



Veeam Agent for Mac

Version 2

User Guide

May, 2024

© 2024 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

CONTACTING VEEAM SOFTWARE	7
ABOUT THIS DOCUMENT	8
OVERVIEW	9
Solution Architecture	10
Standalone and Managed Operation Modes	11
Data Backup	13
File-Level Backup	14
How Backup Works	15
Backup Job	17
Backup Repository	19
Backup Chain	20
Data Compression	25
Data Encryption	27
Backup to Veeam Cloud Connect Repository	36
Backup to Object Storage	37
Data Restore	44
Integration with Veeam Backup & Replication	45
PLANNING AND PREPARATION	46
System Requirements	47
Permissions	50
Ports	52
INSTALLATION AND CONFIGURATION	56
Before You Begin	57
Installing Veeam Agent	58
Granting Full Disk Access	59
Upgrading Veeam Agent	60
Uninstalling Veeam Agent	61
Granting Permissions to Users	62
Installation and Configuration with MDM Solution	63
Installation and Configuration in Command Line Interface	64
Installing Veeam Agent	65
Accepting License Agreements	66
Importing Veeam Backup Server Settings	67
Granting Permissions to Users	68
Uninstalling Veeam Agent	69
Importing Configuration from Veeam Backup Server	70
Managing Veeam Agent Operation Mode	71

Viewing Operation Mode	72
Resetting to Standalone Operation Mode	73
Connecting to Veeam Backup & Replication	74
Synchronizing with Veeam Backup Server	76
Exporting Logs to Veeam Backup Server	77
LICENSING	79
Product Editions	80
Installing License	81
Selecting Product Edition	83
Revoking License	84
Managing License in Command Line Interface	85
Installing License	86
Viewing License Information	87
Removing License	88
GETTING STARTED	89
GETTING TO KNOW USER INTERFACE	90
Veeam Agent for Mac Control Panel	91
Veeam Agent for Mac Status Bar Menu	94
Command Line Interface	95
PERFORMING BACKUP	98
Creating Backup Jobs	99
Creating Backup Job with Backup Job Wizard	100
Creating Backup Job in Command Line Interface	136
Starting and Stopping Backup Jobs	161
Starting and Stopping Backup Jobs from Control Panel	162
Starting and Stopping Backup Jobs in Command Line Interface	168
Managing Backup Jobs	171
Managing Backup Jobs in Control Panel	172
Managing Backup Jobs in Command Line Interface	176
Managing Backup Repositories	184
Managing Backup Repositories in Control Panel	185
Managing Backup Repositories in Command Line Interface	186
Managing Veeam Backup Servers	197
Connecting to Veeam Backup Server	198
Viewing List of Veeam Backup Servers	200
Viewing Backup Server Details	201
Editing Connection to Veeam Backup Server	202
Updating List of Veeam Backup Repositories	204
Deleting Connection to Veeam Backup Server	205
Managing Service Providers	206

Connecting to Service Provider	207
Viewing List of Service Providers	208
Editing Connection to Service Provider	209
Updating List of Cloud Repositories	212
Deleting Connection to Service Provider	213
PERFORMING RESTORE	214
Importing Backups	215
Importing Backups with Import Wizard	216
Importing Backups in Command Line Interface	236
Managing Backups	238
Managing Backups in Control Panel	239
Managing Backups in Command Line Interface	241
Restoring Users Data	245
Before You Begin	246
Restoring User Profiles Data	247
Restoring Files and Folders	249
Before You Begin	250
Step 1. Select Restore Point	251
Step 2. Save Restored Files	252
Restoring Data from Encrypted Backups	254
REPORTING	255
Reporting in Veeam Agent Control Panel	256
Viewing Backup Job Statistics	257
Viewing Statistics and Logs of Backup Sessions	258
Viewing Events with Mac Notification Center	260
Reporting in Command Line Interface	261
Viewing Session Log	262
Viewing Session Information	263
Viewing All Sessions	264
MANAGING CONFIGURATION DATABASE	266
Exporting Configuration Database	267
Importing Configuration Database	268
EXPORTING PRODUCT LOGS	270
Exporting Logs with Control Panel and Status Bar Menu	271
Exporting Logs in Command Line Interface	272
GETTING SUPPORT	273
USING WITH VEEAM BACKUP & REPLICATION	274
Setting Up User Permissions on Backup Repositories	276
Managing License	279
Managing Instance Consumption by Veeam Agents	280

Assigning License to Veeam Agent	281
Viewing Licensed Veeam Agents and Revoking License	282
Performing Data Protection Tasks.....	284
Backing Up to Backup Repositories	285
Backing Up to Cloud Repositories	286
Performing Backup Copy for Veeam Agent Backups	288
Archiving Veeam Agent Backups to Tape	289
Restoring Data from Veeam Agent Backups.....	290
Restoring Files and Folders.....	291
Exporting Disks.....	292
Publishing Disks.....	301
Exporting Restore Point to Full Backup File	312
Performing Administration Tasks	313
Importing Veeam Agent Backups	314
Enabling and Disabling Veeam Agent Backup Jobs	316
Viewing Veeam Agent Backup Job Statistics	317
Deleting Veeam Agent Backup Jobs	318
Viewing Veeam Agent Backup Properties	319
Removing Veeam Agent Backups	320
Deleting Veeam Agent Backups from Disk	321
Configuring Global Settings	322
Assigning Roles to Users	323
APPENDIX A. DEPLOYING DEVICE PROFILE WITH MDM SOLUTION	324

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 version 2.

Intended Audience

The user guide is intended for anyone who wants to use Veeam Agent for Mac to protect their Mac 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 data or individual files and folders. Backups can be stored on a local hard drive, on an external hard drive, in a network shared folder, in an object storage repository, in a Veeam backup repository, or Veeam Cloud Connect repository.

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

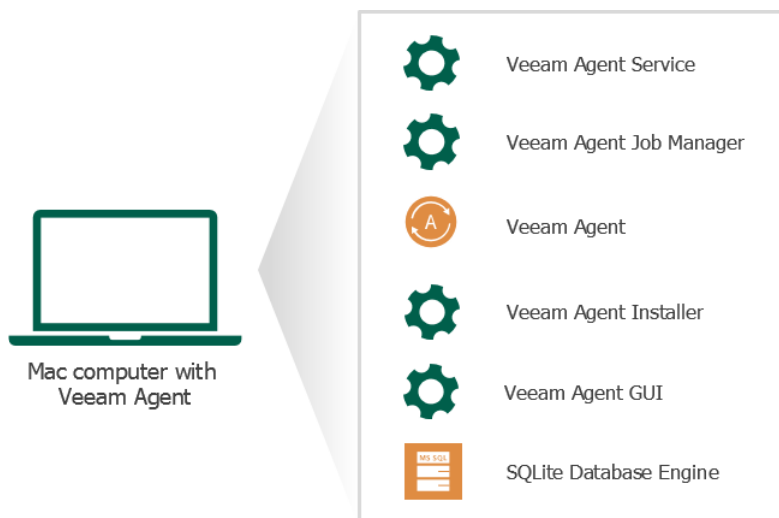
Veeam Agent for Mac integrates with Veeam Backup & Replication. Backup administrators who work with Veeam Backup & Replication can perform tasks with Veeam Agent backups: configure backup policies, manage backups created with backup policies, restore files and folders from backups.

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 *veeamservice* 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 control panel, status bar and tray menus, as well as **Backup Job** and **Import** wizards.
- 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.



Standalone and Managed Operation Modes

Veeam Agent can operate in two modes: *standalone mode* and *managed mode*. The current User Guide covers subjects related to Veeam Agent operating in the standalone mode only. Depending on the operation mode, Veeam Agent has different functionality and limitations.

Standalone Mode

In this mode, Veeam Agent operates as a standalone product. To use Veeam Agent operating in the standalone mode, you must manually install the product directly on the computer whose data you want to protect.

For Veeam Agent operating in the standalone mode, data protection, disaster recovery and administration tasks are performed by the user. You can also use Veeam Agent operating in the standalone mode with Veeam Backup & Replication. In this scenario, you can use backup repositories managed by Veeam Backup & Replication as a target location for Veeam Agent backups and use the Veeam Backup & Replication console to perform a number of tasks with Veeam Agent backup jobs and backups. To learn more, see [Integration with Veeam Backup & Replication](#).

You can also use Veeam Backup & Replication as a gateway for creating backups targeted at the following types of repositories:

- Veeam Cloud Connect repository. To learn more, see [Backup to Veeam Cloud Connect](#).
- Object storage repository.

With Veeam Agent operating in the standalone mode, you can also back up data directly to an object storage repository. To learn more about both options, see [Backup to Object Storage](#).

Managed Mode

In this mode, Veeam Agent operates under control from one of the following Veeam products:

- **Veeam Backup & Replication**

You can automate management of Veeam Agents on multiple computers in your infrastructure in the Veeam Backup & Replication console. You can configure Veeam Agent backup policies and perform other data protection and administration tasks on remote computers.

To manage Veeam Agent from Veeam Backup & Replication, you must create a protection group for pre-installed Veeam Agents and export Veeam Agent installation packages and configuration file. After that, you must install Veeam Agent and apply the configuration file on the computer whose data you want to protect. For more information on managed Veeam Agent deployment, see the [Deploying Veeam Agent for Mac](#) section in Veeam Agent Management User Guide.

For Veeam Agent managed by Veeam Backup & Replication, data protection, data restore and administration tasks are performed by a backup administrator in the Veeam Backup & Replication console. To learn about managing Veeam Agent in Veeam Backup & Replication, see the [Veeam Agent Management Guide](#).

- **Veeam Service Provider Console**

You can use Veeam Service Provider Console to manage Veeam Agents on multiple computers in your infrastructure. When Veeam Agent is managed by Veeam Service Provider Console, you can configure backup job settings, start and stop backup, change global settings, update and uninstall Veeam Agent and collect Veeam Agent data for monitoring and billing.

To manage Veeam Agent from Veeam Service Provider Console, you must install Veeam Service Provider Console management agent and Veeam Agent on the computer whose data you want to protect. After that, in Veeam Service Provider Console, you must activate Veeam Agent on the protected computer to set it into the managed operation mode.

For Veeam Agent managed by Veeam Service Provider Console, data protection, data restore and administration tasks are performed by a backup administrator in Veeam Service Provider Console.

Backup administrator can enable a read-only access mode for Veeam Agent installed on the protected computer. When you work directly with Veeam Agent operating in the read-only access mode, you can perform a limited set of operations, including:

- Running the backup job manually.
- Viewing backup session statistics.
- Restoring individual files.

To learn about deploying and managing Veeam Agent with Veeam Service Provider Console, see [Veeam Service Provider Console User Guides](#). Select the guide that suits your user role.

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 configure 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 data or individual folders and files.

If Veeam Agent operates in the Workstation or Server edition, you can set up Veeam Agent to create multiple backups – with individual backup scope, upon individual schedule or in different locations. 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
- Object storage repository

File-Level Backup

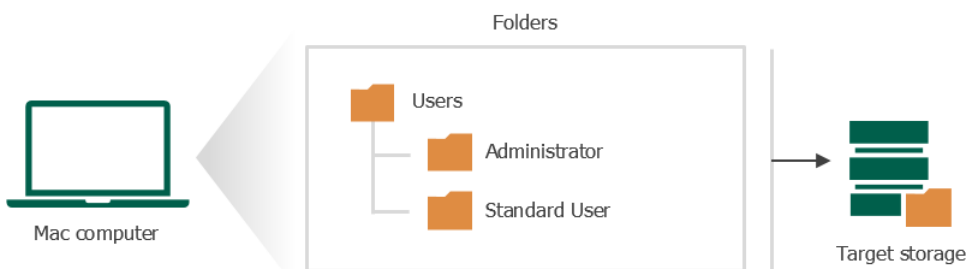
Veeam Agent for Mac copies backed-up data at the file level. The file-level backup captures data of individual folders and files on the machine. You can use the file-level backup to restore files and folders that you have added to the backup scope.

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

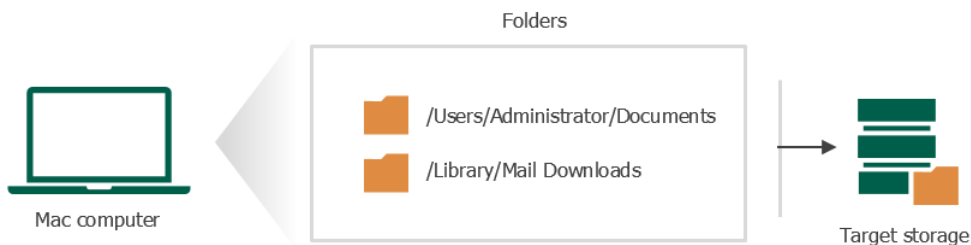
- When you back up user profiles data, Veeam Agent captures the content of the home folders of all users on your computer. When you recover from such backup, you will be able to restore all user profiles data or restore individual subfolders of home folders and files in these folders.

NOTE

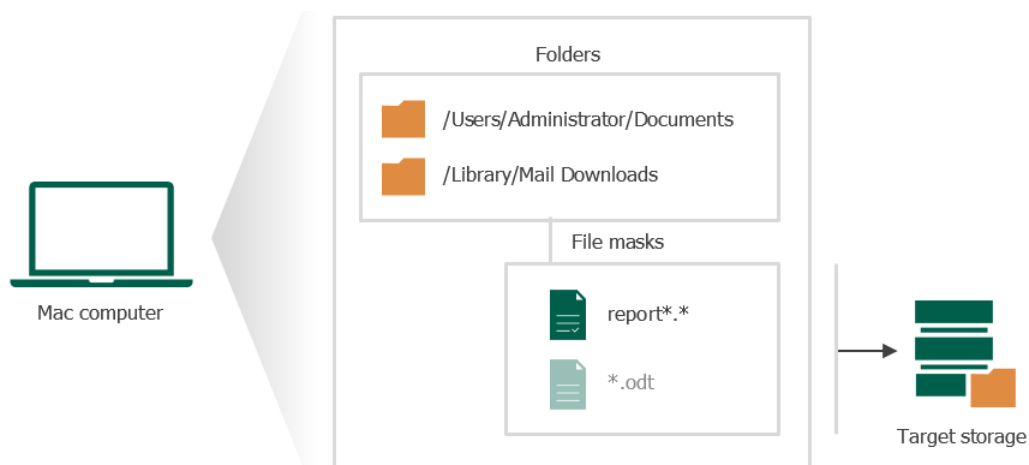
When you back up user profiles data, Veeam Agent does not include data from guest user account into the backup scope.



- 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 specify 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 criteria.



How Backup Works

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

1. When a new backup 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 an ext4 file system.
3. Veeam Agent checks the file system of the volume whose data you selected for backup. If data is located on the volume with an APFS file system, Veeam Agent commands macOS to create an APFS snapshot. Creating an APFS snapshot guarantees that the data on the volume is consistent and does not change during 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 is completed.

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.

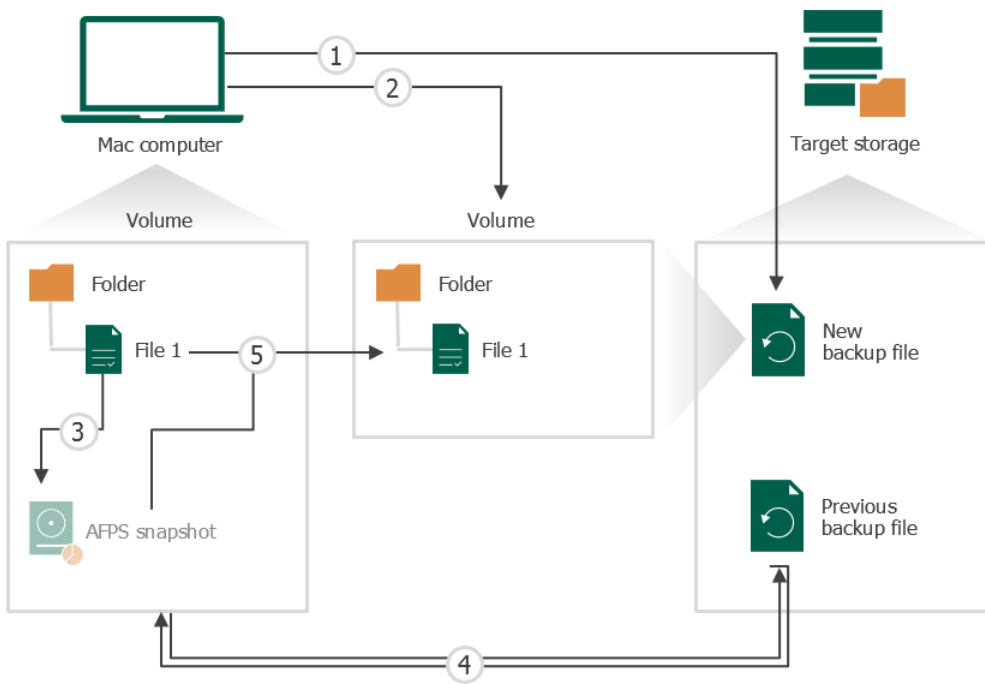
To learn about full and incremental backup, see [Backup Chain](#).

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.

NOTE

The connection between Veeam Agent and the repository may be interrupted when the data is being copied from the Veeam Agent computer to the target backup repository. If the backup job runs on a schedule, after the connection is restored Veeam Agent will retry the backup job. During retry, Veeam Agent will resume the process of data transfer to the backup repository from the point where it was interrupted. For details, see [Resume Backup](#).

6. 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 Job

To back up data of the protected Mac computer, you must configure a Veeam Agent backup job. The backup job settings define what data you want to back up, what the target location and retention policy for created backups are and how to back up your data. If necessary, you can reconfigure the backup job and change its settings at any time.

In Veeam Agent, you can configure multiple backup jobs with different settings. For example, you can configure backup jobs targeted at different backup locations to keep copies of your backed-up data. You can also fine-tune automatic backup creation process by defining an individual schedule for every 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](#).

Automatic Job Retries

If a backup job is launched according to a schedule and fails for any reason, Veeam Agent will automatically retry such backup job up to 3 times with an interval of 10 minutes. For example, Veeam Agent will launch a backup job retry if the backup repository is not available or connection to the repository is interrupted during backup.

NOTE

Starting from version 2.1, if you use the Server edition of Veeam Agent, you can modify the default settings for backup job retries in the backup job wizard. For more information, see [Scheduling Settings in Server Edition](#).

In case the backup job fails, Veeam Agent creates a new session for this backup job with the *Pending* status. The new session for the backup job retry will start in about 10 minutes.

Consider the following about automatic job retries:

- Veeam Agent will not perform a backup job retry if the backup job ended with the *Success* or *Warning* status.
- If a backup job fails because of an interrupted connection to the backup repository, Veeam Agent will retry the backup job and attempt to continue the data transfer that was started before the backup job failed from the point at which it was interrupted. For more information, see [Resume Backup](#).
- [For object storage repositories] Veeam Agent will launch a backup job retry if during the backup job session, a backup health check detects corrupted data in the backup. In case the backup job was run on a schedule, Veeam Agent will retry such backup job up to 3 times. Veeam Agent will retry the backup job only once if the backup job was launched manually. For more information, see [Health Check for Object Storage](#).

Resume Backup

If a backup job fails due to interrupted connection to the backup repository, Veeam Agent will perform a backup job retry. During retry, instead of restarting data transfer from the beginning, Veeam Agent will try to resume the backup process from the point where it was interrupted.

How Resume Backup Works

During the backup process, Veeam Agent flushes the data it copied from the source file system to the target storage at the default interval of 5 minutes. You can fine-tune the interval of the buffer cache flush in the Veeam Agent configuration file, but keep in mind that flushing buffer cache too often during data transfer may have a negative impact on the performance. For every file that is larger than 100 MB, Veeam Agent also creates a sync file that contains information on the amount of data copied from the file.

If the connection to the target repository is interrupted, after it is restored, Veeam Agent retries the backup job. Depending on the type of the source file system, Veeam Agent behaves differently:

- If the data to back up resides on a volume with an APFS file system, Veeam Agent will find the sync file for the file on which the backup process was interrupted. Veeam Agent will read the offset value from the sync file and will resume transferring data from the APFS snapshot to the target repository. After the file is fully copied to the target repository, Veeam Agent deletes its sync file.

NOTE

If for some reason, after the connection to the backup repository is restored, the APFS snapshot is no longer available, Veeam Agent will trigger the creation of a new snapshot. Then Veeam Agent will compare the modification times of the files in the new snapshot and on the target repository. In the backup repository, Veeam Agent will replace all files that have mismatching modification timestamps with their latest versions from the newly created snapshot.

- If the data to back up resides on a volume with any [supported file system](#) excluding APFS, Veeam Agent performs the backup of such data in the snapshot-less mode. In this case, after the connection to the repository is restored, Veeam Agent will compare the modification times of the files in the source file system and in the target repository. In the backup repository, Veeam Agent will replace all files that have mismatching modification timestamps with their latest versions from the source file system.

Limitations of Resume Backup

Consider the following limitations of Resume Backup:

- Resume Backup is initiated during a retry of a scheduled backup job only. If you start the backup job manually and Veeam Agent loses connection to the target repository during backup, after the connection is restored, Veeam Agent will remove the incomplete restore point and create a new restore point.
- Resume Backup is disabled for backups to local and directly attached storage repositories.

Backup Repository

A backup job configured in Veeam Agent creates backup files in a backup repository. A backup repository is a folder in the storage where you want to keep backup files. You can use the following types of 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
- Object storage repository, such as S3 Compatible storage, Amazon S3, Google Cloud or Microsoft Azure Blob
- Network Attached Storage (NAS) able to represent itself as SMB (CIFS) share
- [For Veeam Agent version 2.1] 12.1 or later backup repository (including deduplication appliances)
- [For Veeam Agent version 2.0] Veeam Backup & Replication 12.0 or later backup repository (including deduplication appliances)
- Veeam Cloud Connect 12.0 or later cloud repository

IMPORTANT

Consider the following about backup repositories:

- [For local storage] A backup repository should be created on a separate volume from a volume that contains data you plan to back up.
- [For Veeam backup repository] Backup repositories with enabled KMS encryption are not supported.

If you target a backup job at the network shared folder, every time the backup job starts, Veeam Agent will automatically mount the shared folder to the computer file system and create a backup file in the mount directory. After the backup job completes, Veeam Agent will automatically unmount the network shared folder.

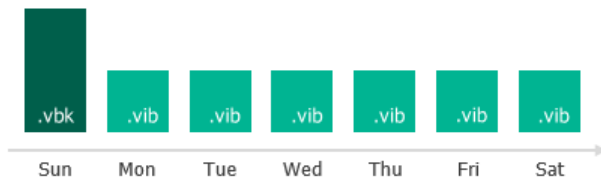
You can target several backup jobs to individual backup repositories or use the same target repository for several backup jobs. This may be useful if you want to back up different types of data to separate locations or to keep all backed-up data at one place.

Veeam Agent for Mac works with backup storage differently depending on the way you configure and start backup jobs – with the Veeam Agent control panel or command line interface. For details, see [Managing Backup Repositories](#).

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.

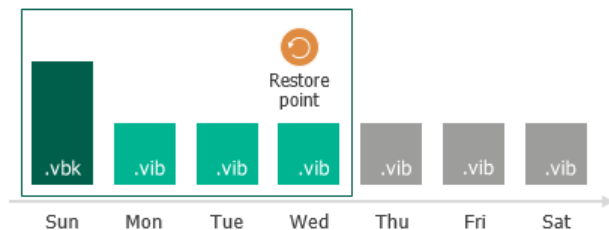
- During the first backup job session, Veeam Agent performs full backup. It copies all data that you have chosen to back up (entire volumes and folders) and stores the resulting full backup file (VBK) in the target location. The full backup takes significant time to complete and produces a large backup 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, we recommend that you do not delete separate backup files manually. To learn more, see [Deleting Backups](#).

Required backup files



Types of Backup Files

Veeam Agent 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 and volume-level restore operations.

Short-Term 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.

By default, Veeam Agent for Mac retains 7 latest restore points. You can define a different number in the backup job settings. During every backup job 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.

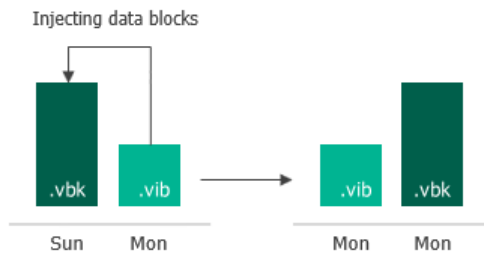
Removing Backups by Retention

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:

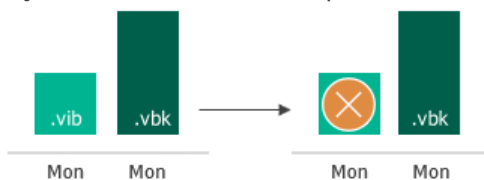
1. During every backup job session, Veeam Agent adds a backup file to the backup chain and checks if there is an obsolete restore point.



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.



Long-Term Retention Policy

Starting from version 2.1, you can configure long-term retention policy for backups.

The long-term or Grandfather-Father-Son (GFS) retention policy allows you to store backup files for long periods of time – for weeks, months and even years. For this purpose, Veeam Agent does not create any special new backup files – it uses backup files created while backup job runs and marks these backups with specific GFS flags.

To mark a backup file for long-term retention, Veeam Agent can assign to the file the following types of GFS flags: weekly (W), monthly (M) and yearly (Y). The types of GFS flags that Veeam Agent assigns depend on the configured [GFS retention policy settings](#).

NOTE

Consider the following:

- GFS flags can be assigned only to full backup files created during the time period specified in GFS policy settings.
- If you store your backups in an object storage repository managed by Veeam Backup & Replication and connection to this repository is set up through a gateway server, configuring active full backups is not required, Veeam Agent will create a full backup based on the last incremental backup and will assign a GFS flag to this full backup. If some data blocks required to create the full backup already reside in the object storage repository, the full backup will contain links to such data blocks. To avoid extra costs, Veeam Agent does not retrieve actual data blocks from the object storage repository.

If Veeam Agent assigns a GFS flag to a full backup file, this backup file can no longer be deleted or modified. Veeam Agent does not apply short-term retention policy settings to the full backup file. For example, Veeam Agent ignores the backup file when determining whether the number of allowed backup files is exceeded.

When the specified retention period ends, Veeam Agent unassigns the GFS flag from the full backup file. If the backup file does not have any other GFS flags assigned, it can be modified and deleted according to the short-term retention policy.

Veeam Agent assigns GFS flags in the similar way as Veeam Backup & Replication does for VM backup files. To learn about logic behind GFS flags, see the [Assignment of GFS Flags](#) and [Removal of GFS Flags](#) sections in the Veeam Backup & Replication User Guide.

Limitations

When planning to use GFS retention policy, consider the following limitations:

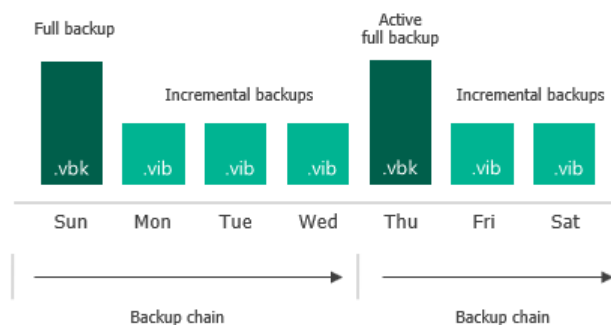
- [Applicable to all backup targets except object storage] While applying the GFS retention policy, Veeam Agent does not create new full backup files. You must configure your backup jobs in a way you do not lose any essential data due to an insufficient number of full backup files. For example, if you configure monthly GFS retention, you need at least one full backup file per month.
- If a GFS flag is assigned to a full backup file in an active backup chain, the following applies:
 - Veeam Agent cannot transform the backup chain according to the short-term retention policy.
 - Veeam Agent is not able to merge data from incremental backup files into the full backup file.
- Veeam Agent assigns GFS flags only after you save GFS retention policy settings. This means that GFS flags are assigned only to those backup files created after the configuration, while backup files created earlier are not affected and previously assigned flags are not modified.
- You cannot store full backups to which GFS flags are assigned in backup repositories with rotated drives.
- Retention policy for deleted items does not apply to full backup files to which GFS flags are assigned.

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 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 create active full backups manually or schedule a backup job to create active full backups periodically. To do this, you can use the Veeam Agent for Mac control panel or command line interface.

- To learn how to configure active full backup schedule and create active full backups in the Veeam Agent for Mac control panel, see [Backup Settings](#) and [Creating Active Full Backups from Control Panel](#).
- To learn how to configure active full backup schedule and create active full backups in the Veeam Agent for Mac command line interface, see [Configuring Active Full Backup Schedule](#) and [Creating Active Full Backups in Command Line Interface](#).

Active Full Backup Schedule

You can schedule a backup job to create active full backups periodically. Active full backup schedule depends on the regular backup schedule.

- In case active full backup is scheduled on a week day, Veeam Agent modifies the regular schedule of the backup job.

For example, the regular backup schedule is set to Monday and Tuesday at 15:00. Active full backup schedule is set to Friday. In this case, the backup job schedule will contain information that the job must start on Monday, Tuesday and Friday at 15:00.

- In case active full backup is scheduled on a day of the month, Veeam Agent runs the backup job on this day at the same time as it must run upon the regular schedule.

Keep in mind that if the job is not scheduled to run automatically, Veeam Agent will not run active full backup.

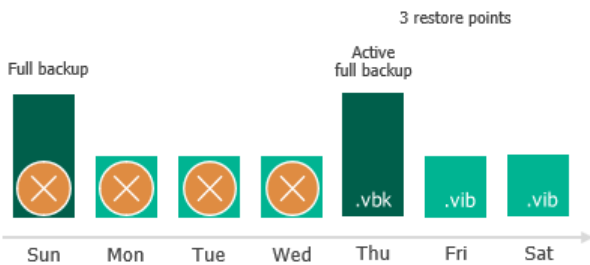
For information about how to configure job schedule, see [Define Backup Schedule](#) and [Configuring Backup Schedule](#).

Retention Job for Active Full Backups

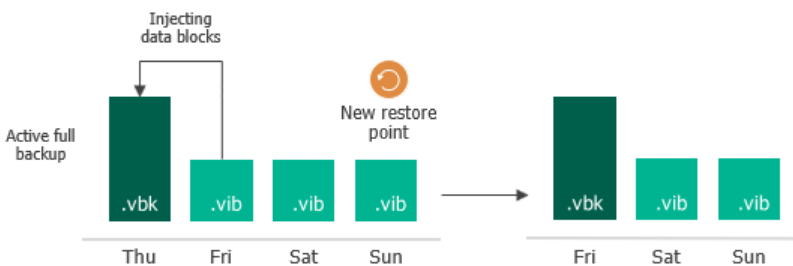
To be able to restore data from a Veeam Agent backup, you need to have a full backup file and a chain of subsequent incremental backup files on the disk. If you delete a full backup file, the whole chain of incremental backup files will become useless. In a similar manner, if you delete any incremental 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.



Data Compression

Veeam Agent provides mechanisms of data compression. Data compression lets you decrease traffic going over the network and disk space required for storing backup files.

Data Compression

Data compression decreases the size of created backups but affects duration of the backup procedure. Veeam Agent allows you to select one of the following compression levels:

Compression Level	CLI Option	Compression Algorithm	Description
None	0	No compression	This compression level is recommended if you plan to store backup files on storage devices that support hardware compression and deduplication.
Dedupe-friendly	1	Rle	Optimized compression level for very low CPU usage. You can select this compression level if you want to decrease the load on the CPU of the Veeam Agent computer.
Optimal	2	Lz4	The default recommended compression level. It provides the best ratio between size of the backup file and time of the backup procedure.
High	3	Zstd 3	Provides up to 60% additional compression ratio over the Optimal level at the cost of 2x higher CPU usage and 2x slower restore.
Extreme	4	Zstd 9	Provides the smallest size of the backup file but reduces the backup performance. We recommend that you use the extreme compression level only on Veeam Agent computers with modern multi-core CPUs (6 cores recommended).

You can change data compression settings for existing backup jobs. New settings will not have any effect on previously created backup files in the backup chain. They will be applied to new backup files created after the settings were changed.

Compression settings are changed on the fly. You do not need to create a new full backup to use new settings – Veeam Agent will automatically apply the new compression level to newly created backup files.

Storage Optimization

Depending on the type of storage you select as a backup target, Veeam Agent uses data blocks of different size, which optimizes the size of a backup file and job performance. You can choose one of the following storage optimization options:

- **4MB** – select this option for backup jobs that can produce very large full backup files (larger than 16 TB). With this option selected, Veeam Agent will use data block size of 4096 KB.
- **1MB** (default) – select this option for backup to SAN, DAS or local storage. With this option selected, Veeam Agent will use data block size of 1024 KB.

The SAN identifies larger blocks of data and therefore can process large amounts of data at a time. This option provides the fastest backup job performance.

- **512KB** – select this option for backup to NAS and onsite backup. With this option selected, Veeam Agent will use data block size of 512 KB. This option reduces the size of an incremental backup file because of reduced data block sizes.
- **256KB** – select this option if you plan to use WAN for offsite backup. With this option selected, Veeam Agent will use data block size of 256 KB. This results in the smallest size of backup files, allowing you to reduce the amount of traffic over WAN.

NOTE

If you change storage optimization settings, the new settings will be applied only after an active full backup is created. Veeam Agent will use the new block size for the active full backup and subsequent backup files in the backup chain. For more information on scheduling active full backups, see [Backup Settings](#).

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, encryption works at the backup job level. Veeam Agent uses the block cipher encryption algorithm and stores data in the encrypted format to a backup file.

Encryption is performed on the trusted side depending on the backup target:

- Encryption is performed on the source side for all backup targets except the Veeam backup repository.
- Encryption is performed on the target side if you store backups in the Veeam backup repository.

Decryption is performed on the same side as encryption.

To create encrypted backups, you must enable the encryption option and specify a password that will be used for data encryption. To learn more, see [Storage Settings](#).

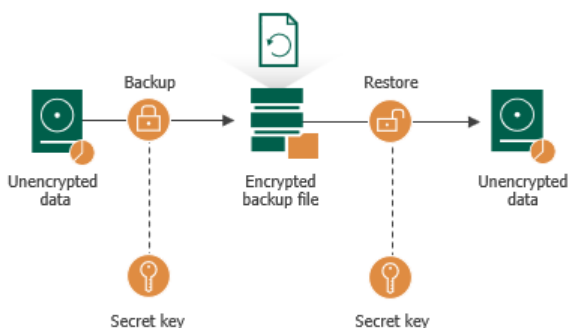
NOTE

You cannot enable encryption options in the properties of the Veeam Agent backup job if you have chosen to create Veeam Agent backups in a Veeam backup repository. For such jobs, encryption options are managed by a backup administrator working with Veeam Backup & Replication. To learn more about data encryption capabilities available in Veeam Backup & Replication, see the [Data Encryption](#) section in the Veeam Backup & Replication User Guide.

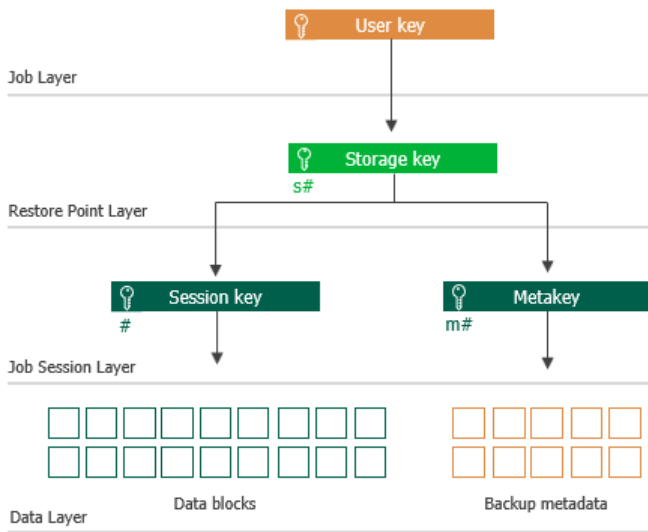
Encryption Algorithms

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 on the trusted side. 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 relies on a hierarchical encryption scheme. Each layer in the hierarchy encrypts the layer below with a key of specific type.

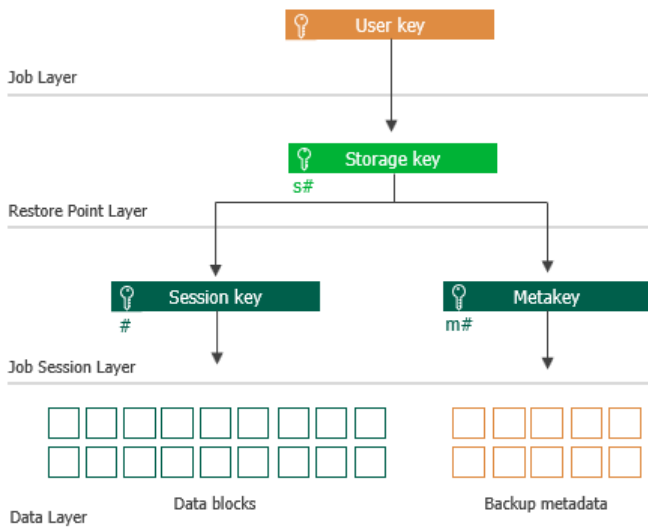


Encryption Keys

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](#).

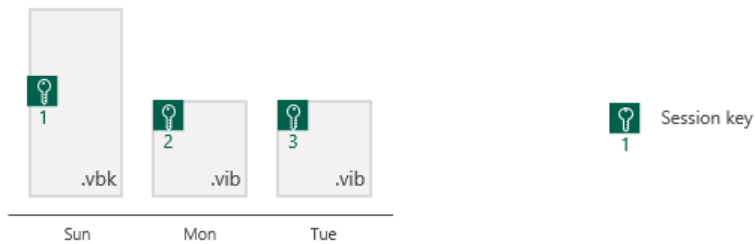


Session Keys and Metakeys

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.

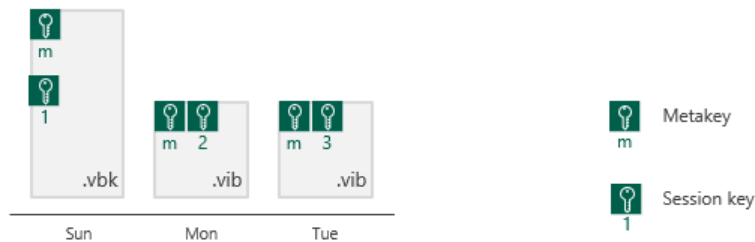
Veeam Agent generates a new session key for every backup job session. For example, if you have created an encrypted backup job and run 3 job sessions, Veeam Agent will produce 3 backup files that will be encrypted with 3 different session keys:

- 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.

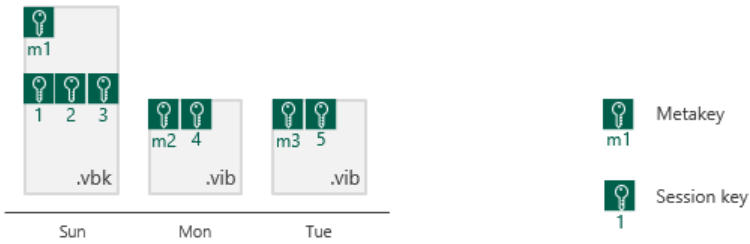


In the encryption process, session keys and metakeys are encrypted with keys of a higher layer – storage keys. Cryptograms of session keys and metakeys are stored in the resulting file next to encrypted data blocks. Metakeys are additionally kept in the Veeam Agent database.

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.

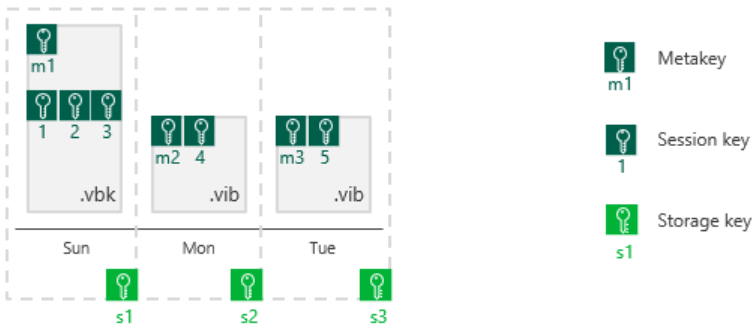
To restore data from such “composed” backup file, Veeam Agent would require a bunch of session keys. For example, if the backup chain contains restore points for 2 months, Veeam Agent would have to keep session keys for a 2-month period.



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.

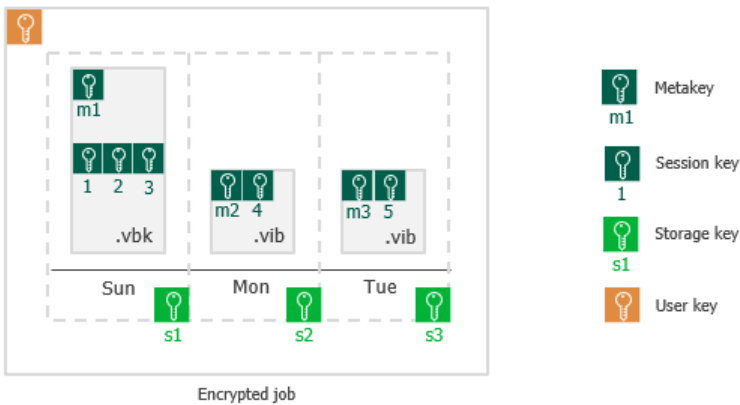
In the encryption process, storage keys are encrypted with a key of a higher layer – a user key. Cryptograms of storage keys are stored in the resulting file next to encrypted data blocks, and cryptograms of session keys and metakeys.

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 policy 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.

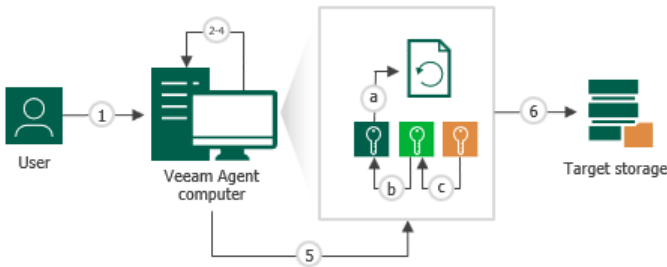
How Data Encryption Works

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

In Veeam Agent, 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 in its database.
4. Veeam Agent creates a session key and a metakey. The metakey is stored in 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 stored to the target location. The cryptograms of the user key, storage key, session key and metakey are stored in the resulting file next to encrypted data blocks.



 Session key

 Storage key

 User key

How Data Decryption Works

When you restore data from an encrypted backup file, Veeam Agent 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.

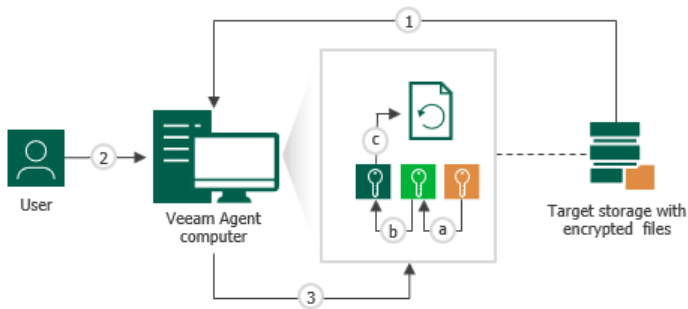
Data decryption is performed on the source or target side depending on the backup target. As a result, encryption keys are not passed to the untrusted side, which helps avoid data interception.




In Veeam Agent, 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.



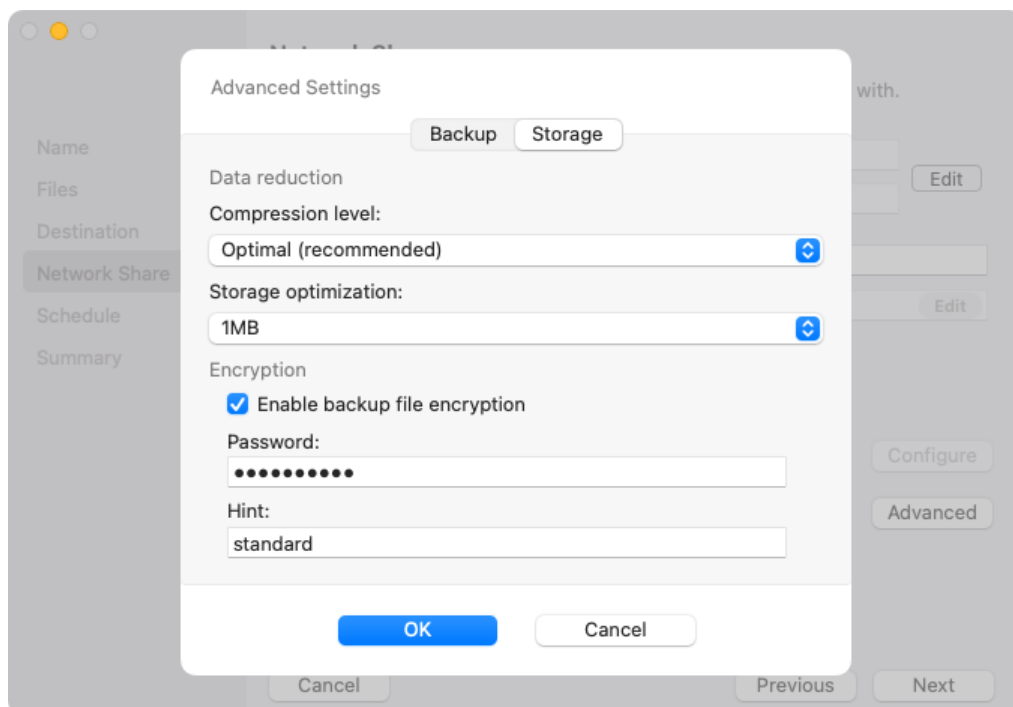
-  Session key
-  Storage key
-  User key

Backup Job 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.

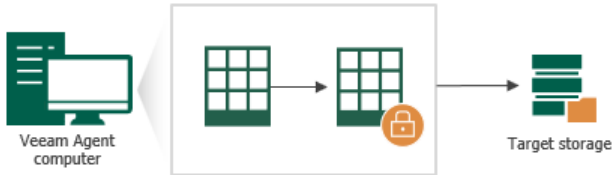
NOTE

You cannot specify encryption options for the backup job if you have chosen to save backup files on a Veeam backup repository. Encryption options for Veeam Agent backup jobs targeted at the backup repository are managed by a backup administrator working with Veeam Backup & Replication. To learn more, see the [Data Encryption](#) section of the Veeam Backup & Replication User Guide.



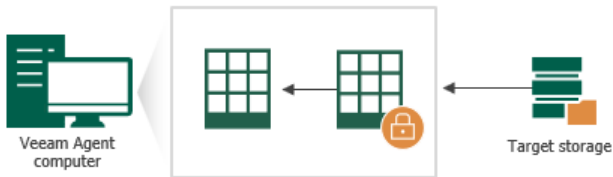
The backup job processing with encryption enabled includes the following steps:

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 in a resulting backup file.



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.



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 jobs 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 to Veeam Cloud Connect Repository

Targeting Backups at Veeam Cloud Repository in Standalone Mode

The current User Guide describes how you can target your backups at a Veeam Cloud Connect repository when Veeam Agent operates in the standalone mode. In the properties of a backup job, you must provide credentials of the tenant (or subtenant) account that you obtained from the service provider and select a cloud repository as a target for backup files. To learn more, see [Veeam Cloud Connect Settings](#).

NOTE

- You can use Veeam Agent for Mac2.1 to create backups in a Veeam Cloud Connect repository only if the backup server of the service provider runs Veeam Backup & Replication 12.0 or later.
- Backup to a Veeam Cloud Connect repository is available if Veeam Agent operates in the Workstation or Server edition.

Targeting Backups at Veeam Cloud Repository in Managed Mode

You can also target backups to a Veeam Cloud Connect repository when Veeam Agent operates in the managed mode.

If Veeam Agent is managed by Veeam Backup & Replication, see [Backup to Veeam Cloud Connect Repository](#) in the Veeam Agent Management Guide.

If Veeam Agent is managed by Veeam Service Provider Console, see [Choose Backup Destination](#) in the Veeam Service Provider Console Guide for Service Providers.

Backup to Object Storage

You can back up your Mac computer data to a cloud-based or on-premises object storage repository. You can configure the repository in the following types of object storage:

- Amazon S3
- Google Cloud Storage
- Microsoft Azure Blob Storage
- S3 compatible – on-premises (for example, MinIO) or cloud (including Wasabi Cloud and IBM Cloud)
- [For Veeam Agent 2.1.2] Veeam Data Cloud Vault added as a Veeam backup repository or Veeam Cloud Connect repository. To learn more, see [Backup Destinations](#).

Depending on your backup infrastructure, object storage can be available in different configurations. To learn more, see the following subsections:

- [Backup Destinations](#)
- [Types of Connection to Object Storage in Veeam Backup & Replication](#)
- [Considerations and Limitations](#)

Backup Destinations

You can back up Veeam Agent computer data to object storage in the following ways:

- Directly to object storage. In this case, Veeam Agent connects to an object storage account and creates a backup repository in this storage.

Keep in mind that to connect to object storage, you need to have an account with access permissions to read and write data.

To learn more, see [Object Storage Settings](#).

- To object storage added as a Veeam backup repository. In this case, Veeam Agent connects to the Veeam backup repository and Veeam Backup & Replication connects to object storage and creates a backup repository in this storage.

To learn more, see [Veeam Backup Server Settings](#).

- To object storage added as a Veeam Cloud Connect repository. In this case, Veeam Agent connects to the cloud backup repository and Veeam Backup & Replication connects to the object storage and creates a backup repository in this storage.

To learn more, see [Veeam Cloud Connect Settings](#).

Types of Connection to Object Storage in Veeam Backup & Replication

If you back up data to object storage added as a Veeam backup repository or Veeam Cloud Connect repository, you must configure a repository beforehand on the Veeam Backup & Replication side. Depending on the repository configuration, Veeam Backup & Replication provides one of the following connection types to the repository in the object storage:

- Connection through a gateway server. With this connection type, Veeam Agent connects to the repository using a proxy component – a gateway server that is assigned in the Veeam Backup & Replication console. The backup data is transferred from the Veeam Agent computer to the gateway server, then it is transferred from the gateway server to the repository.
- Direct connection. With this connection type, Veeam Agent connects directly to the repository. The backup data is transferred from the Veeam Agent computer to the repository without proxy components. The access to this repository is managed by Application Programming Interface (API) that is provided by the object storage provider.

Considerations and Limitations

Before you configure a backup job to store backups in an object storage repository, consider the following:

- Veeam Agent does not support direct backup to the Microsoft Azure Blob Storage under the general-purpose V1 storage account type.
- You can store backups only in those S3 compatible storage repositories that are accessible over the HTTPs protocol.
- If you want to back up your data directly to the S3 compatible storage, you must additionally specify access permissions settings for the storage. For direct access, enable the **Agents share credentials to object storage repository** or the **Provided by IAM/STS object storage capabilities** access control option. For more information, see the [Managing Permissions for S3 Compatible Object Storage](#) section in the Veeam Backup & Replication User Guide.
- Veeam Agent does not support backup to object storage for which lifecycle rules are enabled. Enabling lifecycle rules may result in backup and restore failures.

Health Check for Object Storage

If you keep backups of your Mac computer in an object storage repository, you can schedule regular health checks to validate integrity of the backups in the repository.

Consider the following about health check for object storage:

- Veeam Agent verifies metadata of the whole backup, not just the latest restore point.
- Veeam Agent does not read data from data blocks in the storage; Veeam Agent only lists data blocks to make sure all blocks in the storage are available for rebuilding every restore point in the active backup chain. This mechanism reduces the number of requests to the storage, which makes health check for object storage cost-efficient.

Configuring Health Check Schedule

If you want to run health checks for a backup that resides in an object storage repository, you must set a schedule according to which Veeam Agent will perform health checks. You can set the schedule [in the Backup Job wizard](#) or [in command line interface](#) to run health checks weekly or monthly on specific days.

When you configure a health check schedule, consider the following:

- Health check is run automatically during incremental backup job session on the days specified in the health check schedule. If the backup job runs several times on a specified day, health check is performed only with the first run of the backup job on that day.

Health check is not performed during the first full backup or subsequent active full backup job sessions.

- If Veeam Agent does not run any backup jobs on the day specified in the health check schedule, health check will be performed during the first backup job session following that day.

For example, you may have scheduled to run a health check every last day of a month, while the backup job is scheduled to run every day and to create an active full backup on Sundays. If the last day of a month falls on a Sunday, the health check will be performed on the following Monday with the first incremental backup job session on that day.

How Health Check Works

Veeam Agent performs a health check of a backup in the following way:

1. During the backup job session after a new incremental backup file is created, Veeam Agent starts the health check of the whole backup. Veeam Agent checks if the metadata of the backup is consistent, and no metadata is missing. Veeam Agent also checks if all data blocks for every restore point are available on the storage. Veeam Agent does not read data from data blocks.
2. If Veeam Agent does not find any corrupted data, the health check completes successfully. Otherwise, the health check completes with an error.

You can view the health check result in the session log. If during the health check, Veeam Agent finds corrupted data, it will also display information on where corrupt data has been detected – in backup metadata or data blocks, as well as list all restore points that share the corrupted data blocks.

Depending on the detected data inconsistency, Veeam Agent acts in one of the following ways:

- If the health check detects corrupted metadata, Veeam Agent will mark the backup chain as corrupted in the Veeam Agent configuration database; the backup job session will fail. During the next scheduled or manual backup job session, Veeam Agent will create a full backup and will start a new backup chain. The corrupted backup chain will become orphaned and will remain in the repository – you can keep or delete it.
- If the health check detects corrupted data blocks in the latest restore point of the active backup chain, Veeam Agent launches a health check retry.

During the health check retry, Veeam Agent will restart the backup job to create a new restore point. After that, Veeam Agent will transfer data blocks from the Veeam Agent computer to the backup repository. The transferred data blocks will include the blocks that were corrupted in the object storage repository and the blocks that changed since the start of the backup job session that triggered the health check. Veeam Agent will not perform another health check after the job retry is finished. The next health check will be run according to the defined schedule.

- If the health check detects corrupted data blocks in an inactive backup chain, Veeam Agent will not launch a health check retry. Veeam Agent will mark the backup and all related restore points as corrupted; the backup job session will end with a warning message.

NOTE

If you try to restore data from a corrupted backup, Veeam Agent will display a warning message informing you that the restore operation may fail or the restored data may be corrupted.

Backup Immutability

If you store your backup files in an object storage repository, Veeam Agent allows you to protect backup data from deletion or modification by making that data temporarily immutable. It is done for increased security: immutability protects data in your recent backups from loss as a result of attacks, malware activity or any other injurious actions.

IMPORTANT

Backup immutability uses native object storage capabilities. You may incur additional API and storage charges from the storage provider.

Supported Object Storage Types

Veeam Agent supports backup immutability for the following object storage types:

- Amazon S3
- S3 compatible storage that supports S3 Object Lock (including Wasabi)
- Microsoft Azure Blob Storage
- [For Veeam Agent 2.1.2] Veeam Data Cloud Vault

NOTE

Veeam Agent does not support backup immutability for the Google Cloud storage.

Before You Begin

Before you configure immutability for Veeam Agent backups, you must prepare the target storage account. Depending on the selected object storage type, perform the following actions:

- [S3 Compatible and Amazon S3 storage] When you create the S3 bucket, you must enable versioning and the S3 Object Lock feature for the bucket. For more information, see [AWS documentation](#).
- [S3 Compatible and Amazon S3 storage] After you create the S3 bucket with Object Lock enabled, make sure that the default retention is disabled to avoid unpredictable system behavior and data loss. To disable the default retention, edit the Object Lock retention settings as described in [AWS documentation](#).
- [Microsoft Azure Blob storage] You must enable blob versioning and version-level immutability support in the storage account. For more information, see [Microsoft documentation](#).

Consider the following about backup immutability:

- The effective immutability period consists of the user-defined immutability period and the block generation period automatically appended by Veeam Agent. For more information, see [How Backup Immutability Works](#) and [Block Generation](#).

- [S3 Compatible and Amazon S3 storage] Veeam Agent will use the *compliance* retention mode for each uploaded object. For more information on retention modes of S3 Object Lock, see [AWS documentation](#).
- [Microsoft Azure Blob storage] Do not enable immutability for already existing containers in the Microsoft Azure Portal. Otherwise, Veeam Agent will not be able to process these containers properly and it may result in data loss.

Configuring Backup Immutability

Depending on how you create the backup job and configure [connection to an object storage repository](#), you can define backup immutability settings in one of the following ways:

- [Backup Job wizard] You must specify the immutability period at the Bucket step of the wizard. For more information, see [Object Storage Settings](#).
- [Command line interface] You must specify the immutability period in the advanced options of the command for creating the backup job. For more information, see [Creating Backup Job in CLI](#).

NOTE

If you want to create the backup job in command line interface, you must create the object storage repository first. For details, see [Creating Repository in Object Storage](#).

- If you create the backup job that is targeted at an object storage repository configured as a Veeam backup repository or Veeam Cloud Connect repository, the immutability period in the settings of the repository must be specified in Veeam Backup & Replication. For details, see the [Adding Object Storage Repositories](#) section in the Veeam Backup & Replication User Guide.

Backup Immutability and Retention Policy

Backup immutability operates with backup data and related metadata (checkpoints) on the object storage side. Retention policy operates with logical representation of the stored data, or restore points, on the Veeam Agent side. These two mechanisms act independently from each other.

Veeam Agent will remove the irrelevant restore points per the defined backup retention policy. If the data associated with the removed restore point is still immutable, such data will remain in the repository until expiration of the immutability period. After that it will be automatically removed from the storage.

Limitation of Backup Immutability

If you use Veeam Agent in the standalone mode, you can restore the immutable data that is associated with a restore point removed by retention policy only in Veeam Backup & Replication console. In Veeam Backup & Replication, you must perform the following actions:

1. Add the object storage repository that contains the necessary data to Veeam Backup & Replication. For more information, see the [Adding Object Storage Repositories](#) section in the Veeam Backup & Replication User Guide.
2. Roll back to the necessary checkpoint. For more information, see the [Immutability](#) section in the Veeam PowerShell Reference.
3. Remove the repository from the Veeam Backup & Replication infrastructure. For more information, see the [Removing Backup Repositories](#) section in the Veeam Backup & Replication User Guide.

After that, you will be able to use Veeam Agent to restore data from the object repository in a regular manner.

How Backup Immutability Works

After you specify the immutability period for a backup and run the backup job for the first time, Veeam Agent will append an additional period of 10 days to the specified immutability period. This additional period is called *block generation*. The resulting effective immutability period is the sum of the user-defined immutability period and the block generation period. All data blocks transferred to the target repository within the block generation period will have the same immutability expiration date. For example, data block *a* added on day 1 of the block generation period will have the same immutability expiration date as block *b* added on day 9. For more information, see [Block Generation](#).

During the effective immutability period, the following operations with backup data in the object storage repository will be prohibited:

- Manual removal of data from the backup repository.
- Removal of data by backup retention policy.
- Removal of data using any object storage provider tools.
- Removal of data by the technical support department of the object storage provider.

