Replication, Veeam Agent automatically starts consuming the license. By default, Veeam Agent operates in the Workstation edition. You can switch Veeam Agent to the Server edition manually if needed.

If one or more Veeam Agents operating in the Free edition are already connected to the backup server, they will start consuming the license immediately after the license is installed in Veeam Backup & Replication. Veeam Agents that exceed the license limit will not be able to back up data to the Veeam backup repository.

Veeam Agent keeps information about the license in its database. Information about the license is valid for 32 days. If Veeam Agent for Mac does not connect to Veeam Backup & Replication during this period, Veeam Backup & Replication will revoke its license.
Managing Instance Consumption by Veeam Agents

By default, Veeam Backup & Replication allows Veeam Agents to connect to the Veeam backup server and consume instances in the license. If you do not want Veeam Agents to consume instances, you can restrict instance consumption. After instance consumption is restricted, Veeam Agents will not be able to back up data to a Veeam backup repository.

To restrict instance consumption by Veeam Agents:

1. In Veeam Backup & Replication, from the main menu, select License.
2. In the License Information window, click the Instances tab.
3. On the Instances tab, clear the Allow unlicensed agents to consume instances check box.
4. Click Close.
Assigning License to Veeam Agent

After Veeam Agent connects to Veeam Backup & Replication, Veeam Agent automatically starts consuming the license. If the license allows Veeam Agent to operate in both the Workstation and Server editions, Veeam Agent will operate in the Workstation edition.

You can also assign a license to Veeam Agent manually if needed. When you assign a license, you can select in which edition the licensed Veeam Agent will operate.

To assign a license:

1. In Veeam Backup & Replication, from the main menu, select **License**.
2. In the **License Information** window, select the **Instances** tab and click **Manage**.
3. In the **Licensed Instances** window, select the Veeam Agent to which you want to assign the license, click **Assign** and select the desired edition: **Workstation** or **Server**.
Viewing Licensed Agents and Revoking License

When Veeam Backup & Replication connects to the backup server, Veeam Backup & Replication applies a license to the Veeam Agent. You can view to which Veeam Agents the license is currently applied.

To view a list of licensed Veeam Agents:

1. In Veeam Backup & Replication, from the main menu, select License.
2. In the License Information window, select the Instances tab and click Manage.

In the list of licensed instances, Veeam Backup & Replication displays Veeam Agents that have established a connection with the backup server during a Veeam Agent backup job session.

Revoking License from Veeam Agents

You can revoke the license from some Veeam Agents and re-apply it to other protected workloads. License revoking can be helpful, for example, if you do not want to use some Veeam Agents with Veeam Backup & Replication anymore.

To revoke a license from the Veeam Agent:

1. In Veeam Backup & Replication, from the main menu, select License.
2. In the License Information window, select the Instances tab and click Manage.
3. In the Licensed Instances window, select the Veeam Agent from which you want to revoke the license and click Revoke. Veeam Backup & Replication will revoke the license from the Veeam Agent, and the license will be freed for other workloads protected with Veeam Backup & Replication.
The Veeam Agent from which you have revoked the license will become unable to connect to the Veeam backup server but will remain in the **Licensed Instances** list. To allow this Veeam Agent to create backups in the Veeam backup repository, select the Veeam Agent and click **Remove**. During the next backup job session, the Veeam Agent will connect to the Veeam backup server and start consuming the license.
Appendix A. Deploying Device Profile with MDM Solution

With the MDM solution, to connect Veeam Agent to Veeam backup server and include Veeam Agent computer in the protection group, you must deploy the configuration file as a device profile.

The configuration file is one of the Veeam Agent for Mac setup files that you must obtain from your System Administrator. To learn more about setup files, see the Deploying Veeam Agent for Mac section in the Veeam Agent Management Guide.

The example below can be used to install Veeam Agent for Mac with Microsoft Intune or SimpleMDM. If you use another MDM solution, instructions may differ. For details, refer to the documentation of your MDM solution.

In the example below, the following color coding is applied:

- **Yellow** parts can be replaced with any values of your choice. Mind that UUIDs must be in the UUID format.
- **Green** part must be copied from the configuration file.

Depending on the MDM solution that you use, select one of the following configuration files:

- a. `<protection_group_name>_escaped.xml`
- b. `<protection_group_name>.xml`

where `<protection_group_name>` is a name of the protection group for pre-installed Veeam Agents.

To learn more about Veeam Agent setup files, see the Deploying Veeam Agent for Mac section in the Veeam Agent Management Guide.

All other parts are not supposed to be edited.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple/DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
  <dict>
    <key>PayloadIdentifier</key>
    <string>com.veeam.Agent.managedsettings</string>
    <key>PayloadRemovalDisallowed</key>
    <false />
    <key>PayloadScope</key>
    <string>System</string>
    <key>PayloadType</key>
    <string>Configuration</string>
    <key>PayloadUUID</key>
    <string>fa4b7334-c696-000-87d0-0242ac130003</string>
    <key>PayloadOrganization</key>
    <string>Veeam</string>
    <key>PayloadVersion</key>
    <integer>1</integer>
    <key>PayloadDisplayName</key>
    <string>Veeam Agent for Mac Managed Settings</string>
    <key>PayloadContent</key>
    <array>
      <dict>
        <key>PayloadType</key>
        <string>com.veeam.Agent.managedsettings</string>
        <key>PayloadRemovalDisallowed</key>
        <false />
        <key>PayloadScope</key>
        <string>System</string>
        <key>PayloadType</key>
        <string>Configuration</string>
        <key>PayloadUUID</key>
        <string>fa4b7334-c696-000-87d0-0242ac130003</string>
        <key>PayloadOrganization</key>
        <string>Veeam</string>
        <key>PayloadVersion</key>
        <integer>1</integer>
        <key>PayloadDisplayName</key>
        <string>Veeam Agent for Mac Managed Settings</string>
        <key>PayloadContent</key>
        <array>
          <dict>
            <key>PayloadType</key>
          </dict>
        </array>
      </dict>
    </array>
  </dict>
</plist>
```
After the device profile is installed on the Veeam Agent computer, Veeam Agent will connect to Veeam backup server.

Mind that the connection between Veeam Backup & Replication and Veeam Agent is not persistent. Veeam Agent synchronizes with the backup server periodically. To synchronize Veeam Agent immediately, run the following command:

```
veeamconfig mode syncnow
```