Extension of Effective Immutability Period

During each transfer of data to the object storage repository, Veeam Agent creates a new checkpoint file with metadata that describes the latest state of the backup in the storage. The immutable blocks of data from a previous checkpoint may be reused in the newly created checkpoint. Veeam Agent keeps reused, or dependent, blocks of data locked by continuously assigning them to new generations and extending their effective immutability period. This guarantees that the effective immutability period is no less than the immutability period defined by user.

During data transfer, the effective immutability period for the backup is set as follows:

- [For new data blocks in the checkpoint] Immutability is set anew. The user-defined immutability period is appended with a 10-day block generation period.
- [For data blocks reused from the previous checkpoint] Immutability is extended to the immutability expiration date set for the new blocks.
- [For data blocks that are not reused in the checkpoint] Immutability is not extended. Such data blocks will remain in the repository until their immutability period is over. After that Veeam Agent will automatically remove them from the repository.

Block Generation

When you specify an immutability period for the recent backups, Veeam Agent will automatically add 10 days to the immutability expiration date. This period is called *block generation*. The block generation period serves to reduce the number of requests to the object storage repository, which results in lower traffic and reduced storage costs. You do not have to configure it, the block generation period is applied automatically.

When the block generation period is appended to the user-defined immutability period, it means there is no need to extend the immutability period for old data blocks when adding new data blocks to the backup during that block generation period.

Consider this example. When you create a full backup to start a backup chain, all data blocks transferred to the object storage repository are new. For these new blocks of data, Veeam Agent will add the block generation period of 10 days to the specified immutability period. If the immutability period is set by user to the default period of 30 days, the effective immutability period with the added block generation period will become 40 days. The first full backup starts its generation that will last for 10 days. All new and reused data blocks within this block generation period will have the same immutability expiration date. For instance, a data block that was transferred to the target repository on day 9 will have the same immutability expiration date as a data block transferred on day 1. This mechanism guarantees that the effective immutability period for all the data blocks within a generation is no less than 30 days.

If a block generation period is over but data blocks from that generation are reused in the newly created checkpoint, their effective immutability period is automatically extended to ensure that the effective immutability period for all the data blocks in the new checkpoint is no less than the user-defined immutability period. For more information, see [How Backup Immutability Works](#).

Data Restore

Veeam Agent for Mac offers file-level restore to recover personal user data 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 items from the backup.

Integration with Veeam Backup & Replication

IMPORTANT

To use Veeam Agent for Mac 2.1 with Veeam Backup & Replication, you must install Veeam Backup & Replication 12.1 on the Veeam backup server.

To use Veeam Agent for Mac 2.0 with Veeam Backup & Replication, you must install Veeam Backup & Replication 12.0 or later on the Veeam backup server.

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 Veeam Agent to a Veeam backup server and select a Veeam Backup & Replication backup repository as a target location in the backup job settings.

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 jobs and sessions becomes available in the Veeam Backup & Replication console:

- The Veeam Agent for Mac backup job is displayed in the list of jobs in Veeam Backup & Replication.
- Backup files created with Veeam Agent for Mac are displayed in the list of backups, under the **Agents** node.
- Performed job 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: 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, export disks and export restore points of Veeam Agent backups to standalone full backup files.
- Perform administrative tasks: disable and delete Veeam Agent backup jobs, import and remove Veeam Agent backups, and so on.

Planning and Preparation

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

System Requirements

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

Specification	Requirement
Hardware	<p>The protected Mac computer must meet the following hardware requirements:</p> <ul style="list-style-type: none">• CPU: x64 or ARM Apple-branded hardware.• Memory: 2 GB RAM or more. Memory consumption varies depending on the total amount of backed-up data.• Disk Space: 450 MB free disk space for product installation.• Network: 10 Mbps or faster network connection to a backup target.
OS	<p>Veeam Agent supports the following macOS versions:</p> <ul style="list-style-type: none">• 14 Sonoma¹• 13 Ventura• 12 Monterey• 11 Big Sur• 10.15 Catalina• 10.14 Mojave• 10.13.6 High Sierra <p>¹ MacOS 14 Sonoma is supported starting from version 2.1.</p>

Specification	Requirement
File System	<p>Veeam Agent supports consistent data backup with snapshot for the APFS file system.</p> <p>The following file systems can be backed up in the snapshot-less mode:</p> <ul style="list-style-type: none"> • HFS+ • MS-DOS (FAT) • exFAT • NTFS • FAT32 • SMB <p>Consider the following:</p> <ul style="list-style-type: none"> • Software RAID is not supported. • Backup of files from a cloud storage mounted under the <code>/Users/<user_name>/Library/CloudStorage/</code> directory is not supported. <ul style="list-style-type: none"> • 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. <p>Keep in mind that characters that you can use in the file name may be encoded in 2 bytes or more.</p> <ul style="list-style-type: none"> • Sparse files are not supported. Veeam Agent backs up and restores sparse files as regular files. • [Starting from version 2.1.2] Veeam Agent for Mac automatically excludes from backup the files that have the following extended attribute: <code>com.apple.metadata:com_apple_backup_excludeItem</code>.

Backup Target

Backup can be performed to the following types of storage:

- On-premises or cloud-based object 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
- [For Veeam Agent version 2.1] Veeam Backup & Replication version 12.1 or later backup repository (including deduplication appliances)
- [For Veeam Agent version 2.0] Veeam Backup & Replication version 12.0 or later backup repository (including deduplication appliances)

- Veeam Cloud Connect 12.0 or later cloud repository

IMPORTANT

Consider the following about backup repositories:

- [For local storage] A backup repository should be created on a separate volume from a volume that contains data you plan to back up.
- [For Veeam backup repository] Backup repositories with enabled KMS encryption are not supported.

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 or IPv6 addresses.

Permissions

The following permissions must be granted to the user accounts on the protected computer.

Permissions for Backup to Object Storage

If you plan to back up data to object storage, make sure that the user account that you use to connect to the object storage has the required permissions. The list of required permissions differs depending on the selected object storage:

- [Amazon S3 or S3 compatible](#)
- [Google Cloud Storage](#)

Amazon S3 or S3 compatible

If you plan to back up data to the Amazon S3 or S3 compatible storage, make sure the user account that you plan to use has the following permissions:

Identity-based permission:

```
{
  "s3:ListAllMyBuckets"
}
```

Resource-based permissions:

```
{
  "s3:DeleteObject",
  "s3:GetBucketLocation",
  "s3:GetBucketObjectLockConfiguration",
  "s3:GetBucketVersioning",
  "s3:GetObject",
  "s3:ListBucket",
  "s3:PutObject"
}
```

TIP

For information about required permissions for Amazon S3 storage with immutability enabled, see the [Using Object Storage Repositories](#) section in the Veeam Backup & Replication User Guide.

Google Cloud Storage

If you plan to back up data to the Google Cloud storage, make sure the user account that you plan to use has the following permissions:

```
{  
  "storage.buckets.get",  
  "storage.buckets.list",  
  "storage.objects.create",  
  "storage.objects.delete",  
  "storage.objects.get",  
  "storage.objects.list"  
}
```

Ports

The following tables describe network ports that must be opened to enable communication between Veeam Agent operating in the standalone mode and other backup infrastructure components.

To learn about ports required to enable proper work of Veeam Agent for Mac managed by Veeam Backup & Replication, see the [Ports](#) section in the Veeam Agent Management Guide.

Communication between Veeam Agent Components

The following table describes network ports that must be opened to enable proper communication between Veeam Agent for Mac components.

From	To	Protocol	Port	Notes
Veeam Agent computer	Veeam backup server	TCP	10006	<p>Default port used for communication with the Veeam backup server.</p> <p>Data between the Veeam Agent computer and backup repositories is transferred directly, bypassing Veeam backup servers.</p>
	Shared folder SMB (CIFS) share	TCP UDP	137 to 139, 445	<p>Ports used as a transmission channel from the Veeam Agent for Mac computer to the target SMB (CIFS) share.</p> <p>Ports 137 to 139 are used by backup infrastructure components to communicate using NetBIOS.</p>
	Veeam Agent computer		TCP	10101
TCP			2500 to 3300	<p>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.</p> <p>Ports must be open for incoming and outgoing traffic. Established connections must be allowed.</p>

Communication with Veeam Backup & Replication Repositories

The following table describes network ports that must be opened to ensure proper communication with Veeam backup repositories.

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

Communication with Veeam Cloud Connect Repositories

The following table describes network ports that must be opened to ensure proper communication with Veeam Cloud Connect repositories.

From	To	Protocol	Port	Notes
Veeam Agent computer	Cloud gateway	TCP	6180	Port on the cloud gateway used to transport Veeam Agent backup 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.

Communication with Object Storage

The following table describes network ports that must be opened to ensure proper communication with object storage if you back up data to object storage directly or to object storage added as a Veeam backup repository with the direct connection mode. For more information about object storage connection modes, see [Types of Connection to Object Storage in Veeam Backup & Replication](#).

From	To	Protocol	Port	Notes
Veeam Agent Computer	Amazon S3 object storage	TCP	443	<p>Used to communicate with the Amazon S3 object storage through the following endpoints:</p> <ul style="list-style-type: none"> • *.amazonaws.com (for both <i>Global</i> and <i>Government</i> regions) • *.amazonaws.com.cn (for <i>China</i> region) <p>All AWS service endpoints are specified in the AWS documentation.</p>
			80	<p>Used to verify the certificate status through the following endpoints:</p> <ul style="list-style-type: none"> • *.amazontrust.com <p>Consider that certificate verification endpoints (CRL URLs and OCSP servers) are subject to change. The actual list of addresses can be found in the certificate itself.</p>
	Microsoft Azure object storage	TCP	443	<p>Used to communicate with the Microsoft Azure object storage through the following endpoints:</p> <ul style="list-style-type: none"> • xxx.blob.core.windows.net (for <i>Global</i> region) • xxx.blob.core.chinacloudapi.cn (for <i>China</i> region) • xxx.blob.core.usgovcloudapi.net (for <i>Government</i> region) <p>Consider that the <xxx> part of the address must be replaced with your actual storage account URL that can be found in the Azure management portal.</p>

From	To	Protocol	Port	Notes
			80	<p>Used to verify the certificate status through the following endpoints:</p> <ul style="list-style-type: none"> • <code>ocsp.digicert.com</code> • <code>ocsp.msocsp.com</code> <p>Consider that certificate verification endpoints (CRL URLs and OCSP servers) are subject to change. The actual list of addresses can be found in the certificate itself. For more details, see also Microsoft documentation.</p>
	Google Cloud storage	TCP	443	<p>Used to communicate with Google Cloud storage through the following endpoints:</p> <ul style="list-style-type: none"> • <code>storage.googleapis.com</code> <p>All cloud endpoints are specified in this Google article.</p>
			80	<p>Used to verify the certificate status through the following endpoints:</p> <ul style="list-style-type: none"> • <code>ocsp.pki.goog</code> • <code>pki.goog</code> • <code>crl.pki.goog</code> <p>Consider that certificate verification endpoints (CRL URLs and OCSP servers) are subject to change. The actual list of addresses can be found in the certificate itself.</p>
	IBM Cloud object storage	TCP	Depends on device configuration	Used to communicate with IBM Cloud object storage.
	S3 compatible object storage	TCP	Depends on device configuration	Used to communicate with S3 compatible object storage.

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).

Before You Begin

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

1. The computer on which you plan to install Veeam Agent must satisfy [system requirements](#) specified in this document.
2. To install the Veeam Agent package, you must use the Administrator account on the computer where you plan to install the product.

Installing Veeam Agent

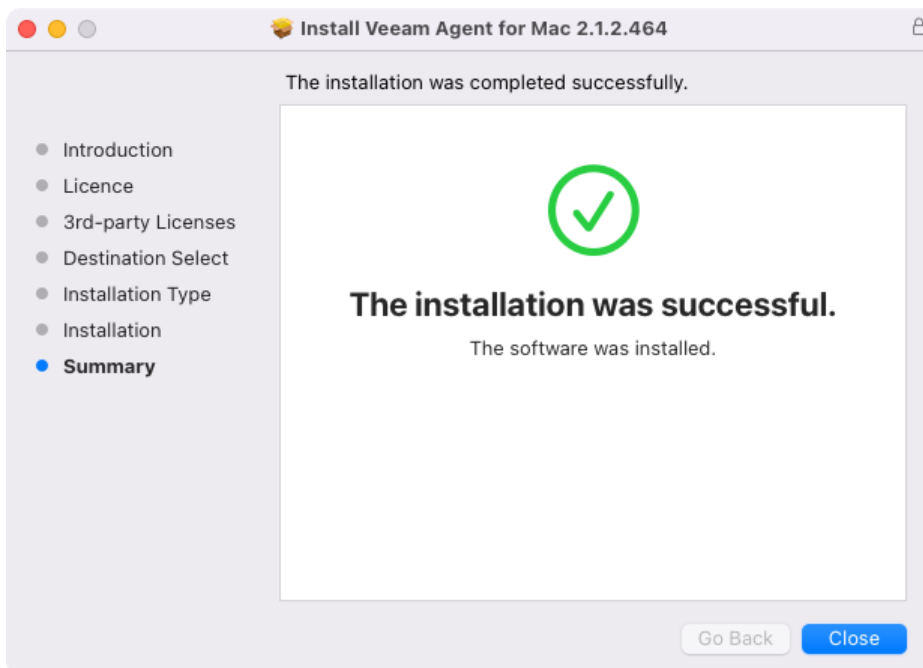
To install Veeam Agent for Mac with the **Installation** wizard:

1. Download the setup archive for standalone Veeam Agent for Mac from [this Veeam webpage](#) and save it on the computer where you plan to install the product.
2. Double-click the downloaded setup archive. In the open archive, double-click the .pkg setup file to launch the installation wizard.
3. 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.
4. [macOS 10.14 or later] 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 in [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 (version 10.13.6), 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](#).

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 the installation package for the newer version of Veeam Agent to the Mac computer where you plan to upgrade the product.
2. Double-click the package.
3. Click **OK** to accept an upgrade of Veeam Agent that is currently installed on the Mac computer.
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.

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 Bin.

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. With the MDM solution, you can connect Veeam Agent to Veeam backup server and include Veeam Agent computer in the protection group.

Veeam Agent for Mac provides setup files for the following MDM solutions:

- Jamf Pro
- 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:

- Application ID: *NX3JU8SRVL*
- Bundle ID: *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 Jamf Pro, 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 in 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:

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

where:

- o </path/package.pkg> – full path to the downloaded package on the computer.
- o <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:

```
user@wrk001 ~ % installer -pkg /Users/User/Desktop/Veeam?Agent?for?Mac-2.1  
.pkg -target /
```

3. After the installation process is complete, grant full disk access for Veeam Agent. To learn more, see [Granting Full Disk Access](#).

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 acceptthirdpartylicen  
ses
```

TIP

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

Importing Veeam Backup Server Settings

If you want to manage Veeam Agent for Mac with Veeam Backup & Replication, in Veeam Backup & Replication you can add your Mac computer to a protection group for pre-installed Veeam Agents. In this case, after you install Veeam Agent, you must import the configuration file generated by Veeam Backup & Replication. 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. 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
```

where <file_name> is a configuration file name.

Alternatively, you can specify the full path to the configuration file without navigating to the directory where you have saved this file – for example:

```
user@wrk001:~% veeamconfig mode setVBRsettings --cfg /Users/user/Mac\ Workstations\ Distributions\Mac\Mac\ Workstations.xml
```

Mind that the connection between Veeam backup server and Veeam Agent computer is not persistent. Veeam Agent synchronizes with Veeam Backup & Replication every 6 hours. To synchronize Veeam Agent immediately, run the following command from the Veeam Agent computer:

```
veeamconfig mode syncnow
```

Granting Permissions to Users

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

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

where:

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

For example:

```
user@wrk001 ~ % 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@wrk001 ~ % groups  
staff adm everyone dip plugdev lpadmin veeam
```

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@wrk001 ~ % sudo /Applications/Veeam/Veeam\ Agent\ for\ Mac.app/Contents/MacOS/veeaminstaller uninstall-agent --purge
```

Importing Configuration from Veeam Backup Server

If you want to manage Veeam Agent for Mac with Veeam Backup & Replication, you can add your Mac computer to a protection group for pre-installed Veeam Agents. In this case, after you install Veeam Agent, you must import the configuration file generated by Veeam Backup & Replication. 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.

You can import a configuration file generated by Veeam Backup & Replication in either of the following ways:

- [With Veeam Agent control panel.](#)
- [With Veeam Agent status bar menu.](#)
- [In command line interface.](#) For more information, see [Connecting to Veeam Backup & Replication.](#)
- With MDM solution. For more information, see [Installation and Configuration with MDM Solution.](#)

Importing Configuration with Control Panel

From the Veeam Agent application menu, select **Settings > Import Configuration**; in the **Finder**, select the configuration file to import.



Importing Configuration with Status Bar Menu

From the Veeam Agent status bar menu, select **Import > Configuration**; in the **Finder**, select the configuration file to import.



After importing the configuration using the control panel or status bar menu, Veeam Agent will automatically connect to the Veeam backup server.

Managing Veeam Agent Operation Mode

Veeam Agent for Mac can operate in different modes. Depending on the selected mode, Veeam Agent offers 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:

Parameter	Description
Owner	Name of the backup repository that manages Veeam Agent. If Veeam Agent operates in the standalone mode, Veeam Agent will display the <i>Not Set</i> value.
Mode	Current Veeam Agent operating mode. Possible values: <ul style="list-style-type: none">• <i>Not Set</i> – Veeam Agent operates in the standalone mode.• <i>Catch-All</i> – Veeam Agent operates in the managed mode. Veeam Agent computer is protected by a backup job managed by Veeam Agent for Mac. Veeam Agent computer is connected to the Veeam backup server as a 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: Catch-All
```

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 the [Standalone and Managed Operation Modes](#).

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

- Veeam Agent computer added to the protection group of pre-installed Veeam Agents 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 the protection group for pre-installed Veeam Agents, you must apply connection settings from the protection group configuration file to Veeam Agent. The configuration file is one of the Veeam Agent 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.

You can import the configuration file generated by Veeam Backup & Replication in either of the following ways:

- [Using Veeam Agent control panel.](#)
- [Using Veeam Agent status bar menu.](#)
- [In Veeam Agent Command Line Interface.](#)
- With MDM solution. For more information, see [Installation and Configuration with MDM Solution.](#)

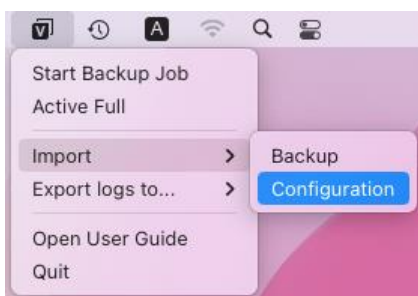
Importing Configuration Using Control Panel

From the Veeam Agent application menu, select **Settings > Import Configuration**; in the **Finder**, select the configuration file to import.



Importing Configuration Using Status Bar Menu

From the Veeam Agent status bar menu, select **Import > Configuration**; in the **Finder**, select the configuration file to import.



After importing the configuration using the control panel or status bar menu, Veeam Agent will automatically connect to the Veeam backup server.

Importing Configuration in Command Line Interface

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> – configuration file name. Alternatively, you can specify the full path to the configuration file with the `--cfg` option.
- `--force` – with this option enabled, Veeam Agent will override additional input prompts and error messages. This parameter is optional.

For example:

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

Synchronizing with Veeam Backup Server

When Veeam Agent is managed by Veeam backup server, the connection between Veeam backup server and Veeam Agent computer added to a protection group 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.

You can immediately synchronize Veeam Agent with backup server in the following ways:

- [Using Veeam Agent control panel.](#)

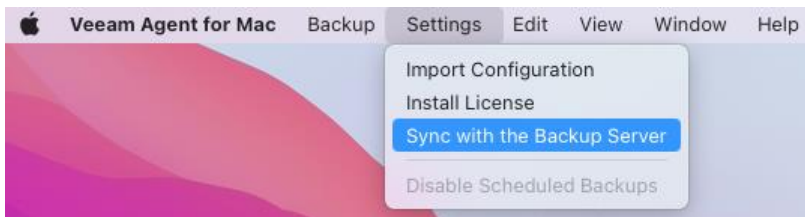
NOTE

Synchronizing with Veeam backup server using control panel is available starting from Veeam Agent version 2.1.2.

- [In Veeam Agent command line interface.](#)

Synchronizing Veeam Agent with Backup Server Using Control Panel

To synchronize immediately, from the Veeam Agent application menu, select **Settings > Sync with the Backup Server**.



Synchronizing Veeam Agent with Backup Server in Command Line Interface

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.

You can export product logs to Veeam backup server in the following ways:

- [Using Veeam Agent control panel.](#)
- [Using Veeam Agent status bar menu.](#)

NOTE

Exporting product logs to Veeam backup server using control panel or status bar menu is available starting from Veeam Agent version 2.1.2.

- [Using Veeam Agent command line interface.](#)

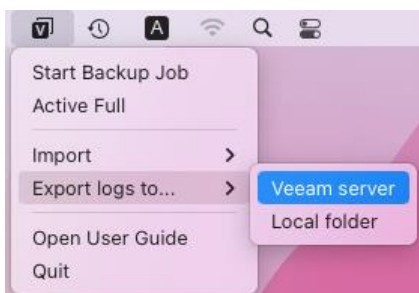
Exporting Logs Using Control Panel

To export logs, from the Veeam Agent application menu, select **Help > Export logs to > Veeam server.**



Exporting Logs Using Status Bar Menu

To export logs, from the Veeam Agent status bar menu, select **Help > Export logs to > Veeam server.**



Exporting Logs Using Command Line Interface

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_<agent>_<date>_<time>.tar.gz` and save the archive to 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

If Veeam Agent operates in the standalone mode, you can export product logs only to a local directory on the Veeam Agent computer. To learn more, see [Exporting Product Logs](#).

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.

Depending on the installation mode, you must accept these license agreements in the following ways:

- [Installation wizard] Confirm you accept these agreements at the respective steps of the Installation wizard.
- [Command line interface] Accept these agreements after the installation using a separate command. For details, see [Accepting License Agreements](#).

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 standalone mode, you can manage product licenses in the Veeam Agent control panel or in command line interface. To learn more, see the topics in this section.
- 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](#).

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.

NOTE

After the license expires, Veeam Agent for Mac automatically switches 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.

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 jobs that you can configure in Veeam Agent for Mac is limited to one.
2. You cannot use a Veeam Cloud Connect repository as a target location for backup files.
3. You cannot perform direct backup to an object storage repository.

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, object storage repository or Veeam backup repository plus unlimited number of backup jobs targeted at a Veeam Cloud Connect repository.

Installing License

Until you install a license, you can use the Free edition of the product. To switch to a commercial version of Veeam Agent for Mac, you need to obtain and install a license.

NOTE

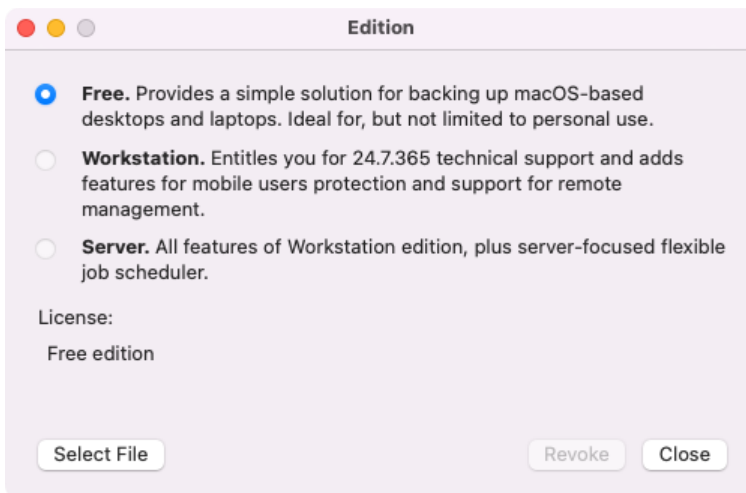
If you plan to use a Veeam backup repository as a target location for backups, you must install a license in Veeam Backup & Replication. The license must have enough instances to protect machines with Veeam Agents that back up data to the Veeam backup repository. To learn more, see [Managing License](#).

To install a license:

1. Launch Veeam Agent for Mac.
2. From the application main menu, select **Settings > Install License**.

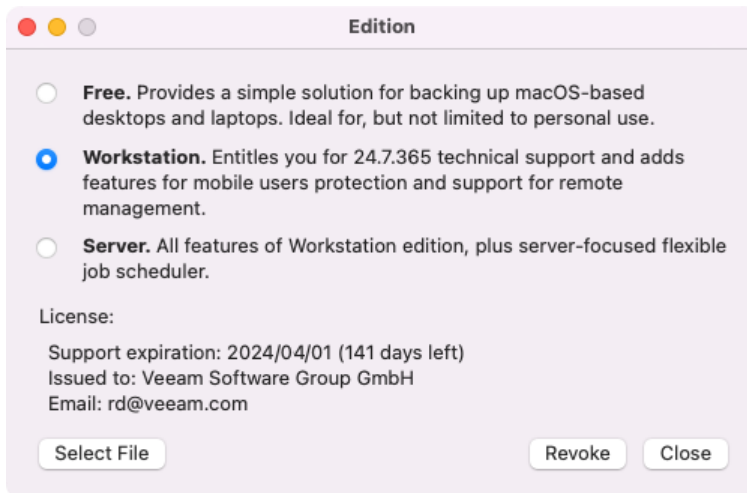


3. In the **Edition** window, click **Select File**:



4. In the **Finder** window, select the LIC file and click **Open**.

Veeam Agent will install the license and select the product edition that is allowed by the license. If a license supports both the Workstation and Server editions, Veeam Agent will select the Workstation edition.



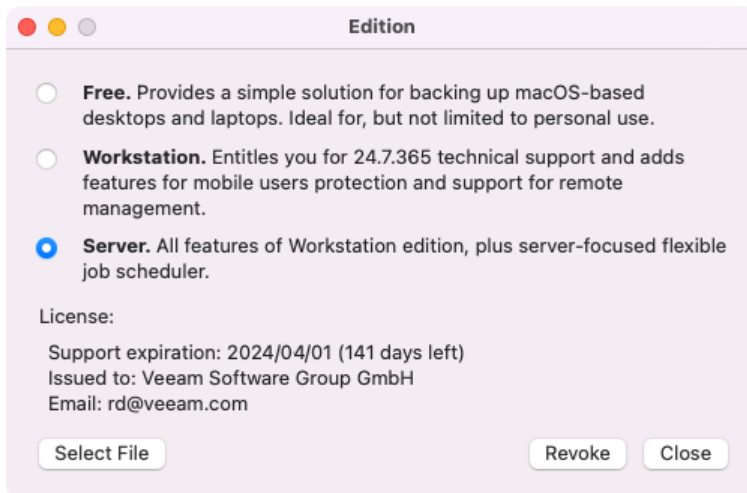
You can change the product edition manually if needed. To learn more, see [Selecting Product Edition](#)

Selecting Product Edition

When you install a license, Veeam Agent automatically selects the product edition that is allowed by the license. If a license supports both the Workstation and Server editions, Veeam Agent will select the Workstation edition.

You can change the product edition manually if needed. To select the product edition:

1. In the application menu, select **Settings > Install License**.
2. In the **Edition** window, select the product edition you need.



To learn more about editions of Veeam Agent for Mac, see [Product Editions](#).

NOTE

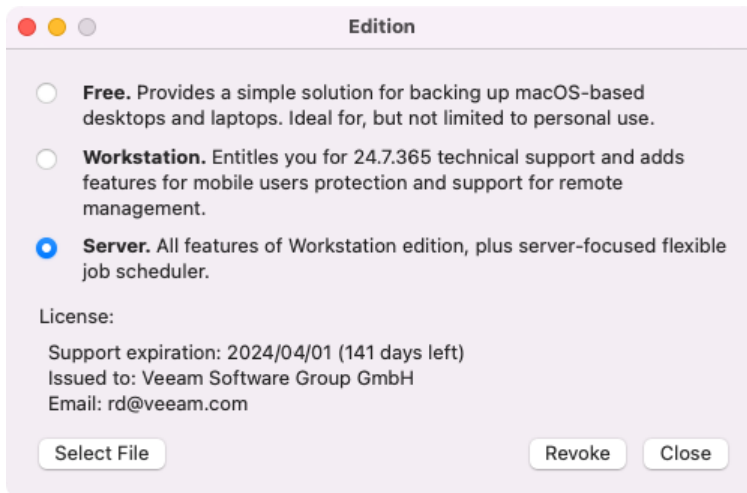
After you switch from the Server edition to the Workstation edition, or vice versa, Veeam Agent will disable the configured backup jobs. This operation is required because backup retention policies and available backup job options differ in Workstation and Server editions. To enable the job, you must edit the backup job settings in accordance with the selected edition.

Revoking License

You can revoke a license at any time if needed – for example, after the license is expired, and you want to continue using the Free edition of Veeam Agent for Mac.

To revoke a license:

1. From the Veeam Agent for Mac application menu, select **Settings > Install License**.
2. In the **Edition** window, click **Revoke**.



After you revoke the license, Veeam Agent for Mac will continue to operate in the Free edition. If Veeam Agent 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 in 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:

- [Install a commercial 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](#).

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: 2024/09/20 (311 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: Workstation
```

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 or Workstation edition and multiple backup jobs were configured, after switching to the Free edition, all backup jobs will be failing.

Getting Started

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

1. Define what data you want to back up and configure the backup job.

Before you configure the backup job, you should decide on the following backup details:

- Backup destination: where you want to store your backed-up data.
- Backup scope: user profiles data or specific folders and files.
- Backup schedule: how often you want to back up your data.

After that, you can configure one or several backup jobs. The backup job 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.

In Veeam Agent, you can configure the backup job in one of the following ways:

- [Using the Backup Job wizard](#)
- [Using command line interface](#)

2. Monitor backup job execution.

You can use the session log window in the Veeam Agent control panel to view how backup tasks are being performed, what errors have occurred during the backup job and other session statistics in real time. You can also use Veeam Agent command line interface to get information on backup and restore sessions status and view session logs. To learn more, see [Reporting](#).

3. 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 data.
- You can restore individual files and folders.

To learn more, see [Performing Restore](#).

Getting to Know User Interface

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

- [Veeam Agent Control Panel](#)
- [Veeam Agent Status Bar Menu](#)
- [Command line interface](#)

Veeam Agent for Mac Control Panel

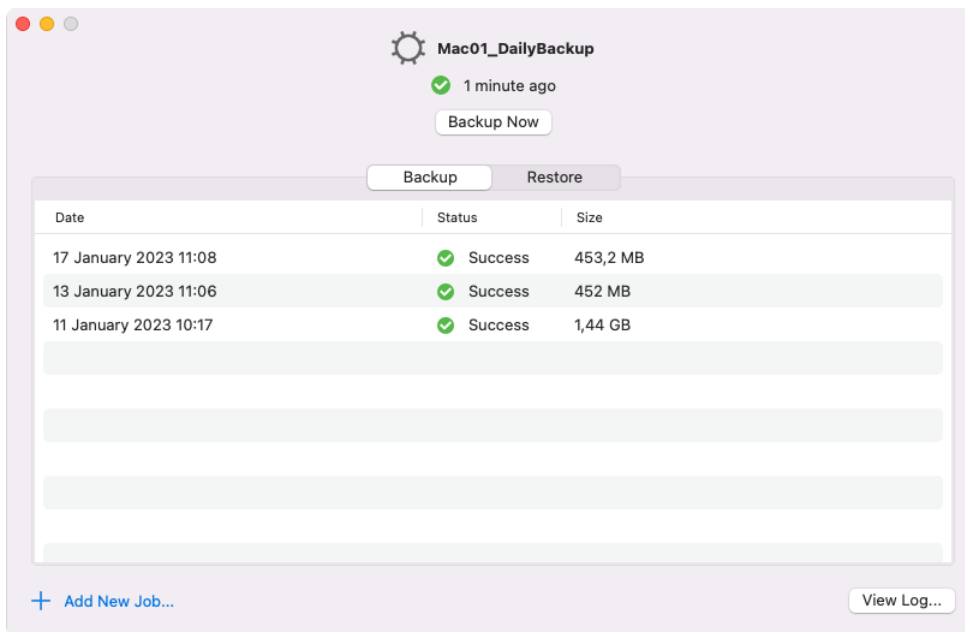
In the Veeam Agent Control Panel, you can perform the following operations:

- Add, edit, start and stop standalone backup jobs. For more information, see [Performing Backup](#).
- Monitor performance and status, as well as view logs of backup sessions. For more information, see [Reporting](#).
- View and browse available restore points, restore files, folders and user profiles data. For more information, see [Performing Restore](#).
- Import backups. For more information, see [Importing Backups](#).
- Manage product license and edition. For more information, see [Licensing](#).
- Temporarily suspend scheduled backups. For more information, see [Suspending Scheduled Backups](#).
- Import configuration from Veeam Backup & Replication. For more information, see [Importing Configuration from Veeam Backup Server](#).

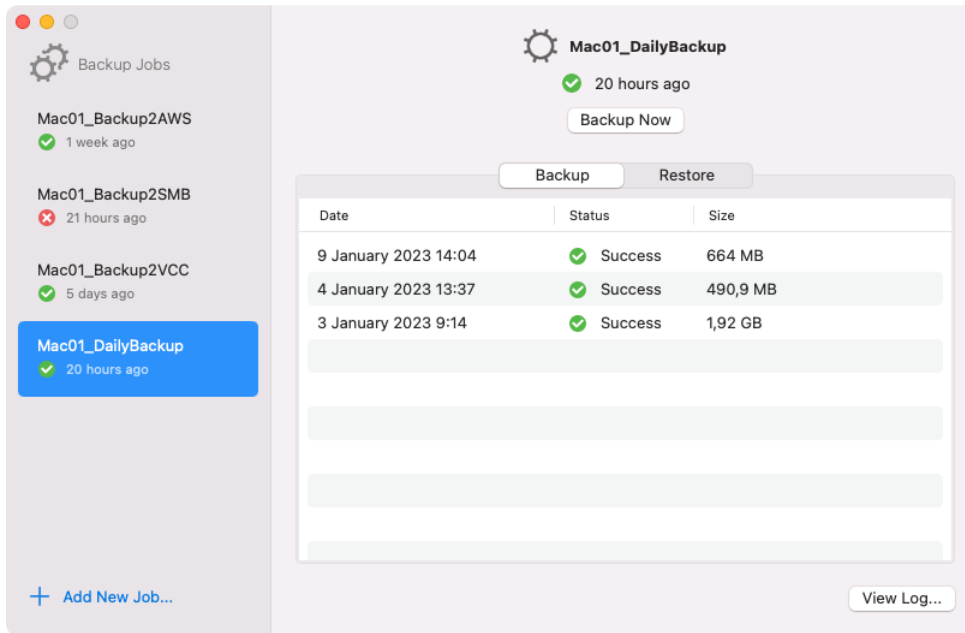
Control Panel View

Depending on how many backup jobs you have configured in Veeam Agent, the layout of the control panel can be different:

- [Single backup job]



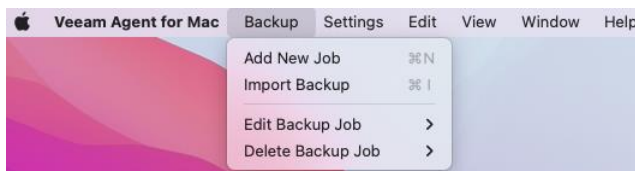
- [Multiple backup jobs]



Application Menu

The Veeam Agent application menu provides the following items:

- **Backup** – this menu contains the following options:
 - *Add New Job* – use this option to create new backup jobs using the **Backup Job** wizard.
 - *Import Backup* – use this option to import backups using the **Import** wizard.
 - *Edit Backup Job* – use this option to select a backup job and edit its settings in the **Backup Job** wizard.
 - *Delete Backup Job* – use this option to select a backup job to delete.

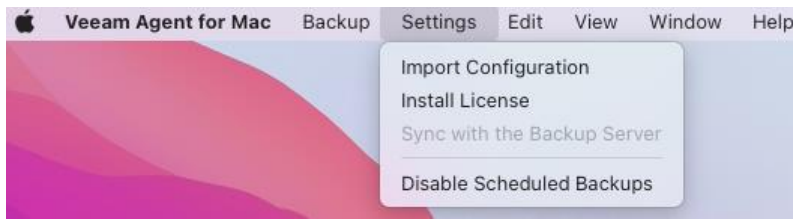


- **Settings** – this menu contains the following options:
 - *Import Configuration* – use this option to import a configuration file from Veeam Backup & Replication.
 - *Install License* – use this option to view and manage the Veeam Agent license.
 - [Starting from version 2.1.2] *Sync with the Backup Server* – if Veeam Agent computer is managed by Veeam Backup & Replication through a protection group for pre-installed Veeam Agents, use this option to immediately synchronize Veeam Agent configuration with Veeam Backup & Replication database.

IMPORTANT

This option is inactive if Veeam Agent operates in the standalone mode. For more information on operation modes, see [Standalone and Managed Operation Modes](#).

- *Disable/Enable Scheduled Backups* – use this option to disable and enable all backups scheduled in Veeam Agent.



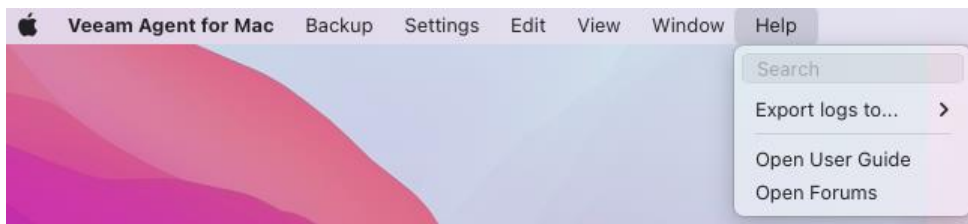
- **Help** – this menu contains the following options:

- *Export Logs to* – use this menu to export product logs. It provides two options:
 - *Local folder* – use this option to save the product logs in a local folder on the Veeam Agent computer.
 - [Starting from version 2.1.2] *Veeam server* – if Veeam Agent computer is managed by Veeam Backup & Replication through a protection group for pre-installed Veeam Agents, use this option to save the product logs in a folder on the Veeam backup server.

IMPORTANT

This option is inactive if Veeam Agent operates in the standalone mode. For more information on operation modes, see [Standalone and Managed Operation Modes](#).

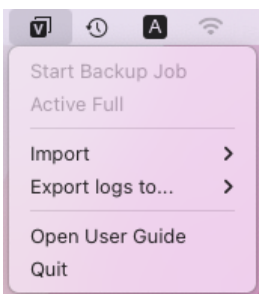
- *Open User Guide* – use this option to open online help.
- *Open Forums* – use this option to open Veeam community forums.



Veeam Agent for Mac Status Bar Menu

When you close Veeam Agent control panel, Veeam Agent Status Bar Menu remains active and allows you to perform the following operations:

- If there is only one job configured in Veeam Agent, you can start and stop the job, as well as run an ad-hoc active full backup. For more information, see [Performing Backup](#).
- Import backups. For more information, see [Importing Backups](#).
- Import configuration from Veeam Backup & Replication. For more information, see [Importing Configuration from Veeam Backup Server](#).
- Export product logs. For more information, see [Exporting Product Logs with Control Panel and Status Bar Menu](#).



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](#).

In Veeam Agent command line interface, in addition to operations that you can perform with the Veeam Agent graphic user interface, you can perform a set of advanced tasks – for example:

- Synchronize Veeam Agent with Veeam backup server.
- Edit backup repository settings.
- Monitor performance and status of any backup, restore and other data transfer session that was started in Veeam Agent.
- Export/import Veeam Agent configuration database to/from a configuration file.

Constructing Commands for Veeam Agent

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
 - healthcheck
 - help
 - job
 - license
 - mode
 - objectstorage

- 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
 - createrepository
 - 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          Typ
e    Accessible Backup server
Repository_1  {818e3a0f-8155-4a51-9430-248a203a43d1} /home/backups    loca
l            true
Repository_2  {2155a2e7-a1e9-4347-9d8b-cf8f3a6f3fcb} 172.17.53.47/veeam cif
s            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
```

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 job. Depending on the product edition, Veeam Agent lets you configure one or several backup jobs targeted at the same or different backup repositories. For more information on licensing options, see [Product Editions](#).

Configuring several backup jobs may be useful in the following situations:

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

You can configure a backup job that will automatically back up your data according to a defined schedule. You can also start backup job manually at any time.

Creating Backup Jobs

With Veeam Agent for Mac, you can configure a backup job in one of the following ways:

- [With the Backup Job wizard](#)
- [In command line interface](#)

Creating Backup Job with Backup Job Wizard

You can configure file-level backup jobs with the Backup Job wizard.

Before You Begin

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

- The target location where you plan to store backup files must have enough free space.
- [For Veeam Backup & Replication repositories] To store backups in a backup repository, the backup server must run the following version of Veeam Backup & Replication:
 - [For Veeam Agent version 2.1] Veeam Backup & Replication version 12.1 or later.
 - [For Veeam Agent version 2.0] Veeam Backup & Replication version 12.0 or later.
- [For Veeam Backup & Replication repositories] If you plan to use a Veeam Backup & Replication repository as a target for backups, you must pre-configure user access permissions on this backup repository. To learn more, see [Setting Up User Permissions on Backup Repositories](#).
- [For object storage repositories] If you plan to use an object storage repository as a target for backups, you must set up an account with the storage provider. The account must have permissions to read and write data.

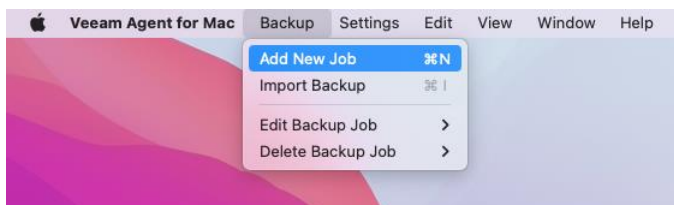
Backup has the following limitations:

- You cannot save the backup of entire computer on the local computer disk. Use an external hard drive or USB drive, network shared folder or backup repository as a target location.
- Veeam Agent does not backup data to which symbolic links are targeted. It only backs up the path information that the symbolic links contain. After restore, identical symbolic links are created in the restore destination.
- Keep in mind that Veeam Agent stops running the backup job after 21 days (504 hours).

Step 1. Launch Backup Job Wizard

To launch the Backup Job wizard, do either of the following:

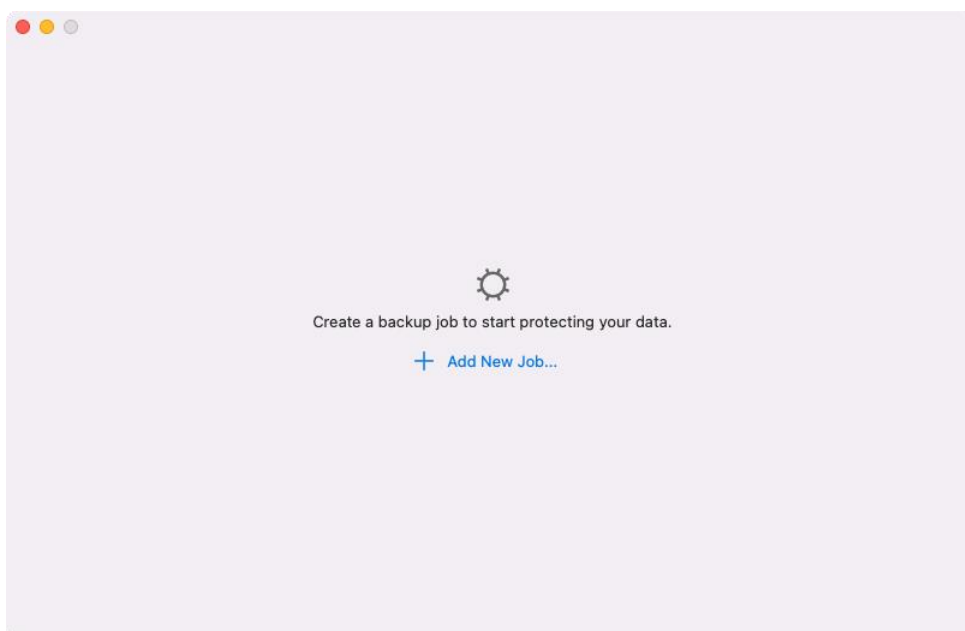
- In the **Veeam Agent for Mac** application menu, select **Backup > Add New Job**.



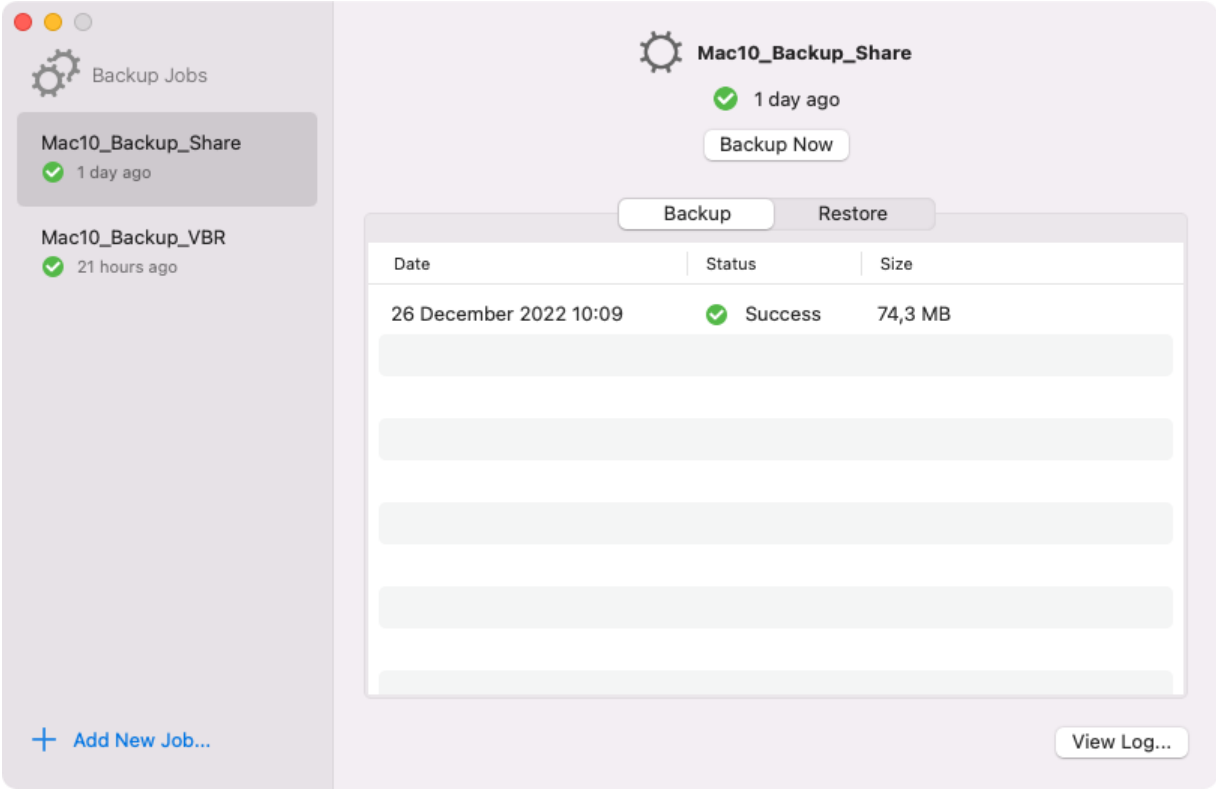
Alternatively, you can use the **Command-N** shortcut on the keyboard.

- In the **Veeam Agent for Mac** control panel, click **Add New Job**.

If you haven't created any backup jobs yet, the control panel will display the **Add New Job** link in the center of the window:

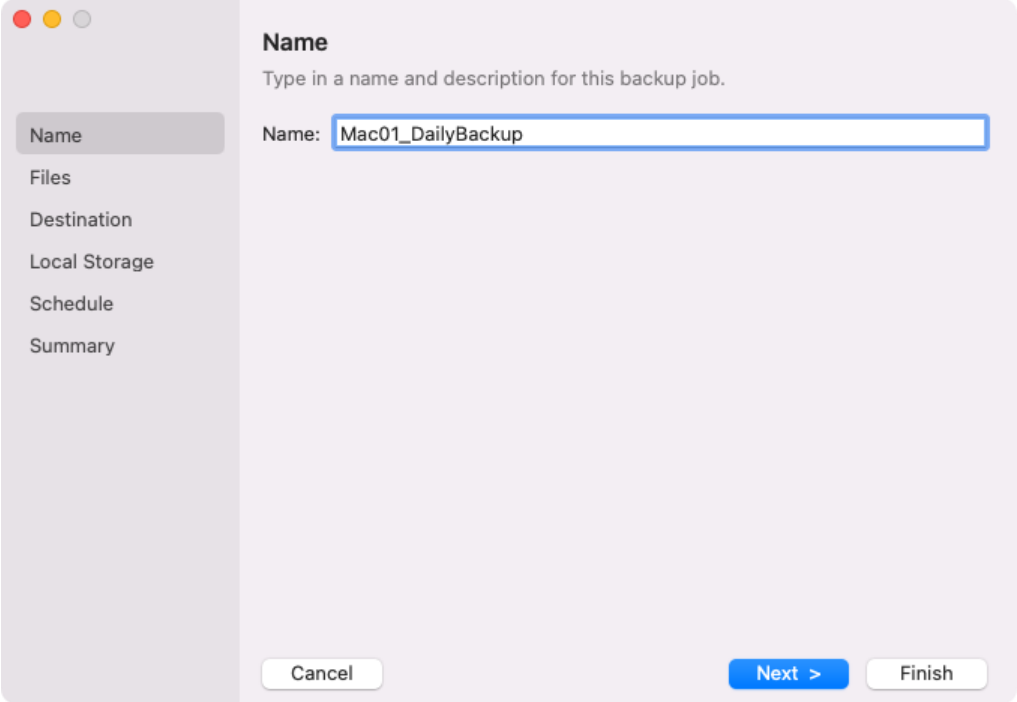


If you already have configured backup jobs in Veeam Agent, the **Add New Job** link is displayed at the bottom of the **Backup Jobs** panel.



Step 2. Add Backup Job Name

At the **Name** step of the wizard, type a name for the backup job.



Step 3. Define Backup Job Scope

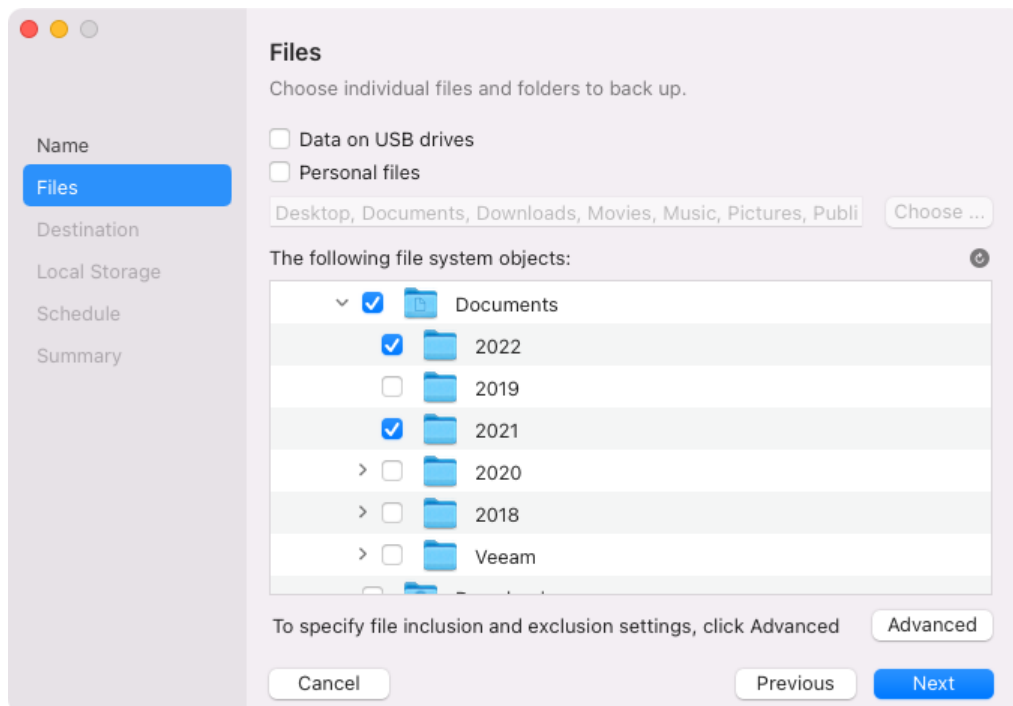
At the **Files** step of the wizard, you must specify the backup scope – define what folders with files you want to include in the backup.

You can include all or either of the following data in the backup:

- Data on USB drives – data that resides on the USB devices attached to your computer.
- Personal files – data related to user profiles. With this option enabled, Veeam Agent will back up data related to all user profiles on the Veeam Agent computer. You can specify what personal data to include in the backup and choose whether to exclude network accounts from the backup. To learn more, see [Protecting User Profiles Data](#).
- Individual folders – data that resides in files on your computer.

NOTE

Starting from version 2.1.2, Veeam Agent provides a more flexible way of selecting folders to back up. To learn more, see [Selecting Folders](#).

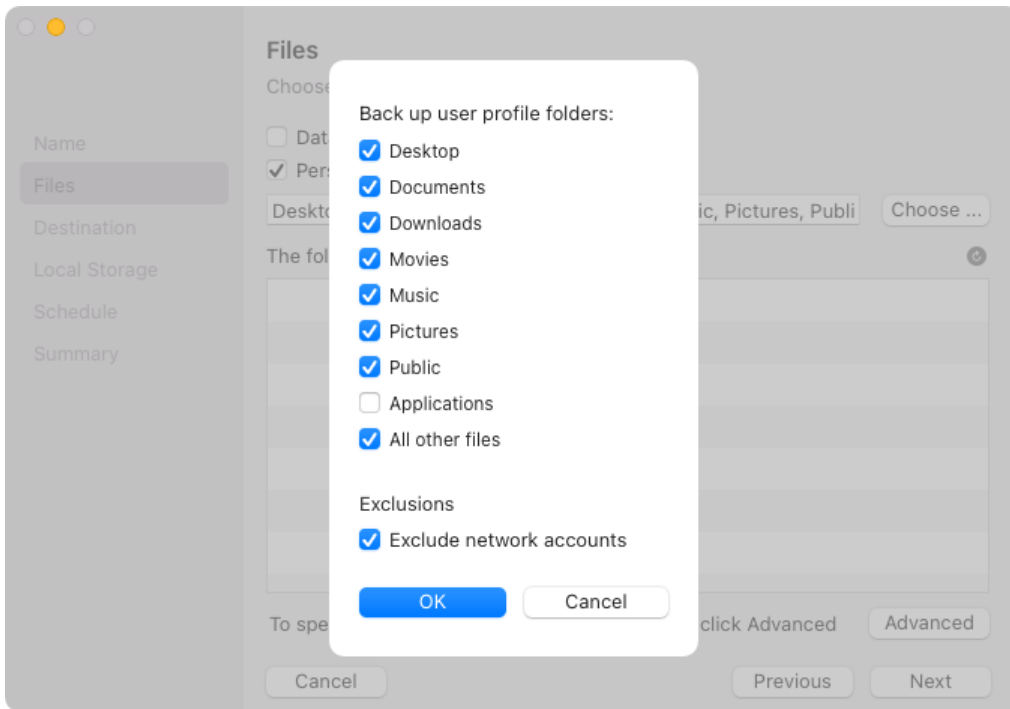


Protecting User Profiles Data

To include personal data in the backup, select the **Personal files** option. When you select to back up personal data, by default Veeam Agent backs up all data stored in the `Users` folder on the system volume excluding application data and data related to network accounts. If you store personal folders of user profiles in custom locations, Veeam Agent backs them up too.

If you do not want to back up default personal data, you can change the backup scope by selecting what folders Veeam Agent includes in the `Users` component. To do this, click **Choose** next to the **Personal files** field and select the necessary options in the **Back up user profile folders** window.

You can use the **All other files** option to back up all folders and files that are located in the `Users` folder on the system volume, but are not available in the **Back up user profile folders** window.



Selecting Folders

You must include in the backup at least one folder. If you do not want to back up some subfolders of the specified folder, you can exclude these subfolders from the backup. If you want to include or exclude specific files or file types in/from the backup, click **Advanced**. To learn more, see [Configuring Filters](#).

NOTE

You can include in the backup scope folders and files that reside on an external USB/eSATA or FireWire drive connected to the Veeam Agent computer.

Depending on the version of Veeam Agent that you use, to include a folder in the backup, do the following:

For Veeam Agent version 2.1.2

1. In the **The following file system objects** section, navigate to the folder that you want to backup in the file system tree.
2. Select the check box next to each folder that you want to back up.
3. If you want to exclude from backup one or more subfolders of the selected folder, expand the folder and clear the check box next to the subfolders that you want to exclude.

For Veeam Agent version 2.0 and 2.1

1. In the **The following file system objects** section, click **Add**.
2. In the file browser window, drill down to the folder that you want to back up and click **Open**.

After you select a folder, Veeam Agent will add its path as an item into the list of file system objects to back up.

You can click **Add** again to add more folders to the backup scope.

You can also remove folders from the scope. To do this, select a folder in the file system objects tree and click **Remove**.

Configuring Filters

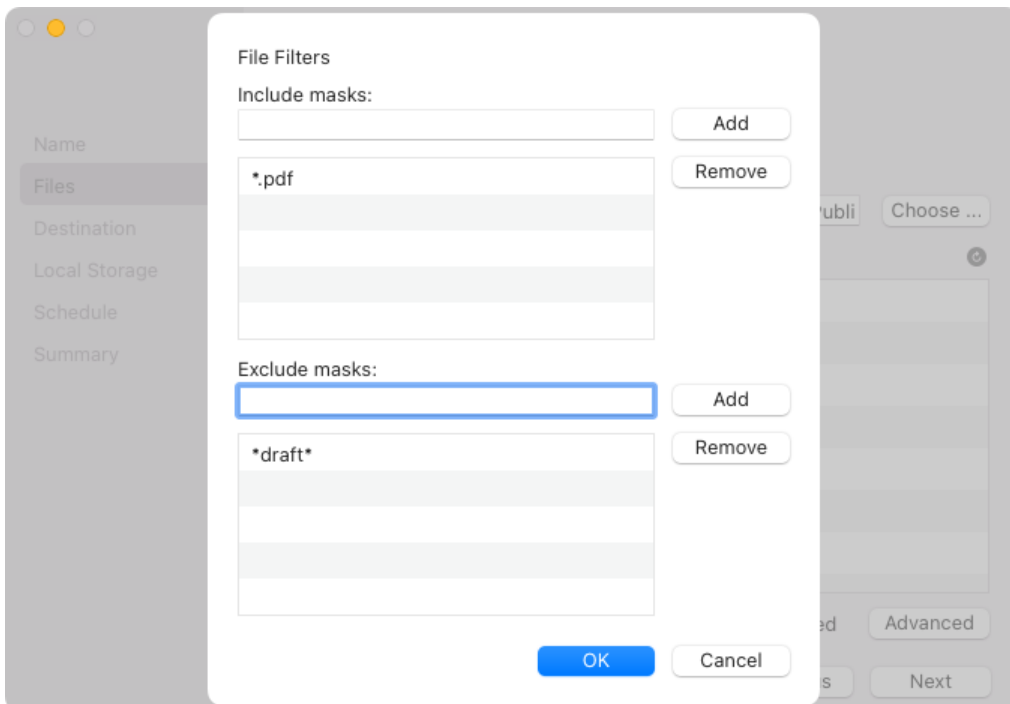
You can specify file name masks for files or file types that you want to include or exclude in/from the backup. To do this:

1. After you added folders to the backup scope, click **Advanced**.
2. In the **File Filters** window, specify file name masks.
 - To include specific files into the backup, enter file names and/or masks in the **Include masks** field – for example, `MyMovie.avi`, `*filename*`, `*.docx`, `*.mp3`. Veeam Agent will create a backup only for the selected files; no other files will be backed up.
 - To exclude specific files from the backup, enter file names and/or masks in the **Exclude masks** field – for example, `OldPhotos.rar`, `*.temp`, `*.tmp`, `*.back`. Veeam Agent will back up all files except the files specified in the exclude mask.
3. Click **Add**.
4. To add more masks, repeat steps 2-3 for each mask.

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

- Include mask: `*.pdf`
- Exclude mask: `*draft*`

Veeam Agent backup will include all files in the PDF format that do not contain `draft` in their names.

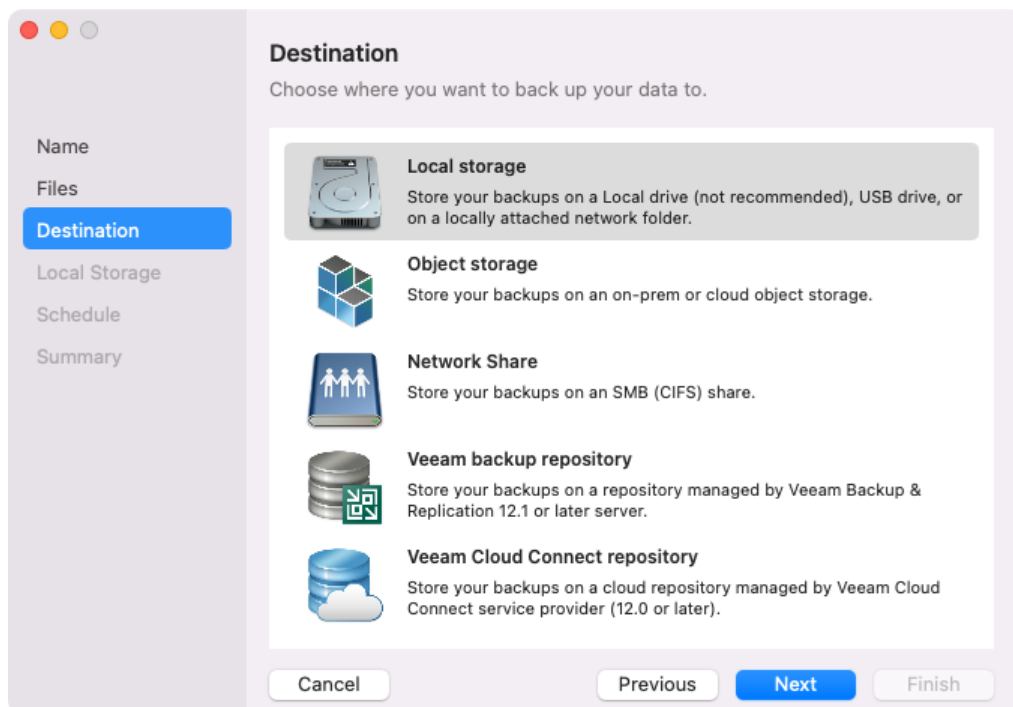


Step 4. Select Backup Destination

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

You can select one of the following options:

- **Local storage** – select this option if you want to save the backup on a local computer drive, direct or network attached storage – for example, a USB flash drive or locally mounted SMB share. With this option selected, you will pass to the [Local Storage](#) step of the wizard.
- **Object storage** – select this option if you want to create the backup on an object storage repository exposed to you by third-party vendors. With this option selected, you will pass to the [Cloud Type](#) step of the wizard.
- **Network Share** – select this option if you want to save the backup to a network shared folder. With this option selected, you will pass to the [Network Share](#) step of the wizard.
- **Veeam backup repository** – select this option if you want to save the backup on a backup repository managed by the Veeam backup server. With this option selected, you will pass to the [Backup Server](#) step of the wizard.
- **Veeam Cloud Connect repository** – select this option if you want to create the backup on a cloud repository exposed to you by the Veeam Cloud Connect service provider. With this option selected, you will pass to the [Service Provider](#) step of the wizard.



Step 5. Specify Backup Storage Settings

Specify backup storage settings for the backup job:

- [Local storage settings](#) – if you have selected the **Local storage** option at the [Destination](#) step of the wizard.
- [Object storage settings](#) – if you have selected the **Object storage** option at the [Destination](#) step of the wizard.
- [Shared folder settings](#) – if you have selected the **Network Share** option at the [Destination](#) step of the wizard.
- [Veeam backup repository settings](#) – if you have selected the **Veeam backup repository** option at the [Destination](#) step of the wizard.
- [Veeam Cloud Connect repository settings](#) – if you have selected the **Veeam Cloud Connect repository** option at the [Destination](#) step of the wizard.

NOTE

The **Veeam Cloud Connect repository** option is available if Veeam Agent operates in the Workstation or Server edition.

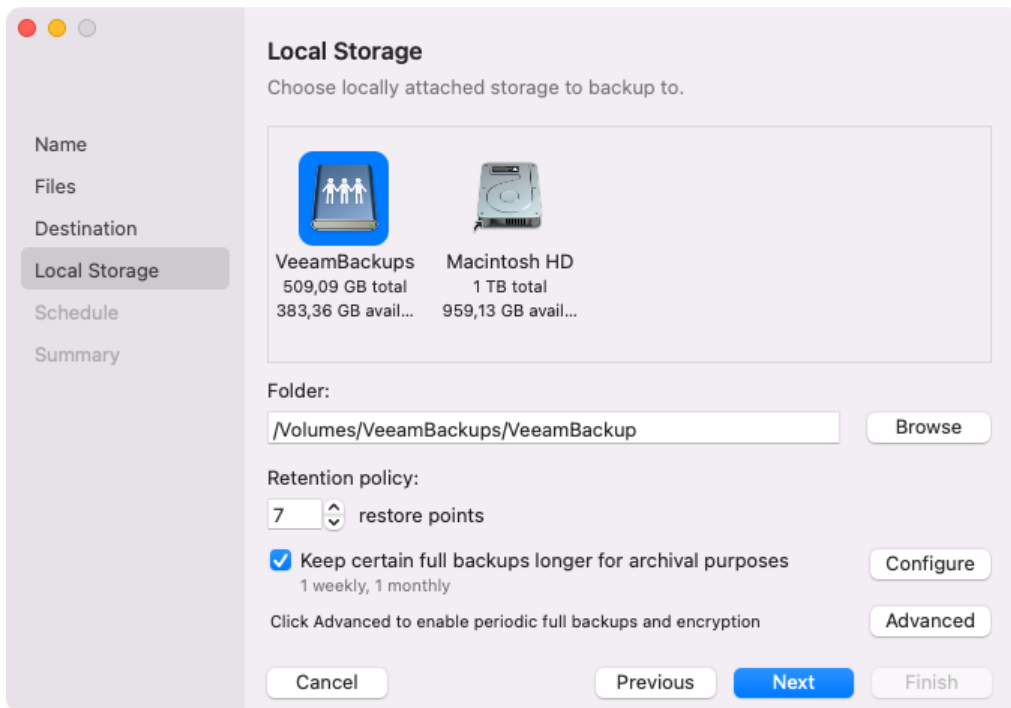
Local Storage Settings

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

Specify local storage settings:

1. In the panel that displays available storage locations, select a location where you want to store the backup.
2. In the **Folder** field, specify a path to the folder where backup files must be saved. By default, Veeam Agent saves files in the `VeeamBackup` folder.
3. In the **Retention policy** section, specify the number of restore points for Veeam Agent to store in the target location. By default, Veeam Agent keeps 7 restore points. To learn more, see [Backup Retention Policy](#).
4. Starting from version 2.1, you can use the GFS (Grandfather-Father-Son) retention scheme. To specify the GFS retention policy, select the **Keep certain full backups longer for archival purposes** check box and press **Configure**. In the **Configure GFS** window, specify how weekly, monthly and yearly full backups must be retained. For details, see [Specify GFS Retention Policy](#).

5. Click **Advanced** to specify advanced settings for the backup job. To learn more, see [Specify Advanced Backup Settings](#).



Object Storage Settings

The **Cloud Type** step of the wizard is available if you have selected the **Object storage** option at the [Destination](#) step of the wizard.

At the **Cloud Type** step of the wizard, select the cloud storage. You can select one of the following options:

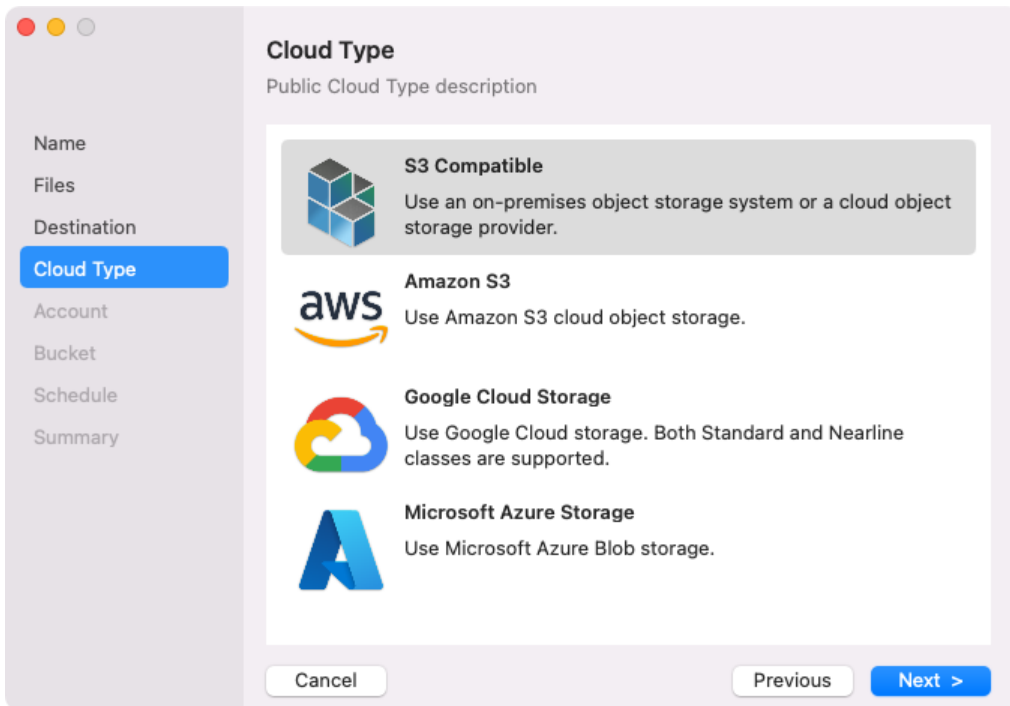
- **S3 Compatible** – select this option if you want to create a backup in an S3 compatible storage repository. With this option selected, you will pass to the [Account](#) step of the wizard.

TIP

If you plan to store backups on an IBM or Wasabi cloud storage, use the **S3 compatible** storage option.

- **Amazon S3** – select this option if you want to create a backup in an Amazon S3 storage repository. With this option selected, you will pass to the [Account](#) step of the wizard.
- **Google Cloud Storage** – select this option if you want to create a backup in a Google Cloud storage repository. With this option selected, you will pass to the [Account](#) step of the wizard.

- **Microsoft Azure Storage** – select this option if you want to create a backup in a Microsoft Azure storage repository. With this option selected, you will pass to the [Account](#) step of the wizard.



S3 Compatible Settings

If you have selected to store backup files on an S3 compatible storage, specify the following settings:

1. [Account settings](#).
2. [Bucket settings](#).

Specifying Account Settings

The **Account** step of the wizard is available if you have chosen to save backup files on an S3 compatible storage.

NOTE

You can store backups only in the S3 compatible storage repositories that are accessible over the HTTPs protocol.

To connect to the S3 compatible storage, specify the following:

1. In the **Service point** field, specify the address of your S3 compatible storage.

NOTE

If you want to connect to the repository using the IPv6 address and the port number, you must use the following format: `IPv6:port`, where:

- `IPv6` is the IPv6 address of the object storage.
 - `port` is the number of the port that Veeam Agent will use to connect to the object storage.
2. In the **Region** field, specify a storage region based on your regulatory and compliance requirements.
 3. In the **Access key** field, enter an access key ID.

4. In the **Secret key** field, enter a secret access key.

Account
Specify S3 compatible storage account

Name

Files

Destination

Cloud Type

Account

Bucket

Schedule

Summary

Service point:
https://myservicepoint.com

Region:
reg-1

S3-compatible account:

Access key:
Access_Key

Secret key:
●●●●●●●●●●●●

Cancel Previous Next >

Specifying Bucket Settings

The **Bucket** step of the wizard is available if you have chosen to save backup files on an S3 compatible storage and specified account settings to connect to the storage.

Specify settings for the bucket on the storage:

1. In the **Bucket** field, specify a bucket on the storage:
 - a. Click **Browse**.
 - b. In the **Buckets** window, select the necessary bucket and click **OK**.
2. In the **Folder** field, specify a folder in the bucket:
 - a. Click **Browse**.
 - b. In the **Folders** window, select the necessary folder and click **OK**.

TIP

You can also create a new folder in the bucket. To do this:

1. In the **Folders** window, click **New Folder**.
 2. In the **Creating new folder** dialog window, enter a name for the folder and click **OK**.
3. In the **Retention policy** section, specify the number of **restore points** that you want to store in the target location. By default, Veeam Agent keeps 7 latest restore points. After this number is exceeded, Veeam Agent will remove the earliest restore points from the backup chain. To learn more, see [Backup Retention Policy](#).
 4. Starting from version 2.1, you can use the GFS (Grandfather-Father-Son) retention scheme. To specify the GFS retention policy, select the **Keep certain full backups longer for archival purposes** check box and press **Configure**. In the **Configure GFS** window, specify how weekly, monthly and yearly full backups must be retained. For details, see [Specify GFS Retention Policy](#).
 5. Click **Advanced** to specify additional backup job settings. For details, see [Specify Advanced Backup Settings](#).

- To prohibit modification and deletion of blocks of data in the object storage repository, select the **Make recent backups immutable for** check box and specify the immutability period in days. For more information, see [Backup Immutability](#).
- After you specified the bucket settings, click **Next**. Veeam Agent will create a new backup repository for the configured cloud storage.

Bucket
Specify S3-compatible folder and bucket settings

Name
Files
Destination
Cloud Type
Account
Bucket
Schedule
Summary

Bucket:
vam-veeam-backups

Folder:
folder01

Retention policy:
7 restore points

Keep certain full backups longer for archival purposes
1 weekly, 1 monthly

Make recent backups immutable for: 30 days

Protects backups from modification or deletion by ransomware, malicious insiders and hackers. This may incur additional API and storage costs. GFS backups are made immutable for the entire duration of their retention policy.

Click Advanced to enable periodic full backups and encryption

Amazon S3 Settings

If you have selected to store backup files on an Amazon S3 storage, specify the following settings:

- [Account settings](#).
- [Bucket settings](#).

Specifying Account Settings

The **Account** step of the wizard is available if you have chosen to save backup files on an Amazon S3 storage.

To connect to the Amazon S3 storage, specify the following:

- In the **Access key** field, enter an access key ID.
- In the **Secret key** field, enter a secret access key.

3. In the **AWS region** window, select an AWS region based on your regulatory and compliance requirements. By default, Veeam Agent uses the **Global** region.

Account
Specify Amazon S3 account

Access key:
AKIA4SIMXVDIFTNXXRF4

Secret key:
.....

AWS region: Global

Cancel Previous Next >

Specifying Bucket Settings

The **Bucket** step of the wizard is available if you have chosen to save backup files on an Amazon S3 storage and specified account settings to connect to the storage.

IMPORTANT

You must create the bucket where you want to store your backup data beforehand. When you create a bucket, consider Amazon bucket naming rules. For example, it is not recommended that you use dots (.) in the bucket name. For more information on bucket naming rules, see [this AWS documentation article](#).

Specify settings for the bucket on the storage:

1. In the **Data center** window, select the geographic region where Veeam Agent will store backups.
2. In the **Bucket** field, specify a bucket on the storage:
 - a. Click **Browse**.
 - b. In the **Buckets** window, select the necessary bucket and click **OK**.
3. In the **Folder** field, specify a folder in the bucket:
 - a. Click **Browse**.
 - b. In the **Folders** window, select the necessary folder and click **OK**.

TIP

You can also create a new folder in the bucket. To do this:

1. In the **Folders** window, click **New Folder**.
2. In the **Creating new folder** dialog window, enter a name for the folder and click **OK**.

- In the **Retention policy** section, specify the number of **restore points** that you want to store in the target location. By default, Veeam Agent keeps 7 latest restore points. After this number is exceeded, Veeam Agent will remove the earliest restore points from the backup chain. To learn more, see [Backup Retention Policy](#).
- Starting from version 2.1, you can use the GFS (Grandfather-Father-Son) retention scheme. To specify the GFS retention policy, select the **Keep certain full backups longer for archival purposes** check box and press **Configure**. In the **Configure GFS** window, specify how weekly, monthly and yearly full backups must be retained. For details, see [Specify GFS Retention Policy](#).
- Click **Advanced** to specify additional backup job settings. For details, see [Specify Advanced Backup Settings](#).
- To prohibit modification and deletion of blocks of data from the object storage repository, select the **Make recent backups immutable for** check box and specify the immutability period in days. For more information, see [Backup Immutability](#).
- After you specified the bucket settings, click **Next**. Veeam Agent will create a new backup repository for the configured cloud storage.

Google Cloud Storage Settings

If you have selected to store backup files on a Google Cloud storage repository, specify the following settings:

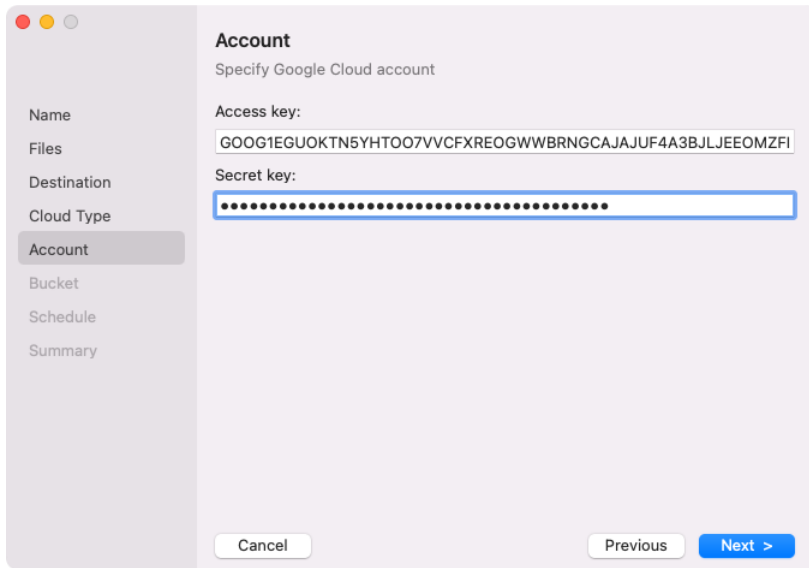
- [Account settings](#).
- [Bucket settings](#).

Specifying Account Settings

The **Account** step of the wizard is available if you have chosen to save backup files on a Google Cloud storage.

To connect to the Google Cloud storage, in the **Access key** and **Secret key** fields, specify the Hash-based Message Authentication Code (HMAC) key associated with the Google Cloud account. Veeam Agent will use the HMAC key to authenticate requests to the Google Cloud storage. For more information on Google Cloud accounts, see the [Google Cloud documentation](#).

If you have not created the HMAC key beforehand, you can create the key in the Google Cloud console, as described in the [Google Cloud documentation](#).



Specifying Bucket Settings

The **Bucket** step of the wizard is available if you have chosen to save backup files on a Google Cloud storage and specified account settings to connect to the storage.

Specify settings for the bucket on the storage:

1. In the **Data center** window, select the geographic region where Veeam Agent will store backups.
2. In the **Bucket** field, specify a bucket on the storage:
 - a. Click **Browse**.
 - b. In the **Buckets** window, select the necessary bucket and click **OK**.
3. In the **Folder** field, specify a folder in the bucket:
 - a. Click **Browse**.
 - b. In the **Folders** window, select the necessary folder and click **OK**.

TIP

You can also create a new folder in the bucket. To do this:

1. In the **Folders** window, click **New Folder**.
 2. In the **Creating new folder** dialog window, enter a name for the folder and click **OK**.
4. In the **Retention policy** section, specify the number of **restore points** that you want to store in the target location. By default, Veeam Agent keeps 7 latest restore points. After this number is exceeded, Veeam Agent will remove the earliest restore points from the backup chain. To learn more, see [Backup Retention Policy](#).
 5. Starting from version 2.1, you can use the GFS (Grandfather-Father-Son) retention scheme. To specify the GFS retention policy, select the **Keep certain full backups longer for archival purposes** check box and press **Configure**. In the **Configure GFS** window, specify how weekly, monthly and yearly full backups must be retained. For details, see [Specify GFS Retention Policy](#).

6. Click **Advanced** to specify additional backup job settings. For details, see [Specify Advanced Backup Settings](#).
7. After you specified the bucket settings, click **Next**. Veeam Agent will create a new backup repository for the configured cloud storage.

Bucket
Specify Google Cloud bucket and folder

Data center:
us-east5 (Columbus)

Bucket:
mac-veeam-backups Browse

Folder:
folder01 Browse

Retention policy:
7 restore points

Keep certain full backups longer for archival purposes
1 weekly, 1 monthly Configure

Click Advanced to enable periodic full backups and encryption Advanced

Cancel Previous Next Finish

Microsoft Azure Storage Settings

If you have selected to store backup files on a Microsoft Azure storage, specify the following settings:

1. [Account settings](#).
2. [Container settings](#).

Specifying Account Settings

The **Account** step of the wizard is available if you have chosen to save backup files on a Microsoft Azure storage.

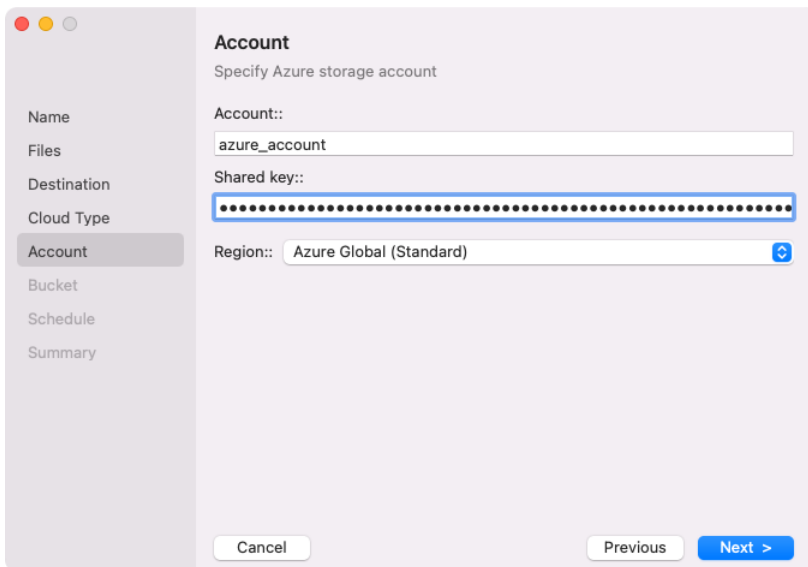
NOTE

The **Allow storage account key access** option for Shared Key authorization must be enabled in the storage account. For more information on how to find this option, see [Microsoft Docs](#).

To connect to the Microsoft Azure storage, specify the following:

1. In the **Account** field, enter the storage account name.
2. In the **Shared key** field, enter the storage account shared key.

3. In the **Region** window, select a Microsoft Azure region based on your regulatory and compliance requirements. By default, Veeam Agent uses the **Azure Global (Standard)** region.



Specifying Container Settings

The **Bucket** step of the wizard is available if you have chosen to save backup files on a Microsoft Azure storage and specified account settings to connect to the storage.

Specify settings for the container on the storage:

1. In the **Container** field, specify a container on the storage:
 - a. Click **Browse**.
 - b. In the **Containers** window, select the necessary container and click **OK**.
2. In the **Folder** field, specify a folder in the bucket:
 - a. Click **Browse**.
 - b. In the **Folders** window, select the necessary folder and click **OK**.

TIP

You can also create a new folder in the bucket. To do this:

1. In the **Folders** window, click **New Folder**.
 2. In the **Creating new folder** dialog window, enter a name for the folder and click **OK**.
3. In the **Retention policy** section, specify the number of **restore points** that you want to store in the target location. By default, Veeam Agent keeps 7 latest restore points. After this number is exceeded, Veeam Agent will remove the earliest restore points from the backup chain. To learn more, see [Backup Retention Policy](#).
 4. Starting from version 2.1, you can use the GFS (Grandfather-Father-Son) retention scheme. To specify the GFS retention policy, select the **Keep certain full backups longer for archival purposes** check box and press **Configure**. In the **Configure GFS** window, specify how weekly, monthly and yearly full backups must be retained. For details, see [Specify GFS Retention Policy](#).
 5. Click **Advanced** to specify additional backup job settings. For details, see [Specify Advanced Backup Settings](#).

- To prohibit modification and deletion of blocks of data from the object storage repository, select the **Make recent backups immutable for** check box and specify the immutability period in days. For more information, see [Backup Immutability](#).
- After you specified the bucket settings, click **Next**. Veeam Agent will create a new backup repository for the configured cloud storage.

Shared Folder Settings

The **Network Share** step of the wizard is available if you have chosen to save the backup to a network shared folder.

Specify the shared folder settings:

- In the **Server** field, type an IP address or domain name of the server that hosts the shared folder.
- In the **Folder** field, type a name of the network shared folder in which you want to store backup files.
- If the network shared folder requires authentication, specify credentials to access the network shared folder:
 - In the **Username** field, type a name of the account that has access permissions on the shared folder.
 - If necessary, in the **Domain** field, type a name of the domain in which the account that has access permissions on the shared folder is registered.
 - In the **Password** field, type a password of the account that has access permissions on the shared folder.
- In the **Retention policy** section, specify the number of restore points for Veeam Agent to store in the target location. By default, Veeam Agent keeps 7 restore points. To learn more, see [Backup Retention Policy](#).
- Starting from version 2.1, you can use the GFS (Grandfather-Father-Son) retention scheme. To specify the GFS retention policy, select the **Keep certain full backups longer for archival purposes** check box and press **Configure**. In the **Configure GFS** window, specify how weekly, monthly and yearly full backups must be retained. For details, see [Specify GFS Retention Policy](#).

6. Click **Advanced** to specify advanced settings for the backup job. To learn more, see [Specify Advanced Backup Settings](#).

Network Share
Specify a shared folder to back up to and credentials to connect with.

Name
Files
Destination
Network Share
Schedule
Summary

Server: 172.24.31.133
Folder: backup01
Username: richard.o
Password: [masked] Edit

Retention policy:
7 restore points
 Keep certain full backups longer for archival purposes
1 weekly, 1 monthly Configure

Click Advanced to enable periodic full backups and encryption Advanced

Cancel Previous Next >

Veeam Backup Server Settings

If you have selected to store backup files on a Veeam backup repository, specify settings to connect to the backup repository:

1. [Specify backup server settings](#).
2. [Select the Veeam backup repository](#).

Specifying Backup Server Settings

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

IMPORTANT

Mind the following:

- If you plan to use a commercial version of Veeam Agent with Veeam Backup & Replication, you must install a license in Veeam Backup & Replication before connecting to the 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.

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

1. In the **Veeam backup server name or IP address** field, specify a DNS name or IP address of the Veeam backup server.
2. In the **Port** field, specify the number of the port over which Veeam Agent must communicate with the backup repository. By default, Veeam Agent for Mac uses port 10006.
3. In the **Specify your personal credentials** section, enter credentials to access the server:
 - a. In the **Username** field, type a name of the account that has access permissions on the Veeam backup repository.

- b. If necessary, in the **Domain** field, type a name of the domain in which the account that has access to the Veeam backup repository is registered.
- c. In the **Password** field, type a password of the account that has access to the Veeam backup repository.

Backup Server
Specify a Veeam Backup & Replication server to see repositories.

Name
Files
Destination
Backup Server
Repository
Schedule
Summary

Veeam backup server name or IP address: Port:

Specify your personal credentials:

Username:

Domain (optional):

Password:

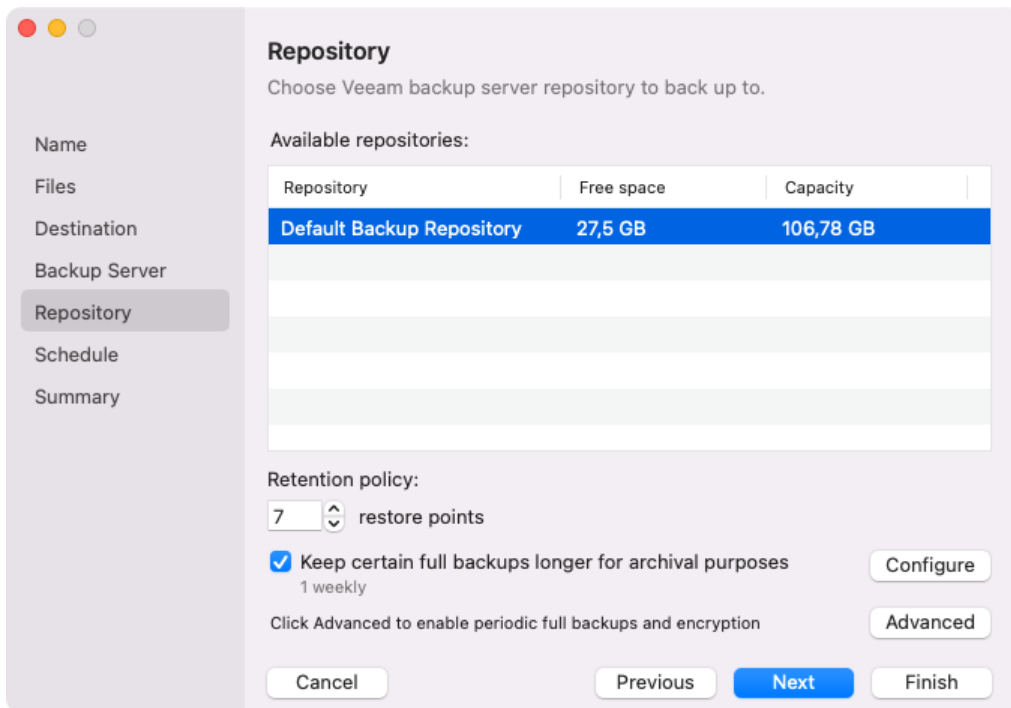
Selecting Backup Repository

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

Specify settings for the target backup repository:

1. From the **Available repositories** list, select a backup repository where you want to store backups. The list of backup repositories displays only those backup repositories on which you have permissions to store data. To learn more, see [Setting Up User Permissions on Backup Repositories](#).
2. In the **Retention policy** section, specify the number of restore points for Veeam Agent to store in the target location. By default, Veeam Agent keeps 7 restore points. To learn more, see [Backup Retention Policy](#).
3. Starting from version 2.1, you can use the GFS (Grandfather-Father-Son) retention scheme. To specify the GFS retention policy, select the **Keep certain full backups longer for archival purposes** check box and press **Configure**. In the **Configure GFS** window, specify how weekly, monthly and yearly full backups must be retained. For details, see [Specify GFS Retention Policy](#).

4. Click **Advanced** to specify advanced settings for the backup job. To learn more, see [Specify Advanced Backup Settings](#).



Veeam Cloud Connect Settings

If you have selected to store backup files on a Veeam Cloud Connect repository, specify settings to connect to the cloud repository:

1. [Specify service provider settings](#).
2. [Specify user account settings and verify certificate](#).
3. [Select the cloud repository](#).

NOTE

The **Veeam Cloud Connect repository** option is available only in the Workstation and Server editions of Veeam Agent for Mac.

Specifying Service Provider Settings

The **Service Provider** step of the wizard is available if you have chosen to save backup files on a Veeam Cloud Connect repository.

Specify settings for the cloud gateway that the Veeam Cloud Connect service provider (SP) or your backup administrator has provided to you:

1. In the **DNS name or IP address** field, enter a full DNS name or IP address of the cloud gateway.

2. In the **Port** field, specify the port over which Veeam Agent will communicate with the cloud gateway. By default, Veeam Agent uses port 6180.

Service Provider
Type in DNS name or IP address received from the service provider.

DNS name or IP address: Port:

Default service provider's port is 6180. If connection cannot be established, contact your service provider to make sure the settings are correct.

Search for resellers and service providers that offer cloud repositories and cloud hosts for off-site backup and disaster recovery. [Click here to open the directory.](#)

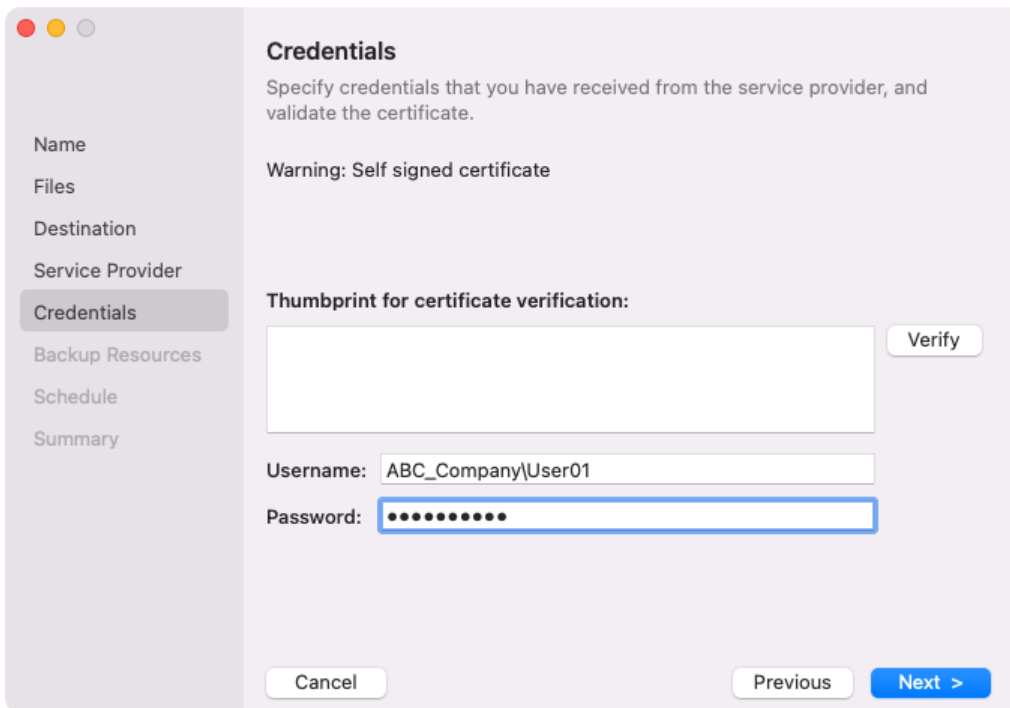
Cancel Previous Next >

Specifying User Account Settings and Verifying Certificate

The **Credentials** step of the wizard is available if you have chosen to save backup files on a cloud repository and specified settings for the cloud gateway.

1. In the **Username** 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.
2. In the **Password** field, provide a password for the tenant or subtenant account.
3. [Optional] To validate the certificate of the SP server with a thumbprint, do the following:
 - a. In the **Thumbprint for certificate verification** field, paste the thumbprint you obtained from the SP.

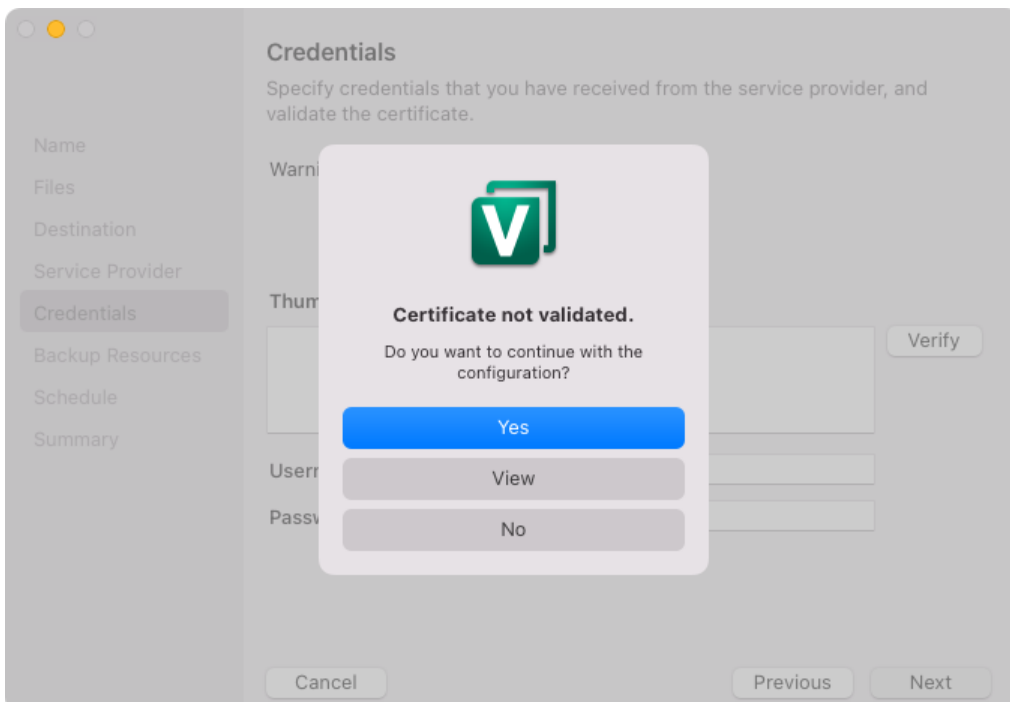
- b. Click **Verify**. Veeam Agent will check if the thumbprint you entered matches the thumbprint of the obtained TLS certificate. To the dialog that confirms successful certificate validation, click **OK**.



If the certificate has not been verified on the Veeam Agent computer, after you click **Next** at the **Credentials** step of the wizard, you will be asked to verify the certificate.

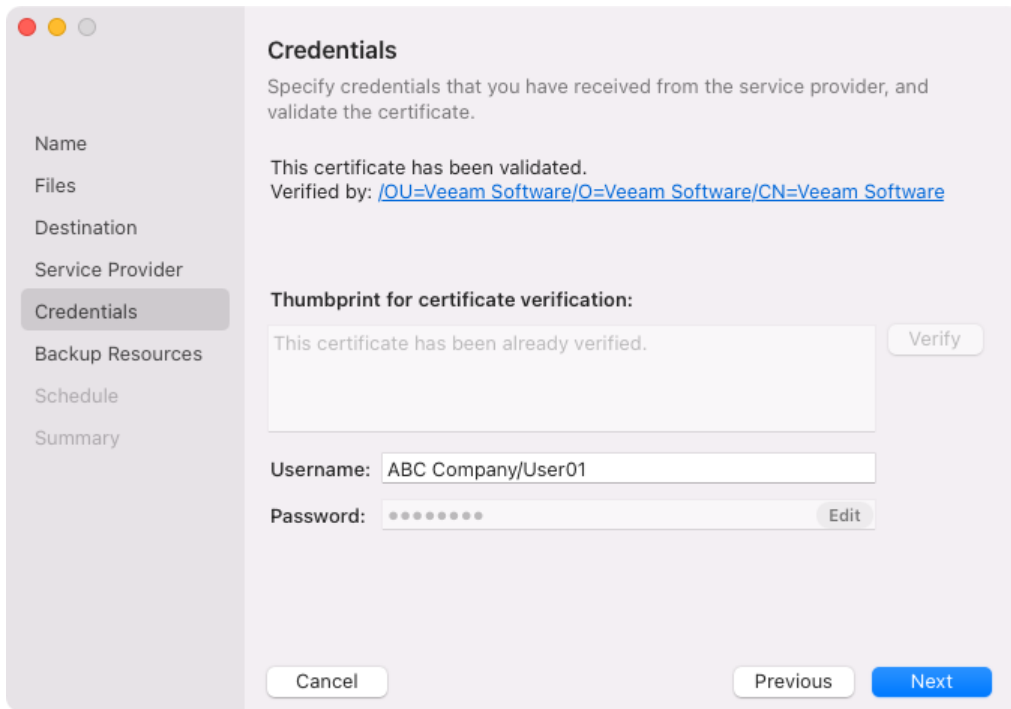
In the displayed dialog window, select one of the following options:

- **Yes** – select this option to immediately verify the certificate.
- **View** – starting from Veeam Agent version 2.1.2, select this option to view the details of the certificate. After you view the certificate details, select **Accept** to verify the certificate.
- **No** – select this option to cancel the certificate verification.



After the certificate is verified, you will automatically move to the **Backup Resources** step of the wizard.

[Starting from Veeam Agent version 2.1.2] you can, at any time, view the details of the verified certificate by clicking the active link in the **Verified by** field at the **Credentials** step of the wizard.



Selecting Cloud Repository

The **Backup Resources** step of the wizard is available if you have chosen to save backup files on a cloud repository and specified settings to connect to the SP.

Specify settings for the cloud repository:

1. From the **Available cloud repositories** list, select a cloud repository where you want to store created backups. The **Available cloud repositories** list displays only those cloud repositories that can be accessed by the tenant or subtenant account that you use to connect to the service provider.
2. In the **Retention policy** section, specify the number of **restore points** for Veeam Agent to store in the target location. By default, Veeam Agent keeps 7 restore points. To learn more, see [Backup Retention Policy](#).
3. Starting from version 2.1, you can use the GFS (Grandfather-Father-Son) retention scheme. To specify the GFS retention policy, select the **Keep certain full backups longer for archival purposes** check box and press **Configure**. In the **Configure GFS** window, specify how weekly, monthly and yearly full backups must be retained. For details, see [Specify GFS Retention Policy](#).

4. Click **Advanced** to specify advanced settings for the backup job. To learn more, see [Specify Advanced Backup Settings](#).

Backup Resources

The following are cloud backup repositories your service provider has assigned to you.

Available cloud repositories:

Repository	Free space	Capacity
User01 Cloud Vol	51,58 GB	161,06 GB

Retention policy:
7 restore points

Keep certain full backups longer for archival purposes
1 weekly, 1 monthly

Click Advanced to enable periodic full backups and encryption

Buttons: Cancel, Previous, **Next**, Finish

Step 6. Specify GFS Retention Policy

Starting from version 2.1, you can configure long-term, or Grandfather-Father-Son (GFS), retention policy for backups. For more information on GFS retention policy, see [Long-Term Retention Policy](#).

To configure GFS retention policy, do the following:

1. Select the **Keep certain full backups longer for archival purposes** option and press **Configure** at one of the following steps of the wizard:
 - **Local Storage** – if you have selected the **Local storage** option at the **Destination** step of the wizard.
 - **Network Share** – if you have selected the **Network Share** option at the **Destination** step of the wizard.
 - **Repository** – if you have selected the **Veeam backup repository** option at the **Destination** step of the wizard.
 - **Repository** – if you have selected the **Veeam Cloud Connect repository** option at the **Destination** step of the wizard.
 - **Bucket** – if you have selected the **Object storage** option at the **Destination** step of the wizard, then selected the **S3 compatible** option at the **Cloud Type** step of the wizard.
 - **Bucket** – if you have selected the **Object storage** option at the **Destination** step of the wizard, then selected the **Amazon S3** option at the **Cloud Type** step of the wizard.
 - **Bucket** – if you have selected the **Object storage** option at the **Destination** step of the wizard, then selected the **Google Cloud Storage** option at the **Cloud Type** step of the wizard.
 - **Bucket** – if you have selected the **Object storage** option at the **Destination** step of the wizard, then selected the **Microsoft Azure Blob Storage** option at the **Cloud Type** step of the wizard.
2. In the **Configure GFS** window, do the following:
 - a. If you want to create weekly restore points for archival purposes, select the **Keep weekly full backups for** check box. Then specify the GFS retention period in weeks. During this period, the restore points will be protected from modification and deletion.

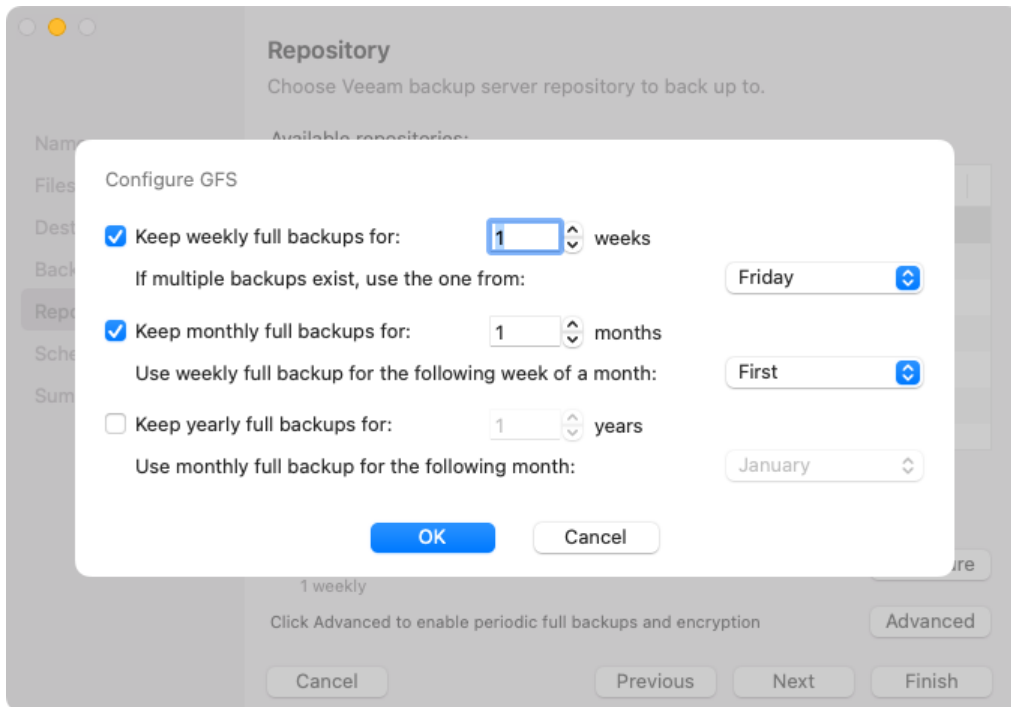
In the **If multiple full backups exist, use the one from** list, select a week day when Veeam Agent must assign the weekly GFS flag to a full restore point.
 - b. If you want to create monthly restore points for archival purposes, select the **Keep monthly full backups for** check box. Then specify the number of months during which you want to prevent restore points from being modified and deleted.

In the **Use weekly full backup for the following week of a month** list, select a week when Veeam Agent must assign the monthly GFS flag to a full restore point. A week equals 7 calendar days; for example, the first week of May is days 1–7, and the last week of May is days 25–31.
 - c. If you want to create yearly restore points for archival purposes, select the **Keep yearly full backups for** check box. Then specify the number of years during which you want to prevent restore points from being modified and deleted.

In the **Use monthly full backup for the following month** list, select a month when Veeam Agent must assign the yearly GFS flag to a full restore point.

NOTE

- If you select to assign multiple types of GFS flags, the flags begin to depend on each other. For more information on this dependency, see [Assignment of GFS Flags](#) section in the Veeam Backup & Replication User Guide.
- To use a GFS retention policy, you must set Veeam Agent to create full backups. To learn more, see [Backup Settings](#).



Step 7. Specify Advanced Backup Settings

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

- [Backup settings](#)
- [Maintenance settings](#)
- [Storage settings](#)

Backup Settings

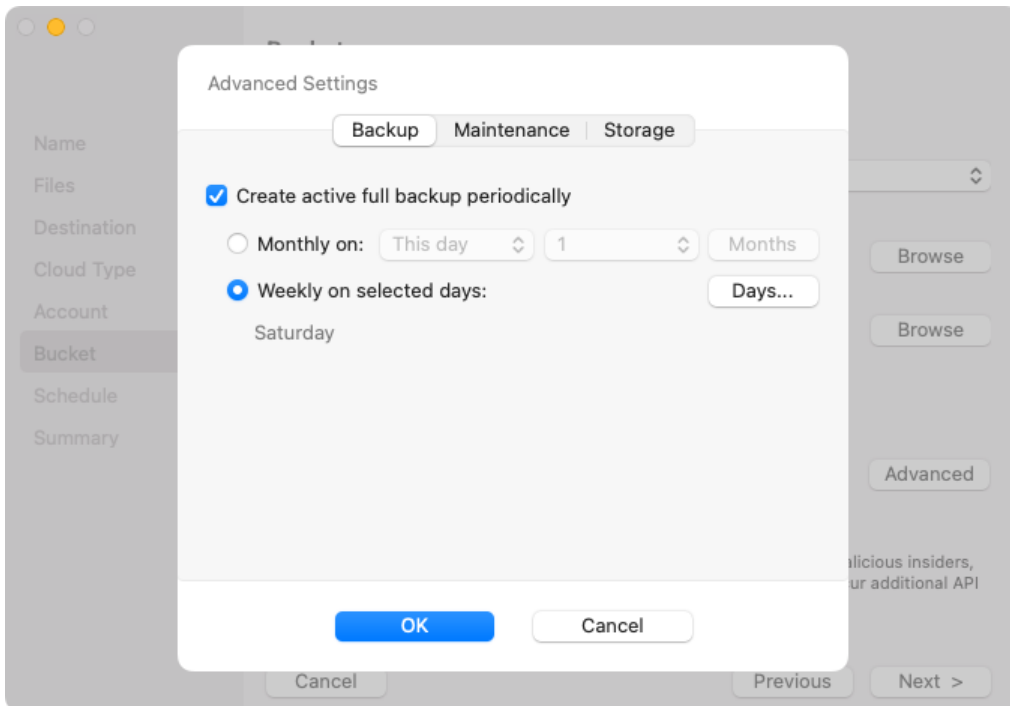
You can use advanced backup settings to schedule a periodic active full backup. For more information on this backup type, see [Active Full Backup](#)

NOTE

Before scheduling a periodic full backup, you must make sure that the target location for the scheduled backup job has enough free space.

To schedule an active full backup:

1. In the **Advanced Settings** window, select the **Backup** tab.
2. Select the **Create active full backups periodically** check box.
3. Use the **Monthly on** or **Weekly on selected days** options to define the schedule for active full backup.



Maintenance Settings

Depending on what storage option you have selected at the [Destination](#) step of the wizard, the **Maintenance** tab in the **Advanced Settings** window offers different settings:

- If you selected **Veeam backup repository** or **Veeam Cloud Connect repository** as a target for your backups, the **Maintenance** tab will display the setting that allows you to define how long the deleted backup files will be stored in the repository before they are permanently removed. For details, see [Configuring Removal of Deleted Items Data](#).
- If you selected **Object Storage** as a target for your backup, the **Maintenance** tab will display the setting that allows you to schedule a regular backup health check. For details, see [Scheduling Health Check](#).

NOTE

The **Maintenance** settings are not available if you have chosen **Local Storage** or **Network Share** as a backup target at the [Destination](#) step of the wizard.

Configuring Removal of Deleted Items Data

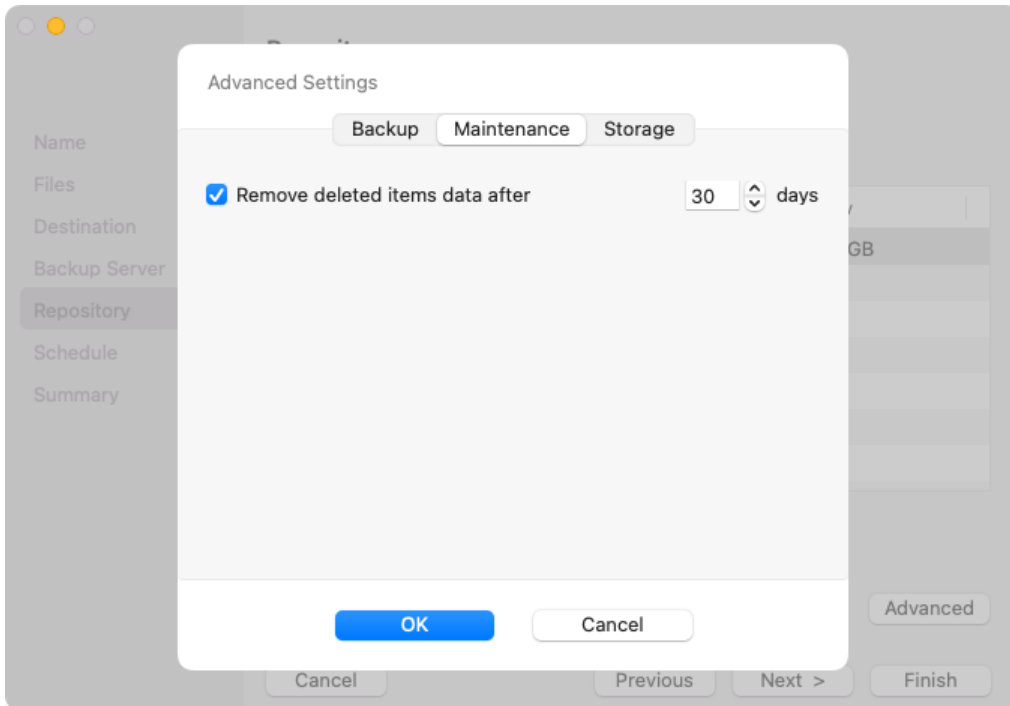
You can specify the number of days for which you want to keep the backup created with the backup job in the target location. If Veeam Agent does not create new restore points for the backup, the backup will remain in the target location for the period that you have specified. When this period is over, the backup will be removed from the target location.

By default, the retention period for outdated backups is 30 days. Do not set this retention period to 1 day or a similar short interval. In the opposite case, the backup job may work not as expected and remove data that you still require.

To specify the retention period for outdated backups, do the following:

1. In the **Advanced Settings** window, select the **Maintenance** tab.
2. Select the **Remove deleted items data after** check box.

3. Specify the number of days for the retention period.



Scheduling Health Check

When you store backup files in an object storage repository, an automatic health check can help you avoid a situation when a restore point gets corrupted, making all dependent restore points corrupted, too. For more information, see [Health Check for Object Storage](#).

NOTE

When you schedule a health check, consider the following:

- Health check runs automatically during incremental backup job session on the days specified in the health check schedule. If the backup job runs several times on a specified day, health check is performed only with the first run of the backup job on that day.

Health check is not performed during the first full backup or subsequent active full backup jobs.

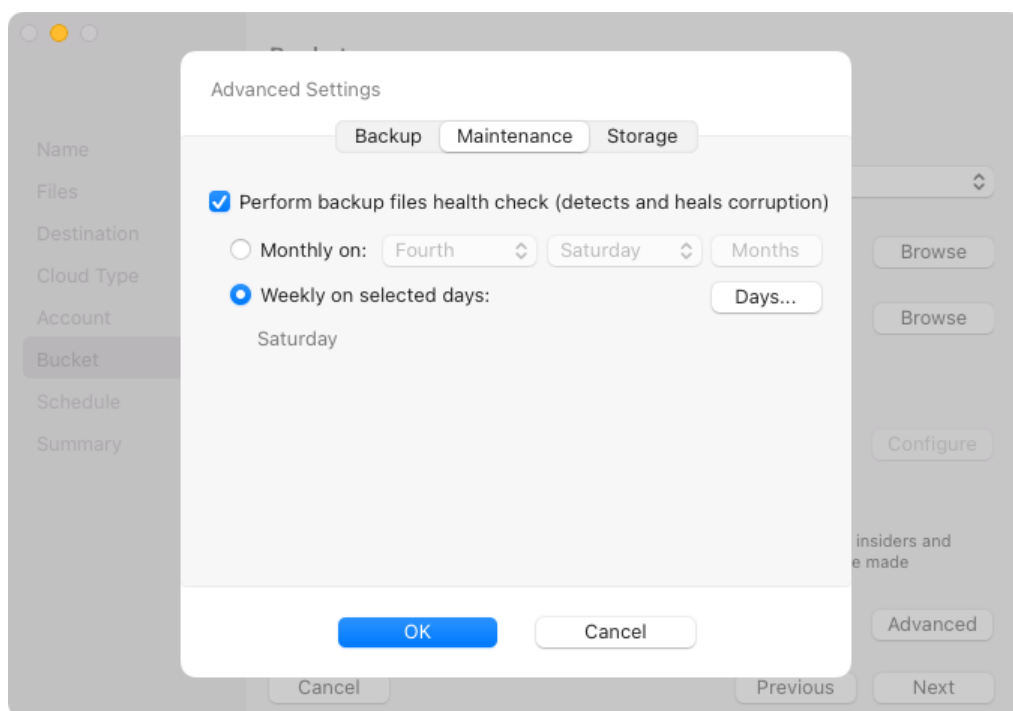
- If Veeam Agent does not run any backup jobs on the day specified in the health check schedule, health check will be performed during the first backup job session following that day.

For example, you may have scheduled to run health check every last day of a month, while the backup job is scheduled to run every day and create an active full backup on Sundays. If the last day of a month falls on a Sunday, health check will be performed on the following Monday with the first incremental backup job session on that day.

To periodically perform a health check of the backup, do the following:

1. In the **Advanced Settings** window, select the **Maintenance** tab.
2. Select the **Perform backup files health check** check box.

3. Use the **Monthly on** or **Weekly on selected days** options to define the schedule for the health check of the backup in the repository.

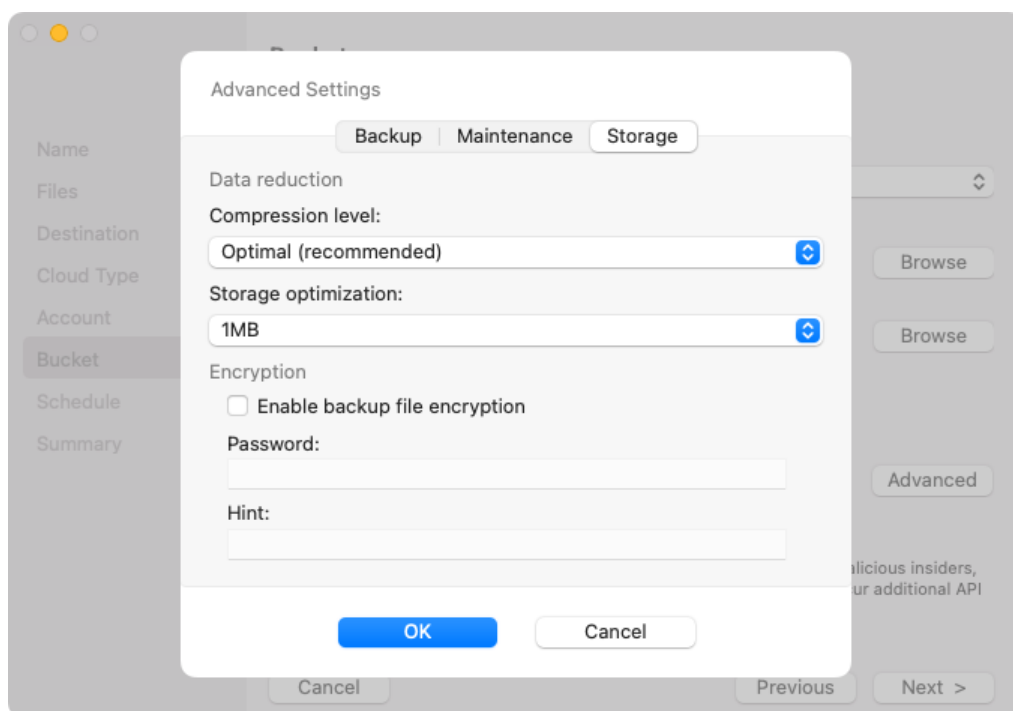


Storage Settings

To specify storage settings for the backup job:

1. In the **Advanced Settings** window, select the **Storage** tab.
2. In the **Compression level** field, select a compression level for the backup: *None*, *Dedupe-friendly*, *Optimal*, *High* or *Extreme*. For more information on compression levels, see [Data Compression](#).
3. In the **Storage optimization** field, select what type of backup target you plan to use: Local, LAN or WAN. Depending on the chosen storage type, Veeam Agent will use data blocks of different size to optimize the size of backup files and job performance. For more information on storage optimization, see [Data Compression](#).
4. If you want to encrypt the content of backup files, in the **Encryption** section, specify encryption settings for the backup job:
 - a. Select the **Enable backup file encryption** check box.
 - b. In the **Password** field, type a password that you want to use for encryption.

- c. In the **Hint** field, type a hint for the password. In case you lose the password, the specified hint will help you to remember the lost password.



NOTE

Consider the following:

- You cannot specify encryption options for the backup job if you have chosen to save backup files on a Veeam backup repository. Encryption of Veeam Agent backups stored on the backup repository are managed per repository by a backup administrator working with Veeam Backup & Replication. To learn more, see the [Data Encryption](#) and [Access Permissions](#) sections in the Veeam Backup & Replication User Guide.
- If you lose a password that was specified for encryption, you can change the password in the encryption settings. After the backup job creates a new restore point encrypted with the new password, you will be able to use this password to restore data from all restore points in the backup chain, including those restore points that were encrypted with an old password.
- If you enable encryption for the existing backup job that has already created one or more restore points, during the next job session, Veeam Agent will create active full backup. The created full backup file and subsequent incremental backup files in the backup chain will be encrypted with the specified password.
- Encryption is not retroactive. If you enable encryption for the existing backup job, Veeam Agent does not encrypt the previous backup chain created with this job.

Step 8. Define Backup Schedule

At the **Schedule** step of the wizard, specify the schedule according to which you want to perform backups. Backup job scheduling options differ depending on the edition of Veeam Agent for Mac:

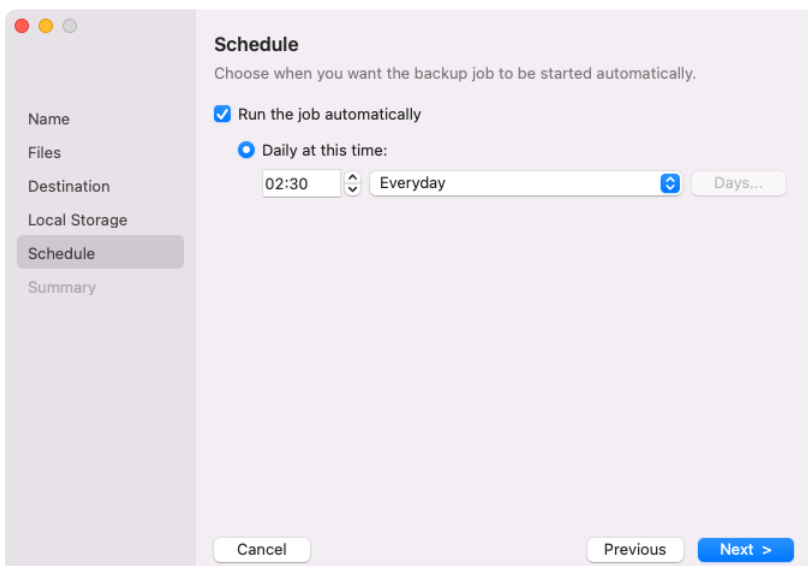
- [Scheduling Settings in Free and Workstation Editions](#)
- [Scheduling Settings in Server Edition](#)

Scheduling Settings in Free and Workstation Editions

In the Free and Workstation editions of Veeam Agent for Mac you can set up the time for Veeam Agent to run the backup job automatically on specific days.

1. Select the **Run the job automatically** check box. If this check box is not selected, you will have to start the backup job manually to create backup.
2. Specify the time to start the backup job.
3. In the drop-down next to the time field, select one of the available options:
 - *Everyday*— select this option to start the job at the specified time daily.
 - *On weekdays*— select this option to start the job at the specified time on every weekday.
 - *On these days*— select this option to start the job at the specified time on selected days.

When you choose this option, the **Days** field is activated. Click **Days** and select check boxes next to the necessary days of the week.



Scheduling Settings in Server Edition

In the Server edition of Veeam Agent for Mac you can set up Veeam Agent to run the backup job automatically daily, monthly or periodically. Starting from version 2.1, you can also specify settings for automatic retries in case of job failure.

To specify the job schedule:

1. Select the **Run the job automatically** check box. If this check box is not selected, you will have to start the backup job manually to create backup.
2. Define scheduling settings for the job:
 - To run the job at specific time daily, on defined week days or with specific periodicity, select **Daily at this time**. Use the fields of this option to configure the necessary schedule.
 - To run the job once a month on specific days, select **Monthly at this time**. Use the fields of this option to configure the necessary schedule.
 - To run the job repeatedly throughout a day with a specific time interval, select **Periodically every**. Use the fields of this option to specify the time interval in hours or minutes.

NOTE

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

3. If the backup job runs according to a schedule and fails for any reason, Veeam Agent will automatically retry the backup job 3 times with an interval of 10 minutes. Starting from version 2.1, you can specify the number of attempts to retry the failed backup job, as well as the period of time between retries. If you do not want to retry the backup job, clear the **Retry failed job** check box.

The screenshot shows the 'Schedule' configuration window in Veeam Agent. The window has a sidebar on the left with options: Name, Files, Destination, Backup Server, Repository, Schedule (highlighted), and Summary. The main area is titled 'Schedule' and contains the following settings:

- Run the job automatically:** (checked)
- Daily at this time:** (selected). Time: 00:30. Days: On these days. Days... button.
- Monthly at this time:** (unselected). Time: 00:30. Day: Fourth. Day of week: Saturday. Months... button.
- Periodically every:** (unselected). Interval: 1 Hours.
- Retry failed job:** (checked). Number of attempts: 3 times. Wait before each retry attempt for: 10 minutes.

At the bottom of the window are four buttons: Cancel, Previous, Next (highlighted in blue), and Finish.

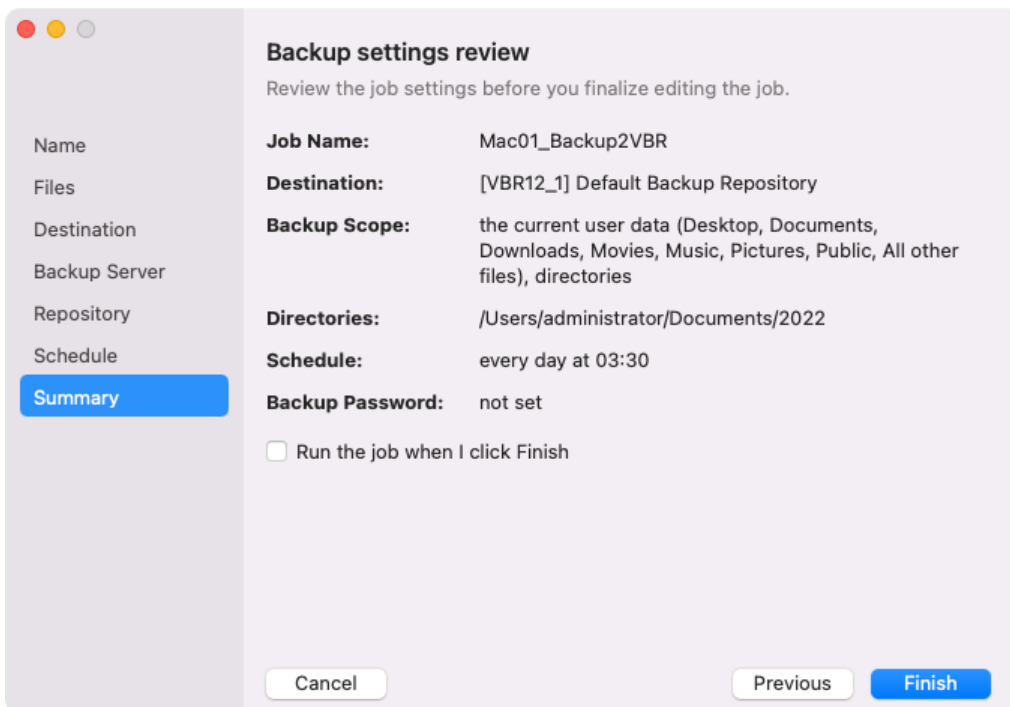
Step 9. Review Backup Job Settings

At the **Backup settings review** step of the wizard, complete the backup job configuration process.

1. Review settings of the configured backup job.
2. To automatically start the job after you close the wizard, make sure that the **Run the job when I click Finish** check box is selected.

If you want to start the backup job later, you can clear the **Run the job when I click Finish** check box. You will be able to start the backup job manually at any time you need. To learn more, see [Starting Backup Job](#).

3. Click **Finish to complete backup job configuration and exit the wizard**.



Creating Backup Job in Command Line Interface

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 backup job in command line interface, use the following command:

```
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 job.
- <repository_name> – name of the backup repository that should be used as a target location for the backup job. 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 job. 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 job. To learn more, see [Advanced Backup job Settings](#).
- <schedule_options> – schedule options for the backup job. To learn more, see [Schedule Settings](#).
- <active_full_backup_options> – active full backup schedule options for the backup job. To learn more, see [Active Full Backup Schedule Settings](#).
- --nosnap – option that sets Veeam Agent to perform the backup operation in the snapshot-less mode. For more information on snapshot-less mode, see [How Backup Works](#).

For example:

```
$ veeamconfig job create filelevel --name HomeFolderBackup --reponame NetworkRe
pository --includedirs /home/user --excludedirs /home/user/temp --excludemasks
*.pdf
```


TIP

Consider the following:

- You can specify backup schedule for the backup job after you create the backup job. For details, see [Configuring Backup Schedule](#).
- You can specify active full backup schedule for the backup job after you create the backup job. For details, see [Configuring Active Full Backup Schedule](#).
- [For object storage repository targets] You can specify a schedule for a backup health check. For details, see [Configuring Health Check Schedule](#).

File Inclusion Options

When you create a backup job, 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 job, you can use the following command-line options:

Option	Description and values
--includedirs	<p>Full path to a folder that should be included in backup, for example: <code>/home/user</code>.</p> <p>You can specify one or several paths to directories in the computer file system. To separate several paths, use the ',' (comma) character, for example: <code>/home/user/Documents, /home/user/reports</code>.</p> <p>Note: You cannot use UNIX wildcard characters in the paths to the folders you want to include.</p> <p>Tip: If you want to back up the root directory and specify the '/' (slash) character, Veeam Agent does not automatically include network file system mount points in the backup scope. To include such mount points, you need to specify paths to these mount points manually.</p> <p>For example, you have a network file system mounted to the <code>/home/media</code> directory. If you add '/' as an object to the backup scope, Veeam Agent will not back up the mounted network file system. To back up the root directory and the mounted network file system, add the following objects to the backup scope: <code>/, /home/media</code>.</p>
--excludedirs	<p>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 <code>--includedirs</code> option. To separate several paths, use the ',' (comma) character, for example, <code>/home/user/Documents, /home/user/reports</code>.</p> <p>Note: You cannot use UNIX wildcard characters in the paths to the folders you want to exclude.</p>

Option	Description and values
--includemasks	<p>Mask for file name or path that should be included in backup. You can use the following UNIX wildcard characters for file name masks:</p> <ul style="list-style-type: none"> • '*' – 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. <p>Keep in mind that you must specify all names with masks in double quotation marks (""). For example: <code>--includemasks "*.bak"</code>.</p> <p>If you want to use several file name masks, you must specify them in double quotation marks ("") and separated with a comma (,). For example: <code>--includemasks "*.bak,*.pdf"</code>.</p> <p>File inclusion option is applied to all directories that are specified with the <code>--includedirs</code> option. For example, if you include in backup the <code>/home/user/Documents</code> folder and files that match the <code>repor?.pdf</code> file name mask, Veeam Agent will back up the <code>/home/user/Documents/report.pdf</code> file and will not back up the <code>/home/user/reports/report.pdf</code> file.</p>

Option	Description and values
--excludemasks	<p>Mask for file name or path that should be excluded from backup. You can use the following UNIX wildcard characters for file name masks:</p> <ul style="list-style-type: none"> • '*' – 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. <p>Keep in mind that you must specify all names with masks in double quotation marks (""). For example: --excludemasks "*.bak".</p> <p>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".</p> <p>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:</p> <ul style="list-style-type: none"> • 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. <p>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.</p>

Advanced Backup Job Settings

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

Option	Description and values
--compressionlevel	<p>Data compression level. Possible values are:</p> <ul style="list-style-type: none">• 0 – None• 1 – Dedupe-friendly• 2 – Optimal• 3 – High• 4 – Extreme <p>For more information on compression levels, see Data Compression.</p>
--blocksize	<p>Data block size in kilobytes. Possible values are 256, 512, 1024 or 4096.</p> <p>The default value is <i>1024</i>.</p>
--maxpoints	<p>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.</p>
--immutabledays	<p>The time period in days during which the backup stored in an object storage repository will be immutable to modification or deletion. For more information, see Backup Immutability.</p>
--setencryption	<p>Defines that data encryption option is enabled for the job. When you use the <code>veeamconfig job create</code> command with the <code>--setencryption</code> option, Veeam Agent will prompt you to specify a password for data encryption and hint for the password.</p>
--deleteold	<p>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.</p> <p>If you do not specify the <code>--deleteold</code> option, Veeam Agent will not apply this setting. As a result, backup will be stored in the target location until you delete it manually.</p>

Schedule Settings

If you use Veeam Agent version 2.0, you can specify schedule options for the backup job to create backups daily or on specific weekdays at specific time. Starting from version 2.1, you can also configure more flexible monthly and periodic schedules by using the following options: `--weeknumber`, `--monthlyweekday`, `--months` and `--every`.

Option	Description and values
<code>--weekdays</code>	<p>[For weekly schedules] Specifies the weekdays when the backup job must run. If you want to run the backup job more than once during the week, the list of weekdays must be separated by a comma (','). Possible values are:</p> <ul style="list-style-type: none">• <i>Mon</i> – Monday• <i>Tue</i> – Tuesday• <i>Wed</i> – Wednesday• <i>Thu</i> – Thursday• <i>Fri</i> – Friday• <i>Sat</i> – Saturday• <i>Sun</i> – Sunday
<code>--daily</code>	<p>[For weekly schedules] Defines that the backup job must start daily at specific time.</p>
<code>--thisday</code>	<p>[For monthly schedules] Specifies the day of the month when the backup job must run. Possible values: from 1 to 31 or <i>Last</i>.</p>
<code>--weeknumber</code>	<p>[For monthly schedules] Specifies the week of the month when the backup job must run. Possible values: <i>First</i>, <i>Second</i>, <i>Third</i>, <i>Fourth</i> or <i>Last</i>. This option must be used in combination with the <code>--monthlyweekday</code> option.</p>
<code>--monthlyweekday</code>	<p>[For monthly schedules] Specifies the day of the week when the backup job must run. You can select only one weekday. Possible values are:</p> <ul style="list-style-type: none">• <i>Mon</i> – Monday• <i>Tue</i> – Tuesday• <i>Wed</i> – Wednesday• <i>Thu</i> – Thursday• <i>Fri</i> – Friday• <i>Sat</i> – Saturday• <i>Sun</i> – Sunday
<code>--months</code>	<p>[For monthly schedules] Specifies the months when the backup job must run. If you specify more than one month, the list must be separated by a comma (',') – for example: <i>Jan</i>, <i>Apr</i>, <i>Jul</i>, <i>Oct</i>. If you do not specify this option, the backup job will run every month.</p>

Option	Description and values
--every	[For periodic schedules] Specifies the period of time in minutes or hours between the runs of the backup job. The period must be specified in the <i>HH:MM</i> format – for example, <i>06:00</i> .
--at	[For weekly and monthly schedules] Specifies the time of day in the <i>HH:MM</i> format when the backup job must start – for example: <i>20:00</i> .

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

Active Full Backup Schedule Settings

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

If you use Veeam Agent version 2.0, you can specify schedule options for the backup job to create active full backups on specific days of the week or month. Starting from version 2.1, you can also configure more flexible monthly schedules for active full backups by using the following options: `--weeknumber-full`, `--monthlyweekday-full` and `--months-full`.

Option	Description and values
--weekdays-full	[For weekly schedules] Specifies the weekdays when the backup job must create an active full backup. If you want to create an active full backup more than once during the week, the list of weekdays must be separated by a comma (','). Possible values are: <ul style="list-style-type: none"> • <i>Mon</i> – Monday • <i>Tue</i> – Tuesday • <i>Wed</i> – Wednesday • <i>Thu</i> – Thursday • <i>Fri</i> – Friday • <i>Sat</i> – Saturday • <i>Sun</i> – Sunday
--thisday-full	[For monthly schedules] Specifies the day of the month when the backup job must create an active full backup. Possible values: from 1 to 31 or <i>Last</i> .
--weeknumber-full	[For monthly schedules] Specifies the week of the month when the backup job must create an active full backup.. Possible values: <i>First</i> , <i>Second</i> , <i>Third</i> , <i>Fourth</i> or <i>Last</i> . This option must be used in combination with the <code>--monthlyweekday</code> option.

Option	Description and values
<code>--monthlyweekday-full</code>	<p>[For monthly schedules] Specifies the day of the week when the backup job must create an active full backup. You can select only one weekday. Possible values are:</p> <ul style="list-style-type: none"> • <i>Mon</i> – Monday • <i>Tue</i> – Tuesday • <i>Wed</i> – Wednesday • <i>Thu</i> – Thursday • <i>Fri</i> – Friday • <i>Sat</i> – Saturday • <i>Sun</i> – Sunday
<code>--months-full</code>	<p>[For monthly schedules] Specifies the months when the backup job must create an active full backup. If you specify more than one month, the list must be separated by a comma (,) – for example: <i>Jan, Apr, Jul, Oct</i>. If you do not specify this option, the backup job will create an active full backup. every month.</p>

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

Configuring Backup Schedule

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

- [Specify schedule settings for the job.](#)
- [Enable schedule for the job.](#)
- [View the schedule defined for the job.](#)
- [Disable schedule for the job.](#)

TIP

You can also specify backup schedule for the backup job when you create the job. For details, see [Creating Standalone Backup Job](#).

Specifying Backup Schedule

Depending on the product edition, Veeam Agent allows you to set [daily](#), [monthly](#) or [periodic](#) schedule for a backup job. Daily schedules are available for the Free and Workstation editions of Veeam Agent. In the Server edition of Veeam Agent, you can additionally set monthly and periodic schedules for backup jobs. For details on Veeam Agent editions, see [Product Editions](#).

After you define the schedule, Veeam Agent automatically enables this schedule for the specified backup job.

Specifying Daily Schedules

You can set the backup job to run automatically on specific weekdays or every day.

- To run the backup job on specific days of the week, use the following command:

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

or

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

where:

- <job_id> – ID of the backup job for which you want to configure the schedule. You should look up the job ID in advance, before configuring the schedule – for example, with the `veeamconfig job list` command. To learn more, see [Viewing List of Backup Jobs](#).
- <job_name> – name of the backup job for which you want to configure the schedule.
- <days> – days when the backup job must start separated by a comma (','), for example: Monday, Tuesday, Wednesday, Thursday, Friday or Mon, Tue, Wed, Thu, Fri.
- <time> – time of day when the backup job must start specified in the HH:MM format – for example, 20:00.

For example:

```
user@srv01:~$ veeamconfig schedule set --jobname DailyBackup --weekdays Monday, Tuesday, Wednesday, Thursday, Friday --at 20:00
```

- To run the backup job every day, use the following command:

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

or

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

where:

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

- o `<time>` – time of day when the backup job must start specified in the `HH:MM` format – for example, `20:00`.

For example:

```
user@wrk01:~$ veeamconfig schedule set --jobid 4849a3ae-1935-4969-98a3-d8acd2f6c73f --daily --at 20:00
```

Specifying Monthly Schedules

You can set the backup job to run automatically on specific months or every month.

- To run the backup job monthly on a specific day of the specific week, use the following command:

```
veeamconfig schedule set --jobid <job_id> --monthlyweekday <day> --weeknumber <week> [--months <months>] --at <time>
```

or

```
veeamconfig schedule set --jobname <job_name> --monthlyweekday <day> --weeknumber <week> [--months <months>] --at <time>
```

where:

- o `<job_id>` – ID of the backup job for which you want to configure the schedule. You should look up the job ID in advance, before configuring the schedule – for example, with the `veeamconfig job list` command. To learn more, see [Viewing List of Backup Jobs](#).
- o `<job_name>` – name of the backup job for which you want to configure the schedule.
- o `<day>` – day of the week when the backup job must start – for example, `Tuesday` or `Tue`.
- o `<week>` – week of the month when the backup job must run. Possible values: `First`, `Second`, `Third`, `Fourth` or `Last`.
- o `<months>` – months when the backup job must run separated by a comma (','), – for example: `Jan, Apr, Jul, Oct`. If you do not specify this option, the backup job will run every month.
- o `<time>` – time of day when the backup job must start specified in the `HH:MM` format, – for example, `20:00`.

For example:

```
user@wrk01:~$ veeamconfig schedule set --jobname DailyBackup --monthlyweekday Mon --weeknumber Second --months Jan, Jul --at 20:00
```

- To run the backup job monthly on a specific day of the month, use the following command:

```
veeamconfig schedule set --jobid <job_id> --thisday <day> [--months <months>] --at <time>
```

or

```
veeamconfig schedule set --jobname <job_name> --thisday <day> [--months <months>] --at <time>
```

where:

- <job_id> – ID of the backup job for which you want to configure the schedule. You should look up the job ID in advance, before configuring the schedule – for example, with the `veeamconfig job list` command. To learn more, see [Viewing List of Backup Jobs](#).
- <job_name> – name of the backup job for which you want to configure the schedule.
- <day> – day of the month when the backup job must start. Possible values range from 1 to 31 or Last.
- <months> – months when the backup job must run separated by a comma (',') – for example: Jan, Apr, Jul, Oct. If you do not specify this option, the backup job will run every month.
- <time> – time of day when the backup job must start specified in the HH:MM format, – for example, 20:00.

For example:

```
user@wrk01:~$ veeamconfig schedule set --jobname DailyBackup --thisday 21 --months Jan,Jul --at 20:00
```

Specifying Periodic Schedules

To run the job periodically, run the following command:

```
veeamconfig schedule set --jobid <job_id> --every <time>
```

or

```
veeamconfig schedule set --jobname <job_name> --every <time>
```

where:

- <job_id> – ID of the backup job for which you want to configure the schedule. You should look up the job ID in advance, before configuring the schedule – for example, with the `veeamconfig job list` command. To learn more, see [Viewing List of Backup Jobs](#).
- <job_name> – name of the backup job for which you want to configure the schedule.
- <time> – period of time when the backup job must start specified in the HH:MM format, – for example, 06:00.

For example:

```
user@wrk01:~$ veeamconfig schedule set --jobname DailyBackup --every 12:00
```

Viewing Backup Schedule

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

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

or

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

where:

- <job_id> – ID of the backup job for which you want to view the schedule.
- <job_name> – name of the backup job for which you want to view the schedule.

Veeam Agent will display the details and the status (enabled or disabled) of the job schedule – 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
```

or

```
user@wrk01:~$ veeamconfig schedule show --jobid 4849a3ae-1935-4969-98a3-d8acd2f6c73f
Every 12 hours
Run automatically: enabled
```

Disabling Backup Schedule

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

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

or

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

where:

- <job_id> – ID of the backup job for which you want to disable the schedule.
- <job_name> – name of the backup job for which you want to disable the schedule.

For example:

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

Enabling Backup Schedule

After you define the schedule, Veeam Agent automatically enables this schedule for the specified backup job. If you disable the schedule for the backup job, you can enable it again by using the following command:

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

or

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

where:

- <job_id> – ID of the backup job for which you want to enable the schedule. You should look up the job ID in advance, for example, with the `veeamconfig job list` command. To learn more, see [Viewing List of Backup Jobs](#).
- <job_name> – name of the backup job for which you want to enable the schedule.

For example:

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

You can disable the schedule for the job at any time. To learn more, see [Disabling Backup Schedule](#).

Configuring Long-Term Retention Policy

Starting from version 2.1, you can configure the backup job to store backup files for long periods of time – for weeks, months and even years, you can set the long-term or Grandfather-Father-Son (GFS) retention policy. This policy uses backup files created while backup job is enabled and marks these backups with specific GFS flags. You can perform the following actions with the long-term retention policy in command line interface:

- [Specify long-term retention policy for the job.](#)
- [View the long-term retention policy defined for the job.](#)
- [Disable long-term retention policy for the job.](#)
- [Enable long-term retention policy for the job.](#)

Specifying Long-Term Retention Policy

You can configure long-term retention policy to keep [weekly](#), [monthly](#) or [yearly](#) full backups.

Configuring Long-Term Retention Policy to Keep Weekly Full Backups

To configure long-term retention policy to keep weekly full backups, use the following command:

```
veeamconfig gfs set --jobid <job_id> weekly --on <weekday> --keep <weeks>
```

or

```
veeamconfig gfs set --jobname <job_name> weekly --on <weekday> --keep <weeks>
```

where:

- `<job_id>` – ID of the backup job for which you want to configure the long-term retention policy. You should look up the job ID in advance, before configuring the schedule, for example, with the `veeamconfig job list` command. To learn more, see [Viewing List of Backup Jobs](#).
- `<job_name>` – name of the backup job for which you want to configure the long-term retention policy.
- `<weekday>` – week day when Veeam Agent must assign a weekly GFS flag to a full restore point – for example, `Tue` or `Tuesday`.
- `<weeks>` – number of weeks to keep the weekly GFS flag on the full restore point.

For example:

```
user@wrk01:~$ veeamconfig gfs set --jobid 4849a3ae-1935-4969-98a3-d8acd2f6c73f  
weekly --on Saturday --keep 1
```

Configuring Long-Term Retention Policy to Keep Monthly Full Backups

To configure long-term retention policy to keep monthly full backups, use the following command:

```
veeamconfig gfs set --jobid <job_id> monthly --on <week_number> --keep <months>
```

or

```
veeamconfig gfs set --jobname <job_name> monthly --on <week_number> --keep <months>
```

where:

- `<job_id>` – ID of the backup job for which you want to configure the long-term retention policy. You should look up the job ID in advance, before configuring the schedule, for example, with the `veeamconfig job list` command. To learn more, see [Viewing List of Backup Jobs](#).
- `<job_name>` – name of the backup job for which you want to configure the long-term retention policy.
- `<week_number>` – number of the week when Veeam Agent must assign a monthly GFS flag to a full restore point. Possible values: `First`, `Second`, `Third`, `Fourth` or `Last`.
- `<months>` – number of months to keep the monthly GFS flag on the full restore point.

For example:

```
user@wrk01:~$ veeamconfig gfs set --jobid 4849a3ae-1935-4969-98a3-d8acd2f6c73f
monthly --on Second --keep 6
```

Configuring Long-Term Retention Policy to Keep Yearly Full Backups

To configure long-term retention policy to keep yearly full backups, use the following command:

```
veeamconfig gfs set --jobid <job_id> yearly --on <month> --keep <years>
```

or

```
veeamconfig gfs set --jobname <job_name> yearly --on <month> --keep <years>
```

where:

- `<job_id>` – ID of the backup job for which you want to configure the long-term retention policy. You should look up the job ID in advance, before configuring the schedule, for example, with the `veeamconfig job list` command. To learn more, see [Viewing List of Backup Jobs](#).
- `<job_name>` – name of the backup job for which you want to configure the long-term retention policy.
- `<month>` – month when Veeam Agent must assign a yearly GFS flag to a full restore point – for example, `Jan` or `January`.
- `<years>` – number of years to keep the yearly GFS flag on the full restore point.

For example:

```
user@wrk01:~$ veeamconfig gfs set --jobid 4849a3ae-1935-4969-98a3-d8acd2f6c73f
yearly --on January --keep 3
```

Enabling Long-Term Retention Policy

To start marking backups with specific GFS flags, you must enable the long-term retention policy for the job. Use the following command:

```
veeamconfig gfs enable --jobid <job_id> [--type <period>]
```

or

```
veeamconfig gfs enable --jobname <job_name> [--type <period>]
```

where:

- `<job_id>` – ID of the backup job for which you want to enable the long-term retention policy. You should look up the job ID in advance, for example, with the `veeamconfig job list` command. To learn more, see [Viewing List of Backup Jobs](#).
- `<job_name>` – name of the backup job for which you want to enable the long-term retention policy.
- `<period>` – type of the long-term retention schedule. Possible values: `weekly`, `monthly` or `yearly`. This parameter is optional. You can use it to enable a specific type of long-term retention policy. To enable several types of retention at once, specify all necessary retention types separated by a comma (',') – for example: `weekly,monthly`.

For example:

```
user@wrk01:~$ veeamconfig gfs enable --jobid 4849a3ae-1935-4969-98a3-d8acd2f6c73f --type monthly
```

You can disable the long-term retention policy for the job at any time. To learn more, see [Disabling Long-Term Retention Policy](#).

Viewing Long-Term Retention Policy

To view the long-term retention policy defined for the backup job, use the following command:

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

or

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

where:

- `<job_id>` – ID of the backup job for which you want to view the long-term retention policy.
- `<job_name>` – name of the backup job for which you want to view the long-term retention policy.

Veeam Agent for Linux displays the following information about the backup job long-term retention policy:

Parameter	Description
GFS state	State of long-term retention policy. Possible values: <ul style="list-style-type: none">• GFS is enabled• GFS is disabled• GFS is not set
Enabled	Possible values: <code>true</code> or <code>false</code> .
Desired time	Weekday, week number or month when Veeam Agent will set the GFS flag on the full restore point.
Keep for	Period of time for retaining the GFS flag on the full restore point.

The information listed in the table above is displayed for weekly, monthly and yearly retention policies.

For example:

```
user@wrk01:~$ veeamconfig gfs show --jobid 4849a3ae-1935-4969-98a3-d8acd2f6c73f
GFS is enabled
Weekly:
  Enabled: true
  Desired time: Friday
  Keep for: 1 weeks
Monthly:
  Enabled: false
  Desired time: First
  Keep for: 1 months
Yearly:
  Enabled: false
  Desired time: January
  Keep for: 1 years
```

Disabling Long-Term Retention Policy

To disable the long-term retention policy for the backup job, use the following command:

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

or

```
veeamconfig gfs disable --jobname <job_name>
```

where:

- `<job_id>` – ID of the backup job for which you want to disable the long-term retention policy.

- `<job_name>` – name of the backup job for which you want to disable the long-term retention policy.

For example:

```
user@wrk01:~$ veeamconfig gfs disable --jobid 4849a3ae-1935-4969-98a3-d8acd2f6c73f
```

Configuring Active Full Backup Schedule

You can schedule a backup job to create active full backups periodically. You can specify active full schedule settings individually for every job created in Veeam Agent. 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 job when you create the job. For details, see [Backup Settings](#).

Specifying Active Full Backup Schedule

You can schedule a backup job to create active full backups on a specific day of the month or on specific week days.

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 job for which you want to configure the active full backup schedule. You should look up the job 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 job 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:

```
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:

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

or

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

where:

- **<job_id>** – ID of the backup job for which you want to configure the active full backup schedule. You should look up the job 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 job for which you want to configure the active full backup schedule.
- **<days>** – days when the backup job must create an active full backup separated by a comma (','). For example: `Monday, Friday`. The backup job will create an active full backup on the specified days at the time specified in the backup job schedule settings.

For example:

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

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

or

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

where:

- `<job_id>` – ID of the backup job for which you want to enable the active full backup schedule. You should look up the job 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 job 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 backup job 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 job, 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 job for which you want to view the active full backup schedule.
- `<job_name>` – name of the backup job 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:

Parameter	Description
Every <value>	Days on which the backup job creates active full backups. For example: <i>Every Monday</i> or <i>Every 1 day of every month</i> .
Run automatically	State of the active full backup schedule. Possible values: <ul style="list-style-type: none">• Enabled• Disabled

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 job, 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 job for which you want to disable the active full backup schedule.
- <job_name> – name of the backup job for which you want to disable the active full backup schedule.

For example:

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

Configuring Health Check Schedule

You can schedule a periodic [health check](#) of a backup that resides in an object storage repository. You can specify backup health check schedule settings individually for every backup job created in Veeam Agent for Mac or backup policy created in Veeam Backup & Replication. For more information on configuring backup health check in a backup policy, see the [Maintenance Settings](#) topic of the Veeam Agent Management Guide.

You can perform the following actions with backup health check schedule in command line interface:

- [Specify health check schedule.](#)
- [Enable health check schedule.](#)
- [View health check schedule.](#)
- [Disable health check schedule.](#)

Specifying Health Check Schedule

You can schedule a backup health check to run on a specific day of a specific month or on specific days of the week.

Specifying Monthly Health Check Schedule

IMPORTANT

Starting from Veeam Agent version 2.1.2, the `--thisday` option for the `veeamconfig healthcheck set` command is no longer available. If in a previous Veeam Agent version, the health check schedule was set to run on a specific day of the month using the `--thisday` option, after upgrade to version 2.1.2, the health check schedule will be automatically reset to the default weekly configuration to run every Saturday.

To instruct Veeam Agent to perform backup health check on a specific weekday of a month, use the following command:

```
veeamconfig healthcheck set --light --jobid <job_id> --monthlyweekday <day> --weeknumber <week> [--months <months>]
```

or

```
veeamconfig healthcheck set --light --jobname <job_name> --monthlyweekday <day> --weeknumber <week> [--months <months>]
```

where:

- `<job_id>` – ID of the backup job for which you want to configure health check schedule. You should look up the backup job ID before you configure the schedule – for example, with the `veeamconfig job list` command. To learn more, see [Viewing List of Backup Jobs](#).
- `<job_name>` – name of the backup job for which you want to configure the health check schedule.

TIP

If the name of the job consists of several words and contains spaces, use quote marks around the name – for example, `--jobName "Files Backup"`.

- `<day>` – day of the week when the backup job must perform health check – for example, `Tuesday` or `Tue`.
- `<week>` – week of the month when the backup job must perform health check. Possible values: `First`, `Second`, `Third`, `Fourth` or `Last`.
- `<months>` – months when the backup job must perform health check, separated by a comma (','), – for example: `Jan, Apr, Jul, Oct`. If you do not specify this option, the health check will run every month.

For example:

```
user@wrk01:~$ veeamconfig healthcheck set --light --jobname SystemBackup --monthlyweekday Fri --weeknumber Last --months Mar, Jun, Sep, Dec
```

Specifying Weekly Health Check Schedule

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

```
veeamconfig healthcheck set --light --jobid <job_id> --weekdays <days>
```

or

```
veeamconfig healthcheck set --light --jobname <job_name> --weekdays <days>
```

where:

- `<job_id>` – ID of the backup job for which you want to configure health check schedule. You should look up the backup job ID before you configure the schedule – for example, with the `veeamconfig job list` command. To learn more, see [Viewing List of Backup Jobs](#).
- `<job_name>` – name of the backup job for which you want to configure the health check schedule.

TIP

If the name of the job consists of several words and contains spaces, use quote marks around the name – for example, `--jobName "Files Backup"`.

- `<days>` – comma-separated list of days when the backup job must run backup health check. For example: `Mon,Fri`. The backup job will run the health check on the specified days at the time specified in the backup job schedule settings.

For example:

```
user@wrk01:~$ veeamconfig healthcheck set --light --jobname "System Backup" --weekdays mon,fri
```

Enabling Health Check Schedule

After you set health check schedule for a backup job, Veeam Agent automatically enables this backup health check schedule for the job. You can also enable health check schedule manually – for example, if you previously disabled it. To enable health check schedule, use the following command:

```
veeamconfig healthcheck enable --light --jobid <job_id>
```

or

```
veeamconfig healthcheck enable --light --jobname <job_name>
```

where:

- `<job_id>` – ID of the backup job for which you want to configure health check schedule. You should look up the backup job ID before you run the command to enable the schedule – for example, with the `veeamconfig job list` command. To learn more, see [Viewing List of Backup Jobs](#).

- `<job_name>` – name of the backup job for which you want to configure the health check schedule.

TIP

If the name of the job consists of several words and contains spaces, use quote marks around the name – for example, `--jobName "Files Backup"`.

For example:

```
user@wrk01:~$ veeamconfig healthcheck enable --light --jobname SystemBackup
```

You can disable health check schedule for a job at any time. To learn more, see [Disabling Health Check Schedule](#).

Viewing Health Check Schedule

To view the health check schedule defined for a backup job, use the following command:

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

or

```
veeamconfig healthcheck show --jobname <job_name>}
```

where:

- `<job_id>` – ID of the backup job for which you want to configure health check schedule. You should look up the backup job ID before you run the command to view the schedule – for example, with the `veeamconfig job list` command. To learn more, see [Viewing List of Backup Jobs](#).
- `<job_name>` – name of the backup job for which you want to configure the health check schedule.

TIP

If the name of the job consists of several words and contains spaces, use quote marks around the name – for example, `--jobName "Files Backup"`.

Veeam Agent for Mac displays the following information about the health check schedule:

Parameter	Description
Every <value>	Days on which the backup job runs the health check – for example, <i>Every last Fri of every month</i> .
Run health-check automatically	State of the backup health check schedule. Possible values: <ul style="list-style-type: none"> • Enabled • Disabled

For example:

```
user@wrk01:~$ veeamconfig healthcheck show --jobname SystemBackup
Every last Fri of Mar, Jun, Sep, Dec
Run health check automatically: enabled (light)
```

Disabling Health Check Schedule

To disable the health check schedule for a backup job, use the following command:

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

or

```
veeamconfig healthcheck disable --jobname <job_name>
```

where:

- `<job_id>` – ID of the backup job for which you want to configure health check schedule. You should look up the backup job ID before you run the command to disable the schedule – for example, with the `veeamconfig job list` command. To learn more, see [Viewing List of Backup Jobs](#).
- `<job_name>` – name of the backup job for which you want to configure the health check schedule.

TIP

If the name of the job consists of several words and contains spaces, use quote marks around the name – for example, `--jobName "Files Backup"`.

For example:

```
user@wrk01:~$ veeamconfig healthcheck disable --jobname SystemBackup
```


Starting and Stopping Backup Jobs

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 job schedule.

You can also start a backup job to 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.

You can stop a 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.

You can start and stop backup jobs in one of the following ways:

- [In the Veeam Agent control panel or status bar menu.](#)
- [In command line interface.](#)

Starting and Stopping Backup Jobs from Control Panel

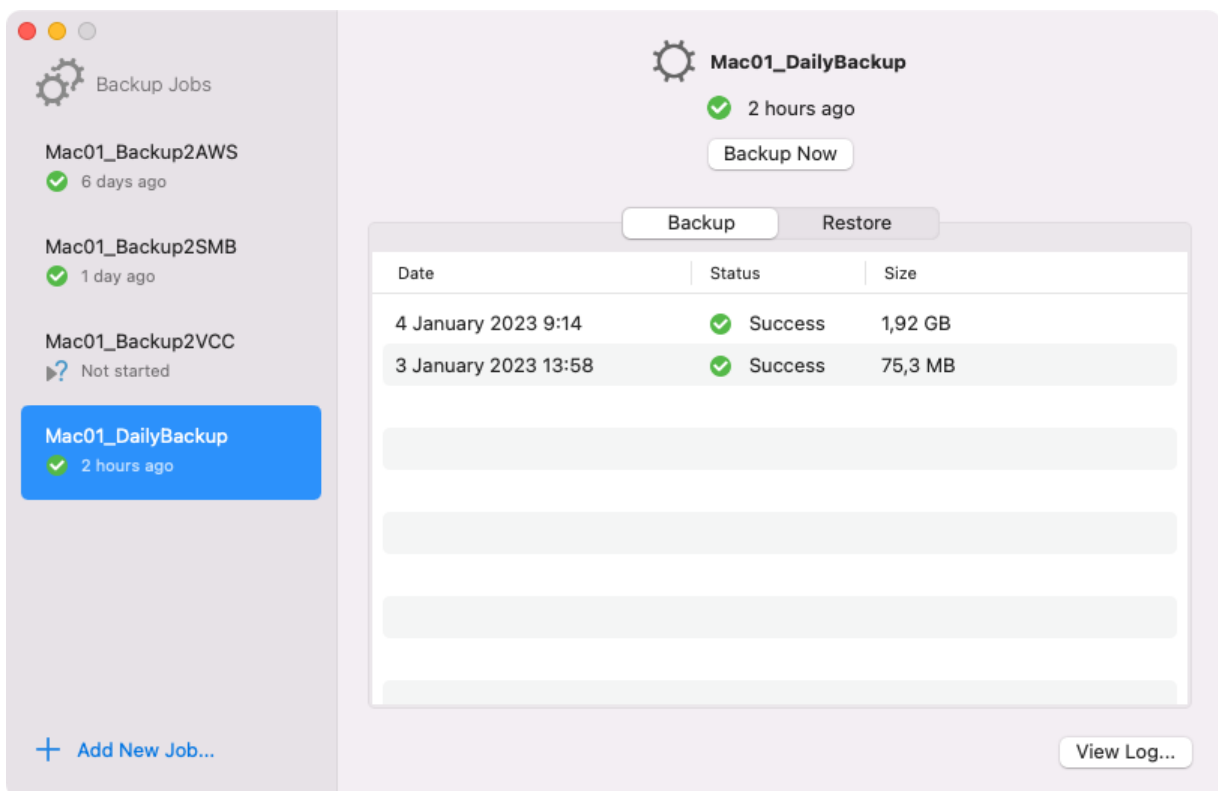
From the Veeam Agent control panel or status bar menu, you can perform the following operations to start or stop a backup job:

- [Start Backup Job](#).
- [Create Active Full Backup](#).
- [Stop Backup Job](#).

Starting Backup Job

In the Veeam Agent graphic user interface, you can start a backup job in one of the following ways depending on how many jobs are configured in Veeam Agent:

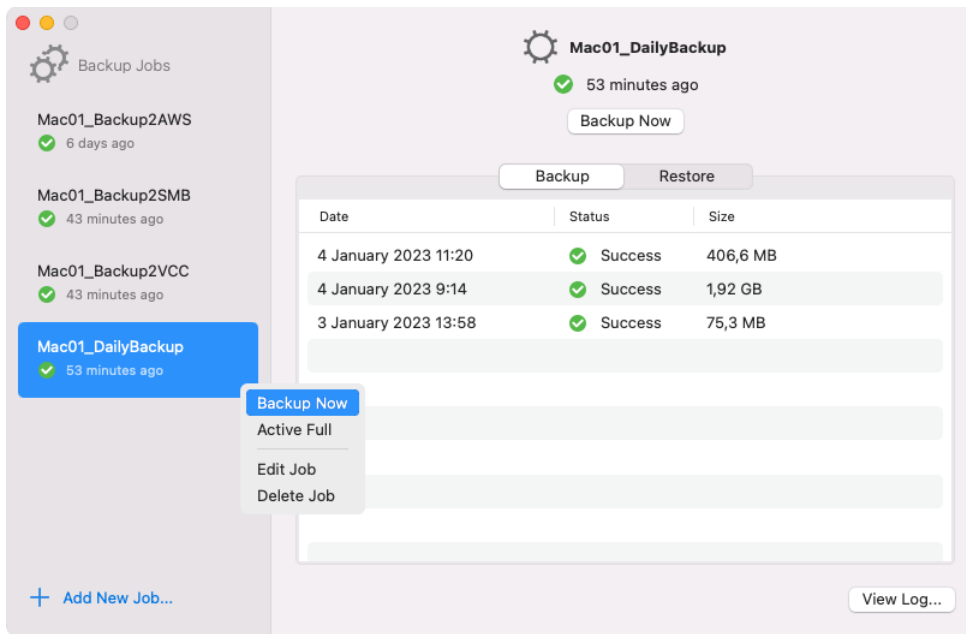
- [Any number of jobs] In the main pane of the control panel, press the **Backup Now** button under the name of the job in focus.



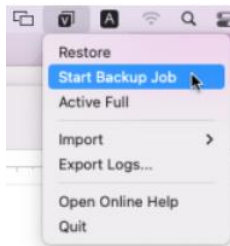
TIP

If there are more than one backup jobs, select the job you want to start in the left-hand **Backup Jobs** pane to set the job in focus and display its details in the main pane of the control panel. If you have only one backup job, this job is displayed in the main pane of the control panel by default.

- [Multiple jobs] In the **Backup Jobs** pane of the control panel, right-click the job that you want to start and select **Backup Now**.



- [Single job] From the Veeam Agent status bar menu, select the **Start Backup Job** option.

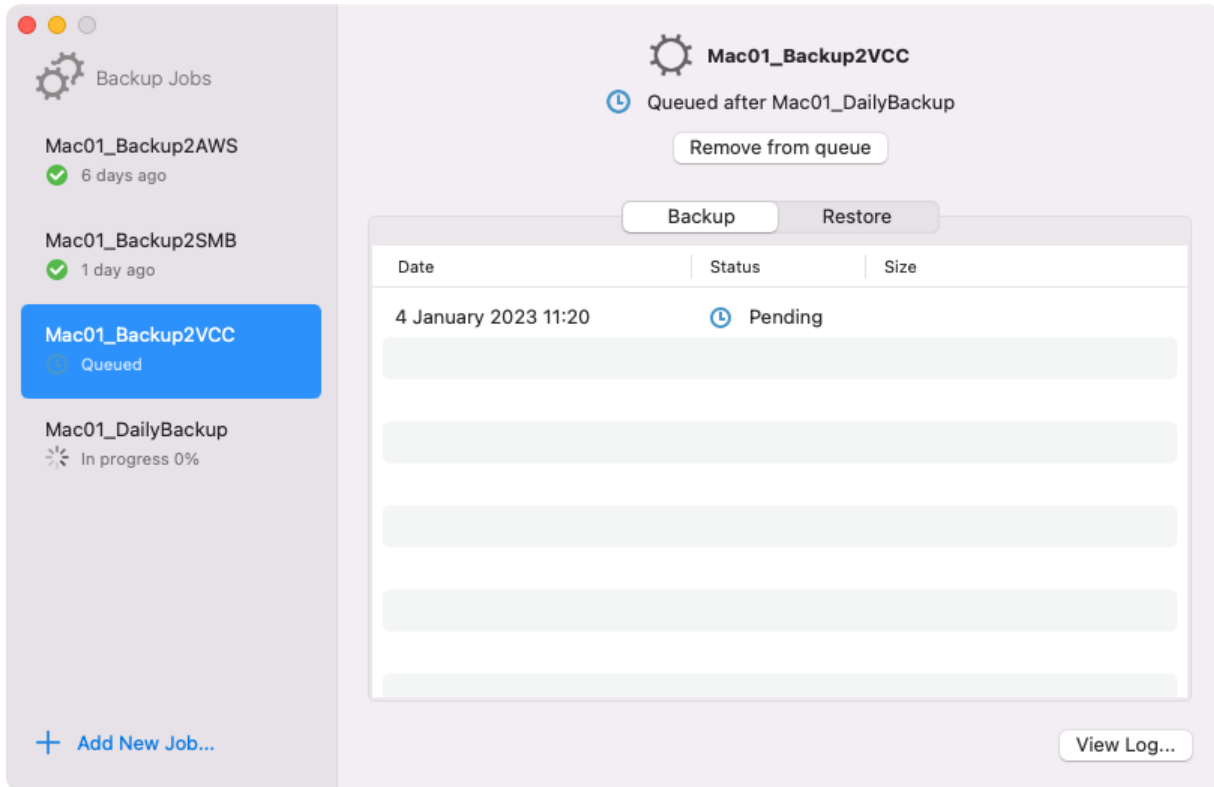


Veeam Agent will immediately start the backup job. You can monitor the progress of the backup job session and view the session log in real time. To do this, select a session and click the **View Log** button in the bottom-right corner of the Veeam Agent control panel. For details, see [Reporting with Veeam Agent Control Panel](#).

If you start the backup job while another backup job is running, Veeam Agent will perform the backup job immediately after the current job is completed. For details, see [Job Queue](#).

Job Queue

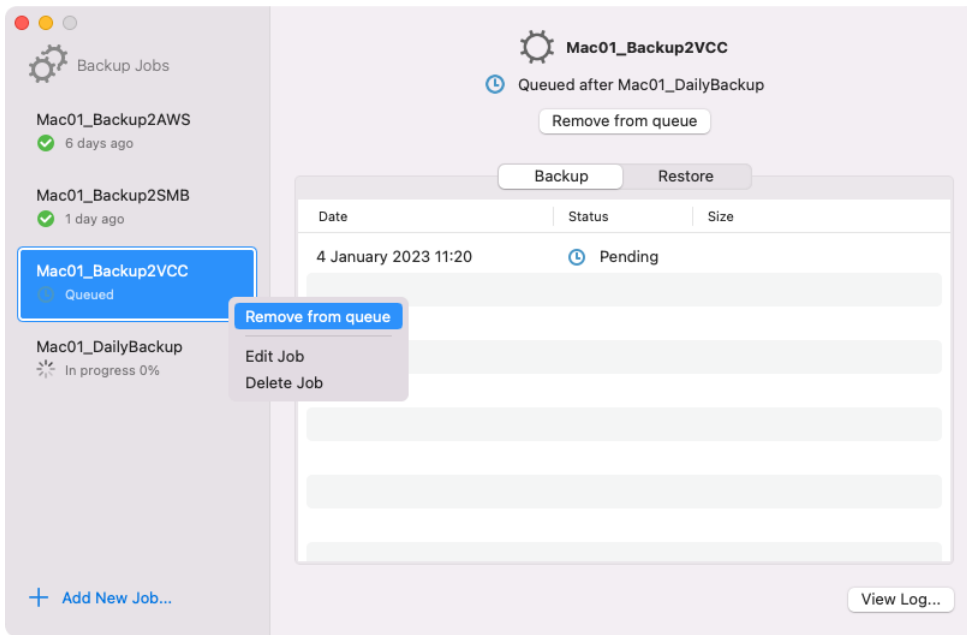
If another backup job is running when you start the backup job, Veeam Agent will submit this backup job to job queue. Veeam Agent will perform the job in the queue as soon as the previous job is completed. The queued backup job creates a new session with the *Pending* status. You can view all jobs in the queue in the **Backup Jobs** pane of the Veeam Agent control panel.



To cancel the backup job that is in the *Pending* status, do either of the following:

- In the main pane of the control panel, press the **Remove from queue** button under the name of the job in focus.

- In the **Backup Jobs** pane of the control panel, right-click the job that you want to start and select **Remove from queue**.



NOTE

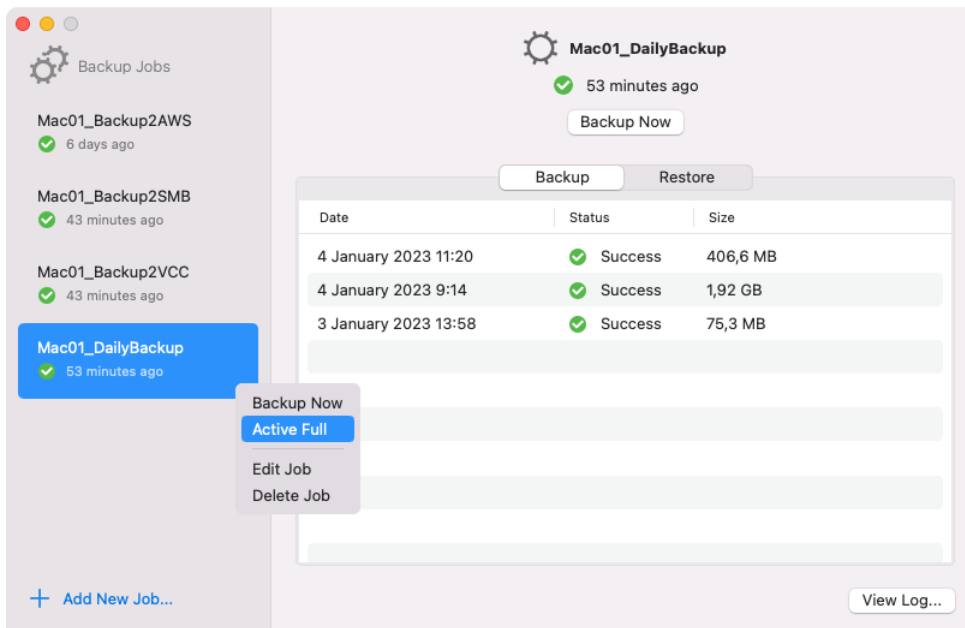
Consider the following about job queue:

- Job queue can contain up to 3 backup jobs besides the job that is already running.
- You cannot submit the same backup job to the queue if it is already running.

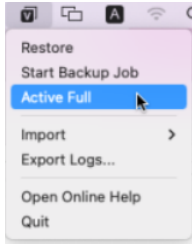
Creating Active Full Backup

In the Veeam Agent graphic user interface, you can create an ad-hoc active full backup in one of the following ways depending on how many jobs are configured in Veeam Agent:

- [Multiple jobs] In the **Backup Jobs** pane of the control panel, right-click the job that you want to run as an active full backup and select **Active Full**.



- [Single job] From the Veeam Agent status bar menu, select the **Active Full** option.

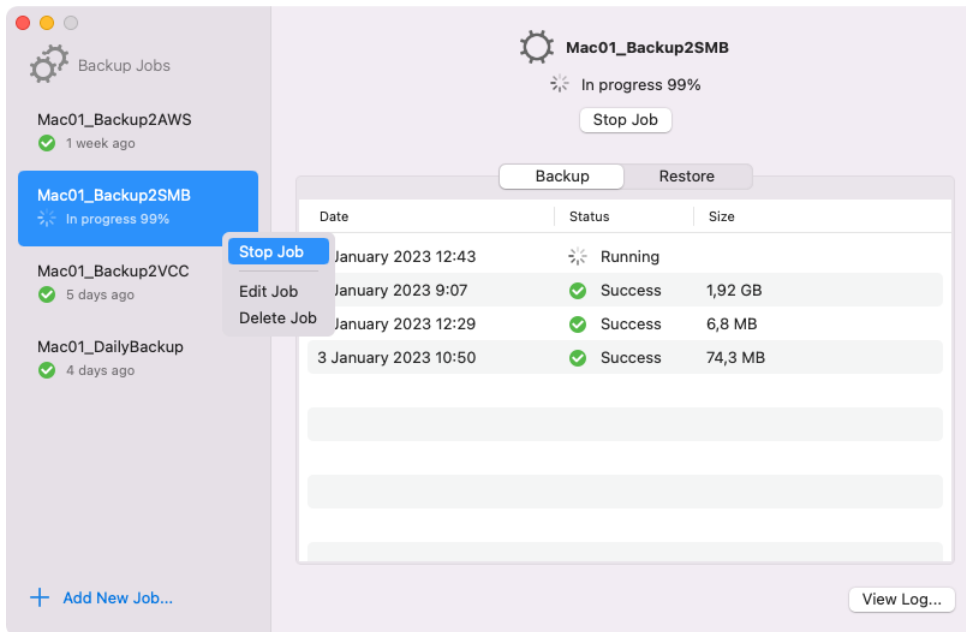


If you start an active full backup job while another backup job is running, Veeam Agent will perform the active full backup immediately after the current job is completed. For details, see [Job Queue](#).

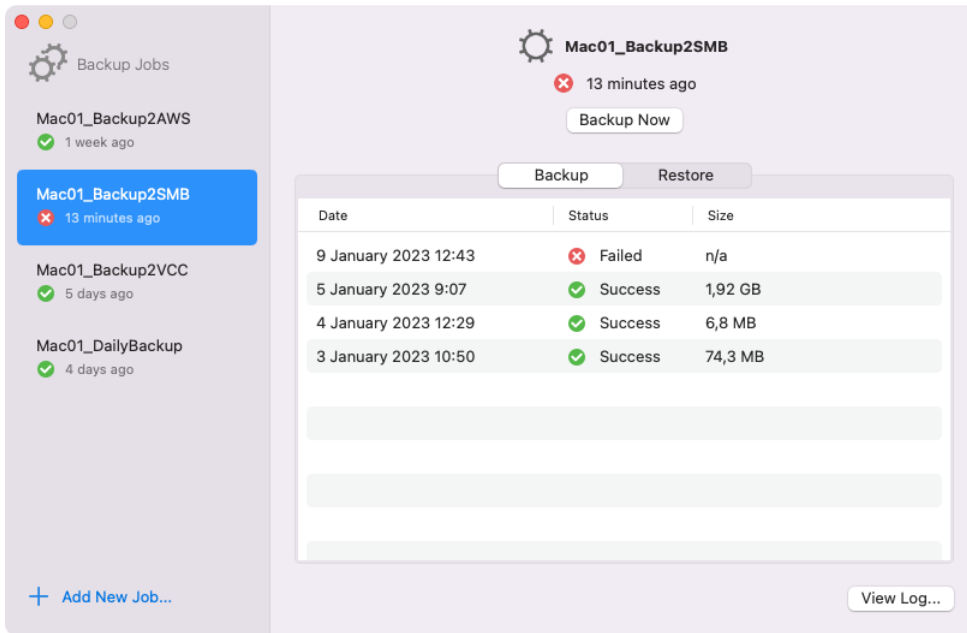
Stopping Backup Job

In the Veeam Agent graphic user interface, you can start a backup job in one of the following ways depending on how many jobs are configured in Veeam Agent:

- In the main pane of the control panel, press the **Stop Job** button under the name of the job in focus.
- In the **Backup Jobs** pane of the control panel, right-click the job that you want to stop and select **Stop Job**.



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.



Starting and Stopping Backup Jobs in Command Line Interface

In command line interface, you can perform the following operations to start or stop a backup job:

- [Start Backup Job](#).
- [Create Active Full Backup](#).
- [Stop Backup Job](#).

Starting Backup Job in CLI

You can start a backup job in the Veeam Agent 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.

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:

```
$ 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}].
```

Veeam Agent will immediately start the backup job. You can [check the backup job session status](#) or [view the backup job session log](#) using the Veeam Agent command line interface.

If you start the backup job while another backup job is running, Veeam Agent will perform the backup job immediately after the current job is completed. For details, see [Job Queue](#).

Job Queue

If another backup job is running when you start the backup job, Veeam Agent will submit this backup job to job queue. Veeam Agent will perform the job in the queue as soon as the previous job is completed.

```
$ veeamconfig job start --name ReportsBackup
Backup job has been added to the queue.
Session ID: [{10e8c599-b2aa-4008-89d9-af9b6e04aeba}].
Logs stored in: [/var/log/veeam/Backup/ReportsBackup/Session_20220913_153342_{10e8c599-b2aa-4008-89d9-af9b6e04aeba}].
```

The queued backup job creates a new session with the *Pending* status. You can view all jobs in the queue by running the `veeamconfig session list` command.

```
$ veeamconfig session list
Job name      Type      ID                               State      Started
at           Finished at
...
SystemBackup Backup {37427202-b139-4b36-9982-e0c33894d0cc} Running 2022-09
-13 15:33
ReportsBackup Backup {10e8c599-b2aa-4008-89d9-af9
b6e04aeba} Pending
```

NOTE

Consider the following about job queue:

- Job queue can contain up to 3 backup jobs besides the job that is already running.
- You cannot submit the same backup job to the queue if it is already running.

Creating Active Full Backup in CLI

In Veeam Agent command line interface, you can manually start a backup job to create an active full backup. To perform active full backup, you must configure a backup job first.

To start 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 job that you want to start to create an active full backup.
- `<job_id>` – ID of the backup job that you want to start to create an active full backup.

For example:

```
$ 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_{ce
864e24-8211-4df7-973a-741adce96fe7}].
```

You can view the progress for the active full backup session in the same way as for any other backup job session. In particular, you can [check the backup job session status](#) or [view the backup job session log](#) using the Veeam Agent command line interface.

If you start an active full backup job while another backup job is running, Veeam Agent will perform the active full backup immediately after the current job is completed. For details, see [Job Queue](#).

Stopping Backup Job in CLI

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:

```
$ veeamconfig session stop --id 381532f7-426a-4e89-b9fc-43d98942c71a
Session has stopped.
```

TIP

You can use the `veeamconfig session stop` command to remove a backup job with the *Pending* status from the job queue.

Managing Backup Jobs

You can view, edit and delete backup jobs:

- [In the Veeam Agent control panel.](#)
- [In command line interface.](#)

Managing Backup Jobs in Control Panel

In the Veeam Agent graphic user interface, you can perform the following actions with backup jobs:

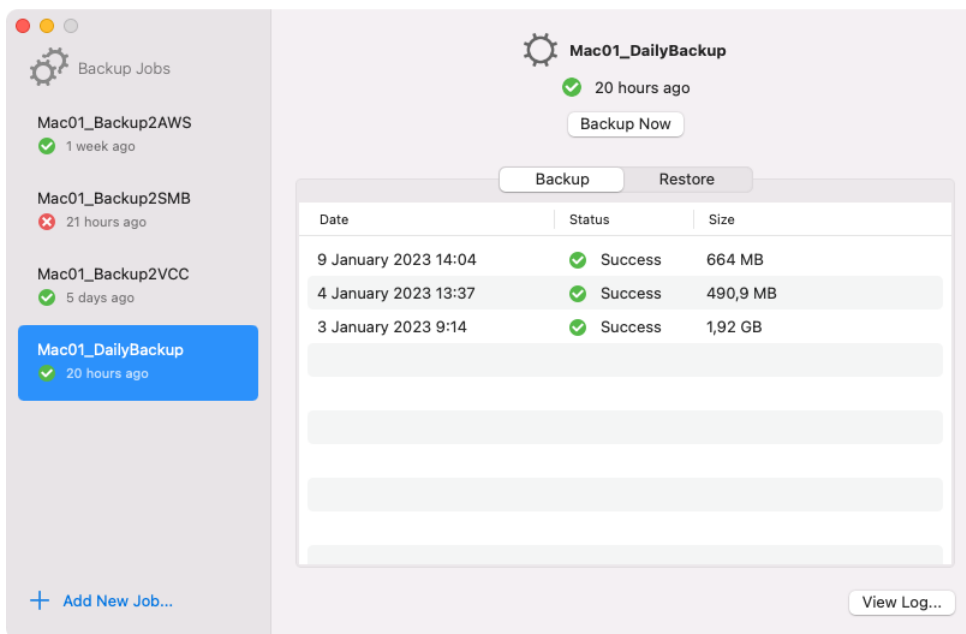
- [View the list of configured backup jobs.](#)
- [Edit backup job settings.](#)
- [Suspend all scheduled backups.](#)
- [Delete backup job.](#)

Viewing List of Backup Jobs

Multiple Backup Jobs

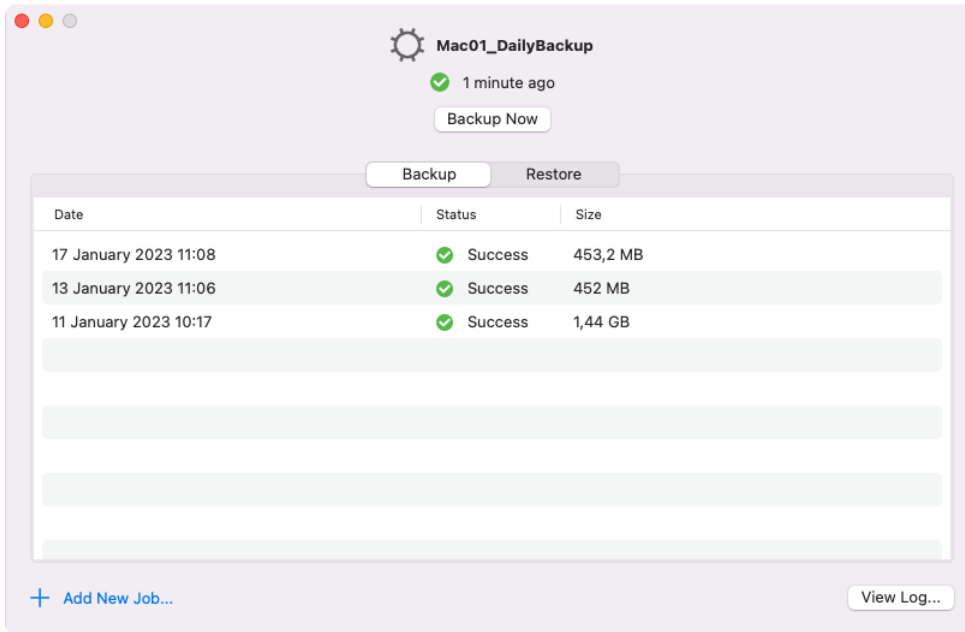
If you have more than one backup job configured in Veeam Agent, you can view the list of all the jobs in the **Backup Jobs** pane of the Veeam Agent control panel.

The backup jobs are sorted by the date and time of job creation: the more recently created jobs are displayed at the top of the list. Select a backup job to view the list of sessions for this backup job.



Single Backup Job

If you only have one configured backup job, Veeam Agent will display the list of the backup job sessions in the main pane of the control panel.



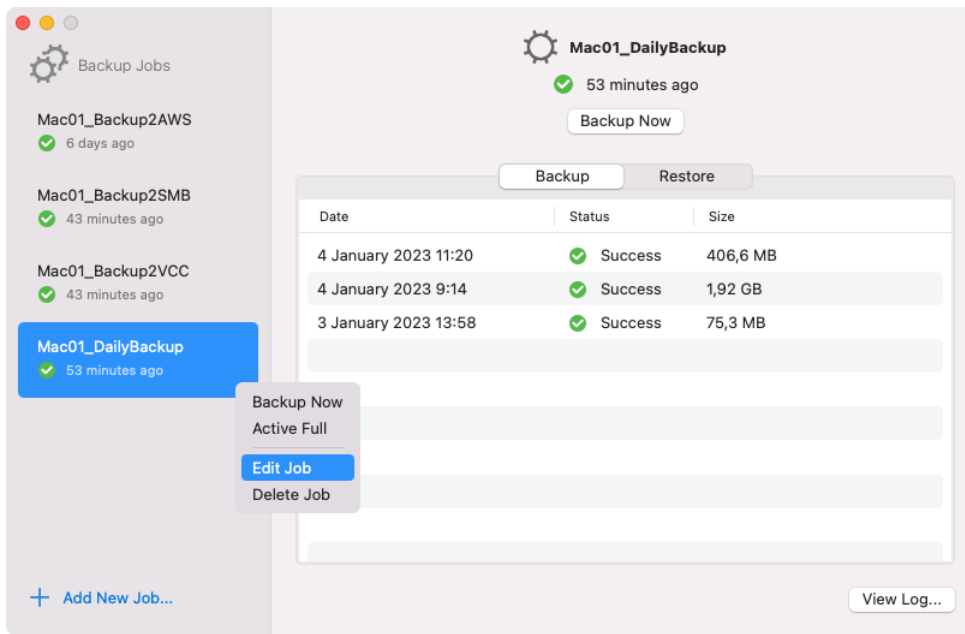
Editing Backup Job Settings

To edit an existing backup job, launch the Backup Job wizard by doing either of the following:

- In the **Veeam Agent for Mac** application menu, select **Backup > Edit Backup Job > <Job Name>**, where **Job Name** is the name of the job you want to edit.



- In the **Backup Jobs** pane of the Veeam Agent control panel, right-click the backup job you want to edit and select the **Edit Job** option from the context menu.



Veeam Agent will launch the Backup Job wizard. For details on backup job settings, see [Creating Backup Job with Backup Job Wizard](#).

Suspending Scheduled Backups

You can disable scheduled backups if you do not want to run automatic backups for some period of time. For example, you may want to put backup activities on hold if you plan to perform resource consuming operations on your computer at the time when the backup job is scheduled. After the operations are completed, you can enable scheduled backups again.

The disabling option is applicable to backup job sessions started upon schedule. You can create standalone full backups and perform ad-hoc incremental backup even if the scheduled backups are disabled.

The disabling option is applicable to all backup jobs configured in Veeam Agent for Mac. If you enable this option, all jobs that you configured will not start automatically upon the defined schedule. If you want to prevent a specific job from starting automatically, disable scheduling options in the properties of this job.

If you configured a backup job that is set up to create database log backups, after you disable scheduled backups, the database log backup job will be disabled, too.

The disabling option does not put on hold the backup cache synchronization process. If Veeam Agent has created one or more backup files in the backup cache, and then the backup target becomes available, Veeam Agent will immediately upload backup files to the target location.

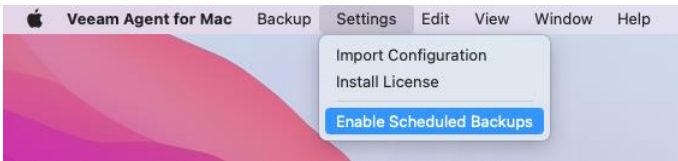
To disable scheduled backups:

1. From the Veeam Agent for Mac application menu, select **Settings**.
2. Select the **Disable scheduled backups** option.



To enable scheduled backups:

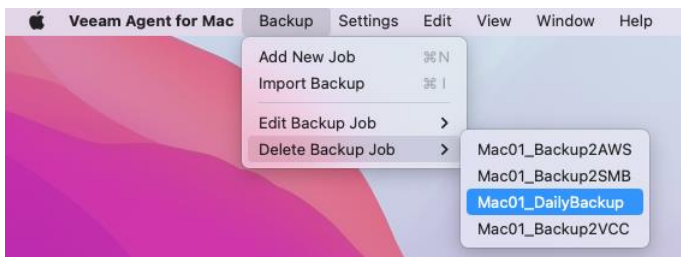
1. From the Veeam Agent for Mac application menu, select **Settings**.
2. Select the **Enable scheduled backups** option.



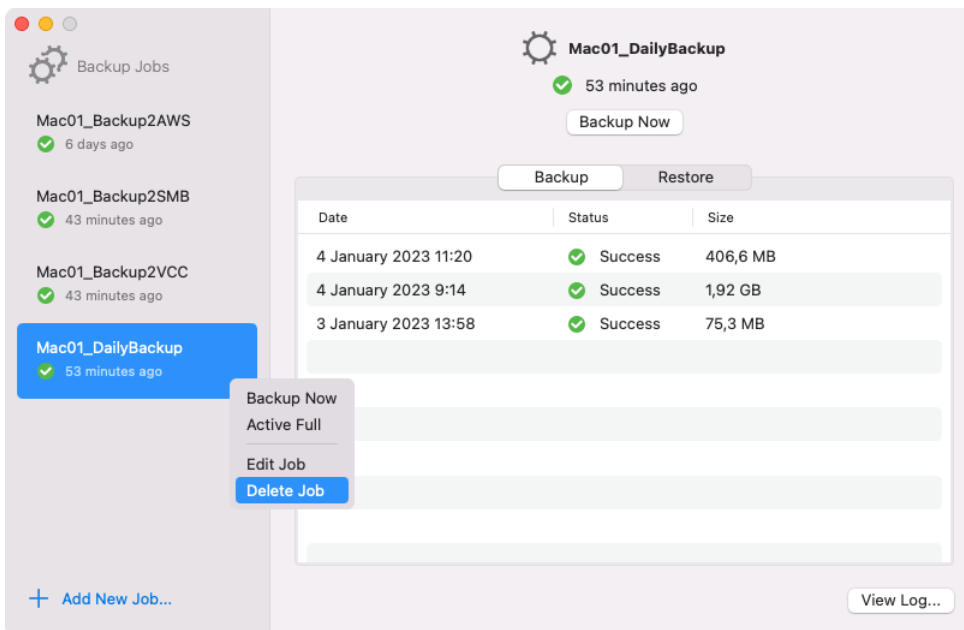
Deleting Backup Job

In the Veeam Agent graphic user interface, you can delete a backup job in one of the following ways:

- In the **Veeam Agent for Mac** application menu, select **Backup > Delete Backup Job > <Job Name>**, where **Job Name** is the name of the job you want to edit.



- In the **Backup Jobs** pane of the Veeam Agent control panel, right-click the backup job you want to edit and select the **Delete Job** option from the context menu.



Managing Backup Jobs in Command Line Interface

You can perform the following actions with backup jobs 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:

```
veeamconfig job list
```

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

Parameter	Description
Name	Name of the backup job.
ID	ID of the backup job.
Repository	Name of the backup repository that is specified as a backup storage for the backup job.

For example:

```
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:

Parameter	Description
ID	ID of the backup job.
Name	Name of the backup job.
Repository ID	ID of the backup repository that is specified as a backup storage for the backup job.
Repository name	Name of the backup repository that is specified as a backup storage for the backup job.
Creation time	Date and time of the backup job creation.
Compression	Data compression level. Possible values are: <ul style="list-style-type: none">• 0 – No compression• 1 – Rle• 2 – Lz4• 3 – ZlibLow• 4 – ZlibHigh
Max Points	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.
Block size	Size of data blocks that Veeam Agent uses to process data.
Retry count	Number of retries specified for the backup job.
Objects for backup	Backup scope specified for the backup job.
Schedule	Schedule specified for the backup job.

For example:

```
user@wrk01:~$ veeamconfig job info --name SystemBackup
Backup job
  ID: {2495911e-58db-4452-b4d1-f53dcfbc600e}
  Name: SystemBackup
  Repository ID: {4557ef7a-9c44-4f28-b8d0-44d78e5ddd5d}
  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:

Option	Description and values
--compressionlevel	Data compression level. Possible values are: <ul style="list-style-type: none">• 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 <i>1024</i> .
--immutabledays	The time period in days during which the backup stored in an object storage repository will be immutable to modification or deletion. For more information, see Backup Immutability .
--maxpoints	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.
--includedirs	Full path to a folder that should be included in backup, for example: <code>/home/user</code> . You can specify one or several paths to directories in the computer file system. To separate several paths, use a ',' (comma) character, for example: <code>/home/user/Documents,/home/user/reports</code> .
--excludedirs	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 <code>--includedirs</code> option. To separate several paths, use a ',' (comma) character, for example, <code>/home/user/Documents,/home/user/reports</code> .

Option	Description and values
--includemasks	<p>Mask for file name or path that should be included in backup.</p> <p>You can use the following UNIX wildcard characters for file name masks:</p> <ul style="list-style-type: none"> • '*' – 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. <p>To separate several masks, use a ',' (comma) character, for example, report.*,reports.*.</p> <p>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.</p>

Option	Description and values
--excludemasks	<p>Mask for file name or path that should be excluded from backup.</p> <p>You can use the following UNIX wildcard characters for file name masks:</p> <ul style="list-style-type: none"> • '*' – 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. <p>To separate several masks, use a ',' (comma) character, for example, report.*,reports.*.</p> <p>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:</p> <ul style="list-style-type: none"> • 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. <p>In this case, Veeam Agent will backup the /home/user/Documents/report.pdf file and will not backup /home/user/Documents/report.odt and /home/user/reports/report.pdf files.</p> <p>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 "*.bak,*.pdf".</p>
--setencryption	<p>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.</p>
--resetencryption	<p>Defines that data encryption option is disabled for the job. You can use this option to disable encryption for the existing backup job.</p>

Option	Description and values
--deleteold	<p>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.</p> <p>If the <code>--deleteold</code> 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.</p> <p>If you specified the value earlier and want to disable this setting, specify the <code>false</code> value for the option: <code>--deleteold false</code>. After the next successful backup session, this setting will be disabled for the backup in the target location.</p>

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:

```
$ veeamconfig job delete --name SystemBackup
```

Managing Backup Repositories

Veeam Agent for Mac allows you to manage backup repositories in two ways:

- [In the Veeam Agent control panel.](#)
- [In command line interface.](#)

Managing Backup Repositories in Control Panel

If you use the Veeam Agent control panel to perform backup tasks, you do not have to deal with creating backup repositories. When you specify a target location for the backup in the Backup Job wizard, Veeam Agent configures the backup repository automatically. Veeam Agent saves path to the specified backup location, assigns to this location a unique name and ID and saves this information in the database.

You can edit the repository properties in the settings of the backup job. For details, see [Specify Backup Storage Settings](#).

Managing Backup Repositories in Command Line Interface

You can perform the following operations with backup repositories in command line interface:

- [Create a backup repository](#)
- [View the list of backup repositories](#)
- [Edit backup repository settings](#)
- [Rescan Veeam backup repository](#)
- [Delete backup repository](#)

Creating Backup Repository

If you target the backup job at a local directory, network shared folder or object storage location, you must create a repository before you configure the backup job. To learn more, see the following topics:

- [Creating Repository in Local Folder](#)
- [Creating Repository in SMB Share](#)
- [Creating Repository in Object Storage](#)

IMPORTANT

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

If you target a backup job at a Veeam backup repository or Veeam Cloud Connect repository, you do not need to create repositories. Before configuring the backup job, you must connect to the Veeam backup server or Veeam Cloud Connect service provider. To learn more, see [Connecting to Veeam Backup Server](#) and [Connecting to Service Provider](#).

Creating Repository in Local Folder

To create a repository in a local folder, you specify a name for the repository and a local directory in which Veeam Agent will create backup files. To do this, use the following command:

```
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:

```
$ veeamconfig repository create --name VeeamBackup --location /home/backups
```

Creating Repository in SMB Share

To create a repository in an SMB share, you must specify a name for the repository, a path to the network shared folder in which Veeam Agent will create backup files, a type of the network shared folder and additional mounting options. To do this, 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.

IMPORTANT

If the directory to which the shared folder should be mounted resides on the backed-up volume, the backup job may fail.

- <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:

```
$ 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.

Creating Repository in Object Storage

To create a repository in an object storage location, you must specify a storage provider name, a name for the backup repository and settings for the object storage account and bucket or container.

Before You Begin

Before you start creating an object storage repository, consider the following:

- [Microsoft Azure Blob storage] The soft delete feature for blobs and containers must be disabled in the storage account.
- [Microsoft Azure Blob storage] To use the [Veeam backup immutability feature](#), you must enable blob versioning and version-level immutability support in the storage account. For more information, see [this Microsoft Azure documentation](#).
- [S3 Compatible and Amazon S3 storage] To use the [Veeam backup immutability feature](#), you must enable versioning and the S3 Object Lock feature in the storage account. For more information, see [this Amazon S3 documentation](#).
- [Google Cloud storage] The Veeam backup immutability feature is not supported for repositories configured in Google Cloud storage.

Creating Object Storage Repository

To create an object storage repository, use the following command:

```
veeamconfig objectstorage createrepository <provider_type> <options>
```

where:

- `<provider_type>` – name of the object storage provider. Veeam Agent supports the following options:
 - `azureblob` – for creating a Microsoft Azure Blob repository.
 - `google` – for creating a Google Cloud repository.
 - `amazons3` – for creating an Amazon S3 repository.
 - `s3compatible` – for creating an S3 Compatible repository (including WasabiCloud and IBM Cloud repositories).
- `<options>` – options necessary to connect to the target object storage. For more information, see the following subsections:
 - [Specifying options for S3 Compatible repository](#)
 - [Specifying options for Amazon S3 repository](#)
 - [Specifying Options for Google Cloud repository](#)
 - [Specifying options for Microsoft Azure Blob repository](#)

After Veeam Agent creates a new backup repository in the object storage location, you can specify object storage as a destination for the backup job.

Specifying Options for S3 Compatible Repository

To create a backup repository in an S3 compatible storage bucket, use the following command:

```
veeamconfig objectstorage createrepository s3compatible --name <repository_name> --servicepoint <address> --region <storage_region> --accesskeyid <id> [--fingerprint <ssl_thumbprint>] --bucketname <bucket_name> --folder <folder_name>
```

where:

- `<repository_name>` – name for the backup repository.
- `<address>` – address of the service point for the object storage.

NOTE

If you want to connect to the repository using the IPv6 address and the port number, you must use the following format: `IPv6:port`, where:

- `IPv6` is the IPv6 address of the object storage.
 - `port` is the number of the port that Veeam Agent will use to connect to the object storage.
- `<storage_region>` – region associated with the bucket.

NOTE

You can find the list of supported regions in the documentation of the selected storage provider.

- `<id>` – access key associated with the object storage account.
- `<ssl_thumbprint>` – fingerprint to verify the SSL certificate.
- `<bucket_name>` – name of the bucket.
- `<folder_name>` – name of the folder in the bucket.

If Veeam Agent does not find a folder with the name specified in the command, Veeam Agent will create a new folder in the bucket under `Veeam/Backup/` – for example, `Veeam/Backup/folder01`.

For example:

```
$ veeamconfig objectstorage createrepository s3compatible --name s3comp --servicepoint fd00:ca19:0:18b0:0:ac8a:abca:c942:9000 --accesskeyid S3ert1D9EIO9DjnZjuD4 --region us-east-1 --fingerprint <value> --bucketname backup01 --folder folder01
```

After you use the command, Veeam Agent will prompt you to specify a secret key associated with the object storage account. Enter the secret key to complete the creation of the repository.

Specifying Options for Amazon S3 Repository

To create a backup repository in an Amazon S3 bucket, use the following command:

```
veeamconfig objectstorage createrepository amazons3 --name <repository_name> --accesskeyid <id> --region <storage_region> --bucketname <bucket_name> --folder <folder_name>
```

where:

- <repository_name> – name for the backup repository.
- <id> – access key associated with the Amazon S3 storage account.
- <storage_region> – region associated with the bucket.

NOTE

You can find the full list of supported regions by storage provider in the `PublicCloudRegions.xml` file located in the `/Library/Application Support/Veeam` folder on Veeam Agent computer.

- <bucket_name> – name of the bucket.

IMPORTANT

You must create the bucket where you want to store your backup data beforehand. When you create a bucket, consider Amazon bucket naming rules. For example, it is not recommended that you use dots (.) in the bucket name. For more information on bucket naming rules, see [this AWS documentation article](#).

- <folder_name> – name of the folder in the bucket.

If Veeam Agent does not find a folder with the name specified in the command, Veeam Agent will create a new folder in the bucket under `Veeam/Backup/` – for example, `Veeam/Backup/folder01`.

For example:

```
$ veeamconfig objectstorage createrepository amazons3 --name amazon --accesskeyid AMAZONKIAWHDY4BDYCJC --region us-east-1 --bucketname bucket01 --folder folder01
```

After you use the command, Veeam Agent will prompt you to specify a secret key associated with the Amazon S3 storage account. Enter the secret key to complete the creation of the repository.

Specifying Options for Google Cloud Repository

To create a backup repository in a Google Cloud storage bucket, use the following command:

```
veeamconfig objectstorage createrepository google --name <repository_name> --accesskeyid <id> --region <storage_region> --bucketname <bucket_name> --folder <folder_name>
```

where:

- `<repository_name>` – name for the backup repository.
- `<id>` – access key associated with the Google Cloud storage account.
- `<storage_region>` – region associated with the bucket.

NOTE

You can find the full list of supported regions by storage provider in the `PublicCloudRegions.xml` file located in the `/Library/Application Support/Veeam` folder on Veeam Agent computer.

- `<bucket_name>` – name of the bucket.
- `<folder_name>` – name of the folder in the bucket.

If Veeam Agent does not find a folder with the name specified in the command, Veeam Agent will create a new folder in the bucket under `Veeam/Backup/` – for example, `Veeam/Backup/folder01`.

For example:

```
$ veeamconfig objectstorage createrepository google --name google --accesskeyid
GOOGLE56L5ATTDKJCLWUQG3E --region europe-west3 --bucketname backup01 --folder f
older01
```

After you use the command, Veeam Agent will prompt you to specify a secret key associated with the Google Cloud storage account. Enter the secret key to complete the creation of the repository.

Specifying Options for Microsoft Azure Blob Repository

To create a backup repository in a Microsoft Azure Blob container, use the following command:

```
veeamconfig objectstorage createrepository azureblob --name <repository_name> -
-account <storage_account_name> --region <storage_region> --bucketname <bucket_
name> --folder <folder_name>
```

- `<repository_name>` – name of the backup repository for the Veeam Agent database.
- `<account>` – name of the Microsoft Azure Blob storage account.
- `<storage_region>` – region associated with the container.

NOTE

Veeam Agent supports specification of 3 generic Microsoft Azure Blob storage locations:

- **Azure Global (Standard)** – can be used for any data center region, except the regions in China and the regions intended for US governments. To specify this region in the command to create the repository, use the following value: `AzureCloud`.
- **Asia China** – can be used for any region in China. To specify this region in the command to create the repository, use the following value: `AzureChinaCloud`.
- **Azure Government** – can be used for Azure Government regions only. To specify this region in the command to create the repository, use the following value: `AzureGovernmentCloud`.

You can find the full list of supported regions by storage provider in the `PublicCloudRegions.xml` file located in the `/Library/Application Support/Veeam` folder on Veeam Agent computer.

- `<bucket_name>` – name of the container.
- `<folder_name>` – name of the folder in the container.

If Veeam Agent does not find a folder with the name specified in the command, Veeam Agent creates a new folder in the container under `Veeam/Backup/` – for example, `Veeam/Backup/folder01`.

For example:

```
$ veeamconfig objectstorage createrepository azureblob --name azure --account my-account --region azurecloud --bucketname backup01 --folder folder01
```

After you use the command, Veeam Agent will prompt you to specify the shared key associated with the object storage account. Enter the shared key to complete the creation of the repository.

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:

Parameter	Description
Name	Name of the backup repository.
ID	ID of the backup repository.

Parameter	Description
Location	Location of the backup repository. Depending on the repository type, this column can contain one of the following: <ul style="list-style-type: none"> • Path to the local or network shared folder. • Name of the Veeam backup server that manages the repository. • Details of the cloud storage location of the repository.
Type	Type of the backup repository. Possible values: <ul style="list-style-type: none"> • local – local directory of the protected computer. • SMB – network shared folder. • backup server – Veeam backup repository. • cloud – Veeam Cloud Connect repository. • object storage – object storage repository (Amazon S3, S3 Compatible, Google Cloud or Microsoft Azure Blob).
Accessible	Availability of the backup repository. Possible values: <ul style="list-style-type: none"> • true • false
Backup server	Backup server on which Veeam backup repository added to Veeam Agent is configured.

For example:

```

$ veeamconfig repository list
Name      ID                               Location      Typ
e Accessible Backup server
BackupVol01 {818e3a0f-8155-4a51-9430-248a203a43d1} /home/backups local
l true
BackupVol02 {2155a2e7-a1e9-4347-9d8b-cf8f3a6f3fcb} /home/backups2 local
l true
BackupVol03 {dd593314-9511-4153-8326-9e0470f7ffc5} //server/VeeamBackups SMB
B true

```

Editing Backup Repository Settings

In command line interface, you can edit settings for a backup repository created with Veeam Agent for Mac in a local or network shared folder.

You can edit properties of the following repository types only in the backup job settings in the Veeam Agent control panel:

- Veeam backup repository.
- Veeam Cloud Connect repository.
- Object storage repository.

You can edit the following properties for a backup repository that resides in a local or network shared folder:

- [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:

```
$ 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:

```
$ 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:

```
$ 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:

```
$ 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
```

NOTE

When you use the `veeamconfig repository rescan` command with the `--all` option, consider the following:

- Rescanning can take significant amount of time if there are multiple repositories configured in Veeam Agent.
- Rescanning multiple object storage repositories may result in greater storage costs due to additional volume of data transactions.

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:

```
$ 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.

Managing Veeam Backup 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

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 used 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.

TIP

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:

Parameter	Description
Name	Name of the Veeam backup server.
ID	ID of the Veeam backup server in the Veeam Agent database.
Endpoint	IP address of the Veeam backup server and port over which Veeam Agent for Mac communicates with Veeam Backup & Replication.

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:

Parameter	Description
ID	ID of the Veeam backup server in the Veeam Agent database.
Name	Display name of the Veeam backup server.
Endpoint	IP address of the Veeam backup server and port over which Veeam Agent for Mac communicates with Veeam Backup & Replication.
Login	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.

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:

```
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:

```
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:

```
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:

```
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 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:

```
veeamconfig 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:

```
user@wrk01:~$ veeamconfig cloud add --name SP --address 172.17.53.15 --port 6180
--login TechCompany/User01 --password P@ssw0rd --fingerprint 92FA988A3D9E80EE
095DDAB75BF06B05DF6F205B
```

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:

Parameter	Description
Name	Name of the service provider.
ID	ID of the service provider in the Veeam Agent database.
Address	IP address of the cloud gateway and port over which Veeam Agent communicates with the cloud gateway.
Gate servers	IP address of the cloud gateway and port over which Veeam Agent communicates with the cloud gateway.
Username	Name of the tenant or subtenant account used for connection to the service provider.

For example:

```
user@wrk01:~$ veeamconfig cloud list
Name          ID                               Address          Gate
servers      Username
SP            {0840f770-354d-426a-b5ce-1aa80f56cc08} 172.17.53.15:618
0              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:

```
veeamconfig cloud edit --fingerprint <sp_thumbprint> for --name <sp_name>
```

or

```
veeamconfig cloud edit --fingerprint <sp_thumbprint> for --id <sp_id>
```

where:

- <sp_thumbprint> – thumbprint used to verify the TLS certificate and connect to the service provider.
- <sp_name> – name of the SP.
- <sp_id> – ID of the SP.

For example:

```
user@wrk01:~$ veeamconfig cloud edit --fingerprint 92FA988A3D9E80EE095DDAB75BF0  
6B05DF6F205B 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:

```
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:

```
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:

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

or

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

where:

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

For example:

```
user@wrk01:~$ veeamconfig cloud delete --name SP
```

Performing Restore

If you experience a problem with your computer and your data gets lost or corrupted, you can restore computer [user profiles](#) or [specific files and folders](#) from a backup file.

If for some reason, Veeam Agent does not have access to the backup file from which you want to restore data, you can [import the backup file](#) to your computer.

Veeam Agent also allows you to view the list of available backups and restore points within those backups, as well as browse backup content and delete backups. For details, see [Managing Backups](#).

Importing Backups

If the backup file from which you need to restore data is not available in Veeam Agent on your computer, you can import the necessary backup file created by Veeam Agent for Mac into the Veeam Agent database. A backup file may be unavailable in the following situations:

- The backup file was created by a Veeam Agent installed on another computer.
- Due to a disaster, the Veeam Agent and Veeam Agent database on your computer have been removed, and the database of the re-installed Veeam Agent does not contain information on the previously created backup file.
- The backup file was deleted from the repository.

Veeam Agent lets you to import backup files in the following ways:

- [With Veeam Agent Status Bar Menu.](#)
- [In command line interface.](#)

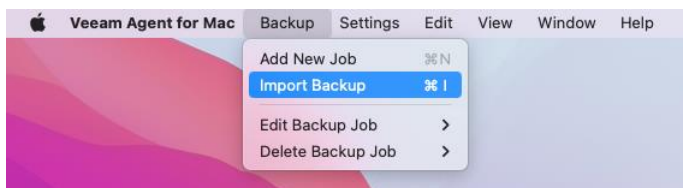
Importing Backups with Import Wizard

You can import a backup using the **Import** wizard.

Step 1. Launch Import Wizard

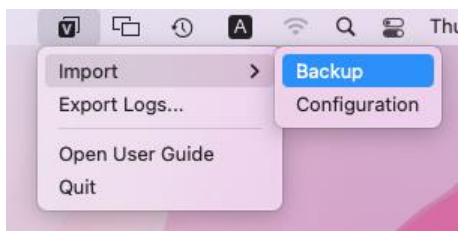
To launch the Import wizard, do either of the following:

- In the **Veeam Agent for Mac** application menu, select **Backup > Import Backup**.



Alternatively, you can use the **Command-I** shortcut on the keyboard.

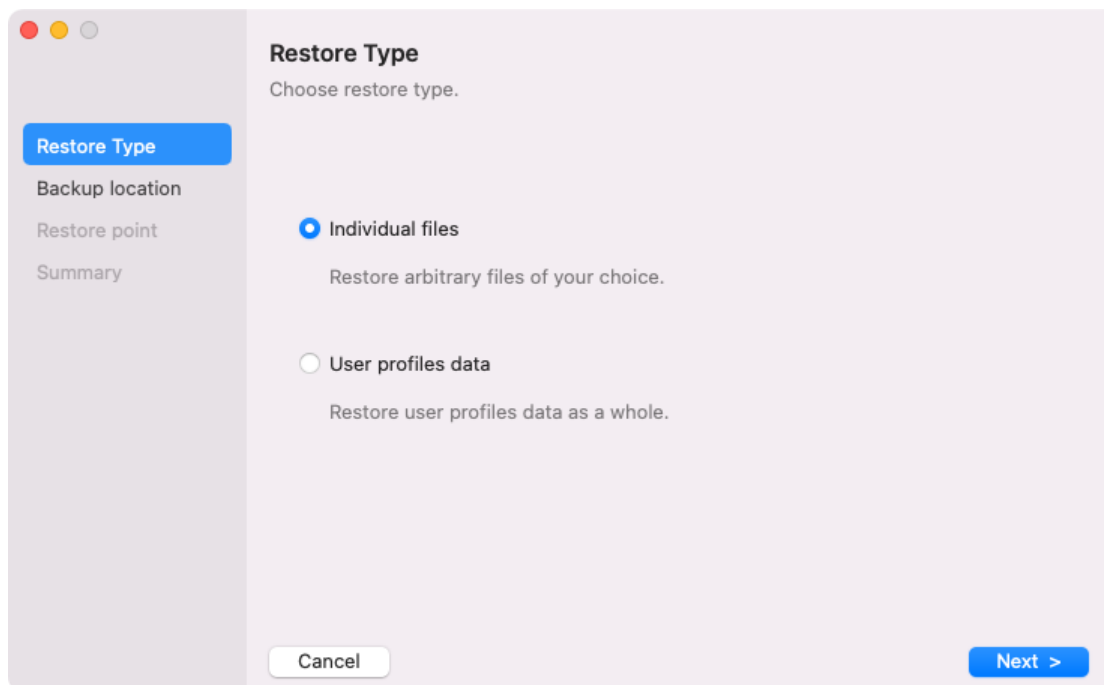
- In the **Veeam Agent for Mac** status bar menu, select **Import > Backup**.



Step 2. Select Restore Type

At the **Restore Type** step of the wizard, select one of the available restore types:

- **Individual files** (default) – allows you to browse the backup and select specific files or folders to restore.
- **User profiles data** – allows you to restore user profiles data as a whole.

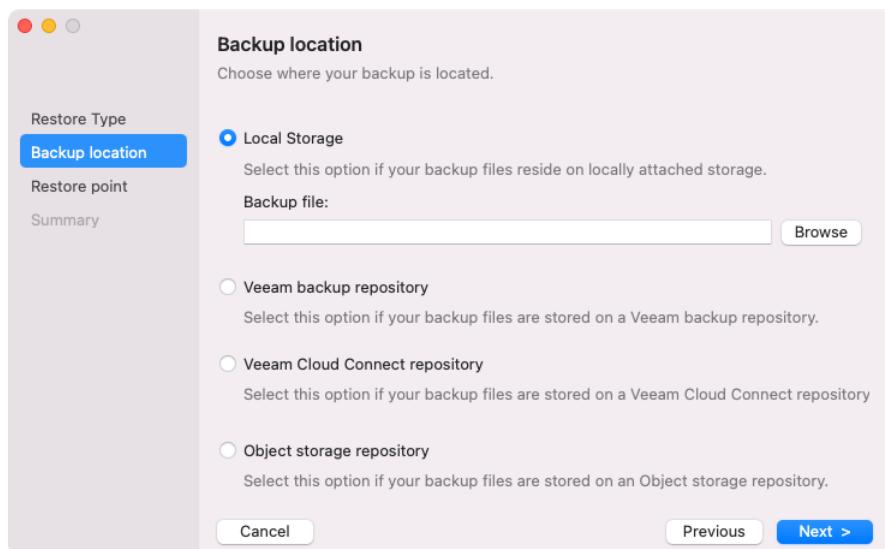


Step 3. Select Backup Location

At the **Backup Location** step of the wizard, select the location of the backup repository.

You can select one of the following options:

- **Local storage** – select this option if you want to restore data from the backup that resides on a local computer drive, direct or network attached storage – for example, a USB flash drive or locally mounted SMB share. After you select this option and [specify the location of the backup file](#), you will pass to the [Restore Point](#) step of the wizard.
- **Veeam backup repository** – select this option if you want to restore data from the backup that resides in a backup repository managed by the Veeam backup server. With this option selected, you will pass to the [Backup Server](#) step of the wizard.
- **Veeam Cloud Connect repository** – select this option if you want to restore data from the backup that resides in a cloud repository exposed to you by the Veeam Cloud Connect service provider. With this option selected, you will pass to the [Service Provider](#) step of the wizard.
- **Object storage repository** – select this option if you want to restore data from the backup that resides in an object storage repository exposed to you by third-party vendors. With this option selected, you will pass to the [Cloud Type](#) step of the wizard.



The screenshot shows a window titled "Backup location" with the instruction "Choose where your backup is located." On the left, a sidebar lists "Restore Type" (selected), "Restore point", and "Summary". The main area contains four radio button options: "Local Storage" (selected), "Veeam backup repository", "Veeam Cloud Connect repository", and "Object storage repository". Below the "Local Storage" option is a "Backup file:" label, a text input field, and a "Browse" button. At the bottom, there are "Cancel", "Previous", and "Next >" buttons.

Step 4. Specify Backup Repository Settings

Specify backup storage settings for data restore:

- [Local storage settings](#) – if you have selected the **Local Storage** option at the [Backup Location](#) step of the wizard.
- [Veeam backup repository settings](#) – if you have selected the **Veeam backup repository** option at the [Backup Location](#) step of the wizard.
- [Veeam Cloud Connect repository settings](#) – if you have selected the **Veeam Cloud Connect repository** option at the [Backup Location](#) step of the wizard.
- [Object storage settings](#) – if you have selected the **Object storage repository** option at the [Backup Location](#) step of the wizard.

Local Backup Repository Settings

If you want to restore data from a backup residing in a local or directly attached network drive, you must specify location of the backup file at the [Backup location](#) step of the wizard.

NOTE

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

To specify the location of a backup file that resides in a local or network drive:

1. At the **Backup Location** step of the wizard, under the selected **Local Storage** option, click **Browse**.
2. In the **Finder** window, open the folder that contains the backup file and select the VBM file of the necessary backup.

Alternatively, you can type a path to the folder that contains the VBM file in the **Backup File** field.

3. In the **Finder** window, click **Open**.

The screenshot shows a dialog box titled "Backup location" with the instruction "Choose where your backup is located." On the left, a sidebar lists "Restore Type" (selected), "Backup location", "Restore point", and "Summary". The main area has four radio button options: "Local Storage" (selected), "Veeam backup repository", "Veeam Cloud Connect repository", and "Object storage repository". Under "Local Storage", there is a "Backup file:" label, a text input field containing the path "/Volumes/backup01/prg10575.local Mac01_Backup2SMB/Mac01_Backup", and a "Browse" button. At the bottom, there are "Cancel", "Previous", and "Next >" buttons.

Veeam Backup Repository Settings

The **Backup Server** step of the wizard is available if you have chosen to store backup files in a Veeam backup repository.

Specify settings for the Veeam backup repository that contains the necessary backup file:

1. In the **Veeam backup server name or IP address** field, specify a DNS name or IP address of the Veeam backup server.
2. In the **Port** field, specify the number of the port over which Veeam Agent must communicate with the backup repository. By default, Veeam Agent for Mac uses port 10006.
3. In the **Specify your personal credentials** section, enter credentials to access the server:
 - a. In the **Username** field, type a name of the account that has access permissions on the Veeam backup repository.
 - b. If necessary, in the **Domain** field, type a name of the domain in which the account that has access to the Veeam backup repository is registered.
 - c. 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](#).

Backup Server
Specify Veeam Backup & Replication server to retrieve the list of backups from.

Restore Type
Backup location
Backup Server
Backup
Restore point
Summary

Veeam backup server name or IP address: 172.24.31.136 Port: 10006

Specify your personal credentials:

Username: Administrator
Domain (optional):
Password: •••••••• Edit

Cancel Previous Next >

Veeam Cloud Connect Repository Settings

If you have selected to restore data from the backup that resides in a Veeam Cloud Connect repository, specify settings to connect to the cloud repository:

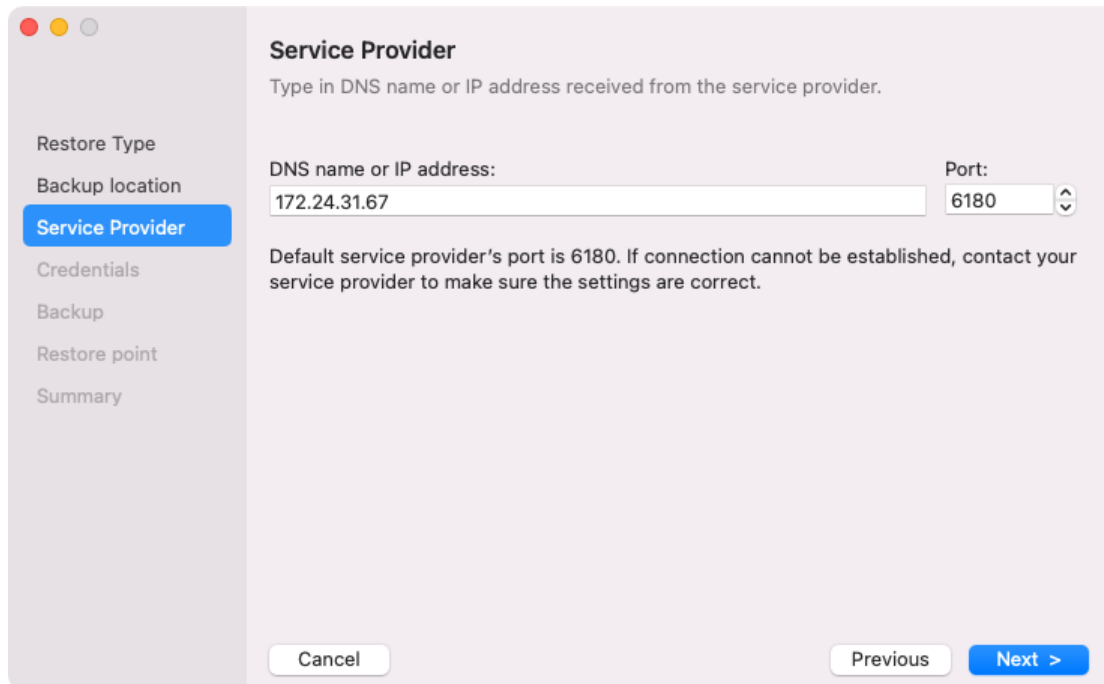
1. [Specify service provider settings](#).
2. [Verify TLS certificate and specify user account settings](#).

Specifying Service Provider Settings

The **Service Provider** step of the wizard is available if you have chosen to restore from the backup that resides in a Veeam Cloud Connect repository.

Specify settings for the cloud gateway that the Veeam Cloud Connect service provider (SP) or your backup administrator has provided to you:

1. In the **DNS name or IP address** field, enter a full DNS name or IP address of the cloud gateway.
2. In the **Port** field, specify the port over which Veeam Agent will communicate with the cloud gateway. By default, Veeam Agent uses port 6180.



The screenshot shows a window titled "Service Provider" with a sidebar on the left containing the following steps: Restore Type, Backup location, Service Provider (highlighted in blue), Credentials, Backup, Restore point, and Summary. The main area of the window contains the following text and fields:

Service Provider
Type in DNS name or IP address received from the service provider.

DNS name or IP address: Port:

Default service provider's port is 6180. If connection cannot be established, contact your service provider to make sure the settings are correct.

At the bottom of the window, there are three buttons: "Cancel", "Previous", and "Next >" (highlighted in blue).

Specifying User Account Settings

The **Credentials** step of the wizard is available if you have chosen to restore data from the backup that resides in a cloud repository and specified settings for the cloud gateway.

Verify TLS certificate settings and specify settings for the tenant account or subtenant account that you want to use to connect to the cloud repository.

1. In the certificate details section, review information about the TLS certificate obtained from the SP side and verify the TLS certificate.
2. [Optional] To verify the TLS certificate with a thumbprint, do the following:
 - a. In the **Thumbprint for certificate verification** field, paste the thumbprint you obtained from the SP.
 - b. Click **Verify**. Veeam Agent will check if the thumbprint you entered matches the thumbprint of the obtained TLS certificate.
5. In the **Username** 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.

6. In the **Password** field, provide a password for the tenant or subtenant account.

Credentials

Specify credentials that you have received from the service provider, and validate the certificate.

This certificate has been validated.
Verified by: /OU=Veeam Software/O=Veeam Software/CN=Veeam Software

Thumbprint for certificate verification:

This certificate has been already verified.

Username:

Password:

Object Storage Repository Settings

The **Cloud Type** step of the wizard is available if you have selected the **Object storage** option at the [Backup Location](#) step of the wizard.

At the **Cloud Type** step of the wizard, select the cloud storage type. You can select one of the following options:

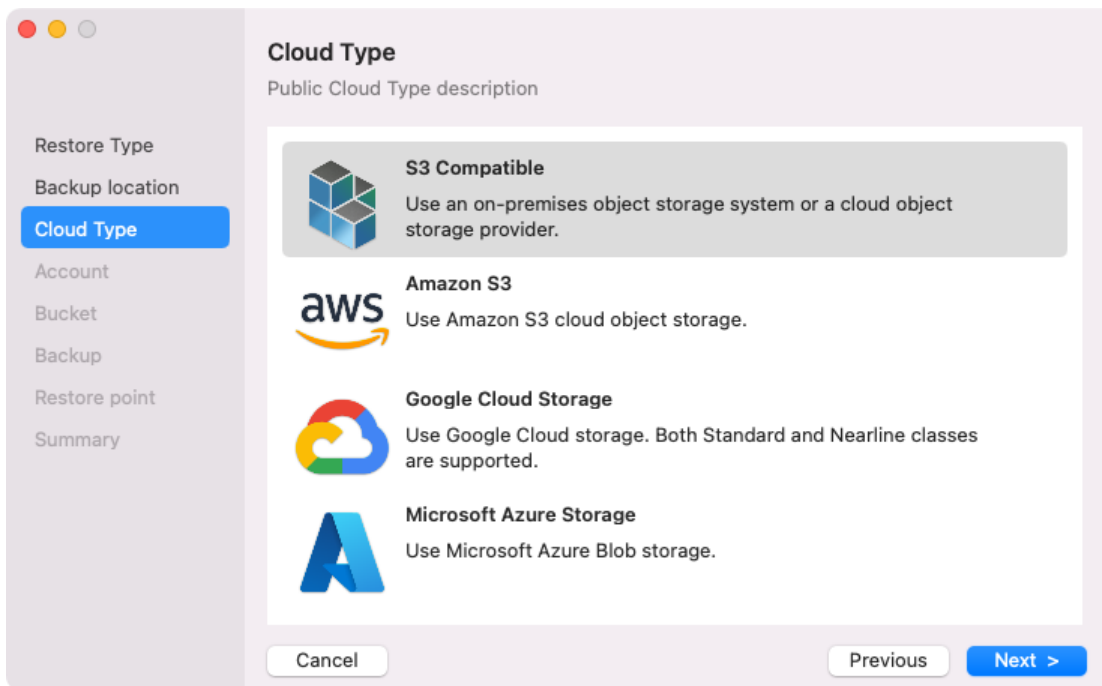
- **S3 compatible** – select this option if you want to import a backup from an S3 compatible storage repository. With this option selected, you will pass to the [Account](#) step of the wizard.

TIP

If you plan to store backups on an IBM or Wasabi cloud storage, use the **S3 compatible** storage option.

- **Amazon S3** – select this option if you want to import a backup from an Amazon S3 storage repository. With this option selected, you will pass to the [Account](#) step of the wizard.
- **Google Cloud Storage** – select this option if you want to import a backup from a Google Cloud storage repository. With this option selected, you will pass to the [Account](#) step of the wizard.

- **Microsoft Azure Storage** – select this option if you want to import a backup from a Microsoft Azure storage repository. With this option selected, you will pass to the [Account](#) step of the wizard.



Specifying Settings for S3 Compatible Repository

If you have selected to import backup from an S3 Compatible storage repository, specify settings to connect to the storage:

1. [Specify account settings.](#)
2. [Specify bucket settings.](#)

Specifying Account Settings

The **Account** step of the wizard is available if you have chosen to import backup from an S3 compatible storage repository.

To connect to the S3 compatible storage, specify the following:

1. In the **Service point** field, specify the address of your S3 compatible storage.

NOTE

If you want to connect to the repository using the IPv6 address and the port number, you must use the following format: `IPv6:port`, where:

- `IPv6` is an IPv6 address of the cloud storage.
 - `port` is a number of a port that Veeam Agent will use to connect to the cloud storage.
2. In the **Region** field, specify a storage region based on your regulatory and compliance requirements.
 3. In the **Access key** field, enter an access key ID.

4. In the **Secret key** field, enter a secret access key.

Account
Specify S3 compatible storage account

Service point:
https://myservicepoint.com

Region:
reg-1

S3-compatible account:

Access key:
Access_Key

Secret key:
..... Edit

Cancel Previous Next >

Specifying Bucket Settings

The **Bucket** step of the wizard is available if you have chosen to import backup from an S3 compatible storage repository and specified account settings to connect to the storage.

Specify settings for the bucket on the storage:

1. In the **Bucket** field, specify a bucket on the storage:
 - a. Click **Browse**.
 - b. In the **Buckets** window, select the necessary bucket and click **OK**.
2. In the **Folder** field, specify a folder in the bucket:
 - a. Click **Browse**.

b. In the **Folders** window, select the necessary folder and click **OK**.

Bucket
Specify S3-compatible folder and bucket settings

Name
Files
Destination
Cloud Type
Account
Bucket
Schedule
Summary

Bucket:
vam-veeam-backups

Folder:
folder01

Retention policy:
7 restore points

Keep certain full backups longer for archival purposes
1 weekly, 1 monthly

Make recent backups immutable for: 30 days

Protects backups from modification or deletion by ransomware, malicious insiders and hackers. This may incur additional API and storage costs. GFS backups are made immutable for the entire duration of their retention policy.

Click Advanced to enable periodic full backups and encryption

Specifying Settings for Amazon S3 Repository

If you have selected to store backup files on an Amazon S3 storage, specify settings to connect to the storage:

1. [Specify account settings.](#)
2. [Specify bucket settings.](#)

Specifying Account Settings

The **Account** step of the wizard is available if you have chosen to import backup from an Amazon S3 storage repository.

To connect to the Amazon S3 storage, specify the following:

1. In the **Access key** field, enter an access key ID.
2. In the **Secret key** field, enter a secret access key.

3. In the **AWS region** window, select an AWS region based on your regulatory and compliance requirements. By default, Veeam Agent uses the **Global** region.

Account
Specify Amazon S3 account

Access key:
AKIA4SIMXVDIFTNXXRF4

Secret key:
..... Edit

AWS region: Global

Cancel Previous Next >

Specifying Bucket Settings

The **Bucket** step of the wizard is available if you have chosen to import backup from an Amazon S3 storage repository and specified account settings to connect to the storage.

Specify settings for the bucket on the storage:

1. In the **Data center** window, select the geographic region where Veeam Agent will store backups.
2. In the **Bucket** field, specify a bucket on the storage:
 - a. Click **Browse**.
 - b. In the **Buckets** window, select the necessary bucket and click **OK**.
3. In the **Folder** field, specify a folder in the bucket:
 - a. Click **Browse**.

b. In the **Folders** window, select the necessary folder and click **OK**.

Bucket
Specify Amazon S3 bucket and folder

Data center:
US East (N. Virginia)

Bucket:
mac-veeam-backups Browse

Folder:
folder01 Browse

Retention policy:
7 restore points

Keep certain full backups longer for archival purposes
1 weekly, 1 monthly Configure

Make recent backups immutable for: 30 days
Protects backups from modification or deletion by ransomware, malicious insiders and hackers. This may incur additional API and storage costs. GFS backups are made immutable for the entire duration of their retention policy.

Click Advanced to enable periodic full backups and encryption Advanced

Cancel Previous Next Finish

Specifying Settings for Google Cloud Repository

If you have selected to import backup from a Google Cloud storage repository, specify settings to connect to the storage:

1. [Specify account settings.](#)
2. [Specify bucket settings.](#)

Specifying Account Settings

The **Account** step of the wizard is available if you have chosen to import backup from a Google Cloud storage repository.

To connect to the Google Cloud storage, in the **Access key** and **Secret key** fields, specify the Hash-based Message Authentication Code (HMAC) key associated with the Google Cloud account. Veeam Agent will use the HMAC key to authenticate requests to the Google Cloud storage. For more information on Google Cloud accounts, see the [Google Cloud documentation](#).

Account
Specify Google Cloud account

Access key:
GOOG1EGUOKTN5YHTOO7VVCFXREOGWWBRNGCAJAJUF4A3BJLJEEOMZFIWNWGGY

Secret key:
..... Edit

Cancel Previous Next >

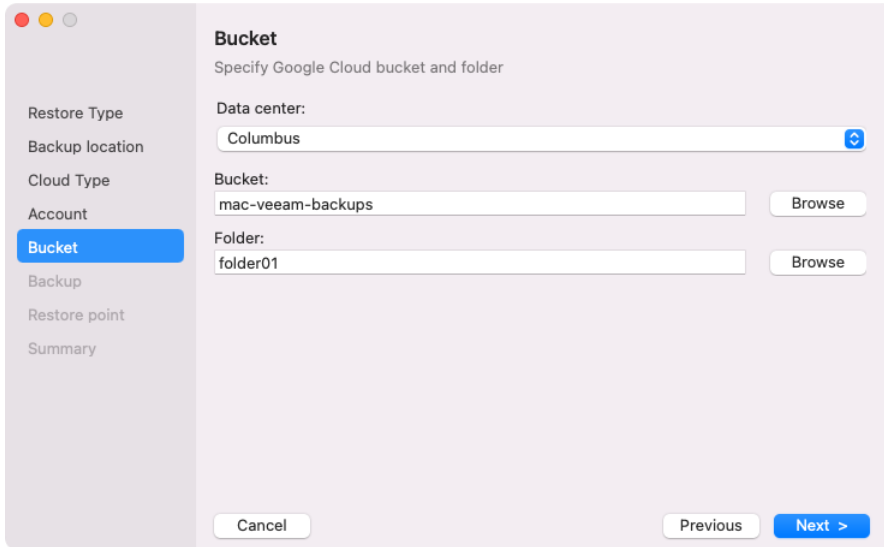
Specifying Bucket Settings

The **Bucket** step of the wizard is available if you have chosen to import backup from a Google Cloud storage repository and specified account settings to connect to the storage.

Specify settings for the bucket on the storage:

1. In the **Data center** window, select the geographic region where Veeam Agent will store backups.
2. In the **Bucket** field, specify a bucket on the storage:
 - a. Click **Browse**.
 - b. In the **Buckets** window, select the necessary bucket and click **OK**.
3. In the **Folder** field, specify a folder in the bucket:
 - a. Click **Browse**.

b. In the **Folders** window, select the necessary folder and click **OK**.



Specifying Settings for Microsoft Azure Repository

If you have selected to import backup from a Microsoft Azure storage repository, specify settings to connect to the storage:

1. [Specify account settings.](#)
2. [Specify container settings.](#)

Specifying Account Settings

The **Account** step of the wizard is available if you have chosen to import backup from a Microsoft Azure storage repository.

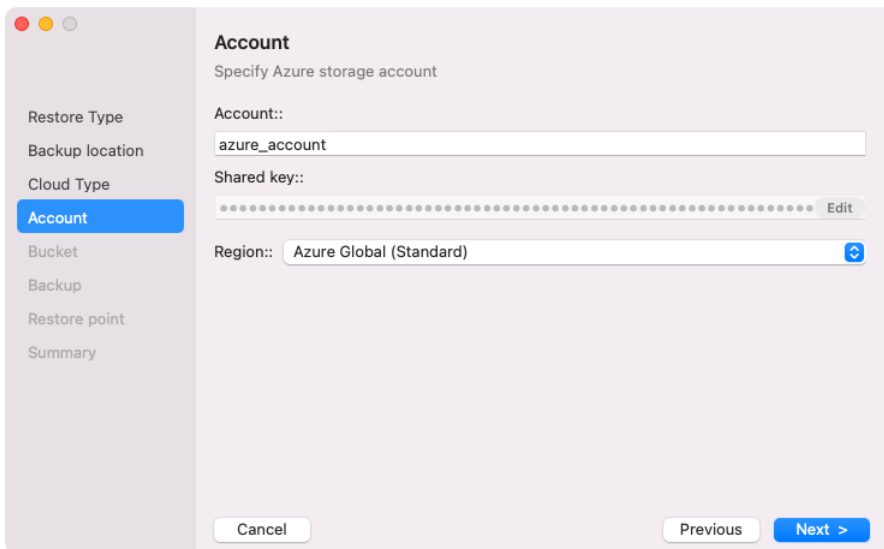
NOTE

The **Allow storage account key access** option for Shared Key authorization must be enabled in the storage account. For more information on how to find this option, see [Microsoft Docs](#).

To connect to the Microsoft Azure storage, specify the following:

1. In the **Account** field, enter the storage account name.
2. In the **Shared key** field, enter the storage account shared key.

3. In the **Region** window, select a Microsoft Azure region based on your regulatory and compliance requirements. By default, Veeam Agent uses the **Azure Global (Standard)** region.

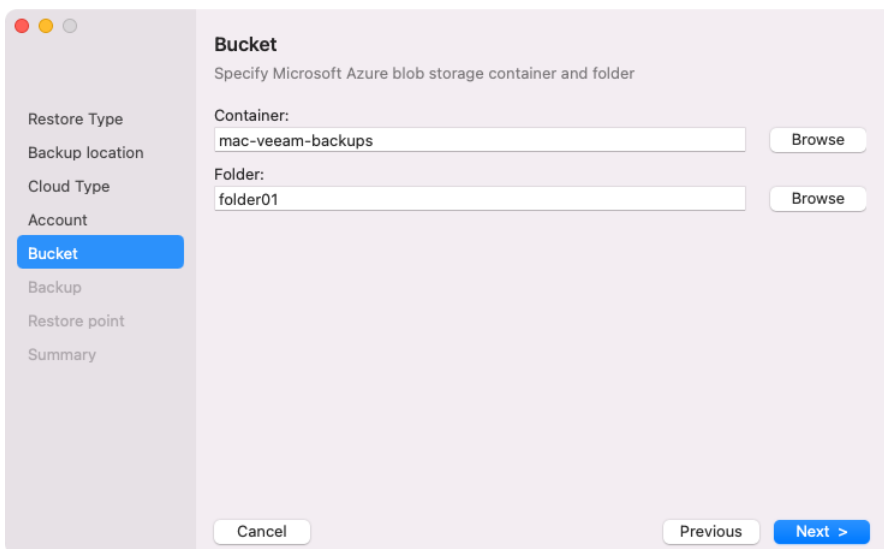


Specifying Container Settings

The **Container** step of the wizard is available if you have chosen to import backup from a Microsoft Azure storage repository and specified account settings to connect to the storage.

Specify settings for the container on the storage:

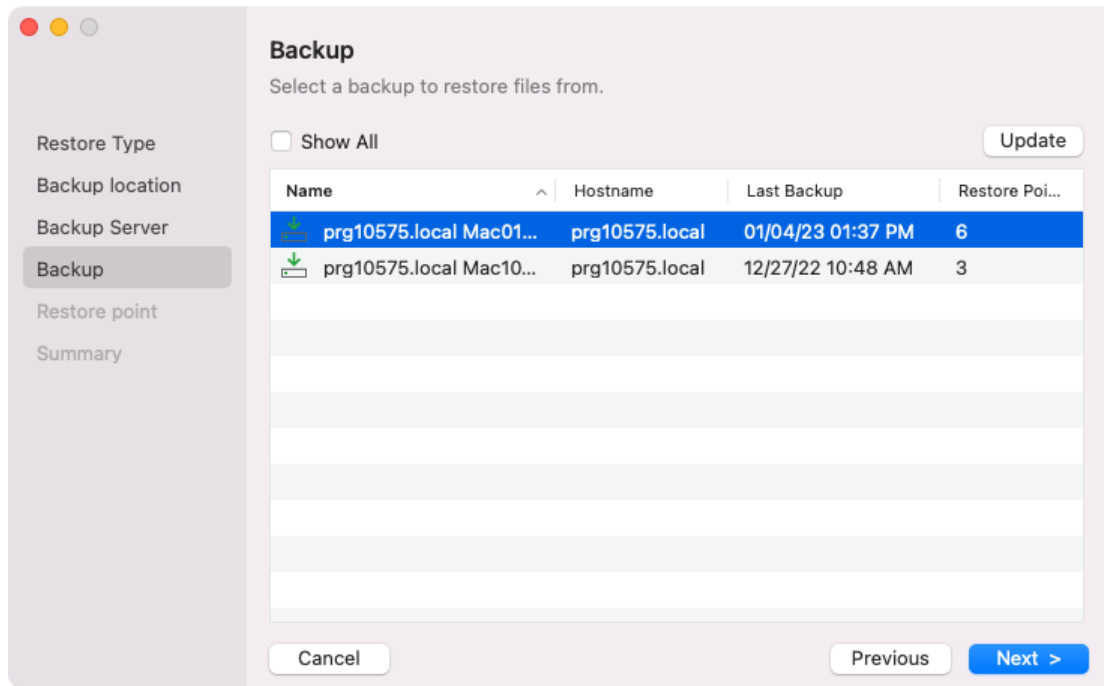
1. In the **Container** field, specify a container on the storage:
 - a. Click **Browse**.
 - b. In the **Containers** window, select the necessary container and click **OK**.
2. In the **Folder** field, specify a folder in the bucket:
 - a. Click **Browse**.
 - b. In the **Folders** window, select the necessary folder and click **OK**.



Step 5. Select Backup

The **Backup** step of the wizard is available if you have chosen to restore data from a backup file that resides in a remote location – in a network shared folder, Veeam backup repository, Veeam Cloud Connect repository or object storage repository.

From the list of backups, select the VBM (backup metadata) file of the necessary backup.



By default, Veeam Agent lists the metadata files for the backups created by Veeam Agent on the computer where Veeam Agent is installed. Select **Show All** to display all the backups available in the Veeam backup repository.

Veeam Agent displays only those backups that are available to the user whose credentials are specified to access the selected repository. Consider the following specifics of the backup display logic depending on the repository type:

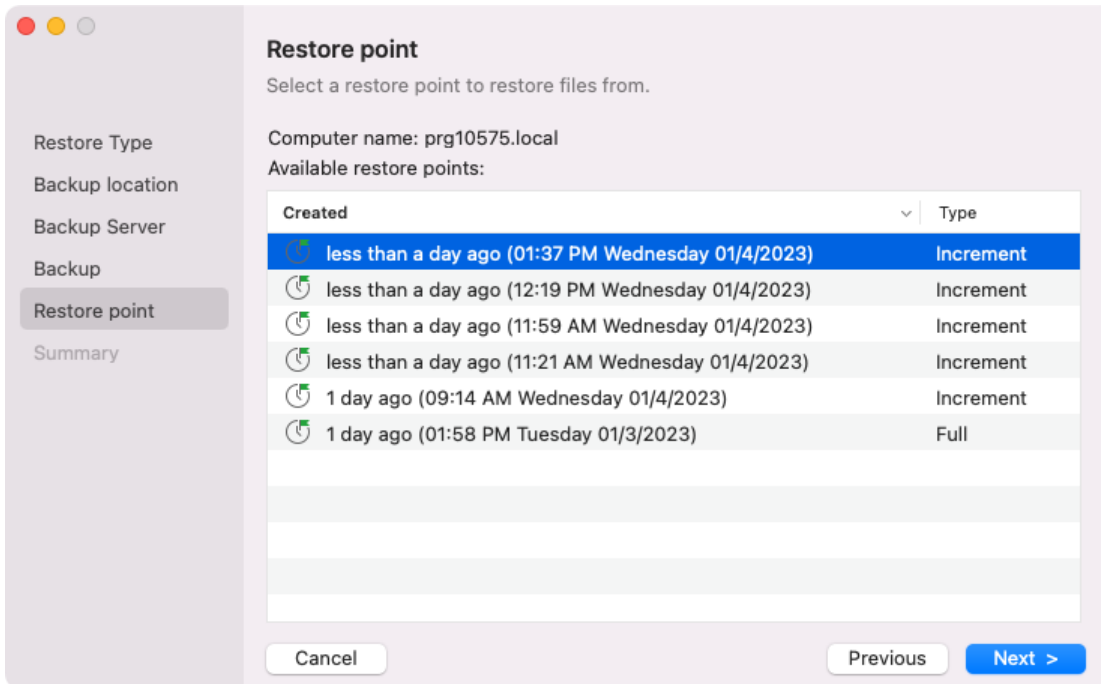
- If you restore data from a backup stored in a Veeam backup repository, Veeam Agent displays only those backups that are accessible by the user whose credentials are specified at the [Backup Server](#) step of the wizard:
 - If you specify credentials for the user who has access to the backup repository, the list of backups will include only backups created by this user.
 - If you specify credentials for the user who is assigned the *Backup Administrator* or *Restore Operator* role on the backup server, the list of backups will include all Veeam Agent backups stored on the backup repository.
- If you restore data from a backup stored in a Veeam Cloud Connect repository, Veeam Agent displays only those backups that are accessible by the user whose credentials are specified at the [Credentials](#) step of the wizard:
 - If you specify credentials for the tenant account, the list of backups will include backups created by all users who create backups under this account.
 - If you specify credentials for the subtenant account, the list of backups will include only those Veeam Agent backups that were created under this subtenant account.

NOTE

If you restore data from an encrypted backup that was created on another Veeam Agent computer, you need to provide a password to unlock the encrypted file. To learn more, see [Restoring Data from Encrypted Backups](#).

Step 6. Select Restore Point

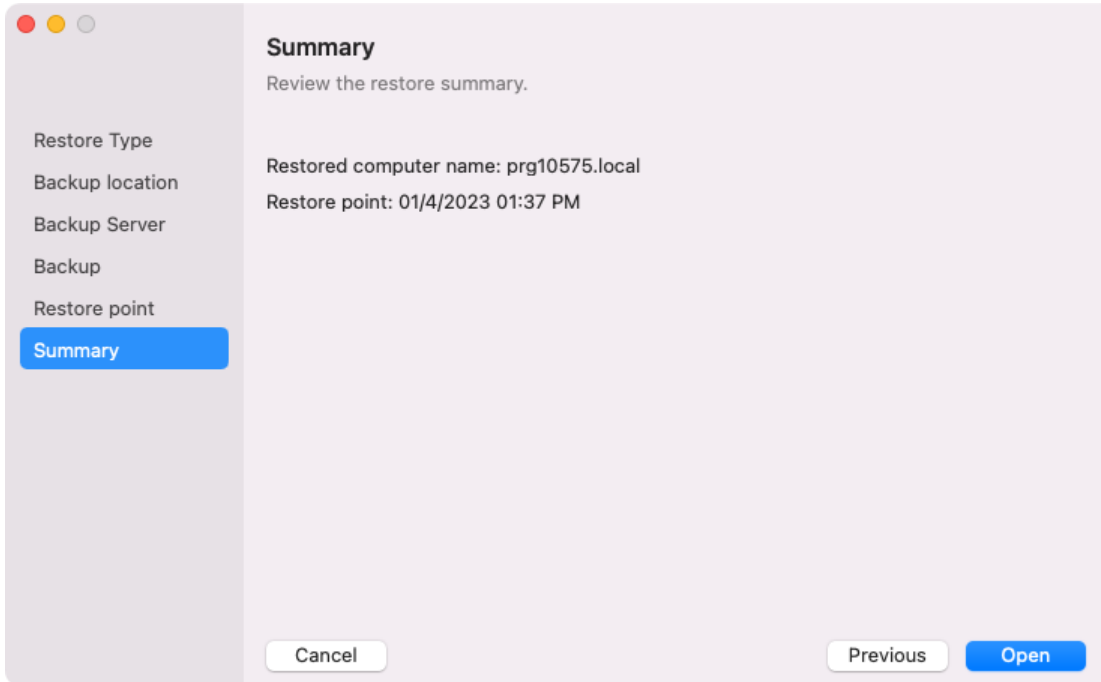
At the **Restore Point** step of the wizard, select a restore point from which you want to restore data.



Step 7. Complete Import Process

At the **Summary** step of the wizard, complete the procedure of backup import.

1. Review the settings of the import process.
2. Click **Open**. Veeam Agent will retrieve the content of the backup file and display it in the Veeam Backup browser.



What You Do Next

When the import process is complete, Veeam Agent opens the Veeam Backup browser and displays the content of the backup file.

You can perform the following operations with the files and folders from the imported backup:

- [Save files and folders to their initial location](#)
- [Save files and folders to a new location](#)

Importing Backups in Command Line Interface

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 {765af178-a9cc-4596-8bf2-03850c5dalac} [info] Job started at 2016-11-19 16:21:33
2016-11-19 13:21:33 UTC {6ae2922d-454b-4a8d-a11b-2b5c7a85029d} [info] Importing backup
2016-11-19 13:21:33 UTC {783f40a7-ead7-4555-9c35-545d875990ee} [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:

```
user@wrk01:~$ veeamconfig backup list
Job name          Backup ID          Repository
y   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-a6b6-4323-9287-1c6c8ceccb6b} Repository_
2   2016-11-15 11:28
BackupJob        {64957b1d-d219-456c-a9cd-9598292c10cd} Importe
d       2016-11-19 19:12
```

Managing Backups

You can view, edit and delete backup jobs:

- [In the Veeam Agent control panel.](#)
- [In command line interface.](#)

Managing Backups in Control Panel

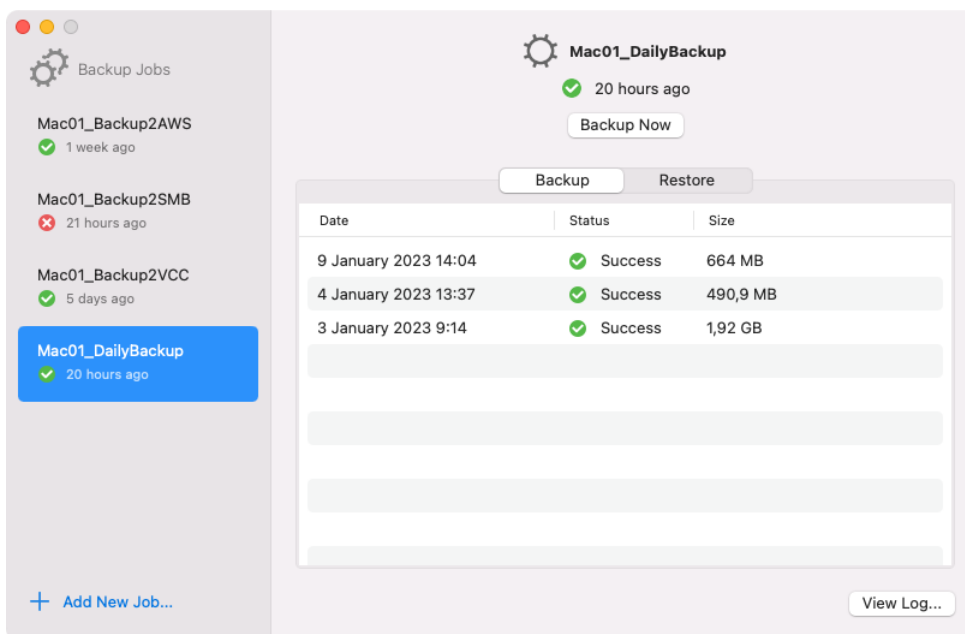
In the Veeam Agent control panel, you can perform the following operations with backups created by backup jobs configured in Veeam Agent for Mac:

- [View backup and restore points.](#)
- [View backup details.](#)

Viewing Backup and Restore Points

To view backup and restore points created by a backup job configured in Veeam Agent, do the following:

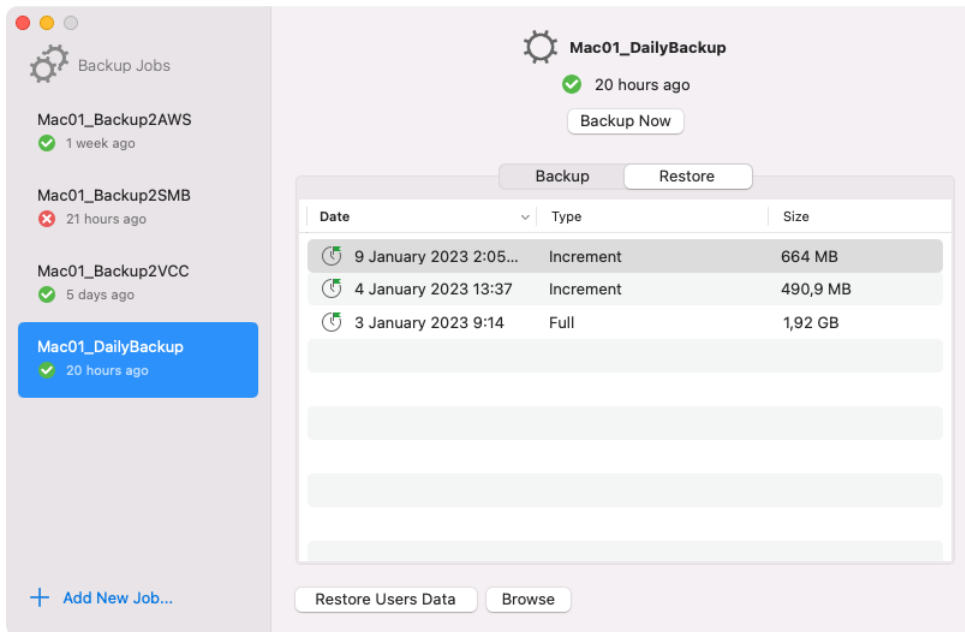
1. If you have multiple backup jobs configured in Veeam Agent, from the **Backup Jobs** list, select the backup job whose backup you want to view.



If you have only one backup job configured in Veeam Agent, its details are displayed in the main pane by default. Proceed to Step 2.

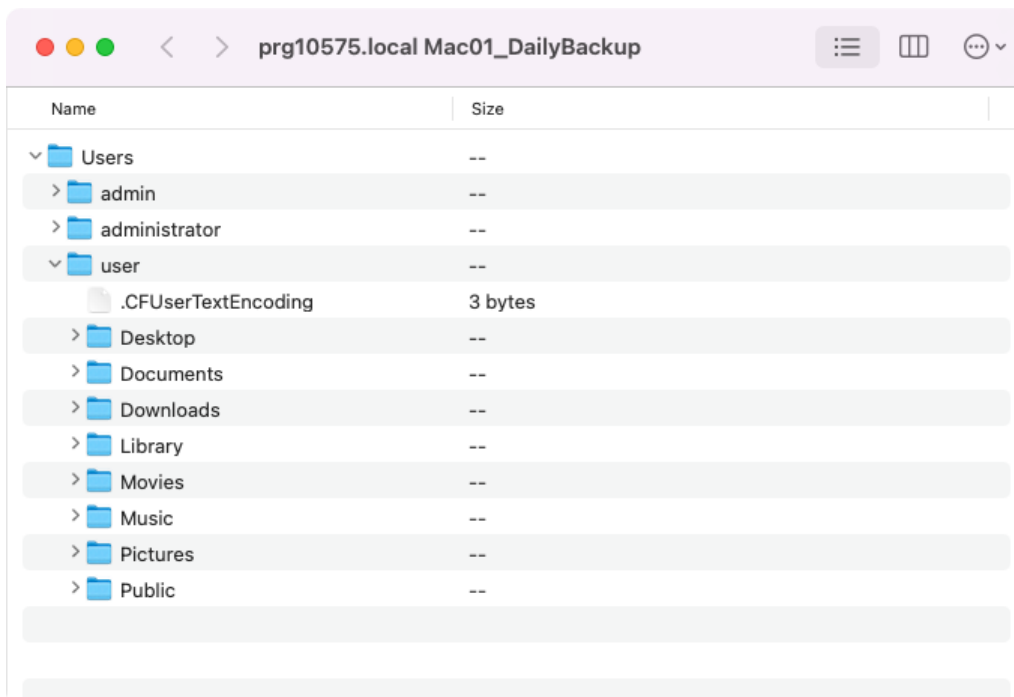
- In the main pane of the Veeam Agent control panel, select the **Restore** tab. Veeam Agent will display the list of restore points in the backup.

For each restore point, Veeam Agent displays the date and time it was created, type (*Full* or *Increment*) and size.



Viewing Backup Details

You can use the Veeam Backup browser to view the scope of the backup. To do this, on the **Restore** tab of the selected job, choose a restore point and click **Browse**. Veeam Agent will launch the Veeam Backup browser and display the content of the backup.



Managing Backups in Command Line Interface

In command line interface, 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:

Parameter	Description
Job name	Name of the backup job by which the backup was created.
Backup ID	ID of the backup.
Repository	Name of the backup repository in which the backup was created. Imported backups are marked as <i>Imported</i> in the Repository column. For information about the import procedure, see Importing Backups .
Created at	Date and time of the backup creation.

For example:

```
user@wrk01:~$ veeamconfig backup list
Job name          Backup ID          Repository        Creat
ed 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-a6b6-4323-9287-1c6c8ceccb6b} 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:

Parameter	Description
Machine name	Host name of the machine on which the backup job is configured and the name of the job.
Backed up	Backup scope for the file-level backup job.

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:

Parameter	Description
Job name	Name of the backup job by which the backup was created.
OIB ID	ID of the restore point in the backup.
Type	Type of the restore point. Possible values: <ul style="list-style-type: none">• Full• Increment
Created at	Date and time of the restore point creation.
Is corrupt	Indicates whether restore point in the backup is corrupted. Possible values: <ul style="list-style-type: none">• True• False
Retention	Displays information about enabled long-term retention per each type: weekly (W), monthly (M) and yearly (Y).

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.

Restoring Users Data

You can restore data of all user profiles configured on the protected computer.

When you restore user profiles data, 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, on which you plan to perform the restore, contains users with the same name as in the backup, all data of these users will be overwritten.

NOTE

Consider the following about restoring user profiles data:

- Computer administrator can restore data of all user profiles that are available in the backup file, standard user can restore only their own user profile.
- Veeam Agent does not back up data of network users that do not have local accounts.

Before You Begin

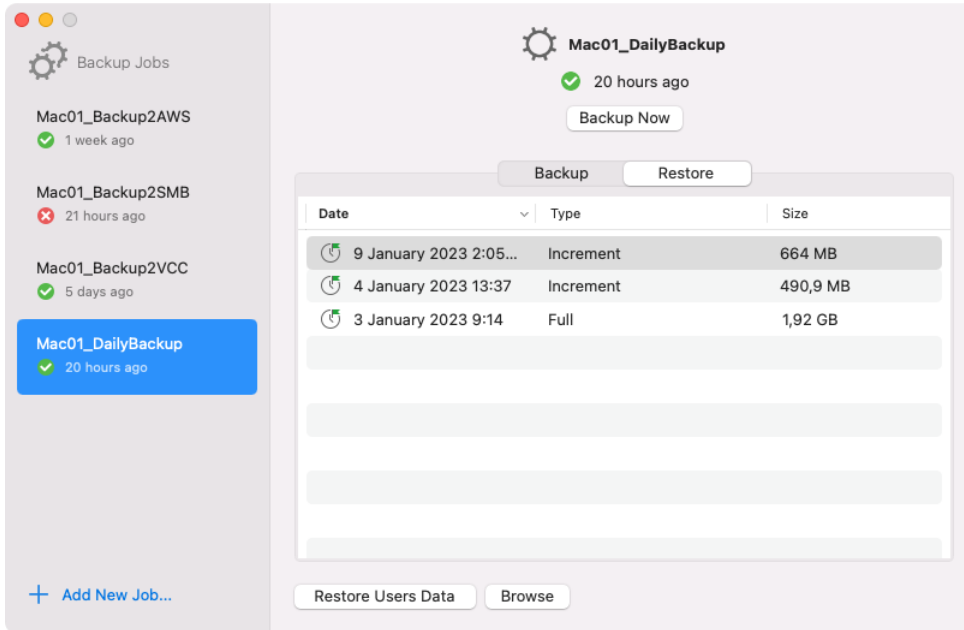
Before you begin the restore process, check the following prerequisites:

- 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 be created by a backup job that has **Personal files** in the backup scope.
- [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](#).

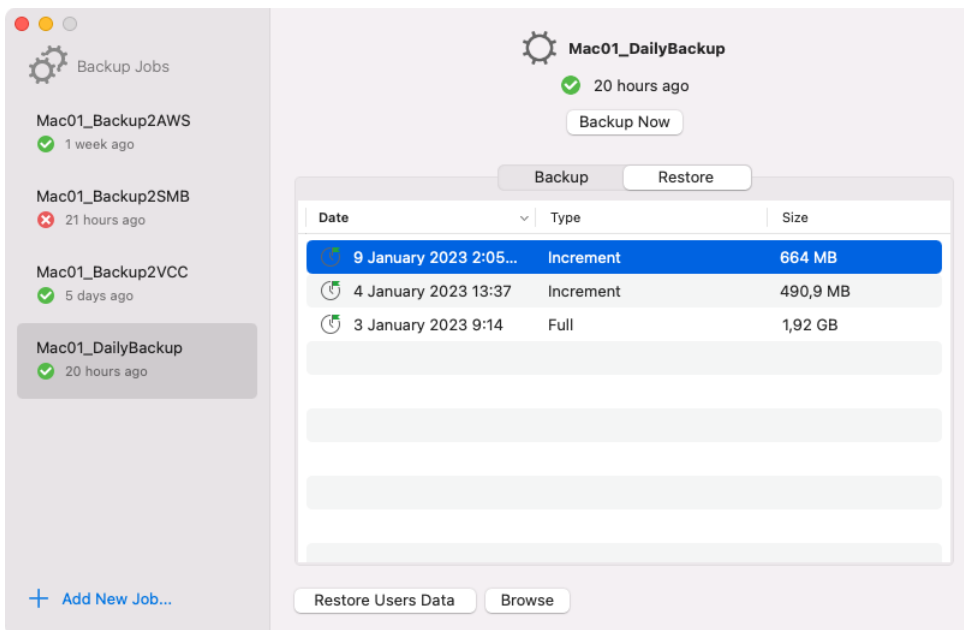
Restoring User Profiles Data

To restore user profiles data:

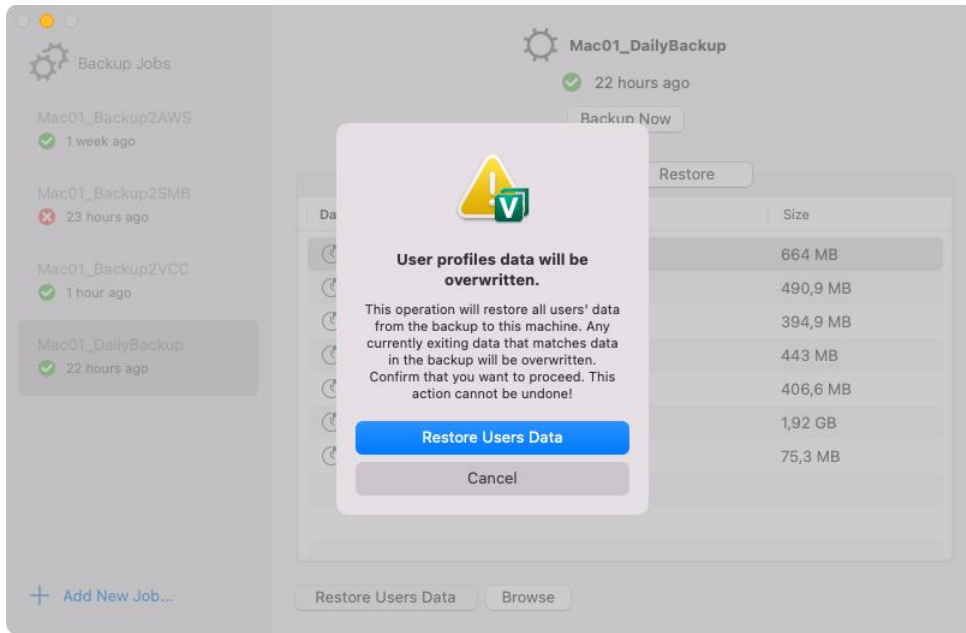
1. In the Veeam Agent control panel, select the backup job that created the backup from which you want to restore users.
2. In the main pane of the control panel, select the **Restore** tab. Veeam Agent will display the list of available restore points in the backup.



3. Select a restore point and click **Restore Users Data**.



4. In the displayed warning dialog, click **Restore Users Data** again.



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

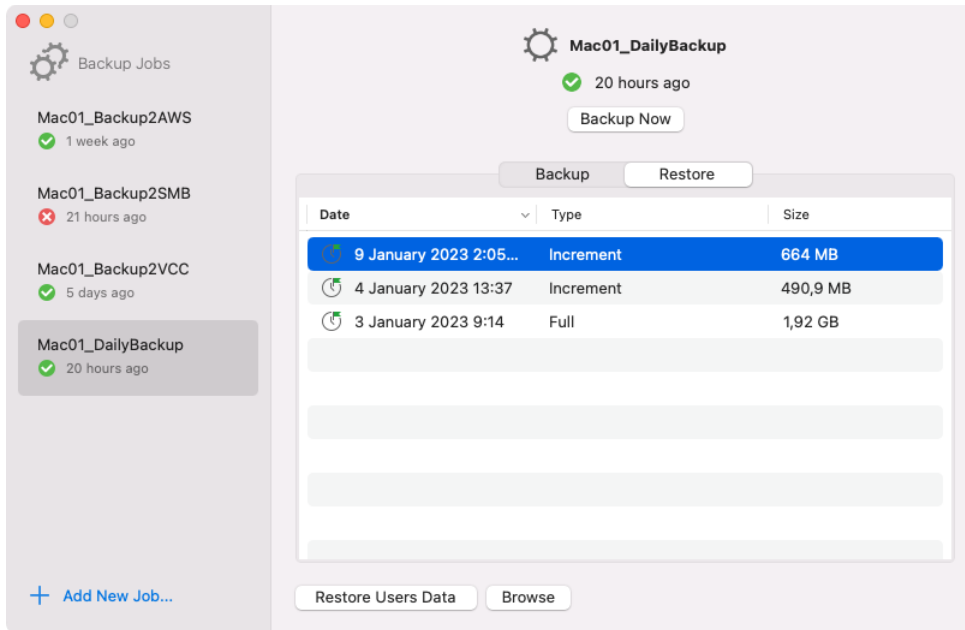
Before you begin the restore process, check the following prerequisites:

- 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](#).

Step 1. Select Restore Point

To restore individual files and folders:

1. In the Veeam Agent control panel, select the backup job that created the backup from which you want to restore users.
2. In the main pane of the control panel, select the **Restore** tab. Veeam Agent will display the list of available restore points in the backup.
3. Select a restore point and click **Browse**.



Veeam Agent will launch the Veeam Backup browser and display the content of the backup.

Step 2. Save Restored Files

After Veeam Agent opens the Veeam Backup browser displaying the contents of the backup file, you can perform the following restore operations with the files and folders:

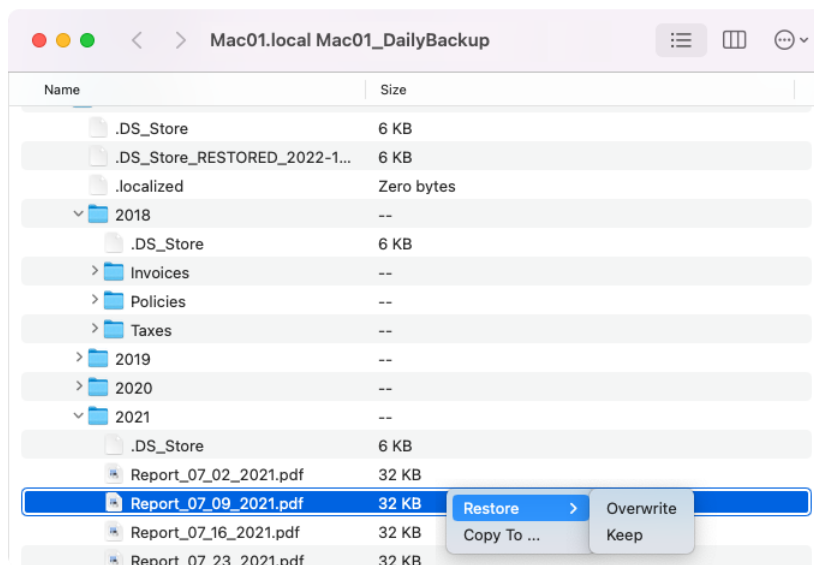
- [Save files and folders to their initial location](#)
- [Save files and folders to a new location](#)

After you finish working with files and folders, [close the Veeam Backup browser](#).

Saving Files to Initial Location

To save files or folders from a backup file to their initial location on the computer:

1. Select the necessary items in the file system tree.
2. Launch the restore options menu by doing either of the following:
 - Right-click the selected items.
 - Open the **Options** menu in the top right corner of the browser window.
3. Select one of the available restore actions.
 - To overwrite the original item on your computer with the item restored from the backup, select **Restore > Overwrite**.
 - To save the item restored from the backup next to the original item on your computer, select **Restore > Keep**. Veeam Agent for Microsoft Windows will add the `-RESTORED` postfix with a time stamp to the restored file or folder name and save it in the same location where the original file resides.

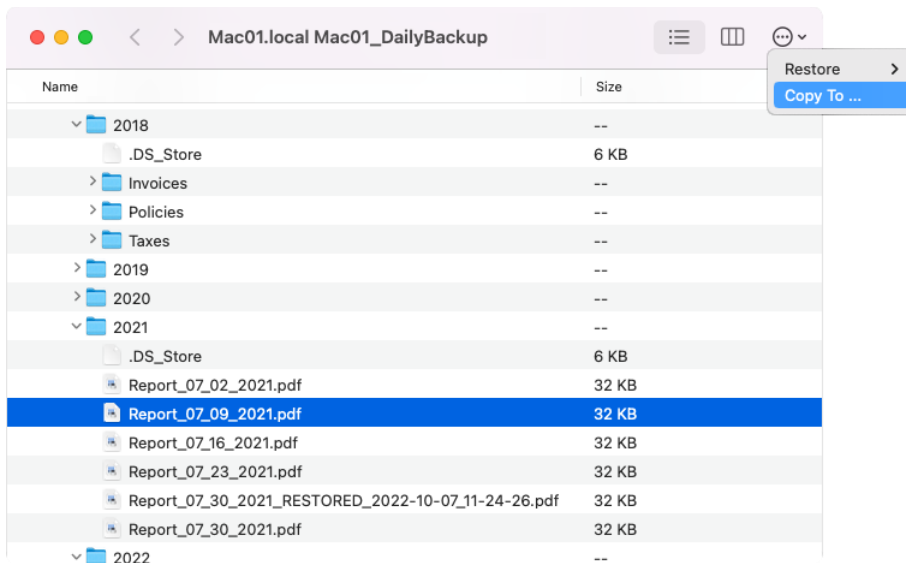


Saving Files to New Location

1. Select the necessary items in the file system tree.
2. Launch the restore options menu by doing either of the following:
 - Right-click the selected items

- Open the **Options** menu in the top right corner of the browser window.

4. Select the **Copy To** action.



5. In the **Finder** window, specify the location for the copied items.

Closing Veeam Backup Browser

You can browse restored files and folders only while the Veeam Backup browser is open. After the Veeam Backup browser is closed, Veeam Agent unmounts the backup content from your computer.

We recommend that you close the Veeam Backup browser after you finish restoring files and folders. Every 5 minutes, Veeam Agent checks if there is any activity in the Veeam Backup browser. If the user or product components and services have not performed any actions for 30 minutes, Veeam Agent automatically closes the Veeam Backup browser.

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 from 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 from 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

For every data transfer operation, for example data backup and restore, backup import and export, Veeam Agent starts a new session. You can get information about operations performed by Veeam Agent in two ways:

- [Using the Veeam Agent control panel](#)
- [In command line interface](#)

NOTE

In the Veeam Agent control panel, you can view information on backup job sessions only. To view information on import or restore sessions, use command line interface.

Reporting in Veeam Agent Control Panel

In the control panel, Veeam Agent provides the following information about backup job sessions:

- [Session list with general session statistics.](#)
- [Detailed session statistics.](#)
- [Notifications from Mac Notification Center.](#)





Viewing Backup Job Statistics

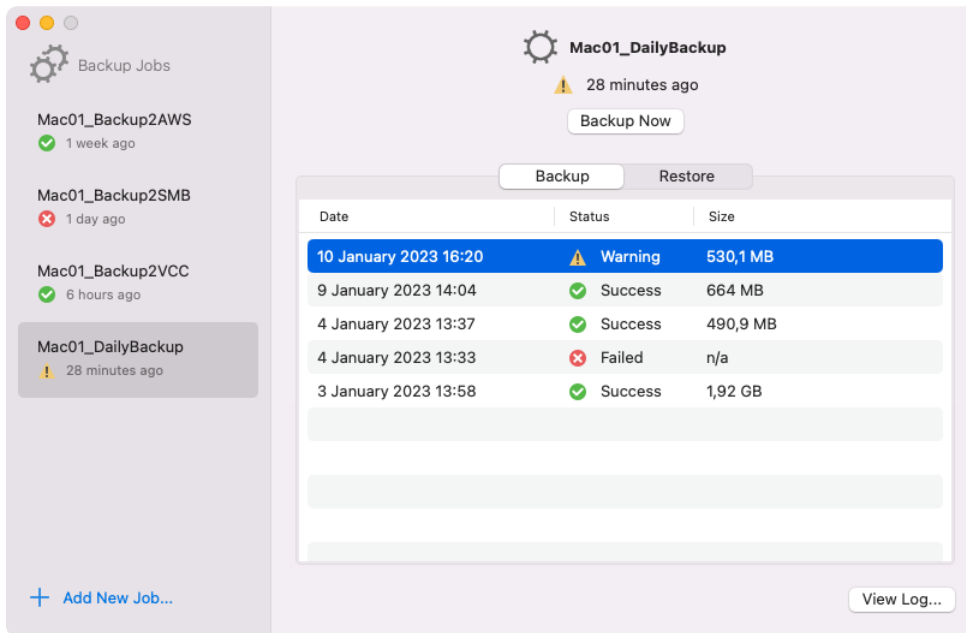
You can use the Veeam Agent control panel to view the list of backups performed by a selected backup job.

For every configured backup job, Veeam Agent displays backup session statistics in the main pane of the control panel. Depending on the number of the configured backup jobs, when you launch Veeam Agent, the control panel displays the following information:

- [Single job] Session statistics for the only backup job configured in Veeam Agent.
- [Multiple jobs] Session statistics for the top job in the **Backup Jobs** pane of the control panel. To view statistics for another job, select the necessary job from the **Backup Jobs** list.

The control panel displays information about backup job sessions that ran previously as well as about the backup job session that is currently running. Veeam Agent provides the following details for every backup session: backup start time and date, backup status and size of the resulting backup file. A session can have one of the following statuses:

-  *Running* – the backup job is currently running.
-  *Success* – the backup job has completed successfully.
-  *Warning* – the backup job has completed with a warning. Veeam Agent has managed to create the resulting backup file, but you need to pay your attention to some alerts, for example: the target location is running low on disk space.
-  *Failed* – the backup job has failed to complete. The resulting backup file has not been created.

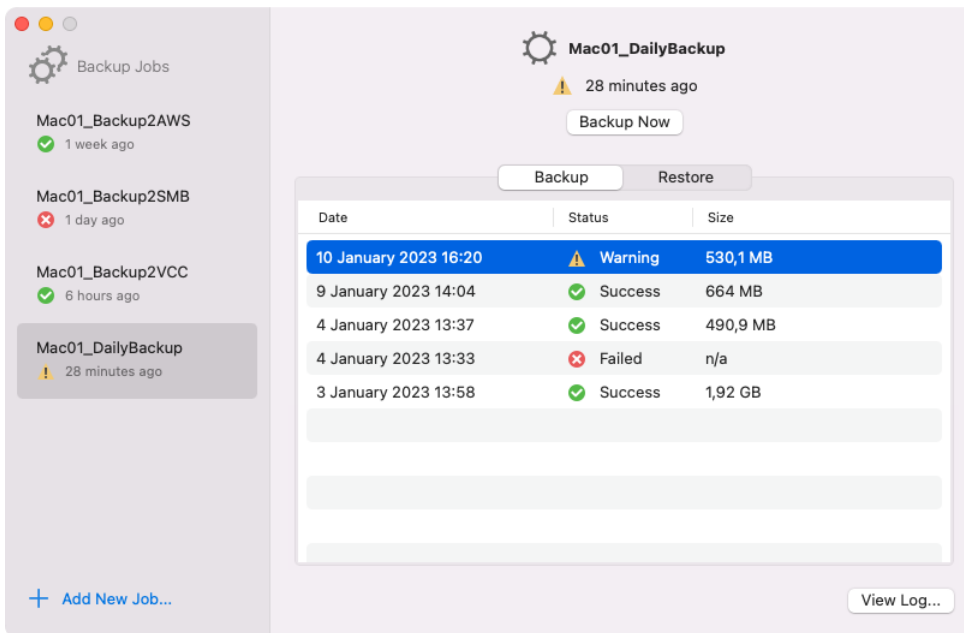


Viewing Statistics and Logs of Backup Sessions

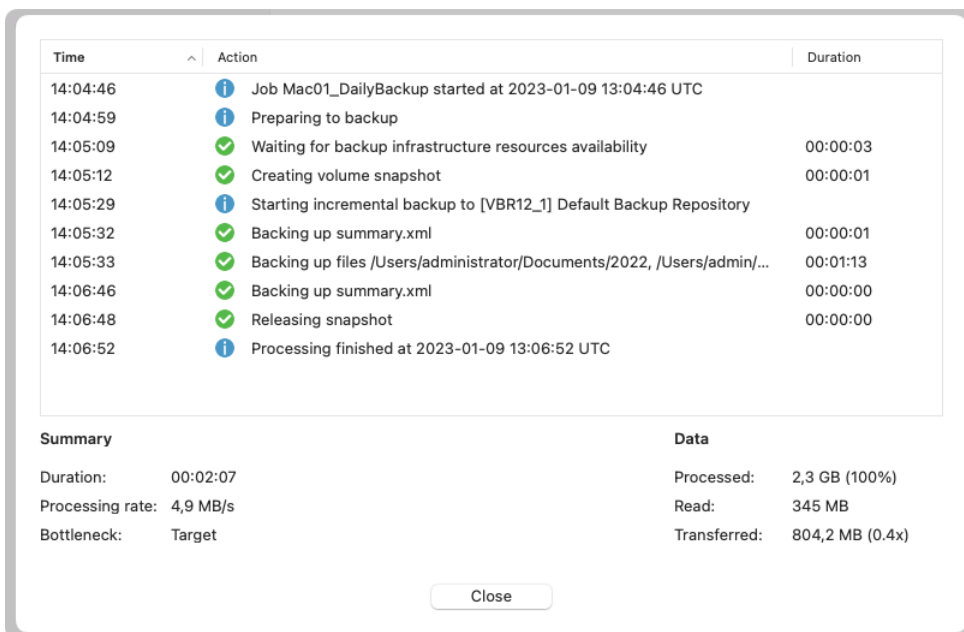
You can view statistics for a job session in the Veeam Agent control panel. Veeam Agent shows detailed data for every backup job session: job progress, duration, processing rate, performance bottlenecks, amount of processed data, read and transferred data, as well as details of the operations performed during the session, including warnings and errors that can occur in the process of the backup. If the session is running, you can view the statistics in real time.

To view the log of a selected backup session, do the following:

1. Select a backup job. In the main pane of the control panel, Veeam Agent will display the list of sessions for the selected backup job.
2. Select a session.



3. Click **View Log**. Veeam Agent will display a window with information on the selected session.



Veeam Agent displays the following for each backup job session:

- The pane at the top of the window lists the operations performed during the backup job session, their start time and duration time, as well as operation status. Operations can have the following statuses:
 - **Information** – marks messages that inform about a certain stage of the process – for example, *Preparing for backup* or *Processing finished*.
 - **In Progress** – marks operations being performed. You can view such operation status if you are monitoring a running session.
 - **Success** – marks operations that completed successfully.
 - **Warning** – marks operations that completed with warnings.
 - **Error** – marks operations that failed.
- The **Summary** section shows general information about the job:
 - **Duration** – time from the job start till the job end.
 - **Processing rate** – average speed of data processing. This counter is a ratio between the amount of processed data (**Processed** counter) and job duration (**Duration** counter).
 - **Bottleneck** – bottleneck in the data transmission process.
- The **Data** section shows information about processed data:
 - **Processed** – total size of data processed by the backup job.
 - **Read** – amount of data read from the backed-up computer by Veeam Agent prior to applying compression. For incremental job runs, the value of this counter is typically lower than the value of the **Processed** counter. Veeam Agent reads only data blocks that have changed since the last job session, processes and copies these data blocks to the target location.
 - **Transferred** – amount of data transferred from the backed-up computer to the backup location after applying compression. This counter does not directly indicate the size of the resulting files. Depending on the backup infrastructure and job settings, Veeam Agent can perform additional activities with data – for example, decompress data prior to writing the file to disk. These activities can impact the size of the resulting file.

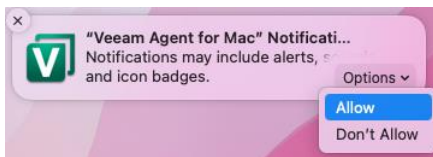
Viewing Events with Mac Notification Center

You can configure Veeam Agent to send notifications through the Mac Notification Center.

Enabling and Disabling Veeam Agent Notifications

When you launch Veeam Agent for Mac for the first time after installation, Veeam Agent will offer to configure Veeam Agent notifications.

To enable desktop notifications, hover over the **"Veeam Agent for Mac" Notifications** message and select **Options > Allow**.



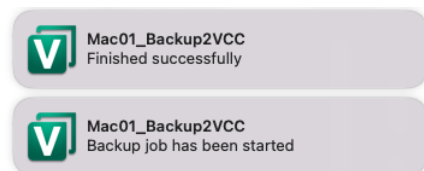
Alternatively, you can enable and disable Veeam Agent notifications in the System Preferences of the Mac computer. For details, see [Apple documentation](#).

Viewing Veeam Agent Notifications

After you enable the notifications, Veeam Agent will display information on the following events:

- Backup job was launched.
- Backup job got a warning during backup session.
- Backup job finished successfully.
- Backup job failed.

Once an event occurs, a message notifying about this event will appear in the notification center.



Reporting in Command Line Interface

You can view different session-related information in the Veeam Agent command line interface:

- [View session logs.](#)
- [View session information.](#)
- [View session list.](#)

Viewing Session Log

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:

```
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
2023-01-26 12:19:52 UTC [info] Job Daily Backup started at 2023-01-26 12:19:52 UTC
2023-01-26 12:19:56 UTC [info] Preparing to backup
2023-01-26 12:20:16 UTC [info] Waiting for backup infrastructure resources availability
2023-01-26 12:20:18 UTC [info] Creating volume snapshot
2023-01-26 12:20:53 UTC [info] Starting full backup to [backupserver001.tech.local] Default Backup Repository
2023-01-26 12:20:57 UTC [info] Backing up files /Users/commonuser, /Users/administrator
2023-01-26 12:21:23 UTC [info] Backing up summary.xml
2023-01-26 12:21:42 UTC [info] Releasing snapshot
2023-01-26 12:21:45 UTC [info] Processing finished at 2023-01-26 12:21:45 UTC
```

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:

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

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-f53dcfbc600e}
  State: Success
  Start time: 2023-01-11 14:37:21 UTC
  End time: 2023-01-11 14:40:02 UTC
```

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:

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

For example:

```
user@wrk001 ~ % veeamconfig session list

Job
name          Type      ID                               State   Created
at           Started at   Finished at

Daily Backup      Backup {404b6874-884c-4735-b19d-
42b1d46e961d} Success 2023-01-19 14:12 2023-01-19 14:12

Daily Backup      Backup {3968c2d4-9672-4049-aec0-
f7cd63520828} Success 2023-01-19 14:22 2023-01-19 14:22

Daily Backup      Backup {bc64e783-5703-48b9-8e5e-
80b88a336f99} Success 2023-01-19 14:32 2023-01-19 14:32

Daily Backup      Backup {49691302-74f3-4edc-891e-
f95f55eba47f} Failed  2023-01-19 14:42 2023-01-19 14:42

Mac Workstations Backup {51ba3622-dd83-4ef3-b381-
175ad1181d1a} Success 2023-01-19 22:05 2023-01-19 22:06
```



```
Mac Workstations Backup {42a01b26-de71-4a2f-9093-  
fc4a5361d73e} Success 2023-01-19 22:07 2023-01-19 22:08
```

Managing Configuration Database

IMPORTANT

Starting from version 2.1, exporting configuration database is no longer available; you can import only configuration files generated by Veeam Backup & Replication. You must import the configuration file generated by Veeam Backup & Replication, if Veeam Agent is managed by Veeam Backup & Replication as a member of a protection group for pre-installed Veeam Agents. For more information on importing configuration using the product UI, see [Importing Configuration from Veeam Backup Server](#).

If you work with Veeam Agent version 2.0, you can perform the following operations with the Veeam Agent configuration database:

- [Export configuration database to a configuration file.](#)
- [Import configuration database to Veeam Agent.](#)

Exporting Configuration Database

IMPORTANT

This functionality is not available in Veeam Agent version 2.1.

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:

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

where:

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

For example:

```
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

IMPORTANT

This functionality is not fully available in Veeam Agent version 2.1. You can import only configuration files generated by Veeam Backup & Replication. You must import the configuration file generated by Veeam Backup & Replication, if Veeam Agent is managed by Veeam Backup & Replication as a member of a protection group for pre-installed Veeam Agents. For more information on importing configuration using the product UI, see [Importing Configuration from Veeam Backup Server](#).

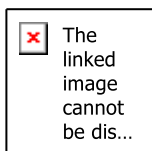
You import the Veeam Agent configuration from a file in the XML format to the configuration database. This may be useful, for example, if you have changed Veeam Agent for Mac settings by editing a configuration file or want to apply configuration of another instance of Veeam Agent to Veeam Agent installed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

You can import a Veeam Agent configuration in either of the following ways:

- [Using Veeam Agent control panel](#)
- [Using Veeam Agent status bar menu](#)
- [In command line interface](#)

Importing Configuration with Control Panel

From the Veeam Agent application menu, select **Settings > Import Configuration**; in the **Finder**, select the configuration file to import.



Importing Configuration with Status Bar Menu

From the Veeam Agent status bar menu, select **Import > Configuration**; in the **Finder**, select the configuration file to import.



Importing Configuration in Command Line Interface

To import the Veeam Agent configuration database in command line interface, 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, you can specify a local folder where Veeam Agent will save the log archive.
- [In command line interface](#) – in this case, Veeam Agent will save the log archive to the current working folder.

NOTE

If Veeam Agent operates in the managed mode, product logs are automatically exported to the Veeam backup server. For more information, see [Exporting Logs to Backup Server](#).

Exporting Logs with Control Panel and Status Bar Menu

You can export Veeam Agent logs from the Veeam Agent control panel or status bar menu. When you export logs, you can choose a folder where Veeam Agent should save the resulting log archive.

NOTE

Starting from version 2.1.2, Veeam Agent provides the **Help > Export logs to** menu with 2 options: *Local folder* and *Veeam server*. The *Veeam Server* option is available only when Veeam Agent operates in the managed mode. For more information on operating modes, see [Standalone and Managed Operation Modes](#).

If you use a prior version of Veeam Agent, to export product logs to a local folder, select **Help > Export Logs**.

Exporting Logs from Control Panel

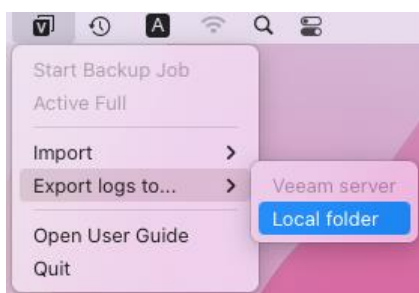
1. From the Veeam Agent application menu, select **Help > Export logs to > Local folder**.



2. In the **Finder** window, specify the location for the resulting log archive.

Exporting Logs from Status Bar Menu

1. From the Veeam Agent status bar menu, select **Help > Export logs to > Local folder**.



2. In the **Finder** window, specify the location for the resulting log archive.

Exporting Logs in 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:

```
veeamconfig grablogs
```

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

For example:

```
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

If you have the Veeam backup infrastructure deployed in the production environment, you can use Veeam Agent together with Veeam Backup & Replication.

IMPORTANT

If you plan to use Veeam Agent for Mac 2.1 with Veeam Backup & Replication, you must install Veeam Backup & Replication 12.1 on the Veeam backup server.

If you plan to use Veeam Agent for Mac 2.0 with Veeam Backup & Replication, you must install Veeam Backup & Replication 12.0 or later on the Veeam backup server.

For more information on managing connection to a Veeam backup server, see [Managing Veeam Backup & Replication Servers](#).

NOTE

This and subsequent sections describe tasks with Veeam Backup & Replication available for Veeam Agent operating in the standalone mode. For information about tasks available in Veeam Backup & Replication within the Veeam Agent management scenario, see the [Veeam Agent Management Guide](#).

Tasks with Veeam Backup & Replication

Veeam Backup & Replication lets you perform a number of additional data protection and disaster recovery tasks, as well as administrative actions with Veeam Agent backups. You can:

- [Grant access permissions on backup repositories](#).
- [Manage Veeam Agent licenses](#).

Data protection tasks

- [Create Veeam Agent backups on backup repositories](#).
- [Create Veeam Agent backups on Veeam Cloud Connect repositories](#).
- [Copy Veeam Agent backups to secondary backup repositories](#).
- [Archive Veeam Agent backups to tape](#).

Restore tasks

- [Restore files and folders from Veeam Agent backups](#).
- [Restore disks from Veeam Agent backups](#).
- [Publish disks to analyze backup content](#).
- [Export restore points of Veeam Agent backups to standalone full backup files](#).

Administrative tasks

- [Import Veeam Agent backups](#).
- [Enable and disable Veeam Agent backup jobs](#).

- [Delete Veeam Agent backup jobs.](#)
- [View Veeam Agent backup properties.](#)
- [Remove Veeam Agent backups.](#)
- [Delete Veeam Agent backups.](#)
- [Configure global settings.](#)
- [Assign roles to users.](#)

Setting Up User Permissions on Backup Repositories

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

IMPORTANT

Veeam Agent for Mac does not support Veeam backup repositories with enabled KMS encryption. To learn more about KMS encryption for Veeam backup repositories, see the [Key Management System Keys](#) section in the Veeam Backup & Replication User Guide.

NOTE

If you plan to create backups in 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 in this backup repository.

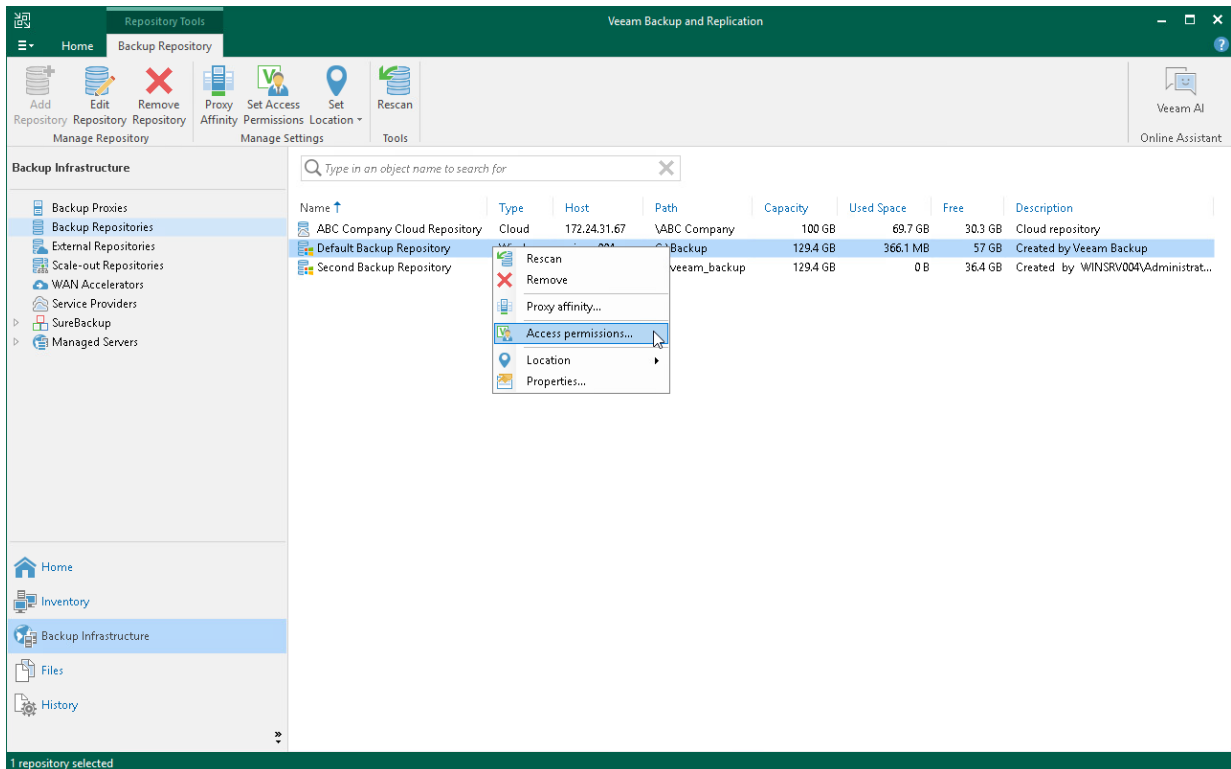
Right after installation, access permissions on the default backup repository are set to *Allow to everyone* for testing and evaluation purposes. If necessary, you can change these settings.

After you create a new backup repository, access permissions on this repository are set to *Deny to everyone*. To allow users to store backups in 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.

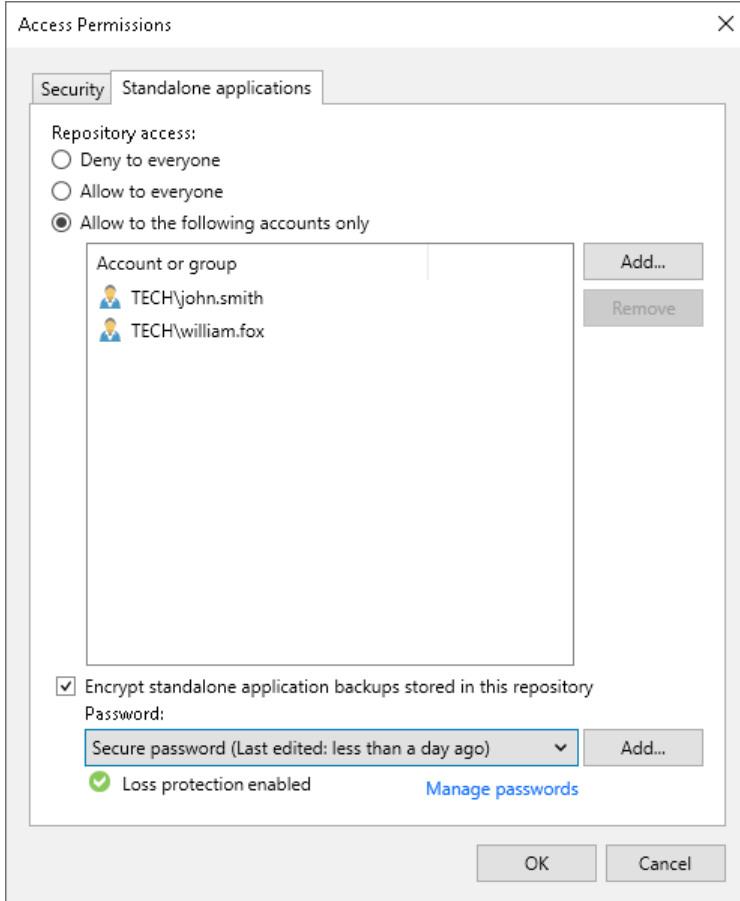
3. In the working area, select the necessary backup repository and click **Set Access Permissions** on the ribbon, or right-click the backup repository and select **Access permissions**. If you do not see the **Set Access Permissions** button on the ribbon or the **Access permissions** command is not 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, in the **Standalone applications** tab, 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). However, we recommend this scenario 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 in 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 at the backup repository side using its built-in encryption mechanism. To learn more, see [Veeam Backup & Replication Documentation](#).

IMPORTANT

If Veeam Agent is set up to use the backup cache, and the backup cache contains one or more restore points, Veeam Agent will automatically remove these restore points from the backup cache after you enable or disable the encryption option for the backup repository.



Managing License

If you plan to use Veeam Agent with Veeam Backup & Replication, you must install a license in Veeam Backup & Replication or Veeam Backup Enterprise Manager. The license must have a total number of instances that is sufficient to protect machines (servers and workstations) on which you plan to install Veeam Agent. For more information, see [Veeam Licensing Policy](#).

After Veeam Agent connects to Veeam Backup & Replication, Veeam Agent automatically starts consuming instances in the license. The product edition for Veeam Agent is selected depending on the type of the OS running on the Veeam Agent computer. You can switch to another commercial edition of Veeam Agent manually if needed. If you do not want Veeam Agents to consume instances, you can restrict instance consumption. For more information, see [Managing Instance Consumption by Veeam Agents](#).

The number of backup jobs configured in Veeam Agent does not impact instance consumption. For example, if 2 backup jobs are configured in Veeam Agent that operates in the Server edition, this Veeam Agent will consume instances required for 1 server.

Veeam Agent obtains information about the license from Veeam Backup & Replication and keeps it locally on the Veeam Agent computer. Information about the license is valid for 32 days. If Veeam Agent does not connect to Veeam Backup & Replication during this period, Veeam Backup & Replication will revoke its license.

NOTE

In addition to managing Veeam Agent licenses, you can use the Veeam Backup & Replication console to manage Veeam Agent backup jobs and perform operations with backups created by these jobs.

If your backup server is connected to Veeam Backup Enterprise Manager, you can use Veeam Backup Enterprise Manager to manage licenses and perform restore tasks with Veeam Agent backups. You cannot manage Veeam Agent backup jobs with Veeam Backup Enterprise Manager.

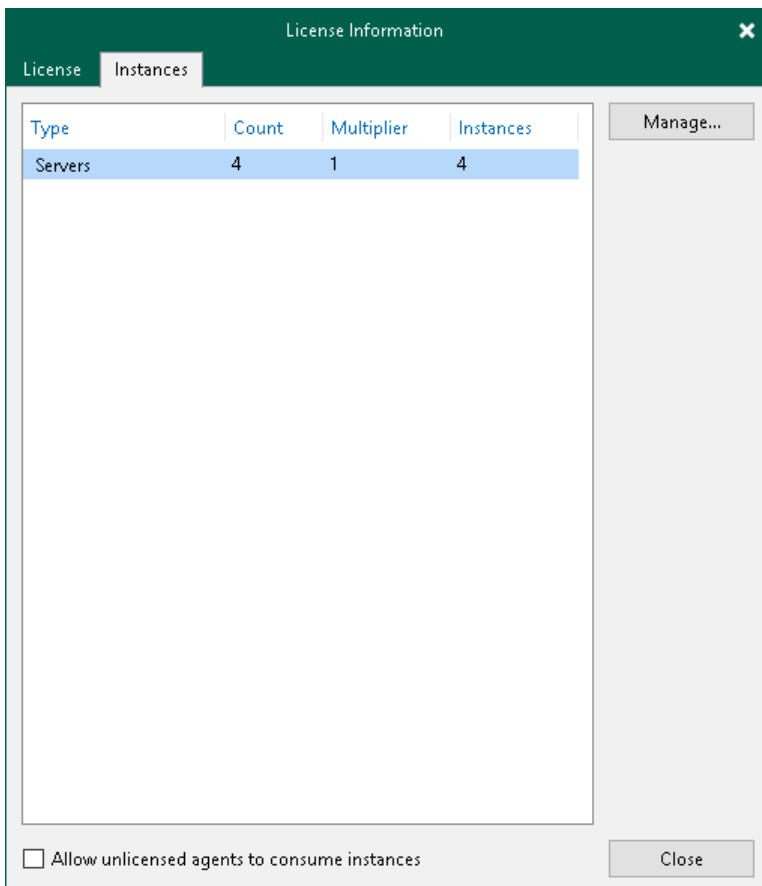
Managing Instance Consumption by Veeam Agents

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.

If you restrict instance consumption, Veeam Backup & Replication will switch all Veeam Agents connected to this Veeam backup server to the free edition that offers limited capabilities. For information about Veeam Agent editions, see [Product Editions](#).

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**.



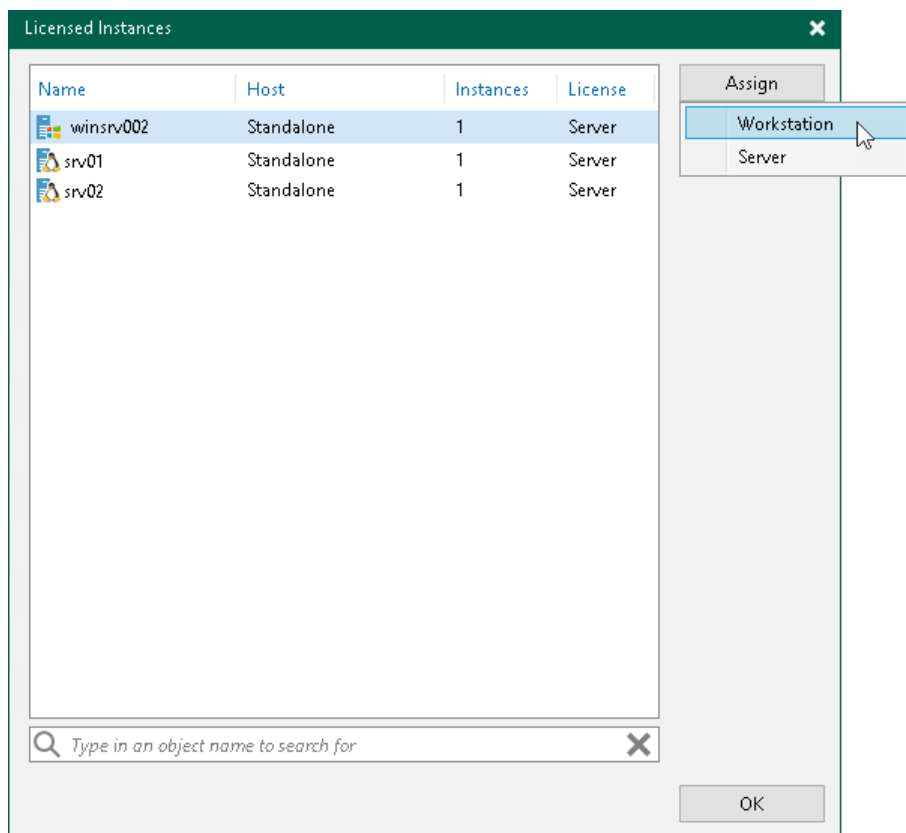
Assigning License to Veeam Agent

After Veeam Agent connects to Veeam Backup & Replication, Veeam Agent automatically starts consuming the license. The product edition for Veeam Agent is selected depending on the type of the OS running on the protected computer.

You can also assign a license to Veeam Agent manually if needed. When you assign a license, you can select the product edition, too.

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 product edition: *Workstation* or *Server*.



Viewing Licensed Veeam Agents and Revoking License

When Veeam Agent 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**.

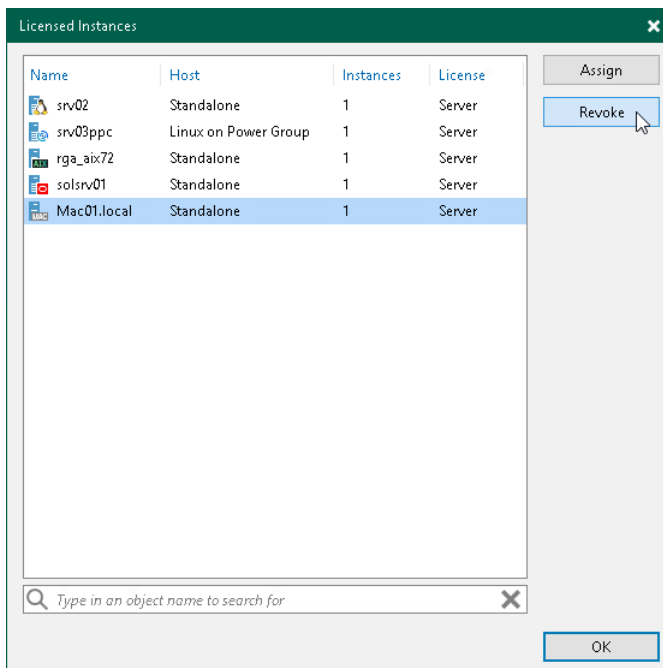
In the list of licensed instances, Veeam Backup & Replication displays Veeam Agents that have established a connection with the backup server when you created the backup job.

Revoking License from Veeam Agents

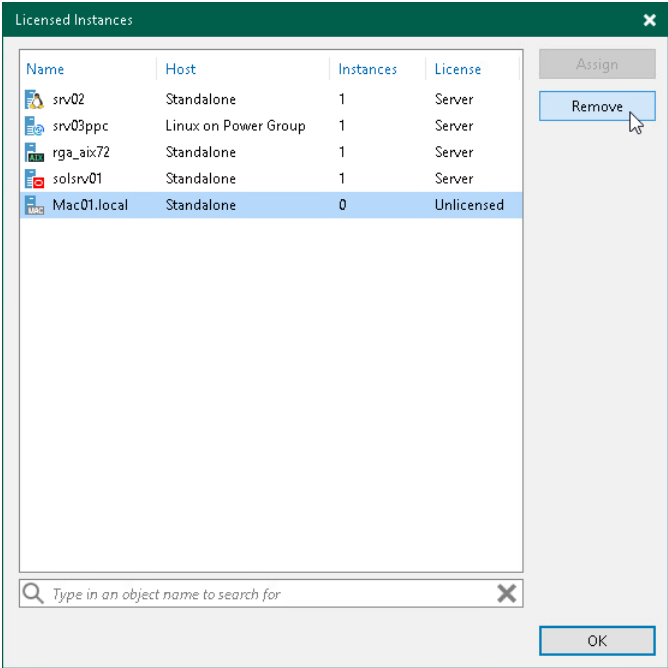
You can revoke the license from some Veeam Agents and re-apply it to other protected workloads. License revoking can be helpful, for example, if you do not want to use some Veeam Agents with Veeam Backup & Replication anymore.

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 a Veeam Agent and click **Revoke**. Veeam Backup & Replication will revoke the license from the Veeam Agent, and the license will be freed for other workloads that you want to protect with Veeam products.



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.



Performing Data Protection Tasks

You can perform the following data protection tasks:

- Back up your data and store the resulting backup files in one of the following types of Veeam backup repositories:
 - [In a backup repository managed by a Veeam backup server](#)
 - [In a Veeam Cloud Connect repository](#)
- [Copy Veeam Agent backups from the backup repository to a secondary backup repository with backup copy jobs.](#)
- [Archive Veeam Agent backups to tapes with backup to tape jobs.](#)

Backing Up to Backup Repositories

You can store backups created with Veeam Agent in backup repositories connected to Veeam backup servers. To do this, you must perform the following actions:

1. [Set up user permissions at the backup repository side.](#)
2. [Point the Veeam Agent backup job to the backup repository.](#)

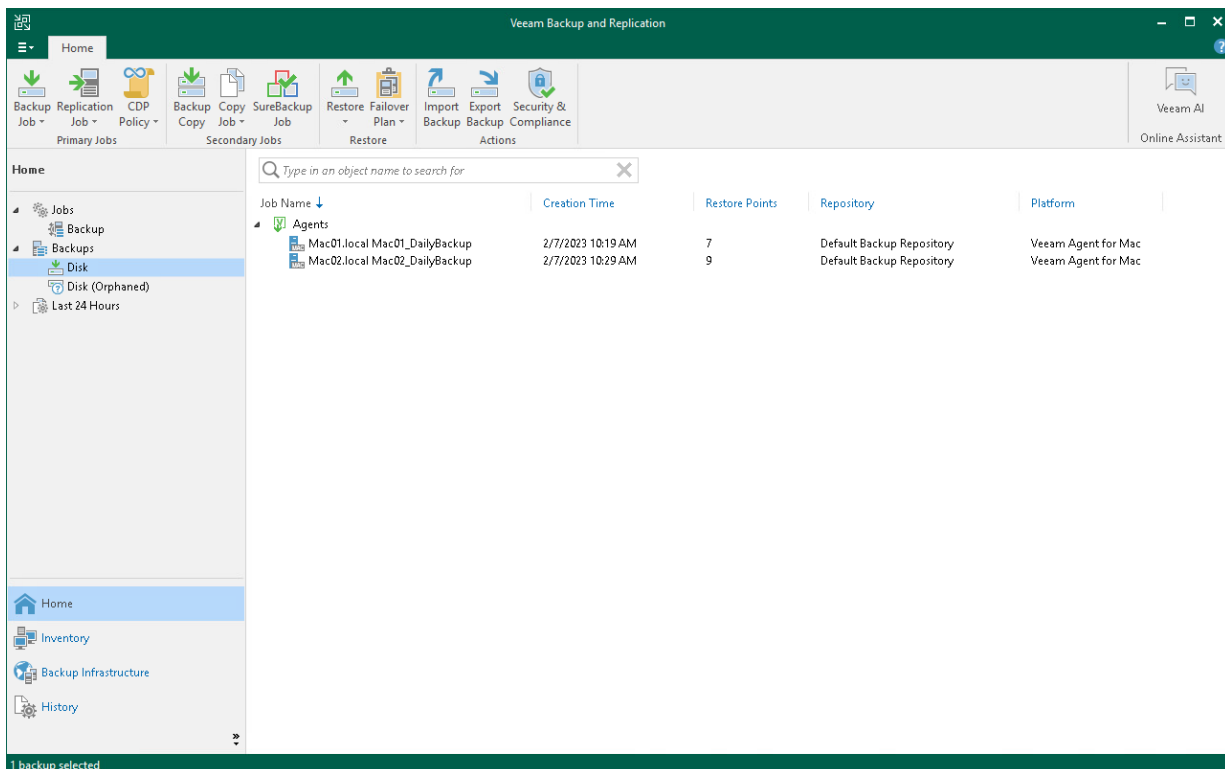
NOTE

Consider the following:

- A Veeam Agent backup job can be started automatically upon the defined schedule or manually from the Veeam Agent computer. You cannot start, stop, retry or edit Veeam Agent backup jobs in the Veeam Backup & Replication console.
- If the user is granted restore permissions on the Veeam backup server, the user will be able to see all backups in the backup repository.
- The user who creates a Veeam Agent backup in the backup repository is set as the owner of the backup file. The backup file owner can access this file and restore data from it. If the user who is not the backup file owner needs to perform operations with the backup file, the user must have the Veeam Backup & Replication role that allows to perform these operations. To learn more about roles, see the [Users and Roles](#) section in the Veeam Backup & Replication User Guide.

Backup jobs targeted at the backup repository become visible in Veeam Backup & Replication under the **Jobs > Backup** node in the **Home** view. Backups created with Veeam Agent are available under the **Backups > Disk** node in the **Home** view.

The Veeam Backup Administrator working with Veeam Backup & Replication can manage Veeam Agent backup jobs and restore data from Veeam Agent backups. To learn more, see [Restoring Data from Veeam Agent Backups](#) and [Performing Administration Tasks](#).



Backing Up to Cloud Repositories

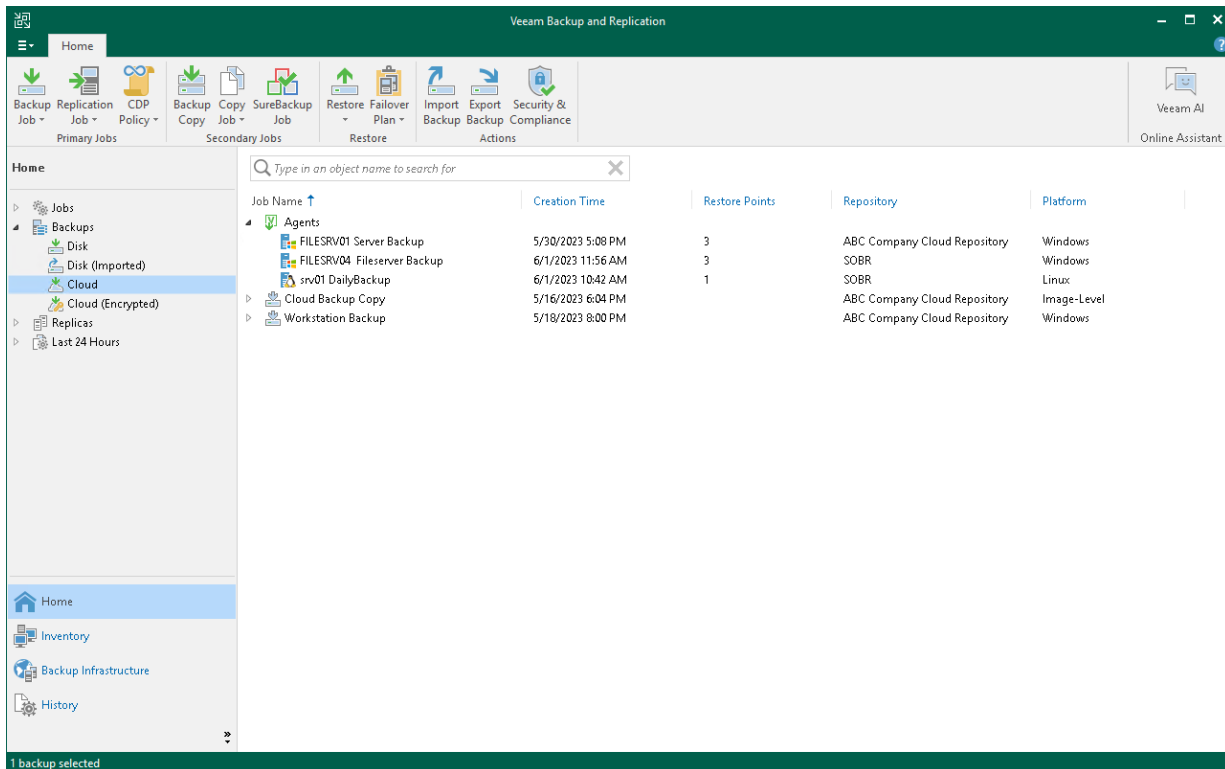
You can store backups created with Veeam Agent in cloud repositories provided to you by a Veeam Cloud Connect service provider. To do this, you must connect to the service provider and point the backup job to the cloud repository. To learn more, see [Specify Service Provider Settings](#).

Veeam Agent Backups on Tenant Side

Backups created with Veeam Agent are available under the **Cloud** node in the **Home** view of the Veeam Backup & Replication console deployed on the tenant side.

The backup administrator working with Veeam Backup & Replication on the tenant side can manage Veeam Agent backups created in the cloud repository and restore data from such backups. To recover data from a Veeam Agent backup, you can perform the following operations:

- [Export computer disks as virtual disks](#).
- [Restore guest OS files](#).
- [Export restore points to standalone full backup files](#).



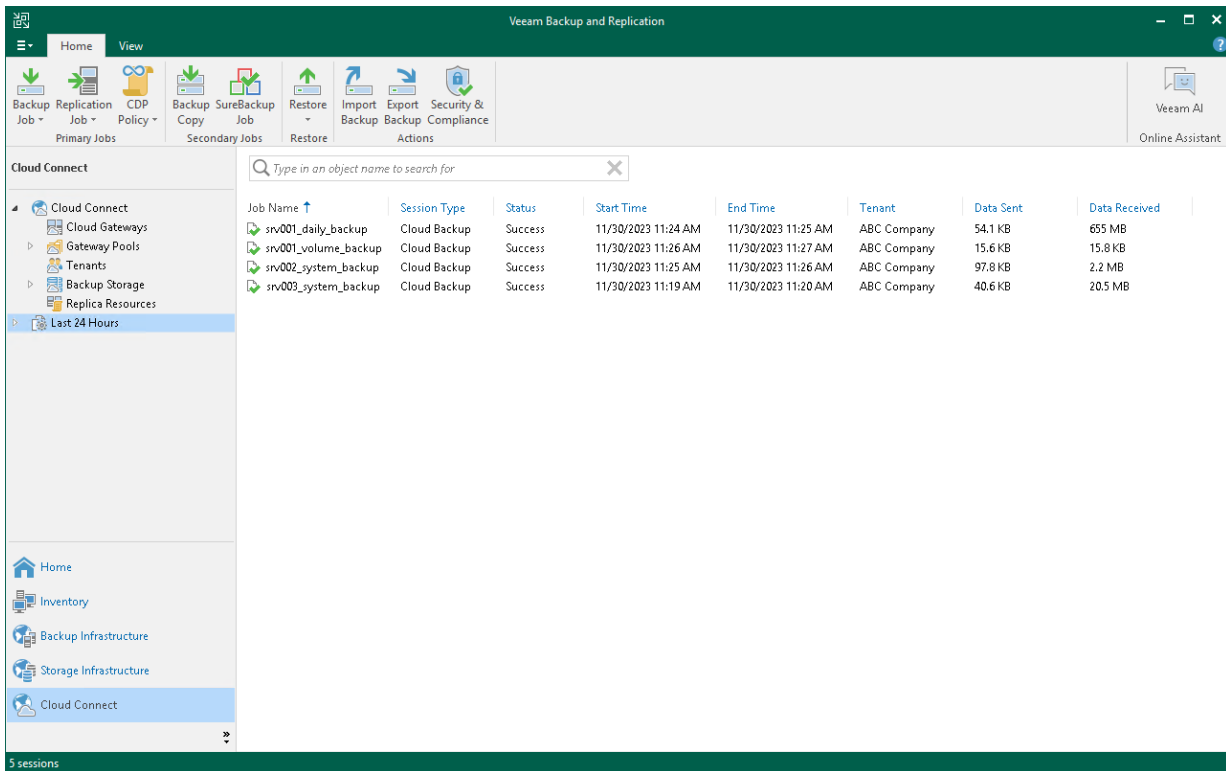
Veeam Agent Backups on Service Provider Side

The service provider can view information about backup and restore sessions performed by Veeam Agent users. The full list of sessions is available in the **History** view of the Veeam backup console deployed on the service provider side. The list of sessions performed within the last 24 hours is available under the **Last 24 hours** node in the **Cloud Connect** view of the Veeam backup console on the service provider side. The service provider cannot view detailed statistics about individual sessions in the list.

The service provider cannot perform restore tasks with Veeam Agent backups that are stored in the cloud repository. The service provider can perform the following restore tasks with unencrypted Veeam Agent backups stored in the cloud repository:

- Instant recovery
- Disk restore
- Disk publish

To learn more, see the [Restoring Data from Tenant Backups](#) section in the Veeam Cloud Connect Guide.

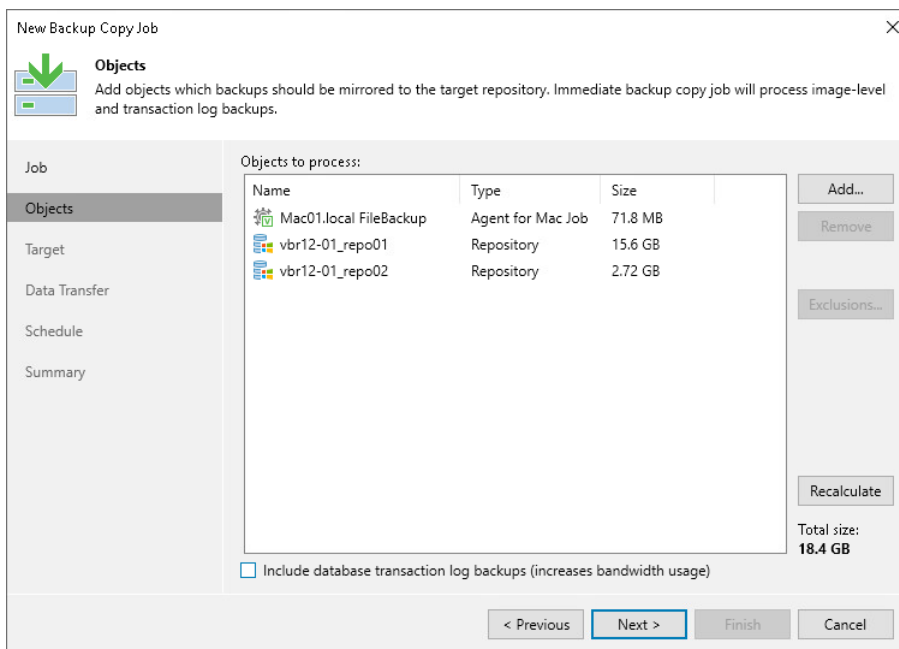


Performing Backup Copy for Veeam Agent Backups

You can configure backup copy jobs that will copy backups created with Veeam Agent to a secondary backup repository.

Backup copy jobs treat Veeam Agent backups as usual backup files. The backup copy job setup and processing procedures practically do not differ from the same procedures for a backup copy job that processes VM backups. To learn more about backup copy jobs, see the [Backup Copy](#) section in the Veeam Backup & Replication User Guide.

When mapping a backup copy job to a Veeam Agent backup, consider the limitations listed in the [Map Backup File](#) section in the Veeam Backup & Replication User Guide.



Restoring Data from Copies of Veeam Agent Backups

Backups copied to the secondary backup repository do not preserve user access permissions. At the same time, users who created backups do not have access permissions on these secondary repositories. For this reason, users cannot restore data from their backups residing in the secondary site.

To overcome this limitation, you can delegate the restore task to backup administrators who work with Veeam Backup & Replication. Backup administrators can use Veeam Backup & Replication options to recover data from such backups: for example, perform file-level restore or retrieve necessary application items with Veeam Explorers.

You can also restore data from the copied backup stored in the target repository using Veeam Agent.

Restoring Data from Veeam Agent Backups

You can perform the following restore operations:

- [Restore individual files and folders from Veeam Agent backups](#)
- [Export computer disks as VMDK, VHD or VHDX disks](#)
- [Publish disks to analyze backup content](#)
 - [Export restore points of Veeam Agent backups to standalone full backup files](#)

Restoring Files and Folders

You can use the Veeam Backup & Replication console to restore individual files and folders from Veeam Agent backups.

The procedure of file-level restore from a Veeam Agent backup is similar to the same procedure for a VM backup. To learn more about file-level restore, see the [Restore from Linux, Unix and Other File Systems](#) section in the Veeam Backup & Replication User Guide.

Consider the following: When you perform the file-level restore procedure, Veeam Backup & Replication provides the following options for mounting disks of the machine from the backup or replica:

- Mounting disks to a helper host – any Linux host from your infrastructure with a [supported operating system](#).
- Mounting disks to a temporary helper appliance – a helper VM required to mount Linux computer disks from the backup.

If you have selected to mount disks to a temporary helper appliance, it is recommended that you add a vCenter Server and not a standalone ESXi host in the Veeam backup console. If Veeam Backup & Replication is set up to deploy a helper appliance on a standalone ESXi host, after Veeam Backup & Replication removes the helper appliance, the helper VM will be displayed in vCenter as *orphaned*. You cannot restore files or folders from Veeam Agent for Mac backup to the original machine. You can only save files and folders to a new location over the network by using the **Copy To** option.

Exporting Disks

You can restore computer disks from Veeam Agent backups created using Veeam Agent for Mac and convert them to disks of the VMDK, VHD or VHDX format.

During disks restore, Veeam Backup & Replication creates standard virtual disks that can be used by VMware vSphere and Microsoft Hyper-V VMs.

- When you restore a disk in the VMDK format, Veeam Backup & Replication creates a pair of files that make up the VM virtual disk: a descriptor file and file with the virtual disk content.
- When you restore a disk in the VHD/VHDX format, Veeam Backup & Replication creates a file of the VHD or VHDX format.

You can save converted disks locally on any server or SMB share added to the backup infrastructure or place disks on a datastore connected to an ESXi host (for VMDK disk format only). VMDK disks can be restored as thin provision and thick disks:

- Disks restored to a datastore are saved in the thin provisioned format.
- Disks restored to a server are saved in the thick provisioned format.

Veeam Backup & Replication supports batch disk restore. For example, if you choose to restore 2 computer disks, Veeam Backup & Replication will convert them to 2 virtual disks and store these disks in the specified location.

IMPORTANT

Consider the following:

- If the backup from which you restore disks contains a Btrfs storage pool, during the disk restore process Veeam Backup & Replication will create a separate disk and restore the Btrfs pool to this disk.
- If the disk you want to restore contains an LVM volume group, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. Among other things, this leads to the increase of the required storage space. For example, you restore a machine with 2 disks, and a separate LVM volume group is configured on each of these disks. In this case, Veeam Agent will restore 4 disks. The restored disks will consume storage space equal to the size of 2 original disks and 2 LVM volume groups from these disks.

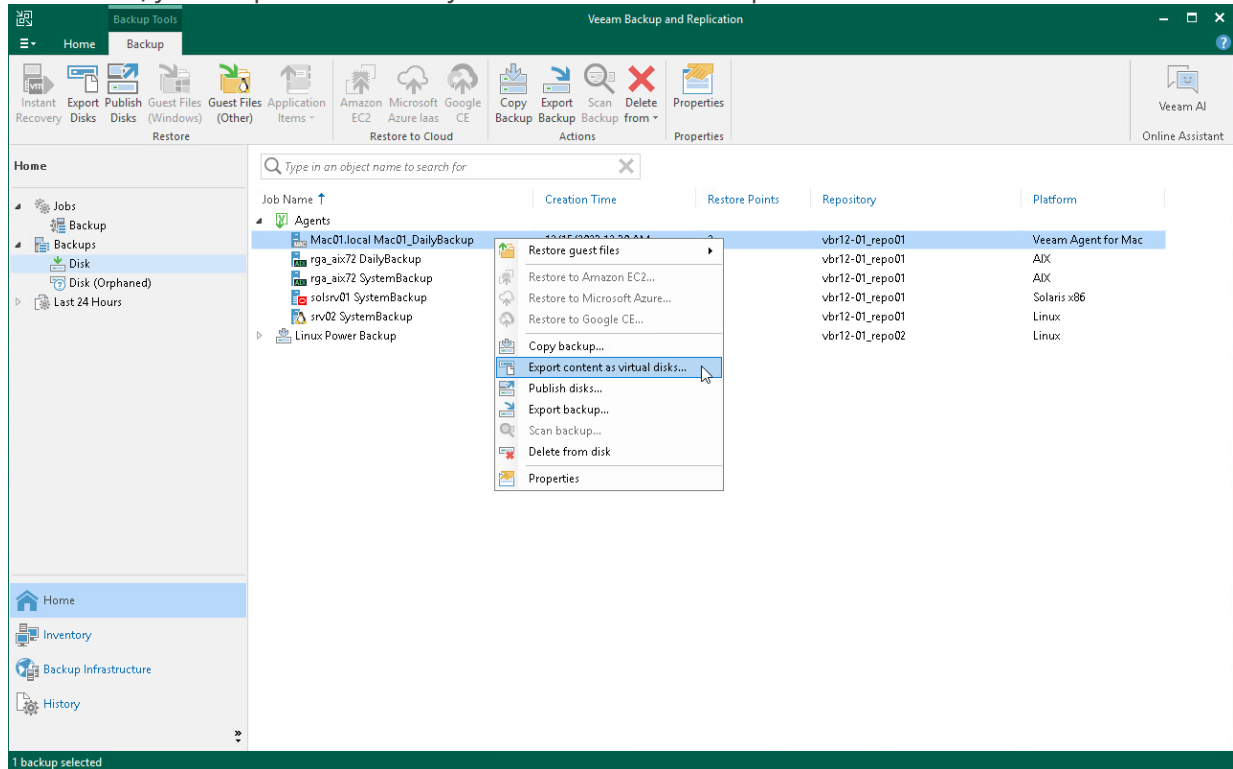
To restore disks and convert them to the VMDK, VHD or VHDX format, perform the following steps in the **Export Disk** wizard:

Step 1. Launch Export Disk Wizard

To launch the **Export Disk** wizard, do either of the following:

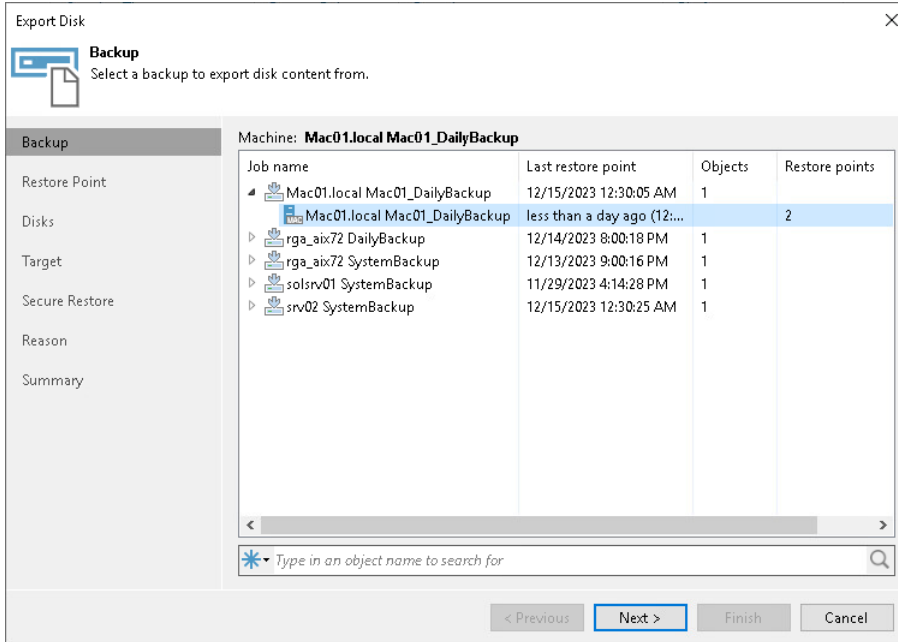
- Open the **Home** tab and click **Restore > Agent > Disk restore > Export disk**. In this case, you will be able to select a backup of the necessary Veeam Agent computer at the **Backup** step of the wizard.
- Open the **Home** view. In the inventory pane, click the **Backups** node. In the working area, expand the necessary Veeam Agent backup, select the necessary computer in the backup and click **Export Disks** on the ribbon or right-click a computer in the backup and select **Export content as virtual disks**.

In this case, you will pass immediately to the **Restore Point** step of the wizard.



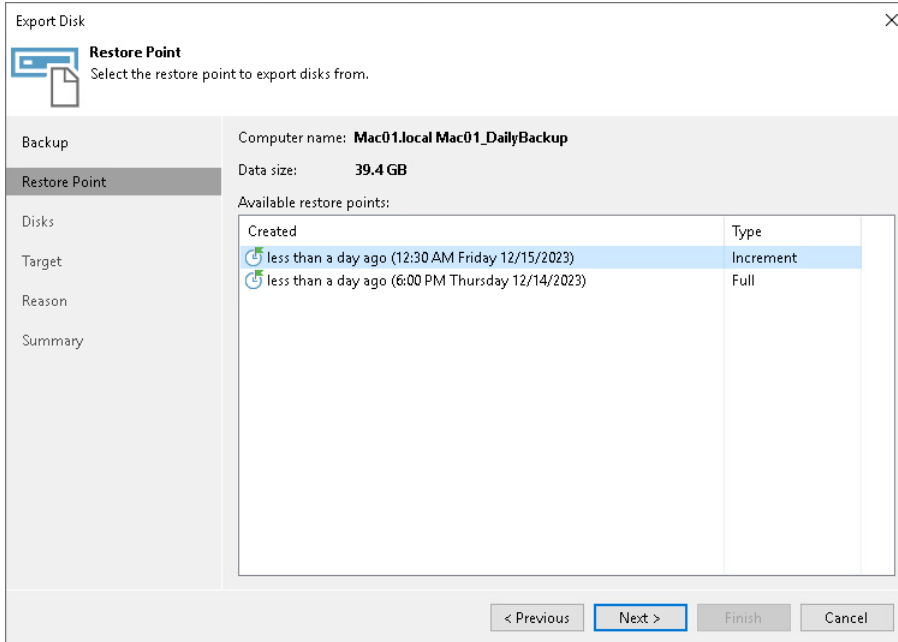
Step 2. Select Backup

At the **Backup** step of the wizard, select a backup from which you want to restore disks. In the list of backups, Veeam Backup & Replication displays all backups that are currently hosted on the Veeam backup repository and Veeam Cloud Connect repository.



Step 3. Select Restore Point

At the **Restore Point** step of the wizard, select the necessary restore point from which you want to restore disks. In the list of points, Veeam Backup & Replication displays all restore points that have been created. Make sure that you select a restore point that relates to the selected backup.



Step 5. Select Destination and Disk Format

At the **Target** step of the wizard, select the destination for disk export and format in which you want to save the resulting virtual disk.

1. From the **Server** list, select a server on which the resulting virtual disks must be saved. If you plan to save the disks in the VMDK format on a datastore, select an ESXi host to which this datastore is connected.
2. In the **Path to folder** field, specify a folder on the server or datastore where the virtual disks must be placed.
3. Select the export format for disks:
 - **VMDK** – select this option if you want to save the resulting virtual disk in the VMware VMDK format.
 - **VHD** – select this option if you want to save resulting virtual disk in the Microsoft Hyper-V VHD format.
 - **VHDX** – select this option if you want to save resulting virtual disk in the Microsoft Hyper-V VHDX format (supported by Microsoft Windows Server 2012 and later).
4. Click **Disk type** to specify how the resulting disk must be saved:
 - [For VMDK disk format] in the thin provisioned, lazy zeroed thick provisioned, or eagerly zeroed thick provisioned format
 - [For VHD and VHDX disk formats] in the dynamic or fixed format
5. [For export of a VMDK disk to an ESXi host] Click the **Pick proxy to use** link to select backup proxies over which backup data must be transported to the target datastore.

NOTE

Consider the following:

- If you have selected to store the resulting virtual disk in a datastore, you will be able to save the virtual disk in the VMDK format only. Other options will be disabled.
- If you have selected to store the resulting virtual disk on the server running Microsoft Windows Server OS and in the VMDK format, you will be able to save the virtual disk in the lazy zeroed thick provisioned format only.

The screenshot shows the 'Export Disk' dialog box with the 'Target' tab selected. The dialog is titled 'Export Disk' and has a close button (X) in the top right corner. Below the title bar, there is a 'Target' icon and the text 'Specify the destination server and folder, and a virtual disk format to export disk content to.' The main area is divided into two columns. The left column contains a list of steps: 'Backup', 'Restore Point', 'Disks', 'Target' (highlighted), 'Reason', and 'Summary'. The right column contains the following fields and options:

- Server:** A dropdown menu with the value 'winsrv0042019.tech.local'.
- Path to folder:** A text input field containing 'C:\WeeamBackup' and a 'Browse...' button to its right.
- Export format:** Three radio button options:
 - VMDK** (selected): This virtual disk type is used by VMware products such as VMware Workstation, or VMware vSphere. Maximum VMDK disk size is 62TB. Pick proxy to use.
 - VHD**: This virtual disk type is used by Microsoft products such as Microsoft Hyper-V or Microsoft Azure. Maximum VHD disk size is 2TB.
 - VHDX**: This virtual disk type is used by more recent versions of Microsoft products such as Microsoft Hyper-V. Maximum VHDX disk size is 64TB.
- Disk type:** A dropdown menu with the value 'Thick (lazy)'.

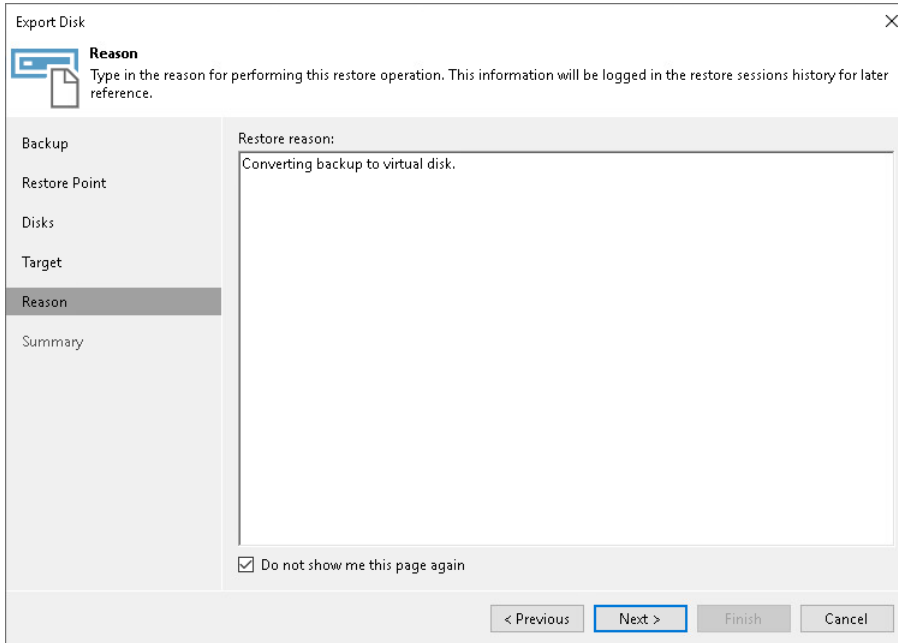
At the bottom of the dialog, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 6. Specify Restore Reason

At the **Reason** step of the wizard, enter a reason for restoring the computer volume.

TIP

If you do not want to display the **Restore Reason** step of the wizard in future, select the **Do not show me this page again** check box.

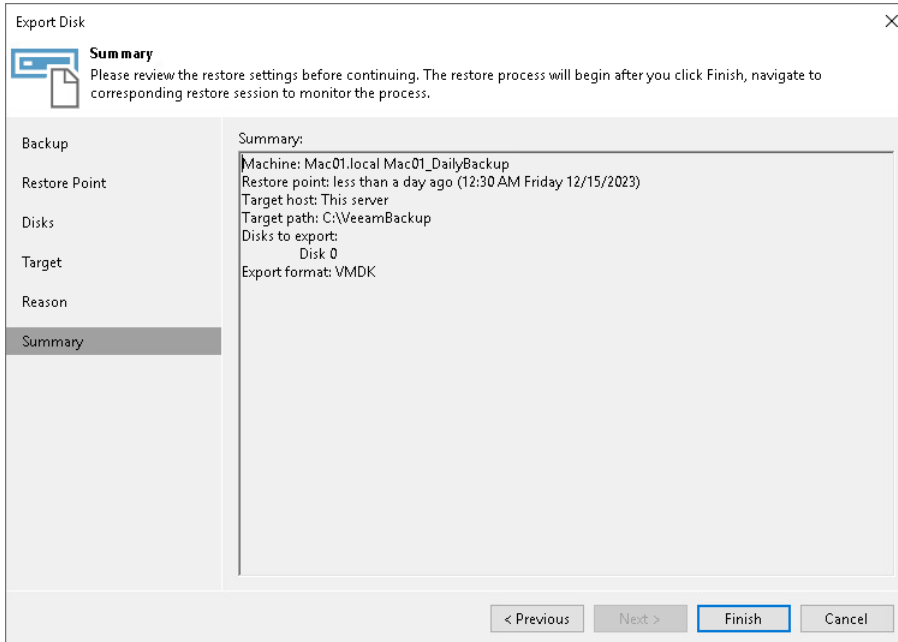


The screenshot shows the 'Export Disk' wizard window, specifically the 'Reason' step. The window title is 'Export Disk' and it has a close button (X) in the top right corner. On the left side, there is a navigation pane with the following steps: Backup, Restore Point, Disks, Target, Reason (highlighted), and Summary. The main area of the wizard is titled 'Reason' and contains the following text: 'Type in the reason for performing this restore operation. This information will be logged in the restore sessions history for later reference.' Below this text is a large text input field with the text 'Converting backup to virtual disk.' entered. At the bottom left of the main area, there is a checkbox labeled 'Do not show me this page again' which is checked. At the bottom right of the window, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

Step 7. Complete Restore Process

At the **Summary** step of the wizard, complete the disk restore procedure.

1. Review details for the disk to be restored.
2. Click **Finish** to start the restore procedure and exit the wizard.



Publishing Disks

Starting from Veeam Backup & Replication version 12.1, you can use the Veeam backup console to publish disks from backups created by Veeam Agent backup jobs and backup copy jobs.

TIP

If you use Veeam Backup & Replication version 12.0 or later, you can publish disks using the PowerShell console. To learn more, see the [Disk Publishing \(Data Integration API\)](#) section in the Veeam PowerShell Reference.

Disk publishing allows you to save time by getting backup content of one or multiple disks instead of all disks from a backup. This technology gives read-only access to data and helps if you want to analyze data of your backup. For example, look for specific documents or usage patterns, or perform antivirus scan of backed-up data.

For macOS-based Veeam Agent computers, disk publishing uses the FUSE protocol. After the publishing, the target server can access the backup content using the FUSE protocol and read the necessary data from the disk.

To learn more, see the [Disk Publishing](#) section in the Veeam Backup & Replication User Guide.

Performing Disk Publish

Before you publish disks, [check prerequisites](#). Then use the **Publish Disks** wizard.

1. [Launch the wizard](#).
2. [Select a Veeam Agent computer whose disks you want to publish](#).
3. [Select a restore point](#).
4. [Select disks](#).
5. [Specify the target server](#).
6. [Specify a reason for disk publishing](#).
7. [Finish working with the wizard](#).

Before You Begin

Before you publish disks, check the following requirements and limitations:

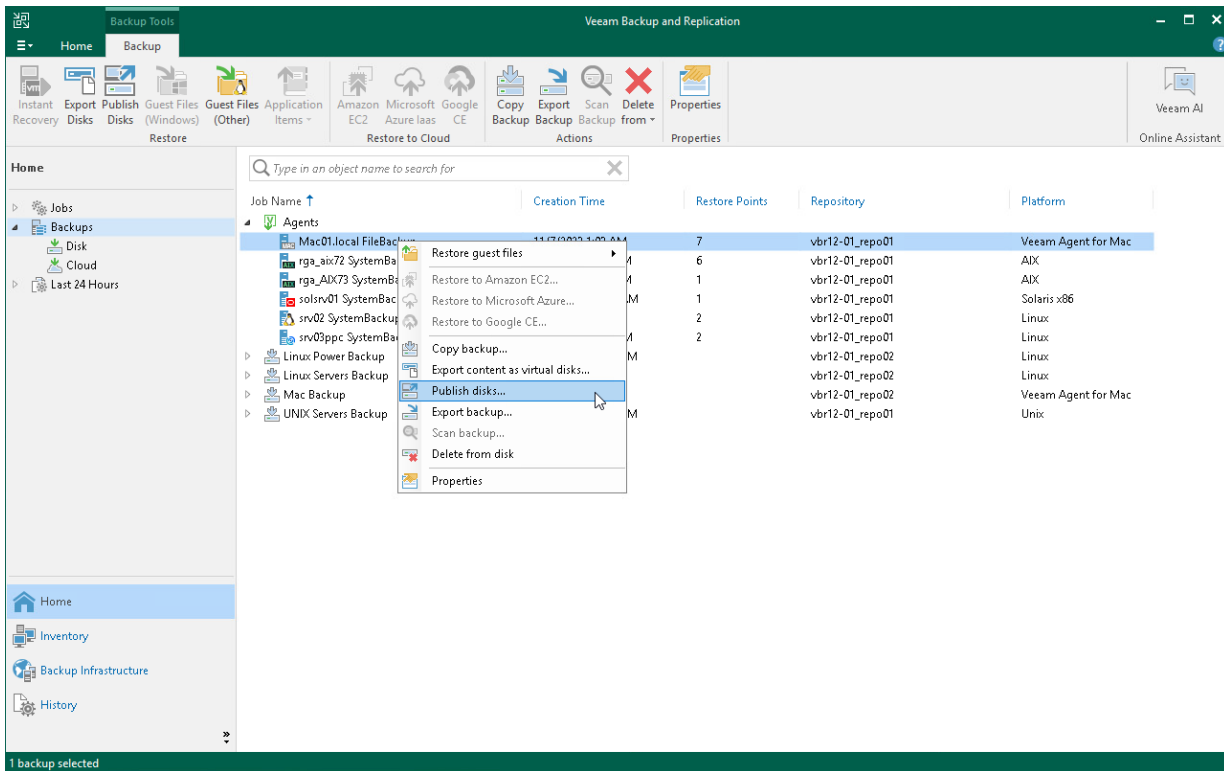
- The necessary ports must be opened on the target server. For more information, see [Ports](#).
- The target server must support the file system of the disk that you plan to publish.
- If data deduplication is enabled for some disks in a backup, data deduplication must be enabled on the target server.
- The 32-bit version of a Linux server is not supported as the target server.
- You cannot publish disks from backups stored in the Veeam Cloud Connect repository.

For the full list of limitations, see the [Considerations and Limitations](#) section in the Veeam Backup & Replication User Guide.

Step 1. Launch Publish Disks Wizard

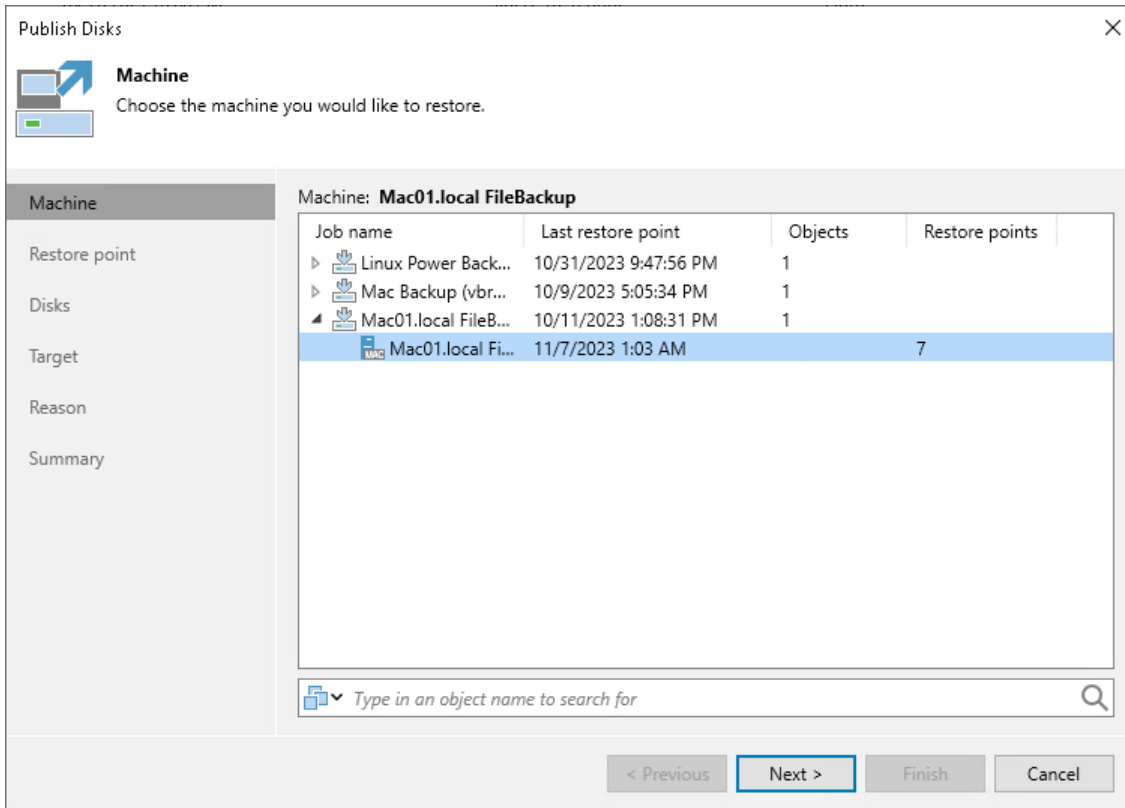
To launch the **Publish Disks** wizard, do either of the following:

- On the **Home** tab, click **Restore > Agent > Disk Restore > Publish disk**.
- Open the **Home** view. In the inventory pane, click **Backups**. In the working area, expand the necessary Veeam Agent backup, select a computer whose disks you want to publish and click **Publish Disks** on the ribbon. Alternatively, you can right-click the computer and select **Publish disks**. In this case, you will proceed to the [Restore point](#) step of the wizard.



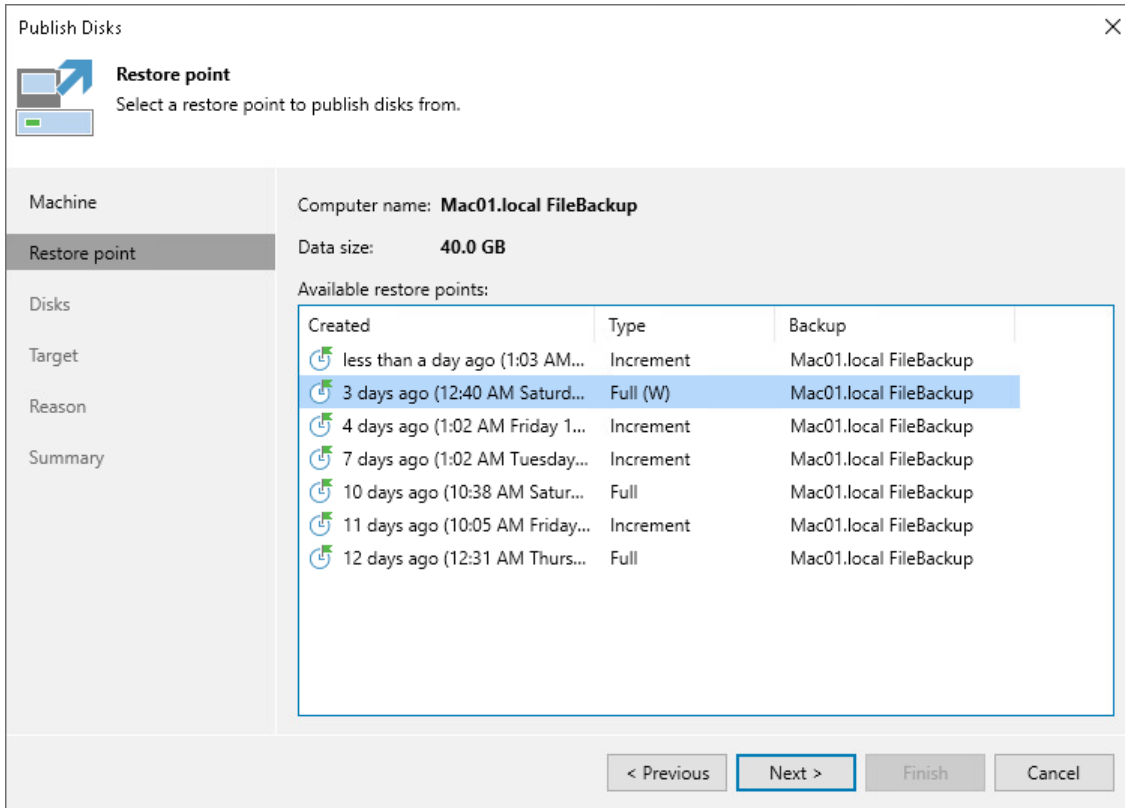
Step 2. Select Computer

At the **Machine** step of the wizard, expand a backup and select a Veeam Agent computer whose disks you want to publish.



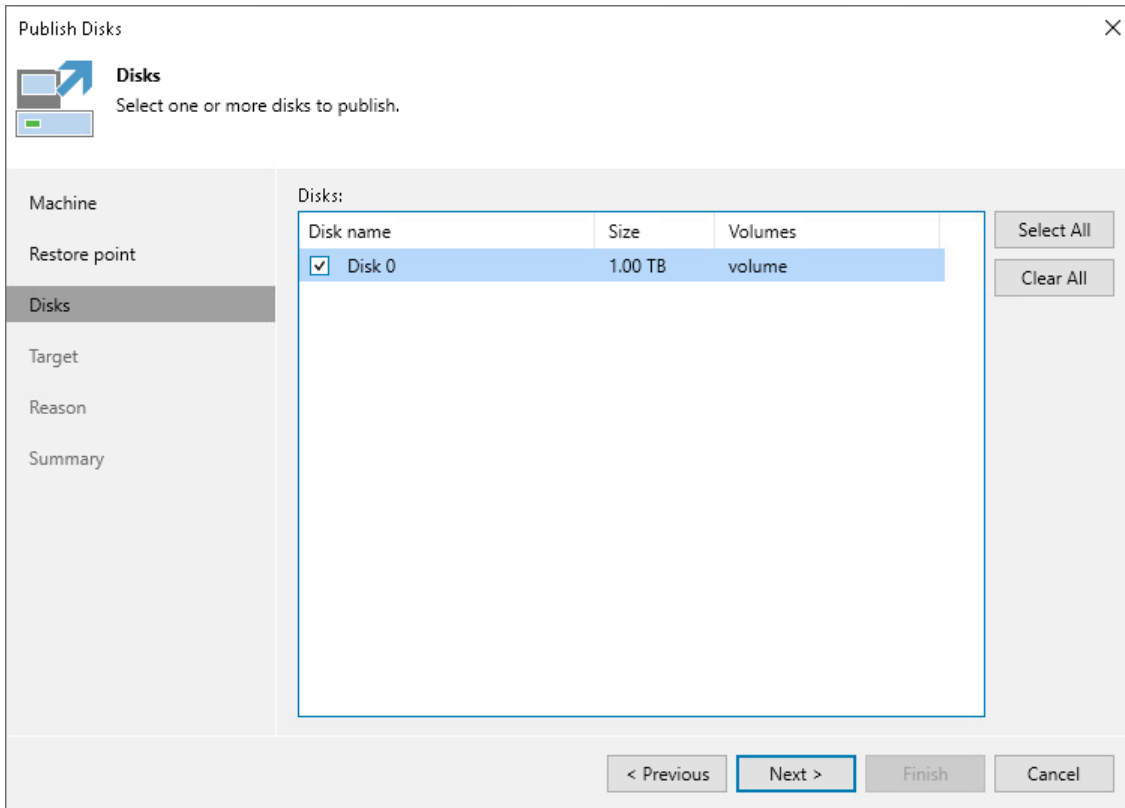
Step 3. Select Restore Point

At the **Restore Point** step of the wizard, select a restore point from which you want to publish disks.



Step 4. Select Disks

At the **Disks** step of the wizard, select a check box next to the disks that you want to publish. Click **Select All** if you want to select all disks from the backup.



Step 5. Select Target Server

At the **Target** step of the wizard, select a Linux server that will have access to disk content.

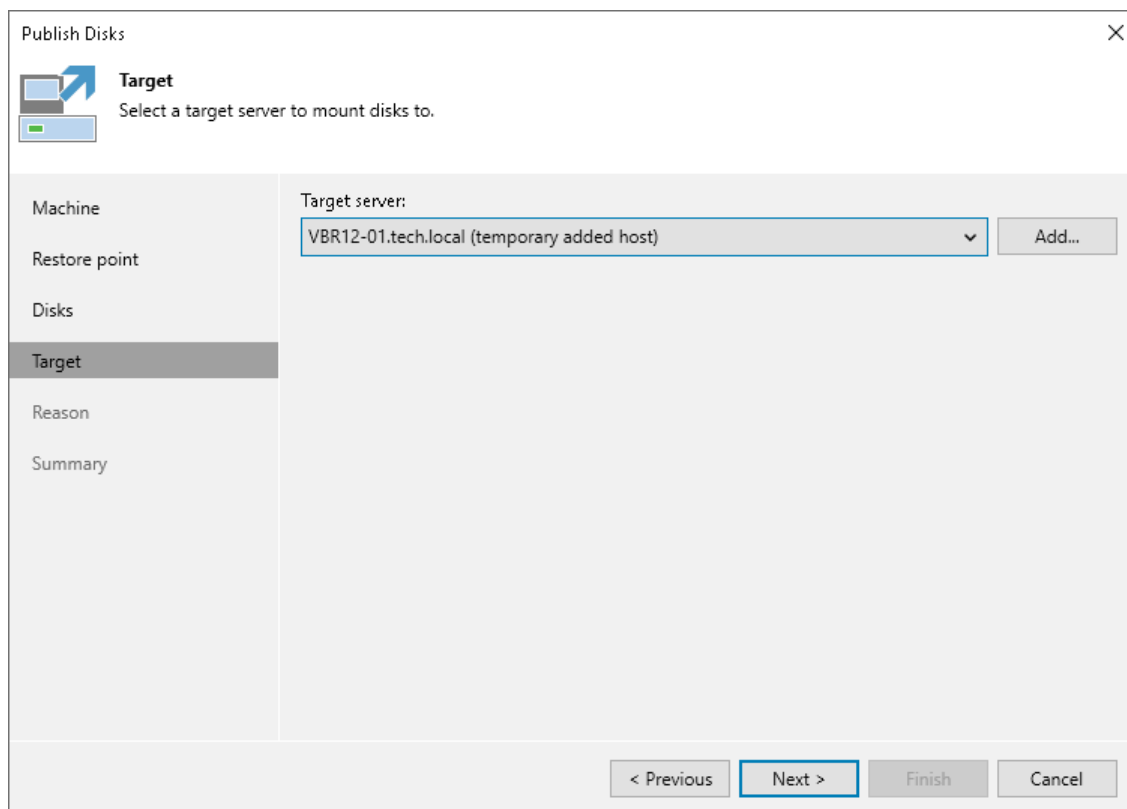
You can select one of the following types of servers:

- A server added to the backup infrastructure.

If you want to add a new backup server to the backup infrastructure at this step, click **Add**. In this case, you will be able to add a new Linux server. To learn more, see the [Adding Linux Servers](#) section in the Veeam Backup & Replication User Guide.

- A temporary server. In this case, select *Specify a different host* from the drop-down list. In the **Target Server** window, specify the following settings:
 - a. In the **Host name** field, specify a server name or IP address of the server.
 - b. Select the account from the **Credentials** list. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add a new account in the Credentials Manager. To learn more, see the [Credentials Manager](#) section in the Veeam Backup & Replication User Guide.
 - c. Click **Advanced** and customize connection settings in the **Network Settings window**. To learn more, see [Customizing Connection Settings](#).

If prompted, specify credentials for the target server.



The screenshot shows the 'Publish Disks' wizard window, specifically the 'Target' step. The window title is 'Publish Disks' and it has a close button (X) in the top right corner. Below the title bar, there is a 'Target' section with a blue arrow icon and the text 'Select a target server to mount disks to.' On the left side, there is a vertical navigation pane with the following items: 'Machine', 'Restore point', 'Disks', 'Target' (which is highlighted), 'Reason', and 'Summary'. The main area of the window is titled 'Target server:' and contains a dropdown menu with the selected value 'VBR12-01.tech.local (temporary added host)' and a small downward arrow. To the right of the dropdown is an 'Add...' button. At the bottom of the window, there are four buttons: '< Previous', 'Next >' (which is highlighted with a blue border), 'Finish', and 'Cancel'.

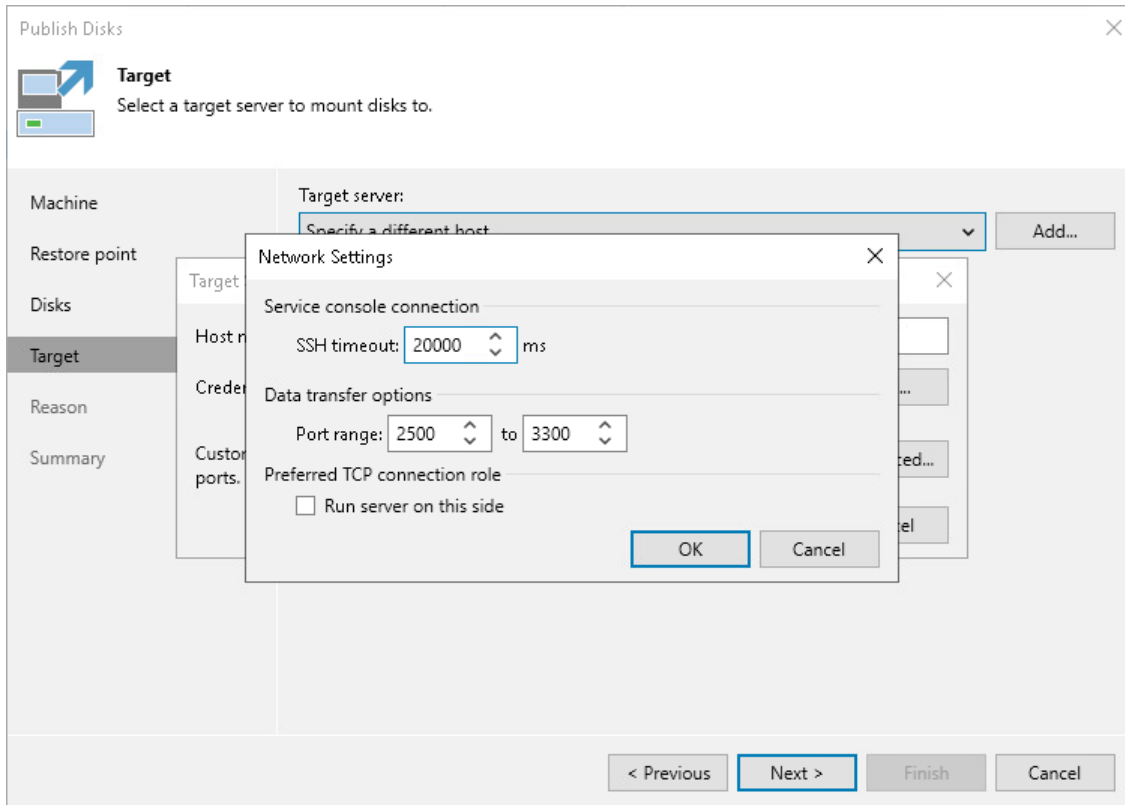
Customizing Connection Settings

If necessary, you can customize connection settings for a target Linux server at the **Target** step of the **Publish Disks** wizard. To do so, click **Advanced** in the **Target Server** window and specify settings in the **Network Settings window**:

1. In the **Service console connection** section, specify an SSH timeout.

2. In the **Data transfer options** section, specify connection settings for file copy operations.
3. [For Linux server deployed outside NAT] In the **Preferred TCP connection role** section, select the **Run server on this side** check box.

To learn more about these settings, see the [Specify Credentials and SSH Settings](#) section in the Veeam Backup & Replication User Guide.

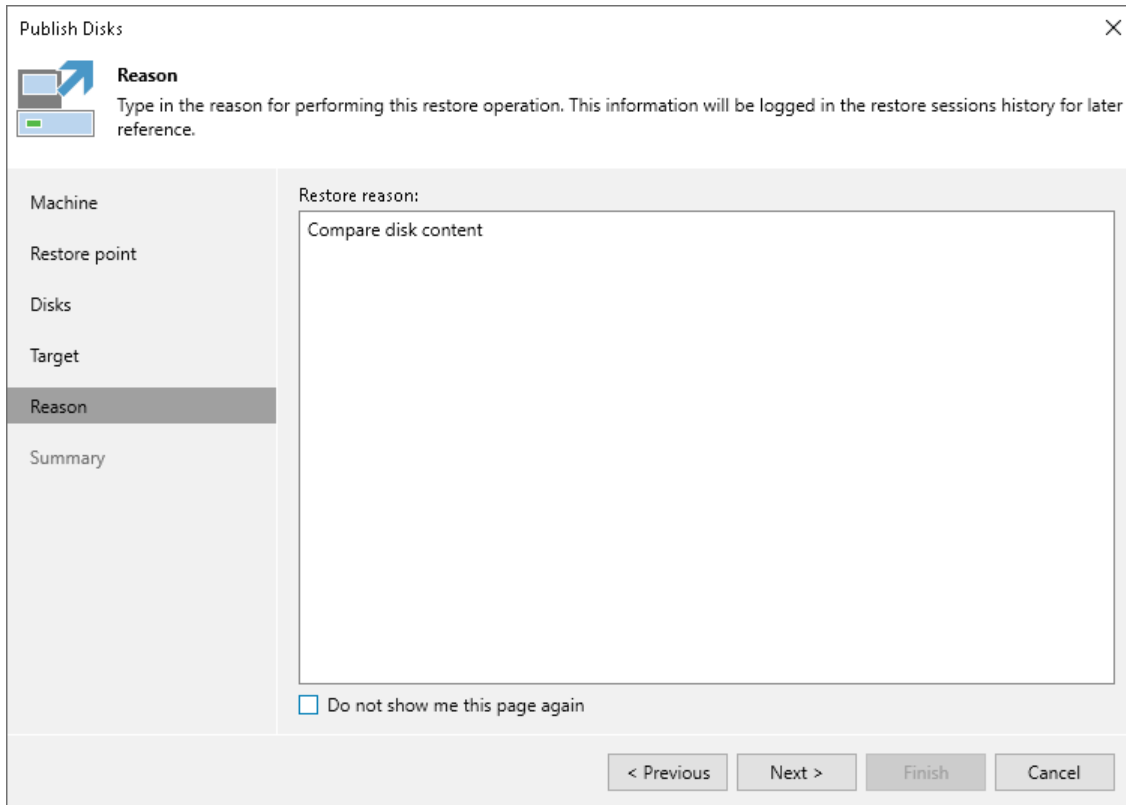


Step 6. Specify Restore Reason

At the **Reason** step of the wizard, enter a reason for publishing disks.

TIP

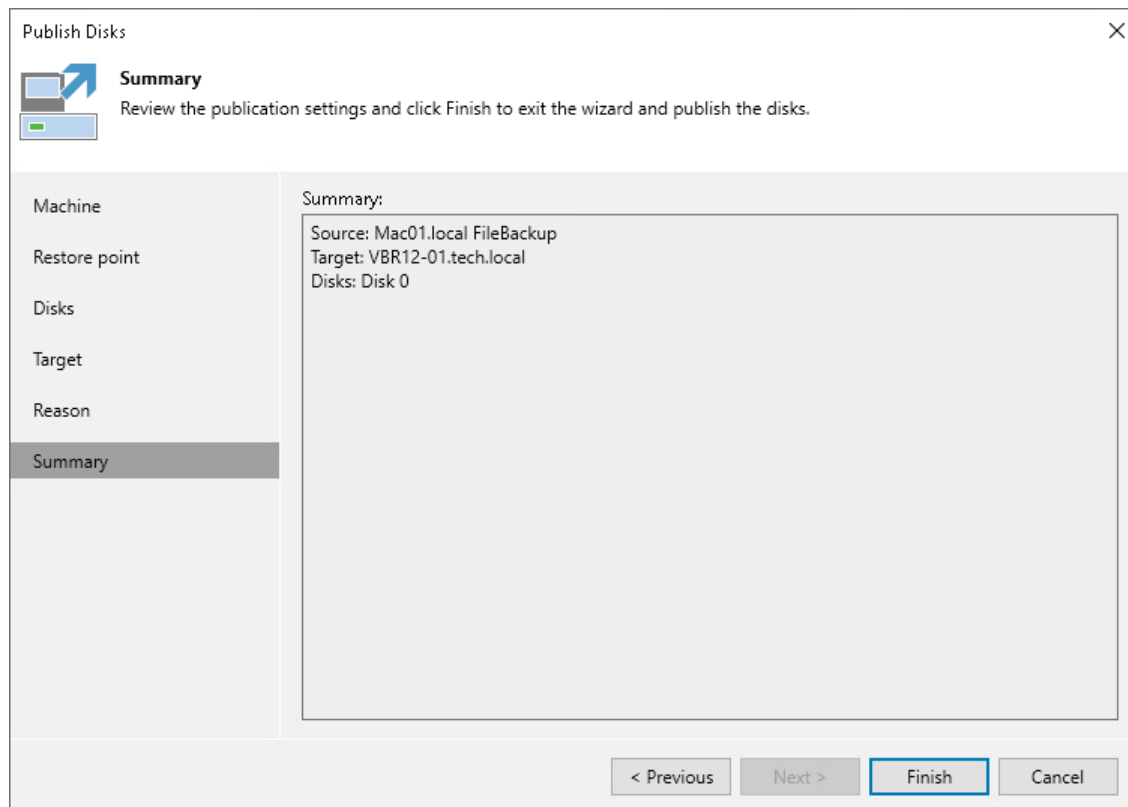
If you do not want to show this page, select the **Do not show me this page again** check box. If you further will want to return this page, follow the instructions described in [this Veeam KB article](#).



The screenshot shows the 'Publish Disks' wizard window. The title bar reads 'Publish Disks' with a close button (X) on the right. Below the title bar is a navigation pane on the left with the following items: Machine, Restore point, Disks, Target, Reason (highlighted), and Summary. To the right of the navigation pane, there is a 'Reason' section with a sub-header 'Reason' and a description: 'Type in the reason for performing this restore operation. This information will be logged in the restore sessions history for later reference.' Below this is a large text area labeled 'Restore reason:' containing the text 'Compare disk content'. At the bottom left of the main area is a checkbox labeled 'Do not show me this page again'. At the bottom right are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 7. Finish Working with Wizard

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



What You Do Next

After the disks are published, go to the following locations on the target server to browse disks content:

- Go to the `/tmp/Veeam.Mount.Disks` location to browse disks images.
- Go to the `/tmp/Veeam.Mount.FS` location to browse disks content.

After you started a disks publishing session, you can view the session statistics or stop the session from the Veeam backup console. To learn more, see [Managing Publishing Disks Session](#).

Managing Publishing Disks Session

After you started a publishing session, you can check details about the session or stop it.

Viewing Statistics on Publishing Session

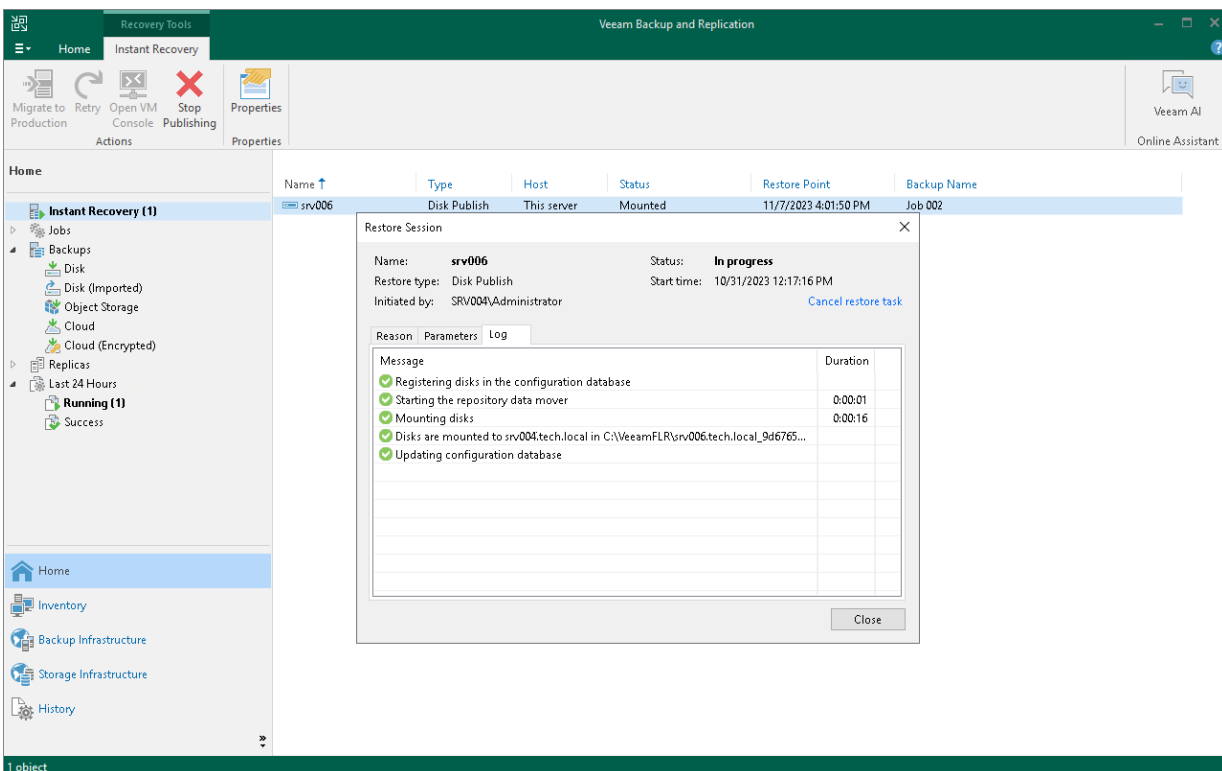
To view publishing session statistics, do one of the following:

- Open the **Home** view. In the inventory pane, select **Instant Recovery**. In the working area, select the necessary publishing session and click **Properties** on the ribbon. Alternatively, right-click the session and **Properties**.
- Open the **Home** view. In the inventory pane select **Last 24 hours**. In the working area, double-click the necessary publishing session. Alternatively, you can select the session and click **Statistics** on the ribbon or right-click the session and select **Statistics**.

- Open the **History** view. In the inventory pane select **Restore**. In the working area, double-click the necessary publishing session. Alternatively, you can select the session and click **Statistics** on the ribbon or right-click the session and select **Statistics**.

The publishing statistics provides the following data:

- At the top of the **Restore Session** window, Veeam Backup & Replication shows general session statistics. It includes a name of the Veeam Agent computer whose disk you want to publish, a name of the backup server which initiated the publishing session, a user name of the account under which the session was started, session status and duration details.
- The **Reason** tab shows the reason for the publishing session.
- The **Parameters** tab shows information about the target server, the Veeam Agent computer whose disks you publish and the restore point selected for publishing.
- The **Log** tab shows the list of operations performed during the session.

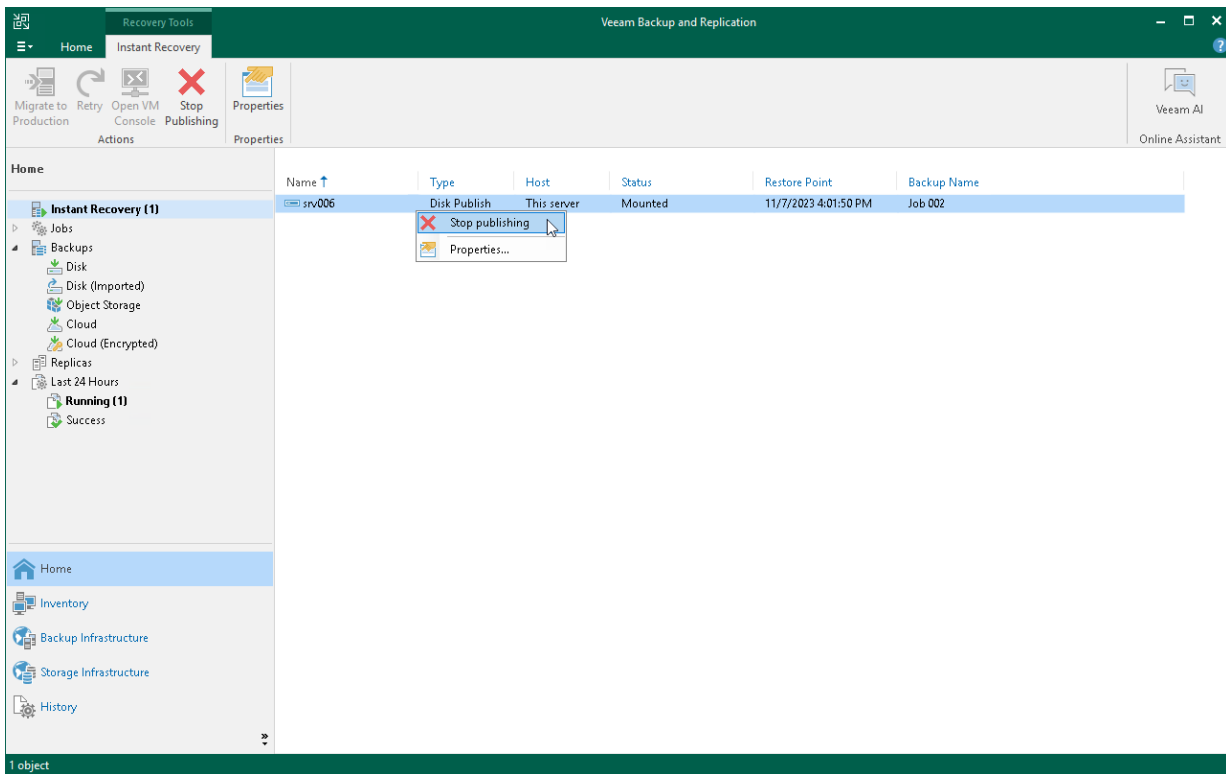


Stopping Publishing Session

To stop a publishing session, do one of the following:

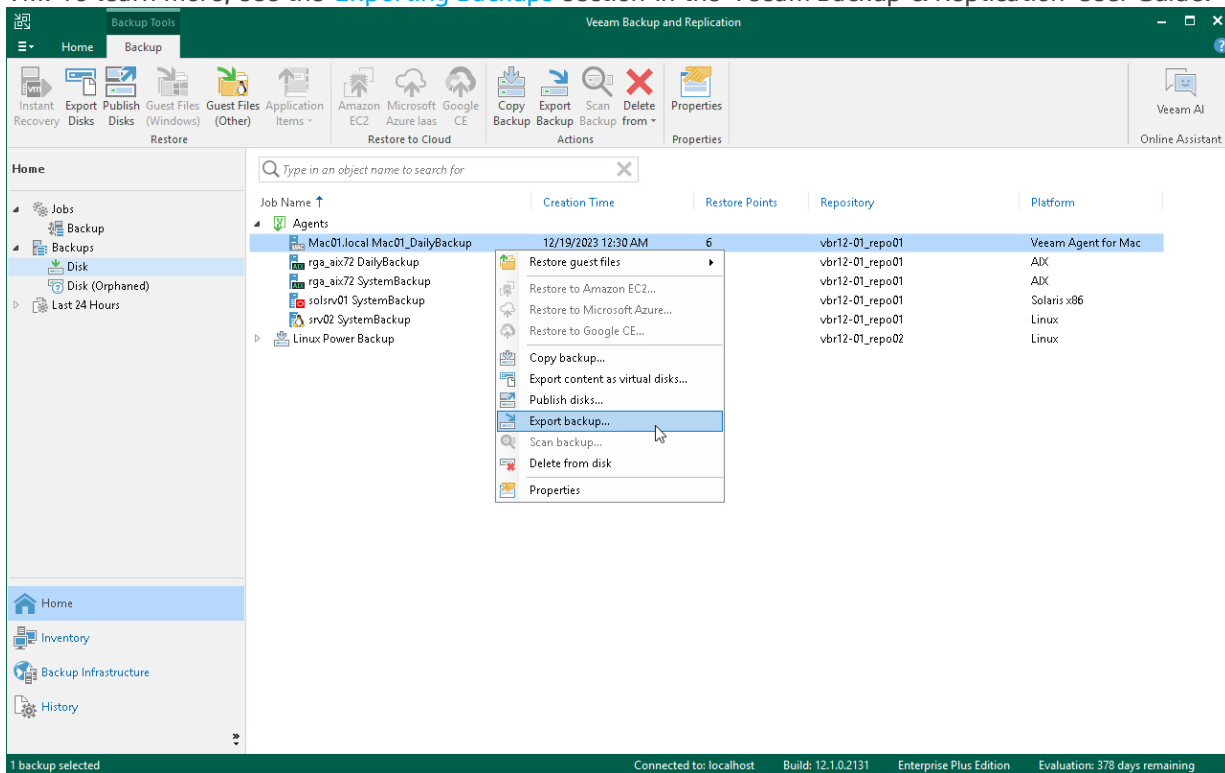
- Open the **Home** view. In the inventory pane select **Instant Recovery**. In the working area, double-click the necessary publishing session and click **Cancel restore task** in the **Restore Session** window. Alternatively, you can select the necessary publishing session and click **Stop Publishing** on the ribbon or right-click the session and click **Stop Publishing**.
- Open the **Home** view. In the inventory pane select **Last 24 hours**. In the working area, double-click the necessary publishing session and click **Cancel restore task** in the **Restore Session** window. Alternatively, you can select the necessary publishing session and click **Stop** on the ribbon or right-click the session and click **Stop session**.

- Open the **History** view. In the inventory pane select **Restore**. In the working area, select the necessary publishing session and double-click it. In the **Restore Session** window, click **Cancel restore task**. Alternatively, you can right-click the publishing session and click **Stop session**.



Exporting Restore Point to Full Backup File

You can restore data from a specific restore point in a Veeam Agent backup and export this data to a standalone full backup file. The procedure of Veeam Agent backup export does not differ from the same procedure for a VM. To learn more, see the [Exporting Backups](#) section in the Veeam Backup & Replication User Guide.



Performing Administration Tasks

You can manage Veeam Agent backup jobs and backups created with these jobs. Veeam Backup & Replication allows you to perform the following administration tasks:

- [Import Veeam Agent backups.](#)
- [Enable and disable Veeam Agent backup jobs.](#)
- [Delete Veeam Agent backup jobs.](#)
- [View Veeam Agent backup properties.](#)
- [Remove Veeam Agent backups.](#)
- [Delete Veeam Agent backups.](#)
- [Configure global settings.](#)
- [Assign roles to users.](#)

Importing Veeam Agent Backups

You may need to import a Veeam Agent backup in the Veeam Backup & Replication console in the following situations:

- The Veeam Agent backup is stored on a drive managed by another computer (not the Veeam backup server).
- The Veeam Agent backup is stored in a backup repository managed by another Veeam backup server.
- The Veeam Agent backup has been removed in the Veeam Backup & Replication console.

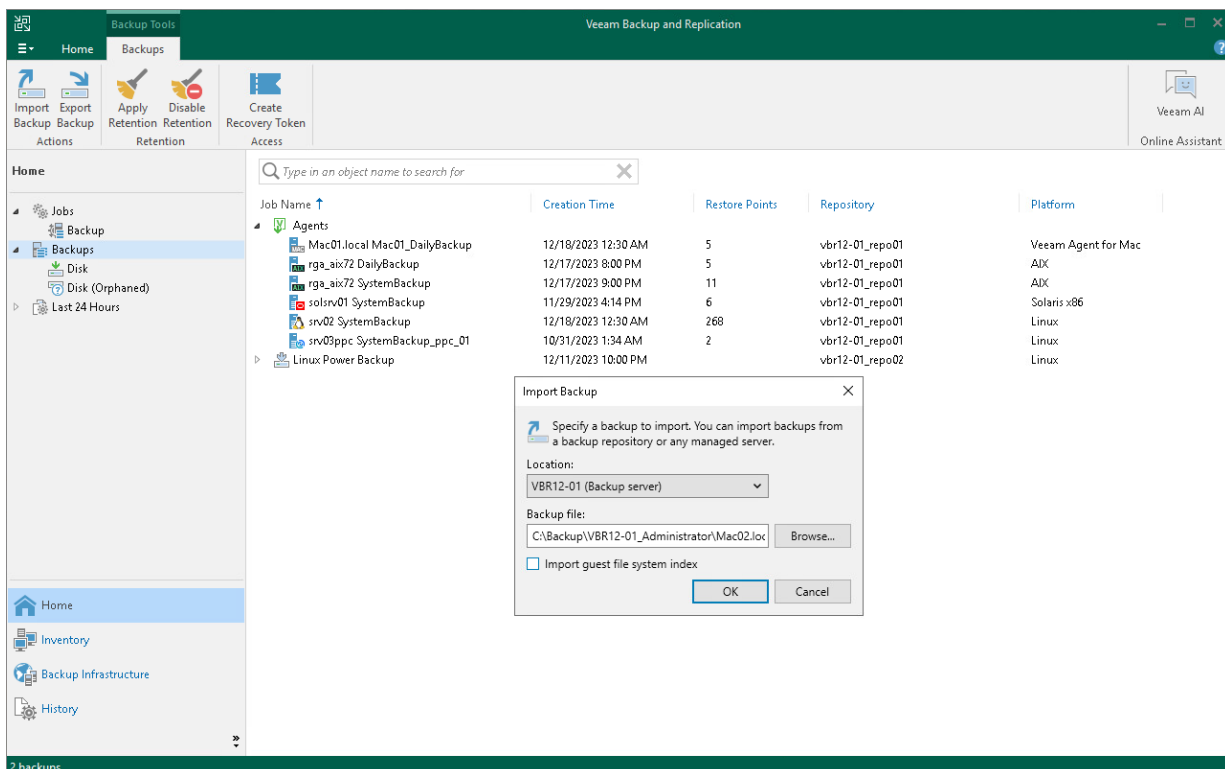
After importing, the Veeam Agent backup becomes available in the Veeam Backup & Replication console. You can restore data from such backup in a regular manner.

Before importing a backup, check the following prerequisites:

- The computer or server from which you plan to import the backup must be added to Veeam Backup & Replication. Otherwise you will not be able to access backup files.
- To be able to restore data from previous backup restore points, make sure that you have all incremental restore points in the same folder where the full backup file resides.

To import a Veeam Agent backup:

1. In Veeam Backup & Replication, click **Import Backup** on the **Home** tab.
2. From the **Computer** list, select the computer or server on which the backup you want to import is stored.
3. Click **Browse** and select the necessary VBM or VBK file. If you select the VBM file, the import process will be notably faster. We recommend that you use the VBK files for import only if a corresponding VBM file is not available.
4. Click **OK**. The imported backup will become available in the **Home** view, under the **Backups > Disk (imported)** node in the inventory pane.



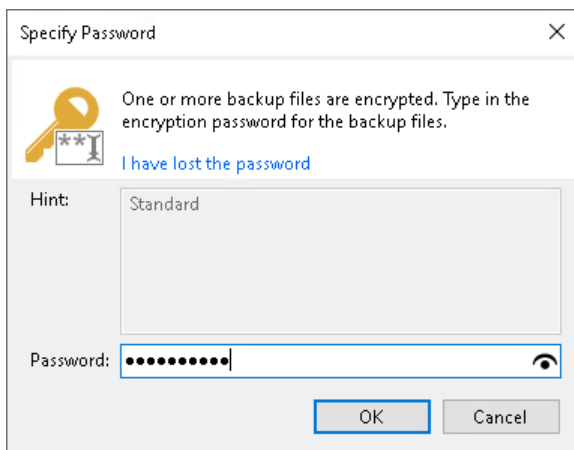
Importing Encrypted Backups

You can import Veeam Agent backups that were encrypted by Veeam Backup & Replication or Veeam Agent for Microsoft Windows.

To import an encrypted backup file:

1. On the **Home** tab, click **Import Backup**.
2. From the **Computer** list, select the host on which the backup you want to import is stored.
3. Click **Browse** and select the VBM or VBK file.
4. Click **OK**. The encrypted backup will appear under the **Backups > Disk (encrypted)** node in the inventory pane.
5. In the working area, select the imported backup and click **Specify Password** on the ribbon, or right-click the backup and select **Specify password**.
6. In the **Password** field, enter the password for the backup file. If you changed the password one or several times while the backup chain was created, you need to specify the latest password. For Veeam Agent backups, 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.

If you enter correct password, Veeam Backup & Replication will decrypt the backup file. The backup will be moved under the **Backups > Disk (imported)** node in the inventory pane.



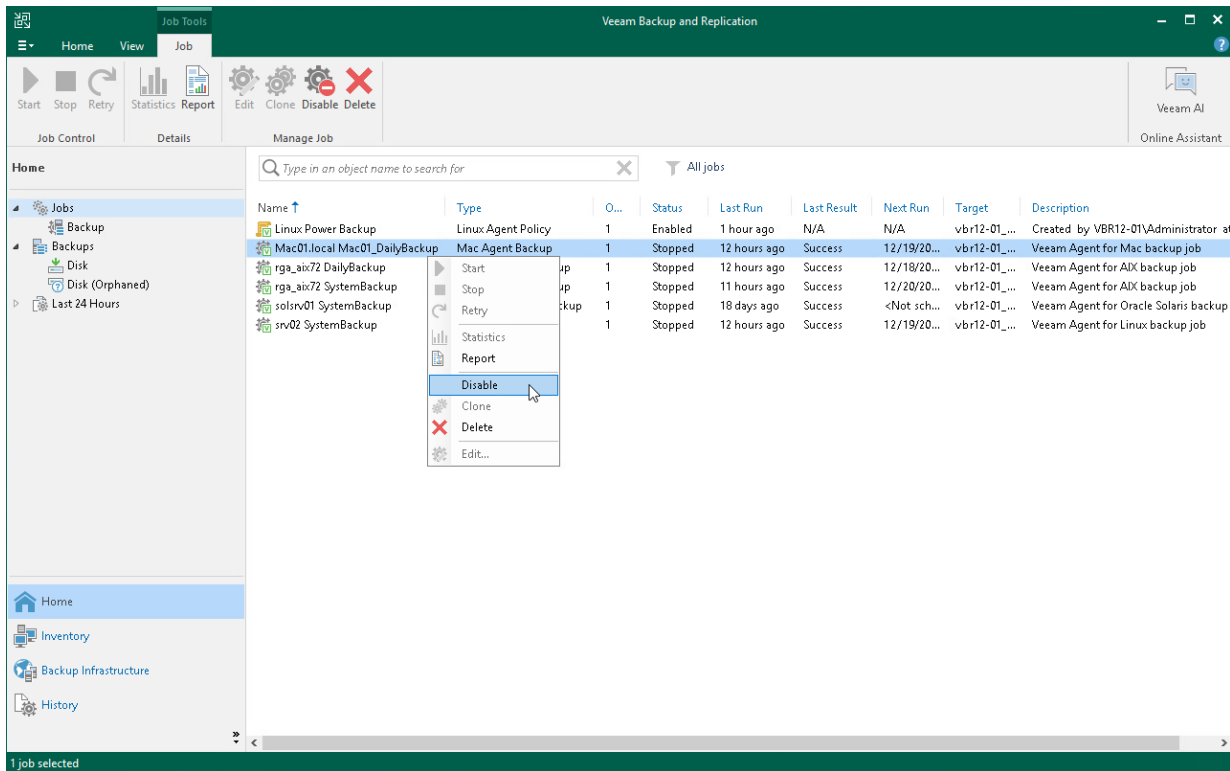
Enabling and Disabling Veeam Agent Backup Jobs

You can disable and enable Veeam Agent jobs in Veeam Backup & Replication.

When you disable the job, you prohibit the user to store the resulting backup in the backup repository. If the user starts a disabled job manually or the job starts by schedule, the job session will fail and report the "*Job is disabled on backup server*" error. To let Veeam Agent store backups in the backup repository again, you must enable the disabled job.

To disable or enable the scheduled backup job in Veeam Backup & Replication:

1. In Veeam Backup & Replication, open the **Home** view.
2. In the inventory pane, click the **Jobs** node.
3. Select the necessary job in the working area and click **Disable** on the ribbon, or right-click the necessary job in the working area and select **Disable**. To enable the disabled job, click **Disable** on the toolbar, or right-click the job and select **Disable** once again.



Viewing Veeam Agent Backup Job Statistics

You can view statistics about Veeam Agent backup jobs in the Veeam Backup & Replication console. Veeam Backup & Replication displays statistics for Veeam Agent backup jobs in the similar way as for regular backup jobs. The difference is that the list of objects included in the job contains a Veeam Agent machine instead of one or several VMs.

To view Veeam Agent backup job statistics:

1. In Veeam Backup & Replication, open the **Home** view.
2. In the inventory pane, click the **Jobs** node.
3. In the working area, select the necessary Veeam Agent backup job and click **Statistics** on the ribbon, or right-click the job and select **Statistics**.

The screenshot displays the Veeam Backup and Replication console interface. The main window shows the job details for 'Mac01.local Mac01_DailyBackup'. The job progress is 100% complete for 1 of 1 hosts. The summary table shows a duration of 06:50, a processing rate of 1 MB/s, and a bottleneck of Proxy. The data section indicates that 3 GB (100%) was processed, 412.6 MB was read, and 572.2 MB (0.7%) was transferred. The status section shows 1 success, 0 warnings, and 0 errors.

Summary	Data	Status
Duration: 06:50	Processed: 3 GB (100%)	Success: 1 ✓
Processing rate: 1 MB/s	Read: 412.6 MB	Warnings: 0
Bottleneck: Proxy	Transferred: 572.2 MB (0.7%)	Errors: 0

THROUGHPUT (ALL TIME)

Name	Status	Action	Duration
Mac01.local	Success	Job Mac01_DailyBackup started at 2024-01-11 23:32:07 UTC	
		Preparing to backup	
		Waiting for backup infrastructure resources availability	00:01
		Creating volume snapshot	
		Starting incremental backup to [VBR12-01] vbr12-01_repo01	
		Backing up summary.xml	
		Backing up files /Users/admin/Public, /Users/admin/Pictures, /Users/admin/Movies, /Users/admin/D...	06:21
		Backing up summary.xml	
		Releasing snapshot	
		Applying retention policy	00:18
		Required backup infrastructure resources have been assigned	
		Full backup file merge completed successfully	00:03
		Processing finished at 2024-01-11 23:38:59 UTC	

Deleting Veeam Agent Backup Jobs

You can delete Veeam Agent backup jobs.

When you delete a Veeam Agent backup job, Veeam Backup & Replication removes all records about the job from its database and console. When the user starts a new Veeam Agent backup job session manually or the job starts automatically by schedule, the job will appear in the Veeam Backup & Replication console again, and records about a new job session will be stored in the Veeam Backup & Replication database.

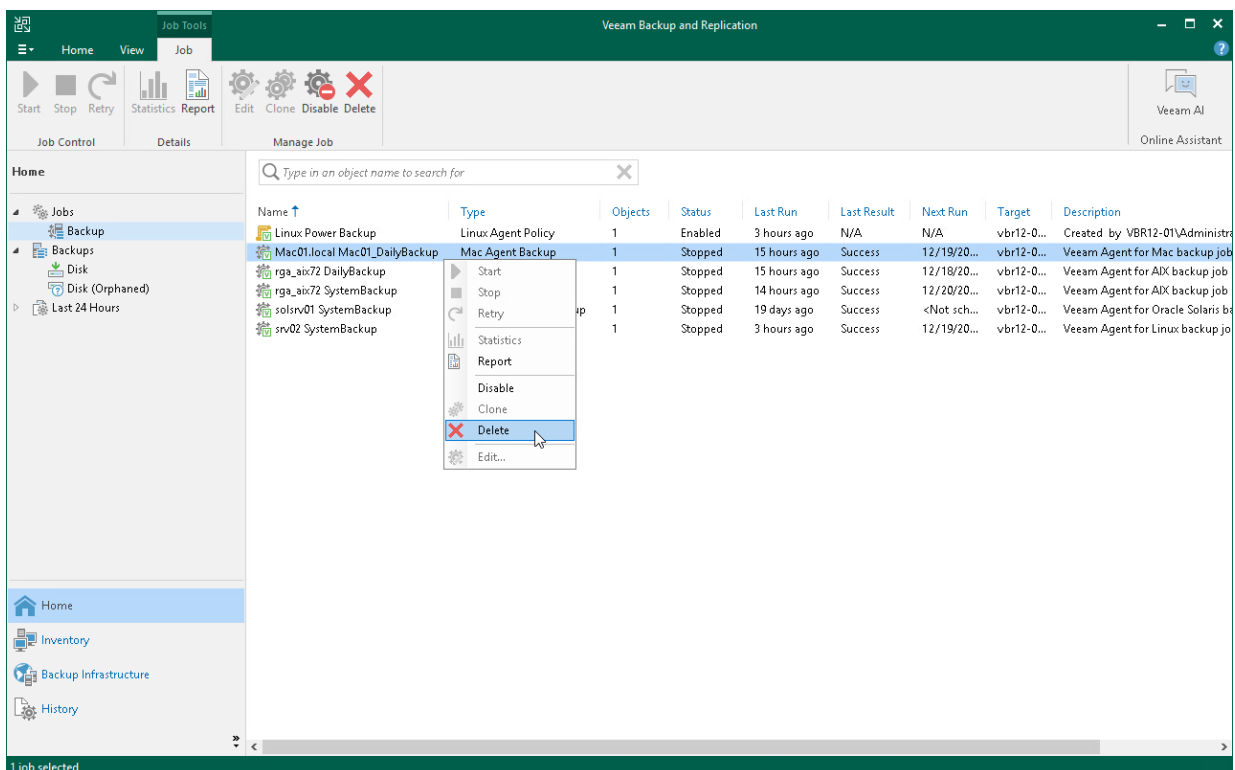
NOTE

When you delete a Veeam Agent backup job, the backup files become orphaned and can be deleted by the background retention. For more information about the background retention, see the [Background Retention](#) section in the Veeam Backup & Replication User Guide.

To prevent the job from starting permanently, you must delete the job and unassign access rights permissions for this user from the backup repository. To completely delete the job, you must perform this operation in Veeam Agent on the Veeam Agent machine.

To remove a job:

1. In Veeam Backup & Replication, open the **Home** view.
2. In the inventory pane, click the **Jobs** node.
3. Select the necessary job in the working area and click **Delete** on the ribbon, or right-click the necessary job in the working area and select **Delete**.



Viewing Veeam Agent Backup Properties

You can view statistics about Veeam Agent backups.

To view Veeam Agent backup statistics:

1. In Veeam Backup & Replication, open the **Home** view.
2. In the inventory pane, click **Disk** under the **Backups** node.
3. In the working area, expand the **Agents** node, select the necessary backup and click **Properties** on the ribbon, or right-click the backup and select **Properties**.

The screenshot displays the Veeam Backup & Replication interface. The 'Home' view is active, and the 'Agents' node is expanded in the inventory pane. A 'VM Backup Properties' dialog box is open, showing details for the 'Mac01.local Mac01_DailyBackup'.

VM Backup Properties: Mac01.local Mac01_DailyBackup

Object: Mac01.local Mac01_DailyBackup
Repository: vbr12-01_repo01
Owner: VBR12-01\Administrator
Folder: C:\Backup\VBR12-01\Administrator\Mac01.local Mac01_DailyBackup\

Name	Data Size	Backup Size	Date
Mac01_DailyBackup_2023-12-18T003014.vib	806 MB	396 MB	12/18/2023 12:30:14 AM
Mac01_DailyBackup_2023-12-17T003007.vib	805 MB	420 MB	12/17/2023 12:30:07 AM
Mac01_DailyBackup_2023-12-16T003015.vib	829 MB	395 MB	12/16/2023 12:30:15 AM
Mac01_DailyBackup_2023-12-15T003007.vib	919 MB	388 MB	12/15/2023 12:30:07 AM
Mac01_DailyBackup_2023-12-14T180013.vbk	1.00 TB	2.40 GB	12/14/2023 6:00:13 PM

Backup size: 3.97 GB

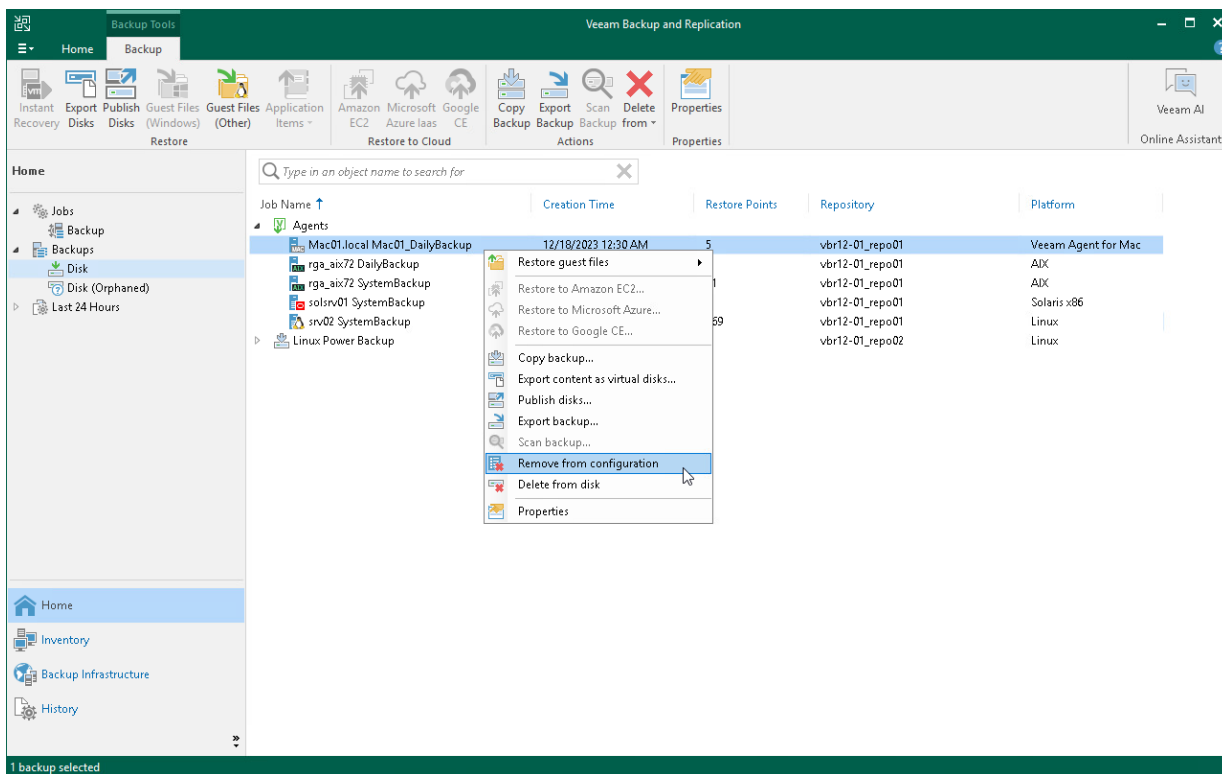
Removing Veeam Agent Backups

If you want to remove records about Veeam Agent backups from the Veeam Backup & Replication console and configuration database, you can use the **Remove from configuration** operation. When you remove a Veeam Agent backup from configuration, the actual backup files remain in the backup repository. You can import the backup to the Veeam Backup & Replication at any time later and restore data from it.

IMPORTANT

Removing backups from configuration is designed for experienced users only. Consider using the [Delete from disk](#) operation instead.

1. Open the **Home** view.
2. In the inventory pane, click **Backups**.
3. Press and hold the [Ctrl] key, select the backup, right-click the backup and select **Remove from configuration**.

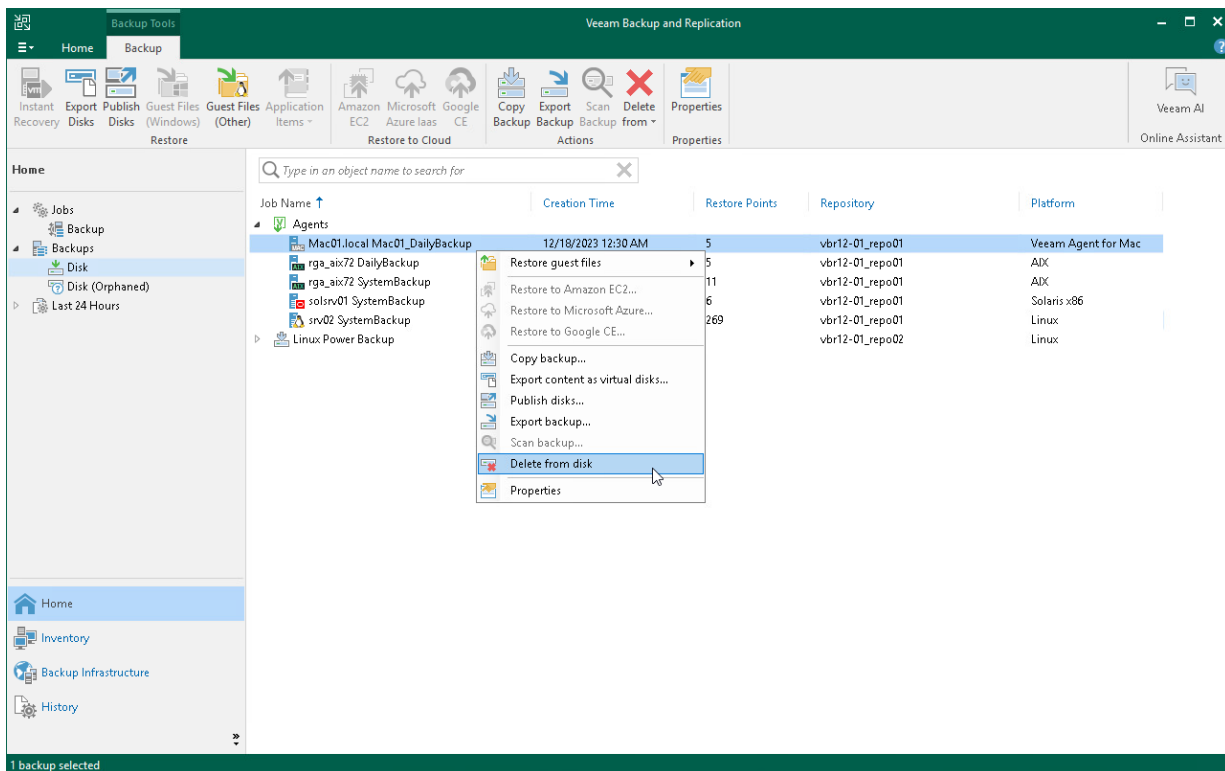


Deleting Veeam Agent Backups from Disk

If you want to delete records about backups from the Veeam Backup & Replication console and configuration database and, additionally, delete backup files from the backup repository, you can use the **Delete from disk** operation.

To remove a Veeam Agent backup from the backup repository:

1. Open the **Home** view.
2. In the inventory pane, click **Backups**.
3. Select the necessary computer backup and click **Delete from > Disk** on the ribbon or right-click the computer and select **Delete from disk**.



Configuring Global Settings

Global settings configured on the Veeam backup server apply to Veeam Agent backup jobs as well. You can:

- Configure network throttling settings so that Veeam Agent backup job does not consume all network resources. To learn more, see the [Specifying I/O Settings](#) topic in the Veeam Backup & Replication User Guide.
- Configure the following global notification settings to get alerted about the Veeam Agent backup job results:
 - Email notifications. To learn more, see the [Specifying Email Notification Settings](#) section in the Veeam Backup & Replication User Guide.
 - SNMP notifications. To learn more, see the [Specifying SNMP Settings](#) section in the Veeam Backup & Replication User Guide.

Assigning Roles to Users

User roles configured on the Veeam backup server apply to Veeam Agent backup jobs as well.

To learn more, see the [Users and Roles](#) section in the Veeam Backup & Replication User Guide.

Appendix A. Deploying Device Profile with MDM Solution

With the MDM solution, you can connect Veeam Agent to Veeam backup server and include Veeam Agent computer in the protection group in Veeam Backup & Replication. To do this, 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 Jamf Pro, 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 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.apple.ManagedClient.preferences</string>
        <key>PayloadUUID</key>
        <string>d463e322-c696-0000-87d0-0242ac130003</string>
        <key>PayloadIdentifier</key>
        <string>com.veeam.Agent.managedsettings.d463e322-c696-11ea-0000-
0242ac130003</string>
        <key>PayloadEnabled</key>
        <true />
        <key>Identifier</key>
        <string>com.veeam.Agent</string>
        <key>IdentifierType</key>
        <string>bundleID</string>
        <key>PayloadContent</key>
        <dict>
          <key>com.veeam.Agent</key>
          <dict>
            <key>Forced</key>
            <array>
              <dict>
                <key>mcx_preference_settings</key>
                <dict>
                  <key>CatchAllConfig</key>
                  <string>&lt;?xml version="1.0" &gt;
&lt;ManagementServerConfiguration Version="1" VbrInstallationId="
t;55ab5848-9c72-4fc0-8c00-d07874d65592" Certificate="MIICcQIBAzCCCjEG
CSqGSIB3DQEHAaCCciIEggoeMIIKgjCCBgEGCSqGSIB3DQEHAaCCBfIEggXuMIIIF6jCCBeYGCyqGSIB
3DQEMCGeCoIIE9jCCBPIwHAYKKoZIHvcNAQwBAzA0BAG9q017ZQXykAICB9AEggTQ/3FXreQ5Mm1OoT
wiRbiMq6k3+HK4sZPDKuSp00OzHQrrPa+Ztr/ElF2Ci0pozDdsQgF3FWzWwZ1XMC9spte0ztlqKqw1j
IjvINJEbfIN/OgtFHY5vjSkv0ltCdF6iQ0hL5R1yt/RZp79q1QR9BlpMpcGtOmksWl4AnBexOBhzSSU
HC5xBM7FprUTfXC0JoP8884o9jVLNTPn18QRRKbVbamoK2ETK7Mesr9X7dqKBlaxKgzYk6qinJAKfch
nIi0hFs/W9OxIsr6wIt9BHNh765wVefsGWWqVh9cYfu0F1EPH0IzyVTpMtPeUkhKZoeSlFBuwDbump5
AElkO3P3sxaUJ2wokDyix4EqTlifrVjLCUqnx6v/kM1hbxt+XikOPuABv6KQHaEEYtLr05JbdCFkqe
i9afWR493SHo75kJG9hg/cIqhLKSspI7Fzyj8hk027azkmoobH1GCU+vt0wXBy+Qztx00FUJ1MDrp80
jjvg74LWmhCuhw9QCnt/Q0xSw+G4SA7dFuc8pVew78ViHivvinQYfXi2++9cFVDAKM29MVxiH87OKri
wGBetcr3fRAsx2mMPTJM2cwRyGFT8jB2hmaRN1+7cm83g08z69C9C335cJFahDdG5YQzYpyquyUcQbi

```

```

DJlKBe6f54XgqIDhFfdhLXZr9AWVLjuVc7t8zUBQQB04o1pfJyCoqqSgiMts819zBqzoWn7Ezr9sM7x
8DNlA5Q8qFPneWSM0ke3MBgNZclTffGP41c0RQH+/7FS3+bulEWEoshs4k+mNfXamCNgEGVZyucbKMO
PpduckxCQJJStaWS4ITSCE5rO3tZz6oR9zx63hpQ0ps6E3eEoCjqdapSptBn92aW9LoPjdvkj/NOrKM
9njOAr4cbPCdU+gsqZ4wnd4jJppww7amHYOQmwz0ncld0EVlu5Oxmy/2rQIZju+qEmEEExbH7fs9rEWR
7w+8gYHSt99FWyfqN5NN9HwOdwPK4c8lH1VvNjpuSdlzn2rPismqsrAaGw2ZbjwuYJnA0HQWUa26cXe
WXtcyoPX3bkC49tj6UuUNAP7RLTydCEhMl/bJi+A6yVgFhq8s5tbaTNxdH3cIsoTDDOTM7XeMooYzKH
+gvW2KPg8gmmncjAhcwk7EPD0iQ39Md1Z+mNuj3lHNJo+esL0zjJEW7vLoEFA/nH9Fcd183vNDw/24Y
503w6xBkO0fKp0vXP7fj5WGk6F0QQKgjwQuhZBnrnGyPbCb/aGGQYYOLHsOvHuezIFzas7snnOJz060
5d7HEayJsJfIP1GAGZCF3uahi57+hv4AeCM2vGaQ2x1l2CRWtd8+QpCSiJOLeVfXifNbH2XXyLxda40
mqm9mg1UFeZhgm33wgY8pz7oXH/L8Q6C53EN4qW/FG2J+tiH3EafUngqvLi/5tKgnbMTxPAb6ErIp0
2xEKMO1tgh3zwe5BG9a2L5swQVAIQ1zTQz84EyE+cTmc9gcnRMtaTh+8OARYq4PIphppCUi/h+Tp+Vg
3XDOTVRPxD09GEFBvyyGY2FfJob0ED1Kz/dBaNbGv1mzlBv+ZHgkt9w7mEheKrNeNC0mqGNaEMxJVrs
2DbyIjn84MiqCaCCSw7RSjof5rp3CZtft27R0LV3a+3ULZ4vN4xgdwwDQYJKwYBBAGCNxECMQAwEwYJK
oZIHvcNAQkVMQYEBAAAAAwVwYJKoZIHvcNAQkUMUoeSAA3ADcANwA5ADkAZQAwADMALQAYAGEANQA4
AC0ANAA5ADAAMAAtAGIAMgA4ADMALQBkADUAZAAyADcAZQA5ADYANQBlADAAMjBdBgkrBgEEAYI3EQE
xUB5OAE0AaQBjAHIAbwBzAG8AZgB0ACAAUwB0AHIAbwBuAGCAIABDAHIAeQBwAHQAbwBnAHIAYQBwAG
gAaQBjACAUAUByAG8AdgBpAGQAZQByMIIEEQYJKoZIHvcNAQcBoIIEAgSCA/4wggP6MIID9gYLKoZIH
vcNAQwKAQOgggMnMIIDIWYKKoZIHvcNAQkWAaCCAXMEggMPMIIDCzCCAfoGawIBAgiQ1cDZIQD+u5BL
YXDQAUIBNzANBqkqhkig9w0BAQsFADAqMSgwJgYDvQDQEx9WZwVhSBcyWNRdXAgU2VydmVyIENlcnR
pZmljYXRlMB4XDTIwMDIwMzIyMDIwMVoXDTMxMDIwNDIyMDIwMVoLzEtMCSGA1UEAxMkOGU1YzA1ND
UtNjcZC00MTgzLWE3ZWQtNGZkZWQ1MGMyZW5kMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCA
QEAvijLF2aptEqBkorf3HWYUhyqUcbRUfwPX/OFOy7y42xoCLP0ZS9iD9v1Xem08BTG0uxCCzwROg4I
shhziNzKPHnqh7WWR5CXL48QhB6Wjeyut5TNQ/93+J9A/6444w6hlZhaW3TlXm/LzWBHO8PwOpV1ivh
ro27ZujLzmWqr/CBbeT6h3WkteImdExGxTaBMXFDZ46xMzPC1+xOftGtla+0mF0rBGE+koNH6GtUFn0
oWLnDrp4ul5cp9IDeiZ7wEAoK1ncEipm6dSurdkIS28ChsVs2ma+3XWcF0Bn0zYjzQvC3BdLghxwmOn
76ethmyOd5eD2211WMT4IXgPZlDMwIDAQABoygwJjAMBgNVHRMBAf8EAjAAMBYGA1UdJQEB/wQMMAoG
CCsGAQUFBwMCMA0GCSqGSIb3DQEBCwUAA4IBAQCIC88hSgWQW3Y2xHcytamvtAEfzBg8FzvvX9w3RjE
qXTS982nTbfnUgg41p9bmsflWno4ovuvovzVaSFEgg/ezwpBO2Ma42DjD59cS5DTJMaEOt7bZFeisMu
cRV9RN8PTD0fxZ0vGGu+m4C6/QyHPY0chcMQkNR62bVzAjElUM4xuxiKZ7hjAvcpO+XkazP18bG11SV
wVh45M4hDOV9kMhQeaCJCSMFjx+kvbnEKxOxt00jfaMoQPfc6/wXZLbN4eyLAU5Bz2ik4t+W0pnrP4i
qdGIWqJJis8nggq11h3zEuETDzToX5hLSReKnVbtQ7QCUR3HGO9RE+i4YIz2ZK4TMYG7MBMGCSqGSib
3DQEJFTEGBAQBAAMIGjBqkqhkiG9w0BCRQxgZUegZiAVgBlAGUAYQBtACAAUABYAG8AdABLAGMAdA
BpAG8AbgAgAeAcAgBvAHUAcAAgAEMAZQByAHQAaQBmAGkAYwBhAHQAZQA6ACAAOABLADUAYwAwADUAN
AA1AC0ANgA3ADMAZAAtADQAMQA4ADMALQBhAdcAZQBkAC0ANABMAGQAZQBkADUAMABjADIAZQBjAGQA
ADA3MB8wBwYFKw4DAhoEFEE55t3wm2wBYKJKVksil9Gfh7mEqOBBQC4HITsGLIn6j7ccbCVeVmEM/jJg=
=&quot; ; VbrVersion=&quot;11.0.0.810&quot; ; &gt; &lt; ; VbrConnectionInfo ServerName=&
quot;PT11&quot; ; Port=&quot;10006&quot; ; &gt; &lt; ; IpAddresses&gt; &lt; ; String value=&
quot;172.24.166.86&quot; ; /&gt; &lt; ; /IpAddresses&gt; &lt; ; /VbrConnectionInfo&gt; &lt;
; SelfDiscoveryOptions /&gt; &lt; ; VbrCatchAllInfo /&gt; &lt; ; /ManagementServerConfig
uration&gt; </string>

```

```

</dict>
</dict>
</array>
</dict>
</dict>
</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
```

